

This document is made available through the declassification efforts
and research of John Greenewald, Jr., creator of:

The Black Vault



The Black Vault is the largest online Freedom of Information Act (FOIA)
document clearinghouse in the world. The research efforts here are
responsible for the declassification of hundreds of thousands of pages
released by the U.S. Government & Military.

Discover the Truth at: **<http://www.theblackvault.com>**



Federal Bureau of Investigation
Washington, D.C. 20535

October 19, 2016

MR. JOHN GREENEWALD JR.

[REDACTED]
[REDACTED]

FOIPA Request No.: 1341703-000
Subject: 080-HQ-612

Dear Mr. Greenwald:

The enclosed documents were reviewed under the Freedom of Information Act (FOIA), Title 5, United States Code, Section 552. Deletions have been made to protect information which is exempt from disclosure, with the appropriate exemptions noted on the page next to the excision. In addition, a deleted page information sheet was inserted in the file to indicate where pages were withheld entirely. The exemptions used to withhold information are marked below and explained on the enclosed Explanation of Exemptions:

Section 552

☐ (b)(1)

☐ (b)(2)

☒ (b)(3)

50 U.S.C. 3024(i)(1)

☐ (b)(4)

☐ (b)(5)

☒ (b)(6)

☐ (b)(7)(A)

☐ (b)(7)(B)

☒ (b)(7)(C)

☒ (b)(7)(D)

☒ (b)(7)(E)

☐ (b)(7)(F)

☐ (b)(8)

☐ (b)(9)

Section 552a

☐ (d)(5)

☐ (j)(2)

☐ (k)(1)

☐ (k)(2)

☐ (k)(3)

☐ (k)(4)

☐ (k)(5)

☐ (k)(6)

☐ (k)(7)

423 pages were reviewed and 350 pages are being released.

☒ Document(s) were located which originated with, or contained information concerning, other Government Agency (ies) [OGA].

☒ This information has been referred to the OGA(s) for review and direct response to you.

☒ We are consulting with another agency. The FBI will correspond with you regarding this information when the consultation is completed.

☐ In accordance with standard FBI practice and pursuant to FOIA exemption (b)(7)(E) and Privacy Act exemption (j)(2) [5 U.S.C. § 552/552a (b)(7)(E)/(j)(2)], this response neither confirms nor denies the existence of your subject's name on any watch lists.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S.C. § 552(c) (2006 & Supp. IV (2010)). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist. Enclosed for your information is a copy of the Explanation of Exemptions.

For questions regarding our determinations, visit the www.fbi.gov/foia website under "Contact Us." The FOIPA Request Number listed above has been assigned to your request. Please use this number in all correspondence concerning your request. Your patience is appreciated.

You may file an appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, Suite 11050, 1425 New York Avenue, NW, Washington, D.C. 20530-0001, or you may submit an appeal through OIP's FOIAonline portal by creating an account on the following web site: <https://foiaonline.regulations.gov/foia/action/public/home>. Your appeal must be postmarked or electronically transmitted within sixty (60) days from the date of this letter in order to be considered timely. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal." Please cite the FOIPA Request Number assigned to your request so that it may be easily identified.

You may seek dispute resolution services by contacting the Office of Government Information Services (OGIS) at 877-684-6448, or by emailing ogis@nara.gov. Alternatively, you may contact the FBI's FOIA Public Liaison by emailing foipaquestions@ic.fbi.gov. If you submit your dispute resolution correspondence by email, the subject heading should clearly state "Dispute Resolution Services." Please also cite the FOIPA Request Number assigned to your request so that it may be easily identified.

☐ The enclosed material is from the main investigative file(s) in which the subject(s) of your request was the focus of the investigation. Our search located additional references, in files relating to other individuals, or matters, which may or may not be about your subject(s). Our experience has shown when identifying references usually contain information similar to the information processed in the main file(s). Because of our significant backlog, we have given priority to processing only the main investigative file(s). If you want the references, you must submit a separate request for them in writing, and they will be reviewed at a later date, as time and resources permit.

☒ See additional information which follows.

Sincerely,



David M. Hardy
Section Chief
Record/Information
Dissemination Section
Records Management Division

Enclosure(s)

In response to your Freedom of Information Act (FOIA) request, enclosed is a processed copy of FBI Headquarters file 80-HQ-612 Section 1-2, EBF MISC, EBF 54, and EBF 127.

The enclosed documents represent the first interim release of information responsive to your FOIA request.

Inquiries regarding your OGA referral(s) may be directed to the following agency(ies) at:

Army
Chief, US Army FOI/PA Office
Attn: AAHS-RDF
7701 Telegraph Road, Suite 150
Alexandria, VA 22315-3905

Office of Management and Budget
Attn: FOIA Officer
9026 New Executive Office Building
725 17th Street, NW
Washington, DC 20503

Office of the Attorney General
Chief of Staff
Office of Information Policy
Suite 11050
1425 New York Ave, NW
Washington, DC 20530-0001

As previously indicated, document(s) were located which originated with, or contained information concerning another agency(ies). We are consulting with the other agency(ies) and are awaiting their response. Our office has processed all other information currently in our possession. Upon the completion of the outstanding consultation by our office, the FBI will correspond with you regarding those documents when the consultation is completed.

This material is being provided to you at no charge.

EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

- (b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;
- (b)(2) related solely to the internal personnel rules and practices of an agency;
- (b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
- (b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;
- (b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
- (b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

- (d)(5) information compiled in reasonable anticipation of a civil action proceeding;
- (j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;
- (k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;
- (k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;
- (k)(4) required by statute to be maintained and used solely as statistical records;
- (k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;
- (k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

FEDERAL BUREAU OF INVESTIGATION
UNITED STATES DEPARTMENT OF JUSTICE
WASHINGTON, D. C.
OFFICIAL BUSINESS

PENALTY FOR PRIVATE USE TO AVOID
PAYMENT OF POSTAGE, \$300

FEDERAL BUREAU OF INVESTIGATION
UNITED STATES DEPARTMENT OF JUSTICE

L-19-77

Laboratory Work Sheet

Re: **Small piece of paper bearing typewriting
found by Mrs. Carl Baughman, Salina, Kansas.**

File # **80-612-45**
Lab. # **81144**

Examination requested by: **Kansas City**

Date of reference communication: **let. 5-27-42**

Date received: **6-1-42jvt**

Examination requested: **Cryptographic**

Result of Examination:

Examination by: **Holland**

Specimens submitted for examination

- Q1 One small piece of paper bearing typewriting beginning "SPECIAL NOTICE Bureau
reopens recessed longer brete...."

Special Instructions:

127

NO. _____

DATE 6-8

MIMEOGRAPHING

XXXXXXXXXX

☐ PHOTOSTATING

☐ DUPLIGRAPHING

☐ MULTI-LITHING

ADDRESSOGRAPHING

REMARKS OR DESCRIPTION as listed, 80-612-75

~~Send to Hesser~~

APPROVED _____

SIGNED E.P. Coffey
jwb

PHOTOGRAPHIC

NEGATIVES	
POSITIVES	
CONTACT-PRINTS	
ENLARGEMENTS	
LANTERN SLIDES	
MOUNTING	
OPAQUING	
DELIVERED	DATE TIME INITIAL

PRINTING

	DATE	INITIALS
SET TYPED		
PROOFED		
CORRECTED		
PLATES MADE		
RUN		
ASSEMBLED FOLDED		
STAPLED PUNCHED CUT		
DELIVERED		

ASSIGNED TO: #1

井 2

井3

REASSIGNMENTS:

CHARGE OUT

CHARGE IN

REMARKS

NAME

CHARGE OUT

CHARGE IN

REMARKS

Holland	6/10	8 ^{6/11} 9/8	all
---------	------	----------------------------------	-----

Lab. File destroyed Date 10-5-45

✓ Container

✓ Original evidence

✓ Work sheet

✓ _____

80-612-127



80-612-127

SPECIAL NOTICE

Beure xsuzmo rexuso toxgar brete incan gxeat yocat urxach lesnal sonxion
boien okxous aning dxajo Biupp blexrel Sunkey dayxogg Masee yxand 31st.

52
425

522
425
100

80-612-127

75

K-
(-)

Q
(1)

RGCHIA
File #80-612 ✓
#62-66727

May 1, 1944

MR. COFFEY, ROOM 7643

RE: ALLOCATION OF CRYPTANALYTIC
WORK - JURISDICTION DURING
WAR TIME.

Reference is made to the attached clipping from the Washington Times Herald, dated March 17, 1944, which mentions a letter read by Senator Mead during the debate on appropriations for the Federal Communications Commission which refers to the cryptographic work of that organization.

As you know a Presidential memorandum dated July 8, 1942, directed that cryptanalytical work be limited to the Army, the Navy, and the F. B. I. It would therefore appear that if the work to which the above mentioned letter refers were done after July 8, 1942, the Federal Communications Commission was at that time undertaking an unauthorized cryptographic function.

It is further pointed out that in the above mentioned Presidential memorandum the cryptanalytical unit of the Federal Communications Commission is specifically mentioned as one of those to be discontinued.

Respectfully,

C. F. Downing

8-12

FEDERAL BUREAU OF INVESTIGATION
UNITED STATES DEPARTMENT OF JUSTICE

STH:MJB

Laboratory Report

June 29, 1942

File # 80-612-75

Re: Small piece of paper bearing typewriting Lab # 81144
found by Mrs. Carl Baughman, Salina, Kansas

Examination requested by: Kansas City

Reference: Letter 5/27/42

Examination requested: Cryptographic Holland

Specimens:

80-612-75 Q1. One small piece of paper bearing typewriting beginning "SPECIAL
NOTICE Beure xsuzmo rexuso toxgar brete...."

Result of Examination:

Specimen Q1 was examined and it was found that when the first two letters of each group were read the following message was conveyed, "Be sure to bring your lesson book and Bible, Sunday May 31." No meaning was found for the remainder of the letters composing the message. It is possible that these letters were merely added to conceal the other message.

The original specimen submitted is being retained in the files of the Laboratory.

2 - Kansas City

1 - Laboratory ✓

6/30/42
ic

KANSAS CITY, MISSOURI
MAY 27, 1942

Director
Federal Bureau of Investigation
Washington, D. C.

Dear Sir:

A Mrs. CARL BAUGHMAN, 603 South 11th Street, Salina, Kansas, has furnished to this office the enclosed piece of paper on which appears the following:

"SPECIAL NOTICE

Beure xsuzmo rexuso toxgar brete incan gxeat yocet urxach lesnal sonxion
boien okxous aning dxajo Biupp blexrel Sunkey dayxegg Masee yxand Slat."

Mrs. BAUGHMAN informed me that this material was found near a filling station in Salina. It does not appear to me to be written in any language, and it may be nothing more than a typing exercise of the nature used in some business colleges. On the other hand it may possibly be cryptographic in its nature, and it is requested that the Bureau make an analysis thereof with the view to determining whether it is a coded or cryptographic message. It is not necessary to return this material to this office.

Very truly yours

DWIGHT BRANTLEY
Special Agent in Charge

DB:MT
Enclosure

80-612-75
6/8/42
Jant

FEDERAL BUREAU OF INVESTIGATION
UNITED STATES DEPARTMENT OF JUSTICE

OFFICIAL BUSINESS

607 U. S. COURT HOUSE
FOLEY SQUARE
NEW YORK, N. Y.

PENALTY FOR PRIVATE USE TO AVOID
PAYMENT OF POSTAGE, \$300

9 Enclosures for Tech. Lab.

Re: Hagelin Cryptographers



80-612-54



80-612-54



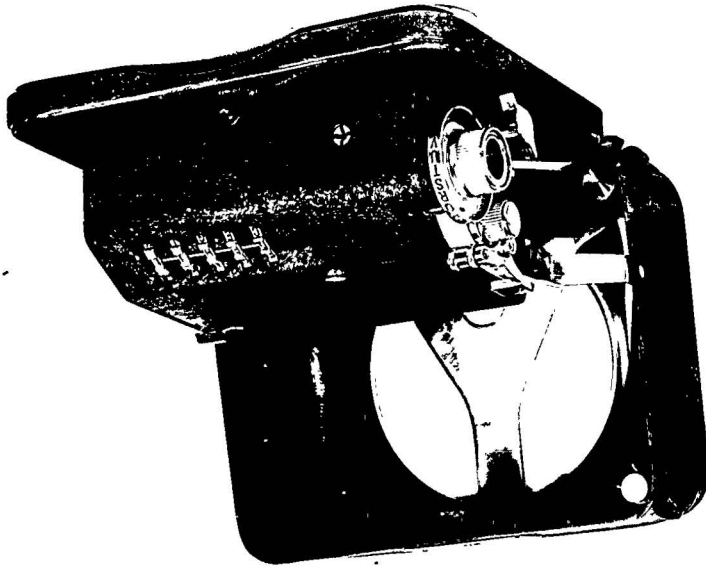
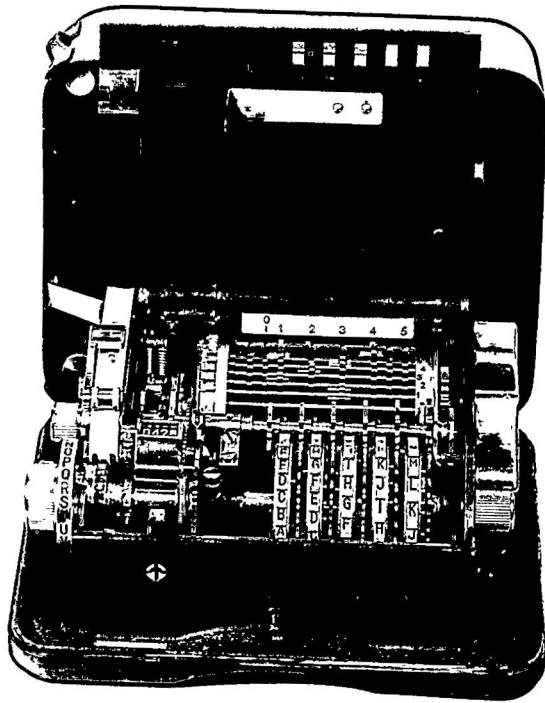
80-612-54



The Hagelin Cryptograph
Ciphering machine.

100-300 machines per
year 5-6 years

150-200 \$ to manufacturer
per machine
+ tools.



86-612-54

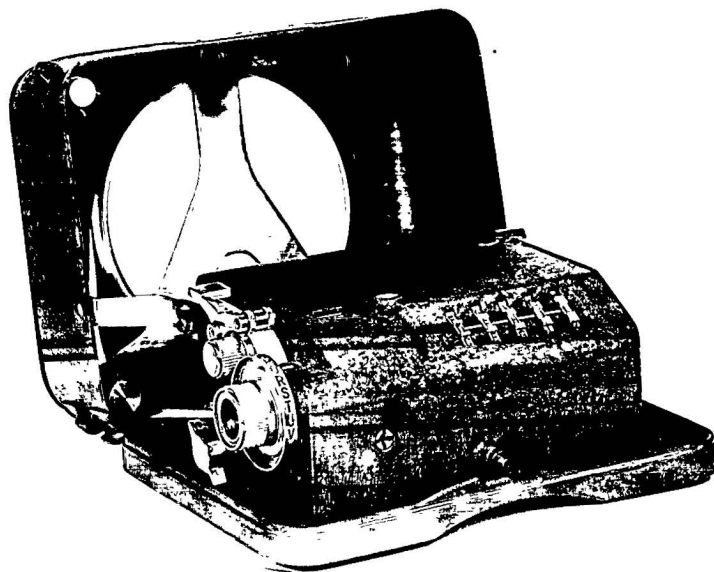
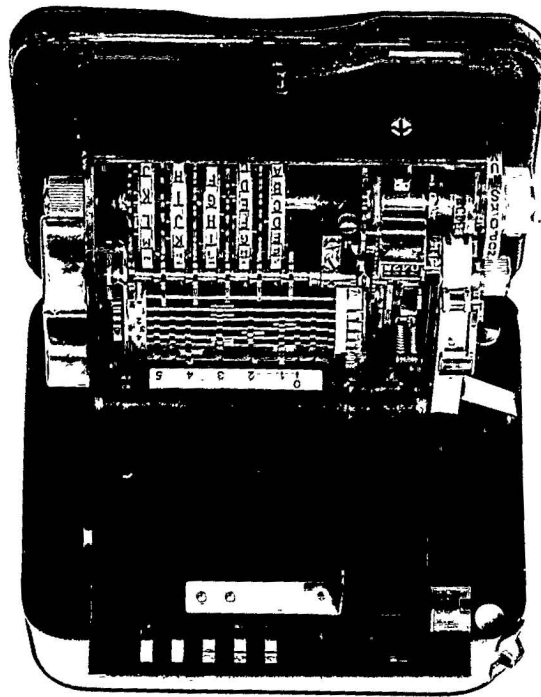
Handwritten signature
Toto

DROTTNINCO. EO-52
11 285065 Stockhold

DROTTNINCO. EO-52
11 285065 Stockhold

Handwritten signature
Toto

80-612-54



80-612-54

STOCKHOLM
COMM. BUREAU
Page 1
1080-271

80-612-54

Hansa
foto

DROTNINGG. 50-52
tel. 235065 Stockholm

The Hagelin Cryptographers

An Analysis

80-612-54

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1341703-0

Total Deleted Page(s) = 2
Page 3 ~ Referral/Consult;
Page 4 ~ Referral/Consult;

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1341703-0

Total Deleted Page(s) = 40
Page 42 ~ Referral/Direct;
Page 43 ~ Referral/Direct;
Page 44 ~ Referral/Direct;
Page 45 ~ Referral/Direct;
Page 46 ~ Referral/Direct;
Page 52 ~ Referral/Consult;
Page 53 ~ Referral/Consult;
Page 54 ~ Referral/Consult;
Page 58 ~ Referral/Consult;
Page 67 ~ Referral/Consult;
Page 68 ~ Referral/Consult;
Page 69 ~ Referral/Consult;
Page 70 ~ Referral/Direct;
Page 71 ~ Referral/Direct;
Page 72 ~ Referral/Direct;
Page 73 ~ Referral/Direct;
Page 76 ~ Referral/Direct;
Page 77 ~ Referral/Direct;
Page 78 ~ Referral/Direct;
Page 79 ~ Referral/Direct;
Page 80 ~ Referral/Direct;
Page 81 ~ Referral/Direct;
Page 82 ~ Referral/Direct;
Page 83 ~ Referral/Direct;
Page 84 ~ Referral/Direct;
Page 85 ~ Referral/Direct;
Page 86 ~ Referral/Direct;
Page 87 ~ Referral/Direct;
Page 88 ~ Referral/Direct;
Page 89 ~ Referral/Direct;
Page 90 ~ Referral/Direct;
Page 98 ~ Referral/Direct;
Page 142 ~ Referral/Consult;
Page 143 ~ Referral/Consult;
Page 163 ~ Referral/Consult;
Page 164 ~ Referral/Consult;
Page 170 ~ Referral/Consult;
Page 171 ~ Referral/Consult;
Page 176 ~ b7D;
Page 186 ~ b7D;

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

Eu

SFP:MM

January 11, 1937.

MEMORANDUM FOR MR. NATHAN.

Re: Instruction in Cryptography
by Mr. Pickering.

H
In March, 1936 a course of instruction in cryptography was begun by Mr. Pickering for the purpose of training other members of the Laboratory's staff in the examination and deciphering of cryptograms submitted to the Laboratory. It was decided to limit the group taking the instruction to three persons and Messrs. Appel, Conrad and Parsons were selected to start the course.

The first part of the course consisted of a study of the common forms of transposition ciphers wherein the letters of the cipher are rearranged. This was followed by a second portion of the course which included the study of the simple single alphabet substitution ciphers together with the numerous methods devised for constructing mixed alphabets which could be constructed from memory using only a code word or phrase. Examples of these types of ciphers were submitted for solution. This study was necessarily slow because of the numerous absences from the city of those persons taking the course, these absences being for the purpose of testifying in court.

A study of multiple alphabet ciphers was assigned and eventually a multiple alphabet was submitted to each of the three members taking the course with the request that attempts be made to solve the cipher. This kind of a cipher is difficult to solve and the particular one submitted was unusually difficult. Because of the amount of work and the length of time involved in connection with the efforts to solve this cipher it has been decided to eliminate this particular problem from the course and substitute a less involved cipher in order that practice may be had with the type of cipher that is more liable to come to the attention of the Bureau.

A second course in the meantime was started with Mr. McCarthy and Mr. Gunsser, who showed an active interest in this work. At the present time Mr. McCarthy has completed a section on normal substitution.

RECORDED

80-612-1


MAILED
JAN 14 1937

Page 2,
Memorandum for Mr. Nathan,
January 11, 1937.

ciphers, together with most of the work on transposition ciphers, and has solved a number of ciphers submitted to him. Mr. Gunsser had completed approximately the same work as Mr. McCarthy, but because he has been transferred from the Laboratory no further instruction has been given to him.

In addition to the absences from the city of the various members taking the course there have been periods of time during which the work in the Laboratory was so voluminous that assignments were curtailed. Arrangements have been made for a more regular schedule and a memorandum regarding the progress of this course of instruction will be submitted at the beginning of each month.

Respectfully,


E. P. Coffey.

SFP:MM

January 11, 1937.

MEMORANDUM FOR MR. NATHAN.

Re: Instruction in Cryptography
by Mr. Pickering.

In March, 1936 a course of instruction in cryptography was begun by Mr. Pickering for the purpose of training other members of the Laboratory's staff in the examination and deciphering of cryptograms submitted to the Laboratory. It was decided to limit the group taking the instruction to three persons and Messrs. Appel, Conrad and Parsons were selected to start the course.

The first part of the course consisted of a study of the common forms of transposition ciphers wherein the letters of the cipher are rearranged. This was followed by a second portion of the course which included the study of the simple single alphabet substitution ciphers together with the numerous methods devised for constructing mixed alphabets which could be constructed from memory using only a code word or phrase. Examples of these types of ciphers were submitted for solution. This study was necessarily slow because of the numerous absences from the city of those persons taking the course, these absences being for the purpose of testifying in court.

A study of multiple alphabet ciphers was assigned and eventually a multiple alphabet was submitted to each of the three members taking the course with the request that attempts be made to solve the cipher. This kind of a cipher is difficult to solve and the particular one submitted was unusually difficult. Because of the amount of work and the length of time involved in connection with the efforts to solve this cipher it has been decided to eliminate this particular problem from the course and substitute a less involved cipher in order that practice may be had with the type of cipher that is more liable to come to the attention of the Bureau.

A second course in the meantime was started with Mr. McCarthy and Mr. Gunasor, who showed an active interest in this work. At the present time Mr. McCarthy has completed a section on normal substitution

Page 2,
Memorandum for Mr. Nathan,
January 11, 1937.

ciphers, together with most of the work on transposition ciphers, and has solved a number of ciphers submitted to him. Mr. Gunsser had completed approximately the same work as Mr. McCarthy, but because he has been transferred from the Laboratory no further instruction has been given to him.

In addition to the absences from the city of the various members taking the course there have been periods of time during which the work in the Laboratory was so voluminous that assignments were curtailed. Arrangements have been made for a more regular schedule and a memorandum regarding the progress of this course of instruction will be submitted at the beginning of each month.

Respectfully,

E. P. Coffey.

SFP:MM

January 11, 1937.

MEMORANDUM FOR MR. NATHAN.

Re: Instruction in Cryptography
by Mr. Pickering.

In March, 1936 a course of instruction in cryptography was begun by Mr. Pickering for the purpose of training other members of the Laboratory's staff in the examination and deciphering of cryptograms submitted to the Laboratory. It was decided to limit the group taking the instruction to three persons and Messrs. Appel, Conrad and Parsons were selected to start the course.

The first part of the course consisted of a study of the common forms of transposition ciphers wherein the letters of the cipher are rearranged. This was followed by a second portion of the course which included the study of the simple single alphabet substitution ciphers together with the numerous methods devised for constructing mixed alphabets which could be constructed from memory using only a code word or phrase. Examples of these types of ciphers were submitted for solution. This study was necessarily slow because of the numerous absences from the city of those persons taking the course, these absences being for the purpose of testifying in court.

A study of multiple alphabet ciphers was assigned and eventually a multiple alphabet was submitted to each of the three members taking the course with the request that attempts be made to solve the cipher. This kind of a cipher is difficult to solve and the particular one submitted was unusually difficult. Because of the amount of work and the length of time involved in connection with the efforts to solve this cipher it has been decided to eliminate this particular problem from the course and substitute a less involved cipher in order that practice may be had with the type of cipher that is more liable to come to the attention of the Bureau.

A second course in the meantime was started with Mr. McCarthy and Mr. Gunesser, who showed an active interest in this work. At the present time Mr. McCarthy has completed a section on normal substitution

SFP:MM

January 11, 1937.

MEMORANDUM FOR MR. NATHAN.

Re: Instruction in Cryptography
by Mr. Pickering.

In March, 1936 a course of instruction in cryptography was begun by Mr. Pickering for the purpose of training other members of the Laboratory's staff in the examination and deciphering of cryptograms submitted to the Laboratory. It was decided to limit the group taking the instruction to three persons and Messrs. Appel, Conrad and Parsons were selected to start the course.

The first part of the course consisted of a study of the common forms of transposition ciphers wherein the letters of the cipher are rearranged. This was followed by a second portion of the course which included the study of the simple single alphabet substitution ciphers together with the numerous methods devised for constructing mixed alphabets which could be constructed from memory using only a code word or phrase. Examples of these types of ciphers were submitted for solution. This study was necessarily slow because of the numerous absences from the city of those persons taking the course, these absences being for the purpose of testifying in court.

A study of multiple alphabet ciphers was assigned and eventually a multiple alphabet was submitted to each of the three members taking the course with the request that attempts be made to solve the cipher. This kind of a cipher is difficult to solve and the particular one submitted was unusually difficult. Because of the amount of work and the length of time involved in connection with the efforts to solve this cipher it has been decided to eliminate this particular problem from the course and substitute a less involved cipher in order that practice may be had with the type of cipher that is more liable to come to the attention of the Bureau.

A second course in the meantime was started with Mr. McCarthy and Mr. Gunsser, who showed an active interest in this work. At the present time Mr. McCarthy has completed a section on normal substitution

Page 2,
Memorandum for Mr. Nathan,
January 11, 1937.

ciphers, together with most of the work on transposition ciphers, and has solved a number of ciphers submitted to him. Mr. Gunsser had completed approximately the same work as Mr. McCarthy, but because he has been transferred from the Laboratory no further instruction has been given to him.

In addition to the absences from the city of the various members taking the course there have been periods of time during which the work in the Laboratory was so voluminous that assignments were curtailed. Arrangements have been made for a more regular schedule and a memorandum regarding the progress of this course of instruction will be submitted at the beginning of each month.

Respectfully,

E. P. Coffey.

MR. PICKERING HAS
SERIALS 2,3, AND 4.

EA

November 7, 1936

MEMORANDUM FOR MR. NATHAN

Re: Instruction in Cryptography
by Mr. Pickering.

In the early part of March, 1936, a course of instruction in cryptography was begun by Mr. Pickering for the purpose of training other members of the Laboratory's staff in the examination and deciphering of cryptograms submitted to the Laboratory. It was decided to limit the group taking the instruction to three persons and Messrs. Appel, Conrad and Parsons were selected to start the course.

The first part of the course consisted of a study of the common forms of transposition ciphers wherein the letters of the cipher are rearranged. This was followed by a second portion of the course which included the study of the simple single alphabet substitution ciphers together with the numerous methods devised for constructing mixed alphabets which could be constructed from memory using only a code word or phrase. Examples of these types of ciphers were submitted for solution. This study was necessarily slow because of the numerous absences from the city of those persons taking the course, these absences being for the purpose of testifying in court.

At the end of June, the study of multiple alphabet ciphers was assigned, after which a multiple alphabet cipher was submitted to each of the three members taking the course with the request that attempts be made to solve the cipher. No solutions of this cipher were forthcoming and periodic inquiries made from time to time revealed that neither Mr. Parsons nor Mr. Conrad had made any serious attempts to solve the cipher. Mr. Appel had done work on the cipher from time to time and had ascertained the number of alphabets used in the cipher and obtained the necessary frequency tables and tables of the relative positions of letters for all of the alphabet. He had not obtained a solution, however, and submitted a large number of sheets of paper containing many data recorded during the various attempts at reaching a solution. Mr. Pickering, who had taken this cipher from one of many that was submitted to him while taking his course at the War Department could not remember the solution to the cipher without looking up his notes which he purposely refrained from doing in order to have an

70-612

Page 2,
Memorandum for Mr. Nathan,
November 7, 1936.

unbiased discussion with Mr. Appel and make suggestions for reaching a solution. It might be said here that this particular cipher is more difficult than the ordinary multiple alphabet cipher in that it was thought that mixed alphabets were used rather than the normal order of the letters of the alphabet and it is not surprising that many difficulties were encountered in reaching a solution.

In view of the inactivity of Mr. Parsons and Mr. Conrad relative to this cipher, Mr. Pickering has recommended that instructions to these individuals be discontinued. In the meantime, a second course was started with Mr. McCarthy and Mr. Gunsser who showed an active interest in this work. At the present time, Mr. McCarthy has completed the section on normal substitution ciphers together with most of the work on transposition ciphers and has solved several of the ciphers submitted to him. Mr. Gunsser has completed approximately the same work as Mr. McCarthy. The multiple alphabet cipher has not been submitted to either one of these individuals.

The instruction to Mr. McCarthy and Mr. Gunsser has been temporarily interrupted, Mr. McCarthy being out of the city, and because of the absence of Mr. Donaldson, Mr. Gunsser has been required to do all of the blood examinations submitted to the Laboratory and this has entailed a considerable amount of extra work and study. With the return of Mr. McCarthy and Mr. Donaldson, the course will be continued.

In the future, a memorandum covering the progress of these courses of instruction will be submitted at the beginning of each month.

Respectfully,

E. P. Coffey.

LBN:AEM

March 7, 1938.

80-612-5

C
X
Honorable Henry Cabot Lodge, Jr.,
United States Senate,
Washington, D. C.

My dear Senator:

V
In compliance with the telephonic request
of your office this morning, it is a pleasure to
enclose herewith a copy of a reprint from the February,
1938, issue of the Law Enforcement Bulletin, on
"Ciphers."

1
It is hoped this publication will be of
assistance to you.

With best wishes and kind regards,

Sincerely yours,
For the Director,

Harold Nathan,
Assistant Director.

Enclosure

11
1578

18

JOHN EDGAR HOOVER
DIRECTOR

CC-161

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

Mr. Nathan _____
Mr. Tolson _____
Mr. Baughman _____
Mr. Clegg _____
Mr. Coffey _____
Mr. Dawsey _____
Mr. Egan _____
Mr. Foxworth _____
Mr. Glavin _____
Mr. Harbo _____
Mr. Joseph _____
Mr. Lester _____
Mr. Nichols _____
Mr. Quinn _____
Mr. Schilder _____
Mr. Tamm _____
Mr. Tracy _____
Miss Gandy _____

Date March 7, 1938.

MEMORANDUM FOR MR. TOLSON

Office of Senator ~~X~~Lodge, of Massachusetts,
called Research Division at 1:00 P. M., asking if we
had any information available on cryptography. I
informed him that an article had appeared at one time
in the Law Enforcement Bulletin on Ciphers, and that the
Director would be glad to send him a copy if any reprints
were available. Accordingly a letter has been prepared
sending this reprint to Senator Lodge.

Respectfully,

✓
17

RECORDED
&
INDEXED

80-612-5

MAR 9 1938

W. J. [unclear]

Signature

EPC:ON

May 18, 1938.

MEMORANDUM FOR MR. APPEL	JERKINS
BLACKBURN	MAJOR
CONRAD	MILLER
DINGLE	PARSONS
GASTEIGER	C. TALL

The above-named have been designated to undertake the study of cryptography under the direction of Mr. Pickering. Classes will be held every Tuesday at 5 P. M. for a period of at least thirty minutes. If Mr. Pickering is absent from the city at the time of any of the scheduled classes the students will individually devote that specific time to various reading work on problems assigned or other phases of cryptography.

Mr. Pickering will be requested to rate the work and efficiency of each of the students.

Very truly yours,

E. P. Coffey.

cc-Mr. Nathan
Bureau

RECORDED

80-612 6

RECORDED COPY FILED IN

Mr. Tolson	✓
Mr. Nathan	✓
Mr. Tamm	✓
Mr. Clegg	✓
Mr. Coffey	✓
Mr. Dawsey	
Mr. Egan	
Mr. Foxworth	
Mr. Glavin	
Mr. Harbo	
Mr. Lester	
Mr. McIntire	
Mr. Nichols	
Mr. Tracy	✓
Miss Gandy	

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

SFP:AWK
80-612

May 26, 1938

MEMORANDUM FOR MR. NATHAN

Re: Instruction in
Cryptography

On Tuesday, May 24, 1938 at 5:00 P. M. the first of the series of meetings was held in connection with instruction of various laboratory men in the subject of cryptography. Of those who are to receive instruction the following were present: Messrs. Appel, Dingle, Gasteiger, Major, Jenkins, Miller, Parsons, Pickering and Q. Tamm.

This instruction is being given by Mr. Pickering who previously received instruction at the War Department. At this meeting the use of key words for the construction of cipher alphabets was discussed following which an explanation of the methods used for solving simple substitution ciphers was shown. This discussion included the use of the frequency table and also the value of word patterns.

The next meeting which is to be held May 31, 1938 will be devoted to a continuation of the discussion of the methods for solving simple substitution ciphers including such ciphers where the actual words themselves are not separated from each other. The advanced assigned work consists of the first two assignments of the course which has been submitted by the Navy Department, and the introduction and discussion of substitution type ciphers (Section Seven of the Text #165 Elementary Military Cryptography Prepared by the Signal Corps). A simple substitution cipher has been given to each one of the members of the class for solution, the solution of this cipher to be turned in on the 31st. A copy of a recently received cipher which has not been solved is also assigned to each member of the class for continued study.

RECORDED

Respectfully,

E. P. Coffey

80-612-7

FILED

JUN 1 1938

U. S. DEPARTMENT OF JUSTICE

NATHAN

TOLSON

TRACY

ENGLE

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

Mr. Tolson	✓
Mr. Nathan	✓
Mr. Tamm	✓
Mr. Clegg	✓
Mr. Coffey	✓
Mr. Crowl	✓
Mr. Egan	✓
Mr. Foxworth	✓
Mr. Glavin	✓
Mr. Harbo	✓
Mr. Lester	✓
Mr. McIntire	✓
Mr. Nichols	✓
Mr. Tracy	✓
Miss Gandy	✓

SFP:EG

June 3, 1938

80-612

MEMORANDUM FOR MR. NATHAN

Re: Instruction in Cryptography

The second meeting in connection with the course of instruction in codes and ciphers being given by Mr. Pickering was scheduled to take place at 5 P. M. on Tuesday, May 31. Of those designated to attend this course, Mr. Appel, Mr. Conrad and Mr. Gasteiger were on leave and Mr. Blackburn was out of the city. Mr. Pickering who is the instructor in this work also was out of the city. At such times as Mr. Pickering is out of the city those taking the course are supposed to proceed with the study of cryptographic work between the hours of 5 and 5:30 on Tuesday. It was ascertained, however, subsequently that with the exception of Mr. Q. Tamm who was absent receiving medical attention, the other members of the class continued with their regular work. All members of the class have been reminded that the period from 5 to 5:30 on Tuesday is to be devoted strictly to the study of cryptography irrespective of the absence of Mr. Pickering from the city. It was ascertained that every member of the class had completed his reading assignment and had solved the problem in cryptography which had been assigned for that date.

At the next meeting scheduled for June 7, 1938 the study of simple substitution ciphers will be continued and a problem will be assigned wherein the words appearing in the cipher are not separated but are run together, this type of cipher being considerably more difficult to solve than those of the same types wherein the words have been separated. A cipher of such a type has been assigned.

RECORDED

Respectfully,

E. P. Coffey
E. P. Coffey

80-612-8
FEDERAL BUREAU OF INVESTIGATION
JUN 5 1938 P.M.
U. S. DEPARTMENT OF JUSTICE
NATHAN
TOLSON
CLERK

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

SFP:DMS
80-612

June 8, 1938.

MEMORANDUM FOR MR. NATHAN.

Re: Instruction in Cryptography.

Mr. Tolson ✓
Mr. Nathan ✓
Mr. Clegg ✓
Mr. Coffey ✓
Mr. Crowl
Mr. Dawsey
Mr. Egan
Mr. Foxworth
Mr. Glavin
Mr. Harbo
Mr. Lester
Mr. McIntire
Mr. Nichols
Mr. Tracy
Miss Gandy

On Tuesday, June 7, 1938, the regular meeting for the study of cryptography was held at 5 P. M. The class was attended by Messrs. Appel, Dingle, Major, Parsons, Pickering, Jenkins and Q. Tamm. Messrs. Blackburn, Conrad, Gasteiger and Miller were out of town. The assignment for this meeting consisted of a straight substitution cipher message wherein all of the words were run together so that no indication was given as to the beginnings or endings of words. It was found that none of the members of the class had been able to solve the cipher which Mr. Pickering had submitted, although considerable effort had been expended by the members in obtaining such a solution. The cipher message was placed on a blackboard together with a frequency table and a table showing the letters preceding and following each of the more common letters appearing in the cipher. This table is known as a trigraphic table. By means of these data Mr. Pickering went through the detailed steps in the process used for obtaining a solution to the cipher. Every one of the steps taken was carefully explained and at the end of one hour most of the cipher had been solved. In explaining the steps used for the solution the cooperation of the members of the class was employed.

Another cipher of the same type has been assigned to the members of the class for the next meeting scheduled to take place June 14, 1938. The purpose of this assignment is to ascertain if the members of the class will be able to apply the instruction which they received in connection with the analysis of the cipher on June 7th sufficiently to enable them to work out this type of cipher.

RECORDED
Respectfully

E. P. Coffey

80-612-9

FEDERAL BUREAU OF INVESTIGATION
JUN 10 1938
U. S. DEPARTMENT OF JUSTICE

FILE

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

SFP:DMS
80-612

June 15, 1938.

Mr. Tolson ✓
Mr. Nathan ✓
Mr. Tamm ✓
Mr. Clegg ✓
Mr. Coffey ✓
Mr. Crowl ✓
Mr. Dawsey ✓
Mr. Egan ✓
Mr. Foxworth ✓
Mr. Glavin ✓
Mr. Ladd ✓
Mr. Lester ✓
Mr. McIntire ✓
Mr. Nichols ✓
Mr. Tracy ✓
Miss Gandy ✓

MEMORANDUM FOR MR. NATHAN.

Re: Instruction course in codes
and ciphers.

On June 14, 1938 the regular meeting for the course of instruction in codes and ciphers was held at 5 P. M. The following members were present: Messrs. Dingle, Gasteiger, Miller, Parsons, Pickering and Jenkins, the other members of the class being either on official duty or on leave. The following members have solved problem #3: Messrs. Appel, Dingle, Gasteiger, Major, Miller, Parsons, Q. Tamm and Jenkins. Most of the time during this meeting was taken up with a detailed review by Mr. Pickering of the method of reconstructing a cipher alphabet which had been based on a key phrase, this method being dependent upon a study of the frequencies of the cipher characters without an attempt being made to solve the cipher itself. The meeting was adjourned at 5:50 P. M. Another cipher of the substitution type has been submitted as the assignment for the next meeting on June 21st. This particular cipher is somewhat different in kind from those previously submitted but it has been selected from the ciphers submitted by outside contributors as a good example of the possible variations of a substitution cipher.

Respectfully,

E. P. Coffey
E. P. Coffey

RECORDED

80-612-10
FEDERAL BUREAU OF INVESTIGATION
JUN 17 1938
U. S. DEPT. OF JUSTICE
NATHAN
COFFEY
TAMM

CAA:ON

June 21, 1938.

MEMORANDUM FOR MR. PICKERING

Copies of various ciphers and code messages which have been from time to time forwarded to the Bureau for various purposes have been placed in a folder. These copies show the file number. Some of them have been deciphered and others have not.

It is desired that all examiners studying cryptography at such times as they have an opportunity to do so, examine the so-called ciphers in this file in an endeavor to solve them. Of course, if a solution is secured, it may then be necessary to pull the file in order to advise the field division should the solution prove of interest from an investigative standpoint.

Some of these are no doubt not true ciphers so that there may be no solution to some of them. They offer, however, a continuous example of the type of thing which is being constantly received.

Please have copies made for this file as additional ciphers of this kind are examined.

Very truly yours,

E. P. Coffey.

RECORDED

cc-Bureau ✓
Mr. Nathan
Mr. Appel
Mr. Blackburn
Mr. Conrad
Mr. Dingle
Mr. Gasteiger

Mr. Jenkins
Mr. Major
Mr. Miller
Mr. Parsons
Mr. Q. Tamm

7-5-611- 11

80-612-12
CHANGED TO



b3
b7E

JOHN EDGAR HOOVER
DIRECTOR

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

EPC:ON

June 28, 1938.

MEMORANDUM FOR MR. NATHAN.

Re: Instruction in Cryptography.

Mr. Tolson	✓
Mr. Nathan	
Mr. Clegg	
Mr. Coffey	
Mr. Crowl	
Mr. Egan	
Mr. Glavin	
Mr. Harbo	
Mr. Lester	
Mr. Nichols	
Mr. Rosen	
Mr. Tracy	
Miss Gandy	

There is attached hereto in memorandum form a report prepared by Mr. Pickering concerning the progress of various employees of the laboratory in the study of cryptography.

I think we have now reached the point where we are able to quite definitely determine of those who have taken the preliminary course, which are best adapted to this work. Accordingly, in the absence of instruction to the contrary, I will arrange for the class to be reduced to Messrs. Blackburn, Appel, and Major, and instruction by Mr. Pickering to these men will continue until their proficiency is established.

Respectfully,

E. P. Coffey

RECORDED

80-612-13

U. S. DEPT. OF JUSTICE

RECEIVED

13

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

SFP:ON
80-612

June 22, 1938.

MEMORANDUM FOR MR. NATHAN.

Re: Instruction in Cryptography.

On Tuesday, June 21, 1938, the regular weekly meeting for instruction in cryptography was held at 5 P. M. Those attending were Messrs. Appel, Blackburn, Dingle, Gasteiger, Jenkins, Parsons, and Pickering, the other members being absent from the city.

At this time a discussion was given by Mr. Pickering of the cipher problem #4 which had been previously assigned to the various members. The only person who obtained a solution to this cipher was Mr. Appel. Attention is called to the fact, however, that Mr. Blackburn did not have this problem assigned inasmuch as he had been out of town during the time the previous lectures had been given. Mr. Blackburn will receive separate instruction to bring him up to date. This problem was a cipher actually submitted to the Bureau by an outside contributor and is listed in the Bureau files as 62-26873-58. While this cipher is of the substitution type it is a little different from those previously submitted in that the cipher is made up by substituting one of the two letters adjacent in the alphabet to each letter appearing in the original message. With this construction each letter in the original message can be represented by either one of two letters in the cipher message and, therefore, the method of solution is somewhat different from that of the straight substitution cipher. This problem was assigned particularly for the purpose of bringing out to the members of the class that the solution of ciphers requires much original thinking besides the mere routine methods of solution. In this particular instance if the members had considered the general makeup of the cipher and had used a little original thought the solution could have been obtained in less than half an hour.

Additional ciphers intended to bring out this aspect in connection with the solutions of ciphers will be assigned from time to time in order to develop originality of thought in the members of the class.

RECORDED

Respectfully,

E. P. Coffey
E. P. Coffey

80-612-13

JUL 29 1938
EOLSON
CU RICH

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

SFP:DMS
80-612

June 29, 1938.

Mr. Tolson	✓
Mr. E. A. Tamm	
Mr. Clegg	
Mr. Coffey	
Mr. Glavin	
Mr. Ladd	
Mr. Nichols	
Mr. Rosen	
Mr. Tracy	
Mr. Carson	
Mr. Egan	
Mr. Gurnea	
Mr. Harbo	
Mr. Hendon	
Mr. Jones	
Mr. Mumford	
Mr. Quinn	
Mr. Nease	
Miss Gandy	

MEMORANDUM FOR MR. NATHAN.

Re: Instruction in Cryptography.

On Tuesday, June 28, 1938, the regular meeting for instruction in cryptography was held, those attending being Messrs. Conrad, Dingle, Gasteiger, Major, Miller, Pickering and Jenkins. The other members of the class were out of town. At this time a general review of the work previously done was given followed by a general discussion of simple substitution ciphers. There was included a description of various kinds of ciphers that appear in various disguised forms but actually can be reduced to the simple substitution cipher.

In accordance with my memorandum of June 28, 1938 the class will be reduced to Messrs. Blackburn, Appel and Major and these men will receive additional instruction regularly. Additional time has been given for all the members to solve problem #5 which is a numerical cipher using numbers to separate the words, which is a more difficult kind of cipher than any of those previously submitted.

Respectfully,

EPC
E. P. Coffey

RECORDED

80-612 - 14	
FEDERAL BUREAU OF INVESTIGATION	
JUN 30 1938 A. M.	
U. S. DEPARTMENT OF JUSTICE	
TOLESON	FILE

JOHN EDGAR HOOVER
DIRECTOR

Federal Bureau of Investigation
United States Department of Justice

SFP:DMS
80-612

Washington, D. C.

July 7, 1938.

Mr. Tolson	✓
Mr. Nathan	
Mr. Tamm	
Mr. Clegg	
Mr. Coffey	
Mr. Glavin	
Mr. Ladd	
Mr. Nichols	
Mr. Rosen	
Mr. Tracy	
Miss Gandy	

MEMORANDUM FOR MR. NATHAN.

Re: Instructions in Cryptography.

On July 5, 1938 the regular meeting for instructions in cryptography was held at 5 P. M., those attending being Messrs. Blackburn, Major and Pickering. Mr. Appel, the other member of the class, is out of the city. The assigned problem #5, which consisted of a numerical cipher having all the numbers run together with no separation of words. The actual separations of words were accomplished by assigning various numbers to represent spaces between words. This cipher was solved by both Mr. Blackburn and Mr. Major. After a short discussion of various methods used for solving this cipher instruction was given by Mr. Pickering relative to the methods used for solving multiple alphabet ciphers as this type of cipher represents the one most frequently met with in cases actually received by the Bureau.

The assignment for the next meeting consists of a problem involving a multiple alphabet cipher together with outside reading on methods of solution. Problem #5 is being transmitted to Mr. Appel at Kansas City.

Respectfully,

E. P. Coffey
E. P. Coffey

RECORDED

80-612-15	
FEDERAL BUREAU OF INVESTIGATION	
JUL 9 1938 A. M.	
U. S. DEPARTMENT OF JUSTICE	
NATHAN	TOLSON
FILE	✓

100-16

August 25, 1938.

Miss Ella K. Alschuler
Brigantine Beach Hotel
Brigantine Beach, New Jersey

Dear Miss Alschuler:

In reply to your letter of August 20, 1938, requesting information relative to codes and cryptograms, I regret to advise you that information of this nature is of necessity released only to duly authorized law enforcement agencies and I am therefore unable to comply with your request. However, as of possible interest, I am transmitting herewith copies of this Bureau's releases entitled "The Federal Bureau of Investigation" and "The Technical Laboratory of the Federal Bureau of Investigation".

The five two-cent postage stamps transmitted by you are accordingly being returned herewith.

Trusting that you will appreciate the necessity for such a policy on the part of this Bureau, I am

Sincerely yours,

John Edgar Hoover
Director

Enclosure

Mr. Tolson _____
Mr. Nathan _____
Mr. Tamm _____
Mr. Clegg _____
Mr. Coffey _____
Mr. Crowl _____
Mr. Dawsey _____
Mr. Egan _____
Mr. Foxworth _____
Mr. Glavin _____
Mr. Harbo _____
Mr. Lester _____
Mr. McIntire _____
Mr. Nichols _____
Mr. Tracy _____
Miss Gandy _____

BRIGANTINE BEACH HOTEL

Brigantine Beach, New Jersey

Federal Department of Investigation
Department of Justice,
Washington, D. C.

Dear Sirs: -

If you still have for dis-
tribution your book of
Codes and Cryptograms, will
you kindly send me a copy
at the above address? I
enclose 10¢ (postage) which
I understand is the cost.

Very Truly

Yours
lently

RECORDED
&
INDEXED

Ella K. Alschuler
E. K. ALSCHULER

August 20, 1938

80-612-16
FEDERAL BUREAU OF INVESTIGATION

AUG 22 1938 P.M.

U. S. DEPARTMENT OF JUSTICE

FILE

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

SFP:AWK

80-612

September 15, 1938

MEMORANDUM FOR MR. NATHAN

Re: Course of Study
in Cryptography

On Tuesday September 13, 1938 the course of study in cryptography given by Mr. Pickering to Messrs. Appel, Blackburn and Major was resumed after having been discontinued owing to the absence of the various members from the city. The instruction period was devoted to a review of the methods for solving multiple substitution ciphers. A new cipher of this type is being submitted to the two members of the class who were present, Messrs. Blackburn and Major, for solution by the meeting on next Tuesday, September 20, 1938.

Respectfully,

E. P. Coffey.

RECORDED

80-612-17

FEDERAL BUREAU OF INVESTIGATION	
SEP 17 1938 A.M.	
U. S. DEPARTMENT OF JUSTICE	
NATHAN	FILE

80-612

SFP:1285
62-26873-228

September 15, 1938.

MEMORANDUM FOR MR. NATHAN.

th

Re: Postal card submitted by
Mr. Eldridge Weaver.

Reference is made to the postal card containing a cipher
message typed with figures, the postal card bearing a postmark
dated March 30, 1914.

As a part of the course of instruction in cryptography
being given by Mr. Pickering, an examination of this cipher was made
by Mr. Hager and Mr. Pickering and it was found to be a numerical
substitution cipher wherein the words and sentences are separated by
means of the use of the figure "3", the other figures being used to
represent letters of the alphabet.

The translation of the cipher is as follows:

"I am sorry Ben and don't feel worthy to write U
before U write. It is well with me. Best wishes."
(your brother S)
(other side of postal card)

"I am indeed sorry and hope U can write me soon
that U love my letters. Again forgive me and write
me. Sam"

Photographic copies of both sides of the postal card are
attached hereto.

- Mr. Tolson _____
- Mr. Nathan _____
- Mr. Tamm _____
- Mr. Clegg _____
- Mr. Coffey _____
- Mr. Crowl _____
- Mr. Dawsey _____
- Mr. Egan _____
- Mr. Foxworth _____
- Mr. Glavin _____
- Mr. Harbo _____
- Mr. Lester _____
- Mr. McIntire _____
- Mr. Nichols _____
- Mr. Tracy _____
- Miss Gandy _____

Respectfully,

RECORDED

E. F. Coffey

80-612-18

FEDERAL BUREAU OF INVESTIGATION

SEP 17 1938

NATHAN
SEP 17 1938
SEP 17 1938

*Restoration of ciphered,
showed + burst meeting*

62 26873-228

g

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

SFP:DMS
80-612

September 23, 1938.

MEMORANDUM FOR MR. NATHAN.

Re: Instruction in Cryptography.

The meeting for instruction in cryptography was held on September 21, 1938, at 5 P. M., those attending being Messrs. Appel, Blackburn, Major and Pickering. The entire time of the meeting was spent in outlining the lecture given by Mr. Pickering to the training schools in order that substitutes will be available to give this lecture when Mr. Pickering is out of town. The scope of the lecture was covered and the lantern slides were shown and explained.

Respectfully,

E. P. Coffey
E. P. Coffey

16

Mr. Tolson	✓
Mr. Nathan	✓
Mr. E. A. Tamm	✓
Mr. Clegg	
Mr. Coffey	
Mr. Crowl	
Mr. Dawsey	
Mr. Egan	
Mr. Foxworth	
Mr. Glavin	
Mr. Harbo	
Mr. Lester	
Mr. McIntire	
Mr. Nichols	
Mr. Quinn Tamm	
Mr. Tracy	
Miss Gandy	

RECORDED

80-612-19

FEDERAL BUREAU OF INVESTIGATION

SEP 25 1938

NATHAN

COFFEY

1012

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

SFP:DMS
80-612

October 13, 1938.

MEMORANDUM FOR MR. NATHAN.

Mr. Tolson ✓
Mr. Nathan ✓
Mr. E. A. Tamm
Mr. Clegg
Mr. Coffey
Mr. Crowl
Mr. Dawsey
Mr. Egan
Mr. Foxworth
Mr. Glavin
Mr. Harbo
Mr. Lester
Mr. McIntire
Mr. Nichols
Mr. Quinn Tamm
Mr. Tracy
Miss Gandy

Re: Instruction in Cryptography.
Opening and Resealing Envelopes.

On October 11, 1938 the course of instruction in cryptography was continued those present being Messrs. Blackburn, Major and Pickering. The instruction continued with information relative to the lecture on codes and ciphers given in the various training schools. At this time it was suggested that those taking the course read both "Cryptography" by Lange, and "The American Black Chamber" by Yardley, in order to get a background of various individual types of ciphers about which questions might be asked in class. Some instruction in the use of code books was also given for use in the lectures.

Some experimental work has been carried out in connection with the possibility of opening envelopes and resealing them without leaving evidence of the operation. It was found that the steaming process which is ordinarily used in this connection was very apt to leave the flap of the envelope in a warped condition. Upon resealing the envelope there usually remains indication that the envelope had been tampered with. Various methods were tried to avert this and it was finally found that if the envelopes were placed inside of a jar in the bottom of which was some water and allowed to stand overnight the flap could be easily opened and showed no trace of warping.

Inasmuch as the time element is usually important in such types of work efforts were made to reduce the length of time necessary for the moisture to soften up the paper. It was found that if the envelope were put in a covered jar in the bottom of which was some water which had been warmed to about 40 degrees Centigrade and then the air pumped out of the jar, the time could be reduced to a little over two hours. Additional work is planned in an attempt to reduce this time limit. When the envelope is resealed best results were found when another envelope was used in order to supply the necessary adhesive to seal the flap. The adhesive on the flap of the second

RECORDED COPY FILED IN
80-693-X
100-427-1
80-612

CC - 80-693


RECORDED

80-612 20
OCT 17 1938
FBI - WASH
b3
b7E

Page Two
Memorandum for Mr. Nathan
October 13, 1938.

envelope would be moistened and rubbed on the flap of the first envelope after which the flap was resealed. It was found that if mucilage were directly applied to the flap it usually resulted in there being too much adhesive present and the evidence thereof became noticeable.

Respectfully,


E. P. Coffey



INVI

From: Laboratory

Date _____ 193

_____ Mr. Nathan	_____ Mr. Parsons
_____ Mr. Appel	_____ Mr. Pfafman
_____ Mr. Baughman	_____ Mr. Pickering
_____ Mr. Beach	_____ Mr. Pike
_____ Mr. Blackburn	_____ Mr. Potter
_____ Mr. Burgess	_____ Mr. Renneberger
_____ Mr. H. M. Clegg	_____ Mr. Row
_____ Mr. Clark	_____ Mr. Q. Tamm
_____ Mr. Coffey	_____ Mr. Willard
_____ Mr. Conrad	_____ Chief Clerk
_____ Mr. Dingle	✓ _____ Files
_____ Mr. Donaldson	_____ Laboratory
_____ Mr. Gasteiger	_____ Stenographer
_____ Mr. Hammack	_____ Messenger
_____ Mr. Millen	_____ Mail Room
_____ Mr. Miller	_____ Mr. _____

80-621

Please consult

Mr. H. M. Clegg

Done

5/12/37

See Me _____
Please Handle _____
Route to #1 Examiner _____

E. P. COFFEY

739 Insurance Exchange	3-8998
911 Federal	Cadillac 2835
202 U.S. Court House	Main 501
313 Federal	6361, Ext. 90
700 West Virginia	8928
506 Fletcher Trust	Riley 5416
507 Federal	643
1612 Federal Reserve Bank	Victor 3113
407 Hamilton National Bank	3-7928
500 Rector	6734
903 Pacific Commerce	Mutual 2201
775 Starks	Jackson 5139
2401 Sterick	8-1850
1300 Biscayne	3-5558
1021 Bankers'	Daly 3431
936 Raymond-Commerce	Market 2-5511
1308 Masonic Temple	Raymond 9354
607 U.S. Ct. House, Foley Sq.	Rector 2-3520
224 Federal	2-8186
629 First Nat'l Bank	Atlantic 8644
300 Commercial Merchants	
Nat'l Bank & Trust Co.	4-5800
1300 Liberty Trust	Locust 0880
620 New Federal	Grant 0800
411 U.S. Court House	Atwater 6171
601 Richmond Trust	3-0169
301 Continental Bank	Wasatch 1797
478 Federal	Fannin 8052
One Eleven Sutter, Room 1729	Exbrook 2679
204 Federal	1311
800 Joseph Vance	Main 0460
423 U.S. Court House &	
Custom House	Garfield 0360*
404 New York	Garfield 7509
2266 U. S. Dep't of Justice	National 5303

and Saturday afternoons call Garfield 2120.

at each Field Office including the Bureau at
the New York City Office which is 1-0711.

Our Offices do not possess teletypewriter equipment.

App: Special Agent in Charge,
Federal Bureau of Investigation,
United States Department of Justice
at the above city and address.

INVESTIGATION

From: Laboratory

Date 1/11/39 193

☐ Mr. Nathan
☐ Mr. Appel
☐ Mr. Baughman
☐ Mr. Beach
☐ Mr. Blackburn
☐ Mr. Burgess
☐ Mr. H. M. Clegg
☐ Mr. Clark
☐ Mr. Coffey
☐ Mr. Conrad
☐ Mr. Dingle
☐ Mr. Donaldson
☐ Mr. Gasteiger
☐ Mr. Hammack
☐ Mr. Millen
☐ Mr. Miller

☒ Mr. Parsons
☐ Mr. Pfafman
☒ Mr. Pickering
☐ Mr. Pike
☐ Mr. Potter
☐ Mr. Renneberger
☐ Mr. Row
☐ Mr. Q. Tamm
☐ Mr. Willard
☐ Chief Clerk
☐ Files
☐ Laboratory
☐ Stenographer
☐ Messenger
☐ Mail Room

*Pl. have these files con-
solidated as we originally con-
templated*

See Me _____
Please Handle _____
Route to #1 Examiner _____

E. P. COFFEY

739 Insurance Exchange	3-8998
911 Federal	Cadillac 2835
202 U.S. Court House	Main 501
313 Federal	6361, Ext. 90
700 West Virginia	8928
506 Fletcher Trust	Riley 5416
507 Federal	643
1612 Federal Reserve Bank	Victor 3113
407 Hamilton National Bank	3-7928
500 Rector.	6734
903 Pacific Commerce	Mutual 2201
775 Starks	Jackson 5139
2401 Sterick	8-1850
1300 Biscayne	3-5558
1021 Bankers'	Daly 3431
936 Raymond-Commerce	Market 2-5511
1308 Masonic Temple	Raymond 9354
607 U.S. Ct. House, Foley Sq.	Rector 2-3520
224 Federal	2-8186
629 First Nat'l Bank	Atlantic 8644
300 Commercial Merchants	
Nat'l Bank & Trust Co.	4-5800
1300 Liberty Trust	Locust 0880
620 New Federal	Grant 0800
411 U.S. Court House	Atwater 6171
601 Richmond Trust	3-0169
301 Continental Bank	Wasatch 1797
478 Federal	Fannin 8052
One Eleven Sutter, Room 1729	Exbrook 2679
204 Federal	1311
800 Joseph Vance	Main 0460
423 U.S. Court House &	
Custom House	Garfield 0360*
404 New York	Garfield 7509
2266 U. S. Dep't of Justice	National 5303

and Saturday afternoons call Garfield 2120.
 r each Field Office including the Bureau at
 the New York City Office which is 1-0711.
 n Offices do not possess teletypewriter equipment.
 aph: Special Agent in Charge,
 Federal Bureau of Investigation,
 United States Department of Justice
 at the above city and address.

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

SFP:EG

December 16, 1938

80-612

MEMORANDUM FOR MR. NATHAN

Re: Instruction in Cryptography

At the last meeting in connection with the course of instruction in cryptography on November 13, 1938 there was a discussion of progressive-alphabet ciphers and their solution by means of symmetrical sequences as described in the Navy Department pamphlet, assignment #6 of the Elementary Course in Cryptanalysis. This meeting was attended by Messrs. Appel, Blackburn and Pickering.

The course of instruction has up to the present time covered the various types of the ordinary simple substitution cipher, the multiple alphabet cipher including several variations of this type of cipher and the progressive-alphabet cipher which is a form of multiple alphabet cipher. It is believed that sufficient instruction has been given in these types of ciphers and that Messrs. Appel and Blackburn are competent to handle such types of ciphers in the event of Mr. Pickering's absence from the city. Mr. Blackburn has completed the multiple alphabet cipher assigned to him as a problem and Mr. Appel has been assigned a cipher which has been received in a current case being investigated by the Bureau.

A comparatively short course in transposition ciphers will be given starting Tuesday, November 20.

Respectfully,

E. P. Coffey.

80-612-21

FEDERAL BUREAU OF INVESTIGATION
DEC 19 1938
U. S. DEPARTMENT OF JUSTICE

NATHAN
TOLSON
EAM

TELETYPE
82-612-25

January 25, 1939.

Mr. David Graham
1822 S. L. Tacoma Street
Portland, Oregon

Dear Mr. Graham:

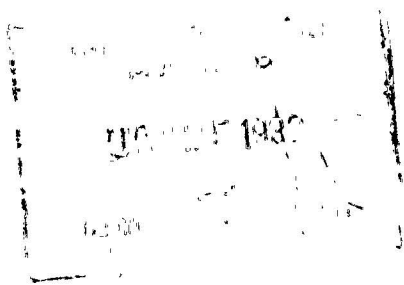
Your letter of January 12, 1939 relative to codes, ciphers and cryptograms has been received.

Please be advised that this Bureau cannot undertake to test your ability along the lines of deciphering codes and cryptograms. For your information there are in the Technical Laboratory of this Bureau technical men who are experts in this field but their work is limited to the investigation of cryptograms obtained during the conduct of criminal investigations. I regret that other information concerning this subject is not available.

Sincerely yours,

John Edgar Hoover
Director

Mr. Tolson _____
Mr. Nathan _____
Mr. E. A. Tamm _____
Mr. Clegg _____
Mr. Coffey _____
Mr. Crowl _____
Mr. Egan _____
Mr. Foxworth _____
Mr. Glavin _____
Mr. Harbo _____
Mr. Lester _____
Mr. McIntire _____
Mr. Nichols _____
Mr. O. Tamm _____
Mr. Tracy _____
Miss Gandy _____



Portland, Oregon
January 12, 1939

Mr. J. Edgar Hoover, Chief
Federal Bureau of Investigation
Washington, D.C.

Dear Mr. Hoover:

I have been referred to you by the local recruiting officer of the U.S. Army, to whom I first addressed my inquiry. He believes the matter now lies in the field of activity of your department.

I sincerely believe that I have a certain moderate talent in codes, ciphers, cryptograms, etc., but I have no adequate way of determining whether I am right. Even our excellent public library here in Portland can do little to help me decide, for most books on the subject devote themselves primarily to "puzzle and amusement" codes rather than to ones of a practical nature.

Is there any way by which I can make a reasonably accurate diagnosis of what ability I may have in this line? I am interested in both phases of the work: 1. Decoding, and 2. Devising of practical, changable codes.

Naturally, if I should have a worthwhile ability, I would want to put it to its best use. Indeed, nothing would please me more than to be able to make it a like work.

Very sincerely yours

David Graham

Data: David Graham 1822 S.E. Tacoma St. Portland, Oregon
Male White Age: 26 Married
Present occupation: State Supervisor Foremanship Training, WPA
Education: Three years Reed College, Portland, Oregon
Born: June 10, 1912--Portland, Oregon

RECORDED

INDEXED

70-612-22

FEDERAL BUREAU OF INVESTIGATION
JAN 13 1939
U. S. DEPARTMENT OF JUSTICE
LAB.

6-125
11-23
11-100

80-612-23
CHANGED TO



b3
b7E

LPC:ON
80-612-

March 3, 1939.

Captain Carter W. Clarke
Chief, Communications Division
Army Signal Corps
War Department
Washington, D. C.

Dear Captain Clarke:

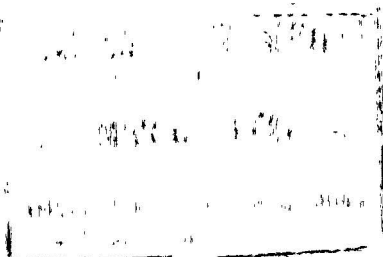
Mr. E. P. Coffey has informed me of the pleasant visit made by him and Mr. I. W. Conrad of the Bureau's Technical Laboratory to the several communication facilities of the Army Signal Corps. I am sure the observations made by these representatives of the Bureau will be valuable in the Bureau's work.

I want to thank you for the kindnesses extended to Messrs. Coffey and Conrad and to assure you of my deep appreciation of your past cooperation with the Bureau in these matters of mutual interest.

Sincerely yours,

Mr. Tolson _____
Mr. Nathan _____
Mr. F. A. Tamm _____
Mr. Clegg _____
Mr. Coffey _____
Mr. Crowl _____
Mr. Egan _____
Mr. Foxworth _____
Mr. Glavin _____
Mr. Harbo _____
Mr. Lester _____
Mr. McIntire _____
Mr. Nichols _____
Mr. Q. Tamm _____
Mr. Tracy _____
Miss Gandy _____

cc-Washington Field



Handwritten notes and signatures, including a large '6' at the top right, a signature 'H. E. Tamm' in the center, and other illegible markings and initials at the bottom right.

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

SFP:RTM
80-612

March 1, 1939

MEMORANDUM FOR MR. NATHAN

Re: Inspection in Cryptography

The original course of instruction in Cryptography has been completed. This course was particularly adapted to cover those types of ciphers most often met with in the course of current work. The kinds of ciphers studied were the simple substitution cipher, the multiple alphabet cipher, a progress alphabet cipher and the usual variations of such substitution ciphers. This is followed by a short course in transposition ciphers as explained by the pamphlets "7 and 8 received from the Navy Department. These two pamphlets cover the most frequently types of transposition ciphers. These pamphlets were assigned to Mr. Blackburn who has completed his study of the same. Mr. Appel has previously had instruction on these types of ciphers.

The various ciphers which have been received time to time and forwarded to the Bureau were placed in a folder as indicated in my memorandum to Mr. Pickering dated June 21, 1938. This folder has been used at various times by the different members of the course but to date none of the ciphers in this folder which had previously been unsolved has been solved since.

The present form of instruction in Cryptography is being discontinued and in its place there will be meetings twice a month for the purpose of working out ciphers received connected with current work and for studying new methods and new types of ciphers. These meetings which will be held on the first and third Tuesdays of each month at 5 P.M., will be in the nature of forums during which the methods will be worked out simultaneously by Mr. Appel, Mr. Blackburn and Mr. Pickering. Pamphlets submitted by the Navy Department in connection with their course in Cryptanalysis will be used.

RECORDED
Respectfully,

E. F. Coffey

80-612-25

FEDERAL BUREAU OF INVESTIGATION
MAR 3 1939
U. S. DEPARTMENT OF JUSTICE
NATHAN
TOLSON
TRACY

H 80-612

SFP:RTM

62-26873

March 24, 1939

MEMORANDUM FOR THE FILE

In accordance with my memorandum to Mr. Pickering dated June 21, 1938 wherein it is stated that a file of unsolved ciphers received by the Bureau has been made, examination of the cipher submitted by Mr. H. E. Anderson of Davenport, Iowa, file #62-26873-175 was made by Mr. Pickering. Mr. Pickering reports that this cipher was arranged in the form of a rectangle having seven vertical columns. After this was done the relative locations of the seven columns were shifted so that the order was different, after which the message could be read by starting at the bottom and reading the horizontal lines upward. The translation of the message reads as follows:

Can you decipher this code. Will you. The only way to test the strength of it is to submit it for the consideration of experts. Please inform me of its real worth. Ever yours. H. E. A.

Mr. Anderson previously submitted a similar cipher to the Bureau with his letter of January 22, 1936, file #62-26873-72. This cipher was deciphered and a projection lantern slide was made which has since been used in the lectures on Codes and Ciphers for the National Police Academy and the Training School.

E. P. Coffey

RECORDED

80-612-26
FEDERAL BUREAU OF INVESTIGATION
MAR 25 1939
U. S. DEPARTMENT OF JUSTICE
FILES

ORIGINAL FILED IN 62-26873-253

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

SFP:DMS
80-612

April 28, 1939.

MEMORANDUM FOR MR. NATHAN.

Re: Instruction in Cryptography.

Since my memorandum of March 1, 1939 in connection with instruction in cryptography, numerous meetings between Messrs. Appel, Blackburn and Pickering have been held for the purpose of mutually working on various cipher systems. As a result of these meetings numerous sets of transparencies containing vertical columns of the letters of the alphabet have been prepared. Some of these have been used for cutting up into vertical strips and for the purpose of placing on thick strips of cardboard so that they can be used for the rapid solution of ciphers where the alphabet has been transposed. Another device for accomplishing this purpose was also constructed and consists of a cardboard cylinder on which have been mounted twenty-six rings each containing a double alphabet. These rings can be rotated on the cylinder so as to set up the cipher message.

Two of the ciphers contained in the booklet of unsolved ciphers received by the Bureau have been solved. These are listed as serials 175 and 250 in the general file of codes and ciphers, 62-26873.

For the past three weeks the entire time devoted to cipher research has been in connection with attempts to solve two of the current unsolved ciphers recently received in the Bureau and an unusually large amount of time and effort has been expended on these ciphers particularly on one which has been received in connection with a case possibly involving espionage. To date neither one of these ciphers has been solved. A copy of the cipher in the espionage case was sent to the Army Signal Corps for examination in the Cryptographic Section there. The report received indicated that no solution had been obtained and that there was a possibility the message was a hoax.

Respectfully

E. P. Coffey

80-612-27

FEDERAL BUREAU OF INVESTIGATION
MAY 2 1939
U. S. DEPARTMENT OF JUSTICE

NATHAN

Federal Bureau of Investigation
United States Department of Justice

WGB:ON

Washington, D. C.

May 26, 1939.

MEMORANDUM FOR MR. NATHAN.

Re: Telephone Call from Congressman
Henry O. Talle.

Congressman Henry O. Talle of Iowa called
my office this afternoon and spoke with Mr. Blackburn.

He merely wanted to know the name of the
science which dealt with codes and ciphers. Mr. Blackburn
informed him that the science was known as cryptography,
the messages were cryptograms, and the person working with
them was known as a cryptographer.

Congressman Talle thanked Mr. Blackburn for the
information and stated that on several occasions repre-
sentatives of the Bureau had spoken to groups in Decorah,
Iowa and he had been informed that they were always well
received.

Respectfully,

E. P. Coffey.

RECEIVED
&
INDEXED

80-612-28

FEDERAL BUREAU OF INVESTIGATION

MAY 27 1939

RECEIVED

SAULT

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

SFP:DMS
80-612

July 18, 1939

Handwritten initials

MEMORANDUM FOR MR. NATHAN.

Re: Instruction in Cryptography.

A great many cipher messages were received in the Laboratory during the months of May and June. In May a group of 34 cipher telegrams was received and because of the great amount of work involved in deciphering these telegrams Messrs. Appel, Blackburn and Pickering had numerous conferences with regard to possible methods of solution instead of the usual semi-monthly meetings for study in cryptography. During June another group of 32 telegrams was received and these telegrams were discussed and studied at the conferences during the month of June. The various ciphers currently received from contributors have also been examined either at these meetings or during special conferences.

Respectfully,

E. P. Coffey
E. P. Coffey

RECORDED

80-612-29

FEDERAL BUREAU OF INVESTIGATION
JUL 19 1939
U. S. DEPARTMENT OF JUSTICE
NATHAN
OK

Augusta Maine,
Aug. 18 1939

Federal Bureau of Investigation,
Department of Justice,
Washington, D. C.

80-112-30

FEDERAL BUREAU OF INVESTIGATION

AUG 19 1939

U. S. DEPARTMENT OF JUSTICE

RECORDED
&
INDEXED

Dear Sir:-

If possible will you please let me know where I may be able to get material on cryptography and cryptanalysis. I have enquired of the several police departments and have been referred to this department.

I am employed in the Post Office Adept. in this city and no one here know anything about it. I have been studying it for the last year during my spare time and now cannot find any books (in English) that are of any assistance to me. There is no one in this state that I can find that does that work; so cannot get any material or information where to find any on that subject.

Yours truly,

Thos. R. Ballard
Post Office

Augusta, Maine,

KFC:ON
80-612

October 3, 1939.

MEMORANDUM FOR MR. APPEL,
BLACKBURN
PICKERING

Re: ⁰ Cryptographic Conferences

Henceforth the semi-monthly cryptographic conference will be held regardless of the absence of a single member. In other words a quorum of two will be sufficient to constitute the conference which is devoted to a discussion of current cryptograms and research into cryptographic methods. These meetings will be held on the first and third Tuesdays of the month.

Very truly yours,

K. P. Coffey.

cc-Mr. Ladd

Mr. Tolson _____
Mr. Nathan _____
Mr. E. A. Tamm _____
Mr. Clegg _____
Mr. Coffey _____
Mr. Egan _____
Mr. Glavin _____
Mr. Crowl _____
Mr. Harbo _____
Mr. Lawler _____
Mr. Lester _____
Mr. McIntire _____
Mr. Nichols _____
Mr. Rosen _____
Mr. Sears _____
Mr. Q. Tamm _____
Mr. Tracy _____
Miss Gandy _____

RECORDED

80-612-31

FEDERAL BUREAU OF INVESTIGATION
OCT 4 1939
U. S. DEPARTMENT OF JUSTICE
RECEIVED

OCT 2 10 43 AM '39

LPC:ON
80-612-30

RECORDED

August 24, 1939.

Mr. Thomas R. Ballard
Post Office
Augusta, Maine

Dear Mr. Ballard:

In response to your letter of August 18, 1939, concerning cryptography, it is possible that you may find in local libraries one of the following volumes which may be of interest to you:

"American Black Chamber" by Herbert Yardley

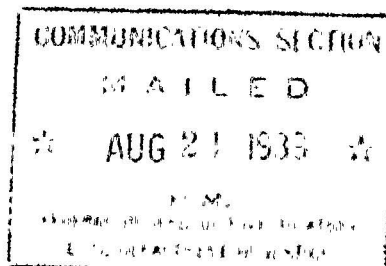
"Secret and Urgent" by Fletcher Pratt,
published by the Bobbs-Merrill Company,
Indianapolis and New York

"Cryptography" by Langie (English Edition).

Sincerely yours,
For the Director

Harold Nathan
Assistant Director

Mr. Tolson _____
Mr. Nathan _____
Mr. E. A. Tamm _____
Mr. Clegg _____
Mr. Coffey _____
Mr. Egan _____
Mr. Glavin _____
Mr. Crowl _____
Mr. Harbo _____
Mr. Lawler _____
Mr. Lester _____
Mr. McIntire _____
Mr. Nichols _____
Mr. Rosen _____
Mr. Sears _____
Mr. Q. Tamm _____
Mr. Tracy _____
Miss Gandy _____



JOHN EDGAR HOOVER
DIRECTOR

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

September 20, 1939

EAT:HA

MEMORANDUM FOR THE DIRECTOR

It is observed from the announcement of correspondence courses offered by the War Department that several courses are given on Cryptography and Cipher Systems. It might be desirable for some member of the Laboratory staff to take these courses in order to improve the Bureau's knowledge of the handling of this type of material.

Respectfully,

Please give this
careful consideration. E. A. Tamm
H.

RECORDED 80-612-3181

PERSON
H. L. LADD

10/13
EPC

10/13
EPC

WGB:ON

3142
October 20, 1939.

Lieutenant Colonel U. B. Akin
U. S. Army Signal Corps
War Department
Washington, D. C.

My dear Colonel:

Mr. E. P. Coffey, Chief of the Technical Laboratory of this Bureau, has advised me of his conversation with you on October 3, 1939, at which time you advised him that a group of reserve officers were commencing a study of ciphers on November 1st, 1939 and that you could arrange for one of the document examiners of this Bureau to attend for approximately 100 hours at a rate of about 10 hours per week.

I greatly appreciate the courtesy shown by you in extending this privilege to one of our men and I am very pleased to designate Mr. W. G. Blackburn of the Technical Laboratory to pursue this suggested course of instruction.

I shall be very pleased if you will advise the date, time and place where Mr. Blackburn should report and any other information which may be necessary for him to properly pursue this course of study.

It is anticipated that he will be available for a total of approximately 100 hours of study at the rate of about 10 hours per week.

Again expressing my appreciation for your courtesy and cooperation in this matter, I am

Sincerely yours,

John Edgar Hoover
Director

COMMUNICATIONS SECTION
MAILED
OCT 25 1939
U. S. DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

Mr. Tolson _____
Mr. Nathan _____
Mr. E. A. Tamm _____
Mr. Clegg _____
Mr. Ladd _____
Mr. Coffey _____
Mr. Egan _____
Mr. Glavin _____
Mr. Crowl _____
Mr. Harbo _____
Mr. Lester _____
Mr. Hendon _____
Mr. Nichols _____
Mr. Rosen _____
Mr. Sears _____
Mr. Quinn Tamm _____
Mr. Tracy _____
Miss Gandy _____

RECORDED COPY FILED IN

JOHN EDGAR HOOVER
DIRECTOR

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

DML:CSH

October 4, 1939

Ind Coffey

MEMORANDUM FOR THE DIRECTOR

9
In line with the attached memoranda from Mr. Coffey, concerning cryptographic instruction, I desire to suggest that Mr. W. G. Blackburn of the Technical Laboratory be assigned to study ciphers at the Army Signal Corps for about 100 hours, at the rate of about 10 hours per week (similar to the training undertaken by Mr. S. F. Pickering of the Laboratory several years ago).

In view of the national emergency, it appears that cipher and cryptographic work will become more important daily, and I believe it would be advantageous for the Bureau to take advantage of this course of training at the present time.

Respectfully,

D. M. Ladd
D. M. Ladd

cryptology Sept 1
Director says
D. K.
Ed
Level 2
183
mm

RECORDED
&
INDEXED

80-612-31X2
FEDERAL BUREAU OF INVESTIGATION
OCT 10 1939
NATHAN

62-75-2991
RECORDED COPY FILED

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

EPC:ON

October 3, 1939

MEMORANDUM FOR MR. LADD

Re: Cryptographic Instruction

In line with our conversation the other day, I talked informally today with Lieutenant Colonel S. B. Akin of the Army Signal Corps. There was also present in his office at the time Mr. Friedman, the Civilian Chief of the Cryptographic Section of the Army Signal Corps. I sounded these gentlemen out as to their receptiveness to having a document examiner from the Bureau undertake cipher study at the Army Signal Corps for about 100 hours at about 10 hours per week in a similar manner to that followed by Mr. S. F. Pickering several years ago.

Lieutenant Colonel Akin was most cordial in this respect and stated that they would be very glad to do this and suggested that November 1st would be a good time to start inasmuch as they were starting a small group of reserve officers at that time. I told him that my inquiry at this time was informal and that I would advise the Director of the fact that the Army Signal Corps was willing to handle this matter and that he would be further advised as to whether or not the Bureau could send a representative.

In view of the anticipated increase in code and cipher work in connection with the Bureau's espionage investigations, I accordingly suggest that the Bureau consider designating either Mr. C. A. Appel or Mr. W. G. Blackburn to undertake this part-time course beginning November 1st. I suggest these two men in view of the fact that they have had considerable cipher experience and therefore would be able to progress most rapidly in the course which is normally a two year affair for beginners.

RECORDED & INDEXED
Respectfully,

E. P. Coffey.

80-612-3112
OCT 10 1939
MAILED
OCT 10 1939
FBI

CAV:OH

October 7, 1939.

b3
b7E

MEMORANDUM FOR MR. LADD

Re: WILLIAM MARCEL DAVIS;
ESPIONAGE.
Cryptographic Analysis.

The examiners have analyzed the original code cable forwarded by teletype from the New York Office dated October 4th as being sent from Berlin to Daycom, New York, signed Baron (Davis) and the translation of this message presented by Mr. Jones. In this cable appear certain new code words, as well as others previously appearing in the recent cables concerning political matters. By applying the translation furnished by Mr. Jones to these words their present meaning has been reestimated as follows:

Rooster means Goering
Heron means Hitler
Moritz Country means United States of America
Rosofish means English Government or the head
of the English Government

The above are new words. Revised meanings for old words are now estimated to be as follows:

"Arzt", which is translated as "doctor" or
"physician" may mean "Doctor Hjalmar Schacht"
who is the economic adviser to the Reich
Government.

"Bidon", previously thought to be "cargo" may
mean "ship" or "shipping".

"Expectable", previously thought to be a business
code abbreviation is now believed to be the
English equivalent of a German expression trans-
lated literally merely meaning "to be expected".

The word "Kleie", the translation of which is "Clay"
or "moldy earth" may mean "stop".

RECORDED
&
INDEXED

32	
FEDERAL BUREAU OF INVESTIGATION	
OCT 9 1939	
U. S. DEPARTMENT OF JUSTICE	
TAMM	TWO

ORIGINAL FILED IN

Mr. Tolson _____
Mr. Nathan _____
Mr. E. A. Tamm _____
Mr. Clegg _____
Mr. Ladd _____
Mr. Coffey _____
Mr. Egan _____
Mr. Glavin _____
Mr. Crowl _____
Mr. Harbo _____
Mr. Lester _____
Mr. Hendon _____
Mr. Nichols _____
Mr. Rosen _____
Mr. Sears _____
Mr. Quinn Tamm _____
Mr. Tracy _____
Miss Gandy _____

10-7-39

"Lunt" translated as "air", may mean "air" or "oil", probably the latter.

"Meyer" now appears to be the code name for Germany.

"Oberin", previously thought to refer to the United States of America, now appears to mean simply "Government".

Copies of the original code cable of October 4th with the code words translated according to the translation of Jones, together with the translation of Jones, are transmitted herewith. In connection with this cable attention is invited to the fact that it is simply addressed "Davcom, New York" and starts immediately with what purports to be a message for the President. This may be an indication of other cables or other communications between Davis in Rome or Berlin and his secretary, Bertzlet, or Jones. Of course, such communications might be by telephone but attention is also invited to the statement of Mr. Jones appended to the translation which he gives wherein he states "Mr. Davis also cabled that the German Foreign Minister has no knowledge of this situation". In this connection attention is also invited to a dispatch in the Washington Star for October 6th dated Copenhagen in which is related that Dr. Schacht, economic adviser to the Reich Government, has already drawn up details of a plan under Hitler's orders in which Scandinavian countries are invited to send representatives to Berlin to discuss new trade agreements whereby the Reich would accept the balance of trade which its blockade prevents neutrals from sending to England and would arrange for transit to the Mediterranean of goods which it could not consume itself. This newspaper clipping is attached hereto.

There are also transmitted herewith a complete list of the revised code words and copies of the cables transmitted with the memorandum of October 2nd giving the new meanings for the code words.

Respectfully,

E. P. Coffey.

EP:ON

October 18, 1939.

MEMORANDUM FOR DOCUMENT EXAMINERS

In accordance with the suggestion of Messrs. Appel and Pickering a segregation will be maintained of photographs of codes, cryptograms, and other unusual messages in espionage and similar cases. The purpose of this segregation will be to provide a file which can be rapidly searched when a current incoming letter is suspected of being prepared in a form similar to one previously received. This segregation will be tried for a period of 90 days to determine its workability and practicability, after which final decision as to its maintenance will be requested of the Bureau.

The procedure for establishing and handling the file will be as follows:

Principal examiners to whom cases of this kind have been assigned will select photographs of letters which in their opinion should be maintained for future reference in this file. These letters will be referred to Mr. Pickering's office where they will be promptly arranged in the file according to the order of receipt (unless some are matched up with others). The filing and maintenance in Mr. Pickering's office will be done by the junior examiners assigned to that office.

Very truly yours,

E. P. Coffey
E. P. Coffey

80-112-33

cc-Mr. Ladd
Mr. Beach
Bureau

Mr. Tolson _____
Mr. Nathan _____
Mr. E. A. Tamm _____
Mr. Clegg _____
Mr. Ladd _____
Mr. Coffey _____
Mr. Egan _____
Mr. Glavin _____
Mr. Crowl _____
Mr. Harbo _____
Mr. Lester _____
Mr. Hendon _____
Mr. Nichols _____
Mr. Rosen _____
Mr. Sears _____
Mr. Quinn Tamm _____
Mr. Tracy _____
Miss Gandy _____

WGB:ON

October 31, 1959.

Colonel S. B. Akin
U. S. Army Signal Corps
War Department
Washington, D. C.

RECORDED

My dear Colonel:

I have for acknowledgement your letter of October 25, 1959, advising that training in cryptography can be furnished to Mr. W. G. Blackburn of our Technical Laboratory and that he should report to Captain Bicher in Room 3412 at 9:00 A. M. on November 1st, 1959.

I want to express to you my appreciation for your courtesy in permitting Mr. Blackburn to attend this course of instruction and he will report to Captain Bicher as suggested at 9:00 A. M. on November 1st, at which time arrangements can be made concerning the time to be spent. At the present time it would appear that it would be preferable for Mr. Blackburn to receive the training three afternoons a week as suggested in your letter.

Again thanking you for your courtesy in this matter, I am

Sincerely yours,

Mr. Adams _____
Mr. Nathan _____
Mrs. A. A. Nelson _____
Mrs. Briggs _____
Mr. Lath _____
Mr. Coffey _____
Mrs. Eggen _____
Mr. Glavin _____
Mrs. Crowl _____
Mr. Harbo _____
Mr. Lester _____
Mrs. Peterson _____
Mrs. Nichols _____
Mrs. Olson _____
Mrs. Price _____
Mr. Charles Tamm _____
Mr. Kelly _____
Miss Percy _____

[Faint, illegible text from bleed-through]

And

November 20, 1939

WCH:jm

62-26873

MEMORANDUM FOR MR. LADD

Re: Cryptographic Instruction

Reference is made to my memorandum of October 3, 1939 with regard to cryptographic instruction for Mr. W. G. Blackburn of the Laboratory.

It was arranged with Colonel Aldin of the Army Signal Corps that Mr. Blackburn pursue a course of instruction in cryptography and cryptanalysis for a total of approximately one hundred hours at the rate of about ten hours per week. Mr. Blackburn reported on November 1, 1939 to Captain Sherr of Colonel Aldin's office at 1 p.m. that day for the initial instruction.

It was arranged that the instruction would be given to Mr. Blackburn by Captain Sherr and that three afternoons a week, Monday, Wednesday, and Thursday from 1 p.m. to 4:15 p.m. would be utilized. Captain Sherr has advised Mr. Blackburn that the first three weeks of instruction will be taken up by elementary and advanced cryptography which will then be followed by a course in cryptanalysis. The elementary and advanced cryptography embraces a study of the methods of enciphering and deciphering cryptograms by the various methods known. The course in cryptanalysis covers the methods of recognizing the type of cipher involved together with methods of deciphering unknown cryptograms.

A further memorandum concerning this cryptographic instruction will be written upon the completion of the course by Mr. Blackburn.

Respectfully,

R. P. Coffey

Mr. Tolson _____
Mr. Nathan _____
Mr. E. A. Tamm _____
Mr. Clegg _____
Mr. Ladd _____
Mr. Coffey _____
Mr. Egan _____
Mr. Glavin _____
Mr. Crowl _____
Mr. Harbo _____
Mr. Lester _____
Mr. Hendon _____
Mr. Nichols _____
Mr. Rosen _____
Mr. Sears _____
Mr. Quinn Tamm _____
Mr. Tracy _____
Miss Gandy _____

80-612-34X

DEC 14 1939

Threat

LADD

CHP. 012

ORIGINAL FILED IN 62-26873-321

New York, N. Y.

DBH:PS

December 8, 1939.

Director
Federal Bureau of Investigation
Washington, D. C.

Re: CRYPTOGRAPHY.

R. L. HEITLINGER, 1356 Walton Avenue,
New York, New York.

Dear Sir:

There are being forwarded to the Bureau, under separate cover, photostatic copies of four volumes on the subject of Cryptography, prepared by DR. R. L. HEITLINGER, a dentist, who resides at 1356 Walton Avenue, New York, New York.

DR. HEITLINGER, who was recently interviewed by Special Agent D. B. Hickman of this office regarding another matter, brought to the agent's attention this work on Cryptography, and at the time he consented that the same be made available for the Bureau if the original volumes were returned to him. In this connection, he stated that in preparing this work he has spent approximately ten years in research and had typed up only one copy for his personal use inasmuch as Cryptography is his hobby.

DR. HEITLINGER'S original work in four volumes is being returned to him personally by an agent of this office.

Very truly yours,

P. E. FOXWORTH
Special Agent in Charge

RECORDED
&
INDEXED

80-612-35
DEC 9 1939
HENDON
L.A.S.

ORIGINAL FILED IN 80-18-1649-1

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

January 3, 1940

SEP:jm
80-612

MEMORANDUM FOR MR. LADD *WHL*

6
Re: Instruction in Cryptography

On December 5, 1939 the regular semimonthly cryptographic conference was held, those being present were Messrs. Appel, Napier and Pickering. I had requested that a discussion be made of the indexing of code words which had been contained in the various coded messages received in connection with various cases.

One important examination in connection with these messages is the checking of the various code words appearing in the different messages for the purpose of determining whether or not any of the same code words appear, indicating that the same code book had been used. Because of the large number of coded words received this becomes a very long drawn out process unless the coded words are filed alphabetically. As a result of the discussion at the meeting regarding the temporary file which was experimentally tried out, it was concluded that the code words of all messages should be filed alphabetically, one code word being on each 3x5 card together with the number of the case.

I am suggesting that this file be maintained in the document room of the Laboratory pending the approval of the executive conference.

There was also a discussion regarding the purchase of additional code books inasmuch as the library of the Laboratory contains only a limited number of these books. I am suggesting a list of code books for purchase in a separate memorandum.

Respectfully,

E. P. Coffey

RECORDED

80-612-36

JAN 5 1940

U. S. DEPARTMENT OF JUSTICE

LADD

CHIEF OF BUREAU

Federal Bureau of Investigation
United States Department of Justice

JAM:ON

Washington, D. C.

January 17, 1940.

MEMORANDUM FOR MR. LADD

Re: Lieutenant G. E. Boone. *JK*

2m
Mr. Naughten of the Tour Room called today and advised that there were a group of Naval Reserve Officers making a tour of the Bureau. He stated that one of the officers, namely Lieutenant G. E. Boone, an architect whose residence is Main Street, Falmouth, Massachusetts, was desirous of talking with me or one of the cryptographers. He stated that he learned from Lieutenant Boone that during his spare time he studied cryptography and lectured to several police agencies in Massachusetts, particularly the Massachusetts State Police. Mr. Naughten stated that it would be impossible for Lieutenant Boone to confer on instant date inasmuch as it was necessary for him to return to his classes at the ONI; however, he had arranged for Lieutenant Boone to communicate with him on a later date and would make it possible, if convenient to me or one of the cryptographers, for him to confer with us.

Respectfully,

E. P. Coffey
E. P. Coffey.

RECORDED
&
INDEXED

80-612-37
SEARCHED
SERIALIZED
INDEXED
FILED
JAN 18 1940
FBI - BOSTON
REH

UNRECORDED COPY FILED IN 44-2-14181

JOHN EDGAR HOOVER
DIRECTOR

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

WGB:RTM

May 28, 1940

MEMORANDUM FOR MR. LADD

Re: Code and Cipher Instruction of
Mr. Blackburn at Signal Corps. *ph*

crypt. May
On May 16, 1940, Mr. W. G. ^VBlackburn
of the Laboratory completed the allotted instruction in
cryptanalysis at the Signal Corps.

Mr. Blackburn spent slightly over a
100 hours at the Signal Corps during which time he received
instruction in the deciphering of cryptograms of the various
types such as substitution, transposition, and combination
of transposition and substitution. Mr. Blackburn informs
me that the instruction was quite thorough and he feels that
he has learned considerable about the deciphering of cryptograms.

Subject to your approval there is
attached hereto a letter to Major General Mauborgne, Chief
Signal Officer, thanking him for making this instruction
available to Mr. Blackburn.

Respectfully,

E. P. Coffey
E. P. Coffey

RECORDED
&
INDEXED

h

80-612- 38	
FEDERAL BUREAU OF INVESTIGATION	
3	JUN 10 1940
U. S. DEPARTMENT OF JUSTICE	
<i>LADD</i>	<i>CLEGG</i>

JOHN EDGAR HOOVER
DIRECTOR

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

LWL:ON

June 12, 1940.

MEMORANDUM FOR MR. LADD

Re: Purchase of Books

It is respectfully requested that the Bureau make arrangements to obtain one copy of Walker's Rhyming Dictionary of the English language which retails for \$4.00.

The above book may be obtained from the local branch of Brentano's Bookstore.

The above-named book is requested for use in crypt-analysis.

Respectfully,

E. P. Coffey.

RECORDED
&
INDEXED

86-612-39
FEDERAL BUREAU OF INVESTIGATION
4 JUN 19 1940
U.S. DEPARTMENT OF JUSTICE
LADD
CHIEF CLK.

sub
6/15/40

W.R.R.

WGB:RTM

June 3, 1940

Major General J. O. Mauborgne
Chief Signal Officer
War Department
Washington, D. C.

My dear General:

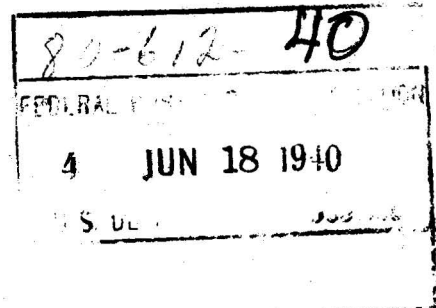
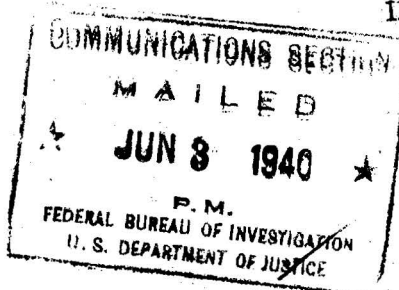
I wish to express to you my appreciation for making available to Mr. ~~W. G.~~ Blackburn of the Technical Laboratory of this Bureau the cryptographic instruction recently afforded to him by the Code Section of your Corps. I am sure that the instruction which he has received will be of great value to him and to this Bureau.

I particularly wish to express my appreciation for the time spent by Captains Sherr, Hays and Bicher with Mr. Blackburn during his course of instruction.

Sincerely yours,

Mr. Tolson _____
Mr. Nathan _____
Mr. E. A. Tamm _____
Mr. Clegg _____
Mr. Ladd _____
Mr. Coffey _____
Mr. Egan _____
Mr. Glavin _____
Mr. Harbo _____
Mr. Hendon _____
Mr. Lester _____
Mr. McIntire _____
Mr. Nichols _____
Mr. Pennington _____
Mr. Rosen _____
Mr. Quinn Tamm _____
Pers. File _____
Adm. File _____
Tele. Room _____
Mr. Tracy _____
Miss Gandy _____

RECORDED
&
INDEXED



WJ. G. P. H. S. R.

WJS:SKL
61-637

New York, N.Y.
July 11, 1940.

Director,
Federal Bureau of Investigation,
Washington, D. C.

Re: REICH-TELEGRAM-ADRESSBUCH

Dear Sir:

Reference is made to Bureau letter of February 7, 1940, directing that a copy of the Reich-Telegram-Adressbuch be obtained from the Central Code Bureau, 76 Broad Street, New York City, for use in connection with the Bureau's crypt-analysis work.

Please be informed that a copy of this book was obtained direct from Europe by T. H. McKenna, Inc., book dealers, which is now being forwarded to the Bureau under separate cover accompanied by a copy of this letter.

Very truly yours,

B. E. SACKETT,
Special Agent in Charge.

RECORDED
&
INDEXED

80-612-41
FEDERAL BUREAU OF INVESTIGATION
JUL 15 1940
U. S. DEPARTMENT OF JUSTICE

ORIGINAL FILED IN 80-11-4030

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

July 17, 1940

LWL:RTM

MEMORANDUM FOR MR. LADD

Re: Purchase of book

It is respectfully requested that the Bureau make arrangements to obtain the latest edition of "Lloyds Shipping Register" which may be obtained from Lloyds, located at 17 Battery Place, New York, New York. This book lists for \$50.00.

The above-mentioned book is desired for use in cryptanalysis.

Respectfully,

E. P. Coffey
E. P. Coffey

RECORDED
&
INDEXED

80-617-42

7/2

I.L.

PAN: MJ

RECORDED 80-612-43

September 9, 1940

MEMORANDUM FOR MR. T. D. QUINN
ADMINISTRATIVE ASSISTANT TO THE ATTORNEY GENERAL

Reference is made to your memorandum of August 16, 1940, concerning the existence in the Library of Congress of the Helle Pabian collection of Baconiana, a set of books relating to codes, ciphers, cryptography and secret writing.

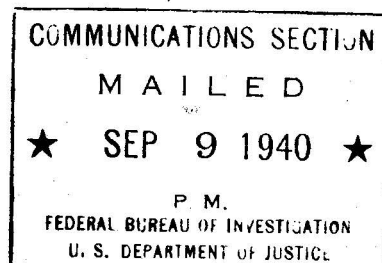
An appropriate study of this material will be made to determine if it contains anything of value for use in connection with the Bureau's cryptographic work.

Very truly yours,

John Edgar Hoover
Director

Mr. Napier is being designated to make a two-day study of this collection.

Mr. Tolson _____
Mr. Clegg _____
Mr. E. A. Tamm _____
Mr. Foxworth _____
Mr. Nathan _____
Mr. Ladd _____
Mr. Egan _____
Mr. Glavin _____
Mr. Nichols _____
Mr. Hendon _____
Mr. Rosen _____
Mr. Tracy _____
Miss Gandy _____



[Handwritten signatures and initials]

T. D. QUINN
ADMINISTRATIVE ASSISTANT TO
THE ATTORNEY GENERAL

Department of Justice
Washington

August 16, 1940

MEMORANDUM FOR MR. J. EDGAR HOOVER
DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

For your information you are advised that the Librarian of Congress has recently informed the Department as follows:

my

"The Nelle Fabyan collection of Baconiana, recently presented to the Library of Congress, proves, upon examination, to contain a large number of books, on codes, ciphers, cryptography and secret writing. These materials are available in the Rare Book Room of the Library of Congress for reference and research under certain conditions. It has occurred to me that members of the staff of your Department might perhaps be interested to know of their presence here."

T. D. Quinn
T. D. QUINN
Administrative Assistant
to the Attorney General.

RECORDED & INDEXED

538
7/45
3

Mr. Tolson	✓
Mr. Clegg	✓
Mr. E. A. Tamm	✓
Mr. Foxworth	✓
Mr. Glavin	✓
Mr. Ladd	✓
Mr. Nichols	✓
Mr. Rosen	✓
Mr. Tracy	✓
Miss Gandy	✓

81-112-43
FEDERAL BUREAU OF INVESTIGATION
2 SEP 11 1940
U.S. DEPT. OF JUSTICE
MAILED

JOHN EDGAR HOOVER
DIRECTOR

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

JAm:AF

September 19, 1940

MEMORANDUM FOR MR. LADD

Mr. Brandt of the National Defense Unit has requested to be furnished with the names of any books which are known or suspected to have been used by foreign countries in the preparation of ciphers.

Mr. Napier of the Laboratory has made a review along this line and there is attached hereto a list of such books. It should be borne in mind that the identity of the book presently being used in the Ducase is of a very highly confidential nature.

Respectfully,

E P Coffey
E. P. Coffey.

RECORDED & INDEXED

80-612-43X
OCT 28 1940
LADD
FIVE

X A review of the cipher methods known to be used by German agents which have come to the Laboratory's attention reveals the names of only three books used or thought to have been intended for such use.

1. X ALL THIS AND HEAVEN, TOO
By Rachel X Field
English Edition

(The above book is in current use in the Ducase and its method of use is known)

2. X WEYER'S TASCHENBUCH DER KRIEGSFLOTEN
1940 Edition

(This book was intended for use in conjunction with a code system, as will be found in the file W. J. H. X Lohrey,)

b3
b7E

3. X CHRISTLICHES VERGLISSEINNICHT
Stuttgart, Germany

(This book is suspected as having been intended for use in connection with some unknown cipher system. Reference is made to Hans X Bauer, 62-23774)

80-612-43X

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

PAN:ATK

October 14, 1940

MEMORANDUM FOR MR. LADD

Re: The Nelle Fabyan
collection of books
relating to codes,
ciphers and allied
subjects recently
added to the Library
of Congress

On August 16, 1940, there was received in the laboratory a memorandum from Mr. T. D. Quinn, Administrative Assistant to the Attorney General, in which it was stated that the above-described collection had been recently bequeathed to the Library of Congress and was available for study.

After a two-day review of this collection of works on cryptography, Mr. Napier, who was assigned the task of studying the same with a view to determining its value in relation to the Bureau's cryptographic work, stated that from this latter viewpoint there is very little of importance. Most of the books in the collection are well over one hundred years old and consequently have very little in them concerning modern ciphers and codes. For one interested in tracing the history of cryptography, or curious about the sources of the simpler present day methods, the collection would be invaluable.

It was noted that in the collection there were 22 copies of various editions of Trithemius' works, the earliest of which was printed in 1564. This

50-612 44

SEARCHED
SERIALIZED
INDEXED
FILED

NOV 1 1940

U.S. DEPT. OF JUSTICE

Page 2
Memo for Mr. Ladd

writer is sometimes known as the "Father of Modern Cryptography". In several of these are translations from the Latin of Trithemius into French by Gabriel de Collange.

The other early writers on cryptography, such as Porta, Vigenere, are also represented by a number of duplicate copies. There is very little in these works, which are written in Latin and French, respectively, to be of any aid to one attempting to solve a modern cipher, since for the most part they are concerned with systems of writing in cipher rather than in descriptions of the means by which such writings may be resolved without the key.

The most recent book appearing in the collection is dated 1917, and contains only a very short chapter on cryptography. The collector of this library, Colonel Fabyan, was more interested in the Baconian theory, than in any other phase of the art. The proponents of this theory insist that Bacon is the author of Shakespeare's plays and attempt to prove this by reading cryptographic messages in the plays themselves.

Mr. Napier borrowed from the Library of Congress a seven-page manuscript containing the names and other data of the books in the above-described collection, and has had a photostatic copy made thereof. This positive photostatic copy is attached hereto for inclusion in the general reference file on cryptography.

Respectfully,

E. P. Coffey
E. P. Coffey.

CIPHERS

- ✓ APPIER (JEAN). Recueil de plusieurs machines militaires.
And also: Methode pour escrire occultement...par l'alphabet.
Pont-Mousson, 1620. In one volume. 8vo., calf.
- ✓ ARCANA ARCANISSIMA hoc est Hieroglyphica Aegyptio-Graeca. 1618.
4to, vellum.
- ✓ BALL (W. W. R.). Mathematical Recreations and Essays. 7 ed.
London, 1917. 8vo. cloth.
- ✓ BAZERIES (COMMANDANT). Les Chiffres Secrets dévoiles. Paris, 1901.
12mo., cloth.
- ✓ _____ Another copy. Paper covers.
- ✓ BEAUDOIRE (THEOPHILE). Genese de la cryptographie. Paris, 1903.
4 to., half morocco. T.-p. has 1902.
- ✓ BECHER (JOHANNES J.). Clavis convenientiae linguarum.
Francofurti, 1661. 12mo., boards. *Printed + p. reads ... Character, po
notitia linguarum universali...*
- ✓ BELLASO, (De Misser Giovan Battista). Il Vero Modo de Scrivere in
Cifra. Small 4to, limp leather, 1564.
- ✓ BOOZ (ADAMAH), (translator). Schutzschrift der Rosenkreutzergesell-
schaft, von dem Engländer Robert de Fluctibus.
Leipzig, 1782. 12mo., boards.
- ✓ BRACHET. Dictionnaire Chiffre...Correspondance occulte. 8vo. paper.
Paris, 1851.
- ✓ BREITHAUP (CHRISTIAN). Ars decifratoria. Helmstadt, 1737.
12mo., boards.
- ✓ _____ Three additional copies in various bindings.
- ✓ BREITHAUP (CHRISTOPHER^{iam}). Disquisitio Historica Critica, Curiosa de
Variis Modis Occulte Scribendi. 4to, folding plate for
Kircher's Cipher, etc. Woodcuts and plates. Small 4to,
half calf. Helmstadt, 1767. 1727
First Edition - rare work on ciphers.
- ✓ BRIDGES (N.). Stenographie and Cryptographie, or the Art of
Short and Secret Writing. London, 1659. 12mo., full calf.
- ✓ _____ Another copy. Calf (worn).
- ✓ BRIGHT (TIMOTHE). Characterie an Arte of shorte, swifte and secrete
Writing by Character. 16mo., calf. London, 1588, reprinted
by Holmes Ulverstone. 1888.
- ✓ BROWN (MAJOR GENERAL). The Lord Digbies Designe to betray Abingdon.
London, 1644. Smal 4to, boards.
- ✓ BULWER (JOHN). Chirologia, or The Natural Language of the Hand.
London, 1644. 12mo., full calf.
- Buscayolo (Marques de). Opusculos--de los servies y Principes
Goberanos de la Cuidad e isla de Scio. Folding plate of
Ciphers, etc. 12mo., old vellum. Valencia, 1669.
- ✓ CARLET (R.M.). La Cryptographie, Contenant une tres-subtile
maniere d'escrire secretement. Toulouse, 1644. 12mo., vellum.
- ✓ CEFFIE (MOISE). Manuscript on his invention of a cipher code. n.d.
Folio, vellum.
- ✓ CHAMPOLLION (M.). Essay on the Hieroglyphic System. 12mo., cloth.
Boston, 1830.
- ✓ COLACO (F.N.). A cryptographia revelata. Pernambuco, 1846.
8vo. boards. *t.p. wanting*

- ✓ COLLETET (FRANCOIS). Traites des Langues Estrangeres de leurs Alphabets et des Chiffres. Small 4to, chiefly Roman type, half morocco. Paris, 1660.
- ✓ COMIERS (d'AMBRUN). Traite de la parole, langues et ecritures. Bruxelles, 1691. 16mo., calf.
- ✓ COMIERS. Traite de la Parole, langues et Ecritures. 12mo. old calf. Bruxelles, 1691.
- ✓ CONRAD (DAVID A.). Cryptographia denudata sive Ars deciferandi. Lugd. Batav., 1739. 8vo., boards.
- ✓ CONRADI (DAVIDES ARNOLDI). Cryptographia Denudata sive Ars Deciferandi. 8vo. boards. *Lugd. Batav. 1739*
- Le Contrespion ou les clefs des toutes les correspondances Secretes. Paris, 1793. 12mo. *(4 copies; 1 half calf, 3 paper)*
- ✓ DALGARNUS (GEORGE). Ars signorum, vulgo Character universalis et Lingua Philosophica. London, 1661. 12mo., full calf.
- ✓ DAVIS (JOHN). An Essay on the Art of Decyphering. London, 1737. 4to, half calf. *2 copies*
- ✓ ~~_____~~ Another copy. 4to half vellum. *In other copy. Paper. London, 1787.*
- ✓ A Treatise on the Art of Decyphering and of Writing Cypher. London, 1772. 12mo., calf.
- ✓ ~~_____~~ Two other copies, London, 1772., various bindings.
- ✓ DEE (JOHN). Monas hieroglyphica. Antwerp, 1564. Small 4to.
- ✓ DONNELLY (IGNATIUS). The Cipher in the Plays, and on the Tombstone. 12mo., cloth. Minneapolis, 1899.
- ✓ DU CARLET (JEAN ROBERT). La Cryptographie Contenant une tres subtile maniere d'escrire secretement. A Toulouse. 12mo. calf. *1644*
- ✓ Ecriture Secrete. Methode Boetzel et O'Keenan. Paris, n.d. Small 4to, cloth. *2 copies*
- ✓ EGENOLFF (CHRISTIAN) (editor). Teutsch Formular und Rhetoric in allen Gerichtshandeln. Frankfort, 1575. 12mo. vellum.
- ✓ ESCANDE (J.). Telescand-Code, vocabulaire pour la correspondance secrete. Paris, 1914. 8vo.
- ✓ FALCONER (J.). Cryptomenysis patefacta, or the Art of Secret Information. London, 1685. 8vo., full calf. *(9 copies)*
- ~~_____~~ *with "The secret and swift messenger"*
~~Three other copies. 16mo., various bindings. London 1641~~
- ~~_____~~ Another copy. 16mo., full calf.
- ✓ ~~_____~~ Another copy. 16mo. old calf. *Rules for plain and deciphering all kinds of secret writing*
~~London 1692~~
~~Another Edition. London, 1702. 16mo., full calf.~~
- ✓ FRIDERICI (JOHANNES BALTHASAR). Cryptographia, oder Geheime Schrift-, mund- und wuckliche Correspondentz. Hamburg, 1684. small quarto, boards. *(2nd copy vellum)*
- ✓ ~~_____~~ *Two* Three other copies. *1685* Small quarto, vellum.
- ✓ ~~_____~~ Another edition, 1685. " " full calf.
- ✓ ~~_____~~ Another copy, 1685. " " old boards.

- ✓ FRY (EDMUND). Pantographia. London, 1799. 8vo., half morocco. (2 copies)
- ✓ GANOE (WILLIAM A.). The English of Military Communications. Menasha, Wis., 1918. 12mo., cloth.
- ✓ Geheime Polizey-Schrift des Grafen des Vergennes. Eisenach, 1793. 12mo. boards.
- ✓ GRAVES (ROBERT). The whole Art of Tachygraphy, by Robert Graves and Samuel Ashton. York, 1775. 16mo., calf. *Front cover leather. Back cover vellum.*
- ✓ HENRICUS (M. LUDWIG). Mysterium Artis Steganographicae Novissimum. Ulmae, 1682. 16mo., half calf.
- ✓ ——— Another copy. Vellum.
- ✓ HERMAN (ANDRE). Stenographie; nouveaux procedes. Cryptographie. Paris, 1859. 8vo.
- ✓ HILTON (JAMES). Chronograms, 5000 and more in number. London, 1882. 4to., half roan.
- ✓ HOFFMAN (WALTER JAMES). The Beginnings of Writing, New York, 1895. 12mo.
- ✓ HULME (F. EDWARD). Cryptography, or the History, Principles and Practice of cipher writing. London, (about 1890).
- ✓ ——— Two other copies
- ✓ JOSSE (H.). La Cryptographie et ses applications a l'art militaire. Paris, 1855. Cloth. *1885*
- ✓ KLAPROTH (J.). Examen Critique des travaux de feu Mr. Champollion, sur les hieroglyphes. Paris, 1852. 8vo. half calf. *1832*
- ✓ KLUBER (D. John). Kryptographik der Geheimschied bekunst Chiffrier und dechiffrierkunst, 8vo. paper. Tübingen, 1809.
- ✓ KORTUM (C.A.). Anfangsgrunde der Entzifferungskunst. Duisburg, 1782. 8vo., boards.
- ✓ LANGIE (ANDRE). Cryptography, New York, 1922, 12mo.
- ✓ LINDENFELS (I.B.). Rettelige Skrivekunst eller Chiffrier af Dechiffrier Kunsten. 8vo. 1/2 calf, Kjobenhavn, 1819.
- ✓ MAILHOL (D.De). Dictionnaire special a clefs multiples. Paris, n.d. 8vo.
- ✓ MARTYS (PETRUS). Prontuario Orthologi-graphico trilingue. Barcelona, (about) 1742. 12mo. vellum.
- ✓ MARCHETTI, (L.). Kryptos. Code telegraphique et postal. Paris, 1898. 12mo., cloth.
- Mercury - See Welkers, John (page 7 of this list)*
- ✓ ~~Mercury, or the Secret and Swift Messenger, London, 1641. 12mo., calf.~~
- ~~++++ Another edition, London, 1695, 12mo., old calf.~~
- ✓ MINK VON WEINSHEUN (STANISLAUS). Dreyfache Kunst-Schnur. Frankfort, 1692. Sm. 4to, 1/2 calf.
- ✓ MORE (ROBERT). Of the First Invention of Writing. (London), 1716. Oblong folio, half calf.
- ✓ MYER (ALBERT J.). A Manuel of Signals. New York, 1872. 8 vo., cloth.

- ✓ Natural History of Nevis and the rest of the English Leeward Charibee Islands in America. Introduction to the Art of Deciphering. 8vo. half cloth, Cambridge, 1745.
- ✓ PALATINO (DI M. GIOVANBATTISTA). Compendio del gran Volume de L'Arte del Beneet leggiadramente Scrivere. 4to, ~~half calf.~~ Venetia, 1578. (2 Copies, 1 half calf, 1 half vellum.)
- ✓ Another copy. 4to, limp vellum. Roma. Very rare, 1545.)
- ✓ PALATINO (Libro di M. Giovanbattiste). Nel qual s'insegna a 1542 Scrivere ogni forte lettera, etc. Small 4to, Roma, 1542.
- ~~Another copy. Half vellum, Venetia, 1578.~~
- ✓ PHIPPS (CHARLES). The Doctrine of Vulgar and Decimal Fractions. 8vo. calf. Dublin, 1745.
- ✓ PLATT (ISAAC HULL). Bacon Cryptograms in Shakespeare. 12mo. Boston, 1905.
- ✓ PORTA (JOHANNES B.). De furtivis literarum notis. Napoli, 1563. Small 4to, half calf.
- ✓ Another copy. Full calf.
- ✓ PORTA (JOAN BAPTISTA) De Furtivis Literarum Notis, vulgo de Ziferis. 4to vellum. Neapoli, 1563. First Edition.
- ✓ PORTA (JOHANNES B.). De furtivis literarum notis. Neapoli, 1602. Folio, full calf.
- ✓ PORTA (JOH. Bapt.) De furtivis literarum notis vulgo Ziferis. Napoli, 1602. 4to, vellum. or folio?
- ✓ Another copy. 4to calf. or folio?
- ✓ PORTA (JOAN BAPTISTA). De Furtivis Literarum Notis vulgo de Ziferis. Small 4to, vellum. Neapoli, 1563.
- ✓ Another copy. Small 4to, vellum. Neapoli, 1563.
- ✓ Another copy. Vellum. 1563.
- ✓ Another copy. 4to, ^{Libro III} old calf, 1591. _{half}
- ✓ PORTA (JOHANNES B.). De Occultis litterarum notis. Montisbelligardi, 1593. 12mo., vellum.
- ✓ Another copy. with this is bound: *magiae naturalis libri*
- ✓ Another copy. 12 mo., half calf. *francofurti, 1597. Vellum*
- ✓ Another edition. Argentorati, 1605. 16mo., calf.
- ✓ PORTA (JOAN BAPTISTA). ^{De 4 furtivis} De Ziferis Libri IIII. 4to, old calf. Londini, 1591.
- ✓ PORTA (JOHANNES B.). Magia naturalis. Libri viginti. Lugd. Batav., 1644. 3 vols. 16mo., half calf.
- ✓ PORTA (JOH. BAPT.). On Secret notations for letters commonly called Ciphers. Translated. Typed manuscript. no date. Folio.
- ✓ Another copy.
- ✓ Regula componendi cipheram communem omnibus: quae interpretari seu deciferari non protest, (and other papers). Roma, 1526. Small 4to, vellum.
- ✓ another copy (paper)

✓ ROMANINI (LE COMTE VESIN DE). La Cryptographie Devoilee. 8vo., half cloth. Paris, 1857.

✓ ROSICRUSIANS. Die theoretischen Bruder oder Zwei Stufe der Rosenkreutzer. Athen, 1785. Half calf.

✓ ROSICRUSIAN CLASSICS. The Fame and the Confession of the Fraternity of R.C. by Eng. Philalethes, London 1652.
✓ Themis Aurea. London, 1656.
✓ The Idea of the Law, by John Heydon. London, 1660.
✓ The Wise Man's Crown, by John Heydon. London, 1664.
Four volumes, 16mo., black calf.

✓ SCHOTT (CASPAR). Schola Steganographica Societatis Jesu. Norimbergae, 1665. 4to. vellum

✓ SCHOTTI (P. GASPARIS). Schola Steganographica in Classes Octo illustrata distributa. Norimbergae, 1680. Small 4to., half calf. "a P. Gaspare Schotto... herbifoli, 1660"
2 copies. 1 half calf + 1 vellum

✓ Another copy. 1665, small 4to, full calf. (2 copies)

✓ SCHOTTI (CASPAR). Schola Steganographica. Norimbergae, 1680. 4to. calf. (2 copies)

✓ SCHRÖTER (CHRYSTOMUS E.) Allzertfertiger Briefsteller. Leipzig, 1748. 12mo., calf.

✓ SELENI (GUSTAVI). Cryptome, Nyctices et Cryptographiae a Johanne Trithemio. 1624, folio, vellum.

✓ SELENUS (GUSTAV). A complete system of Cryptography. Transl. by John W. H. Walden. Typed Manuscript. 3 vols., folio.

✓ SELENUS (GUSTAV). Cryptomenytices et Cryptographiae libri IX. n.p., 1624. Folio, half calf.

✓ SHELTON (THOMAS). Tachygraphy. London, 1641. 16mo., calf.

✓ SHELTON (THOMAS). Tachygraphy. London, 1659. 16mo. calf.

✓ SHINTON (WILLIAM E.). Beauties of Ancient and Modern Penmanship. Lancaster, 1818.

✓ SITTLER (F.J.) Dictionnaire abbreviatif Chiffre. 6 ed. Paris, 1883. 12mo., cloth.

✓ Another edition. 5 ed. Paris, 1882.

✓ SPARTACUS. Die neuesten Arbeiten des Spartacus und Philo in dem Illuminaten-Orden. n.p., 1794. 8vo., boards.

✓ SUNDE (NICHOLAS DE). Steganologia et steganographica aucta, Nurnberg, [about 1720.] 16mo., vellum.

✓ TERCERO (CARLOS). Tratado del origen, y arte de escribir bien. Barcelona, 1768. Folio, calf.

✓ TRITHEME (ABBE). Polygraphie et Universelle esriture Cabalistique. Traduite par Gabriel de Collange. 4to. (2 calf). A Paris, Kerner, 1561. (5 copies) One copy (half calf) has had date changed in ink from 1561 to 1564. Fair Inquis Keruer

✓ TRITHEMII (ABBATIS P.). Polygraphiae Libri Sex. Small 4to., half cloth. Francoforti, 1550.

✓ TRITHEMI (JOANNIS). Polygraphiae Libri sex 12mo., old calf. Coloniae, 1564.

✓ Another copy. 12mo. old calf. Coloniae, 1571.

✓ Another copy. Impunt: R. Amstelredam, Pour Theodore Pierre, 1626

- ✓ TRITHEMIO (JOANNE). ^{huc est} Steganographia Ars per occultam Scripturam. 4to, vellum, Darmstadii, 1621. (2 copies)
- ✓ ~~Another copy, 4to, half cloth, 1621.~~
- ✓ ~~Another copy. Francofurti, 1606~~
- ✓ ~~Another copy. 4to, vellum, Coloniae, 1635.~~
- ✓ ~~Another copy. 4to, calf. Moguntiae, 1676.~~
- ✓ ~~Another copy. 4to, old calf. Norimbergae, 1721.~~
- ✓ TRITHEMIUS (JOHANNES). Libri Polygraphiae VI. Coloniae, 1564. 12mo., vellum, with clasps. Calf
- ✓ ~~Another edition. Argentinae, 1600. 12mo., vellum.~~ with clasps.
- ✓ TRITHEMIUS (JOHANNES). Polygraphiae libri sex. Paesopolitani, 1518. Folio, half calf: full calf (2 copies)
- ✓ TRITHEMIUS (JOHANNES). Polygraphiae libri sex. Coloniae, 1571. 16mo., calf.
- ✓ TRITHEMIUS (JOHANNES). Steganographiae ^{rec non claviculae salomonis} Francofurti, 1606. 4to, half calf. Coloniae ^{agrippinae} 1635, vellum.
- ✓ ~~Another edition. Coloniae, 1635. Boards.~~
- ✓ ~~Another edition. Norimbergae, 1721. 4to, calf. (2 copies)~~
- ✓ TRITHEMIUS (JOHANNES). Viterum sophorum Sigilla et Imagines Magicae, 1612. 16mo., boards. ^{Ernesto Weidmann 1676}
- ✓ Valerianus, Johannes P. Hieroglyphica sive de sacris Aegyptiorum aliarumque gentium literis. Frankfort, on-Main, 1678. 4to., vellum.
- ✓ VESIN (CH. FR.). La Cryptographie devoilee. Bruxelles, 1840. 8vo., half calf.
- ✓ ~~Another copy. Bruxelles 1840 (Paris 1850).~~
- ✓ VESIN (M. CH. FR.). Traite D'Obscurigraphie. 8vo., paper covers. Paris, 1838.
- ✓ ~~Three copies.~~
- ✓ VIARIS (LE MARQUIS DE). L'Art de Chiffrer et Dechiffrer. Paris, n.d. Two copies: 12mo. cloth.
- ✓ VIARIS (MARQUIS DE). L'Art de Chiffrer et Dechiffrer les Depeches secretes. Paris, (about 1890). 12mo., paper.
- ✓ VIGENERE (BLAISE DE). Tracte des Chiffres, on secretes manieres d'escrire. Paris, 1561. 4to., vellum.
- ✓ ~~Another copy. 4to., vellum.~~ ^{Below not previously listed}
- ✓ ~~Another edition. Paris, 1586. 4to., vellum. (2 copies)~~
- ✓ ~~Another edition. 1587. 4to., full calf. (3 copies).~~
- ✓ ~~Another copy. 1587. 4to., vellum~~
- ✓ WILKINS (JOHN). Mathematical and Philosophical Works of. 8vo., calf. London, 1708.

7152 found

- ✓ WILKINS (REV. JOHN). The Mathematical and Philosophical
Work of. 2 vols. 8vo., half vellum. London, 1802.
- ✓ WILKINS (J.). Mathematical Magic, or the Wonders that may
be performed by ~~mathematical~~ ^{Mechanical} Geometry. The Fourth Ed.
London, 1691. 12mo., old calf.
- ✓ WILKINS (BISHOP). Mercury, or the Secret and Swift Messenger.
12mo., half morocco, ^{calf} London, 1641.
First Edition. (2 Copies)
- ✓ _____ Another copy. 12mo., Morocco. London, 1641.
- ✓ _____ Another copy. Second edition. 12mo., calf.
London, 1694. *Printed for Rich. Baldwin*
- ✓ _____ *Second edition. London, Printed for Nathaniel Pells, 1695*
- ✓ WYCK (F. LADG). A Common Writing whereby two although not
understanding one the other's language, yet by the
helpe thereof, may communicate their minds one to
another. Small 4to, calf. Printed for the Author, 1647.
- ✓ YOUNG (THOMAS). An Account of some recent discoveries in
Hieroglyphical literature. 8vo., cloth. London, 1823.

EPC:AF

November 7, 1940

STRICTLY ~~CONFIDENTIAL~~

MEMORANDUM FOR MR. LADD

Re: [REDACTED]
Secret Inks (80-604).
o Cryptography (80-612).

b7D

During the visit last week of [REDACTED]
[REDACTED] both coming under the [REDACTED]
and [REDACTED] of the [REDACTED]
presently assigned to censorship duty, I conferred at considerable
length with [REDACTED] on matters of a Laboratory nature.
[REDACTED] is presently in charge of the censorship work in
Hermuda and although not a technical man is greatly interested
in the technical phases of censorship and has on his staff
people who handle the same. During these conferences, we were
joined at times by Messrs. Pickering, Appel, and Napier of the
Laboratory, as well as Mr. Martin of my office.

During these conferences we discussed at considerable
length the process known as chamfering, which is the invisible
mending of a torn or mutilated document. It sometimes happens
in censorship that an envelope is slit open or torn open for
censorship purposes and after opening the contents are found to
be of such nature that it is considered preferable to forward
the document if possible without any indications thereon that
it has been opened. This is accomplished by a process called
chamfering, according to [REDACTED] He states that women
workers are the most skilled at this, superior to men. As far
as we could gather, the torn edges are carefully beveled with a
special knife and then they are pressed together without the use
of gum or glue, the fibres being worked together by pressure.
The repair must be along a perfect line so that it will not be
discernible. Wherever possible, the envelope is refolded so that
the repair is better hidden in a fold. This latter procedure is
particularly applicable when the envelope was slit along an
original fold. This process was new to us in the Laboratory.

Mr. Tolson _____
Mr. Clegg _____
Mr. E. A. Tamm _____
Mr. Foxworth _____
Mr. Nathan _____
Mr. Ladd _____
Mr. Egan _____
Mr. Glavin _____
Mr. Nichols _____
Mr. Hendon _____
Mr. Rosen _____
Mr. Tracy _____
Miss Gandy _____

INITIALS ON ORIGINAL - 2

80-612-45
TOLSON
CLEGG
TAMM
LADD
FIVE

Memo Mr. Ladd
Page 2

[] explanation was not sufficiently technical to permit us to undertake a test of the process. [] however, offered to have his technicians draw up detailed instructions and a description of the instruments used. He further agreed to send us samples of completed chamfering. For this purpose, we prepared for him several samples of torn envelopes. He will have these repaired in Bermuda and returned to the FBI.

b7D

An extended discussion was had concerning the relative merits of steam and cold humid treatments for the opening of gummed envelopes. There was also discussed a third method of dry opening, by means of a probing instrument. The only new development brought forth in this discussion was the information furnished by [] that Japanese in their more important documents are using a special sealing gum which contains egg yolk. When any dampness sufficient to release the seal reaches the egg yolk it immediately runs thus giving vivid evidence that the envelope has been tampered with. In such situations it was agreed that dry probing was the only possible means of opening such a seal. We in the Laboratory furnished [] with the formula and procedure for detecting previous efforts at dampening. This is known as the liquid iodine test.

With regard to codes and ciphers we were informed by [] that the [] of the [] is equipped to handle some codes and ciphers. These, however, are practically limited to those occasional ones discovered in letters or telegrams passing between individual foreign agents. They usually have no occasion to attempt to decode the more difficult diplomatic codes. As a matter of fact if they are unable to solve their own codes and ciphers they are then referred to the cryptanalysis section of the []. This latter is the highly developed cryptographic section of the [] which is equipped to handle foreign and diplomatic codes and ciphers. [] was unable to state whether that latter section was able to break the German diplomatic code but it was his impression they have not been so able, to date.

Mr. Tolson _____
Mr. Clegg _____
Mr. E. A. Tamm _____
Mr. Foxworth _____
Mr. Nathan _____
Mr. Ladd _____
Mr. Egan _____
Mr. Glavin _____
Mr. Nichols _____
Mr. Hendon _____
Mr. Rosen _____
Mr. Tracy _____
Miss Gandy _____

Secret inks and their detection are handled by chemists of the censorship who are directly under Head Chemist S. W. Collins. Collins is an old hand at this work, was prominent in the last

Memo Mr. Ladd
Page 3

World War and is referred to in Tardley's American book "The Black Chamber". Barrilar discussions between des Gras and myself on secret inks have since been referred to Collins by des Gras. A message was brought back that Collins was in full accord with the FBI Laboratory's views on secret inks and had no additional suggestions to offer. However, in a subsequent discussion Mr. Harbert informed me in a highly confidential manner that they had discovered that foreign secret agents dropped by plane at night with parachutes and subsequently captured were found to have on their person a new form of secret ink made up from the chemical "pyramiden". I immediately arranged for the purchase of a sample of "pyramiden" and Mr. Plastering is working with it in the laboratory and seeking its complementary detector.

We discussed packages, strings, and seals. The only new development was the statement by [] that wherever possible strings and wrappings should be slipped off packages without being untied and without breaking any wire seals on the package than necessary. Where it is necessary to break seals and write the string we were all in accord on methods.

I requested [] to furnish a sample of the "prisoners' paper", which is a special paper considered not receptive to secret inks and which is furnished by the Government to Internees and prisoners for correspondence purposes.

[] was particularly interested in the development of latent fingerprints on paper--the use of a special lamp for reading indented writing--and methods of photographing carbon paper to bring out the impressions thereon--and the use of contact photographic printers for rapid photographing of documents. All these things were shown to him. [] was also particularly interested in sound recording.

I showed him the type of disc recorder (the Presto type) used by the Bureau. He stated he has immediate need for a sound recorder in Bermuda and was planning the purchase of one in New York to carry back with him. He stated he had already looked at some in New York and was considering the purchase of one cheaper than that used by the Bureau. In this connection, I was very much interested when reading the censorship manual which was furnished the Director by these three gentlemen that as part of the regular censorship in England they tap the telephones of citizens (unbeknown to them) for the purpose of getting a cross-section of public opinion. The manual states " - six teams

b7D

Mr. Tolson _____
Mr. Clegg _____
Mr. E. A. Tamm _____
Mr. Foxworth _____
Mr. Nathan _____
Mr. Ladd _____
Mr. Egan _____
Mr. Glavin _____
Mr. Nichols _____
Mr. Hendon _____
Mr. Rosen _____
Mr. Tracy _____
Miss Gandy _____

Memo Mr. Ladd
Page 4

of censors who move from town to town and cut in on both local trunk lines and incoming toll lines into that town listen at random and make précis of the conversation heard for the purpose of summarizing public opinion - state of the morale - rumor mongering, etc."

During these conversations I was also informed that the present censorship staff at Bermuda has increased to 500 persons, that they have taken over a whole resort hotel. Many of these employees are women and many of them have been brought over from London. It was further inferred that the censorship staff would be rapidly increased to 1,000 and possibly 2,000 persons. These gentlemen again urged that an FBI representative visit Bermuda and make a study of censorship organization and their method of procedure.

Respectfully,

E. P. Coffey.

Mr. Tolson _____
Mr. Clegg _____
Mr. E. A. Tamm _____
Mr. Foxworth _____
Mr. Nathan _____
Mr. Ladd _____
Mr. Egan _____
Mr. Glavin _____
Mr. Nichols _____
Mr. Hendon _____
Mr. Rosen _____
Mr. Tracy _____
Miss Gandy _____

FEDERAL BUREAU OF INVESTIGATION

Laboratory

Date 1/30/41 1940☐ Director☐ Mr. Ladd☐ Mr. H. H. Clegg☐ Mr. Nathan☐ Mr. E. A. Tamm☐ Mr. Tolson☐ Mr. Glavin☐ Mr. Hendon☐ Mr. Renneberger☐ Mr. Q. Tamm☐ Single Fingerprint☐ Chief Clerk☐ Stenographer☐ Files☒ Mr. Hince

room - 5243

E. P. COFFEY

EAT:DS

January 14, 1941

80-612-46

Brigadier General Sherman Miles -
Assistant Chief of Staff
G-2, War Department
Washington, D. C.

PERSONAL AND CONFIDENTIAL

Dear General Miles:

With reference to your recent discussion in my office of material which we have requested from the British authorities on the subject of cryptography, I have ascertained that the Bureau's representatives in England were not requested to obtain any specific data. Instructions issued to Mr. Clegg and Mr. Hince upon their departure from Washington were to obtain general information on the method of handling cryptography in all of its aspects in England. Information was requested as to the methods of operation, size and selection of the operators and all other general information which could be obtained relative to the code and cipher sections actually operating in Great Britain. The instructions were issued in the most general terms in order to allow the widest possible latitude for the Bureau's representatives in obtaining data.

I trust that this information will be of some interest to you.

Sincerely yours,

J. Edgar Hoover

John Edgar Hoover
Director

Mr. Tolson _____
Mr. Clegg _____
Mr. E. A. Tamm _____
Mr. Foxworth _____
Mr. Nathan _____
Mr. Ladd _____
Mr. Egan _____
Mr. Glavin _____
Mr. Nichols _____
Mr. Rosen _____
Mr. Tracy _____
Miss Gandy _____

4192

COMMUNICATIONS SECTION
MAILED
★ JAN 15 1941 ★
<u>By special messenger</u>
FEDERAL BUREAU OF INVESTIGATION U. S. DEPARTMENT OF JUSTICE



RECEIVED
U. S. DEPT. OF JUSTICE
JAN 15 1941

EAT: DS

January 14, 1941

RECORDED 80-612-46

Rear Admiral Walter S. Anderson
Director
Naval Intelligence
Navy Department
Washington, D. C.

PERSONAL AND CONFIDENTIAL

My dear Admiral:

With reference to your recent discussion in my office of material which we have requested from the British authorities on the subject of cryptography, I have ascertained that the Bureau's representatives in England were not requested to obtain any specific data. Instructions issued to Mr. Clegg and Mr. Hince upon their departure from Washington were to obtain general information on the method of handling cryptography in all of its aspects in England. Information was requested as to the methods of operation, size and selection of the operators and all other general information which could be obtained relative to the code and cipher sections actually operating in Great Britain. The instructions were issued in the most general terms in order to allow the widest possible latitude for the Bureau's representatives in obtaining data.

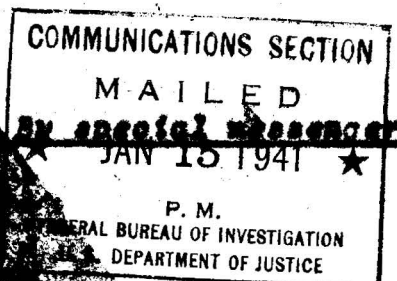
I trust that this information will be of some interest to you.

Sincerely yours,

J. Edgar Hoover

John Edgar Hoover
Director

Mr. Tolson _____
Mr. Clegg _____
Mr. Glavin _____
Mr. Ladd _____
Mr. Nichols _____
Mr. Rosen _____
Mr. Tracy _____
Miss Gandy _____



4193

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.
January 8, 1941

EAT:HA

MEMORANDUM FOR THE DIRECTOR

With reference to your inquiry concerning the information Mr. Clegg and Mr. Hince were to obtain in England on the subject of cryptography you are advised the request for data was made in the most general terms. Originally discussion was had as to the desirability of taking to London a qualified and experienced cryptographer but this idea was rejected. Mr. Coffey talked with Mr. Hince and Mr. Hince agreed to obtain a general report on the methods, size and operation of any code and cypher section operating in Great Britain to which Mr. Clegg and Mr. Hince might have access. Mr. Clegg and Mr. Hince were to obtain all possible information pertaining to codes, cyphers, methods of handling, etc, but as indicated the request was made in the most general terms.

Respectfully,

Ea
E. A. Tamm

*Send letter to Miles &
Anderson explaining that
on checking what I found.
d.*

*Letter Miles & Anderson
1-14-41*

RECORDED

d

80-612-416	
FEDERAL BUREAU OF INVESTIGATION	
3	JAN 17 1941
U.S. DEPARTMENT OF JUSTICE	LABORATORY

0

80-612-45X (Not Recorded)

OFFICE OF CHIEF OF NAVAL OPERATIONS BULLETIN

SUBJECT -- CRYPTANALYSIS --- BULLETIN No. 65

ALSO

80-612 (Not Recorded)

LLOYD'S REGISTER OF SHIPPING

71, FENCHURCH STREET, LONDON, E. C. 3

ENGLAND.

11th November, 1940

NOTE::: The above have been removed from file and
sent to Mr. Blackburn in 1410, at his request,
and upon Ed Bostons authorization, by
Ralph D. House.

Ralph D. House

Received - 12/15/41
WJB
12/15/41

Page two.

of repairing envelopes called chamfering. This process is used by the British in connection with censoring activities. If an envelope has been opened by cutting on one end the flap is removed and the cut flap is refastened to the main body of the envelope by splitting the paper on the flap and on the body and sticking the two together with paste and with pressure so that at this point the completed job resembles the regular machine fold in the paper. This is a very delicate job requiring expert technique and is usually not attempted on envelopes with a printed background like air mail envelopes because of the necessity of matching the printing. In connection with the chamfering operation it is necessary to recut the flaps so that one edge is actually shorter than the other. The flaps on this envelope are actually shorter on one edge than the other and the top flap is also displaced in position.

The examiner reports that microscopic examination of the mark on the edge of the envelope shows a strong resemblance to chamfering although the printing matches with great fidelity. The usual chamfering is comparatively easy to detect by microscopic examination because sufficient care is not taken in the work which is not performed under a microscope. The examiner called attention of another examiner to the appearance of the edge under the microscope and the condition observed by the first examiner was not as clear to him. The machine fold such as that on the bottom of this envelope very closely resembles chamfering if this is expertly done.

Regardless of the possibility of repairing the envelope by chamfering on the right-hand edge there is no question but the envelope has been opened on the flap and for this reason further examination of the edge was abandoned.

The envelope is returned herewith.

Respectfully,


E. P. Coffey

ENCLOSURE

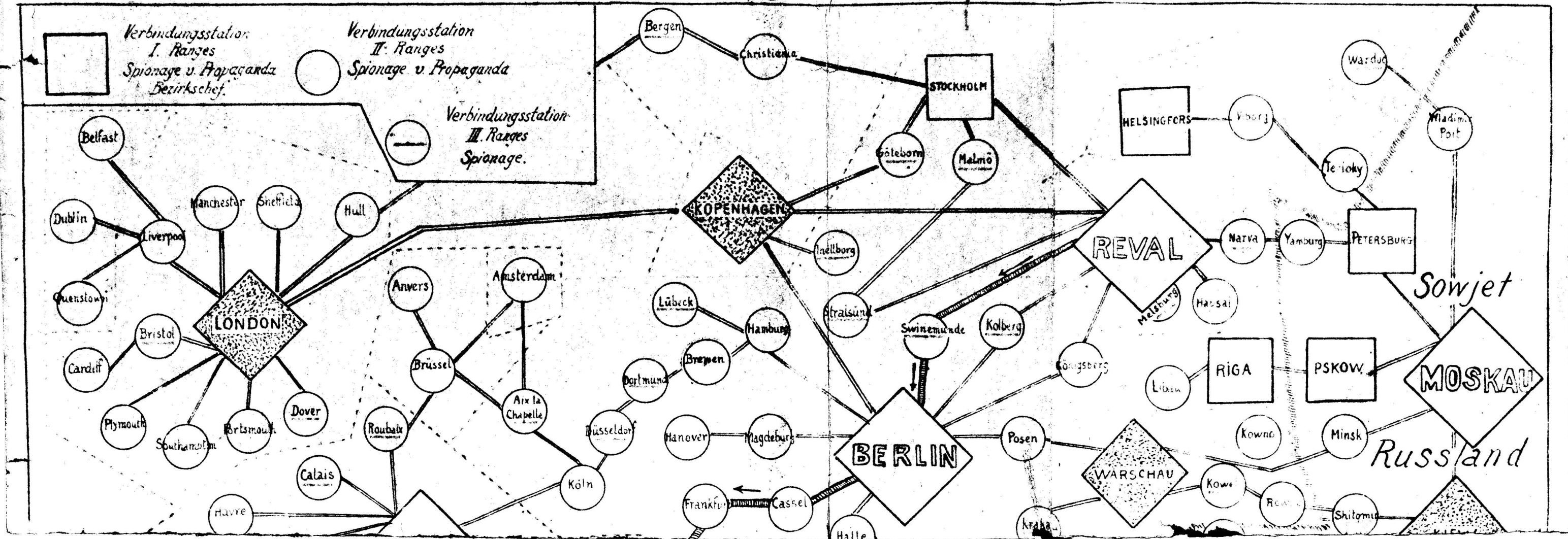


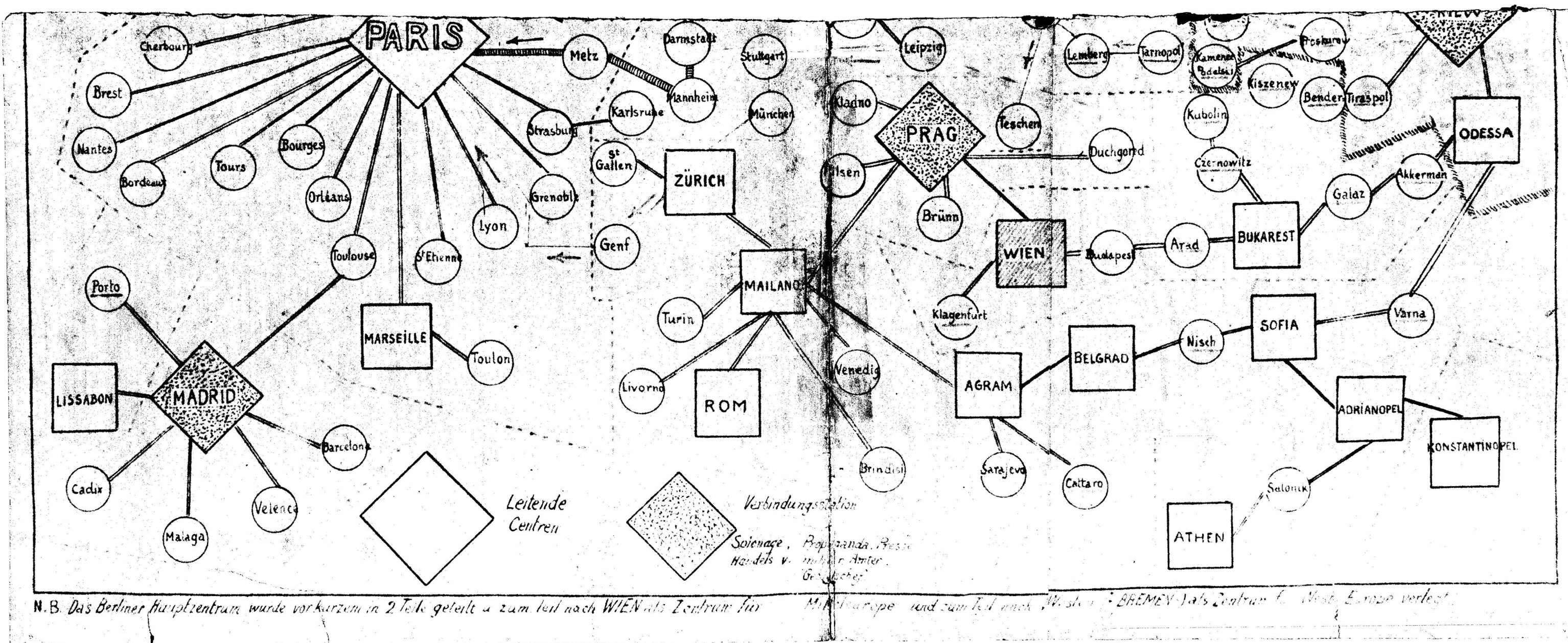
46X

Organisation der bolchewistischen Propaganda

Officielle und geheime Organisationen.

C.





FEDERAL BUREAU OF INVESTIGATION
UNITED STATES DEPARTMENT OF JUSTICE
WASHINGTON, D. C.

OFFICIAL BUSINESS

PENALTY FOR PRIVATE USE TO AVOID
PAYMENT OF POSTAGE, \$300

ENCLOSURE

VIA AEREA
PAR AVION

VIA
PAN AIR



S E L L S

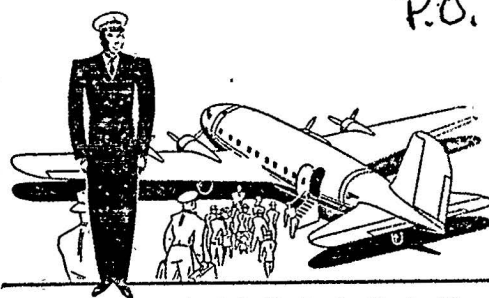
Mr. Sam Eldridge,

P.O. Box 482,

Grand Central Annex,

New York, N.Y.,

U.S.A.



PAN AMERICAN AIRWAYS SYSTEM

80-612-47

RECEIVED TO



b3
b7E

✓

RECORDED
86-

612-49
EPC:AF

February 20, 1941

Dr. Charles F. Kettering
Chairman
National Inventors' Council
Department of Commerce Building
Washington, D. C.

Attention: Mr. J. C. Green
Assistant Chief Engineer

Dear Dr. Kettering:

Reference is made to Mr. Green's letter of February 6, 1941, advising that the National Inventors' Council maintains a file relative to cryptography, coding and decoding machines.

The Council's offer to make this file available for study by technicians of the Bureau's Laboratory is ~~and~~ appreciated and they will undoubtedly ~~use~~ use of the material contained therein from ~~time~~ to time.

Sincerely yours,

Mr. Tolson _____
Mr. Clegg _____
Mr. E. A. Tamm _____
Mr. Foxworth _____
Mr. Nathan _____
Mr. Ladd _____
Mr. Egan _____
Mr. Glavin _____
Mr. Nichols _____
Mr. Hendon _____
Mr. Rosen _____
Mr. Tracy _____
Miss Gandy _____

112
COMMUNICATIONS SECTION
FEB 21 1941
RECEIVED

JK

DEPARTMENT OF COMMERCE
THE NATIONAL INVENTORS COUNCIL
WASHINGTON
February 6, 1941

Director John Edgar Hoover
Federal Bureau of Investigation
Department of Justice
Washington, D. C.

Attention: Technical Laboratories

Dear Mr. Hoover:

The National Inventors Council is receiving from the general public a variety of suggestions relative to cryptography, coding and decoding machines. While it is believed that none of these suggestions approach the devices already known and in use by the governmental agencies, a complete file of material has been made and is available to your department at any time you may wish.

The purpose of this letter is to furnish you with the above information concerning said file since yours is one of the few divisions of the Government which would be interested in the material of this special and confidential character.

Very truly yours,

John C. Green
J. C. Green
Assistant Chief Engineer

*202
Jan 17*

JCG/mch

RECORDED
&
INDEXED

*Copy of this letter
filed in Cryptography
file - 141 - Ltr*

81-112 49	
FEB 26 1941	
U.S. DEPT. OF COMMERCE	
TECHNICAL LABORATORIES	

WCL

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

EPC:AF
80-612

February 25, 1941

MEMORANDUM FOR MR. LADD

Re: German Books
Possibly Cipher Keys

Supervisor Kimball advised me that Mr. Samuel Klaus of the Treasury Department telephoned. The Treasury Department is examining an importation, on the part of the German Embassy, of 41 packing cases containing books. Within these packing cases there are several hundred small packages each containing three or four books having the following titles:

'DIE BURGER VON CALAIS
/DAS FESTE HERZ
DER TOD IN POLAND
DOKUMENTE POLNISCHER GRAUSAMKIST

These packages are individually addressed to different persons throughout the United States. I understand that a list of these addressees is being obtained by Mr. Kimball. Superficially, the above-entitled books appear to be propaganda books concerning the recent occupation of European countries by the German armies.

In addition to the small packages described above, there are several thousand loose books in the shipment intended for the Embassy. Apparently these are of as many different titles. Klaus sent over two of these books picked at random out of these thousands. The two have the same title and appear to be different editions of the same book entitled "Leselust" by Richard Lange, Otto Ubbelohde and Franz Markau. This appears to be a primary school book in reading and elementary writing.

Supervisor Kimball advises me that it is Mr. Klaus' suspicion that these books are either code books or books which may be used for cipher keys. He states that Mrs. Freedman of the Cryptanalysis Section of the Coast Guard has looked some of them over.

RECORDED & INDEXED

A note is being made of the titles submitted as listed above. These will be used for references for cipher keys in the event any of the persons in the list of addressees which Mr. Kimball is reporting appear in any subsequent cryptographic problems which the Bureau's Laboratory may receive.

80-612 50
RECEIVED BY INVESTIGATION
U.S. DEPT. OF JUSTICE

46

Memo Mr. Ladd

Page 2

If the Treasury Department prepares an invoice of all of these several thousand volumes, a copy should also be obtained for the Bureau in view of the possible value of such a list in any subsequent problem concerning books used for cipher keys. Apparently some of the books are in the Congressional Library, inasmuch as Klaus obtained and furnished a copy of DIE BURGER VON CALAIS from the Congressional Library where it was found bound together with a group of small German propaganda pamphlets under the title ~~MUNCHENER~~ LAIENSPIELE (PT-1268 .M8).

The books in question are being returned to Mr. Klaus, Room 192, Treasury Department, who desired them before 2 P. M. Wednesday.

Respectfully,

E. P. Coffey
E. P. Coffey.

**Federal Bureau of Investigation
United States Department of Justice**

POST OFFICE BOX 812
CHICAGO, ILLINOIS

409
3/14
345

March 7, 1941

Director
Federal Bureau of Investigation
Washington, D. C.

Dear Sir:

For the Bureau's information I am transmitting herewith a number of cards which were submitted to this office by Earl L. Fiske of the brokerage firm of Seavey & Flarsheim, 221 North LaSalle Street, Chicago, Illinois. These cards serve as an example of the cipher which has been worked out by Mr. Fiske. I am likewise transmitting herewith a copy of Mr. Fiske's communication dated February 20, 1941.

This is being forwarded to the Bureau for whatever informational value it might have. It would be appreciated if the Bureau would return these cards containing the cipher explanation as soon as they have served their purpose in order that the same may be returned to Mr. Fiske.

Very truly yours,

W. S. Devereaux

W. S. DEVEREAUX,
Special Agent in Charge.

WSD:MG
Encs.

RECORDED & INDEXED

5
EX-113
m
de
(b)

10-612-51	
FEDERAL BUREAU OF INVESTIGATION	
3	MAR 10 1941

C O P Y

SEAVEY & FLARSHEIM BROKERAGE CO.
LaSalle-Wacker Bldg.
221 N. LaSalle Street,
CHICAGO

February 20, 1941

Special Agent in Charge
Federal Bureau of Investigation
P. O. Box 812
Chicago, Illinois

Dear Sir:

In connection with my recent call pertaining to a cipher which I have developed and which I think has some basis for merit in its use, I enclose cards numbered one to seven inclusive in explanation of the cipher.

My particular interest is one of curiosity to determine whether it has any real value as a cipher; from the angle of coding where it is not too bulky and yet easily deciphered by those having the key, yet difficult to decipher without the key.

The cipher, of course, has many variations which I believe a man acquainted with this work can readily appreciate. I am using the simple alphabet with corresponding numbers from one to twenty-six as shown on card No. 1. Cards No. 2, 3 and 4 show the alphabet expressing the number of the letter in denominations which total the figure. For example, take the letter G, which is "7" on card No. 3. You will see that I have expressed "7" in thirty-six different ways, which gives us a large number of frequencies. Then on card No. 5 I have taken the sentence "The quick brown fox jumps over the lazy dog" and for quick assistance in coding I have placed under the letters the corresponding numbers. On card No. 6 I have written these numbers, but I have broken up the (three sequences) by intervening dashes and these can be given in any form, even with the insertion of letters and words, as you will see on Card No. 7, which greatly confuses the numerical order, and to decipher all one need do is set off the letters in series of threes, totaling each group of three. For example "5-8-7" gives you "20" and 20 is "T"; "3-1-4" totals "8" and represents "H"; "3-0-2" totals "7" and represents "E".

Would you mind passing this on to the proper party and if the cipher is of any value in Government use, naturally you are free to use it. However, I should like an acknowledgment as to the merits and whether or not the problem #7 could be readily deciphered by your expert.

- 2 -

Thank you very much for your courtesy in letting me know the outcome.

Yours very truly

/s/ EARL L. FISKE

ENCLOSURE



FEDERAL BUREAU OF INVESTIGATION
U.S. DEPARTMENT OF JUSTICE

PENALTY FOR PRIVATE USE TO AVOID
PAYMENT OF POSTAGE, \$300.

OFFICIAL BUSINESS

ENCLOSURE TO BUREAU - CHICAGO
OFFICE LETTER, 3/7/41 re: Cipher
developed by Earl L. Fiske

HOW TO USE THE SPECIAL GUM.

43584

Place in the small beaker approximately equal volumes of the ^{two} solutions; if anything, take slightly less of the thin solution. Mix thoroughly with the glass rod then apply with the rod to the surface which is to be stuck, using only a thin film of liquid. The gum will then solidify for ever.

NOTES.

Press the surfaces together and iron with the electric iron at "silk heat".

1. The two solutions last for ever if kept ^(in well stoppered bottles) separately, when mixed the mixture will keep fluid for about half an hour at room temperature. It solidifies almost instantaneously when heated. It is therefore important to make sure that the solutions do not become mixed with each other in the bottles, as for instance might happen if a dirty rod is used. Also only just enough for the job on hand should be mixed each time as the stuff left over is always wasted.
2. The original gum on envelopes must always be removed first from all the flaps. It is a good plan to have ready a stock of envelopes with the lower flaps already stuck down with the special gum. Should you be doing a job which takes more than 30 minutes to finish then you will have to make up more than one small batch of mixture. As soon as the gum has begun to solidify in the beaker it's adhesive properties are lost.
3. The mixture is quite soluble in water before ironing. Any extra which has squeezed from the envelope flaps can be blotted off or washed away with water. After ironing, touching up becomes practically impossible owing to the complete insolubility in all solvents of the hardened gum.
4. You should be careful to withdraw the thick solution out of the bottle with a glass rod without touching the ground neck. If the solution gets between the stopper and neck you will have a lot of trouble with the stopper sticking.

RECORDED COPY FILED

File 80-612

March 10th, 1941.

Scientific & Testing,
Imperial Censorship,
Hamilton
Bermuda.

RECORDED

80-612 511
FEDERAL BUREAU OF INVESTIGATION
1 SEP 2 1941
U.S. DEPARTMENT OF JUSTICE

Cryptography

12/12/41 can check with admin

On His Majesty's Service

43582

security - gun

PAN:EK

March 31, 1941

AIR MAIL

80-612 -51

Special Agent in Charge
Chicago, Illinois

Dear Sir:

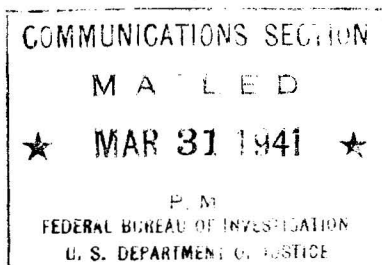
Reference is made to your letter of March 7, 1941 transmitting seven cards bearing descriptive data relative to a cipher system devised by Earl L. Fiske of 221 North LaSalle Street, Chicago, Illinois, and also a copy of Mr. Fiske's letter of transmittal.

You are advised that the cipher system described by Mr. Fiske is from a practical standpoint of very little merit. First of all, it is uneconomical in that it requires the transmission of a text at least three times as large as that of the secret message it conveys, and therefore the cost of telegraphic transmission alone would be prohibitive whenever a large amount of correspondence was involved. Secondly, the cipher system presents no great difficulty of solution since a grouping of the entire series of digits constituting the cryptogram into triads and a totaling of the sums of the digits comprising these triads yield a series of numbers wherein each letter of the secret message is invariably represented by the same number. Thus, it becomes possible to reduce a cryptogram in this system to the terms of a monalphabetic or simple substitution cipher. This latter type of cipher yields very readily to solution by means of the application of the well known principles of frequency.

In accordance with your request, the seven cards of descriptive data referred to in the first paragraph are being returned herewith, appropriate copies thereof having been placed in the Laboratory's Cipher Key Reference File.

Very truly yours,

John Edgar Hoover
Director



WGB:AF

February 27, 1941

Major General J. O. Mauborgne
Chief Signal Officer
United States War Department
Munitions Building
Washington, D. C.

Dear General Mauborgne:

I wish to express to you my appreciation for making available to Messrs. Blackburn and Napier of the Technical Laboratory of this Bureau the week's advanced cryptographic instruction concerning double transposition ciphers.

I am sure that the instruction which was given will be very helpful in connection with the work of the cryptographic section of the Technical Laboratory.

Sincerely yours,

W. F. SHAW

81-111-52
RECEIVED
FEB 28 1941
21
1941

Mr. Tolson _____
Mr. Clegg _____
Mr. E. A. Tamm _____
Foxworth _____
Lathan _____
Ladd _____
Egan _____
Glavin _____
Nichols _____
Tracy _____
Gandy _____

COMMUNICATIONS SECTION
MAILED
FEB 28 1941
U. S. DEPARTMENT OF WAR
WASHINGTON, D. C.

C.A:DNJ

April 10, 1941

80-612-53

Mr. H. S. Bacon
276 Bellevue Street
West Roxbury, Massachusetts

Dear Mr. Bacon:

Reference is made to your letter dated March 13, 1941 advising that you have perfected a cipher system suitable for use by an individual working alone or adaptable to transmission by wire or radio.

The Bureau is not at this time interested in purchasing any ciphers or codes; however, should you care to furnish the details they will be placed on file and consideration given to your plan in the event that a cipher is required. Such information as you may care to furnish may be given to Mr. W. G. Peterson, 10 Post Office Square Building, Room 1016, Boston, Massachusetts.

Your interest in advising the Bureau of your system is greatly appreciated.

Sincerely yours,

John Edgar Hoover
Director

cc-Boston

Mr. Tolson _____
Mr. E. A. Tamm _____
Mr. Clegg _____
Mr. Foxworth _____
Mr. Nathan _____
Mr. Ladd _____
Mr. Glavin _____
Mr. Nichols _____
Mr. Hendon _____
Mr. Rosen _____
Mr. Tracy _____
Miss Gandy _____

XZ
9 am
3/26



HENRY S. BACON
PRES. & GENERAL MGR.

P. O. WEST ROXBURY
MASS.

276 Bellevue St.,
West Roxbury, Mass.,
March 13, 1941.

Mr. J. Edgar Hoover,
Federal Bureau of Investigation,
Washington, D.C.

Dear Sir:

For some time now, I have been endeavoring to interest the cryptographers of both the Army and the Navy in a new cipher system that has been perfected after several years work.

This cipher cannot be deciphered by anyone who has not the specific key tape and method used to encipher, in fact both Army and Navy experts now have test messages and other data explaining the functioning of this system.

The cipher is suitable for use by the individual working alone or it may be adapted for transmission by wire or radio by use of a simple and inexpensive adjunct to a standard teletype, radiotype, electric typewriter or other transmitting receiving or printing mechanism that is electrically operated.

For years I have tried to secure unbiased consideration of this cipher system without avail.

I am willing to submit this cipher to any test under any circumstances in competition with any other cipher system or cipher machine for its simplicity, security, speed, efficiency and general adaptability and economy.

Would your great organization be interested in more details?

Most sincerely,

H. S. Bacon
H. S. Bacon

CWai

RECORDED & INDEXED

80-612-53
FEDERAL BUREAU OF INVESTIGATION
5 MAR 17 1941
U. S. DEPARTMENT OF JUSTICE

FEDERAL BUREAU OF INVESTIGATION
UNITED STATES DEPARTMENT OF JUSTICE

To: COMMUNICATIONS SECTION.

WGB:AF

APRIL 15 1941

Transmit the following message to: SAC NEW YORK

(b) OBTAIN IMMEDIATELY AND FORWARD TO BUREAU LATEST
CATALOGS OF HAGELIN CRYPTOGRAPHY, BOTH HAND OPERATED
AND ELECTRICALLY OPERATED TYPES, FROM STUART HEDDEN
FOUR FOUR WALL STREET NEW YORK CITY.

HOOVER.

RECORDED

NOT RECORDED

80-612-55

FEDERAL BUREAU OF INVESTIGATION	
5	APR 18 1941
U.S. DEPARTMENT OF JUSTICE	

9 33 PM

Per

SENT VIA

FEDERAL BUREAU OF INVESTIGATION
U. S. DEPARTMENT OF JUSTICE
COMMUNICATIONS SECTION

APR 15 1941

TELETYPE

FBI WASH DC 4-15-41 9-23 PM DCN

SAC, NEW YORK.

OBTAIN IMMEDIATELY AND FORWARD TO BUREAU LATEST CATALOGS OF HAGELIN
CRYPTOGRAPHER, BOTH HAND OPERATED AND ELECTRICALLY OPERATED TYPES,
FROM STUART HEDDEN FOUR FOUR WALL STREET NEW YORK CITY.

HOOVER

A AND H

OK FBI NYC HP

May 16, 1941

RECORDED WGB:EHJ
80-612-56
Special Agent in Charge
Boston, Massachusetts

Re: Henry S. Bacon
276 Bellevue Street
West Roxbury, Massachusetts

Dear Sir:

Reference is made to your letter of April 21, 1941 in which you forwarded to the Bureau information concerning a ciphering and deciphering device demonstrated to you by Mr. Henry S. Bacon of 276 Bellevue Street, West Roxbury, Massachusetts.

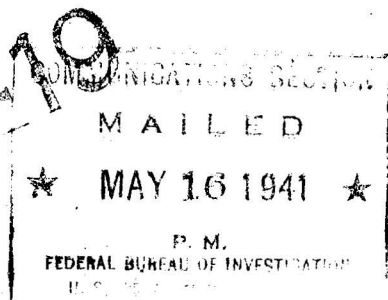
For your information the Bureau is not at the present time interested in purchasing any cipher machine but does desire to keep a complete file on devices of this sort so that the information will be available should the need arise. It is realized that it is rather difficult to describe in a letter the operation of such a cipher machine and it is therefore suggested that you inform Mr. Bacon that should he for any reason be in Washington on other business, the Bureau would be very pleased to look over his device. Please impress upon him, however, the fact that the Bureau is not at present in the market for such a machine but merely wishes to have complete information in the file regarding all machines of this nature.

Because of the extremely large amount of work at present in the Laboratory it would not be possible to spend any time in an attempt to break down a cipher message which was enciphered in Mr. Bacon's device. It is believed that should the opportunity afford itself in the future for the Bureau experts to view his machine they will be able to determine the relative security of messages enciphered by it without the necessity of attempting to decipher messages.

Very truly yours,

John Edgar Hoover
Director

Mr. Tolson _____
Mr. E. A. Tamm _____
Mr. Clegg _____
Mr. Foxworth _____
Mr. Ladd _____
Mr. Glavin _____
Mr. Nichols _____
Mr. Hendon _____
Mr. Rosen _____
Mr. Tracy _____
Miss Gandy _____



FEDERAL BUREAU OF INVESTIGATION
UNITED STATES DEPARTMENT OF JUSTICE

(Handwritten: 1/2)
To: COMMUNICATIONS SECTION.

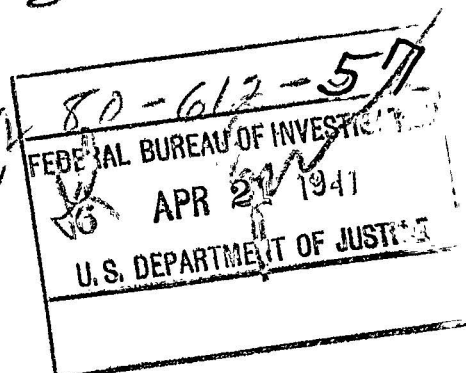
WGB:AF APRIL 19 1941

Transmit the following message to: SAC NEW YORK

(Handwritten: OK, V.A., 3)
YOUR LETTER SEVENTEENTH RE HAGELIN CRYPTOGRAPHER, ASCERTAIN
WHAT EARLIEST DELIVERY WOULD BE ON FIFTY LARGE KEYBOARD
MODELS. THIS DESIRED FOR INFORMATION ONLY.

HOOVER.

(Handwritten: B)
RECORDED
&
INDEXED



Mr. Tolson.....
Mr. E. A. Tamm.....
Mr. Clegg.....
Mr. Foxworth.....
Mr. Glavin.....
Mr. Ladd.....
Mr. Nichols.....
Mr. Rosen.....
Mr. Carson.....
Mr. Quinn Tamm.....
Mr. Hendon.....
Mr. Tracy.....
Miss Gandy.....

SENT VIA

M

Per *(Handwritten: 16.11)*

FBI WASH DC

4-19-41

338 PM

RSW

SAC NEW YORK

YOUR LETTER SEVENTEENTH RE HEGELIN CRYPTOGRAPHER, ASCERTAIN WHAT
EARLIEST DELIVERY WOULD BE ON FIFTY LARGE KEYBOARD MODELS. THIS
DESIRED FOR INFORMATION ONLY.

HOOVER

ACK AND HOLD

OK FBI NYC TJH

AND MAKE THE FIFTH WORD READ HAGELIN HAGELIN

**Federal Bureau of Investigation
United States Department of Justice**

New York, N. Y.

May 2, 1941

JBD:PAS

Director
Federal Bureau of Investigation
Washington, D. C.

~~RE:~~ HAGELIN CRYPTOGRAPHERS

Dear Sir:

In reply to your teletype of April 19, 1941 concerning the availability of fifty large keyboard cryptographers, please be advised that inquiry was made of Mr. Stuart Heddin, 44 Wall Street, New York City, N.Y. by Special Agent J. B. DRURY with reference to this matter.

On this date, a letter was received from Mr. Heddin, advising that beginning next July, three cryptographers could be delivered monthly in Stockholm, Sweden at a cost of \$1,850.00 each. The small portable cryptographers could be delivered almost immediately in Stockholm at a cost of \$325.00 each.

The original letter received from Mr. Heddin is enclosed herewith and the pertinent information was sent to you by teletype on this date.

Very truly yours,

B. E. Sackett

B. E. SACKETT,
Special Agent in Charge

Enclosure

RECORDED

1 ENCL. FM

4-211-59

FEDERAL BUREAU OF INVESTIGATION

4 MAY 5 1941

U.S. DEPARTMENT OF JUSTICE

LAB. CHA. CHA. CHA.

FULLER, RODNEY & CO.

MEMBERS

NEW YORK STOCK EXCHANGE AND OTHER PRINCIPAL EXCHANGES

FORTY-FOUR WALL STREET

NEW YORK

CABLES "RODNEFUL"

TELEPHONE HANOVER 2-2200

May 1st, 1941

Federal Bureau of Investigation,
U. S. Court House,
Foley Square,
New York, N. Y.

Attention: Mr. Drury

Dear Mr. Drury:

I find that in Stockholm they can handle delivery of three (3) Hagelin Cryptographs a month beginning in July and that the price would be \$1,850.00 per machine, C.E.F., Stockholm.

This limited delivery is governed by the necessary priorities to the Swedish Government.

I realize this is not very satisfactory and it may be under these circumstances the small machine would suit your purpose. These small machines could be delivered in Stockholm almost immediately at a price of \$325.00 each.

We, ourselves, would be pleased to loan you a machine for testing purposes. Although the Signal Corp, we are sure, would be pleased to have you benefit by their experience to allow you to examine the machines which they have in Washington.

Naturally I should be pleased to have you call upon me if I can be of any further service to you on this matter.

Very truly yours,



SH:MM


WGB:DMS
80-612-58

RECORDED

May 16, 1941



b7D

My dear 

Reference is made to your letter of April 25, 1941, your reference No. C.11-34-8-3, in which you requested to be advised of any material which would be useful to you in connection with cryptanalysis concerning various publications on the subject.

I regret to advise that there are no Government pamphlets or text books which I know of which contain any comprehensive summary of the various publications on cryptanalysis. However, I am listing below several reference books which contain information of more or less value on the subject:

Elementary Cryptanalysis

Author: Helen Fouche Gaines

Publisher: American Photographic Publishing Company, Boston, 1939.

Cryptography

Author: Andre Langie

Translated by: J. C. H. MacBeth

Publisher: Constable and Company, Limited, London, Bombay, Sydney, 1922.

Traite de Cryptographie

Author: Andre Langie and E. A. Soudart

Publisher: Librairie Felix Alcan, Paris, 1935.

Manuale di Crittografia

Author: Generale Imigi Sacco

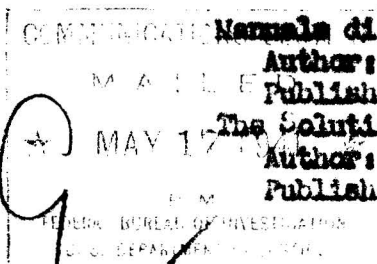
Publisher: Unknown, Rome, 1936.

The Solution of Codes and Ciphers

Author: Louis C. S. Mansfield

Publisher: Alexander Maclehose and Company, London, 1936.

Mr. Tolson _____
Mr. E. A. Tamm _____
Mr. Clegg _____
Mr. Foxworth _____
Mr. Ladd _____
Mr. Glavin _____
Mr. Nichols _____
Mr. Hendon _____
Mr. Rosen _____
Mr. Tracy _____
Miss Gandy _____



IV

Vin

Handwritten signature

Page Two

b7D

Codes and Ciphers

Author: Alexander D'Agapeyeff

Publisher: Oxford University Press,
London, New York, Toronto,
1939.

Secret Writing

Author: Henry Lysing

Publisher: David Kent and Company,
New York, 1936.

The following books which are written in story form also contain information of assistance in connection with the study of cryptanalysis:

Secret and Urgent

Author: Fletcher Pratt

Publisher: The Bobbs-Merrill Company,
Indianapolis, New York, 1939.

Secrets of German Espionage

Author: Bernard Newman

Publisher: Robert Hale, Limited,
London, 1940.

The American Black Chamber

Author: Herbert O. Yardley

Publisher: Faber and Faber, Limited,
London, 1931.

I might also add that there has come to the attention of this Bureau a publication entitled, "Bibliography of Cryptography" which is compiled by one James D. Valtz, 1030 Woodland Avenue, Cincinnati, Ohio, which appears to contain references to a large number of books on the subject.

I trust that this information will be of some assistance to you in connection with your cryptographic work.

Sincerely yours,

WAB
per
PAC

FBI NYC 5-2-41 2-20 PM ERL

DIRECTOR

RETEL/HAGELIN CRYPTOGRAPHERS. STUART/HEDDEN ADVISES KEYBOARD MODELS
CAN BE DELIVERED IN STOCKHOMXX STOCKHOLM AT RATE OF THREE PER MONTH
BEGINNING IN JULY AT COST OF EIGHTEEN HUNDRED FIFTY DOLLARS EACH.
PORTABLE MODELS AVAILABLE IN STOCKHOLM ALMOST IMMEDIATELY
AT COST OF THREE HUNDRED TWENTYFIVE DOLLARS EACH

SACKETT

ACK HOLD

OK FBI WASH RCA

RECORDED & INDEXED

70-111-60
FEDERAL BUREAU OF INVESTIGATION
6 MAY 8 1941
U.S. DEPARTMENT OF JUSTICE

LABY

CHIEF CLK

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

PAN:DMS

May 21, 1941

Mr. Tolson _____
Mr. E. A. Tamm _____
Mr. Clegg _____
Mr. Foxworth _____
Mr. Glavin _____
Mr. Ladd _____
Mr. Nichols _____
Mr. Rosen _____
Mr. Carson _____
Mr. Drayton _____
Mr. Quinn Tamm _____
Mr. Hendon _____
Mr. Coffey _____
Mr. Harbo _____
Tele. Room _____
Tour Room _____
Mr. Nease _____
Mr. Tracy _____
Miss Beahm _____
Miss Gandy _____

MEMORANDUM FOR MR. LADD

Re: Visit to Laboratory of
John Cantwell.

On May 12, 1941, Mr. John Cantwell, who resides locally at 631 Eye Street, N. W. and is from San Francisco, California, paid a visit to my office for the purpose of discussing the possibility of the Bureau's purchasing a cipher system which he devised. After ascertaining from Mr. Cantwell that he was presently unemployed and that he was formerly connected with the Hershey Chocolate Company in a sales capacity, I referred him to Mr. Napier for an interview.

Upon questioning Mr. Cantwell as to the exact purpose of his visit, Mr. Napier elicited the information that Mr. Cantwell was desirous of selling or bartering his cipher system for a position as a cryptographer in the Bureau. Mr. Napier pointed out that the Bureau was fully satisfied with its present cryptographic systems and that it was not in the market for the purchase of a cipher system at this time and also that it prescribed certain qualifications for those seeking positions as cryptographers, whereupon Mr. Cantwell remarked that he had made a cursory perusal of the copy of the job description sheet for this position which he had previously obtained and that since he was only a high school graduate, he could not meet the qualifications outlined therein.

RECORDED
&
INDEXED

After Mr. Cantwell had been informed that the Bureau's interest in his cipher would be purely academic and that it would be willing to receive the same for inclusion in its files where it could be utilized for reference purposes

80-612-61

MAY 23 1941

FEDERAL BUREAU OF INVESTIGATION
U. S. DEPARTMENT OF JUSTICE

LADD

CH-20

CH-20
EX-18

Page Two
Memorandum for Mr. Ladd

and that it was not interested in purchasing a cipher system at this time, he seemed disinclined to go into any great detail in the description of his system. However, he did venture to go over rather sketchily the essentials of his system and it was quite obvious that it was rather clumsy and awkward in operation and probably more theoretical than practical. After a discussion between Mr. Cantwell and Mr. Napier of the general problems confronting the person attempting to devise a new cipher for a practical use, Mr. Cantwell stated that he thought he would try to sell his system to the Army Authorities. He voluntarily suggested that if the latter were uninterested he would either return in person and write up a short description of his system for inclusion in the Bureau's files or else he would write the Bureau a letter and include the description therein.

Mr. Napier and Mr. Cantwell then exchanged greetings and the latter expressed his gratitude for having been extended the courtesy of an interview and departed.

Respectfully,

E. P. Coffey
E. P. Coffey

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

PAN:DMS

May 22, 1941

Mr. Tolson _____
Mr. E. A. Tamm _____
Mr. Clegg _____
Mr. Foxworth _____
Mr. Glavin _____
Mr. Ladd _____
Mr. Nichols _____
Mr. Rosen _____
Mr. Carson _____
Mr. Drayton _____
Mr. Quinn Tamm _____
Mr. Hendon _____
Mr. Coffey _____
Mr. Harbo _____
Tele. Room _____
Tour Room _____
Mr. Nease _____
Mr. Tracy _____
Miss Beahm _____
Miss Gandy _____

MEMORANDUM FOR MR. LADD

Re: Visit to Laboratory of
James Kirke Paulding and
Boris Hagelin.

On Tuesday, May 20, 1941, Messrs. James Kirke Paulding and Boris Hagelin visited the Laboratory for the purpose of demonstrating an enciphering machine invented by the latter and termed the Hagelin Cryptographer.

Mr. Napier conferred with these gentlemen and also inspected the mechanical cipher device which they explained. Mr. Hagelin claims that the keying cycle of his machine runs well into the millions of letters before it begins to repeat. He also advised that messages enciphered with either the large or small machine may be deciphered on the other, thus permitting the use of the large keyboard machine in a central office where speed is required and the use of the smaller units in those areas where not quite so much traffic is handled. Mr. Paulding stated that the machines being demonstrated had been borrowed from the Signal Corps and that similar samples were available at his New York Office at 44 Wall Street, New York City, and further that he would be willing to lend these machines to the Bureau through its New York Office at any time for testing purposes.

RECORDED & INDEXED

No very extensive examination was made of this machine when it was found that the price for the smaller unit is approximately \$325.00 F.O.B., Stockholm, Sweden, and that the larger unit sells for around \$1800.00 F.O.B., Stockholm. Furthermore, neither of these gentlemen could offer any assurance that were an order placed for the machines they could be delivered since the manufacturers would not attempt to guarantee

80-612-63

FEDERAL BUREAU OF INVESTIGATION

MAY 26 1941

LADD
SIX
FIVE

118-5

CH-17

o Cryptography

Handwritten initials and marks.

Page Two
Memorandum for Mr. Ladd

the safety of a shipment to the United States. They did state, however, that approximately one hundred of the smaller units would be available in Stockholm within a month or so.

Although these cipher devices offer a very high degree of cryptographic security, it is not believed advisable to recommend their purchase at this time in view of the virtually insurmountable obstacles existing in the way of obtaining their delivery in the United States.

Respectfully,

E. P. Coffey
E. P. Coffey *EP*

Federal Bureau of Investigation
United States Department of Justice

Chicago, Illinois
July 18, 1941

2m
A

Director
Federal Bureau of Investigation
Washington, D. C.

Dear Sir

There are enclosed several articles on elementary cryptanalysis which were forwarded by Mr. Martin Davis, 3658 West Grenshaw Street, Chicago, Illinois. This material is forwarded merely for the Bureau's information.

Very truly yours

WSD:IAJ
Encl.

W. S. Devereaux
W. S. DEVEREAUX
Special Agent in Charge

RECORDED

INDEXED
MV

80-612-64

FEDERAL BUREAU OF INVESTIGATION
2 JUL 21 1941
U.S. DEPT. OF JUSTICE

[Signature]

2m
1-
ENCLOSURE
2m
WSD

ALPHABETIC CHIPHERS

The Autokey (or Autoclave) Cipher, as indicated by its name is one in which the text serves as a key for enciphering itself. Though originally conceived as a means for complicating the Vigenere, it may be accomplished with any tableau whatever (or slide, or disk).

A short preliminary key is used to encipher the first few letters, after which the message-letters begin to appear as keys. Illustrating with Vigenere:

```

Key:      r u t h w e e x p e c t s h i p m e n t o n t h e f ...
Message w e e x p e c t s h i p m e n t o n t h h e f i r s t t
Cipher: a y x e l i g q h l k i e l v i a r g a s s b y w y.
          x . . . x
          y . . . y

```

It is not possible, of course, to arrange the text in columns or groups for convenient and rapid encipherment, so that this method must in general be applied one letter at a time. However, if the key is first written out in full, any outstanding key-letters can all be used at one setting of the slide.

If the encipherment has been accomplished with an unknown slide, one cryptogram can become an extremely difficult problem. But when the slide is known, it is possible to apply probably words; and when these are present, the problem is merely one of finding out where they are. All jumbled sequences can be discarded at once, and any plaintext which is deciphered can at once be applied as a key.

Even when the alphabet is unknown, provided there are enough messages on which to work, decryptment is not difficult. Since their beginnings are all enciphered with the same short key, these beginnings, placed one below another, form the columns of a periodic cipher.

To illustrate, suppose we have 50 messages (or 20 - the number necessary would vary with the kind of alphabet) enciphered by means of a "Quagmires" slide, and all using the keyword RUTH. By placing their beginnings in column form, we have four "Quagmires" alphabets with 50 (or 20) letters per alphabet. The first column is made up entirely of initial letters, and the second and third columns should be rich in vowels. With so much material, we could easily reconstruct the sliding alphabet - or enough of it which to proceed with the balance of the texts.

With these general facts understood, we will now turn our attention to the Autokey as applied by Vigenere only. The principles through which the straight alphabet autokey is decrypted are to me among the most interesting I have studied. These derive from the work of Commandant Bazeries and show clearly the kind of thing which may come to light when one dissects and analyzes a system to find its peculiarities and weaknesses.

In the first place, it is possible to determine the length of the short preliminary key.

The basis for doing this, in straight Vigenere, lies in the fact that B enciphered by C will give the same letter as C enciphered by B, and so on.

Now in any plaintext, there are always sequences in which some letter is repeated at an interval which is divisible by 2, and among all of the various intervals of this kind, there are many in which this division by 2 would give the same quotient. Five such intervals occur in the following text, although no two would give the same quotient:

c o n s i d e r i n g t h i s f r o m y o u r s t a n d p o i n t

<u>Letters:</u>	<u>Intervals:</u>	<u>Quotient, if divided by 2:</u>
I to E	4	2
E to E	6	3
C to C	16	8
T to T	8	4
D to I	22	11

Now note that the two I's are standing equidistant from an E. If we encipher this in Vigenere with an autokey, using a preliminary key whose length is 2, the first I will be used to encipher the E and the E will be used to encipher the second I. Both encipherments will give M, and the two M's will be standing at an interval of 2, the key-length.

If we use a three-letter key, then the two R's standing equidistant from Y, will act in the same way, and as a result we shall have two P's standing at an interval of 3, the key-length.

If we use an eight-letter key, the two O's and the N will produce two B's standing at an interval of 8, and so on. In our example on the first page two points are indicated where this happened with our four-letter key, RUTH.

By no means all of the repetitions found in an autokey cryptogram are caused in this way, but Commandant Bazeries, after making a great many tabulations, concluded that "a distinct majority" of them are so caused, and that is the intervals between repeated letters are carefully noted, the interval which occurs oftener will usually be that of the key-length.

If the cryptogram happens to be Beaufort or Variant, the principle must be modified to suit the system:

Beaufort encipherment:

B by C : : E)
C by P : : Z) Complements
H by Y : : R)
Y by H : : J)
D by F : : M)
F by D : : C)

Variant encipherment:

B by C : : Z) Complements
C by B : : B
H by F : : J)
Y by H : : R)
D by F : : M)
F by D : : C)

With cipher of these we obtain, not a repeated letter but a pair of complements standing at an interval which represents the key-length. (Except that A and N would be repeated, complements are found by juxtaposing the two A's of the two reverse alphabets: A B C D E F G H I J K L M N)
A Z Y X W V U T S R Q P O N)
X X

When the length of the preliminary key has been determined, this is treated exactly as we do a period; that is, we write the cryptogram into the proper number of columns, or into groups of the proper length.

With this done, there are two processes, either of which may be applied, and we will examine these in connection with the following cryptogram:

5	10	15	20	25
B F U C F	A K P G L	I A C G L	B C J M S	K Z K R G
30	35	40	45	50
G L B C Y	K H R G 3 Z	X N V F D	W A G O J	V B P S G
55	60	65	70	
R L E S K	E D T S R	F L E S I	D X D O T	E F G U

In taking intervals, I followed the rearranged frequency count, as shown at the end of the article. The first G has serial position 4. Starting with this G, intervals were 5, 21, 22, 25, etc. Starting with the next G, at position intervals were 16, 17, 20, etc. It would take an extremely long key-word to make these larger intervals of any importance, and I have not included them beyond the interval 15. Also, there was only one double, a fact which would have been noted in taking the frequency count, so that a one-letter key is out of the question.

The following includes all intervals from 2 to 15:

G:	5	4	9	3	8	6	14	9	7
B:	12	15	11	8					
D:	12	7	5	15	9	11	2		
S:	5	10	15	5	10	9			
F:	3	10							
I:	7								
L:	5	12							

R: 9 9
 A: 6
 K: 2
 T: 7
 V: 8
 Z: 13

Intervals found seven times: 5---
 " five times: 9--
 " four times: 7-

It would seem from this that the preliminary key had five letters (though with the possibility that it could have had nine or seven.)

One interesting point here is the series of 3's at a regular interval of five:

X . . . S . . . S . . . S . . . S
 This apparently points to two letters alternating with each other.

X . . . Y . . . X . . . Y . . . X
 These are probably frequent letters, and it might be possible to get an idea of what they are by consulting the diagonal line of S's which runs across your Vigenere tableau.

Now if the preliminary key-length was five, the first plaintext letter was used to key the 6th, the 6th to key the 11th, the 11th to key the 16th, and so on, forming a series to itself.

Then the second plaintext letter was used to key the 7th, the 7th to key the 12th, the 12th to key the 17th, and so on, forming another series. And similarly, there are three other series beginning with the 3d, 4th, and 5th plaintext letters.

We are going to consider only the first of these five series with the understanding that all five can be treated in the same way - or as many of the five as we find necessary to treat.

If the first letter of the preliminary key was A:

Letter No. 1 of the series was enciphered by A, and must have been B

Letter No 2 of the series was enciphered by B, and must have been Z

Letter No. 3 of the series was enciphered by Z, and must have been J.

(And so on...)

This can be done in several ways:

A	B	Z	J	S
B F U G F	A N P G L	I A C Q L	B C J M S	K Z K R G
B	Z	J	S	S
S	O			
G L B G Y	I H			
O	U			

Down Columns:

Across Rows:

Letter No. 1 ...	B F U G F	P A I J B A G I X J V R H E D F
Letter No. 2 ...	A N P G L	F N A G Z L H F A B L O I X G
Letter No. 3 ...	I A C Q L	U P O J K B R V G P E I T D U
	B G J M S	G G Q M R G G B O S S S O
	K Z K R G	F E L S G Y Z D J C K R I T
	G L E G Y	
	I H R G Z	
	X N V B I	
	W A G O T	
	V B P S C	
	E D E S Y	
	H D I S R	
	F L E S I	
	D K D O T	
	F C U	

Personally, I prefer to work straight across the groups, as shown at the top. This is much more rapid than it looks.

Having deciphered the first cryptogram series, we have the following fifteen letters as a plaintext series derived from A:

B Z F S S O U D T C P S W Q P.

But if the first letter of the preliminary key was B, we get another series:

A A A T R T R T P T W L S E D O T M R O.

And if this first key-letter was C, we get the series:

Z B H U Q Q S F R E N U I S N.

And so on for the remaining letters of the alphabet. Arranged in columns under their proper key-letters, the full 26 decipherments are as follows:

7

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	---	#	#	
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#	
B	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#
C	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#
D	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#
E	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#
F	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#
G	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#
H	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#
I	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#
J	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#
K	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#
L	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#
M	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#
N	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#
O	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#
P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#
Q	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#
R	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#
S	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#
T	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#
U	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#
V	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#
W	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#
X	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#
Y	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#
---	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#
#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#
#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	---	#	#

11

一井

1997

— — —

S K Q W M S P U V F O W H L F U L K V U D C L G J T Y V I A
K Z K N G C L B G Y I H R G Z X N V S D W A G O J V S P S G
S P J V T O W H L F U L K V U D C L G J T Y V I A C D U K G

C D U K G P A K I E S D Y K H N H V I V Q P X
 R D E S K H D I S R F L T S X L K D O T F G U.
 P A K I E S D Y K H N H V I V Q P I G Y P R M.

Having decided that the preliminary key had five letters, we write the cryptogram off into five-letter segments. Using the first segment as a key, we decipher the second segment with it, and obtain the letters Z I V A G. Using this as a key, we decipher the third segment and get J S T Q F. We use this to decipher the fourth segment, and so on, and at the end we have a new cryptogram beginning Z I V A G J S T Q F S X.....

Unfortunately, our present message is too short to show repeated sequences, because this new cryptogram has a period, not of 5, however, but of 10:

1	2	3	4	5	6	7	8	9	10
					Z	I	V	A	G
J	S	T	Q	F	S	K	Q	W	N
S	P	U	V	T	O	W	H	L	F
U	I	K	V	U	D	C	L	G	J
T	Y	<u>V</u>	<u>I</u>	A	C	D	U	K	G
N	I	<u>V</u>	<u>I</u>	V	Q	P	I	G	Y
P	R	M							

This is a straight Vigenere cryptogram. The first five columns are enciphered by the original five letters of the preliminary key, and the other five by their complements.

This has a mathematical explanation, in case anybody cares to figure it out. Vigenere encipherment can be considered as addition and the Beaufort and Variant Beaufort as subtraction, with the following details:

Vigenere = addition of key-letter and message-letter, with message-letters numbered 1 to 26, and key-letters 0 to 25,

Variant = subtraction of key-letter from message-letter, with message-letters numbered 1 to 26 and key-letters 0 to 25,

Beaufort = subtraction of message-letter from key-letter, with key-letters numbered 1 to 26, and message-letters 0 to 25.

Had this been a Variant, the new cryptogram would have had a period of 5, the same length as that of the preliminary key, and the method of obtaining it would have been exactly the same as for straight Vigenere: Decipher group 2 by group 1, decipher group 3 by the result, and so on. The Beaufort proper also reduces to a period of the same length as the preliminary key, but requires a slightly different procedure: The test-development is done, not by the straight Beaufort method, but by the variant method. The

following short example will suffice for those who care to investigate:

Encipherment By straight Beaufort:

Key: DOT F A R A W A Y I N T H E M O U N T A I N S
 Message: F A R A W A Y I N T H E M O U N T A I N S
 Cipher: T O O F E R C O N F B J H T K Z V U F G X

The "period" of three does not show up, and we will have to pretend that we discovered it through spies. The cryptogram is marked off into three-letter groups, and decipherment applied by the variant method:

Trial decipherment by Variant Beaufort:

Test key: . . . Y O C D S T F G G K H P R A Z Q V T
 Cryptogram: Y O C F E R C O N F B J H T K Z V U F G I
 New cryptogram: . . . D S T F G G K H P R A Z Q V T V B B

What we really do is to use A A A as a trial key. Trial keys are applied to Beaufort by using St Cyr Slide in the Variant manner.

This new cryptogram is a straight Beaufort with a period of 3, and can be deciphered with the simple key DOT.

In this letter-at-a-time decipherment, a single error can play havoc with results. But given enough material, and any uncertainty as to which of several is the correct key-length, the process just described is an excellent means for deciding which length to accept. The correct key-length, as a rule, will show repeated sequences. Here we had only one, though a number of repeated single letters showed up in the various columns.

Sometimes the preliminary key has only one letter, resulting in a cryptogram full of doubles. Probably the simplest way of handling it would be to start with A, and cancel it down: there are only 26 keys to try, and they need not be tried over a great deal of territory. However, the method last described could reduce it to a plain Vigenere with a period of 2; and whatever the key to one of the alphabets, the key to the other will be its complement. If it happens to be a Variant of a Beaufort, it can be reduced to a simple substitutor.

Occasionally the autokey idea is found applied with the cryptogram, and not the plaintext, used as the key:

Key: z u t h N Y X E C O Z X U J H M G N U T . .
 Message: W E R X P E C T S H I P M E N T
 Cipher: N Y X E C O Z X U J H M G N U T

Nothing much need be said about this. The key for decipherment is right in front of our eyes, and we need merely find a spot at which to begin using it.

Should this happen to have been done with a one-letter key, say X:

Key: x J J W E R R C C D D P P A I N G Y A A G . . .
 Message: M A N I N A L A B A M A L O F T S C A G E . . .
 Cipher: J J W E R R C C D D P P A I N G Y A A G K . . .
 x x x x x x

then every time an A appears in the cryptogram (three are underscored), the letter which follows it is the original letter (enciphered by A). Also, whenever a double occurs, the second letter of the double represents A. Six of these have been introduced into the text to show this up.

The Beaufort proper also produces doubles:

l l y q d d s s r r f f u m h o w u o k
 a a a a a a

The Variant, however, results in something less obvious: Pairs of complements, in which the second complementary letter represents A:

P L H T S I T H F V
 a a a a a

Sunyam, in his 38th and 39th articles (May 14th and 21st, 1927) shows an autokey cryptogram which is produced by adding numbers. (See also art. 48, July 23rd, 1927)

Alphabet-mixed alphabets are used and numbers from 1 to 24 are assigned to substitutes:

J	F	T	S	L	P
A	I	C	D	E	G
H	K	M	N	O	
R	Q	U	V	W	X
Y	Z				

J	A	E	P	K	Y	C	T	B	F	W	C	I	R	Z	T	M	D	L	F	N	U	V
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23

O G S
 24 25 26

His use of the keyword differs slightly from the method we have used in that the second E, instead of being entirely suppressed, gives place to a blank, so that the keyword retains its length of six letters. The columns which have been taken off by alternates, down and up. The assigning of numbers might also have been done in another way:

J A H P X Y
 10 1 8 16 24 25

Another alphabet:

A	B	C	D	E	F
10	1	8	16	24	25

For encipherment, a preliminary key-number is chosen- in this case the single number 10- and the message "Watch the man in the white mask" undergoes the following transformation:

Message:	W	A	T	C	H	T	H	E	M	A	N	I	N	T	H	E
First substitution:	11	2	16	12	3	16	3	10	17	2	21	8	21	16	3	10
Key addition:	<u>10</u>	<u>11</u>	<u>2</u>	<u>16</u>	<u>12</u>	<u>3</u>	<u>16</u>	<u>3</u>	<u>10</u>	<u>17</u>	<u>2</u>	<u>21</u>	<u>8</u>	<u>21</u>	<u>16</u>	<u>3</u>
Final cryptogram:	21	13	18	28	15	<u>19</u>	<u>19</u>	13	27	19	23	<u>29</u>	<u>29</u>	37	19	13

	W	H	I	T	E	M	A	S	K
	11	3	8	16	10	17	2	26	13
	<u>10</u>	<u>11</u>	<u>3</u>	<u>8</u>	<u>16</u>	<u>10</u>	<u>17</u>	<u>2</u>	<u>26</u>
.....	21	14	11	24	26	27	19	28	39

(Notice the repeated 19 and the repeated 29, both at an interval of 1, the length of the preliminary key).

The recipient of this message, in deciphering, subtracts the known key, 10, from the first cryptogram number, 21, producing 11; he subtracts 11 from the second cryptogram number, 13, and so on.

Decipherment.

Cryptogram:	21	13	18	28	15
Key:	<u>10</u>	<u>11</u>	<u>2</u>	<u>16</u>	<u>12</u>	<u>3</u>
	11	3	8	16	10	17
	W	A		T	C	H

Decryptment follows almost the same path; Sunyam compares it to standing a set of dominoes in a circle, and giving one domino a gentle push.

"In the first place," he says, "the number of possible preliminary keys is limited. In the present example, the initial key-number must run from 1 to 20, since it must be smaller than the first cryptogram number, 21, and at the very worst, all numbers from 1 to 20 can be treid out.

"But the number of trial keys can be further narrowed by considering the smallest numbers found in the cryptogram, and also by rejecting any keys which would result in values smaller than 1 or larger than 26. (Negative values have been avoided here, though they would in no wise complicate the solution)"

To start things going, he adds, taken any number from 1 to 20, say 12, as an initial key-number, and decipher the cryptogram:

Cryptogram:	21	13	18	28	15	19	19	13	27	19	23	29	29
Trial key:	$\frac{12}{9}$	$\frac{9}{4}$	$\frac{4}{14}$	$\frac{14}{14}$	$\frac{14}{1}$	$\frac{1}{18}$	$\frac{18}{1}$	$\frac{1}{12}$	$\frac{12}{15}$	$\frac{15}{4}$	$\frac{4}{19}$	$\frac{19}{10}$	$\frac{10}{19}$

.....	37	19	13	21	14	11	24	26	27	19	28	39
	$\frac{19}{18}$	$\frac{18}{1}$	$\frac{1}{12}$	$\frac{12}{9}$	$\frac{9}{5}$	$\frac{5}{6}$	$\frac{6}{18}$	$\frac{18}{8}$	$\frac{8}{19}$	$\frac{19}{0}$	$\frac{0}{28}$	$\frac{28}{11}$

XX--XX

Now suppose we make a comparison between this trial-decipherment and the true decipherment:

Correct decipherment:	11	2	16	12	3	16	3	10	17	2	21	8	21
Trial decipherment:	$\frac{9}{2}$	$\frac{4}{2}$	$\frac{14}{2}$	$\frac{14}{2}$	$\frac{1}{2}$	$\frac{18}{2}$	$\frac{1}{2}$	$\frac{12}{2}$	$\frac{15}{2}$	$\frac{4}{2}$	$\frac{19}{2}$	$\frac{10}{2}$	$\frac{19}{2}$
	16	3	10	11	3	8	16	10	17	2	26	13	
	$\frac{18}{2}$	$\frac{1}{2}$	$\frac{12}{2}$	$\frac{9}{2}$	$\frac{5}{2}$	$\frac{6}{2}$	$\frac{18}{2}$	$\frac{8}{2}$	$\frac{19}{2}$	$\frac{0}{2}$	$\frac{28}{2}$	$\frac{11}{2}$	

In every corresponding pair of numbers there is a difference of 2. For those occupying the odd serial positions this difference is "plus" and for those occupying the even serial positions it is "minus". That is, we have obtained with our trial key 12 exactly the same result as in the case of a Vigenere with a one-letter key: a new cryptogram having a period of 2 ((twice the length of the preliminary key). By subtracting 1, which is half of the constant difference, from all numbers having odd serial positions, and adding 1 to all numbers having even serial positions in our trial decipherment, we obtain a simple substitution- or the original number-cryptogram.

Now had this trial decipherment been obtained without knowing what the original is, we could have taken the two frequency counts on the two alphabets; then, since those alphabets are parallel, we could have lined them up exactly as described in Friendly Group Article No. 18 in connection with CA'S radio cipher. Subtracting a constant amount from one alphabet, or adding it to the other, reduces both to a "common denominator."

Whenever a one-letter, or one-number, key is used, any repeated trigram in the plaintext will produce a repeated bigram in the cipher:

Plaintext:	T	H	E
Key:	$\frac{T}{A}$	$\frac{H}{L}$	E

This happens twice in the example. The repeated T H E gives a repeated 19-13, and the repeated E M A gives a repeated 27-19

These repeated sequences would have been noticed in the cryptogram, and we should have considered the possibility of their representing repeated sequences of plaintext. If so, the first one is of no use to us, since the distance apart of the two occurrences, 8, is an even distance, and both 19's will belong to one alphabet

and both 13's to the other.

The second one is different. The interval separating the two occurrences of 27-19 is 13, which is odd. One of the 19's is in the same alphabet with one of the 27's, and the other 19 is in the same alphabet with the other 27. Notice that in making our trial decipherment we reproduce the entire repeated sequence 18-1-12 (underscored above) for the repeated bigram occurring at the even interval, but that in deciphering the repeated 27-19, which occurred at the odd interval, we obtained two different results: 15-4 and 19-0 (marked with xxx above.)

Now if this repeated bigram, 27-19, actually does represent a repeated trigram as in the case of the other repeated bigram, then, in our trial decipherment, 15-4 and 19-0, are the same letters, but are in different alphabets. To test this possibility, we try subtracting one bigram from the other:

$$\begin{array}{r} 19 \\ 15 \\ \hline 4 \end{array}$$

Since we find a constant difference of 4, with plus and minus alternating, it seems that our two gibgrams do actually represent the same plaintext bigram. We can subtract 2 from one alphabet and add 2 to the other, and thus eliminating their difference of 4-plus and 4-minus we reduce them not only to the same alphabet but to the original alphabet. Our resulting simple substitution, in the present case, has mixed alphabet, as we know, so that there is still the problem of solving a simple substitution having number-substitutes. Knowing or surmising the method by which the alphabet was disarranged, it should be possible also to recover the keyword JEWELS.

As to whether this procedure contains any ideas which might be of value in solving the various Viggies, I leave it to you to find out.

Noe, for the benefit of those who are interested in frequency characteristics, the following were the data taken from our cryptogram beginning B F U G E .. (75 letters):

Frequency count as originally made:

A B C E D F G H I J K L M N O P Q R S T U V W X Y Z
3 5 1 5 1 4 9 2 4 2 3 4 1 2 4 2 1 4 5 2 2 2 1 2 1 2

Frequency count arranged in decreasing order:

Frequency count arranged in decr. order																									
G	B	D	S	F	I	L	R	A	K	O	H	J	N	P	T	U	V	X	Z	C	E	M	Q	W	Y
9	5	5	5	4	4	4	4	3	3	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1

Entire number of repeated sequences with intervals and factors:

SK	54	-	20	=	34	2				17	34
VB	46	-	38	=	8	2	.	4	8		
RG	33	-	24	=	9		3		9		

LB 27 - 15 = 12 2 3 4 6 12
 GL 26 - 9 = 17 17

(The length of the preliminary key was 5)

Examples for Practice.

1. Vigenere Autokey According to this judge, "a mere breath of suspicion is not sufficient evidence of illegal possession."

Q C M F H W J X C F G J O Z Q G X S D E I X D S I Q K A C E
 Z S D Q J R K K V P K C M J D K C M J L A I X F F Q A Q X D
 L C E Z Q O Q B I Q B L K B Z C K M N E W U K B V K N G J Y
 B S J U H U X D O Y K T F W M J H V G C A N J F D H E U N X.

2. Variant Autokey. This is an appeal to Y C U.

N D W Z B K B Z M A P A U X U G O K Y W G O Q I Z G X U S P
 X Z S W P I L S W Q P J L U A I K F H O W U M N C Z X O L O
 C E O Y Z O Q B I Q L K K B Z C K N M E W U K B V K N G J Y
 T P S T B W U S D K H L D E B M D B L G Z K S Q T Z Y H W M.

3. AUTCKEY - Sunyam style. After you solve this, you can reconstruct my keyword?

28 28 19 34 26 20 32 19 26 42 36 19 21 61 36 16
 27 41 37 28 21 36 43 29 27 33 39 44 40 41 36 26
 24 38 36 37 31 38 43 23 13 5 24 38 41 30 25 25
 29 42 45 27 20 41 43 36 25 29 39 41 35 16 21 28
 28 19 26 48 36 31 31

4. This one was published with the 38th. Sunyam article. It was submitted by a Mr. James Olden of Medicine Hat, Alberta, Canada, who has placed his initial key number at a prearranged point in the cryptogram. This purports to be a police message.

25 39 35 27 17 19 33 28 21 23 30 27 17 25 29 18
 19 34 32 27 18 4 21 25 9 13 23 29 27 18 27 24
 19 23 13 23 36 40 24 24 54 36 41 28 31 28 24 30
 23 18 33 32 19 23 33 21 9 4 15 15 13 31 39 38
 23 10 25 26 7 4 12 23 21 25 27 31 27 25 25 8 15
 21 23 34 23 21 17 19 23 9 24 35 26 28 37 27 24
 20 14 18 6 21 33 22 13 18 23 16 15 28 36 28 13
 15 39 40 36 39 36 19 10 13 24 28 9 21 34 29 29
 19 10 24 22 40 17 21 8 4 17 36 41 39 23 24 28
 16 21 19 9 22 27 24 19 5 15 15 4 25 29 23 21 4
 10 11 13 14 15.

5. Now let's try a slaughterkey furnished by Dan Surr:

R V M U I L T V N L D W A M E E V H I V T D H G D F W A P T
 T M L O R R R I A P W O A T D H N H S A R F U A C G R Y L E
 I I D A L D A N V O V Y S N H A L W U W L L A L P I M A L A
 H A B F Y U B L N U N U Y W Y M R Y A I V I W P T M T B T I
 G B A L P.

6. Beaufort Autokey. Try! Try!

In case you have any trouble understanding the method in No. 5, here is your chance to read all about it!

K	T	J	K	H	Y	N	C	Q	K	T	U	L	Q	E	Y	N	P	A	Q	K	J	H	P	H	F	A	T	E	S
M	M	V	O	U	X	U	T	P	Z	N	A	L	Q	J	U	M	Z	P	S	G	M	U	F	R	F	H	N	O	Z
D	Z	F	A	A	E	M	H	V	P	I	D	H	A	P	Q	M	C	U	D	W	F	R	B	F	X	C	E	Z	P
G	O	R	K	Q	H	X	L	Z	H	A	D	C	G	N	W	I	A	Y	A	K	Y	A	T	Y	L	R	M	S	W
H	C	Q	W	G	P	K	P	I	T	L	Z	P	G	O	H	R	P	W	L	V	W	C	F	N	I	Y	I	K	L
A	E	V	G	R	W	I	L	G	Z	N	W	I	V	W	Z	T	D	F	O	Z	O	P	E	K	I	O	X	E	L
L	B	B	B	G	X	P	K	Z	M	V	L	P	E	P	E	L	A	S	C	W	X	V	P	K	T	G	P	Q	H
E	P	I	Z	M	J	K	E	P	Q	R	Y	T	U	B	L	E	N	K	L	V	S	G	E	E	X	A	C	W	A
E	S	Y	X	S	N	B	Y	V	W	P	L	R	V	L	V	X	K	A	T	R	G	O	A	T	C	D	P	E	S
C	C	R	F	N	M	I	K	R	P	J	T	D	P	H	I	F	E	Y	P	X	N	W	J	U	L	L	O	T	K
G	E	A	O	V	T	F	L	L	L	B	U	K	C	E	Q	Q	L	K	I	K	Q	Z	F	O	X	Q	E	A	N
C	Z	O	X	N	M	M	N	C	J	Z	L	M	A	A	S	P	U	H	D	J	X	X	X	X					

7. As to the hidden key in No. 4. Well, this was it.

T O X O Q P W O M V F O X H F S B U E S P L N G A P

THE NIHILIST TRANSPOSITION CIPHER

There are two ciphers called "Nihilist," a periodic substitution in which numbers take the place of letters and a transposition which is not so well known, although it apparently has a better right to the name than the number cipher has.

The Nihilist which is the subject of the present article is of the double transposition type, but with both transpositions applied geometrically; so that what, in many cases, is a difficult cipher to decrypt, becomes in the case of the Nihilist, a particularly vulnerable one.

The cipher call for a primary unit, based on the length of a keyword, and also for a complete unit, which is the square of the primary unit; and any message enciphered in this system, following its rule for ciphers of the geometric design, must be made to contain exactly the number of letters demanded by the complete unit, or some number of letters which is a multiple of the complete unit. This, of course, is accomplished by adding nulls, or by discarding letters from the text.

The key-word furnishes not only the dimensions of the unit, but the order in which the transposition takes place. Its letters are numbered according to their relative positions in the normal alphabet, and with repeated letters numbered from left to right, thus transforming the literal key into a numerical key:

Literal key:	R E A D E R
Numerical key:	5 3 1 2 4 6

E N C I P H E R M E N T

To illustrate the encipherment, suppose we use the above key READER, to encipher the message: "SEND REGIMENT TO REINFORCE LEFT WING."

Strictly in theory, three steps are necessary.

1. Divide the message (including five nulls inserted at any desired point) into its primary units, and write it into its block:

S	E	N	D	R	E
G	I	M	E	N	T
T	O	R	E	I	N
F	O	R	C	E	L
E	F	T	W	I	N
G	U	H	Q	T	E

2. Transpose each primary unit by the key-numbers 5 3 1 2 4 6:

5 3 1 2 4 6

R N S E D E
N M G I E T
I R T O E N
E R F O C L
I T E F W N
T H G U Q E

3. Using the same key in a vertical position, transpose the units themselves:

5	I T E F W N
3	I R T O E N
1	R N S E D E
2	N M G I E T
4	E R F O C L
6	T H G U Q E

The unit is now complete, and ready to be taken off in groups of five.

In practice, a single operation will accomplish all three steps at once. The key pattern is first laid off, both horizontally and vertically:

5 3 1 2 4 6

5	
3	
1	x
2	
4	
6	

Beginning at the spot where the row numbered 1 crosses the column numbered 1, the first primary unit, SENDRE, is written directly into its place by matching the key-numbers shown at the top: the second unit follows immediately on the row numbered 2, the third on the row numbered 3, and so on:

5 3 1 2 4 6	5 3 1 2 4 6	5 3 1 2 4 6
5	5	5
3	3	3 I R T O E N
1 R N S E D E	1 R N S E D E	1 R N S E D E
2	2 E M G I E T	2 E M G I E T
4	4	4
6	6	6

So that the writing of the message is continuous from beginning to end.

DECRYPTMENT

Decryptment of the Nihilist is very simple, and to illustrate the method, we may use the same message, known to be a Nihilist and handed to us in the following form:

I T E F W N I R T O E N R N S E D E N M G I E T E
R F O C L T H G U Q E.

Since the system requires a square, only two units are to be considered: 9 and 36; and the smaller of these is easily discarded by inspection. The remaining unit, 36, is written back into its original block: (The columns are to be cut apart, and for that reason, the spacing between them must be generous; in addition, each column should be given a serial number, so as not to lose track of its original position:)

1 2 3 4 5 6

I T E F W N
I R T O E N
R N S E D E
N M G I E T
E R F O C L
T H G U Q E

With the columns cut apart, the strips are moved about in an effort to match up words on some one of the horizontal rows, and these, when correct, will cause other words to appear above and below them. If no particular word is suspected, the same effort may be applied to bigrams and trigrams, in which case the commonest point of attack is to find some letter like "Q" which requires a certain definite sequence:

5 4 6

W F N
E O N
D E E
E I T
C O L
Q U E

Here "Q", happens to be a null, the sequence QU and THE having been chosen deliberately for the purpose of causing trouble, but after a little effort the decryptor would abandon both, and make a new trial at some other point.

The present message being of a military nature, such words as "regiment" and "reinforce" might be suspected. Also, with a unit as short as 6, perhaps the word "send" on the third row would catch the eye. With the letter "e" used twice in that row, two different arrangements would have to be inspected:

<u>3</u> <u>4</u> <u>2</u> <u>5</u>	<u>3</u> <u>6</u> <u>2</u> <u>5</u>
E F T W	E N T W
T O R E	T N R E
S E N D	S E N D
G I M E	G T M E
F O R C	F L R C
G U H Q	G E H Q

In the arrangement shown at the left, all combinations are good but for the last row, and if an effort has been made previously to make up the bigram QU, it is not hard to guess what is the matter with that row. The arrangement shown at the right brings out the combinations TNRE, GTME and FLRC, so that the other appears to be much more promising. The two remaining strips are fitted into the proper place and with the correct rearrangement effect, fragments of the message will begin to appear:

<u>3</u> <u>4</u> <u>2</u> <u>5</u> <u>1</u> <u>6</u>
E F T W I N
T O R E I N
S E N D R E
G I M E N T
F O R C E L
G U H Q T E

It would be possible now to make a similar set of strips representing the horizontal rows, but this is hardly necessary in any transposition of the same type, while in the Nihilist, where we know that the same key has served for both transpositions it would be a waste of time. All that is necessary is to observe the serial numbers at the tops of the columns and disarrange the horizontal rows accordingly. It is not always possible to recover the literal key, especially if it is short, but the numerical key is self-evident:

Serial numbers assigned
to Columns:

Original numbers
of the Key

<u>1</u>	should be	<u>5</u>
<u>2</u>	" "	<u>3</u>
<u>3</u>	" "	<u>1</u>
<u>4</u>	" "	<u>2</u>
<u>5</u>	" "	<u>4</u>
<u>6</u>	" "	<u>6</u>

Predetermining the Block Arrangement

So far, attention has not been drawn to the fact that the straight horizontal is not the only order in which a transposition may be taken out of its original block. It may be taken out by alternating horizontals, by straight or alternating verticals or diagonals, in a clockwise or counter-clockwise spiral, or in any other manner agreed upon by two correspondents; and the treatment of this contingency requires a short digression into the subject of the transposition as a whole.

Vowel Distribution

Approximately 40% of any English text is made up of the vowels A E I O U, with variation limits of from 35% to 45%. If you will select ten successive letters at any point in any continuous text, and count the vowels, you will probably find that there are exactly four. There may be as few as three or as many as five, but only an unusual formation will contain six, and it is practically impossible to find ten consecutive letters of reading matter in which there are only two vowels. With fewer than ten letters, the calculation is necessarily less accurate, but there must still be sufficient vowels for the formations of the syllables. No matter at what point the text is cut, the rule holds good for every series of letters, SO LONG AS THE TEXT REMAINS IN ITS ORIGINAL ORDER.

When a transposition employs a unit, or cycle, the same letters remain inside the unit, and are merely thrown out of order with reference to each other; but if such units are afterwards placed end to end to form a long series of letters, it then becomes possible to find long groups containing only consonants or only vowels. Illustrating briefly with the first 20 letters of our above message, "Send regiment", etc., transposed with a unit of ten:

E D E G - I E S N R M F R T N - O N I E O T

If this line of letters is cut at the correct point, each half containing four vowels; but with the division made as indicated by (-), ten letters are found in succession with only a 20% vowel count:

In many kinds of transposition, this observation is used as a means of determining how long the unit is. If a message containing 108 letters is judged by factors only, its unit may be 9, 19, 27, 36, etc., but, if the same message is marked off in units of 9, and it is found that some of the units have too many vowels and other units too few, then the unit 9 may be discarded, and other possible units examined in the same way until some division is found in which every single unit has its

40% vowel count. In cases of indecision, a similar text can be, as to the letters L N R S T, which are presumed to represent 30% of the text with the same unit limit of 5%, but these letters are more subject than vowels to variation. In fact, there are cases in which the application of both tests will not show definitely which of the two units is the more probable, so that both will have to be tried. Obviously this contingency will hardly apply to a unit as large as 36, when it is shown that the nearest units of equal probability are 25 and 49, so that if the transposition in question is a Nihilist, it should never be hard to determine the complete unit, and with it the primary unit.

Identically the same principal may be used for writing a Nihilist (or similar) transposition back into its original block.

As may be verified from a study of its encipherment, each of the primary units, although transposed within itself, and afterwards transposed as a whole with reference to other primary units, has never contained any other letters than those with which it started as a fragment of connected English writing. It is no longer in the right order, but it still is written on a horizontal line, and it has never released its original quota of vowels.

If then the Nihilist message can be written back into its block each horizontal line will be one of the primary units, and except for possible nulls, will show its vowel count to be 40%. All that is necessary is to write the message in various possible arrangements and count the vowels per horizontal line until you find an arrangement in which every horizontal line shows a good vowel count. The more usual arrangements are tried first: the straight horizontal and the alternating horizontal which will provide the vowel counts of the two vertical arrangements; if the count is poor, then the diagonals and spirals may be tried; and if these also fail to distribute the vowels, some other arrangement must be found, but the scope for this is limited if the original method of the transposition is to stand unchanged.

For better demonstration, suppose that we make use of a different message in which the primary group is somewhat nearer to ten:

O F R R T O U I N L I I A I H S D I W T E U P H A
E N E T N D D E E H L S N D P N A N L E D A Y T S
I T S H E I Y A R I S O U D.

The total number of letters is 64, which may represent:

A complete unit of 4, used 16 times.
 A complete unit of 16, used 4 times.
 A complete unit of 64 used once.

A cycle of four may, of course, be discarded by inspection but, assuming that a cycle of 16 is likely, and dividing the cryptogram off into blocks of that length, we find that the vowels are distributed as follows:

1st block of 16 - 8 vowels.....(50%)
 2nd block of 16 - 6 "(
 3rd block of 16 - 5 "(31%)
 4th block of 16 - 7 "(
)

Nulls considered, this unit is not impossible, even though two of the blocks are outside of their limits, and, since a 16 letters makes fairly good sight reading, some one of these - say the second or fourth in which the vowel count is normal - could be tried out hastily in various arrangements.

The natural selection, however, is the single unit of 64, with its vowel count of 40%, and this block is shown below in two of the possible arrangements, from which four separate vowel counts can be taken:

HORIZONTAL	VOWEL COUNT	SIMPLEST DIAGONAL	VOWEL COUNT
O F R R T O U I	4	O R O L H E E L	4
N L I I A I H S	4	F T N I T N H N	1
D I W T E U P H	3	R I A W E E A T	5
A E N E T N D D	3	U I I A E N Y H	5
E E H L S N D P	2	I D H D P A S A	2
N A N L E D A Y	3	S P D D D T E S	0
T S I T S H E I	3	U N N E I I I U	6
Y A R I S O U D	4	T S L S E R O D	2

VERTICAL

3 5 2 3 3 4 4 2

ANOTHER DIAGONAL

4 2 3 3 4 4 4 2

By counting straight down the columns of any horizontal arrangement it becomes possible to discover without re-writing what its count would be when written vertically. A vertical count will also, at times, serve as a selector when two different horizontal counts have been found which seem equally good, since vertical count made from a plain text is never an impossible count.

In a primary unit of 8 letters, the normal number of vowels is 3.2, so that if either of the above arrangements is the original block each horizontal line will contain approximately

3 vowels, and no line should contain fewer than 2 vowels or more than 4 vowels, always keeping in mind the possibility of nulls and the fact that the low frequency vowel, "Y", may have taken the place of one or two others. (In fact, Y may be included in the total 40%, if its presence is not over-emphasized.)

Examining the horizontal arrangement: Each row is within limits and the distribution by rows is uniform - that is, fully half of the rows are exactly normal. Examining the vertical: One column is distinctly off, and the distribution by rows is somewhat more erratic, showing only three which are exactly normal. Either arrangement is possible but there is a distinct difference in favor of the horizontal. And the fact that the vertical count is possible at all is a strengthening factor in favor of the better horizontal.

Examining the two diagonal arrangements: A count taken across the horizontal rows is an impossible one. A count taken down the columns is a possible one, although it shows only two units at the exact normal, but if these columnar units were made horizontal, then the present impossible horizontal units would represent their vertical count, so that this new diagonal is not acceptable either.

Apparently, then, the cryptogram was taken off horizontally and in the arrangement shown above at the left, each 8 letters constitute one of the original primary units standing on its own horizontal line in the original block. As to whether every unit was taken off from left to write, we still do not know. Sometimes the vertical count will act as a selector, but in the present example a vertical count taken from the arrangement by straight horizontals is exactly the same as vertical count taken from the arrangement by alternating horizontals:

O	F	R	R	T	O	U	I
S	H	I	A	I	I	L	N
D	I	W	T	E	U	P	H
D	D	N	T	E	N	E	A
E	E	H	L	S	N	D	P
Y	A	D	E	L	N	A	N
T	S	I	T	S	H	E	I
D	U	O	S	I	R	A	Y

2 4 3 2 4 3 5 3

In such cases, both arrangements must be tried, and it is usual to begin with the one which represents the more natural way of writing. In case you care to complete the solution: The material used in this article was originally prepared in letter form in response to an inquiry about the Nihilist Transposition Cipher. The member who asked for the information was Analyst.

Examples for Practice

1. IMNNS OTAAY TGDRT MYBWE IIEIR
GEHUT EES EY UGORL MMLNO LESRH
OBTHC POIMC BSRE.
2. TTESC BGC OU EOTNI PTOIR TOADA
AUKAC RSMLF AKSRG YTPOE AYDPR
EAOCA SSENI OTPLH OLOEY NEHDM
DRUTO ACTJV NENTU IPNNE SERMR
ASEAS TIK.
3. SETVE ERLTN EXERH ASC EB EG EWE
DTTOR IMANP TASTQ UONEI NOBNS
COTEO ERSID LDETH EREET TLAPH
NCRFI E.
4. EIHSD TADIO YEOSN LOFTO YOYBB
UNSIF REGTN I.
5. ACUCO LOHSL RTOOL OYDAI HDIAR
MESNI AITGK ICNCO LNMUS ERM S.

BEST-KNOWN MEMBERS OF THE VIGENERE FAMILY

The St. Cyr. System

The St. Cyr. cipher employs a sliding device which is easily made from cardboard or heavy paper. My own favorite material is manuscript cover, which possesses both body and pliability. A drawing of such a slide appears in connection with the Porta System, but we may confine ourselves here to a description of the decipherment.

Two normal alphabets are used, one for finding plain text letters and the other for finding cipher letters:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F, etc.

The upper and single alphabet should be placed on a much wider strip of material than the other, so as to allow for slots through which the lower alphabet may slide. This upper alphabet is stationary. The lower alphabet partly shown, contains two alphabets in succession (except that the final Z is not necessary, and there are usually just 51 letters.) This double alphabet is on a narrow strip, so that the two ends of the strip may be inserted into slots. The slots are cut in the wider strip of material just below the stationary alphabet, one to the left of A, the other to the right of Z, in preparing the narrow strip, an inch or so leeway should be left at each end, in order that it may be moved back and forth without coming out of the slots. Above all, the SPACING THROUGHOUT MUST BE UNIFORM.

The original system called for a keyword of four or five letters. Here we have used the keyword FAT to encipher the message "Be here at six".

Key	F A T F A T F A T F A
Message	B E H E R E A T S I X
Three steps of encipherment:	
1st, encipher by F.....	g j f n
2nd, " " A.....	e r t x
3rd, " " T.....	a x l
Cipher completed:	g e a j r x f t l n x

The three steps were as follows: To encipher by F, slide the lower alphabet so that the key-letter F stands below A of the upper alphabet (exactly as shown above) and make the necessary substitutions from the lower alphabet. To encipher by A, merely copy the letters. To encipher by T, move the slide so as to bring the key-letter T below A of the upper alphabet, and perform the third step. Deciphering is the same, except that cipher letters must be found in the lower alphabet, and the substitution of plaintext letters is made from the upper.

This, as may readily be seen, is merely the Vigenere cipher applied by mechanical means.

The United States Army Cipher Disk

The principle of the cipher disk is the same as that of the St. Cyr slide, except that one alphabet runs forward, and the other backward:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A Z Y X W V U T S R Q P O N M L K J I H G F E D C B A Z Y X W, etc.

As applied in disk-form, the device comprises two concentric dials, each having an alphabet arranged in a circle near its outer rim. One dial is smaller than the other, and when the smaller dial is placed on top of the larger, the two circular alphabets will coincide. The disk arrangement, it is needless to say, does away with the necessity for a double alphabet, but demands that certain of the letters appear upside down.

Encipherment and decipherment are the same as in the St. Cyr. system, except for the differences which are noted below.

The cipher disk may also be applied by means of a tableau, the first few lines of which would be as follows:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B
Z	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A
Y	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z
X	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y
W	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X

(etc.)

On the cipher disk, (or its application in slide form,) all alphabets are reciprocal, that is, (see above) if A equals V, then V also equals A; if B equals U, then U equals B; so that for enciphering or deciphering, it is immaterial which of the two alphabets, upper or lower, is used for finding substitutes, and which for originals; whereas, in the St. Cyr system, the substitute letters MUST be taken from the correct alphabet. In this respect, then, the cipher disk is simpler.

However, when it is a matter of decrypting, the St. Cyr has the advantage. To illustrate the difference, we have selected a very short message: "Save them", enciphered in both systems by means of the same key-word "TAM":

<u>St. Cyr</u>		<u>Cipher Disk</u>	
Key:	T A M T A M T A	Key:	T A M T A M T A
Message:	S A V E T H E M	Message:	S A V E T H E M
Cipher:	L A H X T T X M	Cipher:	B A R F H F P O

We know from our acquaintance with the Vigenere proper, that the cipher produced at the left, L A H X T T X M, will be identically

the same in message and key exchange functions. But if these functions are reversed in using the cipher disk, there is a different result:

St. Cyr

Key: S A V E T H E M
Message: T A M T A M T A
Cipher: L A H X T T X M

CIPHER DISK

Key: S A V E T H E M
Message: T A M T A M T A
Cipher: Z A J L T V L M

We know that if we were examining the left-hand sequence as a Vigenere, and suspected that it represented the two words "save them", we need merely use those words as a trial key, and decipher back by means of the same tableau, or the same slide, in order to find the true key, but if we are examining the sequence B A R P H F P O as a disk encipherment, and suspect the same two words, and if we attempt to decipher back to the original key in the same way, using a cipher disk, we find ourselves in hard luck:

Key-test, using St. Cyr Slide

Trial key: S A V E T H E M
Cipher Sequence: L A H X T T X M
Actual key: T A M T A M T A

Key-test, using U.S. Army Disk

Trial key: S A V E T H E M
Cipher sequence: B A R P H F P O
? R A E P M C P Y

This does not mean that you cannot decipher back, using your message as a trial key. It means only that your cipher disk will not serve the purpose. If you will take the same sequence, B A R P H F P O, ENCIPHERED BY MEANS OF THE DISK? AND THE SAME SUSPECTED WORDS, "save them", to be used as a trial key, you can decipher back to the original key with the greatest ease simply by using your St. Cyr slide, and taking your letters from the wrong alphabets.

The two methods are complementary to each other. At first, there are little differences which may confuse; for instance, the A alphabet of the St. Cyr is the regular alphabet, while that of the disk retains only the two letters A and N of that alphabet, all others being changed. After a short acquaintance with both systems, such confusion disappears.

Slides are not always prepared exactly as I have shown them. Sometimes it is the upper alphabet which is double, and the single alphabet which slides. Often it is the lower alphabet which is used for message letters, and the A of this alphabet is made to coincide with a key-letter in the upper alphabet. Quite often a slide is used with both alphabets placed in a vertical position.

It is perhaps needless to add that the principle of the St. Cyr slide can also be applied in the disk form.

The Beaufort System

The Beaufort cipher may be accomplished with a Vigenere tableau, or the Vigenere by means of its Beaufort variation.

Upper Portion of the Beaufort Tableau

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G

The Beaufort tableau, unlike the Vigenere, has no specified MESSAGE ALPHABET, and no key-alphabet at all, the key-letters being scattered throughout the square, so that the encipherment has to be done by letter, an extra alphabet at the right, and another at the bottom, make the four outside alphabets uniform, and any one of the four may serve as the message alphabet at the pleasure of the operator.

A key word is used, as in the Vigenere, and encipherment is accomplished as follows: Find the message letter in the most convenient of the four outer alphabets, trace inward to the key-letter, turn a right angle (in either direction), and trace to the end of the row or column. The cipher letter is always in one of the two outer alphabets adjacent to the one in which the message letter was found.

Using the same message and the same key:

True Beaufort Encipherment.

Key:	T A M T A M T A
Message:	S A V E T H E M
Cipher:	E A R F H F F O

This is presented merely as a matter of interest. If you will compare this result with that of the United States Army Disk Cipher, you will discover that after all we have no new system. The Beaufort system and the cipher disk produce exactly the same cipher, although by different means.

The Vigenere-Beaufort VARIANT

Obviously, there is a third way in which the Vigenere or the Beaufort tableau may be used. By beginning with key-letters, and tracing toward message letters, it is possible to produce what appears to be an entirely new cipher:

Key: T A M T A L T A
 Message: S A V E T H E M
 Cipher: Z A J L T V L M

(Again it may be interesting to compare this result with one which was obtained in examining the cipher disk.)

In certain foreign texts, this process is also called the Beaufort. We prefer to think of it as a VARIANT system partaking of both Vigenere and Beaufort characteristics. It does not produce an alphabet of the Beaufort type, but a Vigenere alphabet in which all of the letters are arranged in their normal order. It can be enciphered letter by letter on the cipher disk, with its message used as a key; but it can be enciphered far more simply on the St. Cyr slide, using the actual key, and simply reversing the functions of the two alphabets.

If this were a longer message, we might solve it as a Vigenere and never know the difference. However, we should not find our original key, but a new key: H A O. We might be satisfied with this key, accepting it as a series of letters, and proceed no further. If we should suspect that this VARIANT system has been used, it is a matter of about ten seconds to convert our jumbled key H A C into the original key T A M, simply set the cipher disk so that the two A's coincide, and make three substitutions:

Restoring the Key, when the VARIANT is used.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B
x											x														

Original Vigenere key:	T A M
Key produced by VARIANT	H A O

The triangular relationship between the Vigenere and Beaufort, whether applied by tableau, slide, or disk, is a very close one, and one which makes a fascinating study. Decryptment, in both, is the same. If possible determine the period, isolate the successive alphabets, and take their frequency counts. Except that these alphabets begin at different points, all the alphabets are the same. In the longer ciphers, an inspection of the frequency counts will show whether the alphabets are forward or backward, and the letter with which each of them begins; and in the shorter messages, the same test for probable trigrams is applicable to both systems. If there is doubt as to which has been used, the same sheet of trigrams may be used to test for both simultaneously.

Not all periodic ciphers employ an unchanged alphabet, but the majority of them use alphabets which are methodized after some fashion, and the problem is merely one of discovering the method.

However, it is entirely possible, and under certain conditions practicable, to employ a series of scrambled alphabets which have no method whatever, and no relationship to each other. The cause of that kind, and in many cases where a relationship exists but is hard to find, the decryptor must have a great deal of material in order to succeed, since, after determining the period and isolating the alphabets, he must sometimes apply simple substitution methods to each alphabet.

In practical work, he quite often knows in advance with what system he is dealing, and is able to solve the problem much more easily because of some special weakness peculiar to the system itself.

Two such systems remain to be described; the Gronsfeld, which, despite its obvious weakness, is said to be not infrequently encountered in actual practice; and the Porta, which, for some reason, has been discarded - probably because it is somewhat less easily reconstructed from memory than the systems just described.

The Gronsfeld Cipher

The Gronsfeld is a derivative of the true Vigenere, and differs from the Vigenere proper in only one respect: Instead of using the full 26 alphabets, it employs only the first ten, and points them out by means of the ten digits.

The encipherment was originally accomplished by counting forward in the alphabet. However, it may be done from the Vigenere tableau (or from the St. Cyr slide) if the first ten key-letters, A B C D E F G H I J, are replaced by the ten digits, 0123456789, again, if desired, a special tableau may be prepared as follows.

Suggested Tableau for Gronsfeld

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I

In the Gronsfeld Cipher, there could not be a key corresponding to the key word "TAM", because the M and T alphabets are not used, although the "A" alphabet appears and would be pointed out by the digit 0. The keyword "BAD" and the key-number 103 would produce the same cryptogram.

A long message would show no difference from a Vigenere message, except that its key might turn out to be a jumble of letters such as H J G F A, and even this would hint at the system if it is noted that none of these letters run beyond J in the alphabet. In a short message, the same series of jumbled letters, as H J G, or J G F, appearing at more than one point on a trial sheet, would suggest a jumbled key, and this, in turn, might suggest the Gronsfeld.

A definitely recognized Gronsfeld, no matter how short, is solved in short order. Take, as an example, the following message:

U E B G X N G T O G G K U

There are no repeated sequences, and even though the period, according to the repeated single characters G and U, seems to be quite clearly 3, the certainty of this fact would not help us to identify alphabets containing only four or five letters. Neither has any probable word been suggested, so that our only recourse is to the probable trigrams method as outlined in the Vigenere article. The 13 letters of the message will furnish 11 cipher trigrams; using the Gronsfeld tableau, and attempting to decipher each of these as THE:

Trial Key:	T H E
Cipher trigram:	U E B E B G B G X G X N X N G N G T G T O
Key digits:	1 . . . 2 8 . . . 9 4 6 2
	T O G O G G G G K G K U
	0 7 2 . . 2 . . 6 . 3 .

The limitations of the system demand that no substitute be more than 9 positions distant from the letter it represents, as counted forward in the alphabet, so that for two of these cipher trigrams no decipherment is possible, and for seven others only one letter can be deciphered. Conclusion: There can be only two points in the entire message at which the trigram THE can possibly be found. Instead of having to try out the entire eleven key-fragments, as may easily happen in the straight Vigenere, we need only try two, and if these fail, pass on to the next trigram AND.

It is even possible to solve a Gronsfeld by inspection - simply writing out the letters of the cryptogram with the remaining nine alphabets below it, and searching for letter combinations.

U	E	B	G	X	N	G	T	O	G	G	K	U
T	D	A	F	W	M	F	S	N	F	F	J	T
S	C	Z	E	V	L	E	R	M	E	E	I	S
R	B	Y	D	U	K	D	Q	L	D	D	H	R
Q	A	X	C	T	J	C	P	K	C	C	G	Q
P	Z	W	B	S	I	B	O	J	B	B	F	F
O	Y	V	A	R	H	A	N	I	A	A	E	O
N	X	U	Z	Q	G	Z	M	E	Z	Z	D	R
M	W	T	Y	P	F	Y	L	G	Y	Y	C	M
L	V	S	X	O	E	X	E	F	X	X	B	L

If some friend has recently handed you a cipher with word divisions (which is not a simple substitution) it may be a good idea to try such an inspection on the first few words. There is a "puzzle" cipher of the Gronsfeld type in which the series of key digits begins anew with each new word. The count may progress backward in the alphabet, although as a rule it is forward, as in the Gronsfeld; and usually no digit greater than 5 is used, since the perpetrators of such atrocities generally do their "shifting" by counting on the fingers of one hand.

The Porta Cipher

And now for the father of the Vigenere, the grandfather of the Gronsfeld, and the progenitor-in-chief of the whole Vigg family.

Keys

Cipher Alphabets

A B	a b c d e f g h i j k l m n o p q r s t u v w x y z
C D	a b c d e f g h i j k l m o p q r s t u v w x y z n
E F	a b c d e f g h i j k l m p q r s t u v w x y z n o
G H	a b c d e f g h i j k l m q r s t u v w x y z n o p
I J	a b c d e f g h i j k l m r s t u v w x y z n o p q
K L	a b c d e f g h i j k l m s t u v w x y z n o p q r
M N	a b c d e f g h i j k l m t u v w x y z n o p q r s
O P	a b c d e f g h i j k l m u v w x y z n o p q r s t
Q R	a b c d e f g h i j k l m v w x y z n o p q r s t u
S T	a b c d e f g h i j k l m w x y z n o p q r s t u v
U V	a b c d e f g h i j k l m x y z n o p q r s t u v w
W X	a b c d e f g h i j k l m y z n o p q r s t u v w x
Y Z	a b c d e f g h i j k l m z n o p q r s t u v w x y

Each of the thirteen cipher alphabets is reciprocal. That is, using the topmost alphabet, A equals N and N equals A; B equals O and O equals B, and so on.

The order of the alphabets is governed by a keyword, as in the Vigenere. However each alphabet may be pointed out by two different key-letters. The key-word ACE would point to the first three alphabets, and so would the keyword ANM, so that even after a cipher has been solved, the original key-word may remain doubtful.

Following is the encipherment of our famous message with its key-word TAM (which the decryptor may read as TAN, SAN or SAM).

Key: T A M T A M T A
Message: S A V E T H E M
Cipher: J N C N G N N Z

The key-letter T points to the 10th alphabet; the key-letter A to the 1st; the key-letter M to the 7th; and in each alphabet the designated message-letters are replaced by the letters with which they are paired.

The original Porta tableau employed only 22 letters, the one shown above is the modern arrangement for the full 26, as taken from one of Sunyam's articles. Sunyam has also pointed out that the Porta can be used in the form of a slide:

First 13 letters common to all alphabets:

	A	B	C	D	E	F	G	H	I	J	K	L	M	
N O P Q	T	U	V	W	X	Y	Z	N	O	P	Q	R	S	V W X Y Z
a c o g	m	o	q	s	u	w	y							
b d f h	n	p	r	t	v	x	z							

In addition to figuring out the slide, Sunyam has reduced the tableau itself to a more compact form, in case anybody finds (as I do) that tableaux are sometimes more convenient than slides for deciphering.

	A	B	C	D	E	F	G	H	I	J	K	L	M
AB	n	o	p	q	r	s	t	u	v	w	x	y	z
CD	o	p	q	r	s	t	u	v	w	x	y	z	n
EF	p	q	r	s	t	u	v	w	x	y	z	n	o
GH	q	r	s	t	u	v	w	x	y	z	n	o	p
IJ	r	s	t	u	v	w	x	y	z	n	o	p	q
KL	s	t	u	v	w	x	y	z	n	o	p	q	r
MM	t	u	v	w	x	y	z	n	o	p	q	r	s
OT	u	v	w	x	y	z	n	o	p	q	r	s	t
QR	v	w	x	y	z	n	o	p	q	r	s	t	u
ST	w	x	y	z	n	o	p	q	r	s	t	u	v
TX	x	y	z	n	o	p	q	r	s	t	u	v	w
YZ	y	z	n	o	p	q	r	s	t	u	v	w	x
YZ	z	n	o	p	q	r	s	t	u	v	w	x	y

The Porta has a limitation which renders its decryptment by the trigram method even more rapid than that of the Gronsfeld; in fact, it is not necessary to prepare a trial sheet at all. Its weakness lies in the fact that every letter must be enciphered by some letter from the other half of the alphabet. If, for instance, the sequence J N O of the foregoing encipherment were under examination as a possibility for the trigram the, it could be discarded at once. T could be represented by J and N could be represented by M, because in each case, the letter and the substitute would be in separate halves of the alphabet. But there is no alphabet in which the letter C can be substituted for E.

A prepared sheet of cipher trigrams may be dispensed with. The trigram THE may be considered as having the formation; 2-1-1. (That is, its three letters, taken successively, belong respectively to the second half, the first half, and the first half of the alphabet). The substitute trigram, then, must be of the formation: 1-2-2. And this may be sought in the cryptogram as it stands. If there is a suspected word, put opposite formation, 2-1, etc., on a strip of paper which can be slid along below the letters of the cipher. No sequence need be deciphered unless it conforms to the pattern.

Examples for Practice

Note: It is usual to complete all final groups by adding nulls for telegraphic transmission, and this has been done in some cases.

1. St. Cyr or straight Vigenere.

O C F I Z O I O E N J S D V A I Z O T Y H H G P Q
I T D D I T L J N J O V Y A G Z L F.

2. Vigenere-Beaufort Variant.

V M G N H J J W W Y K A O W K L Z B T V G N X N T
W F G Y U Z C P C X Z S M N N T O V N Q P B P S O.

3. Beaufort, or U. S. Army Cipher Disk.

Note: In the Beaufort system, any letter enciphered by itself gives A, so that any appearance of the sequence in the cipher is quite likely to represent a common bigram. A sequence NN may also have its points of interest.

U N T A B L Y E W O W X X N I V W W A K U M A T F
G V U A L I W Y C D R W S L X L I L N X Q M U A U
Y F W Z H R H E E O V S F X E.

4. Another Beaufort in case you care to try a second method.

H E F K N Y K K L A A G E B P O N D K L W E F X G
W E K K Z A A O N N Z W E Y K X M J E U T M L T E
A O Y I N X I.

5. Gronsfeld.

Y J E S I K U N P M S V E S I X V I O X M K S C I
D Q N E F J C R O M S I T I I X A S U I R Z X Y E
L Q O E T J T I P H.

6. Porta.

Q G G W Q J J D L G T U R K Q L B U L N E H H F D
Q X U Z M B T F Y R H O R C N I F U M J M S N C T
Y G E Z I J V M B L X N.

7. ?????

Q A K K N G H L Q R K L H N P P T Z E B Z M P N Q
Y U J F Y X X Z W Q I M J K N.

8. ?????

U Z W W Q E N O W S W V Y C Y M C P J C I P V I U
I N A P K Y Z H U O T K D X H B G J G X X C G T Q
X G T Q X G P O I V J C R V C V N W G R W H O P Q.

Banquet of The National Puzzlers' League and American Cryptogram Association, Parker House, Boston, September 1, 1940.

1. Arty Bgs. 2. M. E. 3. Puzzlesmith. 4. Morning Glory. 5. Neon. 6. Amanovletus. 7. The Griffin. 8. Maine-Iac. 9. Posus. 10. Ayemache. 11. Billy Goat. 12. Mother Lamb. 13. B. Natural. 14. Petle-O. 15. "33". 16. Platagone. 17. Plantina. 18. Fred Domino. 19. Mrs. Bryant. 20. Freddie. 21. Budget. 22. F. I. Nance. 23. Sunny. 24. Janita. 25. Girl Friday. 26. Peter. 27. Anne. 28. Al. 29. Beth. 30. Butta Greese. 31. Chess-Nut. 32. Chappi. 33. Reesman. 34. Duntoven. 35. Aristotle. 36. C. Kerr. 37. The Square. 38. Bee Gee. 39. Nebula. 40. "109". 41. Mrs. "109". 42. Port Summer. 43. Florence. 44. Pee Bee. 45. Fantom. 46. Oedipus. 47. Sybil. 48. Ayl Wyone. 49. Rubine. 50. Mr. Perachio. 51. H. S. Law. 52. Renno. 53. Josannah. 54. Chips. 55. Bouncing Bob. 56. Lilo Tusi. 57. Smiles. 58. Evgreen. 59. Doc Sappo. 60. Logosmith. 61. Daisy. 62. Koe Pop. 63. Madcap. 64. Miss Kee Pon. 65. Bzmarc. 66. Apakusan. 67. Beta Sub One. 68. Miss Risenman. 69. Miss Bryant. 70. Aunt Het. 71. Belle Ami. 72. HoHo. 73. Dr. Ross. 74. Quetanon. 75. Bunny. 76. Miss Elsie Bryant. 77. Gold Plate. 78. Ben Ami. 79. Mrs. Koss. 80. Wandu. 81. Birdie. 82. Cookie. Present but not in the picture. Tryit.



VOL. 10
No. 3

JUNE
1941

INDEX

Observations About Transpositions	41, 47
St. Louis Labor Day Convention	43, 48
Primary Alphabets, Pt. II ..	45, 48
You're In The Army Now ...	46
Problems ..	50 to 57
April Solutions ..	57
February Solvers	59
Boston Convention	60

Official Publication of The American Cryptogram Association

Observations About Transpositions *by TRYIT*

In solving a transposition cipher, the first step is to determine whether the cipher has been written into a rectangle or some other geometric form such as a triangle, diamond, pentagon or any of the various other shapes. In the simpler types of rectangular forms this is usually easy to determine but in the others, established formulas may help or recourse taken to a trial and error method. I have had some that the only possible means of solution seemed to be to anagram them but unfortunately this often results in an ambiguous text which is probably incorrect as well.

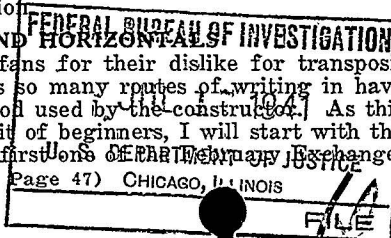
The cipher written in the form of a star, rhomboid or diamond is particularly hard to determine. However in a later issue formulas will be given for these unusual types. Careful examination will break down such as No. 2 of the April Exchange, where letters have been transposed by groups of three, four or five letters. We recently included in the Exchange one in which each group of five letters was transposed by alphabetic order; the fact that it could not fit a rectangle indicated some unusual order of transposition.

The best approach in determining the dimensions of a rectangle is to secure all the numerical factors of the total number of letters in the message. The first cipher in the February issue contained 77 letters so a rectangle to fit this would be seven cells across and eleven cells deep or vice versa. Trials at each shape would soon give the correct one. The second cipher of that issue contained 108 letters. Such a total number of letters offers many possibilities such as a 9x12, two rectangles that are 6x9, three 6x6, or four 3x9. In an extreme case the message might be in three rectangles, one 6x8 with two additional ones 6x5. This would be unusual but I have seen ciphers constructed in this manner. The Nihilist Transposition is much easier to identify because its form must always be a square; in reality the Nihilist is a type of double transposition.

SIMPLE VERTICALS AND HORIZONTALS

One reason given by many cipher fans for their dislike for transpositions is that with the more difficult ones so many routes of writing in have to be tried before you arrive at the method used by the constructor. As this article is written primarily for the benefit of beginners, I will start with the simplest form and use as an example the first one of the February Exchange.

(Continued on Page 47) CHICAGO, ILLINOIS



The Cryptogram

THE CRYPTOGRAM is the official publication of The American Cryptogram Association, and is issued bimonthly. Subscription Price to members of the Association is 75 cents a year. The Annual Membership dues are \$1.00, 75 cents of which is for a year's subscription to THE CRYPTOGRAM. The Subscription Price to non-members is \$1.00 a year.

Editors, Norman Dillinger, (ANNA LIZER), 5725 Walnut St., Pittsburgh, Pa., and Charles N. Sedenger, (SHERLAC), 3835 N. Darien St., Philadelphia, Pa. Publisher, Mrs. W. H. Barber, (JO), Burton, Ohio.

Entered as second-class matter November 27, 1937, at the post office at Burton, Ohio, under the act of March 3, 1879.

Copyright, 1941, by The American Cryptogram Association.

OVER THE DESK

The Associate Editor wishes he could answer every letter received, containing good wishes and promising support, but as this is manifestly impossible, please accept this as a personal "THANK YOU". Such heart warming missives deserve the best efforts in return, and this I pledge to the best of my ability. Again Thanks.

The C O P S, are again in evidence, this time the list reads Tyroe, Quintuplex, S-Tuck, Doodler, Park-in-Sun, Valkyrie, Iminamist, Beetle, Delver, Dr. Cryptogram, Gnilpik, The Lieutenant, Squirrelb, Squirrel-B82, Dmitri. Thanks one and all.

The committee composed of Neoteric, chairman, and Billy Goat, Neon, Park-in-Sun, Posius, and Primrose, took a number of ballots to arrive at a slate for the election of officers in September and now submit their findings:

	First Choice	Second Choice
For President	Neoteric (5)	The Squire (3)
" 1st Vice Pres.	Billy Goat (5)	Park-in-Sun (4)
" 2nd Vice Pres.	Park-in-Sun (3)	Tryit (3)
	Lilo Tusi (2)	Empty (2)
" 3rd Vice Pres.	Morning Glory (5)	Empty (5)
" Secretary	Decibel (5)	Bouncing Bob (2)
" Treasurer	Neon (6)	Fred Domino (5)
" Editors	Anna Lizer & Sherlac (5)	Maine-lac (2)

The committee wishes to inform you that its selections have been arrived at after lengthy consideration, but that nevertheless, the final choice of officers depends upon the ballots of our membership, who may still select candidates of their own choosing.

Respectfully submitted,
NEOTERIC, Chairman.

Many of our members have never selected a Nom for their own individual "Trade Mark". Somehow or other the writer feels that a nom gives its owner a handle by which his (or her) fellow Crypters can get a better grasp when making contacts; comparatively few surnames are unique, on the other hand there is little chance of confusing the noms, these being shorter than real names, are more easily memorized, I would be interested in the opinions of the KREWE on this subject.

In an effort to make the members seem more like Individuals to the rest of the KREWE, here is a suggestion: send me a thumbnail biography of yourself, to be printed in a little box to be known as "The Portrait Gallery". Each month we will try to arrange for several of these sketches, they will be reproduced exactly as sent in, positively no editing, - That's a Promise.

There has been a fairly large number from the Krewes who have entered the Service, so that it would be almost possible to start a small Army composed of A. C. A. members; as we sincerely trust their present addresses will be temporary, there will be no change made in the forthcoming edition of the Directory, their home folks will undoubtedly forward everything to them with the greatest speed possible.

FEBRUARY SOLVERS' LIST

Due to recent changes in our new editorial set-up and the necessity of forwarding mail, some omissions were made in the last issue. We are glad to make these additions to the December ratings. In the Honor Roll, NEOTERIC should have a credit of 147 foreigns. In the monthly list PETIE-O 25 Aristies and 2 ciphers; S-TUCK 21 Aristies, 13 Ciphers, 3 Pats, 5 Arithms and the special; W.B.C. 12 Ciphers and 3 Foreigns; BEGH 24 Aristies and 3 Pats; MISSIS-BEG 24 Aristies and 3 Pats; MECHANIC AL 16 Aristies; BYL 11 ciphers and 2 Foreigns; TUELS 25 Aristies, 9 Ciphers, 3 Pats, 2 Foreigns, 5 Arithms and the special; D. MORGAN everything complete.

EVERYTHING COMPLETE (44)—Drofflet; Dummd; Empty; Fiddle; Knut krakr, Jr.; Nemo; Neoteric; Park-in-Sun; Phoney; Quintuplex; X. Gotky; X. Trax.

12 Completers

ARISTOCRATS (25)—Ah Tin Du; Alpha; Antique; Arty Ess; Aunt Het; Ayemache; Beau Ned; Betty Boop; Blackie; Blotto; B.Y.L.; Comrade; Crystel; C-Sharp; Deiver; Doodler; Double-X; Drofflet; Dunroven; Dummd; Eegh; Empty; Fiddle; Gehuma; Gemuu; Genesian; Ginhuts; G. Fulton; Home Brew; Iminamist; I. N. Joyum; Joy Baby; Juub; Katmat; Kiki; Knut-Krakr; Lily; Lu; Macaw Macropod; Maida Derby; M.E.; Missiseeg; Nemo; Neon; Neoteric; Omar Kyam; Palomita; Park-in-Sun; Persis Tent; Petie O; Phoney; Polygone; Quintuplex; Red Eraser; Sis; Sour Fuss; Squirrelb; Squirrelb-82; S-Tuck; Trihard; Tryit; Tuels; Voyageur Sr.; Whizz Bang; Wolf; X. Gotky; X. Trax. 24—Aloha; Curley; D. Coy; Lilo Tusi; Uncle West. 23—Galupoly. 22—Obsidian; Queen Anne. 21—Tal Vez; Tish; K.B.J. 20—H. Le Care; Jeete; Lo-To-No; Nick Spar; Roch; W.8-EQ-N; Madda Boutem. 19—Captain Jo; Gnilpik. 18—Carso; Gaga; Ho Ho; Mechanic Al; Plantagenet; Silva; Tyroe. 17—Normal Bean. 16—Abstruse; B. Uneek; Tippecanoe. 15—M.A.G.E.; Mark Five; P. Wee. 14—Alma Matre; Dr. Cryptogram; Eluubee; Mahnom; P-UzzlePhann; Tweedles. 13—Bootleg Mutt; Dick Cissel; Quipogam; Wehanowit; X.Y.Z.; Zanycodab. 12—Britt; Connie Firzma; Jay Tee Tee; Lina; Sylvan Dell. 11—Col.A.Korn; Night Owl; The Lieutenant. 10 or less—Contracus; Dips; I Will Duit; Mark Time; Simplicius; Valkyrie; Detto.

Total Solvers 127

Total Solutions 3627

FOREIGNS (5)—Abstruse; Aloha; Antique; D. Coy; Delver; Drofflet; Dummd; Empty; Fiddle; Galupoly; G. Fulton; Home Brew; Howitzer; Kat Mat; Knut-Krakr; Nemo; Neoteric; Park-in-Sun; Peggy; Persis Tent; Phoney; Quintuplex; Tryit; X. Gotky; X. Trax. 4—I.N.Joyum; Lu; Tal Vez; Zanycodab; Madda Boutem. 3—Alaja; Bootleg Mutt; Curley; Doodler; Gemuu; Polygone; Tuels; Valkyrie. 2—Britt; Captain Jo; Ciphersmith; Gehuma; Kiki; Mark Five; Tweedles; Tyroe; W.B.C.; Whizz Bang. 1—Blotto; Dr. Cryptogram; Gaga; Ho Ho; I Will Duit; K.B.J.; Macaw; Manana; Missiseeg; Normal Bean; Russieux; X. Y. Z.

Total Solvers 61

Total Solutions 203

PATRISTOCRATS (3)—Ab Struse; Ah Tin Du; Alma Matre; Aloha; Alpha; Antique; Ayemache; Beau Ned; Betty Boop; Blackie; Blotto; Britt; B.Uneek; Byl; Captain Jo; Ciphersmith; Comrade; Crystel; C-Sharp; D. Coy; Delver; Doodler; Double X; Drofflet; Dunroven; Dummd; EEegh; Eegh; Empty; Fiddle; Galupoly; Gehuma; Gemuu; Genesian; Ginhuts; G. Fulton; Gnilpik; Home Brew; Howitzer; Ianta; Iminamist; I.N.Joyum; Jeete; Joy Baby; Katmat; K.B.J.; Kiki; Kismet; Knut-Krakr; Lily; Lilo Tusi; Lina; Lu; Lo-To-No; Mahnom; Missiseeg; Nemo; Neoteric; Night Owl; Normal Bean; Obsidian; Park-in-Sun; Peggy; Persis Tent; Phoney; Polygone; Queen Anne; Quintuplex; Quipogam; Red Eraser; Russieux; Silva; Sour Fuss; Squirrelb; Squitl B 82; S. Tuck; Sylvan Dell; Tal Vez; Tippecanoe; Tish; Tri-hard; Tryit; W.8-EQ-N; Whizz Bang; Wolf; X. Gotky; X. Trax; Zanycodab; Maddaboutem; Tuels; Tweedles; Ty Roe; Uncle West; Valkyrie; Voyageur Sr. 2—Dr. Cryptogram; Gaga; Guss; Ho Ho; Petie-O; P. Uzzle Phann; Roch. 1—Merle, Morning Glory; Simple X.

CIPHERS (11)—Aloha; Bee Gee; Blackie; Cifra; Drofflet; Dummd; Eegh; Empty; Fiddle; Ianta; I.N.Joyum; Kiki; Knut Krakr; Lu; Nemo; Neon; Neoteric; Park-in-Sun; Peggy; Phoney; Quintuplex; Red Eraser; Sahib; The Squire; Valkyrie; X. Gotky; X. Trax. 10—B.Y.L.; Lilo Tusi. 9—Galupoly; Polygone; S-Tuck; Tuels; The Lieutenant; W.B.C.; Zanycodab. 8—Ah Tin Du; Contracus; C-Sharp; Roch; Trebor. 7—Antique; Bootleg Mutt; Eegh; Kat Mat; K.B.J.; Missiseeg; Night Owl; Simplicius. 6—Alaja; Captain Jo; Delver; Doodler; Gemuu; Obsidian; Quipogam. 5—Ayemache; Gaga; Ho Ho; Whizz Bang. 4—Crystel; C-Sharp; Normal Bean; Tal Vez; Tweedles; Ty Roe. 3—B. Uneek; Lo-To-No; Merle. 2—Ciphersmith; Dr. Cryptogram; Petie O; Simple-X. 1—Alma Matre; Britt; G. Fulton; Gnilpik; Guss; Iminamist; I Will Duit; Macaw; Madda Boutem; Squirrelb; Squirrelb-82.

Total Solvers 83

Total Solutions 581

Grand Total of Solvers 377 Grand Total of Solutions 4716
Let's see how long it will take us to reach 500 Solvers, and a proportionate number of Solutions.

THE CRYPTOGRAM

solving cipher messages.

40. Outstanding progress often goes unnoticed. Aeroplanes, once considered dangerous toys, have grown into world circling transport media.

41. Lonely hound ranges mesa haunts among nomad Navaho tribe. Tribal curs bristle, growl, pursue futilely. Hound ponders repulsed friendly gesture.

42. Handsome policeman caught buxom shoplifter with silk skirt, shirt waist, fox fur hid under heavy cloak. Judge gave culprit long jail term.

43. Southpaw golfbug plows turf. Iried 'pro' urges improved stance whilst caddy hums 'He ain't got no rhythm'.

44. Two smug city boys lying under sumac shrub watch stupid ugly rustic clasp snath, whet scythe, swat plaguy gnats, cut swath.

45. Burly brown arson fraud found fresh vista under empty urban cabin. Fiery glint. Prowl squad spied light, gyved rowdy.

46. Highstrung, spendthrift yachtsmen, syphon knockdown nightcaps. Presto—voyagers downright drunk.

47. Almond-orbed Oriental, queue askew, visions ophidian atop juvia. Frightened chink vanishes, xanthic streak aback.

48. Brutal bandit yields upheld switch struck hungry urchin. Guilty wretch caught, admits tragic result.

49. Whilst lengthy abyss yawns, royal guardsmen ignore lying schema; know only duty; crowd onward, tumble; wreck kingdom.

50. Blind dwarf plays crwth. Brown chimp shows third wrong trick, gnaws knots. Black trunk drops, clips clown. Frank cloy crowd.

Patristocrats

P-4. The trouble with the country is that we are always saying the trouble with this country is, etc.

P-5. If all of your possessions were swept away by a flood in what state would you be. Reply - Ohio.

P-6. Many of the greatest financiers have been driven to the wall dash street. Dash after the street is apt too.

Arithms

- C-6. BECOMINGLY
- C-7. ROUNDPAIS
- C-8. ISOPLEURAN
- C-9. SOLEMNDIVA
- C-10. SUBTRAHEND
- C-11. ILFRACOMBE

buckwheaty

Xenocrypts

6. Il faut souvent plus de courage pour faire simplement son devoir, que pour affronter le feu de l'ennemi.

7. Tout acte porte en lui le germe de ce qu'il engendra fatalement. Qui

rompt un equilibre n'est pas sur d'en trouver un autre.

8. Wie sich Mark Twain einmal humoristisch ausdrückte besitzt die deutsche Sprache ganze "Gebirgsketten" von Werten.

9. Y en un vie jo una mujer es en un olmo una hiedra, que aunque con tan varios lazos la cubre de sus abrazos, se seca y ella medra.

10. Yo tambien amo asistir en todos departamentos, excepto que ay mis contribuciones manifesten necesariamen- os, el se seca y ella medra.

Cipher Exchange

1. An ounce of today is worth a pound of tomorrow and a ton of yesterday.

2. Its easy just reverse every three letters to solve.

3. When you feel disgusted with life in general, leave town and see others misery and you wont be able to get home soon enough.

4. With the coming of spring, plans for vacations are blossoming in some minds, budding in others and still dormant in others.

5. The old saying, "a fool and his money are soon parted" may be true, but I would like to know how the poor fool gets it.

6. Notice on bulletin board in Franklin, Pa.: "Police are hereby notified to shoot all dogs without licenses. This also applies to constables."

7. Trite alibi for solvers: If people did not make mistakes there would be no need of having rubber tips on pencils.

8. Many painters use Kodachrome to preserve details of shades for their pictures instead of relying on sketch books. (Key colour)

9. Bring cash at noon. Butch. (Initials reversed)

10. The expert is sometimes able to break a message in spite of errors in transmission which render it unintelligible to a novice with the key. (Key word Expert)

11. Another thing that keeps some men looking old is trying to make enough money to keep their wives looking young. (Key word "Weary")

12. When working on the problem of solving a tough cipher, the dyed in the wool addict loses all track of everything else in the world. QED. (Three 6x6 squares. Openings 1-8-12-15-17-24-27-32-34)

13. With the ordinary microscope scientists can see the typhoid germ with the new supermicroscope they study its whiskers. (Key "Microscopes")

14. (a) Your job is not as yet complete. (b) Find key from crypt serial numbers. (c) A hint: read ELCY — chapter seven.

15. (Simple Substitution) The road to success remains open and many persons are training at home for a better job and raise in pay.

St. Louis Labor Day Convention by PARADOX

Dear Krewe Members:

Conversations with, and letters from puzzlers, have indicated to the local committee, that most puzzlers who plan to attend the convention would like two things considered, in selecting the hotel: first, keep prices down, and second, select a downtown hotel. For more than a month, we have dined with promotion managers of hotels, visited and inspected hotels, and kept the telephone busy with conversations about hotels. We have balanced what we need, against what hotels have to offer, until we feel we have entered the hotel business. We felt we need an air-conditioned hotel, or at least partly air-conditioned; we need to consider parking facilities for those who drive their cars to St. Louis; we need to consider nearness to good theatres and other places of interest; we need to consider many other details, to plan a good time for you. So we have selected the Melbourne Hotel at Lindell and Grand Boulevards. This is not downtown, but in what is commonly called "midtown". No parking is allowed on the streets downtown as a rule, and garages are rather expensive in the downtown area. Parking is allowed around the Melbourne, and if you choose, you may park right in front of the hotel. For those who wish, the Melbourne garage will give 24-hour parking, with one pick up and one delivery for \$.60. We are trying to get even better rates. The Melbourne is near our three best theatres, one being one of the three largest, or is it five largest, in the country. St. Louis University is across from the Melbourne, farther up Lindell is the Elks Club, the Masonic Temple, the Shriners Temple, the Moolah Temple, and other imposing buildings. The central location of the hotel, and the fact that good street car, bus and service car accommodations are right at the door, make it a good choice. The final determining factor was the fact that this hotel gave us the best prices, and the promotion manager impressed us as one who will give us all possible assistance. But that was the real trouble, all promotion managers were so helpful and so kind about competing hotels, it made a choice very difficult. For single rooms without air-conditioning, there is a rate of \$2.00; double rooms with double bed, \$3.00 for two persons; double room with twin beds, \$4.00 for two persons. For air-conditioned rooms, the rates are: \$2.50 and \$3.00 for single rooms; \$3.50 for double rooms with double beds; \$4.50 for double rooms with twin beds. Where three or four persons occupy a room, the rate is figured at \$1.50 per person. In all rooms, the guest can control the air-conditioning. There are plenty of rooms at the low rates, to accommodate all who wish them. There is running ice water in the rooms. All have bath. The hotel is not one of our newer ones, but is well patronized, by fine people, and well liked.

Breakfast may be had at the hotel for \$.25 to \$.50; lunch \$.25 to \$.40; dinner \$.40 and \$.50. These are served in the popular Corner Grill. Meals in the dining room are a little more expensive. The banquet will cost \$1.50. This hotel serves all dinners and banquets for the adjacent Elks Club. Food here is very good.

Here is how we plan to spend our time: Friday night, a moon-light boat ride on the Admiral; Saturday morning, one of the business meetings; Saturday afternoon, open for shopping, shows, or the ball game between the St. Louis Browns and the Chicago White Sox; Saturday dinner, at a very delightful place called the Castilla; Saturday night, Municipal Theatre to see Balalaika; Sunday morning, sight seeing; Sunday night, banquet; Monday morning, business meeting of the second organization. After consulting officers, time will be assigned to N. P. L. and A. C. A.

The Admiral is an exquisite, streamlined, thoroughly up-to-the-minute boat. Gliders and chromium chairs are made attractive and comfortable

THE CRYPTOGRAM

with gayly-colored, over-stuffed cushions. The top deck has tables surrounded by brightly colored chairs, and umbrellas to match. Two decks are air-conditioned. Here you may dance, dine or converse with fellow puzzlers. The time: 8:30 to 11:00 P. M. The price: \$1.00. This will be a most unusual treat and while you enjoy yourself as you see fit, Ol' Man River who has his legends . . .

"He must know sumpin', but don't say nothin'—
He jes' keeps rollin'; he keeps on rollin' along."

For anything you plan to do Saturday afternoon, the White Dots will be glad to act as escorts. We shall give you a list of what might be done, so that you might choose what you prefer, for this open afternoon.

The 'Castilla is a most unique place. It gives one the impression that he is eating in a Spanish courtyard. The reproduction is authentic. We still think it one of the outstanding eating places that we have come across on our wanderings about the country. Dinner \$.65 to \$1.00. We usually take the \$.65 dinner. Special opera buses run past the Castilla, that will take us right to the Municipal Theatre.

This theatre is a place that is unrivaled and unduplicated. Here you may enjoy this delightful production, Balalaika, under the stars. In its American premier, it was compared with the *Student Prince* and *Desert Song* for its brilliance and tunefulness of music. It is really a musical comedy. Our Municipal Theatre is in Forest Park, the park in which the World's Fair of 1904 was held. This is one of the three largest parks in the country. In this theatre, 10,000 people sit under the stars, in tiers of seats arranged about a natural hill. The proscenium is formed by two huge trees in their natural setting. The orchestra pit seats 150, and the majority of the musicians are from our own symphony orchestra. From the orchestra pit to the last row of seats, there is a rise of 51 feet. The stage is 90 by 120 feet. Scenery is changed by means of a large revolving center in the stage. All operas are directed by experts from New York, and the principals of each opera are selected from the best talent in the United States. All seats are good. We have reserved a bloc of 50 seats at \$1.00 a seat. Since seats will be hard to get the last week, you should let us know if you will attend, so we may get additional seats if necessary. The bus fare will be ten cents each way. You may drive your own car, and park free. Cushions for seats may be had at \$.10, though many people do not get them. Please don't stay away from this attraction because you think you do not like opera or music. There is no doubt everyone will be highly entertained and greatly impressed.

Sunday morning we plan to show you our city. We shall start where the early settlers built the early city, and show you buildings, parks, residential districts, our Shaw's Gardens, and other places of interest, so that you will carry away, not only an idea of what our city is like, but something of its history. Our cageless bear-pits, in our extensive zoo are world famous. Shaw's Garden has the largest collection of plant life in the western hemisphere. The jewel box is an attractive place for exquisite floral displays. Some of the animals of the zoo, put on two performances a day in their own amphitheatre. The Lindbergh trophies are in Jefferson Memorial Museum. The art museum is on Art Hill in Forest Park, the park where the opera will be seen, and the same hill where visitors to the World's Fair saw Festival Hall and the Cascades. Our much talked of memorial parkway along the river front, is well under way. This is a Federal as well as a city project.

Only skeleton plans for the banquet and other puzzle meetings and entertainment have been made to date, so more cannot be given you now. But our midwestern group assure you of a good time.

Should you plan to come several days before the convention, be sure

(Continued on Page 48)

CIPHER EXCHANGE

No. 10. Fleissner Grille — When man comes of age — Valkyrie

ITNRI AWNIS CRMHE LSEAE UEHEE ENTFT
HMAIM AOSFT HGSHF IYOUO MRNMT LSHBN
TNO SI SEIAI EE.

No. 11. Columnar Transposition Irreg. Discovering new methods. Neoteric

NOHNA ERESF TETSR PIWHP RIDEY SRYOO
TOTEN ETMEN EACLN AHMGR IESTE OTSUR
OLIVM INETO AEGPS OBCRO AUILI VECFA
DEMBT SHRDR BPTBE OOTRD.

No. 12. Quagmire Type 2. With Elcy's aid — and probable words "elementary cryptanalysis" — Quintuplex

AKURO EYORF YARPW JXFBV UXBAD RTPXD
IJADC PPRJI ZWGAR ZGMCN GVUER UFGPE
UEEPS VZDWX SXNKK MDEEI FT LAV KEP SH
XPMNB TCFJD ZXGTM K.

No. 13. Plafair — Messages by (H)air. Prob. word "Examining". — Empty

OS SK PT HZ WG HS HS PG HW IU OD NC CH GN FG CI RB IQ SQ FY
FY CN BO BY IW WI OD DV NI IH ND WB FB ZC PB RS MT IW AN MC
DI ZL CW DA UO IV YR AN QY PD AK BW HS DG NW UD CN BO BI
BG SC FW ZE QI XS BY BW ST YB IF DN IF AK MB IP FO OS TB.

No. 14. Playfair — Probable word PLAYFAIR — D. Morgan

KA DB BN EK PG TP WQ QU GC SH CE ET EZ WE PX QW VI QA ZK
GQ EA LT WB BN BK HX DB WG IB QM QB IH KQ SY AC UB KQ OT
TQ PW DL EA TW CW NB AH MF WQ ON GB XH CE WG TB GQ EA
LP TB AF GP.

No. 15. Unclassified — We wonder too. What do you think? — Contracus

IODRO MCTOB ERIFN EOLBW TOTTP FWNEH
WUHRU LAALE CWUDE IHUAI OF.

APRIL SOLUTIONS

26. A few factors are to be considered in writing the text of an Aristocrat so as to conceal the clues expecting to be within the rules.

27. The schoolmarm comes in happy throng, fair maid, with book and pen, a lovely sight that makes us long to be in school again.

28. It's easy enough to be grouchy when things aren't coming your way, but the prize old growl is the man who will howl when everything is going O. K.

29. If a man spends less than he earns he is rich. If more he is poor. The amount is immaterial.

30. "May I print a kiss upon your lips?", I asked. She nodded her sweet permission so we went to press and I rather guess we printed a large edition.

31. Coroner's verdict reads thus: the deceased came to his death by excessive drinking, producing apoplexy in the minds of the jury.

32. The easiest way to obtain completes is to construct crypts that Ye Ed can use. Then you won't have to solve them. No Robot could improve

this method.

33. Rainbows in the evening mean fair day follows that is, if the rain does not wash it out of the sky.

34. Nothing could be comparable to the unnecessary waste of time and effort in carrying coals to Newcastle unless it might be carrying milk to Cowes.

35. The gorilla, which of all animals most nearly resembles man is the most terrifying and unpredictable of jungle creatures.

36. Any person who produces valuable work may not always be ready to give an account of his performances.

37. Fix your mind firmly on your work and try this if you think you can do cryptography. You can accomplish it by continuous application.

38. What we get out of life depends upon the knowledge and understanding we have of people and things about us; let us look for good in others.

39. Well-known fact: familiarity with a large number of words of a language is an important factor in

THE CIPHER TRYIT EXCHANGE

EDITOR

GREETINGS CIPHERS. Many thanks for your response to my appeal for contributions. Please be sure to have your Nom on each sheet, on each cipher would be better yet.

HINTS. No. 1 needs none. No. 2 is an eight by twelve rectangle. No. 3 is a seven by six rectangle. No. 4 is written in by rows. No. 5 single letters "A" and "I", apostrophies "T", "S" and "D". No. 6 period at "XPJ", also trigram "THE". No. 7, period at "44-96", "47-54" and "75-56". **GOOD LUCK.**

No. 1. Rail Fence — For variation see Elcy No. 44 — Bootleg Mutt

HRIFN EIHRE MTONV RAINN ITEEO EAIYE
DHNHM TOIKO NTEAL ECCPE PRISF OAI-
TO AD SHR FRESL RAWET EEHDS NW.

No. 2. Transposition — A novice says thanks — Doodler

MMAOT ICETR TTAOK NHVEN HOHNN TE-
AEO IIAFE EYMOR RNWMN UEMOE NOSAA
DKUNE FEEYO GND SM CGYSE RBNTA TE-
OOO UNTEI TOOGU R.

No. 3. Transposition — Its hard to say no — Mark Time

ORFTE TNAIE WWNMN NEITP MTRLT OOP-
IL HROSP AWWOE OR.

No. 4. Nihilist Transposition — The Queen drinks — N. Soforth

FIYUQ ALFNI QUSAS QAUES URARQ LODUN
HCEEQ EEQEU QEMNU UCISE QRIKL UUREU
QOSTT QAUNG IYNLS IT OEG Y.

No. 5. Key Phrase — Cross-examination — Galupoly

PNTDOAO: LN LNT OTEEAOW DA TOR WD-
TAC? ATWDAOO: T PNTOLD'W ORL DA'OR
WDTAC, OTD, ETW TC T ARO R PDTPEAD
T'U OTRA RNNOW DTED!

No. 6. Vigenere — The pleasure is ours — Genesian

MFVPW WURFE XPJQD NZBBG PGEUF HRYWF
ZYS CM MAZDZ XPJGM UKZHL AGJTG KWFIJ
IJVOK NPV.

No. 7. Nihilist Substitution — Teacher's Pet? — Lotono

68 90 87 67 46 57 66 76 44 48 78 47 54 26 73 55 87 45 44 96 47 56 38 57
48 75 43 44 96 66 54 39 36 39 46 46 68 68 47 54 58 86 47 48 55 57 68 56
43 39 85 68 76 56 65 60 55 46 67 53 59 68 37 44 76 75 56 49 74 39 68 37
75 68 43 47 58 54 39 46 33 74 88 47 36 59 85 39 44 65 57 60 75 56.

No. 8. Beaufort — Time and time again — S-Tuck

CQBLI CUPEO UKTYU AWGAP FYSKZ KGGMN
KPHYW ZEXHO EOTQS AKDSC BNNCG LNQNH
NCASR LEGOS PEWWY CV.

No. 9. Running Key Vigenere — Haste makes waste — Sherlock

SYPNC FKMEP GQHUS KMSVH WSMLR QITSY
SORHV HVZLO MIHQA YBSOD RXKFN BVWTY
BESOU JCYLJ VIFZG NIKTC FQ.

Recovery of Primary Alphabets - Part II.

Having obtained an alphabetic sequence in the preceding article which reads D A N S U R C Y H O G F L B E I J K M P Q T V W X Z, we are now ready to consider a crypt suspected of having been enciphered by the same alphabet. It reads C K O L R S U H G U I V F U J K X. An attempt to decipher it by the formula D/I as the former description gave it, we obtain k m q w j e i p t i d y v i a n o. (Since this is as unintelligible as the original short crypt and if our assumption is correct that the same equivalent alphabet (or alphabetic sequence) was used, this indicates that a formula different than D/I was used.

If this is the case, there are two methods of attempting to solve the new short crypt. The first is to set down the message and then run down the alphabet, Caesar style, until an intelligible text appears horizontally. In doing this though the normal ABC alphabet sequence is not used but the newly recovered sequence starting D A N S as above. Let us see how this would look. Write the first six letters of the message (CKOLRS in the first line. Starting with C in the new sequence, in vertical lines under it would come y h o g, etc.; under K would come m p q t, etc., and so on for the remaining letters. For the sake of illustration the first six letters of the message with a few lines under it would look like this:

C	K	O	L	R	S
Y	M	G	B	C	U
H	P	F	E	Y	R
O	Q	L	I	H	C
G	T	B	J	O	Y

Reading across nothing appears that seems to form words. Continuing down, in the eleventh line the first three letters would show J A P which might lead to something but the remaining three columns follow with V I B, so we decide that can not be correct. However, on the twenty-fourth line S E C O N D appears and then by continuing the remaining letters of the message on this line we find the new clear SECONDARY ALPHABET which is the solution to the short crypt.

The second way to use the alphabetic sequence is by means of sliding strips. One strip, the D A N S sequence will be the plain; the other strip twice as long will contain the same sequence twice in succession and this will be the cipher strip. It does not matter what letter either is started with, just so that the sequence is maintained. Having made the two strips place the plain or short strip above the cipher or long strip. Then examine the crypt for repeating letters. This particular one shows U appearing in a short message three times. So U must be the cipher letter for one of the high frequency letters. Now set the U of the longer strip under E (highest frequency letter) of the shorter strip and decipher the first three letters of the crypt; C K O would give a plain of J D P obviously an impossible combination. Trying U under the next highest frequency letter, T, no better results are obtained. The same occurs with O but when U is placed under A, our cipher letters give S E C and continuing the substitution we come out with the message, SECONDARY ALPHABET, with a formula of I/M.

Either the Caesaring method or the use of strips can be used and it is just a matter of choice. Sometimes one is more speedy, but then again it may take more time. Fundamentally, they are the same process.

In the last issue of the magazine a sample cryptogram was given to practice on in obtaining the primary alphabet. As a simple substitution it was easy and left only three letters to place, they being H, I, and T, which have been placed in the following table:

(Continued on Page 48)

You're In The Army Now

... by TAL VEZ and TY ROE

(The following apparently illiterate letter is suspected of being a cipher or containing a hidden message. Should you be able to determine anything in the way of conclusive evidence that such is the case will you kindly send it and any comments to Anna Lizer at the earliest possible moment.)

North Road Camp Blue, Pennsylvucky, june first, Alice my deary if you could have saw what i looked like after we got to camp. it sure give our capt Dunkle the heby jebies he didnt think we looked funny he made us go up to a corner of the Camp till we could wash away the dirt of hiking and clean up spotty clothes. last week we all had a free dinner in town as our leut said all of our rifles were kept cleaner than the ones B co used. when the leut told us that our boys made plenty noise but the Capt said you cant tear down your new bunks like that. we give three yells to tell him we were glad of the oportoonity to dine away from this mess hall then the sargint hollerd SHUN and we give him the bird. the captain didnt like for us to act like that. They put us into trucks and carried us to the restrant. WHAT A FEED we had no slum or beans, good pork chopos swimming in gravy then aple cobbler. Boy it sure was great. for this week my dutys has been on k of peas this is said to mean kutting potatos only we dont cut any of the spuds just peal the skin we have all the deserts we want after dinner or super.

Tomorrow we go on hike once again we march five miles and back again all with full pack rifles helmet gas mask and hob nail shoes. Now if the Capt or Lieut will let me censure this trial at letter writing im sure that i will miss nothing and will not give away military info. Could you come up to camp while i am here. I must stop this letter now and help cook the supper. If you come up soon you could maybe ride up along with bill Smiths sister we could all have a great time. I send kisses and i hope we will see you rideing with susie Smith. good bye for this time write a sweet letter very soon honey. as ever yours

John parker

JUNE

Foreign Crypt Department

EEGH
EDITOR

Here are five good chances to boost that solving score. These five xenocrypts, the first four by new contributors, are all comparatively easy.

No. 11, by Genesian, is the first foreign contribution from the Bedwarmers. Bootleg Mutt says of No. 12, that it "should be the novice's delight." In No. 13 Mechanic Al comments briefly on a certain modern invention. Roch goes to Victor Hugo for the memorable quotation enciphered in No. 14. To these new xenocryptors the editor extends a cordial welcome, and for all the contributions, his hearty thanks.

No. 15 is by the real old-timer, I Will Duit, who was one of the solvers of the first foreign crypts ever published in this magazine (August, 1933). During the next five years he contributed several French crypts. In April, 1934 he submitted a xenocrypt in which he asked a certain question, promising to answer it later himself if no one else did. At last, after seven years, he's given us the answer! Now, aren't you curious to know what it is?

11. French . . . Les souvenirs photographiques chez nous. (DE, DHA, BJ, D', M is Z)

A B C D E F E G D H I E J A B J H A E D D H K L H M J M
B A H A F D' P O E R H I H J N F C H Q H C H H F O H C H
H F E B Q C H A I H D E T H J H F C H H A F B J D P S C H
I' P O E R H A I H F N B F H A D H A E O P H A I H O E
A N H B C.

Fall River, Mass.

GENESIAN

12. Spanish . . . Dolora. (DK, DH, DQ, IDH, DQSD, M is P)

D K D Q S D J Z K I L S P T E I L P K T I T D Q Y D P I T I
K E J D K S E P T; S L I L D Q Q D B Z K D H A L H L P
I D H A P E Q S T H A L K N Z D Q D J E P T. * P T J L K
I D * A T J M L T J L P.

Lebanon, Tenn.

BOOTLEG MUTT

13. Spanish . . . Que le parece a V?

U N O E N S A L M O C M B D M H B D I C D J D M L M H
H N Y I A U M S M H Y M I B M L B I C M U T I U N L B N S
M L B D I U K R M O M V R M C M B N H B M C M L I U I
Y M U M J N H D I O D H E D U N O.

St. Paul, Minn.

MECHANIC AL

14. French . . . Une verite imperissable.

E Q I L F I K D K Q I G Q C Q P H G U P H C U V H G D U I V
B Z D Z H V K Q U P H W V U K H F I ' Z B Q I V E Q V
E I Q K B B Z Y U I B Q J K Q P P Q Q H D V K Q; Q P H
V Q B Q Q D B I G N Q Z I L P U C G B Q I V P U C Q G H
B Q D B I G N Q Z I.

Meriden, Conn.

ROCH

15. French . . . Apres sept annees, la reponse!

O' R M G H O R G H T R U G H Y N H Q Q H H A R M A Q R
G H D M C H B R U R G M H U H - J Z R U B R M C H. V U U H
T' R O T R M C Z H X V U G N. H L S M H U! Q R D V M
B M: "O H T H C V N D M H U C!"

Woonsocket, R.I.

I WILL DUIT

THE CRYPTOGRAM

75. Riding Habit.

M Q V Y B S I W, M C I F O A T C R D Z V S Y D Z A F Y Z
U I O, L C G Z H I J, Z W U I O V C B O V E C Q A - U Q C V
Q F Z B O, B Z U I Q D W N Z E S C G C B Y J I - W H C B U
N C D V U.

Clarksdale, Miss.

SOUR PUSS

Send all solutions to C. N. Sedenger, 3835 N. Darien St., Philadelphia, Pa., postmarked not later than August 1, 1941.

PATRISTOCRATS

P-7. With a heart affection. (Probable word 'probably')

W H O L E L A O U X T S T B G U C O U C A C R Z C E M
L Z N S R S U U X M T C W S H A C X P A X V C A X U Z X
P S T C S H.

P-8. And they last for hours. (KOV, USE, BAA)

K O V T U S P K V D C M K O V T V V K U S E B X V B A
A M U, A A V Y P N Q U K O D V J C S Y D C M K O V T C K
U C S.

P-9. A grain of truth. (UVX, JLW, AY)

U V X C S R N X P A Y T V X J U J L W N A S L N J L Z A M C
J L W W A T L F M U U V X C S R N X A Y T R G W A J U
P S X Q J R L P U V X P J Q X.

Muncie, Ind.

X TRAX

CRYPTARITHMS

C-11. Division by Try It (Two words 0-9)

W A S) P A S T T I M E (P W T T M: — M N E W = E M E T
— N E M P = R N A I — R M S T = R A T M — R M S T =
M T N E — W A S = E P W.

C-12. Division by X Trax. One word 1-0)

T R Y) H E L I C A L (S Y R S: — H S C R = H Y H C — A Y T
= Y A T A — Y I I Y = H I I L — H S C R = S C T.

C-13. Division by Piccola. (Two words 1-0)

E A T) B R I S K L Y (T I K Y: — B L E A = K R A K — K I T I =
S A R L — S A I E = S E Y — Y Y Y = S E Y.

C-14. Double key-word division by Edmeca. (Key-words incoherent but ten digits)

C G W E) N W D Y N C E G (e t a g: — g o y g u = Y G U A C
— u o g p l = C H N C E — o g p p o = A C E Y G — y o m u p,
no remainder.

C-15. Duodecimal by X Gnaff. (Key, two words)

S R B N X O A E = H R E W E + I R S D A + M R I I O = S I S
A S S E.

Observations About Transpositions (Continued)

As it contained 77 letters, the cipher was written into a block eleven cells across and seven deep, thus:

I F T H I S I S N O T
T O O S E V E R E L Y
C R I T I C I Z E D I
M A Y F E E L E N C O
U R A G E D T O U N D
E R T A K E O T H E R
T R A M P S G E M U U

As will be seen, all ciphers are not written in horizontally as this was. In taking off, or obtaining the cipher message the author took it off by verticals in five letter groups starting at the top of the first column with I T C M U. The next five letter group completed that column and continued from the top of the second column, thus giving him E T F O R, the next A R R R T and so on through the complete rectangle.

In solving, the worker uses the same method except that he is dealing with cipher letters instead of plain text letters. Having decided to use a block 11x7, he starts to write in vertically filling up each column in turn. In attempting to read the message, he takes it off horizontally in this case thus obtaining the clear message. This type of writing in and taking off can be referred to as horizontal - vertical. A variation of the same method would have been to reverse it and write in vertically and take off horizontally. Still another variation of this routing would be for the author to start at some other corner, such as at the upper right hand, or lower left. When this is done, the message will be a little harder to read but you soon become accustomed to being on the lookout for such an arrangement. In any case, the solving is just a matter of writing in the cipher the same way it was taken off.

SIMPLE DIAGONALS

Another route that might be used is that of diagonals. These are of two kinds; diagonals that proceed downward and those that proceed upward. Also the simple diagonal routing might start in any of the four corners of the block. Using the block above, which is written in horizontally, let us take off the cipher message with down diagonals starting in the upper left hand corner and the first few groups will be I F T T O C H O R M etc. If up diagonals had been used the cipher groups would then read I T F C O T M R O H etc. As a variation the cipher groups might have started, let us say in the lower right hand corner. With down diagonals the groups would have started U R U D E M O N H E etc, or if up diagonals had been used they would have read U U R M E D E H N O etc. The block in the illustration was written in originally horizontally but keep in mind that it could have been written in vertically or by any of the diagonal routes described above. In such a case, after writing the cipher groups by some selected routing, the solver must keep his eyes open to see if he can take it off or read the message following one of the diagonal routes. Do not expect to always find the clear text reading horizontally — it rarely does.

ALTERNATE ROUTES

Each of the routes described, vertical, horizontal and diagonal may have a variation known as alternate, in which the writing in or taking off follows a weaving back and forth. For instance, in an alternate vertical the route might start at the upper left hand corner, read down to the bottom of the first column then turn and go up the second column to the top, turning down the third, etc. By following these directions trace out the route on the il-

THE CRYPTOGRAM

Illustration:

Alternate Vertical — (start in upper left) ITCMU ETRRR AROFT OIYAT etc.

Alternate Horizontal — (start in lower right) UUMEG SPMAR TERTA KEOTH etc.

Alternate Diagonal — (start in lower left) TREUR AMTRM CAAAP SKGYR etc.

Alternate Diagonal — (start also in lower left) TERAR UMRTM PAA AC TRYGK etc.

If you want to follow an alternate diagonal throughout, see the second cipher of the February issue, which was written in this way and taken off by horizontals from the left end.

St. Louis Convention (Continued)

to write to Molemi or Paradox for ways of planning your vacation in our city and nearby places in Missouri and Illinois. Many lovely and interesting trips can be made in a day. Should you drive, be sure to write to us for routes. We are inveterate drivers, and know all roads to either coast, and to and through Canada and Mexico. From the East, highway No. 40 is most direct. Across the north we have used No. 20 and No. 6 so know the road. No. 50 from Cincinnati, is good for any who visit the Shenandoah Valley and the Smokies, and come north to No. 50 via No. 60. From Chicago, the best route is through Kankakee, Decatur, Taylorville to No. 66, then into St. Louis over the Chain of Rocks bridge. From the west, No. 40 is good. From the north there are several routes, finally entering St. Louis over No. 61. We shall be glad to help anyone with a good route to our city.

We are anxiously awaiting our puzzle friends and guests of the American Cryptogram, and the National Puzzlers League. We shall extend to you the good fellowship for which our organizations are famous. We shall extend the hospitality for which our city is famous. Come and meet such puzzlers as Sherlock Holmes, Hercules, Molemi, Sabio, Eegh, Fred and Freddie Domino, the youthful White Dots and all others who are working on this convention, and who all hope to be here.

—The Committee.

Primary Alphabets (Continued)

Plain—ABCDEFGHIJKLMNPOQRSTUVWXYZ

Cipher—RQSUWXYGCHZBJDMAVKEFLPINT

If you were successful in following out the directions for the recovery of the primary alphabet you obtained

—JAVELINTHROWBCDFGKMPQSUXYZ

We are now going to give a short crypt based on this recovered alphabet and by following one or the other of the methods outlined above, you work out the new message.

It reads M G O C J X M S C Z W N S Z J X Z J.

JUNE

ARISTOCRATS

69. Proceed with caution.

UZYTG IWVXB KMIG. XYWUAWVL BVMI
SGMQHB YMTX. KWLKITR JTAYMG UWLKAB
VTA FYZ. BVMIJGMI AYWFOJKB.

Rochester, N. Y.

NEON

70. Uncle Sam's Nephews. (Key word)

EYNQC UNPZ EYNP BUABJ BXUOYTZ, ZAH-
LAYHC BUVPJ OH, ZANMO THNMOZ. TFHZ-
QVUT PFCSSVUE XSFUEYOH PSFUZC LUA-
ZSQUA JNFEZ LFE LONAG NEFOA.

Pittsburgh, Penna.

ANNA LIZER

71. "Tank Youse"

ABCDEFGHI GAHI JAKLAK, HDFMNMJAIO F P Q-
MMB, ERMLE HCSHBQO NMCOIE; HGNP JD-
POGE IATO HGNGMGO C JMCP, RAKROG RM-
GEOVMLOG.

Corinth, Miss.

FRED DOMINO

72. A narrow escape.

XYZAB SWDP CZUVWH IYLUMN MWXNIV-
ZCO YPMVZH QBMVRN ABR S WCIW ILVT.
XZCOBH NYRTI XBCI RNDBX.

Brooklyn, N. Y.

AB STRUSE

73. Jig-saw puzzle?

ABKXRL HBCMG POTK MNB CPDA FDGNBU-
CATKS FDANBRKEG FDACSLOEH MFAOHB-
GPL HALFBCE DRCEHMG FACHEDGBON UL-
ZKAEM.

New York City

IXAXAR

74. Hard trade-like wharf.

XNTUIE; - UNTOURTO, HUMNOW LAW; MRACD
MLXWAU FDNAC XNRPKRMX YMLEYUPD
HONXLLWX RAWK XLKACMRXW. FLMRMD
URTUNTH, FLEW MIA.

Brewerton, N. Y.

HOME BREW

1941

53

THE CRYPTOGRAM

63. Protective Custody.

A X I X A W B C F Y W V W S X W T U Y W I W V Z Z Q W S
O Y C S O C Y S X V M N V N K K X N V E W N V A Z Q W V
Y F K W G B E C V H F W Y X V M Z Q W S T X V M K B.

Rochester, N. Y.

BEE GEE

64. Jazz-bow.

H U D F F T W S Q Y C X N M I Y T Q Y U Y C G D G G N W S
G C F Q D C C Y F W H C Y F O D Y Q C C P Y G F X N C
G T "B D V G Y W N" — F B T P M O T Q Q T P C P Y G X Q T
H M D S S Q D H C N.

Tolono, Ill.

LO-TO-NO

65. Think nothing of it, just a heavy dew.

R T C O U F U R R Z U F C U K R I U F F U Y * Y U F F U J U
W W D D W K S Y P K R G J D W. Y J K W P D U C T E D C
W K S Y P - D K Q J Y K R G J D W I D F F L Z C K R Q I K C
W Y D K Q J Y O T R Y J W.

Tallahassee, Fla.

CIPHERSMITH

66. Simple subs.

A B C D E F D G C H A, I G B J K L A M G A I K N O P Q C
R M L H. A L B R S H, I T O C H A I C O S F Q K G N L C A
T D P E K L M G C A O I N E G B J U O L K H, U R C B L A T
G J L D Q.

Ames, Iowa.

D. MORGAN

67. A low-down dive.

C R Y P T I C F E W B E E Z Y T W O C B A C H S O I C R.
T C W I L C F E E S C O B Z H I O C B L, E O C S T I C F,
O W O E H F C F, I W E K C B S C O G Z I. T I C F K C O E
G B S C O C B L R G S K E C T S O Y C O.

Minneapolis, Minn.

BYL

68. Is this a crypt or a sneeze?

B U M I M P Y L U E Y M P F O Y R A K S Y B G I K R R Y
E O F: E G I F P R N K P F I K B U M B O P H R B U I K F
B O I K B H O Y A P S U M B Y M E K M B U M M T B U M
B U M U V F P G B U B O K B O U ?

Bartlesville, Okla.

TY ROE

JUNE

THE CHATTERBOX

B. Uneek, (Marshall R. Beymer, Jr., 4711 Drexel Blvd., Chicago, Ill.) wishes to announce to a waiting world, that he has a 1000 word story containing a single "e" which is the only clue to the accompanying murder, it may be had, either for a five spot, or a brand new never before used rejection slip. The line forms to the right, please do not crowd Quite a number of the Krewes have changed their respective addresses without notifying us of the new one, consequently their copies of the February issue were returned by the Postal Authorities; if there be any who see this notice, they can have the mag sent to them by forwarding the correct address Ginhuts reports that she had a most pleasant surprise, upon answering a knock at her door, Lol on her threshold stood none other than Arty Ess in person, they had a most enjoyable half-hour of chat and used up at the least, nearly enough words to fill a good sized Mag., You know how Puzzlers are The EX-mpts have returned from Hawaii and are back at the old familiar Piedmont address, but how long they will stay put is something else again, they are most ardent puzzlers and the little Mag. is standard equipment for every journey I. N. Joyum included with her sols an analysis of the Rotating Grill Cipher which was appended to Omar's article on this subject in the February magazine A card on the desk reveals that Alpha spent the Easter holidays in the area made famous by John Smith and Pocohontas; if she contacted either of them, it remains her own personal secret The December Mag. contained notice to the effect that Cryptarithms would not be counted as solving requirements, but so many members lifted their voices in protest, that, beginning with the April Sols the records will be carefully kept and credit given in the Annual Honor Roll to "Mathematicallymindedmembersmakingmeritoriousmarks" There is a new pair of "Heavenly Twins" on the Cryptic Horizon, viz: X. Gotky and X. Trax, for 1940, and continuing through February of this year they are staging a "Photofinish" Have you got "A little SCYTALE in your Home"? Well if not, why not? NEON has plenty of them for everyone. Send him 1½ Frogskins for a sample copy, they are supposed to bring good luck — or at least they will to the A. C. A. . . . To clear up any confusion that may exist send all solutions to SHERLAC,—Charles N. Sedenger, 3835 N. Darien St., Philadelphia, Pa.; contributions of Aristocrats, Patristocrats and Arithms to ANNA LIZER—Norman Dillinger, 5725 Walnut St., Pittsburgh, Pa.; Foreigns to EEGH—Charles Eginton, Apt. 4, 1923 Feronia Ave., St. Paul Minn.; Ciphers to TRY IT—R. Hayes, 107 Mt. Vernon Ave., Rochester, N. Y., and dues and other correspondence to NEON—E. E. Alden, 189 Montcalm Drive, Rochester, N. Y. Are you moving? If so, notify Neon of your change of address as he is preparing a new directory which will be ready for the printer in a short time. . . . Contributions of cryptograms and ciphers are hereby solicited by the various department editors. Did you ever try to make one up? It is sometimes more difficult to construct a good cryptogram than it is to solve a difficult one Include your clear text, ciphering alphabet and your name and date The first of a series of articles on Cryptometry Simplified by Nyphe's Robot which appeared in recent issues was intended to show the basic principles of the system as it applies to the average (or medium difficult substitution) crypt. NYPHO will be glad to hear from all who are interested in learning more about this method of solving difficult crypts. Write H. C. Wiltbank, 926 Gordon St., Allentown, Penna., enclosing self-addressed, stamped envelope For the information of the new members, there are still available a few of the official A. C. A. pins which may be obtained for \$1.50 by writing to NEON NEON reports that the new directory is taking shape and will be ready for the printers within a short time.

ARISTOCRATS

ANNA LIZER
EDITOR

51. A Penny for your thoughts. (PAT, BK, KBJ, —TS)

EXMPTS KBJ QG FZNP — EBJSN BK PAT NX-
QT YXPPTJM XN "FZPPFT". LBMPJZUWPZB-
MN EZFF UT RJXPTKWFFG XLVMBEFTSRTS
UG PAT WMSTJNZRMTS.
Piedmont, Cal. EMPTY

52. CHERRY Blossoms, Too. (JQU, VJQX, JUXXPJVXPTZ)

JQU, *KPMJXPIJ VL *IVZAWRPT QTM WVXU
CJVCZU CUX MBATXU WPZU JQTY JQU
VJQUX JUXXPJVXPTZ KPGMPVYM PY
*TWUXPIT.
Washington, D. C. LIGHTNING

53. D'ye ever see a medicine show? (VQS, YOO, YLU)

LR NVFY LISF YIIFSIYVCRL RA GQYFOYV-
YLN, HDYGMN, YLU NSFCDN CLUCPCUDYON
GYL ES ARDLU CL YOO QCNVRFB VQYL
YWR LI VQS YOGQSWCNVN.
Meriden, Conn. ROCH

54. A current event. (VRN, VRTV, H)

"H RNTWO VRTV *NOOHN ZTB BRPALNO PQ-
NW VRN ONTVR PI RHB ZNTUVRX TGFV."
"BRPALNO — RN ZTB NUNAVWPAGVNO."
Cleveland, Ohio PLIN, JR.

55. Oh, Pshaw! (K, NLH, KJR)

EITH OQ K BUIQQ HFKBBHUKNOIJ ID NLH
RODDHUHJMH PHNYHHJ IJH SHUQIJ KJR
HTHUWPIRW HEQH. — *PHUJKUR *QLKY.
Rich Hill, Mo. NORMAL BEAN

56. But the vest gets the gravy. (MOD, -PAB, T, B)

P OTMD ME WD T NFLTKZDG, P TYKTIN
YEAB CEG HDTUD; WLM MOD KODDY MOTM
VEDN MOD NFLDTZPAB PN MOD KODDY MO-
TM BDMN MOD BGD TND.
St. Paul, Minn. MARK TIME

JUNE

ARISTOCRATS

57. Sounds like a hair-curler. (NBA, L, -CGM)

NBA FLNAON NBCGM CG WXS OA NILUO: L
WANLF FCGAH NSEA JCNB UFSM-CG LNNL-
TBWAGN, JBCTB AFATNIXTSNAO NBA WX-
SOA JBAG BA GSVVFAO L UCATA XR TBAA-
O A.
Davenport, Ia. BUBBLES

58. The same difference. (Z, VIL, UV)

ZY XWVUTURV PUOO OXXN ZV Z MXVVOL
ZYK RZH VIZV UV UR IZOG GFOO. Z WLRR-
UTURV PUOO OXXN ZV VIL RZTL MXVVOL
ZYK RZH UV UR IZOG LTWVH.
Holyoke, Mass. BEETLE

59. Chamber of Commerce says — (MOY, YUKMO)

ZHK MCH EYUKL *IKHBPXYGWY, *KOHXY
*PLSUGX OUL OYSX MOY YGBPUVSY IHLP-
MPHG HZ MOY LUZYLM WPME HG YUKMO.
*YAKHIYUG WPMPLY MURY GHMPWY.
Providence, R. I. VOLUND

60. Times aint changed much! (CR, CQ, RBT, ZGG)

CR CQ ETNLJCKA RBT NSQRLJ HLP JLITPK
JCQQQTQ RL IZRT JTK ZKI MZX ZGG RBT
TVMTKQTQ TVNTMR, RZVC, RCNFTTRQ, RBT
TZRQ, ZKI RBT IPCKFQ.
Chicago, Ill. SUNNY

61. Scanty enough. (J, Z, -TSR)

ZYYXVUTSR PX NXEKS'J IZJFTXS ZLPFX-
VTPTKJ, JLEEKV NTAA CK Z JAZYB JKZJ-
XS, SXP Z JFXVP XSK.
Fall River, Mass. GENESIAN

62. Finding one's way. (OTL, VJS)

INTERVALS OTL IOVRVALS BRY INDOVR-
NTH. NTS RH BNATL CF VRUS LRBBSGSTD-
SH, VJS NVJSG CF LRHVOTDSH NB MTNKT
HVOGH BGNU VJS DSISHVROI WNIS.
Drexel Hill, Penna. NEOTERIC

PAN:MJ

August 15, 1941

~~CONFIDENTIAL~~

b3
b7E

Assistant Director E. J. Connelley
New York, New York

Re: DUCASE

Dear Sir:

There is being transmitted herewith for incorporation into the general prosecutive summary in the Ducase a summary of the cryptographic testimony to be presented by Mr. Napier, the expert who will testify in this matter. Also included is a qualification sheet listing Mr. Napier's qualifications.

You will note that the Laboratory desires to be put on record as strenuously objecting to the introduction of any more cryptographic testimony than is absolutely necessary to the successful prosecution of this case, since it believes that public disclosures of such testimony will only result in a complete change of cipher systems and keys by the German Intelligence Service and thus will render valueless all the information so far collected concerning that organization's cipher systems. This will also mean that the valuable information presently being furnished through the decipherment of such messages will be no longer available, the resultant change in systems which is feared requiring months of work before solutions can be achieved.

It is suggested that in the event you have any comments or criticisms to make regarding this summary, you return the summary along with such comments and criticisms in order that a proper revision may be made.

Very truly yours,

RECORDED

John Edgar Hoover
Director

80-612-65
FEDERAL BUREAU OF INVESTIGATION

AUG 1941

U. S. DEPT. OF JUSTICE

FIVE

CH-23

INITIALS ON ORIGINAL

ORIGINAL FILED IN

0 Cryptography

Summary filed
with original

October 7, 1941

EPC:JR

MR. TRACY

Re: [redacted]
[redacted]

b7D

[redacted] office
telephoned from New York. He stated that he had just
talked with [redacted] and advised him that their [redacted]

[redacted] was

[redacted] He stated he was anxious to bring
[redacted] to Washington and discuss the subject of radio
intercepts and cryptanalysis with the Bureau. He stated
that [redacted] was of the opinion that this should be done.

[redacted] stated he was arriving in Washington
early Friday morning, October 10, bringing [redacted] with him
and he would ring the Bureau on arrival.

I have so far received no word from [redacted] on
this and Bureau instructions are requested as to the extent
to which these subjects should be discussed with [redacted] and
[redacted]

Respectfully,

E. P. Coffey

Mr. Tolson _____
Mr. E. A. Tamm _____
Mr. Clegg _____
Mr. Foxworth _____
Mr. Glavin _____
Mr. Ladd _____
Mr. Nichols _____
Mr. Rosen _____
Mr. Carson _____
Mr. Drayton _____
Mr. Quinn Tamm _____
Mr. Hendon _____
Mr. Tracy _____
Miss Gandy _____

250
4 DEC 27 1941

RECORDED
INDEXED
132

80-612-66
FEDERAL BUREAU OF INVESTIGATION
NOV 5 1941
U. S. DEPARTMENT OF JUSTICE
[Signature]

PN:IG

December 18, 1941

80-612 -67 RECORDED

Special Agent in Charge
New York, New York

Dear Sir:

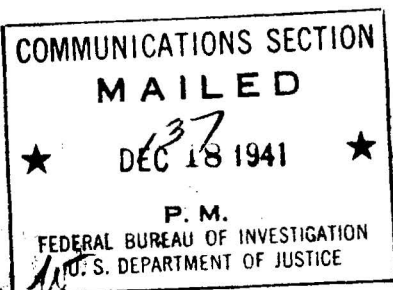
Reference is made to your letter of December 2, 1941 regarding the separate transmittal of the book on cryptography entitled "Methode Pilener".

It is desired that you express to Special Agent George J. Starr, who purchased this book, the Bureau's appreciation for his interest in the work of the Technical Laboratory which prompted him to do so. The book is being made a part of the Laboratory's collection of works on cryptography and related subjects for reference purposes.

Very truly yours,

John Edgar Hoover
Director

Mr. Tolson _____
Mr. E. A. Tamm _____
Mr. Clegg _____
Mr. Glavin _____
Mr. Ladd _____
Mr. Nichols _____
Mr. Tracy _____
Mr. Rosen _____
Mr. Carson _____
Mr. Coffey _____
Mr. Hendon _____
Mr. Holloman _____
Mr. Quinn Tamm _____
Mr. Nease _____
Miss Gandy _____



Handwritten signature/initials.

Handwritten notes: "P1" and "GAC" with a checkmark.

1A
902
12/16

**Federal Bureau of Investigation
United States Department of Justice**

GJS-MON

New York, N.Y.
December 2, 1941

Director
Federal Bureau of Investigation
Washington, D. C.

Re: CRIME DETECTION, DATA AND METHODS
Att: Mr. E. J. Coffey

Dear Sir:

There is forwarded to the Bureau under separate cover a book bearing the title "Methode Pilener." This is a book of Cryptography published in France and bearing no text to explain it's purpose. It appears to consist of pages of various arrangements of symbols to be used in place of letters of the alphabet. This book was obtained from Nelson Frank, a dealer in used books, by Special Agent George J. Starr of this office who, having no knowledge of the exact purpose of this source of a publication, purchased it for one dollar on the theory that it might be of interest to the Technical Laboratory of the Bureau.

Yours very truly,

P. E. Foxworth
P. E. FOXWORTH, *at*
Assistant Director

RECORDED
mb
INDEXED

12-18-41
PN

80-612-617	
FEDERAL BUREAU OF INVESTIGATION	
7	DEC 4 1941
U. S. DEPARTMENT OF JUSTICE	
LAB <i>ep</i>	



Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

December 31, 1941

SJT:jm

MEMORANDUM FOR MR. TOLSON

RE: NAVAL CENSORSHIP

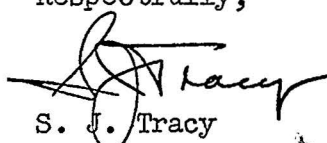
Lieutenant ^{Boone} Bone, attached to the Naval Censorship Office in the Arlington Medical Center, telephone branch D, telephoned this afternoon.

Lieutenant ^{Boone} Bone was interested in the work of the Bureau's Laboratory in cryptanalysis. He desired to know the size of the unit and to what extent the Bureau works on espionage matters, as to whether or not the Bureau has analyzed the use of black ink by the Germans, to what extent we are able to handle commercial code analysis, the amount of work we are able to handle, and so forth.

I suggested to Lieutenant ^{Boone} Bone that probably he and Captain Fenn might desire to call personally at the Bureau and discuss the matter, that this would be more satisfactory than to attempt to discuss the problem telephonically. He agreed that this would be a good idea and will make the necessary arrangements to call at the Bureau within the next day or two.

Unless otherwise advised arrangements will be made for Mr. Coffey to interview the gentlemen and ascertain the type of information they are interested in. Mr. Coffey will be instructed to furnish no specific information without prior Bureau approval.

Respectfully,


S. J. Tracy

Mr. Tolson _____
Mr. E. A. Tamm _____
Mr. Clegg _____
Mr. Glavin _____
Mr. Ladd _____
Mr. Nichols _____
Mr. Tracy _____
Mr. Rosen _____
Mr. Carson _____
Mr. Coffey _____
Mr. Hendon _____
Mr. Holloman _____
Mr. Quinn Tamm _____
Mr. Harbo _____
Tele. Room _____
Mr. Nease _____
Miss Beahm _____
Miss Gandy _____

INDEXED
JAN 1 1942

RECORDED

100-612-68	
FEDERAL BUREAU OF INVESTIGATION	
7	JAN 8 1942
U. S. DEPARTMENT OF JUSTICE	

6 JAN 15 1942



Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

March 13, 1942

CEB:AF:AL

MEMORANDUM FOR THE CRYPTOGRAPHIC MANUAL

Hereafter, it will not be necessary to furnish Mr. Holloman with copies of deciphered messages received by the Bureau from the Coast Guard which have previously been distributed by the latter to the interested Government agencies such as MID, ONI, COI, etc.

Of course, it will still be necessary to write the usual memorandum and the letter to New York transmitting copies of decipherments and translations of those messages not previously received in the Laboratory from other sources. In this case the usual two copies of the decipherments and translations will be forwarded to Mr. Little.

Very truly yours,

E. P. Coffey

Series B-13

7-12-161
MAR 31 1942
[Signature]

80-112-69

FEDERAL BUREAU OF INVESTIGATION
MAR 23 1942
U. S. DEPARTMENT OF JUSTICE

146 Hargrave Street

April 6th 1942

Winnipeg Man.

Canada

Mr J Edgar Hoover,

Sir,

4-14

I have an "Undicpherable " System of Writing , which I believe should be of value in the War Effort.

I can teach it in Five lessons.

It resembles Pitman shorthand , but has no relation whatever to it, It is so simple ,that the instructions of it need never be printed, thus making it easier to keep it secret,

I can go anywhere and bring out information, as much as

Five hundred words on each square inch of paper.

I would be glad to show it to any one whom you may suggest, and all I want is practice teaching it so that I can have it in perfect shape by the time the war is finished, so that I will be prepared to open a shorthand School then.

I have not yet obtained permission from Ottawa to send it accross the Line I would send it to London But they are so slow to take up anything new.

I have asked my Nephew , Prof. John Murray Rothnie M.D. of Harvard University , to see if he could get anyone interested in it but of course he knows nothing about it , as I must maintain the strictest secrecy possible.

Yours faithfully

Peter Rothnie

4-22-42
and
22-13-42

30-612-70

RECEIVED
APR 9 1942
U.S. DEPT. OF JUSTICE

9

TDB:AF
80-612-70

April 20, 1942

RECORDED

EX-2

Mr. Peter Rothnie
146 Hargrave Street
Winnipeg, Manitoba
Canada

Dear Mr. Rothnie:

I have your letter of April 6, 1942,
concerning a system of what you term indecipherable
writing.

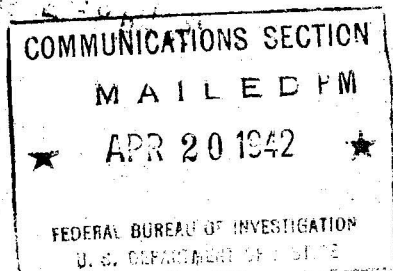
I want to thank you for your kind offer
to furnish your system to this Bureau and should
you wish to forward by mail detailed information
concerning it I am sure it would be of considerable
interest to the technicians of the Bureau's Laboratory
here in Washington.

Please be assured that any information
concerning your system which you care to submit to
this Bureau will be held in strictest confidence.

Sincerely yours,

John Edgar Hoover
Director

Mr. Tolson _____
Mr. E. A. Tamm _____
Mr. Clegg _____
Mr. Glavin _____
Mr. Ladd _____
Mr. Nichols _____
Mr. Tracy _____
Mr. Rosen _____
Mr. Carson _____
Mr. Coffey _____
Mr. Hendon _____
Mr. Holloman _____
Mr. Quinn Tamm _____
Mr. Nease _____
Miss Gandy _____



58 APR 23 1942

143 West Concord St.
Boston Mass.

April 20 1942

Mr. J. Edgar Hoover,
Chief F.B.I.

Dear Sir:

I have some general information that I think will be of value to you. About ten years ago I read an article in the Sat. Eve. Post by Major Herbert Yardley in which he said that no mechanical cipher system had ever been invented that could not be broken. That interested me. I had time and went to work on the problem. I solved it, but as the characters that had to be sent were double, our own government wasn't interested. A few years later I simplified it. Another system in which only one letter would be transmitted. I tried to interest the Signal Service of the Army, but they would not test it as I instructed. They wanted a long cryptogram, and twenty short ones, but ALL to be enciphered with the SAME key. That was exactly what my system was intended to avoid. I tried The British government and also France. Then I put it on the market. A German was the only one that took any intelligent interest in it. I sold him a few, and I also gave him a system by which he could get his messages out of England to Germany. The spy group would consist of three; one a war correspondent. This one would collect information. What he would send to his papers would go through the censor's office, but he could have a dictagraph without suspicion. Of course, he would be under suspicion, but he could communicate with the engineer in his apartment house. At prearranged times, the engineer would shut off his water. He would take off the water faucet and take out the ends of telephone wires. Attach them to one ear phone of the dictaphone to be the phone receiver, the other ear would be the phone sender. The engineer would send to a radio man who would put it on the air. It would

RECORDED & INDEXED 80-612-71
FEDERAL BUREAU OF INVESTIGATION
APR 22 1942
U.S. DEPT. OF JUSTICE

1-10-42
W.B.3

be speeded up until a long message could be sent in a minute or less. The sending stations would be five or more in a big circle, two or more miles apart. The advantage of this is that no conspicuous antenna would be needed and also that the stations could not be located by triangulation. As my system can not be broken, this is a perfect method of gathering and sending secret information. Messages can not be taken off the dial telephone without having every one of the telephones in London wired to a dictaphone. Too many to be practical.

I failed to sell my system to the general public. I have a few left. I am inclosing an instruction sheet that goes with the Simplified System. If I have told you enough to make you interested, I am willing to sell you some of each system. I would give you them, but I can not do so for several reasons. I have other ideas in my head that I want patent protection for. I believe that I can design a perfect stream lined projectile that can be fired through a smooth bore gun with the accuracy of the rifled bullet and get great distance. This would be valuable for anti aircraft guns where shocking power is wanted and where penetration isn't needed. I have an improved life saving device that I want to patent. It is an improved signal buoy and diving bell. I am inclosing a circular letter. I haven't been able to get any interest in this. People haven't intellectual imagination enough to appreciate it. I have others that I want to experiment with. I must have some money before it is too late. I can give you samples of both of my cipher systems and all information that I can for one thousand dollars. If you are interested, I think that it would be best to send some one to see me and we can go into the matter in greater detail and with less loss of time than by correspondence, than by mail. Sincerely, Warner W. Williams, *Warner W. Williams*

Instructions for using the **WILLIAMS SIMPLIFIED CIPHER**

The regular alphabet which is on the outside card is for the message which is to be enciphered into the false alphabet which is on the red card. These are double for convenience. There are 27 of these double scrambled alphabets. Any one of them may be used, or others made up. Infinite variety is possible. The oftener that the key can be changed, the safer it will be. The one used to demonstrate is the one numbered I that is in sight.

First: The correspondents must agree on which false alphabet is to be used, and the letter, word or combination of letters for the key. The entire false alphabet or any part of it may be used as the key. As it happens to be set now, the letter B of the false alphabet is opposite the letter A of the true alphabet, so the letter B will be used as the key letter in the first cryptogram.

We suppose that you are sending messages to the police stations. They know that B is the key letter and number one is the alphabet used. You see a wanted car, you write your message, but you send the letter that is opposite the real letter, thus:

KIDNAP CAR RED CORD SEDAN GOING SOUTH U S ROUTE FIFTEEN.

PINABW HBS SUN HZSN EUNBA MZIAM EZCDK C E SZCDU JIJDUUA
would be the message as you sent it. This is a simple substitution cryptogram and could be deciphered by an expert in a half an hour without his knowing the key, but the criminals, even though they were experts would not have time to break it.

If the messages were important and the enemy could get them and had the time and the skill to decipher them, the complex substitution system would be used. We suppose that in this message, the entire false alphabet is used as the key, starting with the letter X and going down. Write your message and the key underneath it. With A in the true alphabet in line with X of the false alphabet, you see that the letter D of your message is opposite Y in the false alphabet, so you write Y under the key letter X. Then you shift so that the letter G of the false alphabet is in line with A in the true alphabet and then T of the false alphabet is opposite to R in your message, and so through the entire message. Thus: The first line is your message, the second line is the key and the third line is the cryptogram as you send it, except it is best to make a different grouping so that the number of letters in each word does not give a clew,

DR. KING ASKS, "WILL YOU ACCEPT \$1 000 000 FOR YOUR PLANS?"
XGBYHNU JMKIOPQAZ WTS EDCRFV XG BYH NUJ MKI OPLQ AZWTSED
YTULPTP JXSBAKPCXG AUL ERFGLT GK ZWT SED LRG KXJN HGWNOC

In deciphering you would pay no attention to punctuation until the entire message was deciphered, then you could see which letters should be deciphered as punctuation.

For practice, decipher this cryptogram. It is a different message, but it has been enciphered with the same key as was used in the above message. To make it easier for you, the key has been written in under the cryptogram.

Number one:

QUJJD NMKPF YAAWU SYEDI EZAMP PYAAY CREDD KBXXN URWBC
XGBYH NUJMK IOPLQ AZWTS EDCRF VXGBY HNUJM KIOPL QAZWT

Number two is the same message as number one, but has been enciphered with a different key:

BEDDK SCRXP WYYNE JWMKF MQYCX XWYYF IOMKK RZQQS EONZI

When you have solved these two problems, you are an expert. It wasn't as hard as a cross word puzzle, now was it? A little study and practice and it will be easy, and then your private correspondence will be *strictly private*.

11

Warner W. Williams

143 West Concord St

Boston Mass.



Mr. J. Edgar Hoover

Chief F.B.I.

Washington D.C.

Warner W. Williams

143 West Concord St.

Boston Mass.

April 20 1942

Mr. J. Edgar Hoover,

Chief F.B.I.

Dear Sir:

Recently we lost a submarine ship, the O-9. She was crushed and flooded, and was too deep for divers to work, so had to be abandoned; but I thought, suppose that she was intact, but too deep for divers to work. The pictures in the papers and a talk that I had with a Naval officer who had been aboard the ship that had rescued the sailors on the Squalus, told me that in a case of that kind, the present diving bell would be useless. I thought that I could improve it. I found a number of mechanical problems. The men might be alive and well when they lost their power, might have released the signal buoy, and then smothered to death before the rescue ship contacted the signal buoy. The most important problem would be fresh air. I would have a light cable attached to the signal buoy in which would be two air hose, one to give fresh air, the other to pump out foul air. Almost as important would be to give them electric power and light, and telephone.

The pressure of the sea is about 1/2 pound per square inch for each foot of depth, but a spherical diving buoy with the best of steel boiler plate will solve that problem, and make a bell so much lighter than the present one, which is ten tons, that air or lead will ballast it so that it can be manipulated. Suspended by three cables, fastened to the bell below the center of gravity it can be tilted to make the manhole parallel, or nearly so, to the

RECORDED 80-612-111
FEDERAL BUREAU OF INVESTIGATION
6 APR 22 1942
U.S. DEPT. OF JUSTICE
SUSPENDED
center of gravity

escape hatch of the submarine. A ball and socket joint connection, lined with plastic, will avoid the use of bolts and enable a water-tight connection to be made, even if the manholes are not exactly parallel to each other. Manhole covers must be on the pressure side of the bell and the sub, and they must be opened from either side. That problem wasn't difficult. It took me only a week to figure out that I could put the adjustable gland for the signal buoy cable between the bolts of two yokes that hold the manhole covers. Lock pins solved the problem of opening or closing the manhole covers from either side. The water between the bell and the sub could be evacuated faster than water could enter, so sea pressure would attach the bell to the sub. An equalizing pipe could release the bell after the men had entered. If the men were alive and well, the bell would be sent down filled with water, except for enough air to ballast it; if they were disabled or dead, men would be sent down inside of it, lead bars being attached to it to ballast it. This isn't all of it, but it is enough to prove that I have solved all of the mechanical problems. Just a new combination of old mechanical principles, as simple as that. I know what can be done even if I do not always know exactly how to do it.

BUT --

I haven't solved the financial problem of getting the money for a patent, and I know from experience that no one can sell an idea to the government until a patent application has at least been filed. I would like to give it to the United States Navy, but I can not afford to do that. I am a disabled engineer and can not work, and am now living on charity. Whatever I do or fail to do, the reader of this letter will be partly responsible. To any one who will send me ten dollars or more, I will, just as soon as I can,

send a complete disclosure, a reproduction of my drawings and a full description. This public disclosure gives me temporary protection, but as I said, to sell an invention, a patent application is necessary. I am willing to assign a one-half interest in it for the money to patent it, five hundred dollars. If any individual or organization would like to buy it outright to give to the Navy, an offer will be favorably received. Will you help me? It may be the means of saving the life of some one that you love.

NOTE. Later. I received a letter from Lieut. A. L. Becker of the Submarine base at New London, Conn., in which he says, - "the present bell does not permit the men inside the submarine to get fresh air as soon as the signal buoy surfaces." As I said, my diving bell not only does, but as important, the foul air can be expelled as it may be poisoned from acid fumes. - "The present bell has been used with lists up to 60 degrees." Mine can be used if the sub is laying flat on its side, 90 degrees. - "It is not practicable to get the bell to the sub at greater depths than divers can work." Mine can save them if the sub is not crushed and flooded, no matter how deep it is, as no one must go down with the bell. How would YOU like to lay there and talk with the surface rescue ship and have them tell you that they could do nothing for you? Just YOU put YOURSELF in THEIR place.

If you are interested, I am willing that your own consulting engineers give their professional opinion on my invention, but it is so simple that anyone with a High School Technical education can understand it.

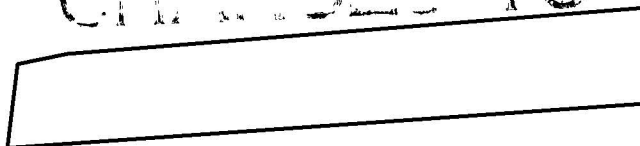
Sincerely and truly,

Warner W. Williams

Warner W. Williams.

80-612-72

CHANGED TO



b3
b7E

WGG:IG

May 6, 1942

RECORDED
65-612-71

Mr. Warner W. Williams
143 West Concord Street
Boston, Massachusetts

Dear Mr. Williams:

Thank you for your letter of April 20, 1942
transmitting the cipher message and a partial outline of your cipher
system.

You are advised that the great volume of current
investigations presently before the Bureau and the limited amount of
personnel in its Technical Laboratory preclude it from making a
critical analysis of cipher systems submitted. Any additional
information which you care to submit relative to your cipher, however,
I shall be glad to have placed in the files which the Bureau maintains
relative to this subject, for future reference.

The Bureau is not presently contemplating the purchase
of a new cipher.

Sincerely yours,

John Edgar Hoover
Director

Tolson _____
E. A. Tamm _____
Clegg _____
Glavin _____
Ladd _____
Nichols _____
Tracy _____
Harbo _____
Mohr _____
Tele. Rm. _____
Holloman _____

COMMUNICATIONS SECTION
MAILED 11

MAY 7 1942 P.M.

FEDERAL BUREAU OF INVESTIGATION
DEPARTMENT OF JUSTICE

49

1942-26

RECEIVED
FBI
MAY 10 1942

RECEIVED-ROOM 3
MAY 10 1942

MAY 9 1942

Handwritten signatures and initials: AS, W, and others.

PN:IG

RECORDED

73

April 30, 1942

Mr. Paul Kovach
244 James Street, West
Hamilton, Ontario, Canada

Dear Mr. Kovach:

I wish to thank you for your letter of April 10, 1942 in which you transmitted a cipher message of your own construction.

You are advised that the great amount of current investigations presently before the Bureau and the limited amount of personnel in its Technical Laboratory preclude it from making a critical analysis of cipher systems submitted. Any additional information which you care to submit relative to your cipher, however, I shall be very glad to have placed in the file which the Bureau maintains relative to this subject, for possible future reference.

Assuring you that your kindness in forwarding a sample of your system to this Bureau is appreciated, I am

Sincerely yours,

John Edgar Hoover,
Director

Tolson

E. A. Tamm

COMMUNICATIONS SECTION
RECEIVED

APR 30 1942

April 10/42.

244 James St. W.

Hamilton, Ont.

Canada

RECORDED & INDEXED
MCO

Dear Sir,

86-112-72

FEDERAL BUREAU OF INVESTIGATION

1 MAY 1 1942

U.S. DEPT. OF JUSTICE

LAB. *JC*

7775 8699319352 100 35612005285

447431 521585 828535 263007585 5277

995824 4477310.6 0447731 937731286 131003380

2875 997544 197758200523007775, 79619998-

99952644, 8 26459975 827561 86855285-

933003385 99261/2 447731 137752 8 8677

2861. 15777,8561 8 5285999315 2885

827761 521585 99289961200939975 827717

52617752 997588 521585 723577

58528579 9.6 447731 15993385 2.

0 Copy to [unclear]

EX-9

357775-2-75-242-2, 75-2882

7577 95157775-9385 10026 1/2 4 9979 1/2

114554100995285 6 100 939975 15759961

42617728 447731 5877 1/2 75 1 447731

61859946 521575-28 6 447731 792688-

995485 1577 1/2 85 95-90044

RECEIVED
APR 13 9 49 AM '42
TECHNICAL LABORATORY
F. B. I.
U. S. DEPT. OF JUSTICE

Yours very truly
Paul H. Harbach
Paul H. Harbach

RECEIVED
TECHNICAL LABORATORY
F. B. I.
U. S. DEPT. OF JUSTICE

APR 13 7 42 PM '42

RECEIVED

APR 13 7 43 AM '42
RECEIVED
F. B. I.
U. S. DEPT. OF JUSTICE

~~CONFIDENTIAL~~

W.C.A.

April 25, 1942

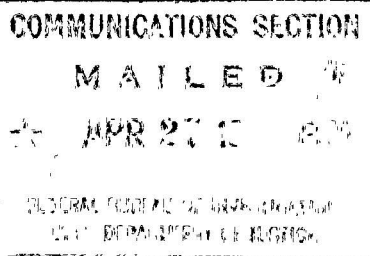
Re: Information for Cryptanalysis Purposes

Dear Sir:

The attention of all Bureau supervisors reviewing Reports is directed to the fact that the Laboratory should be furnished promptly any information which may be helpful in decoding work. Particularly any intelligence which appears to have originated in an intercepted telegram or which is in the form of a plain text confirmation of a previously transmitted coded telegram should be routed to the Laboratory. It is then possible in many instances for the Laboratory to obtain a copy of the original telegram in its coded form and by comparing the translated intelligence with the original code solve that code for future purposes.

Mr. Tolson _____
Mr. E.A. Tamm _____
Mr. Clegg _____
Mr. Glavin _____
Mr. Ladd _____
Mr. Nichols _____
Mr. Rosen _____
Mr. Tracy _____
Mr. Carson _____
Mr. Coffey _____
Mr. Hendon _____
Mr. Kramer _____
Mr. McGuire _____
Mr. Quinn Tamm _____
Mr. Nease _____
Miss Gandy _____

Such intelligence as described above is sometimes found in routine reports referred by MID and ONI. Intelligence in the form of letters which confirm previously sent coded telegrams is sometimes obtained by our own field investigators and submitted to the Bureau.



Very truly yours,

John Edgar Hoover
Director

80-612-74
[Handwritten signature]

6-1
11

Federal Bureau of Investigation
United States Department of Justice

KANSAS CITY, MISSOURI
MAY 27, 1942

Director
Federal Bureau of Investigation
Washington, D. C.

Dear Sir:

A Mrs. CARL BAUGHMAN, 603 South 11th Street, Salina, Kansas, has furnished to this office the enclosed piece of paper on which appears the following:

"SPECIAL NOTICE

Beure xsuzmo rexuso toxgar brete incan gxeat yocat urxach lesnal sonxion
boien okxous aning dxajo Biupp blexrel Sunkey dayxogg Masee yxand 31st."

Mrs. BAUGHMAN informed me that this material was found near a filling station in Salina. It does not appear to me to be written in any language, and it may be nothing more than a typing exercise of the nature used in some business colleges. On the other hand it may possibly be cryptographic in its nature, and it is requested that the Bureau make an analysis thereof with the view to determining whether it is a coded or cryptographic message. It is not necessary to return this material to this office.

Very truly yours

Dwight Brantley
DWIGHT BRANTLEY
Special Agent in Charge

DB:MT
Enclosure

RECORDED
&
INDEXED

80-612-75
INVESTIGATION
MAY 30 1942
U. S. DEPT. OF JUSTICE

10 JUN 10 1942

FEDERAL BUREAU OF INVESTIGATION
UNITED STATES DEPARTMENT OF JUSTICE

STH:MJB

Laboratory Report

RECORDED

June 29, 1942

File #

80-612-75 ✓

Lab #

81144

Re:

Small piece of paper bearing typewriting
found by Mrs. Carl Baughman, Salina, Kansas

Examination requested by:

Kansas City

Reference:

Letter 5/27/42

Examination requested:

Cryptographic

Holland

Specimens:

80-612-75 Q1. One small piece of paper bearing typewriting beginning "SPECIAL
NOTICE Beure xsuzmo rexuso toxgar brete....."

Result of Examination:

Specimen Q1 was examined and it was found that when the first two letters of each group were read the following message was conveyed, "Be sure to bring your lesson book and Bible, Sunday May 31." No meaning was found for the remainder of the letters composing the message. It is possible that these letters were merely added to conceal the other message.

The original specimen submitted is being retained in the files of the Laboratory.

Mr. Tolson _____
Mr. E. A. Tamm _____
Mr. Clegg _____
Mr. Glavin _____
Mr. Ladd _____
Mr. Nichols _____
Mr. Rosen _____
Mr. Tracy _____
Mr. Carson _____
Mr. Coffey _____
Mr. Hendon _____
Mr. Holloman _____
Mr. McGuire _____
Mr. Quinn Tamm _____
Mr. Nease _____
Miss Gandy _____

2 - Kansas City

1 - Laboratory

COMMUNICATIONS SECTION

MAILED 13

★ JUN 29 1942 P.M.

FEDERAL BUREAU OF INVESTIGATION
U. S. DEPARTMENT OF JUSTICE

18 JUL 3 1942

STH/RAJ

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1341703-0

Total Deleted Page(s) = 31

Page 9 ~ b7D;

Page 11 ~ Referral/Direct;

Page 12 ~ Referral/Direct;

Page 26 ~ Referral/Direct;

Page 28 ~ Referral/Consult;

Page 29 ~ Referral/Direct;

Page 42 ~ Referral/Direct;

Page 43 ~ Referral/Direct;

Page 44 ~ Referral/Direct;

Page 45 ~ Referral/Direct;

Page 46 ~ Referral/Direct;

Page 59 ~ Referral/Consult;

Page 60 ~ Referral/Consult;

Page 61 ~ Referral/Consult;

Page 62 ~ Referral/Consult;

Page 63 ~ Referral/Consult;

Page 64 ~ Referral/Consult;

Page 65 ~ Referral/Consult;

Page 66 ~ Referral/Direct;

Page 67 ~ Referral/Consult;

Page 68 ~ Referral/Consult;

Page 69 ~ Referral/Consult;

Page 71 ~ Referral/Direct;

Page 77 ~ Referral/Consult;

Page 79 ~ Referral/Consult;

Page 80 ~ Referral/Direct;

Page 83 ~ Referral/Direct;

Page 84 ~ Referral/Direct;

Page 85 ~ Referral/Direct;

Page 86 ~ Referral/Direct;

Page 87 ~ Referral/Direct;

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX



Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

EAT:JDR
Call 11:45 AM
Typed 3:35 PM

June 1, 1942

MEMORANDUM FOR THE DIRECTOR

Mr. Tolson _____
Mr. E.A. Tamm _____
Mr. Clegg _____
Mr. Glavin _____
Mr. Ladd _____
Mr. Nichols _____
Mr. Rosen _____
Mr. Tracy _____
Mr. Carson _____
Mr. Coffey ✓
Mr. Hendon _____
Mr. Kramer _____
Mr. McGuire _____
Mr. Harbo _____
Mr. Quinn Tamm _____
Tele. Room _____
Mr. Nease _____
Miss Beahm _____
Miss Gandy _____

Mr. C. A. Quattlebaum, Legislative Reference Bureau of the Library of Congress, called and advised a member of Congress has asked his bureau to investigate for him alleged courses in cryptography being offered in Hunter College in New York. Mr. Quattlebaum said an examination of the annual catalogue of that institution revealed no such courses, the Office of Education knew of no such courses, and he wondered if the Bureau knew of any such courses being offered there.

I advised him I knew of no such courses at Hunter College or anyplace else, that the agencies which have occasion to use cryptographers generally train their own men which is the method used by the Bureau. I told him men are selected here who are qualified in scientific fields and who have an avocation for cryptography, and they are trained in the Bureau's laboratory. To his asking if any other agencies train persons in this field, I replied I assumed the Army Signal Corps and the Communications Section of the Army train their own people, but I knew of no other group doing it.

Respectfully,

Edward A. Tamm

FOR DEFENSE



BUY
UNITED
STATES
SAVINGS
BONDS
AND STAMPS

RECORDED
&
INDEXED

80-612-76
JUN 4

June 2, 1942

SJT:EPC:jm

46091

MR. TOLSON

~~SECRET~~ (U)

~~ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 1-2-82 BY SP-5 JMS~~

Re: [redacted] (S) (U)

During a conference on other matters on this date which was attended by Mr. B. deF. Bayly, Mr. B. P. Bouverie, Mr. Coffey and myself, the [redacted] was mentioned. Some interesting comments were made thereon which it is believed should be a matter of record. (S) (U)

Mr. Bayly indicated that the [redacted] was actually referred to by other sections as [redacted] and that it has developed into a mighty, all-powerful organization. Not only does [redacted] dictate to other services as to what intercepts shall be made and forwarded to it for decoding but it also rigidly controls the dissemination of decoded intelligence and if the material is considered by it too highly confidential to disseminate at all, it may decline to disseminate it. (S) (U)

The work of [redacted] and its policies and the dissemination of information et cetera, is controlled by the so-called "Y Committee" which consists of 5 or 6 persons representing the big intelligence services. (S) (U)

Mr. Bayly indicated that very recently a mission from [redacted] visited the United States and spent about 3 weeks in conference with Army and Navy cryptanalytical section representatives. He advised upon inquiry that this mission was concerned entirely with military and naval ciphers and that clandestine radios or intelligence cipher materials were not considered. (S) (U)

Although it was not indicated it would appear from the above that the visit of the mission from [redacted] to the United States may be the forerunner of an attempt to create a similar central cryptanalytical pool in the United States governed by a Y committee. Mr. Bayly in his conversation stated that the [redacted] strongly dominates the existing setup of [redacted] and the "Y Committee". In this country, it will be noted that our United States Navy claims to have the largest cryptanalysis setup. It was noted by Mr. Coffey in another conference a week or so ago attended by Commander Redmond of the Cryptanalysis Section of the Navy that Commander Redmond made several references to a "Y Committee" leaving the impression that some plans may exist to attempt to establish a "Y Committee" over here. (S) (U)

- Tolson
- E. A. Tamm
- Clegg
- Glavin
- Ladd
- Nichols
- Rosen
- Tracy
- Harbo
- Healy
- Hendon
- Homan
- Hire
- Tamm

5 JUL 1 1942

SP-10008
11-16-73
2338154

~~SECRET~~ (U)

ORIGINAL FILED IN 65-

b7D

Mr. Coffey and I pointed out to Bayly and Bouverie that the FBI would have a direct interest in cryptanalytical activities where they would concern espionage or intelligence in the western hemisphere or other matters under our jurisdiction and we specifically asked these gentlemen to request Stott to keep the FBI advised of any developments of [redacted] such as missions to this country which might have a proper interest to the FBI. (S) (U)

~~SECRET~~ (U)

Respectfully,

~~SECRET~~ (U)

46000

S. J. Tracy

Addendum: True Name: "Code and Cipher School" for [redacted] Committee for Committee "y".
See memoranda on our studies in [redacted]

~~(S)~~ (U)

b7D

ion _____
1. Tamm _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____
11. _____
12. _____
13. _____
14. _____
15. _____
16. _____
17. _____
18. _____
19. _____
20. _____

~~SECRET~~ (U)

~~SECRET~~ (U)

June 15, 1942

PAN:AL

46090

MR. TRACY

Re: Bermuda Censorship Submission
2034/42

Reference is made to a Bermuda Censorship submission
#BERFIN 2034/42, setting forth comments concerning a letter intercepted
between one "Rosen, International Book Service, P. O. Box 227, Croton
on Hudson, N. Y., U. S.A." and a Mr. H. Roubakins, 38 Mousquines,
Lausanne, Switzerland.

It is pointed out by Mr. Napier of the Laboratory the sender
of this letter operates a book service in New York and specializes in works
on Cryptography and in the Russian language. He has purchased some books
through Mrs. Rosen at this address and found her to be reliable in all of
her business dealings with him. Furthermore, it is Mr. Napier's understanding
that Mrs. Rosen, the writer of the letter referred to in the submission slip
is the mother of Captain Leo Rosen of the Cryptanalytic Section in the Signal
Corps in Washington.

Respectfully,

E. P. Coffey

Mr. Tolson _____
Mr. E. A. Tamm _____
Mr. Clegg _____
Mr. Glavin _____
Mr. Ladd _____
Mr. Nichols _____
Mr. Rosen _____
Mr. Tracy _____
Mr. Carson _____
Mr. Coffey _____
Mr. McGuire _____
Mr. Holloman _____
Mr. Hendon _____
Mr. Quinn Tamm _____
Mr. Nease _____
Mr. Gandy _____

RECORDED

80-612-78

JUN 19 1942

INITIALS ON ORIGINAL - 13

275
10 JUN 29 1942

115132-1

80-612-79

CHANGED TO

62-26873-624X

PANAL

August 31, 1942

~~CONFIDENTIAL~~

MEMORANDUM FOR [REDACTED]

895

Reference is made to a recent conversation between two of your representatives and one of ours regarding the possibility that the [REDACTED] may have borrowed the idea of their syllable cipher system which provides for the concealment of secret cipher messages in innocuous appearing open texts from the book "Elementary Cryptanalysis", by Helen Fouché Gaines.

b7D

For your information in connection with this matter, there is attached hereto a photostatic copy of the list containing the names and addresses of persons and organizations purchasing copies of this book. In this connection your particular attention is invited to the purchase of one copy by the New York book store, E. Westerman Company, appearing on 5-A of the photostatic enclosures. You will also note that six copies of the book are listed as having been sold in March 1940 to "Maruzen, P. O. Box 605, Tokyo Central, Japan." This information appears at the bottom of page 3 of the photostatic enclosures.

It is requested that the contents of the attachments be kept in strictest confidence.

Colonel Wren requested the above information.

Mr. Tolson _____
Mr. E. A. Tamm _____
Mr. Clegg _____
Mr. Glavin _____
Mr. Ladd _____
Mr. Nichols _____
Mr. Rosen _____
Mr. Tracy _____
Mr. Carson _____
Mr. Coffey _____
Mr. Hendon _____
Mr. Kramer _____
Mr. McGuire _____
Mr. Quinn Tamm _____
Mr. Nease _____
Miss Gandy _____

Enclosure

cc-Mr. Ladd

MAILED FROM DIVISION FIVE

SEP - 1 1942

Handwritten initials and signatures: "TRK", "AS", and a large signature.

CARBON
COPY

FEDERAL BUREAU OF INVESTIGATION
U. S. DEPARTMENT OF JUSTICE
COMMUNICATIONS SECTION

AUG 5 1942

TELETYPE

Mr. E. A. Tamm
Mr. Clegg
Mr. Glavin
Mr. Ladd
Mr. Nichols
Mr. Rosen
Mr. Tracy
Mr. Carson
Mr. Coffey
Mr. Hendon
Mr. Kramer
Mr. McGuire
Mr. Quinn Tamm
Mr. Nease
Miss Gandy

FBI BOSTON 8-5-42 12-08 KG
DIRECTOR
TRAY

RE LETTER FROM BOSTON DATED AUGUST FOUR ENTITLED HIGHLY CONFIDENTIAL
ELEMENTARY CRYPTANALYSIS BY HELEN FONGHE GAINES, THROUGH ERROR ENCLOSURES
NOT SENT TO BUREAU, BEING SENT TODAY.

MADIGAN

END BOS S 1 KG
END WA R 1 JAH

RECORDED & INDEXED

mm/60

7

80-612-82	
FEDERAL	IGATION
SEP 25 1942	1.
U. S. DEI	TICE
8 - TYING NO STILL	
Called Laboratory	
M. J. [Signature]	
BY [Signature]	

37

54 SEP 30 1942
401

ORIGINAL FILE IN 80-11-5103

J.S.

80-612-84

CHANGED TO

62-26873-645X

C

80-612-85 November 7, 1942

RECORDED

INDEXED 170

EX-38

MEMORANDUM FOR MR. HOOVER

TOLSON
TAMM, E. A.
CLEGG
GLAVIN
LADD
NICHOLS
ROSEN
TRACY
ALDEN
CARSON
COFFEY

CUNNINGHAM

EGAN
FITCH
HARBO
HENDON
HINCE
KIMBALL
KRAMER
LAUGHLIN, R. H.
McGUIRE
MUMFORD
NEASE

PATTERSON

PENNINGTON
RENNERBERGER
SKOUSEN
STRICKLAND
TAMM, Q.
TIMM
TRAYNOR
WACKS
WALKART
AND SUPERVISORS

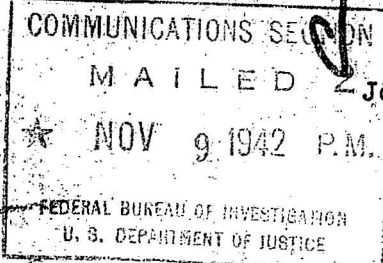
Dear Sir:

The Laboratory from time to time receives cryptograms, the basis of which is shorthand systems. It is important, therefore, to know the skill that exists at the Seat of Government in various systems of shorthand other than modern Gregg. It is requested, accordingly, that you submit a memorandum for the attention of the Laboratory listing the stenographers or other persons in your Section who have a knowledge of shorthand systems other than the Gregg. You should indicate the system or systems with which each person so listed is acquainted.

Information on obsolete and little-used systems is really the most valuable, and it is not necessary that complete mastery be had so long as a basic knowledge of the system is known.

Yours truly,

Mr. Tolson
Mr. E. A. Tamm
Mr. Clegg
Mr. Glavin
Mr. Ladd
Mr. Nichols
Mr. Rosen
Mr. Tracy
Mr. Carson
Mr. Coffey
Mr. Hendon
Mr. Kramer
Mr. McGuire
Mr. Quinn Tamm
Mr. Nease
Miss Gandy



John Edgar Hoover
Director

52 NOV 7 1942



Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

Mr. Tolson _____
Mr. E. A. Tamm _____
Mr. Clegg _____
Mr. Glavin _____
Mr. Ladd _____
Mr. Nichols _____
Mr. Rosen _____
Mr. Tracy _____
Mr. Carson _____
Mr. Coffey _____
Mr. Hendon _____
Mr. Kramer _____
Mr. McGuire _____
Mr. Harbo _____
Mr. Quinn Tamm _____
Tele. Room _____
Mr. Nease _____
Miss Beahm _____
Miss Gandy _____

MEMORANDUM FOR MR. COFFEY

We have a large number of shorthand books, both ancient and modern (all that we have been able to obtain through the New York office and through photostats of Library of Congress books).

There are two problems to shorthand examinations: (1) Identification of the system, which is a document problem depending on the comparison of the forms and (2) Translation. It has been our practice to first identify the system by the use of our library, and then find a person, either in the Bureau or elsewhere, who can read the system. When such a person can't be found, then there is always a consideration of the necessity of analysis, from the cryptographic standpoint. If the material is very lengthy, such an analysis is seldom warranted by the exigencies of the case. If the case is such a one as the Ludwig case, then such an extensive analysis is warranted.

The question of qualifying as a witness determines the procedure also, as any person who is a qualified stenographer in that system can testify as a stenographer. The only way a cryptographer or other examiner can testify is on the basis of his cryptographic training, and study of the system to read the material only and not write it. No one person can become familiar with all of the systems because it is only the odd or old systems in which cryptographic examination is necessary.

The most important assistance needed is to compile an analysis of the forms in comparison with each other, so as to enable a quick determination of the kind of system employed. We have the same problem with reference to odd languages, and some time ago I discussed with English the preparation of the analysis. This work has not actually been started, except in a meager way, because of pressure of current business, but complete plans have been made.

Very truly yours,

C. A. Appel

INDEXED

7

NOV 10 1942

EX-38



WGB:EGK

November 2, 1942

MR. TRACY

RE: Examination of Alleged
Open Code Messages by
National Censorship

Under the agreement made between Army, Navy, and FBI, regarding the distribution of code and cipher work, the Laboratory was given the responsibility of examining open code messages. This distribution was made following the President's Directive calling for the abolishment of all code and cipher examinations by all Departments with the exception of the Army, Navy, and FBI. Examination of material coming into the Laboratory definitely indicates that Censorship, both Cable Censorship and Postal Censorship, are still carrying on examinations of coded and enciphered material, particularly examination of letters and cables for "open code" messages.

In connection with Censorship's examinations of this so-called "open code" material, the Laboratory has not been able to confirm the findings of Censorship, and in addition has on numerous instances shown their results to be absolutely unreliable. I am giving below a resume of several such instances which caused the Bureau considerable time and effort in determining that the information given by Censorship was false.

SUB LIEUTENANT GEOFFREY STUART, WITH ALIASES, SABOTAGE. On February 7, 1942, a teletype message was received from the New York office advising that a cablegram intercepted and suppressed by the Canadian Censor in Montreal, Canada, had been referred to the Naval Censor in New York, reading: "VITALLY IMPORTANT GRANDPOP HAVE SHAVE TONIGHT WAY DOWN BLUEBERRY HILL. LOVE GEOFF STUARD." The Naval Censor in New York advised the New York office that the above message had been decoded to read: "TROOPS LEAVING VALENTINE DAY 8.00 PM SHARP. WILL DO NOTHING TO SABOTAGE FORWD BY ER." On February 8, 1942, the Boston office advised that two other cablegrams sent by Geoffrey Stuart read: "ALL BEST LOVE FOR NEW YEAR. HAVE ARRIVED DESTINATION. GIVE THEM THE GUN. SIGNED GEOFF STUARD," and "ALL WELL. HAD GOOD TRIP. JUST GOING TO SEE THE CRATE. LOVE. SIGNED GEOFFREY STUARD." On February 10 the New York office advised by teletype that these two cablegrams had been decoded by the Naval Censor in New York to read respectively: "NORMANDY SAILING TREE ELEVENTH. GET WIRE OFF TO HAVE VESSEL SABOTAGE AT FT HUD RIVER." or "NORMANDY SAILING ROUTE V ELEVENTH. GET WIRE AFT VESSEL SABOTAGE AT HUD RIVER." and the second telegram, "LARGE AEF TROOP SHIP LEAVING LATE TUES. JUST LOST CODE WORD LOG G," or "LARGE AEF TROOP SHIP LEAVING LATE TUES. JUST LOST LOG CODE WORD G."

Mr. Hendon _____
Mr. Kramer _____
Mr. McGuire _____
Mr. Quinn Tamm _____
Mr. Nease _____
Miss Gandy _____

RECEIVED
NOV 10 1942
FBI - BOSTON

RECEIVED
NOV 10 1942
FBI - NEW YORK

An extensive examination of this material was conducted in the Laboratory where it was necessary to conclude that the effected decodes must be based on the imagination of the Censor inasmuch as it was not possible to determine any system for obtaining the decodes. Inquiry by the New York office of the Naval Censor brought out the fact that the cryptographer had merely cut out all of the letters of each of the messages and re-arranged them to suit himself in order to make a message. The New York office also advised that they believed the cryptographer obtained a pre-conceived notion of what the message should be and then reconstructed the letters to suit that pre-conceived notion. Investigation by the Boston office revealed that the sender of the telegraph was a Sub-Lieutenant in the British Navy awaiting assignment to a submarine at the Portsmouth, New Hampshire, Navy Yard. He explained satisfactorily the contents of the messages which contained an entirely innocent meaning.

EL ESTUCHE DE LABORES; CARLOS TROCONIS, ESPIONAGE C. Under cover of a letter dated October 14, 1942, the Bureau received from the Miami office photo-static copies of a letter in Spanish dated September 28, 1942, from "Isola" whose address was given as El Estuche de Labores, Sociedad a Camejo, 14-2, Caracas, Venezuela, which was addressed to Senor Carlos Troconis, 80 Wall Street, New York City. Among other things the letter requested that the Recipient order certain quantities of cloth from the Continental Felt Company, 380 Broadway, Corner 19th Street, New York City. The Miami Censorship intercepted this letter and examiner #4594 found what purports to be an open code message contained in the list of cloth. This list is composed of three columns, the first column containing the color number, the second column containing the code word for the color, and the third column containing the number of yards desired. All of the code words denoting the color begin with the letter D, such as "Depth, Dean, Dog, etc.". According to the examiner in the Miami Censorship office, the open code messages was found by means of a dictionary. The numbers to the left of the so-called code words were used to count forward and backwards from the code words in Webster's Standard Dictionary and two columns of meanings were set down on the page. After doing this for each of the words in the list, the examiner then picked at random meanings from the two columns thus obtained. The message arrived at in this manner does not form any real sensible text.

This is a clear example of an examiner permitting his imagination to run away with him since there is absolutely no system used in his method of decoding. It is quite obvious that if an open code message appears in correspondence there must be a system by which the recipient is able to decode the open code message and know that he has obtained a correct solution. Any method of solution which permits an arbitrary selection of assigned meanings has no scientific basis and can therefore be concluded to be incorrect.

Memorandum for Mr. Tracy
Page Three

BUREAU CASES 100-144151, [REDACTED] and 100-36281. These cases consist of submissions from the Miami Postal Censorship in which alleged open code messages were found in correspondence from and to different individuals wherein dots and dashes in the writing were "decoded" by the Censorship examiner who found readable messages. Examination of these messages in the Laboratory failed to corroborate this Censorship examiner's results because it was found that the Censorship examiner had taken arbitrarily certain of the marks to mean dots and certain of the marks to mean dashes according to which would best fit into his interpretation. Furthermore, the spacing of these so-called dots and dashes was again arbitrarily taken by him to fit the meaning desired.

The Bureau questioned these solutions and after investigation Colonel Chet W. Wadsworth, Chief of the Examination Section in Washington, called Mr. Little with respect to these letters and stated that Censorship had been placed in a most embarrassing position. He advised that all the work papers had been received in Washington which had been checked by Censorship at Miami and that Censorship was unable to figure out a plan whereby the decoded messages were determined. Colonel Wadsworth stated that these submissions were sent out by the Miami office of Censorship while the Chief Examiner was sick and the alleged decodes are based on imagination and strained interpretation.

In connection with the so-called open code messages from the Miami Censorship office, it is noted that special examination unit examiner #3980 appears on practically all of the solutions with examiner #4981 appearing on the next largest number of submissions. Examiners #3980 and #4981 apparently collaborate on many of these so-called open code solutions.

ROBERT J. GIBSON, WITH ALIASES, INTERNAL SECURITY. On October 22, 1942, the New Orleans Field Office forwarded to the Bureau a submission from the Censorship office at New Orleans wherein a "decode" of an open code message in a letter was submitted. Here again examination in the Laboratory failed to concern in any way the results of the Censorship examiner's examination. It is noted that the writer who is apparently a 68 year old man has a habit of resting his pen on the paper, giving the impression that there are numerous periods interspersed in his writing at places where they should not be. The examiner has arbitrarily made counts consisting of the three words preceding and the three words following the so-called extraneous periods and has then attempted to read a message from the various columns, arbitrarily taking three words from each of the first four columns and one word from the fifth column. Here again we have an arbitrary method of solution which is not susceptible to any scientific test for accuracy. The message obtained by the censor in itself makes little or no sense.

The above is being called to your attention for any action you may deem appropriate.

Respectfully,

E. P. Coffey

b3
b7E

THE JENA TIMES
Jena, Louisiana
November 5, 1942

BLACK PAPER

Mr. Tolson
Mr. E. A. Tamm
Mr. Clegg
Mr. Glavin
Mr. Ladd
Mr. Nichols
Mr. Rosen
Mr. Tracy
Mr. Carson
Mr. Coffey
Mr. Hendon
Mr. Kramer
Mr. McGuire
Mr. Quinn Tamm
Mr. Nease
Miss Gandy

W. J. [unclear]
Kenny

FBI Men Proved They Weren't Knit-Wits, Anyway

FBI men thought they were on to something big when Seattle police discovered a notebook containing this cryptic entry: "K 1, P 2, C O 8, K 5, Y O, K 3, P 2, DECR 6, K 5, INC 4." They spent quite a while trying to decode it but finally even the cipher experts confessed they were stumped.

In desperation they set out to find the owner of the notebook, who turned out to be an attractive brunette. Upon request she obligingly translated the coded entry: "Knit one, purl two, cast on eight, knit five, yarn over, knit three, purl two, decrease six, knit five, increase four."

NOT RECORDED

1-612

CH-24

pr

2/0
FBI NYC
DIRECTOR
NINE

11-17-42

10-39 PM

WHS

--- ATTENTION TECHNICAL LABORATORY ---

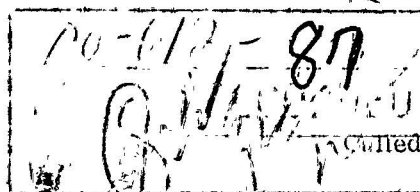
NINE

RELET NOV THIRTEENTH, FORTY TWO, REGARDING HAGELIN CRYPTOGRAPHER. TWO
UNITS OF CRYPTOGRAPHER WILL BE DELIVERED HERE THURSDAY AND FORWARDED
IMMEDIATELY THEREAFTER TO BUREAU. COST NOW REDUCED TO ONE HUNDRED DOL-
WARS PER UNIT. HAGELIN CRYPTOGRAPHER CIPHER CO. REQUESTS THEY BE FUR-
NISHED WITH PRIORITY WHICH SHOULD BE FORWARDED TO THIS OFFICE.

FOXWORTH
HOLD

*Received
at Bureau
11-25-42
COR*

INDEXED



By

WGB:HW:LAD

Date:

43578

~~PERSONAL AND CONFIDENTIAL~~

BY SPECIAL MESSENGER

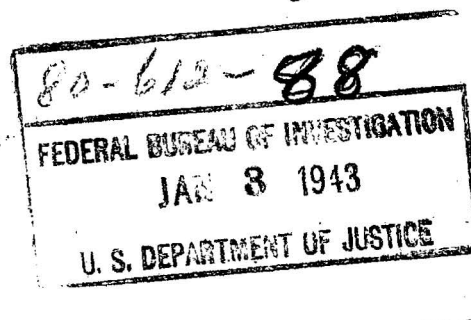
To: Colonel Carter W. Clarke
Military Intelligence Service
Special Branch
Room 2E727 Pentagon Building
Washington, D. C.

From: J. Edgar Hoover - Director, Federal Bureau of Investigation

Subject: ~~X~~ Hagelin Cryptographer

It will be appreciated if you would advise your opinion, from the security standpoint, of the use of the Hagelin Cryptographer Model C-38, manufactured by L. C. Smith & Corona Typewriters Inc., for use on land wire circuits and radio circuits on the basis of not more than ten to twenty-five messages per day. Any suggestions you might care to make concerning the periodic changing of the interior keys of the machine will be appreciated.

RECORDED
&
INDEXED



11902

RECEIVED READING ROOM
FBI
U.S. DEPT. OF JUSTICE

DEC 30 7 21 PM '42

COMMUNICATIONS SECTION
MAILED 2
★ DEC 31 1942 P.M.
FEDERAL BUREAU OF INVESTIGATION
U. S. DEPARTMENT OF JUSTICE

Quinn Tamm
Hease
Gandy

1943

345

~~SECRET~~

80-612-89

CHANGED TO

62-26873-6897

80-612-90
CHANGED TO
80-693-X

27²

Federal Bureau of Investigation
United States Department of Justice
New York, New York

66-847
SLD:RRC

January 9, 1943

Director, FBI

Re: ~~X~~HAGELIN CRYPTOGRAPHER

Attention Technical Laboratory

Dear Sir:

Reference is made to the telephone call of Mr. Williams of the Bureau to Special Agent in Charge T. J. Donegan on December 30, 1942 concerning photographs of the cipher machine used by the [redacted]

b7D

It is noted that this office previously contacted the J. K. Paulding Company, 44 Wall Street, relative to ordering Hagelin cryptographs through Mr. STUART HEDDEN.

On January 7, 1943 it was determined that the J. K. Paulding Company had gone out of business approximately December 1, 1942 since Mr. PAULDING had gone into the Navy Department.

On January 8, 1943 Mr. EDWARD M. BACON of the firm Merrill Lynch, Pierce, Fenner and Beane, 70 Pine Street, advised that the Hagelin Company had discontinued business in New York City and that Mr. STUART HEDDEN, former Hagelin representative in New York, had retired and presently resides in New Milford, Connecticut, telephone 1042.

Mr. BACON stated that he presently handles any inquiries concerning the Hagelin Company in New York in winding up their business and further that the Hagelin Cryptograph Company of New Milford, Connecticut has been entirely taken over by the United States Government.

Relative to any machines sent into New York for repairs, Mr. BACON stated that he had no knowledge of such a thing since the office closed and indicated any defective machines or machines in need of repair would be sent to the New Milford plant, who in turn would have the necessary repairs made by the L. C. Smith and Corona Typewriters, Inc.

Very truly yours,

P. E. FOXWORTH
Assistant Director



55 FEB 4 1943

347



WGB:LAD

Federal Bureau of Investigation
United States Department of Justice
Washington, D. C.

January 4, 1943

MEMORANDUM FOR MR. COFFEY

RE: ~~H~~Hagelin Cryptographer

Mr. Tolson _____
Mr. E. A. Tamm _____
Mr. Clegg _____
Mr. Glavin _____
Mr. Ladd _____
Mr. Nichols _____
Mr. Rosen _____
Mr. Tracy _____
Mr. Carson _____
Mr. Coffey _____
Mr. Hendon _____
Mr. Kramer _____
Mr. McGuire _____
Mr. Harbo _____
Mr. Quinn Tamm _____
Tele. Room _____
Mr. Nease _____
Miss Beahm _____
Miss Gandy _____

In response to the Bureau's letter to Colonel Carter
*Clarke, Lieutenant J. G. Moak of the Army Signal Corps came over
to the Laboratory on Saturday, January 2, 1943, to discuss the
Hagelin Cryptographer from the security standpoint.

Lieutenant Moak advised that he felt that messages enciphered
by means of the Hagelin Cryptographer were quite secure provided the keys
were changed often enough and that there was no excessive transmission of
messages in one key. I asked him what amount would be excessive and he
stated that forty or fifty messages in one internal key would be considered
excessive.

He suggested that the pins and lugs in the machine be changed at
least once a week providing not more than ten to twenty messages a day were
being transmitted. The literal key should of course be changed with each
message and he made some suggestions as to the manner of deriving the literal
key. In this connection there are two ways in which the literal key can be
known to the offices using the Cryptographer, the first being to supply
lists of literal keys and the second being methods of transmitting the
literal key in each message. Since it is necessary to change the literal
key for each message, the latter appears to be the best method. Since this
should not be transmitted plain, Lieutenant Moak suggested one or two methods
of enciphering the literal key.

Lieutenant Moak advised that his telephone number at Arlington
Hall was Glebe 4300 and his extension 262.

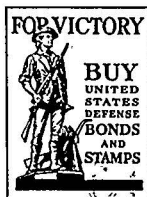
Respectfully,

W. G. Blackburn

RECORDED
&
INDEXED
1117
EX-54

62-93

F	B
8	FEB 23 1943



FEB 20 1943

RDD:ed

May 15, 1943

MR. E. P. COFFEY

RE: CENSORSHIP INTERCEPTS
CONTAINING CODE AND CIPHER

Mr. Wolgemuth of the Office of Censorship, who handles Bureau matters at that organization, called on May 12, 1943, at the Censorship Unit and in discussing other matters, stated that Censorship's Mr. Janovski, their "code and cipher man," is anxious to improve his service to the Bureau. In this connection, he is anxious to know if the type of code and cipher material which he has been sending to the Bureau is satisfactory.

Wolgemuth stated that Janovski would appreciate any information from the Bureau which would aid him in detecting the presence of code in intercepted material. Wolgemuth stated that Censorship is anxious to refer to the Bureau all code and cipher material which is intercepted and that if the Bureau Laboratory has any suggestions which would aid Censorship in being able to recognize code in harmless looking material, such suggestions would be appreciated.

ACTION:

It is recommended that such suggestions be furnished to Censorship as will aid that organization in detecting the presence of code, but that no information be given concerning the work of decoding such messages.

Very truly yours,

D. M. Ladd

Mr. Tolson_____
Mr. E. A. Tamm_____
Mr. Clegg_____
Mr. Glavin_____
Mr. Ladd_____
Mr. Nichols_____
Mr. Rosen_____
Mr. Tracy_____
Mr. Carson_____
Mr. Coffey_____
Mr. Hendon_____
Mr. Kramer_____
Mr. McGuire_____
Mr. Quinn Tamm_____
Mr. Nease_____
Miss Gandy_____

RECORDED

80-612-96

57 JUN 26 1943

ORIGINAL FILED IN 62-62776-1-312

7

ROOM 7643

In answer to your query, and to facilitate Mr. D. M. Ladd's request that suggestions be furnished to Censorship that will aid that organization in detecting suspicious mail, the following information is offered.

Very truly yours,

- ORIGINAL FILED IN
92-1067

- 3) Summarized analysis sheets of obviously suspicious cases.
- 4) Summaries of selected recorded telephone conversations.
- 5) Cable correspondence of individuals on the Bureau's Deleted Watch List.
- 6) Censored cables offered for information and attention.
- 7) The Bureau also receives submission slips of examinations by the Censorship Office of Bermuda, Trinidad and Brazil.

Trinidad and Brazil.
D. & *PA-612-97*
FEDERAL BUREAU OF INVESTIGATION
JUN 19 1948
RIP

INITIALS ON ORIGINAL

MISS GANDY _____

JUN 23 1943

Page Two
Memorandum for Mr. Coffey

Censorship submission slips which are routed to the Laboratory are examined for elements of possible significance. In accordance with the data appearing on this submission, the Laboratory obtains whenever possible the original evidence from Censorship in those cases in which it expresses an interest.

With regards to item No. 2 above, it may be noted that such submission slips contain one of the following notations: Condemned, Held, or Released. The original evidence is accessible to the Bureau in the case of Condemned material, but only occasionally available with regards to Held material, depending upon the time factor.

In the study of these submission slips in the Laboratory it has often been observed that slips marked Release sometimes contained examination reports which appeared highly significant. In such cases the original evidence is unfortunately unavailable to the Bureau.

In item No. 3 above, it would appear that in the preparation by Censorship of a summarized analysis report, it has not been considered expedient to include foreign language translations. It has been the experience of examiners in the Laboratory that the translations which appear on Censorship's regular submission forms have been useful, and that their inclusion in the summarized analysis sheets would tend to facilitate examinations.

In item 7 above, the original evidence described in these submission slips is only rarely available.

It is felt that the area of Censorship in which the Laboratory is interested is fairly adequately covered, and that the continued submission of such intercepts is desirable. However, it is felt that the frequency of cases wherein evidence has been released in spite of its latent interest to the Laboratory could be reduced if characteristics of open code were more thoroughly recognized. In this connection, therefore, it is recommended that the Bureau consider submitting the attached open-code detection sheet for the attention of Mr. Janovski of the Office of Censorship who has expressed an interest in information of this type.

Respectfully,

W. G. Blackburn

Attachment

ADDENDUM:

It may be noted that up to the present time, Office of Censorship has made no request that the examinations of questioned material be assumed by the Bureau's Laboratory. It is customary procedure for a prior examination to be conducted by Censorship before the material is submitted to the Bureau.

W.G.B.

NOT USED

80-612-98

CHANGED TO

80-174-78X

not

Capt. [illegible]
McGuire
Miss [illegible]
Aug
[illegible]

* * *
 FBI men of the Cleveland office still blush if you mention a certain little black book, full of mysterious letters and figures. A stranger dashed into the office said he had found the book in the street and it was full of mysterious entries such as "K1, P2, CO8, K5, P2, etc." Unable to make heads or tails of it, the Cleveland office sent it to Washington. A woman expert in the code bureau soon put the baffled men straight. She notified the strong silent men that the code means, "Knit 1, purl 2, cast on 8, knit 5," and so on.
 * * *

"STARS AND STRIPES"
London, England
August 10, 1943

100
 1 27-612-A
 NOT RECORDED
 87 AUG 19 1943

"FORWARDED BY A. M. THURSTON, AMERICAN EMBASSY, LONDON, ENGLAND"

61 SEP 6 1943

FEDERAL BUREAU OF INVESTIGATION
FILES DIVISION

8/19/ 1943

___ Mr. Tolson	___ Mr. Jones, M. A.
___ Mr. Tamm, E. A.	___ Mr. Kleinkauf
✓ ___ Mr. Clegg <i>etc.</i>	___ Mr. Laughlin, L. L.
___ Mr. Coffey	___ Mr. Laughlin, R. H.
___ Mr. Glavin	___ Mr. Lawrence
___ Mr. Ladd	___ Mr. MacCartee
___ Mr. Nichols	___ Mr. McCabe
___ Mr. Rosen	___ Mr. McGuire
___ Mr. Tracy	___ Mr. McIntire
___ Mr. Alden	___ Mr. Martin
___ Mr. Bellino	___ Mr. Mumford
___ Mr. Bernard	___ Mr. Minor
___ Mr. Breese	___ Mr. Nease
___ Mr. Buckley	___ Mr. Newman
___ Mr. Burton	___ Mr. Nugent
___ Mr. Callan	___ Mr. Pennington
___ Mr. Cannon, J. W.	___ Mr. Ranstad
___ Mr. Carson	___ Mr. Reed
___ Mr. Carter	___ Mr. Renneberger
___ Mr. Cartwright	___ Mr. Richardson
___ Mr. Clements	___ Mr. Sandweg
___ Mr. Coyne	___ Mr. Scott
___ Mr. Cunningham	___ Mr. Skousen
___ Mr. Fitch	___ Mr. Smith, R. E.
___ Mr. Fletcher, R. G.	___ Mr. Stetter
___ Mr. Flinn	___ Mr. Stone
___ Miss Gandy	___ Mr. Suttler
___ Mr. Gannon	___ Mr. Tamm, Q.
___ Mr. Gearty	___ Mr. Timm
___ Mr. Grill	___ Mr. Wacks
___ Mr. Halter	___ Mr. Welch
___ Mr. Harbo	___ Mr. West
___ Mr. Harvey	___ Mr. Whitson
___ Mr. Hayes	___ Mr. Williams
___ Mr. Hendon	___ Mr. _____
___ Mr. Hince	___ Mr. _____
___ Mr. Huston	___ Mr. _____
___ Mr. Johnson, W. A.	___ Mr. _____

W. J. P. H. Patterson
O. H. Patterson

WANTED BY

BERNARD FREDERICK

While impersonating FBI A States Army Officers and United State Bernard Frederick Champagne, a thirty-New York, has professed his devotion coast in furtherance of his schemes to whose only previous gainful occupations er, and grocery clerk, was once married ly 30's he turned his "talents" of a g ity toward earning a detestable living

His victims included your many of whom refused to believe he wa exposed. In many instances his smoot with his extravagant claims as to his States Government, and his family's al to public announcements of his engagem confine his affection to one woman at become engaged to two of his victims s

Doubtless there are innume have not been reported to the authori women victims have been investigated by Impersonation Statute and Federal proc in New York City; San Francisco, Calif

In each case Champagne is tained money by impersonating Federal of many aliases, it required exhaustive amination of much evidence by the FBI's rious escapades were identified as bein

His criminal record was the came the subject of a nationwide search

In 1935, Champagne, using personation activities in the vicinity representing himself as an Agent of th States Treasury Department. In the n Lake, and Port Henry, he would call u identification card stating he was an I uor stocks.

He would then advise the stamps were missing therefrom and wou stamps to be delivered at a later date sion, including recommendations of ear

NOT USED

- - - 99

CHANGED TO

15' 100 - 6.5 - 1
51 OCT 22 301

Mr. Tolson ✓
 Mr. E. A. Tamm ✓
 Mr. Clegg ✓
 Mr. Coffey ✓
 Mr. Glavin ✓
 Mr. Ladd ✓
 Mr. Nichols ✓
 Mr. Rosen ✓
 Mr. Tracy ✓
 Mr. Acers ✓
 Mr. Carson ✓
 Mr. Harbo ✓
 Mr. Hendon ✓
 Mr. Mumford ✓
 Mr. Starke ✓
 Mr. Quinn Tamm ✓
 Mr. Nease ✓
 Miss Gandy ✓

FBI Deciphers Queer Code-Find A Puzzle Contest

There's a certain topic that brings a pained and anguished look into the eyes of J. Edgar Hoover's brightest code experts—morning, noon and night.

Recently the FBI received from the Office of Censorship a mysterious pile of letters from South America, all in intricate code.

Busy experts deciphered them, only to learn that they were entries in a puzzle contest sponsored by a breakfast food concern trying to teach Latins to eat Strawmush or whatnot instead of tortillas for breakfast.

The Justice Department stepped in and said in effect:

"Please don't. We'll eat your breakfast food, but don't ask us to decode it."

NOT RECORDED
 87 JUN 3 1944

May 1, 1944

RCC:HIA

File #80-612

#62-66727

MR. CONFEY, ROOM 7643

RE: ALLOCATION OF CRYPTANALYTIC
WORK - JURISDICTION DURING
WAR TIME.

Reference is made to the attached clipping from the Washington Times Herald, dated March 17, 1944, which mentions a letter read by Senator Mead during the debate on appropriations for the Federal Communications Commission which refers to the cryptographic work of that organization.

As you know a Presidential memorandum dated July 8, 1942, directed that cryptanalytical work be limited to the Army, the Navy, and the F. B. I. It would therefore appear that if the work to which the above mentioned letter refers were done after July 8, 1942, the Federal Communications Commission was at that time undertaking an unauthorized cryptographic function.

It is further pointed out that in the above mentioned Presidential memorandum the cryptanalytical unit of the Federal Communications Commission is specifically mentioned as one of those to be discontinued.

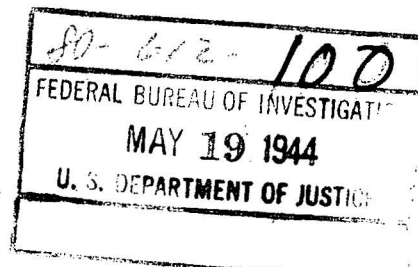
Respectfully,

C. F. Downing

olson
A. Tamm
legg
orrey
lavin
add
ichols
deen
racy
pers
arson
arbo
endon
unford
turke
lunn Tamm
case
andy

RECORDED

EX - 26



ORIGINAL COPY FILED IN 62-7794-53

5-20

Office Memorandum • UNITED STATES GOVERNMENT

TO : MR. C. F. DOWNING

BDB:EB
DATE: May 16, 1944

FROM : MR. B. D. BENTLEY

SUBJECT:

File
80-612

Mr. Tolson	_____
Mr. E. A. Tamm	_____
Mr. Clegg	_____
Mr. Coffey	_____
Mr. Glavin	_____
Mr. Ladd	_____
Mr. Nichols	_____
Mr. Rosen	_____
Mr. Tracy	_____
Mr. Acers	_____
Mr. Carson	_____
Mr. Harbo	_____
Mr. Mumford	_____
Mr. Starke	_____
Mr. Quinn Tamm	_____
Tele. Room	_____
Mr. Nease	_____
Miss Beahm	_____
Miss Gandy	_____

For your information there are at the present time three Hagelin cipher machines in the cryptanalysis section of the Laboratory. It was noted according to a memorandum over Mr. Coffey's signature dated December 7, 1942 that two of the above cipher machines had recently been acquired. One of these machines was sent to San Juan. This machine was returned to the Laboratory May 18, 1943 by courier.

The third machine mentioned above was borrowed from the army for comparison purposes. These machines are presently being used to decipher Finnish Diplomatic communications.

Should we not return
the Army machines?

80-612 -
NOT RECORDED
25 JUN 8 1944

MPC:AF

Assistant Solicitor General Hugh B. Cox

May 19, 1945

John Edgar Hoover, Director, Federal Bureau of Investigation

RECORDED
612-101
Proposed Executive Order "Establishing a Board for the Coordination and Supervision of Cryptographic Systems and Procedures of Federal Departments and Agencies".

Reference is made to your memorandum of May 9, 1945, attaching a confidential communication of May 5, 1945, from the Bureau of the Budget and the proposed Executive Order relative to the above matter.

I believe this proposed Order is a very serious intrusion into the confidential work and procedures of the Federal Bureau of Investigation and I have prepared a memorandum to the Attorney General urging him to protest this. A copy of my memorandum is attached hereto.

Attachment

EW

Tolson	
E. A. Tamm	
Clegg	
Coffey	
Glavin	
Ladd	
Nichols	
Rosen	
Tracy	
Carson	
Egan	
Hendon	
Pennington	
Quinn Tamm	
Nease	
Gandy	

11:45 AM
5-24-45

May 29, 1944

F:1/2.
86-612

MEMORANDUM FOR MR. DOWNING

For your information regarding the conditions under which a Hagelin cipher machine was borrowed from the army, reference is made to a memorandum over Mr. Coffey's signature dated December 7, 1942, in which the request was made for the Bureau's liaison officer to discuss with General Strong the possibilities of arranging for the temporary loan, for comparison purposes, of one of the army's model C-38 Hagelin cryptographers.

According to a memorandum written by Brigadier General Frank E. Strong dated December 31, 1942, the above-mentioned cipher machine was turned over to the Bureau on a loan basis with no other conditions specified.

Respectfully submitted,

B. D. Bentley

B. D. Bentley

1815K

7/30/44
OK - we
need it - could
it while anyone

Office Memorandum • UNITED STATES GOVERNMENT

TO : MR. DOWNING ✓ *J. G. [unclear]*

FROM : MR. BENTLEY *R. B. [unclear]*

SUBJECT: CIPHER MACHINES

BDB:EB
DATE: May 23, 1944

File
80-61

Mr. Tolson	_____
Mr. E. A. Tamm	_____
Mr. Clegg	_____
Mr. Glavin	_____
Mr. Ladd	_____
Mr. Nichols	_____
Mr. Rosen	_____
Mr. Tracy	_____
Mr. Acers	_____
Mr. Carson	_____
Mr. Harbo	_____
Mr. Hendon	_____
Mr. Mumford	_____
Mr. Starke	_____
Mr. Quinn Tamm	_____
Tele. Room	_____
Mr. Nease	_____
Miss Gandy	_____

Reference is made to my blue memorandum dated May 16, 1944 in which it was stated there are three cipher machines in the Laboratory, one of them belonging to the Army. In view of the fact the cipher machine belonging to the Army is different from those owned by the Bureau, it is recommended that this machine be retained in the Laboratory for further study of the Finnish and Swedish Diplomatic communications.

180-112-

NOT RECORDED
35 JUN 8 1944

The Attorney General

May 19, 1945

John Edgar Hoover, Director, Federal Bureau of Investigation

Proposed Executive Order Establishing a Board for the Coordination and Supervision of Cryptographic Systems and Procedures of Federal Departments and Agencies.

Mr. Hugh B. Cox has referred to me a matter which I consider of such importance that I would like to bring it to your personal attention.

The Bureau of the Budget, under date of May 5, 1945, referred to you for your views a proposed Executive Order. This Order, which has obviously been drafted by the Army and Navy authorities, undertakes to create a board consisting of the Secretaries of State, War, and the Navy, which will be given the supervision of all cryptographic systems and related procedures of the Federal departments and agencies.

Under this Order it would appear quite possible, if it is not actually intended, to require Government agencies, including the Federal Bureau of Investigation, to turn over to the representatives of the board all of their cryptographic systems. It further appears that the board and its representatives will be empowered to come in and make periodic inspections and surveys not only of cryptographic systems but of the so-called "related procedures". Furthermore, the board is empowered to establish security standards and policies and to promulgate such directives as may be necessary to implement its policies. Furthermore, the board and its committees are empowered to call for consultation such representatives of Government departments and agencies as may be deemed advisable in obtaining full knowledge of the situation being studied. To this end the other Government agencies (including the FBI) are directed to cooperate in providing assistance and to comply with the directions promulgated by or on behalf of the board.

The only attempt, and it is a feeble one, to limit the powers of this board is found in paragraph 7 of the proposed Executive Order. Here it is provided that no agency will be required to make available to the board for use by any other department or agency any cryptographic aid or device, the restricted or exclusive use of which it considers essential to the proper discharge of its duties in the national interest. This would appear to me to mean that the proposed board still has the power to itself take over the cryptographic systems but that it may not pass them on for use in other agencies if the originating department considers them restricted or exclusive.

Paragraph 7, at first glance, would also appear to protect an agency against being required to disclose the contents of any official communication concerning its activities, if in the opinion of the head of such department or agency the disclosure might be contrary to the national interest. However, I point out that if the cryptographic systems and copies of the cipher keys of the various Federal agencies are not filed with the board in the first instance then it would be readily able to

Mr. Tolson
Mr. E. A. Tamm
Mr. Clegg
Mr. Coffey
Mr. Glavin
Mr. Ladd
Mr. Nichols
Mr. Rosen
Mr. Tracy
Mr. Carson
Mr. Egan
Mr. Gurnea
Mr. Harbo
Mr. Hendon
Mr. Pennington
Mr. Quinn Tamm
Mr. Nease
Miss Gandy

RECORDED
INDEXED
MAY 24 1945
5-24-45

6 MAY 29 1945

RECORDED
INDEXED
MAY 24 1945
5-24-45

read any communication whatsoever that it was able to lay its hands on. You are, of course, aware that many Governmental communications are filed for transmission (after having been coded) with the Army and Navy communication networks and in many other instances, including many FBI coded messages, they are transmitted over the radio where they can be copied in their coded form.

In the memorandum of explanation which accompanies the Executive Order, the Joint Chiefs of Staff indicate that the Order is a result of surveys conducted by them of the cryptographic systems and related procedures of the various Federal departments and agencies. As I have previously advised you, the Joint Chiefs of Staff did, in fact, on two occasions send their representatives over here supposedly to make a study of the security of the FBI's coding systems. On the first occasion, which was in December, 1942, we received a copy of the committee's report on the FBI survey, the summation of which I quote below:

- "a. Cryptographic security - excellent.
- b. Physical security (cryptographic systems) - excellent.
- c. Documentary and information security - excellent.
- d. Qualifications of personnel - excellent.
- e. Cooperation was given fully and willingly.

"2. In view of the above it is considered that no concern need be felt over communications originating or passed in the Federal Bureau of Investigation organization at this time."

Again they sent their cryptographic experts over to make a similar study in July, 1944. I again agreed to allow them access to our systems and again on this occasion they could make no criticism of our cryptographic systems. They undertook on this occasion, however, to begin to make administrative recommendations. For instance, they recommended that we not file plain language copies of messages in the same file with coded copies of the same message, but rather that the plain language copies be filed elsewhere. Inasmuch as the code system which was being used on these messages is what is known as a non-repeating key system, this suggestion had no merit because the plain language copies would have no value in breaking our codes of this type. They undertook to make a similar recommendation concerning our internal routing. They made a further recommendation that the instructions for the use of our codes be reduced to writing, whereas I have always required that our top secret codes be taught orally only. I informed the Joint Chiefs of Staff that I considered their recommendation in this latter regard improper.

The above comments refer to cryptography, which is the mechanics of coding our own messages. It is not clear from the wording of the proposed Executive Order whether it is broad enough to also include cryptanalysis, which is the breaking of the codes of the enemy. In the latter connection, I would like to point out that in a memorandum dated at the White House July 8, 1942, and addressed to the Director of the Budget, the President approved a memorandum of July 6, 1942, submitted by the Joint Chiefs of Staff and as a result of this, the President instructed that

" . . . cryptanalytical activities should be limited to the Army, the Navy, and the Federal Bureau of Investigation". At that time, the Joint Chiefs of Staff commented: "As the Army, the Navy, and the Federal Bureau of Investigation now have large organizations well equipped and capable of handling the processing of all the raw material currently intercepted, the Joint Chiefs of Staff recommend that these activities be limited to the three agencies mentioned". Of course, if this presently proposed Executive Order is used in an attempt to also take over the cryptanalysis activities, then the FBI would be subject to the directives and instructions of this newly proposed board and its subcommittees concerning our important work in breaking ciphers in espionage, internal security, and criminal cases.

I am very definitely of the opinion that the proposed Executive Order should not embrace the FBI and that the Bureau should be specifically excluded in the Order if the President decides to issue the Order as regards other Government agencies.

I believe this position is a sound one, based upon the fact that the FBI is primarily and basically a security organization and has always been such. I point out that our experience and study in problems of security cover a long period of years and that we do not need a newly created board of so-called specialists to take over our code and cipher systems and to issue us security instructions. In this connection, I refer to the explanatory memorandum in which it is stated that "due to the lack of over-all supervision and coordination and the absence of effective standards of security, leaks of classified information vital to the national interest have occurred and will continue to occur unless corrective measures are taken". I submit that if any leaks of important information have occurred they have occurred in the Army, Navy, and State Departments and they have not occurred in the Federal Bureau of Investigation. As a matter of fact, I am unable to see how I can be expected to assume the responsibility of the security of this Bureau's highly confidential communications if I am obliged to turn over its cryptographic systems and open up its files and procedures to the study and direction of this board's representatives and appointees who will undoubtedly be personnel of the very departments in which these leaks of information have occurred. I therefore recommend that you urge that if this proposed Executive Order is to be issued it contain a specific exemption of the FBI.

I am attaching the papers pertaining to this Executive Order, which were forwarded to me by Mr. Cox.

Attachments

cc-ASG Hugh B. Cox

Office Memorandum • UNITED STATES GOVERNMENT
EPC:AF

TO : THE DIRECTOR

DATE: May 19, 1945

FROM : E. A. TAMM

SUBJECT: PROPOSED EXECUTIVE ORDER ESTABLISHING BOARD TO COORDINATE
AND SUPERVISE CRYPTOGRAPHIC SYSTEMS AND PROCEDURES OF
FEDERAL DEPARTMENTS AND AGENCIES

Mr. Tolson	
Mr. E. A. Tamm	
Mr. Clegg	
Mr. Coffey	
Mr. Glavin	
Mr. Ladd	
Mr. Nichols	
Mr. Rosen	
Mr. Tracy	
Mr. Carson	
Mr. Egan	
Mr. Hendon	
Mr. Pennington	
Mr. Quinn Tamm	
Tele. Room	
Mr. Nease	
Miss Beahm	
Miss Gandy	

The Attorney General has received for his views a proposed Executive Order which sets up a super board consisting of the Secretaries of State, War, and the Navy, which will have absolute control over all cryptographic systems and procedures in the Federal agencies. It would appear under this Order that the FBI would be required to turn over to the board and its subcommittees all of our cryptographic and cipher systems and furthermore that the board would be empowered at will to send in to all Government agencies, including the FBI, its inspectors to study not only the cryptographic systems but what they call "related procedures", which include the routing of communications and the filing thereof, et cetera. There also appears to be a possibility that under the Order this super board would have power to include in its supervision cryptanalytical work.

This Order seems to be the outgrowth of the inspection made by the Joint Chiefs of Staff last year of cryptographic systems in the Federal agencies. It is a dictatorial maneuver which would seem to give almost unlimited powers to the Army and the Navy and the State Department to nose into everything that is going on of a confidential nature.

I have had prepared a strong protest to the Attorney General which is being submitted for your consideration and there are also attached copies of the proposed Executive Order and an accompanying memorandum for the President dated March 8, 1945, prepared by the Joint Chiefs of Staff, which undertakes to justify their recommendations.

There is also a cover memorandum furnishing Assistant Solicitor General Hugh B. Cox with a carbon copy of your memorandum to the Attorney General.

RECORDED

INDEXED
DEX

126

EX - 20

57 JUN 9 1945

80-612-104

NOT USED

Office Memorandum • UNITED STATES GOVERNMENT

DGB:SGH

TO : MR. COFFEY *JWC*

FROM : I. W. Conrad

SUBJECT: Weekly Radio Cryptanalysis Conference

DATE: May 15, 1945

Mr. Tolson _____

Mr. E. A. Tamm _____

Mr. Clegg _____

Mr. Coffey _____

Mr. Glavin _____

Mr. Ladd _____

Mr. Nichols _____

Mr. Rosen _____

Mr. Tracy _____

Mr. Carson _____

Mr. Hendon _____

Mr. Pennington _____

Mr. Quinn Tamm _____

Tele. Room _____

Mr. Nease _____

Miss Beahm _____

Miss Gandy _____

The regular weekly conference of the Radio, Cryptanalysis, SIS, and Espionage Sections was held May 11, 1945, attended by Messrs. Bardin, Davis, Downing, Millen, and Tyler. No conference was held for the week of May 2, 1945, and the above conference was regularly continued from May 9, 1945.

The various circuits upon which monitoring and cryptanalysis work is being performed were discussed.

Mr. Bardin announced that all German clandestine circuits of interest to the Bureau, except the double-agent cases operating out of Madrid, were now silent. He advised that all such circuits are being continued on their present monitoring priorities.

Mr. Tyler announced the following status of the Bureau double-agent cases:

- PAT J CASE - Bureau station continues to call on schedule but does not send traffic blind.
- RUCASE - Bureau station sends traffic blind
- PEASANT CASE - Bureau station sends traffic blind
- MOONSTONE CASE - Bureau station calling twice a day -- No contact as yet.
- BROMO CASE - The Germans have ordered that radio circuit closed.
- JAR CASE - Not yet in operation.
- SPANIP CASE - Two "Hello Jimmie" greeting messages received from Radio Tokyo. Radio contact being continued in the German circuit but no contact has been established with the Japanese in Madrid.

Coffey, pursuant to Mr. E. A. TAMM'S DESIRES,

Mr. Downing advised that Mr. ~~W. A. Tamm~~ suggests that the Crown Case be given a "A" priority, to which the conference agreed.

Mr. Davis stated that in view of developments, radio monitoring in the Lodge Case was being terminated at Montevideo but that it should be continued from Clinton.

RECORDED
&
INDEXED

57 JUN 7 1945
cc - Mr. Downing, 2252
Mr. Davis, 2252
Mr. Newby, 1649

EX-44

Memorandum for Mr. Coffey
Page Two

Following is the resume of the principal monitoring cases for May 1-11,
1945:

<u>CIRCUIT</u>	<u>INTERCEPTS</u>	<u>MESSAGES</u>	<u>DATE LAST HEARD (C)</u>	<u>DATE LAST HEARD(A)</u>
*AADA	2	7	5-9	4-19
CAB	1	0	5-1	4-20
DKS	1	0	5-2	-----
DOG	0	0	3-7	4-22
HDZ	0	0	3-15	-----
HEID	0	0	4-24	-----
LOD	0	0	4-26	4-19
MOA	0	0	4-19	-----
NAE	0	0	3-17	-----
NAS	0	0	4-12	-----
NUD	0	0	3-4	8-20
PAK	8	3	5-5	2-19
PBD	0	0	4-16	-----
RAP	0	0	4-19	-----
SCH	11	5	5-1	5-6
SPI	0	0	3-13	-----
TTE	0	0	3-24	-----
V9X	0	0	2-5	3-28
WTV	0	0	4-18	11-12

*Six of the messages contained in the two intercepts were German plain text and one message was in code. On one of the intercepts the call AADA was used and on the other intercept the call JXAA was used.

To date on circuit SMOLNY 28 intercepts have been received containing 85 messages.

Office Memorandum • UNITED STATES GOVERNMENT
EPC:AF

TO : MR. E. A. TAMM - 5734

DATE: May 29, 1945

FROM : E. P. COFFEY *EC* ✓SUBJECT: ~~X~~CRYPTOGRAPHIC SECURITY BOARD - UNDER EXECUTIVE ORDER

Mr. Tolson	✓
Mr. E. A. Tamm	✓
Mr. Clegg	
Mr. Coffey	
Mr. Glavin	
Mr. Ladd	
Mr. Nichols	
Mr. Rosen	
Mr. Tracy	
Mr. Mohr	
Mr. Carson	
Mr. Hendon	
Mr. Mumford	
Mr. Jones	
Mr. Quinn Tamm	
Tele. Room	
Mr. Nease	
Miss Beahm	
Miss Gandy	

Mr. Titus of the Bureau of the Budget called at my office, referring to a recently proposed Executive Order which would create a super-security cryptographic board consisting of the Secretaries of War, State, and the Navy. He stated he had a minor revision in the Executive Order and that he also wanted to informally determine whether Departmental consideration of the order had been completed. After talking with Mr. Ladd on the telephone I informed Titus it was our understanding that the matter was being handled by Mr. Hugh Cox in the Department.

RECORDED & INDEXED

215
EX-53180-612-106
H. E. H.
32 JUN 2 1945JUN 12 1945
167

RECORDED 80-612-112

EPC:AF

August 15, 1945

~~PERSONAL AND CONFIDENTIAL~~
~~BY SPECIAL MESSENGER~~

Major General Clayton Bissell
Assistant Chief of Staff, G-2
War Department
Washington, D. C.

Dear General:

I am in receipt of your letter of August 7, 1945, concerning a large quantity of unclassified cryptographic devices in the possession of the Army, which may become surplus property.

The Federal Bureau of Investigation has no views or comments to offer concerning the disposition of these cryptographic devices as surplus property.

Sincerely yours,

J. Edgar Hoover

John Edgar Hoover
Director

Mr. Tolson
Mr. E. A. Tamm
Mr. Clegg
Mr. Coffey
Mr. Glavin
Mr. Ladd
Mr. Nichols
Mr. Rosen
Mr. Tracy
Mr. Carson
Mr. Egan
Mr. Hendon
Mr. Pennington
Mr. Quinn Tamm
Mr. Nease
Miss Gandy

COMMUNICATIONS SECTION

MAILED 12

★ AUG 17 1945 P.M.

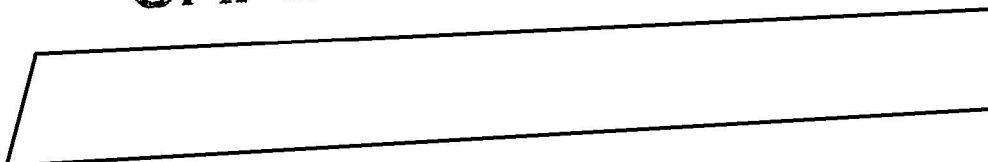
FEDERAL BUREAU OF INVESTIGATION
U. S. DEPARTMENT OF JUSTICE

52 SEP 14 1945

wh

80-612-113

CHANGE TO



b3
b7E

✓

Office Memorandum • UNITED STATES GOVERNMENT

DML:CSH

TO : THE DIRECTOR

DATE:

FROM : D. M. Ladd

August 29, 1945

SUBJECT: ~~CRYPTANALYTICAL~~ WORK OF THE GOVERNMENT

While talking with Fred Lyon of the State Department this morning on other matters, he exhibited to me an order from the White House, signed by President Truman, addressed to all Cabinet officers (a copy of which was designated for the Attorney General), dated August 28, 1945 and instructing that no information be given out by any governmental agency concerning the results of or progress in connection with any cryptanalytical work of the government, without the express approval of the President. I imagine the Attorney General will refer his copy to the Bureau.

Mr. Tolson
Mr. E. A. Tamm
Mr. Clegg
Mr. Glavin
Mr. Ladd
Mr. Nichols
Mr. Rosen
Mr. Tracy
Mr. Mohr
Mr. Carson
Mr. Hendon
Mr. Mumford
Mr. Jones
Mr. Quinn Tamm
Tele. Room
Mr. Nease
Miss Beahm
Miss Gandy

RECORDED
&
INDEXED

180-612-114
JUL 13
32 SEP 13 1945

EX-25

71
57 SEP 21 1945

FEDERAL BUREAU OF INVESTIGATION
U. S. DEPARTMENT OF JUSTICE

VPK:mr

To: COMMUNICATIONS SECTION.

September 10, 1945

80-612-115
Transmit the following message to:

ALL LEGAL ATTACHES WHOSE NAMES APPEAR ON
THE ATTACHED LIST

RECORDED
RADIOGRAM - CABLEGRAM - CIPHER PAD

U R G E N T

THE PRESIDENT HAS DIRECTED THAT STEPS BE TAKEN TO PREVENT RELEASE, EXCEPT WITH
HIS PERMISSION, OF CRYPTANALYTIC EFFORTS OR SPECIFIC RESULTS OBTAINED FROM
CRYPTANALYSIS BY ANY AGENCY OF THE U.S. GOVERNMENT. YOU ARE INSTRUCTED TO BE
MOST CAREFUL WITH BUREAU'S INFORMATION OBTAINED THROUGH CRYPTANALYSIS, TO
INSURE THAT THIS DIRECTIVE IS NOT VIOLATED. IN NO CASE SHOULD INFORMATION
FURNISHED BY YOU BE RELEASED TO LOCAL AUTHORITIES OR TO ANYONE ELSE.

SIS copies
detailed

Emerson
H 418-2 P1L
in RBA

RECEIVED
SEP 11 4 08 PM '45

SEP 11 4 08 PM '45

SEP 11 4 08 PM '45

SEP 11 4 08 PM '45

Mr. Tolson
Mr. E. A. Tamm
Mr. Clegg
Mr. Coffey
Mr. Glavin
Mr. Ladd
Mr. Nichols
Mr. Rosen
Mr. Tracy
Mr. Egan
Mr. Gurnea
Mr. Harbo
Mr. Hendon
Mr. Mumford
Mr. Quinn
Mr. Nease
Miss Gandy

SENT VIA

Radio & Cable 9/12/45 M

Per

met

52 OCT 8 1945

Office Memorandum • UNITED STATES GOVERNMENT

TO : MR. D. M. LADD

FROM : Mr. R. R. Roach

SUBJECT: CRYPTANALYTIC WORK

DATE: September 1, 1945

RRR:MGC

Mr. Tolson
Mr. E. A. Tamm
Mr. Clegg
Mr. Coffey
Mr. Glavin
Mr. Ladd
Mr. Nichols
Mr. Rosen
Mr. Tracy
Mr. Carson
Mr. Egan
Mr. Gurnea
Mr. Hendon
Mr. Pennington
Mr. Quinn Tamm
Tele. Room
Mr. Nease
Miss Beahm
Miss Gandy

On August 31, 1945, Colonel Gene Winters of OWI called and stated that OWI had received the following memorandum from President Truman concerning disclosure of information obtained through cryptanalytic work by United States Government agencies.

Colonel Winters stated that he had been requested to make the substance of the President's memorandum available to those agencies handling such work and who were not addressed directly in the memorandum. He stated that it was noted that the Attorney General had received a copy, but he felt that it would be sometime before the Bureau got it from the Attorney General and, therefore, desired to pass it on direct.

The memorandum is quoted as follows:

RESTRICTED

From the White House dated August 28, 1945:

Memorandum for the Secretary of State

War
Navy
Attorney General
Joint Chiefs of Staff
Director of the Budget
Office of War Information

Appropriate departments of the Government and the Joint Chiefs of Staff are hereby directed to take such steps as are necessary to prevent release to the public, except with the specific approval of the President in each case, of information regarding the past or present status, technique or procedures, degree of success attained, or any specific results of any cryptanalytic unit acting under the authority of the United States Government or any department thereof.

/S/ Harry S. Truman

RECORDED

RESTRICTED

SEP 13 1945

EX - 66

Handwritten:
Rosenberg to all
Legats in Embassy
& Consulates
9/13/45
W.P.K.

WASHINGTON TIMES-HERALD 10/31/45

Handwritten signature and initials

Photostated and Replaced:

**U. S. Embassy Papers Stolen
In Berlin Before War by Spies**

WIESBADEN, Germany, Oct. 30 (UP)—German spies planted in the American embassy in Berlin stole highly secret documents from under the very noses of United States diplomats before the war, Maj. Johannes Gaenzer of German counter-intelligence said today.

The documents were lifted, photostated and replaced unobserved while the diplomats lingered at luncheon, Gaenzer told American 3d army intelligence agents.

Gaenzer told the Americans

that months before the war German intelligence agents were infiltrated into all the Allied embassies as domestic help and the like. They stole everything they could get their hands on.

A quick job of photostating was the most efficient means of preserving the information they garnered. This he indicated was done right at the embassy. Often valuable official reports were obtained from the markings on discarded carbon paper retrieved from waste baskets, he said.

Handwritten word: "Photostating"

100-100-4
NOV 26 1945

RECEIVED
89

Handwritten: "Fill" and "FX-45"

80-612

50 DEC 6 1945

Handwritten: "148"

7

IWN:MS

Mr. Tolson _____
 Mr. E. A. Tamm _____
 Mr. Clegg _____
 Mr. Coffey _____
 Mr. Glavin _____
 Mr. Ladd V _____
 Mr. Nichols _____
 Mr. Rosen _____
 Mr. Tracy _____
 Mr. Carson _____
 Mr. Egan _____
 Mr. Hendon _____
 Mr. Pennington _____
 Mr. Quinn Tamm _____
 Mr. Nease _____
 Miss Gandy _____

December 13, 1945

MEMORANDUM FOR MR. HARBO
 ROOM 7643

RE: PROCURING SIGNAL CORPS PAPER
 "STATISTICAL METHODS IN CRYPTANALYSIS"

Several years ago Dr. S. Kullback, an Army Signal Corps Cryptanalyst, wrote a paper entitled "Statistical Methods in Cryptanalysis". A copy of this paper as well as any additional similar material which the Signal Corps might wish to make available would be of considerable aid to the Bureau's Cryptanalysis Section.

RECOMMENDATION:

That the Bureau Liaison representative attempt to procure from the Army Signal Corps a copy of the above noted paper and any available similar type material.

Respectfully,

C. F. Downing

RECORDED
 &
 INDEXED

EX-8

APR 1

THIS MEMORANDUM IS FOR ADMINISTRATIVE PURPOSES
 TO BE DESTROYED AFTER ACTION IS TAKEN AND NOT SENT TO FILES

OFFICE OF DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

TO

OFFICIAL INDICATED BELOW BY CHECK MARK

Mr. Tolson _____ ()
 Mr. E. A. Tamm _____ ()
 Mr. Clegg _____ ()
 Mr. Glavin _____ ()
 Mr. Ladd _____ ()
 Mr. Nichols _____ ()
 Mr. Rosen _____ ()
 Mr. Tracy _____ ()
 Mr. Carson _____ ()
 Mr. Gurnea _____ ()
 Mr. Harbo _____ ()
 Mr. Hendon _____ ()
 Mr. Quinn Tamm _____ ()
 Mr. Nease _____ ()
 Miss Gandy _____ ()
 _____ ()

What is this
all about?

See Me _____ ()
 Note and Return _____ ()
 For Your Recommendation _____ ()
 What are the facts? _____ ()

Remarks:

ALL INFORMATION CONTAINED
 HEREIN IS UNCLASSIFIED
 DATE 3-19-90 BY SP8BJL/g
 286,521

20-612-119

The Attorney General

February 13, 1946

John Edgar Hoover, Director, Federal Bureau of Investigation

RECORDED

80-612-119

I am in receipt of your memorandum dated February 11, 1946, transmitting a copy of a letter from Secretary of State Byrnes dated February 1, 1946, requesting the Department of Justice to designate a representative familiar with cryptographic problems to work with personnel designated by the Coordinating Committee of the Cryptographic Security Board.

In view of the fact that the Executive Order contains a clause to the effect that it shall not apply to the Federal Bureau of Investigation, I do not believe it would be in order to have an employee of this Bureau designated as a representative for the Department. You may, however, wish to designate someone from the Department itself and I defer to your judgment in that regard.

The original of Mr. Byrnes' letter, together with a copy of the Executive Order, is returned herewith.

Enclosure

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 3-19-90 BY 2885/BJ/ab
286,521

Mr. Tolson
Mr. E. A. Tamm
Mr. Clegg
Mr. Coffey
Mr. Glavin
Mr. Ladd
Mr. Nichols
Mr. Rosen
Mr. Tracy
Mr. Carson
Mr. Egan
Mr. Gurnea
Mr. Hendon
Mr. Pennington
Mr. Quinn Tamm
Mr. Nease
Miss Gandy

50 FEB 20 1946

6:46 pm

2-13-46

see held

Office Memorandum • UNITED STATES GOVERNMENT

TO : MR. EDW. A. TAMM

DATE: 2/15/46

FROM : Mr. D. M. Ladd

Call: 10:59 A.M.

SUBJECT:

Mr. Tolson	
Mr. E. A. Tamm	
Mr. Clegg	
Mr. Coffey	
Mr. Glavin	
Mr. Ladd	
Mr. Nichols	
Mr. Rosen	
Mr. Tracy	
Mr. Carson	
Mr. Egan	
Mr. Gurnea	
Mr. Hendon	
Mr. Pennington	
Mr. Quinn Tamm	
Tele. Room	
Mr. Nease	
Miss Beahm	
Miss Gandy	

A call from Mr. Don Cook of the Department of Justice was referred to me by the Director's Office at the above time. He advised that early in February the Secretary of State sent a letter to the Department in which he requested the Attorney General to designate a representative to serve on the Cryptographic Security Board. He said there is a provision in the executive order which states that the provisions of this order shall not apply to the Federal Bureau of Investigation. When the above-mentioned letter arrived, Mr. Cook stated he sent this to the Bureau thinking that the Bureau might have some suggestions to make on it. He advised that a memorandum came back to the Department from the Director in which the Director points to this provision in the order and concludes that it would not be in order to have an employee designated as a representative.

Mr. Cook said the Attorney General has asked him whether the Department should have any representative at all and Mr. Cook stated he would need help to decide. He thought the Bureau would have some ideas in this regard and would be able to aid in this decision. He asked whether I felt it would be desirable for the Department to have such a representative. I advised him that the question arising is one that came up about a year ago when the Army and the Navy came over and make a survey of the Department of Justice as well as of the Bureau in order to see how the cryptographic messages were being handled to see whether there was sufficient security attached to them to permit the Department of Justice to receive any information developed through that method which might be of interest to it. For future protection in the event something of this kind arises in case they want to furnish the Department copies of any decoded material possibly of interest to the Department, it might be well, I thought, to have someone designated at least as an observer to sit on the committee and to look out for the Department's interests and prevent their coming over to survey the Department every so often.

He stated the function of this board, as outlined in the letter, is to study the systems, to establish standards and to promulgate various directives to implement the standards and policies. They ask for a man who is familiar with cryptographic problems to work with the personnel designated by this co-ordinating committee. In view of the fact that they have asked for someone who is familiar with those problems and since Mr. Cook knows no one in the Department outside of the Bureau who is familiar with these problems, Mr. Cook wondered whether we are being invited to provide merely an observer or whether we are being invited to provide a technical man.

58 MAR 28 1946

and in which case our suggestion to have an observer might not be appropriate. I stated this is apparently being sent to all Government departments not knowing who might be doing cryptographic work although they probably are not sure whether any is done. They probably do not know whether it is necessary to have special codes in Department communications with its U. S. Attorneys, Judges, et cetera. I stated that if this is going to deal solely with technical problems the Department might not have any interest in it. I advised Mr. Cook that the Bureau is in touch with them in handling decodes, and so forth, and if there were any technical problems with this, the Department would most likely contact the Bureau. Mr. Cook said he certainly thought they would do this.

Mr. Cook said he felt the only reason it would be desirable to have any connection with this Board, even though the provisions of the order did not apply to the Bureau, if the Department had a representative it might be helpful in various ways to the Bureau. However, he stated his feeling has been if the Bureau did not want any part of it there was perhaps little or no reason for having a representative. I told him I thought this was right and since we were specifically excluded, I did not think the Bureau should be in on it. I further stated that this opinion was in line with our desires and that we have previously communicated with the Attorney General in this connection. From both a technical standpoint and standpoint of receiving material of interest the Bureau is in touch with the Army and Navy Code Sections, Mr. Cook was advised.

He wanted my reaction to a reply stating the only technical people in this field are in the Federal Bureau of Investigation with reference to their request for a technical person, and pointing out that the provisions of the executive order itself do not apply to the Bureau and, therefore, it is deemed undesirable to have a representative of the Bureau on this committee. In view of that fact, while the Department would be perfectly willing to designate an individual to be an observer, it would have to be understood that this person would not himself be in a position to render technical assistance. I stated I thought this would be a very good answer.

DML:dmg

Office Memorandum • UNITED STATES GOVERNMENT

TO : The Director

DATE: 2/13/46

FROM : D. M. Ladd

SUBJECT:

Mr. Tolson	✓
Mr. E. A. Tamm	
Mr. Clegg	
Mr. Coffey	
Mr. Glavin	
Mr. Ladd	
Mr. Nichols	
Mr. Rosen	
Mr. Tracy	
Mr. Carson	
Mr. Egan	
Mr. Gurnea	
Mr. Hendon	
Mr. Pennington	
Mr. Quinn Tamm	
Tele. Room	
Mr. Nease	
Miss Beahm	
Miss Gandy	

Reference is made to the attached letter from Secretary of State Byrnes to the Attorney General dated February 1, 1946, requesting the Attorney General to designate a representative of the Department of Justice familiar with cryptographic problems to work with personnel designated by the Cryptographic Coordinating Committee to accomplish a survey of cryptographic systems and related procedures in line with the Executive Order of the President issued on July 3, 1945.

Secretary Byrnes specifically points out that paragraph 5 of the Executive Order states, "The provisions of this order shall not apply to the Federal Bureau of Investigation of the Department of Justice." Mr. Byrnes' letter was checked to you by Don Cook with a notation, "For your recommendation as to a representative."

BACKGROUND

You will recall that prior to the issuance of the Executive Order of July 3, 1945, which sets up a super-board consisting of the Secretaries of State, War and Navy to control cryptographic systems and procedures in the Federal agencies, a copy was submitted to the Attorney General, who sent it to us for our views. On May 19, 1945, a memorandum was sent to the Attorney General pointing out that the Executive Order should not embrace the FBI and that the Bureau should be specifically excluded in the order if the President decides to issue it as regards other Government agencies. It is noted from the Executive Order actually issued on July 3, 1945, that paragraph 5 states specifically, "The provisions of this order shall not apply to the Federal Bureau of Investigation of the Department of Justice."

ACTION

There is attached a memorandum to the Attorney General advising him that since the FBI is specifically excluded in this Executive Order we are not in a position to recommend a representative to work with this committee.

Attachment

RGF:ECR

59 MAR 14 1946

RECORDED
&
INDEXED

EX-38

80-612-121

Office Memorandum • UNITED STATES GOVERNMENT

TO : MR. D. M. LADD *DL*

DATE: 3/8/46

FROM : Mr. E. G. Fitch *E. G. Fitch*

SNR:MCC

SUBJECT:

Reference is made to a pink memorandum from Mr. C. F. Downing to Mr. Harbo entitled "Procuring Signal Corps Paper 'Statistical Methods in Cryptanalysis'"

Mr. Reynolds discussed this matter with General Clarke upon his return from sick leave. General Clarke indicated that he would be delighted to make this information available to the Bureau and he would have Arlington Hall procure the material and make it available.

This matter will be followed with General Clarke, and you will be advised as to all results obtained.

RECORDED
&
INDEXED

EX-2

188-612-122
7 MAR 1946

33.7

Office Memorandum • UNITED STATES GOVERNMENT

TO : MR. HARBO - 7641 *RH*

FROM : C. F. DOWNING *CD*

SUBJECT: CRYPTOGRAPHIC DEVICES

DATE: April 2, 1946

Bureau File 80-612

CC: 80-682

Mr. Tolson	
Mr. E. A. Tamm	
Mr. Clegg	
Mr. Coffey	
Mr. Glavin	
Mr. Ladd	
Mr. Nichols	
Mr. Rosen	
Mr. Tracy	
Mr. Carson	
Mr. Egan	
Mr. Gurnea	
Mr. Hendon	
Mr. Pennington	
Mr. Quinn Tamm	
Tele. Room	
Mr. Nease	
Miss Gandy	

By a memorandum dated March 8 from Mr. E. G. Fitch to Mr. D. M. Ladd the information was set forth that General Clarke would try to have Army cryptographic devices made available to us.

For the aid of the Liaison Section we wish to reiterate the specific nature of the material we desire. For research and reference purposes, we would like to get one working sample of each different type of mechanical cipher device which the Army may wish to make available to us, whether obsolete or not. The only exception is the M-209 with which we are already familiar.

IWN:JCW

RECORDED

80-612-123

EX-14

APR 2 1946

*CD**Dec*

1-1

memo to Ladd

4-30-46

SWR:VPS

56 MAY 16 1946

RECORDED COPY FILED TO 80-612-123

Office Memorandum • UNITED STATES GOVERNMENT

TO : Mr. D. M. Ladd *DL*
 FROM : E. G. Fitch *EF*
 SUBJECT: CRYPTOGRAPHIC DEVICES

DATE: April 30, 1946

Mr. Tolson _____
 Mr. E. A. Tamm _____
 Mr. Clegg _____
 Mr. Coffey _____
 Mr. Glavin _____
 Mr. Ladd _____
 Mr. Nichols _____
 Mr. Rosen _____
 Mr. Tracy _____
 Mr. Mohr _____
 Mr. Carson _____
 Mr. Hendon _____
 Mr. Mumford _____
 Mr. Jones _____
 Mr. Quinn Tamm _____
 Tele. Room _____
 Mr. Nease _____
 Miss Beahm _____
 Miss Gandy _____

NEUPH
 Reference is made to the memorandum to Mr. Harbo from Mr. C. F. Downing in the above-captioned matter dated April 2, 1946. It indicates that for research and reference purposes, the Laboratory would like to obtain one working sample of each different type of mechanical cipher device which the Army may wish to make available to the FBI, whether obsolete or not. It points out that the only exception is the M-209 with which the Bureau is already familiar.

Considerable discussion has been had in the past by Special Agent S. W. Reynolds of the Liaison Section with Colonel C. W. Clarke of the Military Intelligence Service. Colonel Clarke has indicated a willingness to have all material developed at Arlington Hall made available to the Bureau. As you will recall, Colonel Clarke has brought to the attention of the Bureau that he desires the Bureau to participate in the obtaining of intercepts and decodes. He specifically mentioned that he would like to have the Bureau take over the world-wide clandestine field. As you will also recall, Colonel Clarke has indicated in this connection that he would be willing to make his technicians available to the Bureau to train and assist in setting up the necessary machinery to handle this assignment.

In view of the uncertainty as to whether or not the Bureau will participate in world-wide intelligence, it does not appear wise to request Colonel Clarke at this time to make available to the Bureau one working sample of each different type of mechanical cipher device, and it is suggested that this matter be held in abeyance until it is ascertained just what will be the Bureau's participation in world-wide intelligence.

SWR:VPS
 80-612
 80-682

RECORDED
 INDEXED

112-124

EX-63

70 MAY 21 1946

Office Memorandum • UNITED STATES GOVERNMENT

TO : MR. D. M. LADD

DATE: 3/18/46

FROM : Mr. E. G. Fitch

SUBJECT:

Mr. Tolson	_____
Mr. E. A. Tamm	_____
Mr. Clegg	_____
Mr. Coffey	_____
Mr. Glavin	_____
Mr. Ladd	_____
Mr. Nichols	_____
Mr. Rosen	_____
Mr. Tracy	_____
Mr. Carson	_____
Mr. Egan	_____
Mr. Gurnea	_____
Mr. Hendon	_____
Mr. Pennington	_____
Mr. Quinn Tamm	_____
Tele. Room	_____
Mr. Nease	_____
Miss Beahm	_____
Miss Gandy	_____

Reference is made to my memorandum to you dated March 8, 1946, which referred to a pink memorandum from Mr. C. F. Downing to Mr. Harbo entitled "Procuring Signal Corps Paper 'Statistical Methods in Cryptanalysis'". The referenced memorandum indicated that Special Agent Reynolds had discussed this matter with General Clarke who indicated that he would be delighted to make any information available on cryptanalytic methods available to the Bureau.

There is attached hereto a copy of a list of 23 publications, which consists of all publications available at Arlington Hall regarding cryptanalytic methods. It is noted that "Statistical Methods in Cryptanalysis" and the revised edition of this publication are contained in this list. There is also attached hereto one copy of each of the publications which was made available to Mr. Reynolds for the Bureau by General Clarke. General Clarke advised Reynolds that the Bureau could have these publications on a permanent loan basis.

RECOMMENDATION:

RECORDED

It is recommended that this be forwarded to the Technical Laboratory for its information.

Attachments

SWR:ems

53 MAY 15 1946

Enclosures Attached
Publications retained
in Crypt section
Library 5/9/46
1 wmv.

40

~~SECRET~~

Received the following publications:

- ✓ STUDIES IN GERMAN DIPLOMATIC CODES EMPLOYED
DURING THE WORLD WAR (~~Confidential~~) Register No. 3 1 copy
- ✓ THE PRINCIPLES OF INDIRECT SYMMETRY OF POSITION
IN SECONDARY ALPHABETS AND THEIR APPLICATION IN
THE SOLUTION OF POLYALPHABETIC SUBSTITUTION
CIPHERS (~~Confidential~~) Register No. 5 1 copy
- ✓ GERMAN MILITARY CIPHERS FROM FEBRUARY TO
NOVEMBER 1918 (~~Confidential~~) Register No. 6 1 copy
- ✓ PRINCIPLES OF SOLUTION OF CRYPTOGRAMS PRODUCED
BY THE I. T. & T. CIPHER MACHINE (~~Confidential~~)
Register No. 7 1 copy
- ✓ GENERAL SOLUTION FOR THE DOUBLE TRANSPOSITION
CIPHER (~~SECRET~~) Register No. 7 1 copy
- ✓ GENERAL SOLUTION FOR THE ADFGVX CIPHER SYSTEM
(~~Confidential~~) Register No. 8 1 copy
- ✓ AN ENCIPHERMENT OF THE GERMAN DIPLOMATIC
CODE 7500 (~~Confidential~~) Register No. 9 1 copy
- ✓ PRINCIPLES OF SOLUTION OF MILITARY FIELD CODES
USED BY THE GERMAN ARMY IN 1917 (~~Confidential~~)
Register No. 10 1 copy
- ✓ FURTHER APPLICATIONS OF THE PRINCIPLES OF INDIRECT
SYMMETRY OF POSITION IN SECONDARY ALPHABETS
(~~Confidential~~) Register No. 11 1 copy
- ✓ REPORT OF CODE COMPILATION SECTION GENERAL HEADQUAR-
TERS AMERICAN EXPEDITIONARY FORCES DEC 1917-Nov 1918
(~~Confidential~~) Register No. 11 1 copy
- ✓ PERMUTATION TABLES INVOLVING A FEATURE OF NON-
TRANSPOSABILITY (~~Restricted~~) Register No. 16 1 copy
- ✓ STATISTICAL METHODS IN CRYPTANALYSIS (~~Confidential~~)
Register No. 16 1 copy
- ✓ STATISTICAL METHODS IN CRYPTANALYSIS (~~Confidential~~)
Register No. 206 (REVISED EDITION) 1 copy

~~SECRET~~

~~SECRET~~

- ✓ FINAL REPORT OF THE RADIO INTELLIGENCE SECTION,
GENERAL STAFF GHQ AMERICAN EXPEDITIONARY FORCES
(~~Confidential~~) Register No. 28 1 copy
- ✓ NOTES ON THE LIAISON SERVICE AND THE LIAISON INTELLIGENCE SERVICE OF THE GERMAN ARMY DURING THE WORLD WAR (~~Confidential~~) Register No. 28 1 copy
- ✓ ANALYSIS OF THE HAGELIN CRYPTOGRAPH TYPE B-211
(~~Confidential~~) No. 69 1 copy
- ✓ THE EXISTENCE OF ALPHABETS HAVING NO INTERVAL REPETITIONS (~~Restricted~~) Register No. 80 1 copy
- ✓ THE ZIMMERMANN TELEGRAPH OF JANUARY 16, 1917 AND ITS CRYPTOGRAPHIC BACKGROUND (~~Confidential~~) Register No. 155 1 copy
- ✓ ANALYSIS OF A MECHANICO-ELECTRICAL CRYPTOGRAPH PART I (~~Secret~~) Register No. 201 1 copy
- ✓ THE INDEX OF COINCIDENCE AND ITS APPLICATIONS IN CRYPTANALYSIS (~~Confidential~~) Register No. 214 1 copy
- ✓ FIELD CODES USED BY THE GERMAN ARMY DURING THE WORLD WAR (~~Confidential~~) Register No. 217 1 copy
- ✓ ANALYSIS OF A MECHANICO-ELECTRICAL CRYPTOGRAPH PART II (~~Secret~~) Register No. 219 1 copy
- ✓ Navy Dept Pamphlet No. 25 TREATISE ON CRYPTOGRAPHY (~~Restricted~~) Register No. 979 1 copy

Date _____

Name _____

Rank _____

~~SECRET~~

Office Memorandum • UNITED STATES GOVERNMENT

TO : MR. D. M. LADD

DATE: March 8, 1946

FROM : Mr. E. G. Fitch

SUBJECT:

Mr. Tolson	_____
Mr. E. A. Tamm	_____
Mr. Clegg	_____
Mr. Coffey	_____
Mr. Glavin	_____
Mr. Ladd	_____
Mr. Nichols	_____
Mr. Rosen	_____
Mr. Tracy	_____
Mr. Mohr	_____
Mr. Carson	_____
Mr. Hendon	_____
Mr. Mumford	_____
Mr. Jones	_____
Mr. Quinn Tamm	_____
Tele. Room	_____
Mr. Nease	_____
Miss Beahm	_____
Miss Gandy	_____

Reference is made to a letter received from General P. E. Peabody dated February 6, 1946, which referred to a Bureau letter of January 23, 1946. The reference communication indicated that the Syko is a British cipher device over which the Military Intelligence Service has no authority. Also that M-94 cipher devices are obsolete, but if same are available there is no objection to Bureau using same, and further that M-209 cryptographic devices will be made available to the Bureau in quantities if the Bureau desires.

Mr. Newpher advised Mr. Reynolds that General Peabody apparently misinterpreted the Bureau's request and that the Bureau was merely interested in the devices mentioned for research purposes, and has no intention of using this material for the sending of messages.

This fact was made known to General Clarke who stated he appreciated the Bureau's point of view, and he would see to it that whatever devices the Bureau desires will be, if possible, made available.

RECOMMENDATION:

It is recommended this be forwarded to the Technical Laboratory for their information.

ADDENDUM: SWR:ems March 18, 1946

General Clarke advised Mr. Reynolds that the M-209 cryptographic devices could be obtained by the Bureau from the War Assets Corporation, Surplus Property Declaration Number 11-019-SC-2731C, dated November 7, 1945.

RECORDED
&
INDEXED
EX-17 9

52 JUN 5 1946

186-612 126

7C-D

Office Memorandum • UNITED STATES GOVERNMENT

TO : R. T. HARBO *RTB*

DATE: 11-1-46

FROM : H. B. LONG

SUBJECT: Small peice of paper bearing typewritting found by Mrs. Carl
Baughman, Salina, Kansas
Bureau file 80-612
copying of file in my

Mr. Tolson	_____
Mr. E. A. Tamm	_____
Mr. Clegg	_____
Mr. Glavin	_____
Mr. Ladd	_____
Mr. Nichols	_____
Mr. Rosen	_____
Mr. Tracy	_____
Mr. Carson	_____
Mr. Egan	_____
Mr. Gurnea	_____
Mr. Harbo	_____
Mr. Hendon	_____
Mr. Pennington	_____
Mr. Quinn Tamm	_____
Tele. Room	_____
Mr. Nease	_____
Miss Beahm	_____
Miss Gandy	_____

There is attached the file which has been maintained in the Laboratory in connection with the above captioned matter. It is desired that this file be maintained as an enclosure behind the main file in the Records Section.

Attachment

18-612-127
NOT RECORDED
 31 NOV 4 1946

ENCLOSURE BEHIND FILE

54 NOV 6 1946

87

RTB

Office Memorandum • UNITED STATES GOVERNMENT

TO : MR. HARBO, Room 7639 *RL*

FROM : C. F. DOWNING *CFD*

SUBJECT: *1* CIPHER MACHINES AND MACHINES
USED IN CRYPTANALYSIS

DATE: January 23, 1947

Mr. Tolson	_____
Mr. E. A. Tamm	_____
Mr. Clegg	_____
Mr. Coffey	_____
Mr. Glavin	_____
Mr. Ladd	_____
Mr. Nichols	_____
Mr. Rosen	_____
Mr. Tracy	_____
Mr. Carson	_____
Mr. Egan	_____
Mr. Gurnea	_____
Mr. Hendon	_____
Mr. Pennington	_____
Mr. Quinn Tamm	_____
Tele. Room	_____
Mr. Nease	_____
Miss Beahm	_____
Miss Gandy	_____

Attached is a description of confidential information concerning certain foreign cipher machines and the use of calculating type machines in cryptanalysis work.

Attachment

cc - 80-731 80-728

62-26872

IWN:EB
80-612

EB

IN

RECORDED COPY FILED IN

55 FEB 19 1947 *45*173
100-28b3
b7E

CIPHER MACHINES AND MACHINES
USED IN CRYPTANALYSIS

There follows a brief description of three different cipher machines used by the German, Japanese and British Governments.

In addition to the regular Enigma type machines and the Hagelin machine the German Government also made use of a very complex "On line" equipment for enciphering and transmitting confidential information. According to the information we have thus far obtained this particular German machine was very similar in operation to the "Sig-oba" apparatus developed by Arlington Hall. It appears to have been referred to by Arlington Hall as the "Green" machine and they had the highest respect for the security it afforded in encipherment. As a matter of fact Arlington Hall looked upon this German machine and their own "Sig-oba" as the two best cipher machines known. Furthermore, Arlington Hall apparently was never able to decrypt any traffic enciphered by the use of the German machine. In appearance this machine looks very much like the "Sig-oba" and is believed to be an electrical rotor device of the basic Enigma principle. The Army was fortunate in being able to recover one of these German machines intact sometime soon after the Belgian Bulge.

The latest Japanese type of machine, referred to by Arlington Hall as the "Blue" machine, was recovered intact by the United States Army in the campaign of the Philippine Islands. This apparatus was set up by the Japanese on a special cable laid on the floor of the ocean between Manila and Canton, China during the late stages of the Japanese control of the Philippines. The apparatus apparently looked very much like a large teletype machine and made use of a set of ^(electrical?) rotors, mechanically operated, on the basic Enigma principles. Three rows of rotors were used with about ten rotors on each row. The rotors are believed to contain ten electrical contacts rather than the conventional twenty-six and were numerically described. It would thus appear that the keyboard was set up on a numerical substitution basis; however, this is pure conjecture. The entire machine was supposed to have been a very close imitation of German principles. The machine was not used to any extent by the Japanese prior to its being seized.

The British Government used a large teletype type machine called the "Type-X". It was extremely cumbersome and according to our source not too practical. The encipherment was based on (mechanical?) rotors electrically driven. These rotors, as in many Enigma cases, were rotated irregularly but in a constant direction. The apparatus was slow and difficult to operate. It was used for British-American liaison and also for British Headquarters traffic.

20-612-128

The use of accounting and tabulating type machines has been for some time an integral part of the functioning of the Arlington Hall Cryptanalysis Unit. Navy cryptanalysis efforts have also been supplemented to considerable extent by the use of machines for performing clerical and statistical types of work. The machines in Arlington Hall are of two general types, one group manufactured by International Business Machines (IBM) and the second classified as "Rapid Analytical Machines" designed and made at Arlington Hall. A large portion of two buildings are used to house the machine work. Every type of IBM machine is used which is applicable to statistical work in cryptanalysis including card punch machines, collators, sorters, alphabetical accounting machines, and so forth. Many of the standard IBM machines have been torn down and rebuilt for specialized performance. The design and building of such specialized machines is carried out by a group of former IBM engineers now employed by Arlington Hall for that particular purpose.

Although our information on this particular matter is somewhat vague it appears that Arlington Hall uses alphabetical accounting machines for printing purposes, these connected in series with huge banks of relays set up for comparison purposes. By this means it is possible to collate unenciphered code groups with the actual plain text values, the technique of stripping off additives in an encipherment process having previously been performed by the use of counters in the alphabetical accounting machine.

See memorandum from Downing to Harbo dated January 10, 1947 re "United States Codes" for description of the "Sig-oba" machine mentioned above.

R39
30 APR 24 1947

RECORDED | 80-115-129
E432 FBI
76 APR 10 1947

ORIGINAL COPY FILED IN

Office Memorandum • UNITED STATES GOVERNMENT

TO : C. F. DOWNING

DATE: March 22, 1947

FROM : J. M. HART

SUBJECT: SUPPLEMENT TO SEMI-ANNUAL READING REPORT DATED MARCH 15, 1947

Mr. Tolson	
Mr. E. A. Tamm	
Mr. Clegg	
Mr. Glavin	
Mr. Ladd	
Mr. Nichols	
Mr. Rosen	
Mr. Tracy	
Mr. Carson	
Mr. Egan	
Mr. Gurnea	
Mr. Harbo	
Mr. Hendon	
Mr. Pennington	
Mr. Quinn Tamm	
Tele. Room	
Mr. Nease	
Miss Gandy	

While on "Military Leave", I studied the following Cryptanalysis courses: (MOST OF THESE WERE SEPARATE COURSES IN WHICH WE DID READING)

I. Reviewed Military Cryptanalysis I, II, III, IV.

II. Military Cryptanalysis IV B & C by W. F. Friedman.

- a. General & Special Solutions of Double Transposition.
- b. " " " " of Transposition-Substitution.
- c. " " " " of "ADFGVX" Ciphers.
- d. " " " " of Fractionating Systems.
- e. Elementary Machine-Run Analysis for a Mechanico-Electrical cipher.

III. U. S. Army Converter M-209.

- a. General Solutions.
- b. Advanced Problems.
- c. Reconstruction of Internal Settings.

IV. Security Analysis of U. S. Army Systems.

V. Machine-Run Analysis.

"Analysis of the Mechanico-Electrical Cryptograph" parts I & II.
 "The Index of Coincidence and its Applications in Cryptanalysis"

VI. Traffic Analysis.

The analysis of Japanese and German "Unread Traffic" in order to determine identity, size, location, movement and overall strategy of enemy units.

VII. Enciphered Code Analysis. (Japanese)

- a. Analysis of Messages in Depth.
- b. Reconstruction of Enciphering Tables.
- c. Conversion Square Reconstruction.
- d. Analysis of Japanese "Mail Line" Systems. { MOST SECURED TRC. HIGHEST FORMER SYSTEMS

VIII. U.S. Navy Weather Analysis.

- a. Study of U. S. Weather Bureau Forecasting.
- b. International and Japanese Synoptic Forms and Procedure.
- c. Japanese Weather Codes and Cipher Systems.
- d. Analysis of Enciphered Synoptics.
- e. Use of Security Violations, Isolation and Forecasting.

SAC, NEW YORK

MARCH 21, 1947

DIRECTOR, FBI

HAGELIN CRYPTOGRAPHIC DEVICES

Prior to the war, Mr. Stewart Haddon was the New York representative of the Hagelin Company, located in the offices of Fuller Rodney and Company, 14 Wall Street, New York City. Haddon subsequently retired and the Bureau's file reflects that the firm of Merrill, Lynch, Pierce, Fenner and Beane of 70 Pine Street, New York City, took over the closing out of the Hagelin Company's interests in New York City, it being noted that the Hagelin Company is of Swedish origin.

It is desired that the firm of Merrill, Lynch, Pierce, Fenner and Beane be contacted by your office to ascertain whether this Company still represents the Hagelin Company's interests in the United States, and, if not, whether they are in a position to advise as to who the present Hagelin representative is. The Bureau is interested in ascertaining, if possible, whether the Hagelin Company is currently producing or contemplates producing an automatic encoding device operated by a keyboard, such as the keyboard on the ordinary typewriter.

It is desired that this matter be given expeditious attention and your reply be directed to the Bureau for the attention of the Laboratory.

RECORDED
& 34
INDEXED

180-612-130
F B I
68 MAR 22 1947

EX-28

COMMUNICATIONS SECTION
INC: PJB

MAILED 4

★ MAR 21 1947

FEDERAL BUREAU OF INVESTIGATION

U. S. DEPARTMENT OF JUSTICE

Mr. Tolson
Mr. E. A. Tamm
Mr. Clegg
Mr. Glavin
Mr. Ladd
Mr. Nichols
Mr. Rosen
Mr. Tracy
Mr. Carson
Mr. Egan
Mr. Gurnea
Mr. Harbo
Mr. Hendon
Mr. Pennington
Mr. Quinn Tamm
Tele. Room
Mr. Nease
Miss Gandy

62 APR 2 1947

Office Memorandum • UNITED STATES GOVERNMENT

TO : Director, FBI Attention: FBI Laboratory

FROM : SAC, New York

SUBJECT: HAGELIN CRYPTOGRAPHIC DEVICES

DATE: March 25, 1947

cryptograph

Reference is made to Bureau letter, dated March 21, 1947, regarding the above entitled matter.

Mr. EDWARD M. BACON of the firm of MERRILL, LYNCH, PIERCE, FENNER & BEANE, 70 Pine Street, New York City, advised today that his firm presently handles the financial matters of BORIS HAGELIN in the United States but that they had no information at the present time as to Mr. HAGELIN's activities in the field of cryptographic devices.

He stated that Mr. STEWART HEDDEN, a retired lawyer now living in New Milford, Connecticut, also carried on his financial dealings through the firm of MERRILL, LYNCH, PIERCE, FENNER & BEANE and formerly represented Mr. HAGELIN's interests in this country. He stated that Mr. HEDDEN is still in close touch with Mr. HAGELIN and would be in a better position to give any advice concerning HAGELIN's activities than anyone he could mention. Mr. BACON also advised that HAGELIN is coming to the United States sometime in April, at which time he will come in to see Mr. BACON or some other member of the firm concerning his financial interests in this country. He also believed that Mr. HEDDEN would know of the exact date of Mr. HAGELIN's arrival in the United States.

New York, N.Y.

For the information of the New Haven Field Division, reference Bureau letter advised that prior to the war, Mr. STEWART HEDDEN was the New York representative of the HAGELIN COMPANY, and that when HEDDEN subsequently retired, the firm of MERRILL, LYNCH, PIERCE, FENNER & BEANE took over the closing out of HAGELIN interests in New York City, it being noted that the HAGELIN COMPANY is of Swedish origin. The Bureau requested the New York Field Division to inquire of the above-mentioned firm whether or not that firm still represents the HAGELIN interests in order that we might ascertain whether or not the HAGELIN COMPANY is currently, or contemplates producing an automatic encoding device operated by a key-board, such as the keyboard on the ordinary typewriter. The Bureau requested that this matter be given expeditious attention and that the reply be directed to the Bureau for the attention of the Laboratory.

EX-20 57

RECORDED

80-612-131

It is requested that an Agent of the New Haven Field Division contact Mr. STEWART HEDDEN at New Milford, Connecticut, and that he be questioned in accordance with the facts set out herein and his reply be made available to the Bureau immediately.

cc New Haven (2)

WOMcC:HJR

137

60

7-10

Office Memorandum • UNITED STATES GOVERNMENT

TO : Director, FBI Attention: FBI Laboratory

DATE: April 2, 1947

FROM : SAC, New Haven

SUBJECT: HAGELIN CRYPTOGRAPHIC DEVICES
0 Cryptography

Reference is made to a letter from the New York Field Division to the Bureau dated March 25, 1947, in the above captioned matter.

This is to advise that an agent of the New Haven Field Division contacted Mr. STEWART HEDDEN, a retired lawyer, at his home on Route 129, New Milford, Connecticut, and Mr. HEDDEN furnished the following information. He stated that Mr. HAGELIN is expected to arrive in New York City from Sweden sometime during the early part of April, 1947. He said he is waiting to hear from Mr. HAGELIN regarding the exact date and time of his arrival as he is to meet him and Mr. HAGELIN is to spend several weeks as his guest in his home at New Milford, Connecticut.

In regard to the automatic encoding device operated by a key-board, such as the key-board on the ordinary typewriter, Mr. HEDDEN advised that this machine is being made by the Hagelin Company in Stockholm, Sweden and that this is the only place where the machine is being manufactured. He stated if anyone is interested in placing an order with this company he is the sole survivor of the company in this country and represents any and all of their business dealings. He further advised that any orders that are to be placed with this company should be placed through him. He said that the company is not contemplating manufacturing any of these devices in the United States.

During the agent's conversation with Mr. HEDDEN, the latter voiced the opinion that he thought that the Bureau was already in possession of one of these machines as he recalls several years ago going to the Bureau for demonstration purposes. In this regard he stated that he did not know whether or not the Bureau was interested in purchasing a machine of this type but as a suggestion stated that probably the simplest way of procuring one would be from the office of OWI or the office of OSS. Mr. HEDDEN stated that during the recent war both of these offices, in addition to the U.S. armed forces, were furnished a large number of these machines and due to the curtailment of their work and their reduction in force was of the opinion that both of these organizations had surplus machines of this type.

Inasmuch as this machine is a foreign make and at the present time is only being manufactured in Stockholm, the agent asked Mr. HEDDEN how a machine of this type could be repaired and Mr. HEDDEN advised that one ARTHUR

HJS:mmm
94-71RECORDED
INDEXED64 180-612-132
IF 12 II
31 APR 5 194750 APR 18 1947
11-27-*ack. signed*
R.H.

Letter to the Director
Page Two 94-71

JOHNSON, who resides at 365 Ridge Street, Newark, N.J., trained field men for the OWI and the OSS in the repairing of this machine and is, in Mr. HEDDEN's opinion, one of the best mechanics in this particular field that he knows.

In conclusion Mr. HEDDEN stated that he personally knows that Mr. HAGELIN would be glad to assist the Bureau in any way possible regarding this device. He said that should the Bureau require any additional information concerning the machine or any information from Mr. HAGELIN that the Bureau could contact Mr. HAGELIN at his New Milford address. In this regard HEDDEN stated that before Mr. HAGELIN returns to Stockholm he is to visit friends in Washington and would be only too glad to discuss this matter with any of the Bureau representatives if the Bureau so desires. As stated above, Mr. HEDDEN advised that the best way to contact Mr. HAGELIN would be at HEDDEN's New Milford, Connecticut residence.

2454 North 48th Street
Milwaukee 10, Wisconsin
September 25, 1949

Mr. John Edgar Hoover, Director
Federal Bureau of Investigation
Department of Justice
Washington, D. C.

Dear Mr. Hoover:

CRYPTOGRAPHY

Enclosed please find description of a new "Three-Way Cipher", which I hope will be of interest to the Bureau's cryptographic section.

It is a long time since I last filed ciphers with the Bureau, but cryptography still remains my pet among many hobbies. Nothing else affords the same mental stimulus and challenge. However, since the war, I have not spent too much time on the construction of new ciphers, preferring to work at acquiring a reading knowledge of as many foreign languages as possible in long-range preparation for a future career as cryptanalyst.

Your agent, Mr. Maurice Price of the local office, first fostered my interest in foreign languages. I now read fourteen (besides English and some Latin) sufficiently well to do cryptanalysis in them. In several, I am able to read medical journals, scientific texts, etc.; others require considerable more work before they will be brought up to that level.

This is not nearly the feat it seems, for as you know all European languages have many common root words....so many, in fact, that when I tackle a new language, I can count on finding from three to five thousand cognates available to me at once, carried over from other languages I have already learned to read. I must spend some two hours daily riding the busses to and from work, and in that time (which otherwise would be wasted) a surprising amount of language study can be accomplished....especially when the principles of cryptanalysis are applied.

INDEXED 50

RECORDED 50

150-612-133

Re: the queer advertisement which appeared in the Wednesday, August 31, 1949 issue of the DETROIT FREE PRESS, hindsight is always better than foresight, unfortunately. I wish to change my snap interpretation (as given to your agent, Mr. Roethke) of the code message I believe was hidden in it. Text of the advertisement, exactly as printed in the "#31 Personals" column (page 23, column 4, lower half of the page) is as follows:

Danny Smith, meet Nina Di Mito,
at same shoe store, 8 to 9 p. m.,
Sept. 5th, thru Sept. 14th. Friends
advise.

NEW/HEAVEN

SEVEN

W978
GOER
500R

91
10-13400
10-13400
10-13400

Note odd punctuation. "Friends advise" fits the Soviet jargon code; stet. "Shoe store" could mean Russia or a certain part of Russia, instead of "passport forger's office" as first supposed.

If the principles of the Nihilist transposition cipher are applied to the syllables of the first line of the advertisement and the first word of the second line, a most startling phonetic message in Russian appears! In the light of recent newspaper developments, this cannot be mere coincidence.

Rearranged syllables, numbered to show the transposition pattern, with the Russian words they phonetically resemble and translations written underneath, are as follows:

Smith	Dan	- ny	meet	at	Ni	Di	na	mi	- tø
3	1	2	4	10	5	7	6	8	9
сметание			метать		не	динамитъ			

Translations:

"sweeping"	root word meaning "to launch, cast or throw"; could also be an abbreviated form of the word метательный which means "missile."	"not"	"dynamite"
------------	---	-------	------------

The name "Smith" is rendered **СМИТ** in Russian, the "h" being dropped. If Smith is given its Russian pronunciation and if "Danny" is said rapidly after it, giving the vowel "a" its Russian sound, the words "Smith Danny" sound very much like the Russian word which means "sweeping", or **сметание**.

The message could, therefore, be rendered:

"A sweeping missile, not dynamite," (i.e. an atomic bomb) will be exploded at the testing grounds in Russia) 8 to 9 p.m. (your time) Sept. 5 thru Sept. 14. Friends (i.e. Communist officials) (so) advise (you.)"

See also attached copy of translation of a Russian poem entitled "Atomic Lullaby" which appeared on page 40 of the September 26, 1949 issue of **NEWSWEEK** magazine. Note underlined reference to a power "not TNT or dynamite," used to describe atomic explosives. That phrase clicked in my mind, making possible the solution of the syllable transposition in the advertisement. Note, also, the underlined reference to an "appointed hour" which implies that the bomb was set off in accordance with a known schedule.

Question: Do the dates and times mentioned in the advertisement mean anything to Central Intelligence? (The Lund observatory in Sweden reported that its seismograph registered an earth tremor on September 14th which might have been caused by an atomic

3.
explosion in Siberia. I find that bit of news most interesting,
as the date coincides with one of the dates in the DETROIT FREE
PRESS advertisement.)

Question: Was the advertisement inserted to warn Soviet agents
to be on duty at certain times to test for radioactivity in the
Detroit atmosphere? ???????????

Sincerely yours,

Frieda L. Niemzyk

Frieda L. Niemzyk

Encls.

ATOMIC LULLABY

Even Russian babies can now reasonably surmise that the Soviet Union has made or is making atom bombs. Edmund Stevens, Christian Science Monitor correspondent writing from Stockholm, last week reported that the latest Soviet nursery lullaby, composed by one Yevgeny Dolmatovsky, runs as follows:

In the taiga (Siberian forest) many leagues hence
At the country's other end
A granite mountain stands,
Blocking our way.
The time was more than ripe
To turn it upside down.
The time was more than ripe
For it to yield its ore.
Sleep, daughter dear. The night is dark.
Rock-a-bye.

A band of geologists lived there.
Through summer heat and winter cold,
Twelve months in a row,
They crawled about the mountain.
Then professors landed there by plane,
Next a company of sappers came,
Big, strapping boys they were.

Their young commander
Acting on his orders
Laid an explosive charge --
Not TNT or dynamite.
There's a stronger substance
In your country now.
I shall not name it.
Rock-a-bye.

At the appointed hour there came a blast.
The granite vanished into smoke,
Lighting the surrounding taiga
With golden brilliance.
Let the wave from the blast
Roll on to foreign shores
Where it will sound
A warning to our foes.

(Copied from page 40 of the September 26, 1949 issue of NEWSWEEK.)



ENCLOSURE



80-611. 133

THREE-WAY CIPHER

The attached cipher table may be used in three different ways.

(1) Double substitution, employing a keyword. The keyword is written repeatedly under the clear, as in the example given. To encipher, find the first letter of the clear in the vertical alphabet to the left of the table. Next, look for the first letter of the keyword in the horizontal alphabet above the numbers immediately to the right of the letter denoting the clear. The letter appearing in the alphabet beneath the numbers is then written down as the first letter of the enciphered message. Repeat with the second letter of the clear and the second letter of the keyword, etc., until the entire message is enciphered.

To decipher, write the keyword above the enciphered message as often as necessary. Look for the combination of keyletter and cipher letter in the table. When located, the letter to the left is the clear.

Example: (Keyword - Kashmir)

Clear: T H E U T M O S T A N Y M O D E R N C I P H E R C A N

Keyword: k a s h m i r k a s h m i r k a s h m i r k a s h m i

Message: W Z W Y U X N D G Y Q Y X N T O V Q F N F P O V K E P

Clear: H O P E T O A C C O M P L I S H I S T O F O R C E T H

Keyword: r k a s h m i r k a s h m i r k a s h m i r k a s h m

Message: I U W W Z S I A H E N P X N X P V V Z S S N D R W Z N

Clear: E D E C I P H E R E R T O E M P L O Y H I S L A S T R

Keyword: i r k a s h m i r k a s h m i r k a s h m i r k a s h

Message: G M E R D P N G W E N O X C X F Z E S S J F S G N O G

Clear: E S O U R C E S P A R T I C U L A R L Y H I S R E S O

Keyword: m i r k a s h m i r k a s h m i r k a s h m i r k a s

Message: C F N V N Z H B O Z D G D K T B Z D J S S J F W E N M

80-612-133

Clear: U R C E S O F T I M E T O D E L A Y D E C I P H E R M
 Keyword: h m i r k a s h m i r k a s h m i r k a s h m i r k a

Message: Y B J X D E I Z J X X W E L H X I T T O Z O K R X D F

Clear: E N T U N T I L T H E I N F O R M A T I O N O B T A I
 Keyword: s h m i r k a s h m i r k a s h m i r k a s h m i r k

Message: W Z U X G W V R Z N G E N A M G T I P L E F X Y Y Z L

Clear: N E D B Y T H E P R O C E S S I S N O L O N G E R O F
 Keyword: a s h m i r k a s h m i r k a s h m i r k a s h m i r

Message: X W W Y C P P O E G S J X D N D G L W S U X W H B W J

Clear: V A L U E.
 Keyword: k a s h m

Message: P Q R Y C

THE UTMOST ANY MODERN CIPHER CAN HOPE TO ACCOMPLISH IS TO FORCE
 THE DECIPHERER TO EMPLOY HIS LAST RESOURCES, PARTICULARLY HIS
 RESOURCES OF TIME, TO DELAY DECIPHERMENT UNTIL THE INFORMATION
 OBTAINED BY THE PROCESS IS NO LONGER OF VALUE.

Send in conventional groups of five letters:

WZWYU XNDGY QYXNT OVQFN FPOVK EPIUW WZSIA HENPX NXPVV
 ZSSND RWZNG MERDP NGWEN OXCXF ZESSJ FSGNO GCFNV NZHBO
 ZDGDK TBZDJ SSJFW ENMYB JXDEI ZJXXW ELHXI TTOZO KRXDF
 WQUXG WVRZN GENAM GTIPL EFXYY ZLXWW YCPPO EGSJX DNDGL
 WSUXW HBWJP QRYCz

Frequency count:

A....2	E....11	I.....5	M.....3	Q.....4	V.....6
B....4	F.....8	J.....7	N.....16	R.....5	W.....15
C....4	G....11	K.....3	O.....8	S....10	X....16
D...10	H.....4	L.....4	P.....9	T.....5	Y.....8
				U.....4	Z....12

Since the table is composed of irrational alphabets, and since the number of letters used out of each horizontal set depends entirely upon the length of the keyword, it speeds decipherment tremendously if only those groups of key letter and cipher letter which could be used are charted beside each clear letter. In the example given, using the keyword "Kashmir", only seven groups per letter of the clear are used.

Note the successful suppression of frequencies.

(2) Number symbols, 01 through 26, the same set of symbols being used for twenty-seven alphabets, are employed in the second version of this cipher.

Encipherment is by pairs of letters, the first letter of each bigram being found in the vertical alphabet to the left of the table. The number beside this letter is set down. The second letter of each bigram is found in the horizontal alphabet to the right. The number beneath this letter forms the second symbol of the enciphered bigram.

Decipherment is simple: merely find the right combination of numbers to denote the letters of the en claire bigram.

Frequencies are adequately suppressed, as proved by the count appended. The message given in the following example is the same used to illustrate the first version of this three-way cipher.

Clear:	T	H	E	U	T	M	O	S	T	A
Cipher:	11	15	08	10	11	20	04	05	11	08
Clear:	N	Y	M	O	D	E	R	N	C	I
Cipher:	02	19	18	10	09	21	06	23	24	26
Clear:	P	H	E	R	C	A	N	H	O	P
Cipher:	15	19	08	07	24	18	02	02	04	02
Clear:	E	T	O	A	C	C	O	M	P	L
Cipher:	08	09	04	13	24	20	04	25	15	23
Clear:	I	S	H	I	S	T	O	F	O	R
Cipher:	07	18	26	09	14	02	04	18	04	04
Clear:	C	E	T	H	E	D	E	C	I	P
Cipher:	24	22	11	15	08	19	08	18	07	15
Clear:	H	E	R	E	R	T	O	E	M	P
Cipher:	26	05	06	14	06	03	04	17	18	11
Clear:	L	O	Y	H	I	S	L	A	S	T
Cipher:	01	11	21	10	07	18	01	23	14	02

Clear: R E	S O	U R	C E	S P
Cipher: 06 14	14 23	17 24	24 22	14 24
Clear: A R	T I	C U	L A	R L
Cipher: 10 11	11 16	24 12	01 23	06 21
Clear: Y H	I S	R E	S O	U R
Cipher: 21 10	07 18	06 14	14 23	17 24
Clear: C E	S O	F T	I M	E T
Cipher: 24 22	14 23	05 08	07 12	08 09
Clear: O D	E L	A Y	D E	C I
Cipher: 04 16	08 01	10 18	09 21	24 26
Clear: P H	E R	M E	N T	U N
Cipher: 15 19	08 07	18 26	02 14	17 20
Clear: T I	L T	H E	I N	F O
Cipher: 11 16	01 16	26 05	07 13	05 03
Clear: R M	A T	I O	N O	B T
Cipher: 06 22	10 13	07 14	02 09	16 12
Clear: A I	N E	D B	Y T	H E
Cipher: 10 02	02 25	09 18	21 22	26 05
Clear: P R	O C	E S	S I	S N
Cipher: 15 03	04 15	08 08	14 17	14 22
Clear: O L	O N	G E	R O	F V
Cipher: 04 24	04 26	13 18	06 24	05 10
Clear: A L	U E			
Cipher: 10 05	17 11			

Frequency count:

01 - 5	06 - 8	11 - 10	16 - 5	21 - 6
02 - 10	07 - 9	12 - 3	17 - 6	22 - 6
03 - 3	08 - 12	13 - 4	18 - 12	23 - 7
04 - 12	09 - 7	14 - 13	19 - 4	24 - 13
05 - 8	10 - 10	15 - 8	20 - 3	25 - 2
				26 - 8

(3) The third version of this cipher employs a number (consisting of two digits) and a letter to denote a bigram of the clear.

To illustrate: the words, "Federal Bureau of Investigation," would be enciphered as follows:

- a. Divide the text of the clear into bigrams.
- b. Locate the first letter of each bigram in the vertical alphabet to the left of the table.
- c. Find the second letter of each bigram in the corresponding horizontal alphabet above the row of numbers.
- d. Set down both the number and the letter immediately beneath the letter located in step c.

Example:

Clear:	F	E	D	E	R	A	L	B	U	R	E	A	U	O
Cipher	19w	21z	10n	24i	24o	16o	21r							
Clear:	F	I	N	V	E	S	T	I	G	A	T	I	O	N
Cipher:	23s	16c	08w	16y	14o	16y	26r							

To decipher: Run down the columns of numbers to locate each cipher group, as for example, the first group above (19w) which denotes the letters "FE" of the clear. Follow the 19 column down until the combination of the number 19 with the letter w beneath it is found. The letter of the vertical alphabet to the left is the first letter of the bigram in the clear. The letter in the horizontal alphabet immediately above the number is the second letter of the bigram.

Here, again, frequencies are adequately suppressed.

Cipher tables, consisting of four pages of graph paper, are attached hereto.

Frieda L. Niemzyk

2454 North 48th Street
Milwaukee 10, Wisconsin

Table - Three-Way Cipher

A	10	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	II	E	F	G
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
		J	I	H	G	F	E	II	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K
B	16	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	II	E	F	G	H
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
		C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	II
C	24	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	II	E	F	G	H	I
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
		I	H	G	F	E	II	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J
II	09	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	II	E	F	G	H	I	J
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
		T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	II	C	B	A	Z	Y	X	W	V	U
E	08	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	II	E	F	G	H	I	J	K
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
		II	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E
F	05	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	II	E	F	G	H	I	J	K	L
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
		O	N	M	L	K	J	I	H	G	F	E	II	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P
G	13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	II	E	F	G	H	I	J	K	L	M
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
		B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	II	C

80-612-133

H	26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
		Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

I	07	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
		U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V

J	19	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
		P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q

K	22	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
		K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L

L	01	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
		F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G

M	18	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
		A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B

N	02	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
		R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S

O 04

O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	II	E	F	G	H	I	J	K	L	M	N
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Q	P	O	N	M	L	K	J	I	H	G	F	E	II	C	B	A	Z	Y	X	W	V	U	T	S	R

P 15

P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	II	E	F	G	H	I	J	K	L	M	N	O
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
H	G	F	E	II	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I

Q 25

Q	R	S	T	U	V	W	X	Y	Z	A	B	C	II	E	F	G	H	I	J	K	L	M	N	O	P
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	II	C	B	A	Z	Y

R 06

R	S	T	U	V	W	X	Y	Z	A	B	C	II	E	F	G	H	I	J	K	L	M	N	O	P	Q
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	II	C	B	A	Z	Y	X

S 14

S	T	U	V	W	X	Y	Z	A	B	C	II	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	II	C	B	A	Z	Y	X	W

T 11

T	U	V	W	X	Y	Z	A	B	C	II	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
N	M	L	K	J	I	H	G	F	E	II	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O

U 17

U	V	W	X	Y	Z	A	B	C	II	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
L	K	J	I	H	G	F	E	II	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M

V 20

V	W	X	Y	Z	A	B	C	II	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
E	II	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F

W 23

W	X	Y	Z	A	B	C	II	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	II	C	B	A	Z

X 12

X	Y	Z	A	B	C	II	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	II	C	B	A	Z	Y	X	W	V	U	T

Y 21

Y	Z	A	B	C	II	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
M	L	K	J	I	H	G	F	E	II	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N

Z 03

Z	A	B	C	II	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
G	F	E	II	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H

Frieda L. Niemzyk

2454 N. 48 St.

Milwaukee 10, Wis.

43579

Date : August 8, 1950

To : Legal Attache
London, England

From : Director, FBI

SECRET AIR CARRIER

Subject: Cryptanalysis Publications.

Information has come to the attention of the FBI Laboratory that there exist certain technical publications prepared by the British Code and Cipher School, as follows:

1. "Solution of German H.L.C. Hand Ciphers"
2. "Encyclopedia of Plaintext Systems"

The FBI Laboratory desires copies of these publications if the British Authorities can make them available to us.

80-612

*cc: Foreign Liaison Div
let off
C-70*

RECEIVED READING ROOM
F B I
U.S. DEPT. OF JUSTICE
AUG 8 5 26 PM '50

Mr. Tolson _____
Mr. Clegg _____
Mr. Glavin _____
Mr. Ladd _____
Mr. Nichols _____
Mr. Rosen _____
Mr. Tracy _____
Mr. Egan _____
Mr. Gurnea _____
Mr. Harbo _____
Mr. Mohr _____
Mr. Pennington _____
Mr. Quinn Tamm _____
Tele. Room _____
Mr. Nease _____
Miss Gandy _____

IWN:LWH

RECORDED - 122

EX-30

AUG 10 1950
COMM - FBI

134

UNRECORDED COPY FILED IN

September 14, 1950

RECORDED - 64

70-617-135

TO: Legal Attache
London, England

FROM: Director, FBI

~~CONFIDENTIAL~~ - AIR COURIER POUCH

SUBJECT: CRYPTANALYSIS PUBLICATIONS

Reurlet August 30, 1950. Since arrangements have been made by you for the Bureau to be furnished the entire revised set of publications in question, it will be unnecessary for items 1 and 2, mentioned in relet, to be photographed.

cc: Foreign Service Desk, Room 7629

CFD/DMD

[Handwritten signature]

Mr. Tolson _____
Mr. Clegg _____
Mr. Glavin _____
Mr. Ladd _____
Mr. Nichols _____
Mr. Rosen _____
Mr. Tracy _____
Mr. Egan _____
Mr. Gurnea _____
Mr. Harbo _____
Mr. Mohr _____
Mr. Pennington _____
Mr. Quinn Tamm _____
Tele. Room _____
Mr. Nease _____
Miss Gandy _____

SEP 18 1950
COMM - FBI

SEP 15 11 22 AM '50
RECEIVED READING ROOM
F B I
U. S. DEPT. OF JUSTICE

[Handwritten signature]

✓ 13

W. Newell



United States Department of Justice
Federal Bureau of Investigation

American Embassy
1, Grosvenor Square
London, W. 1

~~CONFIDENTIAL~~ - AIR COURIER POUCH

Date: August 30, 1950
To: Director, FBI
From: Legal Attache
London, England
Subject: CRYPTANALYSIS PUBLICATIONS

Rebulet August 8, 1950, requesting that this office obtain the following technical publications from the British Code and Cipher School:

1. "Solution of German S.I.S. Hand Ciphers"
2. "Encyclopedia of Clandestine Systems"

This is to advise that writer has been informed by SIGINT that there are no extra copies of these publications available. However, if the Bureau so desires, these publications can be photographed and the microfilm sent to the Bureau for printing.

According to SIGINT, these publications are two of a four-volume set, which is presently being revised and will be published some time during the end of this year. Arrangements are being made so that the Bureau will obtain copies of the entire revised set. In view of this, SIGINT are not being asked to microfilm the current publications unless the Bureau so desires.

I would appreciate being advised further in this regard.

JAC:LL

RECORDED - 117

EX-16

80-612-136, 137

CHANGED TO

66-629-677X, 732X

APR 22 1952

RS

2

4K
December 15, 1953

Mr. Nichols:

The deciphered message quoted by Laraine Day Durocher is from the textbook entitled "Elementary Cryptanalysis" by Helen Fouche Gaines, published by American Photographic Publishing Company, Boston, Massachusetts. The message appears as problem 74 on page 96 of the text; however, the decipherment does not appear in the book.

It happens that Mr. Downing has used this book to some extent in connection with our training course in cryptanalysis and that this message had been previously deciphered. It is as follows:

"Dancing down fairway, madcap
ouphe, ugly face aglow, saw bald
golf tyro drive into rough, heard
awful language."

Ouphe - elf or goblin, per Webster's
unabridged dictionary.

RY

R. T. Harbo

File mltu

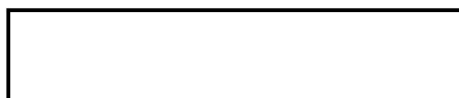
RECORDED - 60

82-612-138
JAN 8 1954

53 JAN 8 1954

83-612-139

CHANGED TO



b3
b7E

JAN 19 1954

1 - Mr. Conrad
1 - Mr. DeLoach
1 - Mr. Downing
1 - Mr. Newpher

SAC, Tampa (95-0-56)

August 14, 1964

Director, FBI

REC-21 80-612-140

CRYPTOGRAPHIC MATTERS

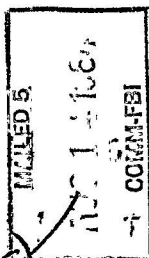
Reurlet 8/10/64 submitting cryptographic information supplied by an individual who identified himself as Col. Frederick E. Day.

For your information the cipher system and associated technical concepts supplied by Col. Day and reflected in the copy of a letter to Mr. William F. Friedman are technically irrational and untenable. They strongly indicate the source as being a mentally unbalanced individual.

Please advise Col. Day that the pressure of official business precludes a technical evaluation by the FBI Laboratory of the cipher system devised by his friend.

IWN:maa
(7)

Tolson _____
Belmont _____
Mohr _____
Casper _____
Callahan _____
Conrad _____
DeLoach _____
Evans _____
Gale _____
Rosen _____
Sullivan _____
Tavel _____
Trotter _____
Tele. Room _____
Holmes _____
Gandy _____



MAIL ROOM ☒ TELETYPE UNIT ☐

UNITED STATES GOVERNMENT

Memorandum

TO : DIRECTOR, FBI
(ATTN: FBI Laboratory)

FROM : SAC, TAMPA (95-0-56)

SUBJECT: CRYPTOGRAPHIC MATTERS

DATE: 8/10/64

Mr. Tolson	
Mr. Belmont	
Mr. Mohr	
Mr. Casper	
Mr. Callahan	
Mr. Conrad	
Mr. DeLoach	
Mr. Evans	
Mr. Gale	
Mr. Rosen	
Mr. Sullivan	
Mr. Tavel	
Mr. Trotter	
Tele. Room	
Miss Holmes	
Miss Gandy	

On 7/23/64, an individual who identified himself as Col. FREDERICK E. DAY, 4017 Bullard Parkway, Temple Terrace, Fla., telephoned the Tampa Office and advised that he had a friend who had been working for the last 20 years on cryptography and had been able to break a number of codes in Shakespearan works. He wanted to know whether there was any individual in the Tampa Office who would be interested in receiving such material. He was advised that the Laboratory may be interested in such matters and he said that he would consider furnishing the FBI Laboratory such information. He insisted that there was nothing wrong with his friend who had been working on cryptography and there was nothing wrong with him.

On 8/10/64, Col. DAY appeared at the Tampa Office and presented a letter addressed to the FBI Laboratory, dated 8/5/64, together with a copy of a letter which he had sent to Mr. WILLIAM F. FRIEDMAN of 310 2nd Street, S.E., Washington 3, D.C. The above communications are being enclosed for the information of the FBI Laboratory.

The attention of the Bureau is invited to Page 2, Paragraph 2 of the letter from Col. DAY to the Laboratory in which he states he would be honored to have the Director as a guest during any visit the Director may make to Tampa.

Relative to Col. DAY, it was noted that he is an extremely nervous individual and during conversation with him, he repeated himself many times on seemingly immaterial points. He appears to be intensely interested in cryptography and indicated that although he is not a cryptologist himself, he worked in the development of ciphering machines.

No further action is being taken in this regard by Tampa.

2 - Bureau (Enc. 2)
2 - Tampa
LEB/mw
(4)

ENCLOSURE

EX-112 REC-21

AUG 12 1964

89-112-140

SEVEN

EXP. PROC.

plw

Set to Sag TP
Thon:maa
8-14-64



41 Bullard Parkway,
Temple Terrace, Fla.
5 Aug 64

The FBI Laboratory
Washington, D.C.

Thru: Tampa FBI Office

Dear Sirs,

I find myself in possession of the key to a certain code of communication, which I predict will be recognized one day as the greatest cipher ever devised. I consider it my duty as a citizen and as a member of the armed forces to reveal this knowledge to you. I hope your laboratory will receive credit as the first to verify this discovery and I need your backing to convince the world of its authenticity.

For over 300 years great students of Shakespear's works have suspected that they were written so as to contain some sort of code. Brilliant experts and psychic charlatans have searched in vain for the key to any such code. After most extensive study and research, Mr William Friedman wrote a book, entitled Shakespearian Ciphers Examined, in which he concludes that he had not been able to unearth any evidence to indicate the discovery of any true cipher. He was absolutely correct, but someday he may learn how close he came. He is a recognized expert on the subject and I am enclosing a copy of a letter I have written to him. I fear that his infirmities and his admitted skepticism may prevent him from rendering the required assistance.

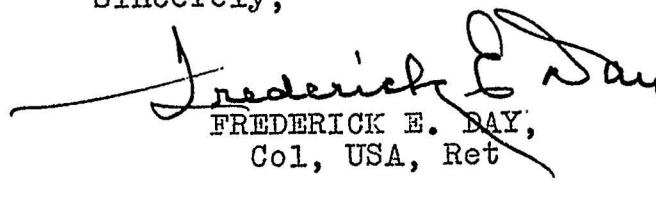
The discoverer of this ingenious, deceptive, powerful, and rigorous cipher is now an 86 year old, alert, retired educator and research physicist, who lives in Tampa. He is widely recognized for many of his accomplishments, but it appears that those who know of his work with Shakespear do not realize its importance or are in no position to do anything about it. He has used this cipher to extract hundreds of messages which are hidden behind the clear text of the First Folio. They vary in length from a single sentence to stories containing over 2,000 words. They are spicy, fascinating, and completely fabulous; but that is beside the point. You are not being asked to believe them, just to verify the fact that the cipher exists as claimed and that the messages are the result of following the rules of the cipher exactly. My friend is able to type clear text containing messages so enciphered, but brilliant as he is, he is no match for the superman who designed it and used it with such ease.

Are you interested in participating in unraveling what may prove to be one of the greatest mysteries the world has ever known? Can qualified cryptological experts from your laboratory visit me, or your Tampa FBI office? One hour spent with my friend and his work will convince them of the undeniable truth of my claim. I do not believe that I can secure his permission to send you a sample of his work for evaluation, and such a single example would not be likely to demonstrate every element of the cipher. A few very intelligent individuals have attempted to steal his discovery and pass it off as their own, but none of them happened to have the faintest knowledge of cryptography. I understand the cipher thoroughly but I am somewhat ashamed to admit that so far I have not been able to produce the message from the clear text and I doubt very much if Mr Friedman can do so either. I can verify it once its extraction has been completed. As you might suspect, each message comes from a relatively small concentrated portion of the clear text. I am now helping with the preparation of 13 messages taken from the last partial page of Two Gentlemen of Verona. One of them concerns a certain old stone house. Do you remember the last line of that play "One feast, one house, one mutuall happiness"?

After the conclusion of the visit of your experts, I would expect to receive a letter, signed by Mr Hoover, stating that the cipher revealed to them did in fact exist in Shakespear's First Folio and that the messages examined by them were taken from there by following the rules of the cipher. I would be honored to have Mr Hoover as my guest during your visit, and I really believe that what you may see revealed is sufficiently momentous to warrant his presence. This is especially true in view of the fact that he is a 33d degree Mason, for if the cryptologists can convince him that this is not a hoax, he will have information known by no other member of that organization.

I only hope that some of my actions will bear fruit, for it is my aim to greatly enhance my Country's cultural, literary, and intellectual prestige. I am at your service,

Sincerely,


FREDERICK E. DAY,
Col, USA, Ret

This isn't too rigorous a cipher. You can find words which weren't intended, but with these words you want make a story from START to STOP, and it won't be Shakespeare. There are also a few cleverly concealed letters which create skepticism or disbelief. Here is the sample:

Sonnet No 1 1
 7 4 9 4
 7 6

L M M P
 L E S F
 L E W V
 S T O P
 A N I E
 T A D S
 Y H T S
 A D I E
 E R M T
 L A S A
 S M R B
 F A W W
 S F W S
 U N S A

Most anyone can see STOP for this story and START for the next one, and TAMPA BAY FLORIDA. What was Shakespeare doing writing about Tampa? Maybe we had better wait on this one. Someday you may read this whole story of over 1,000 words taken from a much better cipher, and which could have been written by only one man who ever lived. It does seem strange that, a short time ago, the discovery of the key to any one of these ciphers might have gained world wide acclaim, and yet they may be relegated now to positions of relative minor importance, as compared to his really great cipher.

Anyone desiring to go along with me to the ultimate end of this affair must be capable of conceiving of a superman with a brain and capabilities several orders of magnitude greater than those of any other human who ever lived. He must be capable of stretching his bounds of credibility to encompass finding the First Folio honey-combed with a number of concurrent ciphers. He must be inured to tales of incest, and worse, and to finding decoded messages containing an occasional use of somewhat more "vile language" than is found in the clear text. He must be prepared to accept a more powerful, rigorous, deceptive cipher than any with which he is now familiar. Do you know of any cipher which will produce a decoded message 10 times the length of the clear text? The superman who designed and used it knew what he was doing. Contrary to your expressed opinion, time has proved that he was safe in putting the key to this one, as well as those to the other codes, in the clear text, rather than entrusting them to someone else or in hiding them in a less safe place. In this connection, I might say that there are relatively few unintentional printer's errors in the First Folio, for a better reason than you might suspect.

41 Bullard Parkway,
Temple Terrace, Fla.
5 Aug 64

Mr William F. Friedman
310 Second St SE
Washington 3, D.C.

Dear Sir,

Permit me to express my appreciation for your hand written reply to my letter of 6 July 64. I beg your indulgence to carry on our correspondence for a few more chapters. I, too, am no longer as young and as capable as I once was, but I am sure that both of us can be thankful that senility has not yet inhibited the functioning of the brains with which we were endowed. I am also sure that your interest in cryptology is as keen as ever.

Before I go further, I feel that I must bare to you my limited association with cryptography. I worked my way across the wastelands of the US during the early stages of WW II sending out messages on an M209 Converter, the inner workings of which I never understood. My formal education in cryptography was conducted on the Play Fair System in a Normandy fox-hole. There I learned to go across Europe, sending out messages on transmitters, which chance and my position made available to me, and which I had been assured the enemy could intercept and decode, much to his later confusion. I recognize your great contribution in the field of cryptology to our WW II effort and I am the first to admit that mine was negligible.

Pardon such digressions from the real subject matter, but let me make just one more. Why did you not give Bacon credit as the original inventor of a certain dot and dash code, so universally used and known by another name? He states, in his presentation of the biliteral cipher, that he could transmit it by means of any two dissimilar sounds from trumpets, bells, or cannon. Incidentally, if you don't give me up as hopeless, you may yet be convinced of the existence of the biliteral cipher in the First Folio, in spite of the many founts of type. It is there. There is a word count cipher there too, but who is going to live long enough to bring out any great number of stories in this fashion? I really believe that he put these other codes in just to prove that he could do it, and perhaps to give you a few crumbs if you weren't smart enough to discover his best.

Of course, there is a cipher in the Sonnets too, as there is in everything he ever wrote. The initial letters of each of the 14 lines of the 154 verses form a cylindrical cipher, with some 350 settings. You find the words by the king's move method in not too badly scrambled anagram form. Might I arouse your interest and create a slight suspicion that one does exist if I gave you a tiny sample? This story really began back several columns at the word START.

-140

Please do not think that I intend anything derogatory in this paragraph. I have high regard for your ability; but don't feel too badly if my predictions turn out to be correct, for I hope to pit you against the greatest cryptographer of all time. I am sure that I can select a short innocuous story, send you a copy of the properly marked clear text and the decoded message, and that you can verify the message and define the cipher. Following this, I believe I can send you a prepared clear text of another message, indicate the subject matter of the enciphered message, and hope that you could produce the message. I would still feel confident that I could send you a bare piece of clear text and rest assured that you could not produce the message. If we add to this the problem of locating the clear text, you can realize why this cipher has remained uncracked for so many hundred years.

It would be nice to enlist the aid of Dr Wright of the Folger Library in this venture. However, I am sure that he and so many of our noted authorities are so convinced in their own minds that the drunken, illiterate, murdering swineherd of Stratford used a 22,000 word English vocabulary (twice Milton's) to produce the world's most enduring literature, that even seeing the original manuscripts in the author's own handwriting would not deter them from this belief. I believe the FBI entered your examination to some extent. I may send them a copy of this letter. Surely they will be willing to verify the cipher and they just might be very much interested in one which was good enough to remain hidden before the very eyes of the world's greatest scholars for such a long time.

If you think that I am just another crackpot, or the gullible victim of the senile delusions of a most scholarly friend, please throw this in the wastebasket and forget you ever heard of me. If you entertain the faintest suspicion that I know anything about cryptography and if you wish to cross your last bridge in possession of the key to the greatest cipher ever devised by mortal man, keep in touch with me. Sending you any material depends upon the wishes of my friend, who is almost unaware of our correspondence.

Sincerely,

FREDERICK W. DAY

UNITED STATES GOVERNMENT

Memorandum

TO : Mr. Conrad *Joe*

DATE: July 27, 1971

FROM : I. W. Newpher *IWN*

SUBJECT: CRYPTANALYSIS-GAMBLING-
TRANSLATION SECTION; ADMINISTRATIVE;
X EXTRA SHIFT USE OF COMPUTER

Tolson _____
Felt _____
Sullivan _____
Mohr _____
Bishop _____
Brennan, G.D. _____
Callahan _____
Casper _____
Conrad _____
Dalbey _____
Gale _____
Ponder _____
Rosen _____
Tavel _____
Walters _____
Soyars _____
Tele. Room _____
Holmes _____
Gandy _____

We are using Electronic Data Processing equipment for cryptanalysis examinations and production of Bureau coding materials at monthly rental of \$5,414 for the basic computer, 8 hours per day. Our workload has been expanding for some time and currently we have a sizable backlog plus pressure of special cases which include analysis of specimens associated with the Medburg (52-94527) and Gardburg Attempt (52-94781) cases, also a buildup of letters from [REDACTED]

b7E

Our computer can be used at an overtime rate of \$9.34 per hour which on an extra-shift basis of 8 hours daily would amount to \$1,494.40* for 4 weeks, 5 days per week. As an alternative the company, RCA, will rent the computer on an unlimited basis for \$1,082.80* per month. Night differential for operators to run the computer 2 extra shifts per day for 4 weeks, 5 days per week would amount to \$146.40. Total cost to operate our computer for one month on 2 additional shifts, including rental and night differential, would be \$1,229.20*, which means we could get three times as much use of our computer at an increased cost of less than 25 percent.

Two additional shifts per day would be handled by one cryptanalyst operator each shift, supervised by a Special Agent examiner already on duty in the FBI Annex for security protection. It is believed this would be a very economical and efficient use of our equipment for the month of August, 1971, and would alleviate a buildup of work which we are experiencing.

80-H-3

*in addition to present
cost of \$5,414.

- 1 - Mr. Sullivan
- 1 - Mr. Mohr
- 1 - Mr. Callahan
- 1 - Mr. Conrad
- 1 - Mr. Newpher

ENCLOSURE ATTACHED

ENCLOSURE

IWN:ms

(6)
5 AUG 2 1971
065 JUL 30

CONTINUED - OVER

PERS. REC. UNIT

REC-59
EX-104
12 AUG 5 1971
3 Jackson
31 NRC

Memorandum to Mr. Conrad
Re: Cryptanalysis-Gambling-Translation; Administrative
Extra Shift Use of Computer

RECOMMENDATION:

The Cryptanalysis-Gambling-Translation Section be authorized to use its computer for two extra shifts daily, 5 days per week, 4 weeks August, 1971, at the additional rental and salary cost of \$1,229.20.

Handwritten signatures and initials:
JAN, WEL, JAY, BOW, \$5, DD, Jm

Handwritten note:
Handled in Prop Mgt on P.O.#6653
JAY

F239 RC



ENCLOSURE

80-612-141

**PURCHASE ORDER
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
WASHINGTON, D. C. 20535**

THIS NUMBER MUST APPEAR ON
ALL PACKAGES AND PAPERS
RELATING TO THIS ORDER

ORDER NO.

FBI 6653

DATE

JULY 30, 1971

APPROPRIATION SYMBOL AND TITLE

SALARIES & EXPENSES, FBI,**1972**

REQUISITION NO.

65

ALLOTMENT

0705 F 92

PLEASE FURNISH AND DELIVER TO THE CONSIGNEE THE ARTICLES SPECIFIED BELOW:

TO
S
E
L
L
E
R

RCA
MR. [REDACTED]
MANAGER, CIVIL PROGRAMS
1901 N. MOORE STREET
ARLINGTON, VIRGINIA 22209

CONSIGNEE AND DESTINATION

S
H
I
P
T
O

FEDERAL BUREAU OF INVESTIGATION
215 PENNSYLVANIA AVENUE, S. E.
WASHINGTON, D. C. 20537

b6

b7C

INVITATION NO.

CONTRACT NO.

TIME FOR DELIVERY

DISCOUNT TERMS

F. O. B. POINT

SHIP VIA

GOV'T. B/L NO.

ITEM NO.

ARTICLES OR SERVICES

QUANTITY

UNIT

UNIT PRICE

AMOUNT

FOR UNLIMITED USE OF RCA 301 COMPUTER
FOR MONTH OF AUGUST 1971

1,082.80

RECEIVED ABOVE-MENTIONED SUPPLIES

TOTAL**1,082.80**

Official Title

Date

Items listed on this purchase order have been purchased for your official use and should be as requested by your office. Should any discrepancies appear hereon you should advise the Property Management Unit at once.

Upon receipt of these items prompt acknowledgement is required. Your signature and date above signifies that the material has been received and is correct.

C 6653

R
80-812 —

April 5, 1971

Special Agent in Charge, Savannah (66-1277)

Re: TECHNICAL EQUIPMENT - PHOTOGRAPHIC
SAVANNAH DIVISION

Dear Sir:

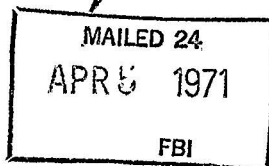
Reurlet 3/30/71.

- ☒ Equipment listed below has been received. After repairs have been made it will be returned to your office.
- ☐ Equipment listed below has been repaired and is being returned to your office.
- ☐ Equipment listed below is being shipped to your office for ☐ permanent ☐ temporary assignment. Appropriate inventory changes should be made.
- ☐

Camera, Tessina 35mm

SN 363109

FEW:taw (5)



Very truly yours,

J. Edgar Hoover
John Edgar Hoover
Director

MAIL ROOM
62 APR 14 1971
FBI

FEDERAL BUREAU OF INVESTIGATION
WASHINGTON, D. C. 20535

DATE: **11/7/66**

Re: **PHOTOGRAPHIC EQUIPMENT-
35 mm CAMERA**

TO: **SAC, HOUSTON (66-371)**

Re: **Urlet 10/21/66 ED/cb1**

Invoice of Contents

1-Beseler Topcon Super D 35 mm Camera, SN 4612173
1-RE. Auto-Topcor, 58 mm f 1.8 lens, SN 11610950-with leather carrying case

☐ Crypt.-Trans.
☒ Document
☐ Electronics
☐ P & C
☐ LFPS

Sent 11/7/66

716408

Registered

Special Instructions:

Mail **11/7/66** - Show shipment date and registry number.
Shipping room: Show shipment date; bill of lading number;
initial invoice; return to Section checked in block; after
initialing in block, invoice to be placed in administrative file.

FEW:mff- (2)

FBI File No.

80-612

11/7/66

MAILED Z

1966

COMM-FBI

Mr. I. M. Conrad

March 3, 1966

W. O. Griffith

Cryptography
AMERICAN ACADEMY OF FORENSIC SCIENCES
16TH ANNUAL MEETING, CHICAGO, ILLINOIS
2/24, 25, 26/66

b7E

SA [redacted], of the Document Section appeared in Chicago at captioned meeting where he presented a paper entitled "A Study of the Training and Continuing Educational Needs of Examiners of Questioned Documents" before the Questioned Documents Section of this meeting. This paper was well received. Also present were SA [redacted] and SA [redacted] who participated in the discussions of various papers and related matters.

b6
b7C

In addition to the paper presented by SA [redacted] some of the other papers are as follows:

1. "Typography and Questioned Documents," by Jan Beck. This paper related to the classification of various types of printing. This was supplemented with several slides. (80-701)
2. "Handwriting by the Blind," by Mary T. Bacon. (80-15)
3. "Thin-Layer Chromatography Technique Utilizing the Eastman Chromagram Sheet and Developing Apparatus," by Joseph Thall. This was supplemented with numerous slides. This method purports to be superior to paper chromatography and the electrophoretic methods currently employed. One of the problems

84-28130

1 - Mr. Mohr
1 - Mr. DeLoach
1 - Mr. Conrad
1 - Mr. Griffith
1 - Mr. Miller

1 - Bufile 80-15
1 - Bufile 80-806
1 - Bufile 80-608
① - Bufile 80-612
1 - Bufile 80-652 *clg*

1 - Bufile 80-693
1 - Bufile 80-729
1 - Bufile 80-738
1 - Bufile 80-758
1 - Bufile 80-782

80-612
NOT RECORDED
46 MAR 4 1966

MAR 10 1966 *md*

(CONTINUED OVER)

ORIGINAL FILED IN 84-28130

Memorandum to Mr. Conrad
Re: American Academy of Forensic Sciences
94-38136

encountered but not solved by the author is the unusually large samples required to make these tests. Such samples would seriously disfigure the questioned writing, particularly small amounts, such as signatures. It is possible that additional research in the FBI Laboratory would correct this deficiency. (60-603, 60-782, 60-785, 60-729)

4. "Historical Research, Document Examination and Crown Prince Rudolph of Austria," by David A. Green. This was supplemented with a few slides. Except for its historical interest, this paper contained nothing of interest.
5. "Paper Tapes and Labels Encountered in Document Examination," by David J. Ruppell. Included are tests for glue, starch, alkalinity, etc. (60-739, 60-617, 60-251, 60-693)
6. "Maschinen Forger," by Alwyn Cole. This covered the work done by the author for the Warren Commission and contains nothing of particular scientific interest.
7. "The Importance of Copies in Document Inquiries," by George C. Swart. In this paper the author points out that only limited examinations can be made from photocopies.
8. "Perception and Handwriting Identification," by Rafael Fernandez Ruesen. This contains nothing of particular scientific value. (60-15)
9. "Forgery and Check Frauds Affecting Banking and Business," by Orville B. Livingston. This paper was passed out but not delivered at this meeting. Included in this paper is a discussion of the use of Heber punch cards for handwriting specimen forms. (60-608)

Memorandum to Mr. Conrad
Re: American Academy of Forensic Sciences
34-58136

Other subjects discussed included office copying machines, what's new, the training of forensic science experts, the quantum of proof, working techniques in photography, and related matters. The various methods and techniques will be applied to the operations of the Document Section in so far as they can be used to apply to our work. We will also try to make improvements wherever possible.

The various papers will be placed in the Document Section Library for the convenience of the examiners.

ACTION: None. For information only.

Memorandum

APR 28 1988



SSP

CLASS

SRC'D

SER

REG

FBI Laboratory Division
Evidence Control Center
Room 3233, TL 241

Date 4-25-88

From : SA [redacted]

Section & Symbol Doc 4D

b6
b7C

Subject : NEW YORK SPECIAL

OCryptograph

TESTIMONY

Bufile # _____
(circle one) Court Grand Jury Other - _____ Dates _____
Supporting: (circle one) Bureau Federal Local Workdays _____
City & State _____ Category 1 2 3 4
Testified? ☐ Yes ☐ No If No, then circle Reason Below for Appearing in Court but not Testifying.
01. Guilty Plea 03. Case Dismissed 05. Testimony not Needed
02. Case Continued 04. Stipulation 06. Mistrial
07. Other _____

Results of Trial _____ Judge _____
Prosecuting Attorney _____ Defense Attorney _____

OTHER COMMITMENTS

Bufile # 80-612 City & State NEW YORK CITY, N.Y.
Agency FBI Dates 4-23 + 24-88
(circle one) Bureau Federal Local Workdays 2

Purpose: (circle one)

- | | |
|--------------------------------------|-------------------------------|
| 01. Lecture/Training (Others) | 06. Research/Data Acquisition |
| 01A. Tours, Training, etc., at FBIHQ | 07. _____ |
| 02. Training (Self) | 08. Investigative Support |
| 03. Speech | 09. Communication Support |
| 04. Pretrial Conference | 10. Conference/Meeting |
| 05. Field Examination of Evidence | 11. Deposition |

80-612

NOTED
6 NOV 18 1983

Details/Unusual or Interesting Circumstances

SEVEN
HS
FBI/DOJ

APR 88 ENT'D

Evidence Control Center

SSE

CLASS

SRC'D

SER

Memorandum



To : FBI Laboratory Division
Evidence Control Center
Room 3233, TL 241

Date 4/18/88

From

Section & Symbol Doc - XD
0728b6
b7CSubject : *New York Special**CRY ptology*

TESTIMONY

Bufile # _____
 (circle one) **Court** **Grand Jury** **Other** - _____ Dates _____
 Supporting: (circle one) **Bureau** **Federal** **Local** Workdays _____
 City & State _____ Category **1** **2** **3** **4**
 Testified? ☐ Yes ☐ No If No, then circle Reason Below for Appearing in Court but not Testifying.
 01. Guilty Plea 03. Case Dismissed 05. Testimony not Needed
 02. Case Continued 04. Stipulation 06. Mistrial
 07. Other _____

Results of Trial _____ Judge _____
 Prosecuting Attorney _____ Defense Attorney _____

OTHER COMMITMENTS

Bufile # 80-612 City & State New York, New York
 Agency FBI Dates 4/15-17/88
 (circle one) **Bureau** **Federal** **Local** Workdays 3

Purpose: (circle one)
 01. Lecture/Training (Others) 06. Research/Data Acquisition
 01A. Tours, Training, etc., at FBIHQ 07. _____
 02. Training (Self) 08. Investigative Support
 03. Speech 09. Communication Support
 04. Pretrial Conference 10. Conference/Meeting
 05. Field Examination of Evidence 11. Deposition

80 1012

Details/Unusual or Interesting Circumstances

NOT RECORDED

7 NOV 18 1988

SEVEN
CK

FBI/DOJ

Memorandum



JUL 87 EDTD

To : FBI Laboratory Division
Evidence Control Center
Room 8233 TL 241

Date 7/6/87

From

Section & Symbol Doc-XD
0728

b6
b7C

Subject :

WTB
New York Special
O Cryptography -

b7E

TESTIMONY

Bufile # _____
(circle one) **Court** **Grand Jury** **Other** - _____ Dates _____
Supporting: (circle one) **Bureau** **Federal** **Local** Workdays _____
City & State _____ Category **1 2 3 4**
Testified? ☐ Yes ☐ No If No, then circle Reason Below for Appearing in Court but not Testifying.
01. Guilty Plea 03. Case Dismissed 05. Testimony not Needed
02. Case Continued 04. Stipulation 06. Mistrial
07. Other _____

Results of Trial _____ Judge _____
Prosecuting Attorney _____ Defense Attorney _____

OTHER COMMITMENTS

Bufile # 80-612 City & State New York, New York
Agency FBI Dates 6/12-13/87
(circle one) Bureau **Federal** **Local** Workdays 2

Purpose: (circle one)

01. Lecture/Training (Others)
01A. Tours, Training, etc., at FBIHQ
02. Training (Self)
03. Speech
04. Pretrial Conference
05. Field Examination of Evidence

06. Research/Data Acquisition

07. _____

08 Investigative Support

09. Communication Support

10. Conference/Meeting

11. Deposition

SEP 22 1987

Details/Unusual or Interesting Circumstances

SEVEN

OCT 86 EN

Memorandum



To : FBI Laboratory Division
Evidence Control Center
Room 3223, TL 241

Date 10/10/86

From: SA [redacted]

Section & Symbol Dec - XD

b6
b7C

Subject: New York Special

Cryptography - [redacted]

b7E

TESTIMONY

Bufile # _____
(circle one) Court Grand Jury Other - _____ Dates _____
Supporting: (circle one) Bureau Federal Local Workdays _____
City & State _____ Category 1 2 3 4
Testified? ☐ Yes ☐ No If No, then circle Reason Below for Appearing in Court but not Testifying.
01. Guilty Plea 03. Case Dismissed 05. Testimony not Needed
02. Case Continued 04. Stipulation 06. Mistrial
07. Other _____

Results of Trial _____ Judge _____
Prosecuting Attorney _____ Defense Attorney _____

OTHER COMMITMENTS

Bufile # 80-612 City & State New York, N.Y.
Agency FBI Dates 9/8-9/86
(circle one) Bureau Federal Local Workdays 2

Purpose: (circle one)
01. Lecture/Training (Others) 06. Research/Data Acquisition
01A. Tours, Training, etc., at FBIHQ 07. _____
02. Training (Self) 08. Investigative Support
03. Speech 09. Communication Support
04. Pretrial Conference 10. Conference/Meeting
05. Field Examination of Evidence 11. Deposition

80-612-

Details/Unusual or Interesting Circumstances

NOT RECORDED

JAN 22 1987

98 FEB 4 1987

FBI/DOJ

Memorandum

SEP 86 ENT'D



To : FBI Laboratory Division
Evidence Control Center
Room 3233, TL 241

Date 9/10/86

From : SA [redacted]

Section & Symbol D UE

b6
b7C

Subject : NEW YORK SPECIAL

Cryptography - [redacted]

b7E

TESTIMONY

Bufile # _____
(circle one) Court Grand Jury Other - _____ Dates _____
Supporting: (circle one) Bureau Federal Local Workdays _____
City & State _____ Category 1 2 3 4
Testified? ☐ Yes ☐ No If No, then circle Reason Below for Appearing in Court but not Testifying.
01. Guilty Plea 03. Case Dismissed 05. Testimony not Needed
02. Case Continued 04. Stipulation 06. Mistrial
07. Other _____

Results of Trial _____ Judge _____
Prosecuting Attorney _____ Defense Attorney _____

OTHER COMMITMENTS

Bufile # 80-612 City & State NEW YORK, N.Y.
Agency FBI Dates 9/8-9/86
(circle one) Bureau Federal Local Workdays 1 1/2

Purpose: (circle one)

- | | |
|--------------------------------------|-------------------------------|
| 01. Lecture/Training (Others) | 06. Research/Data Acquisition |
| 01A. Tours, Training, etc., at FBIHQ | 07. _____ |
| 02. Training (Self) | 08. Investigative Support |
| 03. Speech | 09. Communication Support |
| 04. Pretrial Conference | 10. Conference/Meeting |
| 05. Field Examination of Evidence | 11. Deposition |

80-612-

Details/Unusual or Interesting Circumstances

20 DEC 10 1986

1 - SPECIAL OPERATIONS TICKLER

SEVEN

Memorandum

OCT 8 6 ENT'D



To : FBI Laboratory Division,
Evidence Control Center
Room 3223, TL 241

Date 8/27/86

From : SA [redacted]

Section & Symbol Doc - XD

b6
b7C

Subject : New York Special

Cryptology - [redacted]

b7E

TESTIMONY

Bufile # _____
 (circle one) **Court** **Grand Jury** **Other** - _____ Dates _____
 Supporting: (circle one) **Bureau** **Federal** **Local** Workdays _____
 City & State _____ Category **1** **2** **3** **4**
 Testified? ☐ Yes ☐ No If No, then circle Reason Below for Appearing in Court but not Testifying.
 01. Guilty Plea 03. Case Dismissed 05. Testimony not Needed
 02. Case Continued 04. Stipulation 06. Mistrial
 07. Other _____

Results of Trial _____ Judge _____
 Prosecuting Attorney _____ Defense Attorney _____

OTHER COMMITMENTS

Bufile # 80-612 City & State New York City, N.Y.
 Agency FBI Dates 8/26/86
 (circle one) **Bureau** **Federal** **Local** Workdays 1

Purpose: (circle one)
 01. Lecture/Training (Others) 06. Research/Data Acquisition
 01A. Tours, Training, etc., at FBIHQ 07. _____
 02. Training (Self) 08. Investigative Support
 03. Speech 09. Communication Support
 04. Pretrial Conference 10. Conference/Meeting
 05. Field Examination of Evidence 11. Deposition

Details/Unusual or Interesting Circumstances

80-612 -

NOT RECORDED

JAN 22 1987

98 FEB 4 1987

SEVEN

FBI/DOJ

Memorandum

AUG 1986



To : FBI Laboratory Division
Evidence Control Center */mas*
Room 3233, TL 241

Date

8/27/86

From :

Section & Symbol

D UE

b6
b7C

Subject : NEW YORK SPECIAL

Cryptography -

b7E

TESTIMONY

Bufile # _____
(circle one) **Court** **Grand Jury** **Other** - _____ Dates _____
Supporting: (circle one) **Bureau** **Federal** **Local** Workdays _____
City & State _____ Category **1** **2** **3** **4**
Testified? ☐ Yes ☐ No If No, then circle Reason Below for Appearing in Court but not Testifying.
01. Guilty Plea 03. Case Dismissed 05. Testimony not Needed
02. Case Continued 04. Stipulation 06. Mistrial
07. Other _____

Results of Trial _____ Judge _____
Prosecuting Attorney _____ Defense Attorney _____

OTHER COMMITMENTS

Bufile # 80-612 City & State NEW YORK, N.Y.
Agency FBI Dates 8/26/86
(circle one) Bureau **Federal** **Local** Workdays 1

Purpose: (circle one)

- | | |
|--------------------------------------|----------------------------------|
| 01. Lecture/Training (Others) | 06. Research/Data Acquisition |
| 01A. Tours, Training, etc., at FBIHQ | 07. <u>80-612</u> |
| 02. Training (Self) | <u>08.</u> Investigative Support |
| 03. Speech | 09. Communication Support |
| 04. Pretrial Conference | 10. Conference/Meeting |
| 05. Field Examination of Evidence | 11. Deposition |

NOT RECORDED

11 NOV 6 1986

Details/Unusual or Interesting Circumstances

RECORDED

1- SPECIAL OPERATIONS TICKLER

SEVEN

Memorandum



To : FBI Laboratory Division
Evidence Control Center
Room 3223, TL 241

Date 5/27/86

From : SA [redacted]

Section & Symbol Doc - XD
0727b6
b7C

Subject : Chicago Special
O Cryptography

TESTIMONY

Bufile # 80-612
(circle one) Court Grand Jury Other Field Support Dates 5/4-5/86
Supporting: (circle one) Bureau Federal Local Workdays 8/1
City & State Chicago, Ill. Category 1 2 3 4
Testified? ☐ Yes ☒ No If No, then circle Reason Below for Appearing in Court but not Testifying.
01. Guilty Plea 03. Case Dismissed 05. Testimony not Needed
02. Case Continued 04. Stipulation 06. Mistrial
07. Other N/A

Results of Trial _____ Judge _____
Prosecuting Attorney _____ Defense Attorney _____

OTHER COMMITMENTS

Bufile # _____ City & State _____
Agency _____ Dates _____
(circle one) Bureau Federal Local Workdays _____

Purpose: (circle one)

- | | |
|--------------------------------------|--------------------------------|
| 01. Lecture/Training (Others) | 06. Research/Data Acquisition. |
| 01A. Tours, Training, etc., at FBIHQ | 07. _____ |
| 02. Training (Self) | 08. Investigative Support |
| 03. Speech | 09. Communication Support |
| 04. Pretrial Conference | 10. Conference/Meeting |
| 05. Field Examination of Evidence | 11. Deposition |

80-612

NOT RECORDED

Details/Unusual or Interesting Circumstances

7 JUL 28 1986

235

64 AUG 10 1986

SEVEN
[Signature]
FBI/DOJ

Memorandum



MAY 86 ENTU

To : FBI Laboratory Division
Evidence Control Center
Room 3233, TL 241

Date MAY 5, 1986

From : SA [redacted]

Section & Symbol D UE

b6
b7C

Subject : CHICAGO SPECIAL
CRYPTOGRAPHY

TESTIMONY

Bufile # _____
(circle one) Court Grand Jury Other - _____ Dates _____
Supporting: (circle one) Bureau Federal Local Workdays _____
City & State _____ Category 1 2 3 4
Testified? ☐ Yes ☐ No If No, then circle Reason Below for Appearing in Court but not Testifying.
01. Guilty Plea 03. Case Dismissed 05. Testimony not Needed
02. Case Continued 04. Stipulation 06. Mistrial
07. Other _____

Results of Trial _____ Judge _____
Prosecuting Attorney _____ Defense Attorney _____

OTHER COMMITMENTS

Bufile # 80-612 City & State CHICAGO, ILL
Agency FBI Dates 5/4-5/86
(circle one) Bureau Federal Local Workdays 2

Purpose: (circle one)
01. Lecture/Training (Others) 06. Research/Data Acquisition
01A. Tours, Training, etc., at FBIHQ 07. _____
02. Training (Self) 08. Investigative Support
03. Speech 09. Communication Support
04. Pretrial Conference 10. Conference/Meeting
05. Field Examination of Evidence 11. Deposition

80-612-

Details/Unusual or Interesting Circumstances

JUN 23 1986

Memorandum

FEB 8 6 ENTD



To : FBI Laboratory Division
Evidence Control Center
Room 3233, TL 241

Date 2/24/86

From : SA [redacted]

Section & Symbol DOC-TY

Subject : FCI SWAVET

b6
b7C

Cryptography

TESTIMONY

Bufile # _____
(circle one) **Court** **Grand Jury** **Other** - _____ Dates _____
Supporting: (circle one) **Bureau** **Federal** **Local** Workdays _____
City & State _____ Category **1** **2** **3** **4**
Testified? ☐ Yes ☐ No If No, then circle Reason Below for Appearing in Court but not Testifying.
01. Guilty Plea 03. Case Dismissed 05. Testimony not Needed
02. Case Continued 04. Stipulation 06. Mistrial
07. Other _____

Results of Trial _____ Judge _____
Prosecuting Attorney _____ Defense Attorney _____

OTHER COMMITMENTS

Bufile # 80-612 City & State NEW YORK, N.Y.
Agency FBI Dates 2/11/86
(circle one) **Bureau** **Federal** **Local** Workdays 1

Purpose: (circle one)
01. Lecture/Training (Others) 06. Research/Data Acquisition
01A. Tours, Training, etc., at FBIHQ 07. _____
02. Training (Self) 08. **Investigative Support**
03. Speech 09. Communication Support
04. Pretrial Conference 10. Conference/Meeting
05. Field Examination of Evidence 11. Deposition

Details/Unusual or Interesting Circumstances

NOT RECORDED
12 MAR 12 1986

2 APR 20 1986

SEVEN

FEB 8 6 ENT

Memorandum



To : FBI Laboratory Division
Evidence Control Center
Room 3223, TL 241

Date 2-12-86

From : SA [redacted]

Section & Symbol D WJ

b6
b7C

Subject : Special Laboratory Support
New York Division
Cryptography - [redacted]

b7E

TESTIMONY

Bufile # _____
(circle one) **Court** **Grand Jury** **Other** - _____ Dates _____
Supporting: (circle one) **Bureau** **Federal** **Local** Workdays _____
City & State _____ Category **1 2 3 4**
Testified? ☐ Yes ☐ No If No, then circle Reason Below for Appearing in Court but not Testifying.
01. Guilty Plea 03. Case Dismissed 05. Testimony not Needed
02. Case Continued 04. Stipulation 06. Mistrial
07. Other _____

Results of Trial _____ Judge _____
Prosecuting Attorney _____ Defense Attorney _____

OTHER COMMITMENTS

Bufile # 80-612
Agency FBI City & State NY, NY
(circle one) **Bureau** **Federal** **Local** Dates 2-11-86
Workdays 1

Purpose: (circle one)

- | | |
|--------------------------------------|-------------------------------|
| 01. Lecture/Training (Others) | 06. Research/Data Acquisition |
| 01A. Tours, Training, etc., at FBIHQ | 07. _____ |
| 02. Training (Self) | 08. Investigative Support |
| 03. Speech | 09. Communication Support |
| 04. Pretrial Conference | 10. Conference/Meeting |
| 05. Field Examination of Evidence | 11. Deposition |

80-612-

Details/Unusual or Interesting Circumstances

NOTED
3 FEB 11 1986

MAR 6 - 1986

SEVEN

Memorandum



To : FBI Laboratory Division
Evidence Control Center
Room 3223, TL 241

Date

12/5/85

From :

Section & Symbol

D UE

b6
b7C

Subject :

NEW YORK SPECIAL

Cryptography

TESTIMONY

Bufile #

(circle one) Court Grand Jury Other -

Dates

Supporting: (circle one) Bureau Federal Local

Workdays

City & State

Category 1 2 3 4

Testified? ☐ Yes ☐ No If No, then circle Reason Below for Appearing in Court but not Testifying.

01. Guilty Plea

03. Case Dismissed

05. Testimony not Needed

02. Case Continued

04. Stipulation

06. Mistrial

07. Other

Results of Trial

Judge

Prosecuting Attorney

Defense Attorney

OTHER COMMITMENTS

Bufile #

80-612

City & State

NEW YORK, NY

Agency

FBI

Dates

12/4/85

(circle one)

Bureau

Federal

Local

Workdays

1

Purpose: (circle one)

01. Lecture/Training (Others)

01A. Tours, Training, etc., at FBIHQ

02. Training (Self)

03. Speech

04. Pretrial Conference

05. Field Examination of Evidence

06. Research/Data Acquisition.

07.

08. Investigative Support

09. Communication Support

10. Conference/Meeting

11. Deposition

Details/Unusual or Interesting Circumstances

MAR 2 1986

SEVEN

FBI/DOJ

Memorandum



SEP 8 5 ENT

To : FBI Laboratory Division
Evidence Control Center
Room 3223, TL 241

Date 9/16/85

From : SA [redacted]

Section & Symbol SAS - TD

b6
b7C

Subject : New York Operation. (Serial)

CRYPTOGRAPHY - [redacted]

b7E

TESTIMONY

Bufile # _____
 (circle one) Court Grand Jury Other - _____ Dates _____
 Supporting: (circle one) Bureau Federal Local Workdays _____
 City & State _____ Category 1 2 3 4
 Testified? ☐ Yes ☐ No If No, then circle Reason Below for Appearing in Court but not Testifying.
 01. Guilty Plea 03. Case Dismissed 05. Testimony not Needed
 02. Case Continued 04. Stipulation 06. Mistrial
 07. Other _____

Results of Trial _____ Judge _____
 Prosecuting Attorney _____ Defense Attorney _____

OTHER COMMITMENTS

Bufile # 80-612
 Agency FBF
 (circle one) Bureau Federal Local
 City & State New York, NY.
 Dates 9/14-15/85
 Workdays 2

Purpose: (circle one)
 01. Lecture/Training (Others)
 01A. Tours, Training, etc., at FBIHQ
 02. Training (Self)
 03. Speech
 04. Pretrial Conference
 05. Field Examination of Evidence
 06. Research/Data Acquisition.
 07. _____
 08. Investigative Support
 09. Communication Support
 10. Conference/Meeting
 11. Deposition

NOT RECORDED

23 NOV 26 1985

Details/Unusual or Interesting Circumstances

52-13-1

SEVEN

Memorandum



To : FBI Laboratory Division
Evidence Control Center
Room 3223, TL 241

OCT 8 5 ENTD

Date

10/29/85

From :

SA [redacted]

Section & Symbol

DUE

b6
b7C

Subject :

WFO SPECIAL

Cryptography - [redacted]

b7E

TESTIMONY

Bufile # _____

(circle one) Court Grand Jury Other - _____

Dates _____

Supporting: (circle one) Bureau Federal Local Workdays _____

City & State _____ Category 1 2 3 4

Testified? ☐ Yes ☐ No If No, then circle Reason Below for Appearing in Court but not Testifying.

01. Guilty Plea

03. Case Dismissed

05. Testimony not Needed

02. Case Continued

04. Stipulation

06. Mistrial

07. Other _____

Results of Trial _____ Judge _____

Prosecuting Attorney _____ Defense Attorney _____

OTHER COMMITMENTS

Bufile #

80-612

City & State

WASHINGTON DC

Agency

FBI

Dates

10/21/85

(circle one)

Bureau

Federal

Local

Workdays

1

Purpose: (circle one)

01. Lecture/Training (Others)

01A. Tours, Training, etc., at FBIHQ

02. Training (Self)

03. Speech

04. Pretrial Conference

05. Field Examination of Evidence

06. Research/Data Acquisition

07. _____

08. Investigative Support

09. Communication Support

10. Conference/Meeting

11. Deposition

80-612 -

Details/Unusual or Interesting Circumstances

NOT RECORDED

17 NOV 19 1985

11 DEC 2 1985

SEVEN

Memorandum



To : FBI Laboratory Division
Evidence Control Center
Room 3223, TL 241

OCT 18 5 ENT

Date

9/18/85

From : SA

Section & Symbol DUEb6
b7C

Subject :

NEW YORK SPECIAL

b7E

TESTIMONY

Bufile # _____
(circle one) Court Grand Jury Other - _____ Dates _____
Supporting: (circle one) Bureau Federal Local Workdays _____
City & State _____ Category 1 2 3 4
Testified? ☐ Yes ☐ No If No, then circle Reason Below for Appearing in Court but not Testifying.
01. Guilty Plea 03. Case Dismissed 05. Testimony not Needed
02. Case Continued 04. Stipulation 06. Mistrial
07. Other _____

Results of Trial _____ Judge _____
Prosecuting Attorney _____ Defense Attorney _____

OTHER COMMITMENTS

80-612

Bufile # _____
Agency FBI
(circle one) Bureau Federal Local

City & State N.Y., N.Y.
Dates 9/14-15/85
Workdays 2 0 (Ecc/wh)

Purpose: (circle one)
01. Lecture/Training (Others)
01A. Tours, Training, etc., at FBIHQ
02. Training (Self)
03. Speech
04. Pretrial Conference
05. Field Examination of Evidence

06. Research/Data Acquisition.
07. _____
08 Investigative Support
09. Communication Support
10. Conference/Meeting
11. Deposition

NOT RECORDED

4 NOV 20 1985

Details/Unusual or Interesting Circumstances

77 NOV 27 1985

SEVEN

Memorandum



To : FBI Laboratory Division
Evidence Control Center
Room 3223, TL 241

Date 4/25/85

From : SA [redacted]

Section & Symbol *Special Project* b6
QC b7C

Subject : *Special Laboratory Support*
New York Div.

b7E

TESTIMONY

Bufile # _____
(circle one) Court Grand Jury Other - _____ Dates _____
Supporting: (circle one) Bureau Federal Local Workdays _____
City & State _____ Category 1 2 3 4
Testified? ☐ Yes ☐ No If No, then circle Reason Below for Appearing in Court but not Testifying.
01. Guilty Plea 03. Case Dismissed 05. Testimony not Needed
02. Case Continued 04. Stipulation 06. Mistrial
07. Other _____

Results of Trial _____ Judge _____
Prosecuting Attorney _____ Defense Attorney _____

OTHER COMMITMENTS

Bufile # *80-612* City & State *New York City*
Agency *FBI* Dates *4/20-22/85*
(circle one) Bureau Federal Local Workdays *3*

Purpose: (circle one)
01. Lecture/Training (Others) 06. Research/Data Acquisition
01A. Tours, Training, etc., at FBIHQ 07. _____
02. Training (Self) 08. Investigative Support
03. Speech 09. Communication Support
04. Pretrial Conference 10. Conference/Meeting
05. Field Examination of Evidence 11. Deposition

Details/Unusual or Interesting Circumstances

\$ 104 Travel

NOT RECORDED

MAY 21 1985

SEVEN

APR 85 EMD

Memorandum

DEC 8 4 ENTB



To : FBI Laboratory Division
Evidence Control Center
Room 3223 TL 241

Date 11/11/84

From :

Section & Symbol

Special Projects
Q Cb6
b7C

Subject :

Special Laboratory Support -
New York Dist

b7E

TESTIMONY

Bufile # _____
(circle one) Court Grand Jury Other - _____ Dates _____
Supporting: (circle one) Bureau Federal Local Workdays _____
City & State _____ Category 1 2 3 4
Testified? ☐ Yes ☐ No If No, then circle Reason Below for Appearing in Court but not Testifying.
01. Guilty Plea 03. Case Dismissed 05. Testimony not Needed
02. Case Continued 04. Stipulation 06. Mistrial
07. Other _____

Results of Trial _____ Judge _____
Prosecuting Attorney _____ Defense Attorney _____

OTHER COMMITMENTS

Bufile # 80-612 City & State New York, N.Y.
Agency FBI Dates 11/9-11/84
(circle one) Bureau Federal Local Workdays 3

Purpose: (circle one)

- | | |
|--------------------------------------|----------------------------------|
| 01. Lecture/Training (Others) | 06. Research/Data Acquisition |
| 01A. Tours, Training, etc., at FBIHQ | 07. _____ |
| 02. Training (Self) | 08. <u>Investigative Support</u> |
| 03. Speech | 09. Communication Support |
| 04. Pretrial Conference | 10. Conference/Meeting |
| 05. Field Examination of Evidence | 11. Deposition |

80-612-

Details/Unusual or Interesting Circumstances

NOT RECD 1010

2 JAN 18 1985

40

57 FEB 11 1985

SEVEN

FBI/DOJ

Memorandum



To : FBI Laboratory Division
Evidence Control Center
Room 3223, TL 241

Date 2/14/84b6
b7cFrom : SA Section & Symbol Special Projects QCSubject : Special Laboratory Support - New York Div.

TESTIMONY

Cryptography

Bufile # _____
 (circle one) Court Grand Jury Other - _____ Dates _____
 Supporting: (circle one) Bureau Federal Local Workdays _____
 City & State _____ Category 1 2 3 4
 Testified? ☐ Yes ☐ No If No, then circle Reason Below for Appearing in Court but not Testifying.
 01. Guilty Plea 03. Case Dismissed 05. Testimony not Needed
 02. Case Continued 04. Stipulation 06. Mistrial
 07. Other _____

Results of Trial _____ Judge _____
 Prosecuting Attorney _____ Defense Attorney _____

OTHER COMMITMENTS

Bufile # 80-612 City & State New York City
 Agency FBI Dates 2/13/84
 (circle one) Bureau Federal Local Workdays 1

* Purpose: (circle one)
 01. Lecture/Training (Others) 06. Research/Data Acquisition
 01A. Tours, Training, etc., at FBIHQ 07. _____
 02. Training (Self) 08. Investigative Support
 03. Speech 09. Communication Support
 04. Pretrial Conference 10. Conference/Meeting
 05. Field Examination of Evidence 11. Deposition

80-612Details/Unusual or Interesting Circumstances NoneTrans - \$86Per Diem \$32.50207
40 APR 3 1984SEVEN

Memorandum



To : FBI Laboratory Division
Evidence Control Center
Room 3223 TL 241

NOV 8 3 ENT

Date 11/8/83

From :

SA [redacted]

Section & Symbol

Special Projects
QCb6
b7C

Subject :

Document Training
F + S

Cryptography

b7E

TESTIMONY

Bufile # _____
(circle one) Court Grand Jury Other - _____ Dates _____
Supporting: (circle one) Bureau Federal Local Workdays _____
City & State _____ Category 1 2 3 4
Testified? ☐ Yes ☐ No If No, then circle Reason Below for Appearing in Court but not Testifying.
01. Guilty Plea 03. Case Dismissed 05. Testimony not Needed
02. Case Continued 04. Stipulation 06. Mistrial
07. Other _____

Results of Trial _____ Judge _____
Prosecuting Attorney _____ Defense Attorney _____

OTHER COMMITMENTS

Bufile # ~~80-612~~ 80-612 City & State Quantico
Agency FBI Dates 10/28/83
(circle one) Bureau Federal Local Workdays 1

Purpose: (circle one)
(01) Lecture/Training (Others)
01A. Tours, Training, etc., at FBIHQ
02. Training (Self)
03. Speech
04. Pretrial Conference
05. Field Examination of Evidence
06. Research/Data Acquisition
07. _____
08. Investigative Support
09. Communication Support
10. Conference/Meeting
11. Deposition

80-612

NOT RECORDED

Details/Unusual or Interesting Circumstances 7 DEC 20 1983

POA - \$26.65
64 FEB 10 1984

BIVEN

1 - Mrs. [redacted]
1 - Miss [redacted]
1 - Mr. [redacted]

b6
b7c

SAC, Los Angeles (66-205)

May 22, 1975

Director, FBI

(80-812)

TECHNICAL EQUIPMENT

PHOTOGRAPHIC

LOS ANGELES DIVISION

Reurlet 5-5-75, and Bulet 5-14-75.

- ☐ Equipment listed below has been received. After repairs have been made it will be returned to your office.
- ☐ Equipment listed below has been repaired and is being returned to your office.
- ☐ Equipment listed below is being shipped to your office for ☐ permanent ☐ temporary assignment. Appropriate inventory changes should be made.
- ☐

Lens, RE Auto Topecor 500mm f5.6

SN 1110219

LS:mcw

NOT RECORDED

5 MAY 27 1975

MAILED 3

MAY 23 1975

A-FBI

54 JUN 2 1975

MAIL ROOM

TELETYPE UNIT

Memorandum

APR 88 EDT

Evidence Control Center



To : FBI Laboratory Division
Evidence Control Center
Room 3233, TL 241

Date 4/25/88

From

Section & Symbol XD - Doc.
0728

b6
b7C

Subject :

*New York Special
FCI Search*

TESTIMONY

Bufile # _____
(circle one) **Court** **Grand Jury** **Other** - _____ Dates _____
Supporting: (circle one) **Bureau** **Federal** **Local** Workdays _____
City & State _____ Category **1 2 3 4**
Testified? ☐ Yes ☐ No If No, then circle Reason Below for Appearing in Court but not Testifying.
01. Guilty Plea 03. Case Dismissed 05. Testimony not Needed
02. Case Continued 04. Stipulation 06. Mistrial
07. Other _____

Results of Trial _____ Judge _____
Prosecuting Attorney _____ Defense Attorney _____

OTHER COMMITMENTS

Bufile # 80-612 City & State New York, New York
Agency FBI Dates 4/23-24/88
(circle one) Bureau **Federal** **Local** Workdays 2

Purpose: (circle one)

01. Lecture/Training (Others)
01A. Tours, Training, etc., at FBIHQ
02. Training (Self)
03. Speech
04. Pretrial Conference
05. Field Examination of Evidence

06. Research/Data Acquisition
07. _____
08 Investigative Support
09. Communication Support
10. Conference/Meeting
11. Deposition

502

Details/Unusual or Interesting Circumstances

NOT RECORDED

7 NOV 18 1988

SEVEN
C/S

FBI/DOJ

Memorandum

APR 88 ENT'D



To : FBI Laboratory Division
Evidence Control Center
Room 3233, TL 241

Date 4/19

From

Section & Symbol uk Doc

0728

b6
b7C

Subject :

Ny special

Cryptography

SSP
CLASS
SRC'D
SER
REC

TESTIMONY

Bufile # _____
(circle one) **Court** **Grand Jury** **Other** - _____ Dates _____
Supporting: (circle one) **Bureau** **Federal** **Local** Workdays _____
City & State _____ Category **1** **2** **3** **4**
Testified? ☐ Yes ☐ No If No, then circle Reason Below for Appearing in Court but not Testifying.
01. Guilty Plea 03. Case Dismissed 05. Testimony not Needed
02. Case Continued 04. Stipulation 06. Mistrial
07. Other _____

Results of Trial _____ Judge _____
Prosecuting Attorney _____ Defense Attorney _____

OTHER COMMITMENTS

Bufile # 80-612 City & State Ny, NY
Agency FBI Dates 4/19/88 + 4/20/88
(circle one) **Bureau** **Federal** **Local** Workdays 11 17

Purpose: (circle one)
01. Lecture/Training (Others) 06. Research/Data Acquisition
01A. Tours, Training, etc., at FBIHQ 07. _____
02. Training (Self) 08. Investigative Support
03. Speech 09. Communication Support
04. Pretrial Conference 10. Conference/Meeting
05. Field Examination of Evidence 11. Deposition

Details/Unusual or Interesting Circumstances

80-612-

NOT RECORDED
16 NOV 18 1988

65 FEB 22 1989

SEVEN
C/S

FBI/DOJ

Memorandum

APR 88 ENT'D



To : *Y/T*
FBI Laboratory Division
Evidence Control Center
Room 3233, TL 241

Date *4/26/88*

From :

Section & Symbol *UK Doc*
*0728*b6
b7C

SSP
CLASS
SRC'D
SER
REC

Subject:

*NY SPECIAL**Cryptography*

TESTIMONY

Bufile # _____
(circle one) **Court** **Grand Jury** **Other** - _____ Dates _____
Supporting: (circle one) **Bureau** **Federal** **Local** Workdays _____
City & State _____ Category **1** **2** **3** **4**
Testified? ☐ Yes ☐ No If No, then circle Reason Below for Appearing in Court but not Testifying.
01. Guilty Plea 03. Case Dismissed 05. Testimony not Needed
02. Case Continued 04. Stipulation 06. Mistrial
07. Other _____

Results of Trial _____ Judge _____
Prosecuting Attorney _____ Defense Attorney _____

OTHER COMMITMENTS

Bufile # *80-612* City & State *NY, NY*
Agency *FBI* Dates *4/23 + 4/24/88*
(circle one) **Bureau** **Federal** **Local** Workdays *0*

Purpose: (circle one)
01. Lecture/Training (Others) 06. Research/Data Acquisition
01A. Tours, Training, etc., at FBIHQ 07. _____
02. Training (Self) **08** Investigative Support
03. Speech 09. Communication Support
04. Pretrial Conference 10. Conference/Meeting
05. Field Examination of Evidence 11. Deposition

Details/Unusual or Interesting Circumstances

80-612-
NOT RECORDED
16 NOV 18 1988

65 FEB 22 1988

SEVEN
CS
FBI/DOJ

Memorandum

① Evidence Control Center



JUN 88 ENT

To KAT
FBI Laboratory Division
Evidence Control Center
Room 3233 TL 241

Date 6-7-88From : SA gmmSection & Symbol UD - Doc. SECb6
b7CSubject: NEW YORK SPECIAL

SSP
CLASS
C'D
R
1-0

CRYPTOGRAPHY

b7E

TESTIMONY

Bufile # _____
(circle one) Court Grand Jury Other - _____ Dates _____
Supporting: (circle one) Bureau Federal Local Workdays _____
City & State _____ Category 1 2 3 4
Testified? ☐ Yes ☐ No If No, then circle Reason Below for Appearing in Court but not Testifying.
01. Guilty Plea 03. Case Dismissed 05. Testimony not Needed
02. Case Continued 04. Stipulation 06. Mistrial
07. Other _____

Results of Trial _____ Judge _____
Prosecuting Attorney _____ Defense Attorney _____

OTHER COMMITMENTS

Bufile # 80-612 City & State NEW YORK, N.Y.
Agency FBI Dates 6-2 thru 6-3-88
(circle one) Bureau Federal Local Workdays 2

Purpose: (circle one)

- | | |
|--------------------------------------|----------------------------------|
| 01. Lecture/Training (Others) | 06. Research/Data Acquisition |
| 01A. Tours, Training, etc., at FBIHQ | 07. _____ |
| 02. Training (Self) | <u>08. Investigative Support</u> |
| 03. Speech | 09. Communication Support |
| 04. Pretrial Conference | 10. Conference/Meeting |
| 05. Field Examination of Evidence | 11. Deposition |

80-612

Details/Unusual or Interesting Circumstances

16 MAY 11 1988

SEVEN
C/S