Q. E. D.—2 Hours, 41 Minutes

BY LAMBROS D. CALLIMAHOS

Unclassified

An account of the solution by William F. Friedman[1] *of a test message, enciphered on the presumably "impregnable" Kryha cipher machine and sent to the War Department in the days when the Army's entire cryptologic organization consisted of just five people.*

On January 4, 1933, a lawyer in New York City named Robert C. Birkhahn entered into correspondence with the Office of the Chief Signal Officer on behalf of a client, A. M. Evalenko, who bought (for $100,000, no less!) the North American rights to a cipher machine invented in 1924 by Alexander von Kryha of Germany. In that letter, addressed to Mr. Friedman, Birkhahn praised the machine, saying that it had been used extensively for over two years by governmental departments and commercial firms abroad who had adopted it only after "repeated attempts by leading experts" to solve it. His closing challenge, "Will gladly send you a two hundred word message to decipher, if you are interested in making the attempt and believe that you may succeed where the European experts failed," was to be repeated in subsequent letters.

The reply from the Signal Corps was courteous, but brief; on January 6 Major Spencer B. Akin (later to become the Chief Signal Officer) wrote:

> "This device came to the attention of this office some time ago and a study was made of it to determine its merits for use in the military service. However, the provisions of Army Regulations prevent us from making available to the public the results of our studies on such matters."

Right back from Birkhahn came a rebuttal on January 9:

> "While the provision of the Army of Regulations [sic] to which you refer, is of course understandable, may I venture to note that my client and I are not the 'public.' As a member of the Bar, I am accustomed to conveying and re-

[1] For the benefit of those who are newcomers to the National Security Agency, William F. Friedman (1891–1969) was the dean of modern American cryptologists, the most eminent pioneer in the application of scientific principles to cryptology who laid the foundation for present-day concepts. He retired from NSA in 1955, after 35 years of service with U.S. cryptologic activities, and died at the age of 78 at his home in Washington, D.C. His impressive curriculum vitae *in extenso* may be found on p. 107 of the *NSA Technical Journal*, Vol. XVIII, No. 3, Summer 1973.

ceiving communications in strictest confidence and I believe that any comment from your office on the result of the study of the device could not logically be deemed a violation of the Army of Regulations."

On the same day Birkhahn sent a brief letter to Mr. Friedman:

"I am informed that you are the author of the article on 'Codes and Ciphers' appearing in the 14th edition of the Encyclopaedia Britannica. You stated therein,

'There is at least one cipher system which may be mathematically demonstrated [here Birkhahn inadvertently dropped some words] without the specific key, even though the basic method be completely unknown.'

Please let me know whether you had reference to the Kryha Coding Machine and, if not, what was the device. Thank you."

From Friedman on January 13 came the answer:

"In reply to your query as to whether this statement refers to the Kryha Coding Machine, I beg leave to call your attention to the fact that the statement does not refer to a 'device' but to a 'system.' There need be no hesitancy in my telling you, firstly, that the system I mean is one in which a random-mixed, unintelligible, nonrepeating sequence of elements is used as the key for encipherment, this key being coincident in length with the text to be enciphered; and secondly, that so far as I am aware, there has not yet been placed upon the market any practical device embodying or based upon such a system of cryptography."

Not one to lose any time, Birkhahn wrote to Friedman on January 16:

"Although not a cryptologist may I, nevertheless, venture the opinion that, a 'system' in which 'random-mixed, unintelligible, non-repeating sequence of elements is used as the key for encipherment, this key being coincident in length with the text to be enciphered,' is correctly and fully descriptive of the system upon which the Kryha Coding Machine operates."

Birkhahn then concluded with

"I shall be only too happy to submit a 200 word cipher statement to be deciphered without the aid of the machine; or, for that matter, with the aid of the machine but without prior knowledge of the particular key on which the text was enciphered."

Busy as a little bee, Birkhahn also wrote to Major Akin on the same day, repeating his offer of a 200-word test of the machine. An interim reply was sent by Major Akin to Birkhahn on January 20, acknowledging receipt of his letter and saying that a detailed reply would be made within a very few days.

On January 24 Major Akin sent to Birkhahn the following letter, quoted in its entirety:

"The descriptive pamphlet accompanying your letter of January 16, 1933, has been examined and found applicable to the Kryha model studied by this office several years ago .

Your letter of January 9 indicates that the purpose of your entering into communication with this office on the subject of the Kryha cipher machine is to bring the latter to our attention and to present its merits for consideration for use in the military service.

As noted in the first paragraph of this letter as well as in our letter of January 6, however, this device has already been studied and, I regret to advise, was found unsuitable for adoption in the military service.

The principal defects which our studies disclosed are two in number. The first and major defect is that the degree of cryptographic security afforded by the machine is not sufficient for military usage. For your own information, I may add in this connection that the interesting study made by the German Professor, Dr. Georg Hamel, whose quite technical brochure has been examined by this office, shows that although he is an excellent mathematician, his knowledge of the science of cryptanalysis is rather limited. His study is based solely upon the number of permutations and combinations which the Kryha machine affords; but unfortunately, the number of permutations and combinations which a given cryptographic system or device affords is by no means an index of the cryptographic security of the messages produced by the system or device; in some cases, indeed, the relationship may be rather remote and of little significance.

The second defect which the Kryha device presents for military use is its comparative slowness of operation. One of the principal assumptions upon which the adoption of an *automatic* cipher device for military usage is predicated is that it will perform the cryptographic operations much more rapidly than they can be performed by hand. This means that automatic encipherment and decipherment should be effected at the rate of 100 or more characters per minute, or, if possible, as fast as an average typist can operate a typewriter keyboard. This rate of speed is, of course, far beyond that possible on the Standard or Lilliput Models of the Kryha machine. It is noted that the rate of speed of the electrically-operated model is stated as being 'about 300 letters per minute', which is excellent, but this advantage is quite counter-balanced by the cryptographic insecurity of the system for military use, since it is also noted that the cryptographic principle is the same in all three models.

It is realized, of course, that our statements regarding the cryptographic weakness of the Kryha system will be met with some scepticism on your part, and although this office hesitates to depart from a procedure which has proved most practicable over a long period, it is willing to bring this correspondence to what is hoped will be a mutually satisfactory close by endeavoring, in your own words, 'to decipher a statement of approximately 200 words ciphered on this machine'. All it asks is your assurance that the cipher text submitted for test represents a continuous, intelligible statement of the length indicated, in good English, enciphered on the Kryha machine in exact accordance with the instructions set forth in the descriptive pamphlet and that the cryptographic letters have been carefully checked on the machine and found to be correct by actual decipherment by a second party. If convenient, the cipher message should be submitted in triplicate.

In undertaking such a test, it is understood, of course, that this office makes no commitment as to its future course of action in any respect whatsoever. It will endeavor to find time for the study so as not to interfere with the regular course of official business, and hence can make no preliminary statement as to when a report on this matter may be expected. Finally, it is necessary to in-

dicate that, should it turn out that the test message cannot be deciphered within a reasonable length of time, such a failure will in and of itself alone constitute no basis for representations with a view to pressing the adoption of the machine by the War Department."

The die was cast, and Birkhahn's challenge was accepted.

On February 23 Birkhahn sent to Major Akin a letter enclosing a cipher message of 1135 letters in triplicate as had been requested. The letter was received the next day and was date-time stamped "Feb 24 AM 11:13." Since time was of the essence, the cipher message was stamped first, and thus was recorded as one minute earlier, at 11:12 A.M., with the notation in Mr. Friedman's handwriting, "Commenced work. W.F.F." On another part of the message was the pixie-ish observation, "Time out during lunch period, 50 minutes. W.F.F." And then, over the date-time stamp "Feb 24 PM 2:43," was the cryptic (what a happy word!) notation, "Solved. W.F.F." Elapsed time: 3 hours and 31 minutes, less 50 minutes for lunch—2 hours and 41 minutes! (In Fig. 1 is shown the upper part of the cipher message, including the notations and decipherment of the message beginning.)

That afternoon the following letter was sent to Birkhahn signed by Colonel G. S. Kumpe, Excutive Officer in the Office of the Chief Signal Officer:

"Receipt of your letter of February 23, 1933, enclosing a test message prepared by you on the Kryha Cipher Machine in accordance with our letter of January 24, 1933, is acknowledged.

The solution of the aforesaid message was accomplished in approximately two and a half hours, as shown by the time stamp indications on the copy being returned herewith. You will no doubt agree that a complete translation would be unnecessary, since this involves mere clerical work after the alphabets and initial position have been determined.

The cipher alphabets used by you were as follows:

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

The initial position of the toothed cipher wheel was 15.

It is felt that the statements made in our letter of January 24 with regard to the cryptographic security of this model of the Kryha machine are fully substantiated by the present demonstration.

The Chief Signal Officer desires to thank you for the opportunity you have afforded for testing in a practical manner theoretical studies made some time ago."

With the letter was enclosed one of Birkhahn's copies of the test message, with the plain text of the first four lines filled in as in Fig. 1.

Birkhahn wrote to Colonel Kumpe on March 3, expressing his admiration for the solution, particularly since he was informed that leading foreign cryptanalysts had proclaimed the Kryha machine cryptographically secure.

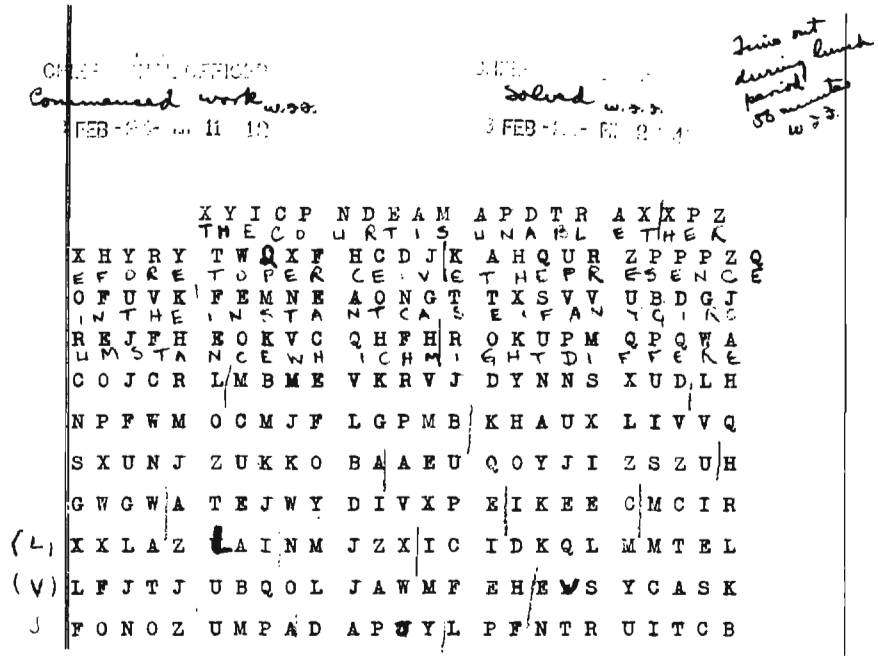


Figure 1

Mr. Friedman now prepared the following memorandum for Major Akin's signature:

> "During the months of January and February this office engaged in some correspondence with Mr. Robert C. Birkhahn, counsel for the American owner of the U.S. rights to the Kryha cipher machine, a cryptographic device originated and marketed in Europe by a German manufacturer. As a result of this correspondence, during the course of which this office indicated that it had already studied this machine and had found that the degree of cryptographic security afforded by it was not sufficiently great for military use, Mr. Birkhahn issued what was tantamount to a challenge to solve a 200-word message enciphered upon his machine, with keys, settings, and alphabets known only to him. The challenge was accepted by this office and on February 24 the cryptogram was received. It was solved within two and a half hours, and the solution was placed in the outgoing mail in the afternoon of the same day, together with a letter giving the key and the alphabets used.
>
> The cryptographic principles upon which the machine operates are of a somewhat more complicated type than is usually the case with devices of this charater. This machine employs a key that is irregular in its functioning, and 442 elements in length, controlling the successive displacements of two variable alphabets that can be constructed at will. Under ordinary circumstances, a single cryptanalyst working alone, no matter how skillful he might be, would require at least 24 to 26 hours to solve such a message. In this case a team of three trained junior cryptanalysts were assigned the problem, under the direction of the principal cryptanalyst. The speed with which the solution was ac-

> complished in this case shows what proper organization, effective coordination, and experienced direction of trained cryptanalysts can accomplish."

This memorandum was sent to the Chief of the Military Intelligence Division, G-2, who forwarded it on March 28 to the Deputy Chief of Staff of the Army with the following note:

> "You will find this very interesting—and I hope we can meet the requests of the Chief Signal Officer for development of his Signal Intelligence Section, personnel and funds for research and construction of the additional codes as per recent programs."

As a result of this happy solution the Signal Intelligence Section gained renewed respect—and, far more important—recognition at the highest Army levels and increased fiscal support.

This solution in 2 hours and 41 minutes is remarkable not only because of the absence of any machine aids at that time,[2] but particularly so for the light it throws on Mr. Friedman's direction and organization of the cryptologic effort of the three junior cryptanalysts, Solomon Kullback, Frank B. Rowlett, and Abraham Sinkov, who had been recruited by him in April 1930 as the nucleus of an expanded Signal Intelligence Section.[3]

For those readers wishing to try their own hand at the solution, there is given below in Fig. 2 the entire text of the cipher message. (It took the present author the better part of a working day to solve the test message by hand, going through all the steps of the 1933 solution without recourse to any machine aids.[4]) For the impatient reader, the detailed steps of the solution are shown in the Appendix which follows.

---

[2] It was not until 1936 that the Army obtained its first IBM data processing machines for cryptologic purposes.

[3] And what a nucleus it was! Until April 1, 1930, the Signal Intelligence Section consisted only of Mr. Friedman and one clerk-typist. Kullback, Rowlett, and Sinkov joined the staff during that first week in April and were to remain in cryptologic work, making notable contributions for over three decades and rising to high positions in NSA and its predecessor organizations. Kullback became Assistant Director, NSA, for Research and Development in 1958 and retired in 1962; Rowlett became Special Assistant to the Director, NSA, in 1958, and the National Cryptologic School's first Commandant for two months just before he retired at the end of December 1965; and Sinkov became Technical Director of NSA's Production Organization in 1952, retiring in 1962.

[4] A philosophical question: if one man can solve a cryptogram in a unit length of time, can n men solve it in $\frac{1}{n}$ th of the time?

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

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

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

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

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

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

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

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

Figure 2

Appendix

The original Kryha machine of 1924 is a spring-operated polyalphabetic cipher machine which has as its principle the irregular displacement of two concentric disks which comprise the plain and cipher components. (Actually, the cipher component is a 52-element disk while the plain component is in the shape of a semicircular frame juxtaposed against the revolving cipher component.) The letters of the two components are printed on small metal tabs which are inserted in slots on the two disks so that the sequence of the letters in the components may be varied according to prearranged keys. The displacement of the alphabets occurring after each encipherment is accomplished through a selector wheel having on its periphery 17 toothed sectors consisting of from one to six teeth each, the sectors being designated by the numbers 1–17. These teeth serve to displace the components a distance equivalent to the number of teeth in the sector; however, owing to the manner of spacing between the toothed portions of the wheel, an additional displacement of four positions is added at each operation of the machine. The selector wheel has the following effective displacements between its 17 numbered positions:

Position:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	1
Displacement:	7	6	7	5	6	7	6	8	6	10	5	6	5	7	6	5	9	

Since the sum of these displacements is 111 ($\equiv$ 7, mod 26) it follows that after a complete revolution of the selector wheel the cipher component will be displaced 7 positions to the left from its original juxtaposition; and since this number, 7, is prime to 26, there will be 26 series of 17 displacements each, making the period of the machine $17 \times 26 = 442$. (A subsequent model of the Kryha machine incorporated a selector wheel with 52 adjustable screws or "stops," each screw having the function of bringing into play a particular displacement, of at least 3, of the alphabets. Any combination of these 52 screws could be used to generate a series of successive displacements which summed to 179 or 23, mod 26.)

As an illustration of encipherment, let us assume that the components of the machine have been arranged as follows:

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

If the initial juxtaposition of the components is that shown above (i.e., in the key of H), the first plaintext letter is enciphered in the H alphabet, and a stepping button is pressed to bring the next alphabet into position. If the setting of the selector wheel was at position 1 at the beginning of the encipherment, the next alphabet to be brought into play

will be 7 to the right of the first or H alphabet (i.e., the 8th or I alphabet), and the one after that will be 6 places to the right of the I alphabet (i.e., the 14th or J alphabet), and so on. At the end of 17 encipherments the alphabets shall have been displaced 111 ($\equiv$ 7, mod 26), positions relative to the initial setting, so that the key series 1, 8, 14 . . . becomes the isomorphic equivalent 8, 15, 21 . . .; in other words, the elements in each succeeding row are 7 more than the corresponding elements in the preceding row. The first five rows of 17 elements of the key are shown in the diagram below:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
7	6	7	5	6	7	6	8	6	10	5	6	5	7	6	5	9
1	8	14	21	26	6	13	19	1	7	17	22	2	7	14	20	25
8	15	21	2	7	13	20	26	8	14	24	3	9	14	21	1	6
15	22	2	9	14	20	1	7	15	21	5	10	16	21	2	8	13
22	3	9	16	21	1	8	14	22	2	12	17	23	2	9	15	20
3	10	16	23	2	8	15	21	3	9	19	24	4	9	16	22	1 . . .

Translating the foregoing numbers into literal form as 1 = A, 2 = B, . . . 26 = Z for typographic convenience, we obtain the complete key diagram as shown in Fig. 3:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
	7	6	7	5	6	7	6	8	6	10	5	6	5	7	6	5	9
Ⓐ	H	N	U	Z	F	M	S	Ⓐ	G	Q	V	B	G	N	T	Y
H	O	U	B	G	M	T	Z	H	N	X	C	I	N	U	Ⓐ	F
O	V	B	I	N	T	Ⓐ	G	O	U	E	J	P	U	B	H	M
V	C	I	P	U	Ⓐ	H	N	V	B	L	Q	W	B	I	O	T
C	J	P	W	B	H	O	U	C	I	S	X	D	I	P	V	A
J	Q	W	D	I	O	V	B	J	P	Z	E	K	P	W	C	H
Q	X	D	K	P	V	C	I	Q	W	G	L	R	W	D	J	O
X	E	K	R	W	C	J	P	X	D	N	S	Y	D	K	Q	V
E	L	R	Y	D	J	Q	W	E	K	U	Z	F	K	R	X	C
L	S	Y	F	K	Q	X	D	L	R	B	G	M	R	Y	E	J
S	Z	F	M	R	X	E	K	S	Y	I	N	T	Y	F	L	Q
Z	G	M	T	Y	E	L	R	Z	F	P	U	A	F	M	S	X
G	N	T	A	F	L	S	Y	G	M	W	B	H	M	T	Z	E
N	U	A	H	M	S	Z	F	N	T	D	I	O	T	A	G	L
U	B	H	O	T	Z	G	M	U	A	K	P	V	A	H	N	S
B	I	O	V	A	G	N	T	B	H	R	W	C	H	O	U	Z
I	P	V	C	H	N	U	A	I	O	Y	D	J	O	V	B	G
P	W	C	J	O	U	B	H	P	V	F	K	Q	V	C	I	N
W	D	J	Q	V	B	I	O	W	C	M	R	X	C	J	P	U
D	K	Q	X	C	I	P	V	D	J	T	Y	E	J	Q	W	B
K	R	X	E	J	P	W	C	K	Q	A	F	L	Q	X	D	I
R	Y	E	L	Q	W	D	J	R	X	H	M	S	X	E	K	P
Y	F	L	S	X	D	K	Q	Y	E	O	T	Z	E	L	R	W
F	M	S	Z	E	K	R	X	F	L	V	A	G	L	S	Y	D
M	T	Z	G	L	R	Y	E	M	S	C	H	N	S	Z	F	K
T	A	G	N	S	Y	F	L	T	Z	J	O	U	Z	G	M	R
A	H	N	U	Z	. . .											

Figure 3

Now if a message were encrypted starting at, say, position 1 of the selector wheel and "alphabet 1" of the enciphering components, it is clear from Fig. 3 that the 1st, 9th, 33d, 42d, and 58th letters, for example, would be enciphered in the key of A, and would therefore belong to one monoalphabetic distribution; it may also be seen that, owing to the isomorphism of the key, even if a different initial alphabet were used (take any other letter in the first column of Fig. 3), as long as the selector wheel was set at position 1 the 1st, 9th, 33d, 42d, and 58th letters would still be monoalphabetically distributed. Thus for a particular starting position of the selector wheel there are 26 distributions that come into consideration, one for each (unknown) key letter. Thus in analysis 17 sets of 26 distributions each would have to be made, and the

correct initial position of the selector wheel would be that in which all 26 distributions of one of the 17 sets revealed a close approximation to the expected δ I.C. for the language in question.

In the 1933 solution the method was to allocate the cipher letters of column 1 (considering the text to have been written out in a block consisting of rows of 17 letters) into 26 distributions; each succeeding letter in the column was recorded in a distribution 7 away from its predecessor because of the +7 isomorphic progression of the key, so that the letters of column 1 would go into distributions 1, 8, 15, 22, 3. . . . Then the letters of column 2 would likewise be allocated into the same distributions, but starting with the proper distribution for the first letter of column 2 (which depends upon the selector position used for the first letter of column 1). For example, with selector position 1 the keying sequence is that shown in line (1) of Fig. 4, below; so the first letter

```
     1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17
        7  6  7  5  6  7  6  8  6 10  5  6  5  7  6  5  9
(1)  1  8 14 21 26  6 13 19  1  7 17 22  2  7 14 20 25
     8 15 21  2  7 ...

(2)     1  7 14 19 25  6 12 20 26 10 15 21 26  7 13 18
     1  8 14 21 26  6...

                        * * * * *

(17)                                                 1
    10 17 23  4  9 15 22  2 10 16 26  5 11 16 23  3  8
    17 24  4 11 ...
```

Figure 4

of column 2 would be put into the 8th distribution, the first letter of column 3 into the 14th distribution, and so on to the first letter of column 17 which would be placed into the 25th distribution. In testing for initial selector position 2, the keying sequence is that shown in line (2) of Fig. 4; so if the first letter of column 1 is arbitrarily put into distribution 1, the first letter of column 2 would be put into the 7th distribution, the first letter of column 3 into the 14th distribution, and so on to the first letter of the last column which would be placed into the 1st distribution. Finally, in testing for initial selector position 17 with the keying sequence shown in line (17) of Fig. 4, the first letter of column 1 would be put into distribution 1, while the first letter of the last column would go into distribution 3.

A much easier and quicker way of making the distributions presents itself, using a grille to be placed over the cipher text which is to be writ-

ten in a block of 17-letter rows. Using the key diagram of Fig. 3, we cut holes into our grille at the locations of any arbitrary key letter, say the letter A, as shown in Fig. 5, below. We then complete the grille as illustrated in Fig. 6, with the necessary cyclically offset portion shown in dotted lines, and the grille doubled in length for convenience in use. (The heavy circles show the index or reference position used in designating the placement of the grille over the cipher text.)

We now place the grille so that the index position is over the first letter of the cipher text, as illustrated in Fig. 7 (only the top 40 of the 67 lines are shown here), and we make the following distribution of the letters exposed through the apertures:

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	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17									
	7		6		7		5		6		7		6		8		6		10		5		6		5		7		6		5		9
(A)	H	N	U	Z	F	M	S	(A)	G	Q	V	B	G	N	T	Y									
H	O	U	B	G	M	T	Z	H	N	X	C	I	N	U	(A)	F									
O	V	B	I	N	T	(A)	G	O	U	E	J	P	U	B	H	M									
V	C	I	P	U	(A)	H	N	V	B	L	Q	W	B	I	O	T									
C	J	P	W	B	H	O	U	C	I	S	X	D	I	P	V	(A)									
J	Q	W	D	I	O	V	B	J	P	Z	E	K	P	W	C	H									
Q	X	D	K	P	V	C	I	Q	W	G	L	R	W	D	J	O									
X	E	K	R	W	C	J	P	X	D	N	S	Y	D	K	Q	V									
E	L	R	Y	D	J	Q	W	E	K	U	Z	F	K	R	X	C									
L	S	Y	F	K	Q	X	D	L	R	B	G	M	R	Y	E	J									
S	Z	F	M	R	X	E	K	S	Y	I	N	T	Y	F	L	Q									
Z	G	M	T	Y	E	L	R	Z	F	P	U	(A)	F	M	S	X									
G	N	T	(A)	F	L	S	Y	G	M	W	B	H	M	T	Z	E									
N	U	(A)	H	M	S	Z	F	N	T	D	I	O	T	(A)	G	L									
U	B	H	O	T	Z	G	M	U	(A)	K	P	V	(A)	H	N	S									
B	I	O	V	(A)	G	N	T	B	H	R	W	C	H	O	U	Z									
I	P	V	C	H	N	U	(A)	I	O	Y	D	J	O	V	B	G									
P	W	C	J	O	U	B	H	P	V	F	K	Q	V	C	I	N									
W	D	J	Q	V	B	I	O	W	C	M	R	X	C	J	P	U									
D	K	Q	X	C	I	P	V	D	J	T	Y	E	J	Q	W	B									
K	R	X	E	J	P	W	C	K	Q	(A)	F	L	Q	X	D	I									
R	Y	E	L	Q	W	D	J	R	X	H	M	S	X	E	K	P									
Y	F	L	S	X	D	K	Q	Y	E	O	T	Z	E	L	R	W									
F	M	S	Z	E	K	R	X	F	L	V	(A)	G	L	S	Y	D									
M	T	Z	G	L	R	Y	E	M	S	C	H	N	S	Z	F	K									
T	(A)	G	N	S	Y	F	L	T	Z	J	O	U	Z	G	M	R									
(A)	H	N	U	Z	...																				

Figure 5

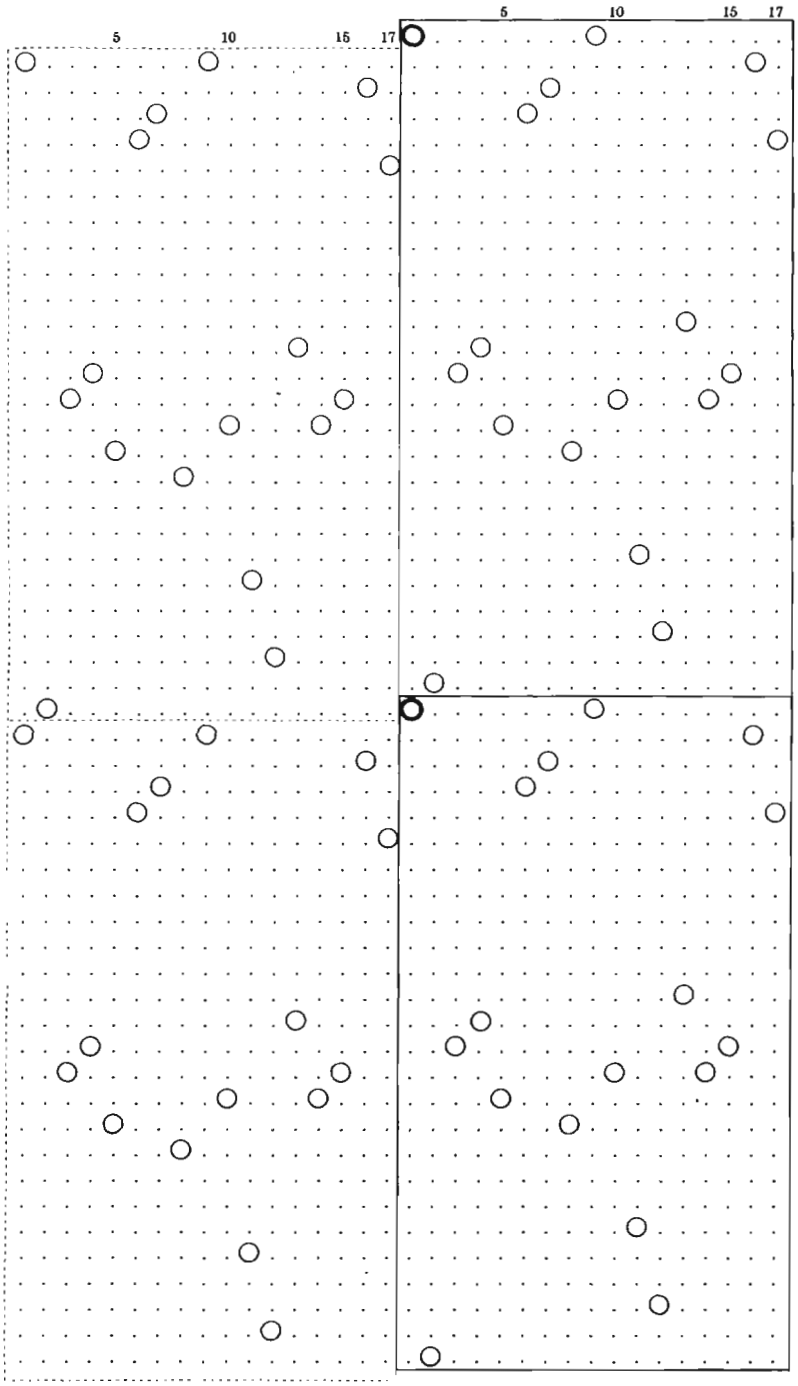


Figure 6

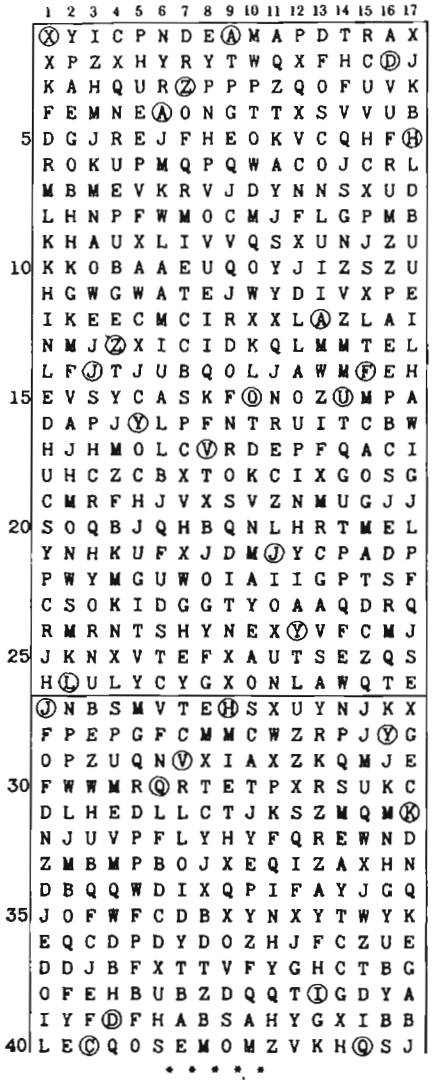


Figure 7

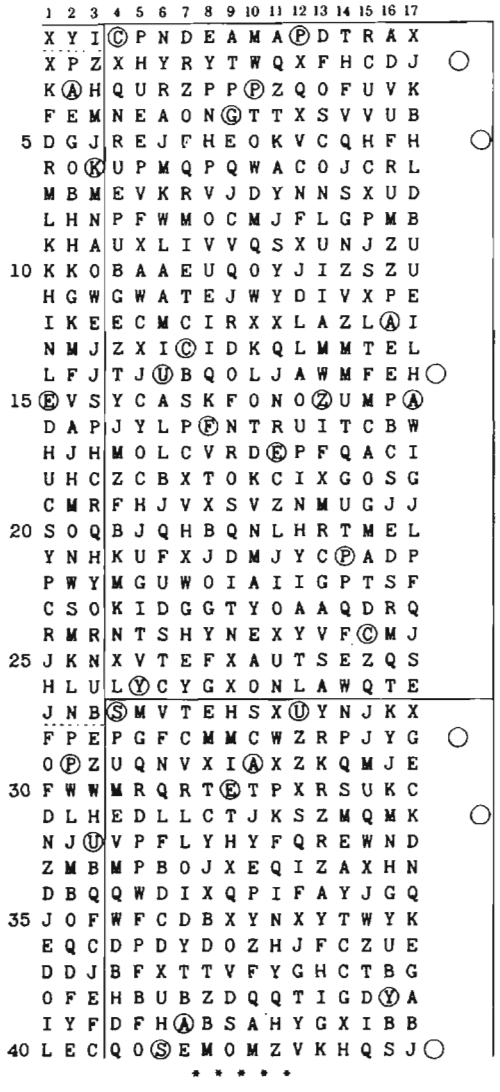
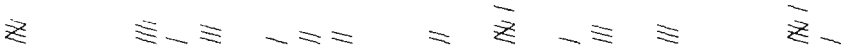

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
X Y I C P N D E A M A P D T R A X
X P Z X H Y R Y T W Q X F H C D J
K A H Q U R Z P P P Z Q O F U V K
F E M N E A O N G T T X S V V U B
5 D G J R E J F H E O K V C Q H F H
R O K U P M Q P Q W A C O J C R L
M B M E V K R V J D Y N N S X U D
L H N P F W M O C M J F L G P M B
K H A U X L I V V Q S X U N J Z U
10 K K O B A A E U Q O Y J I Z S Z U
H G W G W A T E J W Y D I V X P E
I K E E C M C I R X X L A Z L A I
N M J Z X I C I D K Q L M M T E L
L F J T J U B Q O L J A W M F E H
15 E V S Y C A S K F O N O Z U M P A
D A P J Y L P F N T R U I T C B W
H J H M O L C V R D E P F Q A C I
U H C Z C B X T O K C I X G O S G
C M R F H J V X S V Z N M U G J J
20 S O Q B J Q H B Q N L H R T M E L
Y N H K U F X J D M J Y C P A D P
P W Y M G U W O I A I I G P T S F
C S O K I D G G T Y O A A Q D R Q
R M R N T S H Y N E X Y V F C M J
25 J K N X V T E F X A U T S E Z Q S
H L U L Y C Y G X O N L A W Q T E
J N B S M V T E H S X U Y N J K X
F P E P G F C M M C W Z R P J Y G
O P Z U Q N V X I A X Z K Q M J E
30 F W W M R Q R T E T P X R S U K C
D L H E D L L C T J K S Z M Q M K
N J U V P F L Y H Y F Q R E W N D
Z M B M P B O J X E Q I Z A X H N
D B Q Q W D I X Q P I F A Y J G Q
35 J O F W F C D B X Y N X Y T W Y K
E Q C D P D Y D O Z H J F C Z U E
D D J B F X T T V F Y G H C T B G
O F E H B U B Z D Q Q T I G D Y A
I Y F D F H A B S A H Y G X I B B
40 L E C Q O S E M O M Z V K H Q S J

Figure 8

This distribution has a δ I.C. of 1.18, nothing to write home about. We then slide the grille over one position to the right, so that the index position is over the second letter of the cipher text, and we arrive at a distribution with an I.C. of 0.95. Sliding the grille so that the index position is over the third letter of the cipher, we obtain a distribution with an I.C. of 0.97. When we slide the grille so that the index position is over the fourth letter of the cipher (as illustrated in fragmentary form in Fig. 8), we obtain the following distribution:



The I.C. of this distribution is 1.79, so now we know that, barring the touch of a Mephistophelian (or rather, Bernoullian) finger, the fourth letter of text was enciphered at position 1 of the selector wheel; therefore, the initial setting for the first letter must have been position 15. In any case, we shall prove or disprove this point very quickly.

If this is the correct initial setting of the selector wheel and we drop the grille vertically one position, the letters exposed through the apertures will still be monoalphabetically distributed, but in an alphabet +7 away from that which we have just obtained above; in other words if, referring to Fig. 5, the letters exposed in Fig. 8 belong to the A or 1st alphabet, then sliding the grille down one position would reveal the letters belonging to the H or 8th alphabet. Sure enough, the I.C. of the distribution of these letters is 1.92, so we know that we are on the right track. By successively sliding the grille down one position at a time in Fig. 8, we obtain the 26 distributions shown in Fig. 9, given together with the numerical designations of these alphabets and their I.C.'s. The average I.C. of these distributions, 1.88, makes us very happy, the expected I.C. for English plain text being 1.73.

The next step, which might appear puzzling at first, is to rewrite the successive columns of Fig. 9 as *rows* of a new matrix for convenience in the matching process on which we are about to embark. This new matrix is shown in Fig. 10, in which the cipher letters are at the left, and tally totals for each row at the right. The frequencies within each row represent the frequencies of the successive plaintext equivalents of the cipher letter designated at the left, and therefore the method of solution bears a close resemblance to that of the classic progressive alphabet cipher in which we match the cipher-letter rows to obtain a statistical reconstruction of the cipher component, regardless of the identity of the plain component.[5]

[5] Cf. L. D. Callimahos and W. F. Friedman, *Military Cryptanalytics, Part II*, pp. 161-168.

	Alph.	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.C.
1.	(21)	5		5		4	1	3		1	2	2			2		6		1	3		3				6	1	1.79
2.	(2)	2	3	2	1	6				2				2		1	5				5		1	6	3		5	1.92
3.	(9)				1	3	1	4	6	1	1	1	3		1	2		7	1	3	1	1	1	1	1		3	1.58
4.	(16)	3			4		2	1		1	4		2	1	2	1	2	3	1			2		4	8	1		1.72
5.	(23)		6	7	2	4	1			1	4			4	2	1	1	1	3	3	1		1					1.87
6.	(4)		1	2	1	1			1	1	7		4	2			2	1	1	2		2	6	4	4			1.78
7.	(11)	1		2		4			2	1				2	4	6	3	5		1	1	2	5	1		3		1.64
8.	(18)					1	8	7	4	1	3	1				2	5	3			1		2		3	1	1	2.19
9.	(25)	1		3	3	2	5	6			1						1	2	1	1		5		6	3	3		1.84
10.	(6)	2	1		4		4				5	2			1			1	4	6			5	3	5			1.96
11.	(13)	4	1		2	1		4			2	3		5		4	5	1	2	4					2	2	1	1.50
12.	(20)	2		1		9	4	1	4		4		2	4		1		1	3		3		1	3		1		1.95
13.	(1)	1	1	4	3	1			2		1		2	6	1	2				4			1		7	7	3	1.96
14.	(8)	2					5	3	1		1		1		3		3	2	3		8		6		4	2	1	1.94
15.	(15)				4	4	3				5	6	1	1	2	7		1	1		6		1			4		1.73
16.	(22)	6	1	10			4		3	2	1	3	1	1	1	1			3	2	1	1			3		1	2.10
17.	(3)	2		2	3		1		1			4		4			2	5	1			1	6			6	6	2.01
18.	(10)	3			2			3		3	6		3	1	3	7			5				3				3	2.05
19.	(17)			4	2		4		1	1		3	3	7	6	2				1	1	1		1	3		3	1.79
20.	(24)	3	5		2		3		8	1		1	6	2	1			2	1		2		2	2		2		1.90
21.	(5)		1		2						3	3			5	4	1		2	5		6		2		8		2.36
22.	(12)	2	2	3		4	3	2	1	4		1	2	2			1	1	2	1	4	5			2		1	1.18
23.	(19)	3			4	2	1	6	5	5		5		2	2			2				1			3		2	1.63
24.	(26)	7	1			1		3	3	6	1	1	2		2	3			2					3	1	5	3	1.76
25.	(7)		2					1		1			2	7	4		1	2		3	13	3		3	1	1	2	2.96
26.	(14)		2	2	3				3	5	2	4	6		2		6		1	2	1		2	4				1.68

Figure 9

	21	2	9	16	23	4	11	18	25	6	13	20	1	8	15	22	3	10	17	24	5	12	19	26	7	14	
A	5	2	-	3	-	-	1	-	1	2	4	2	1	2	-	6	2	3	-	3	-	2	3	7	-	-	49
B	-	3	-	-	6	1	-	-	-	1	1	-	1	-	-	1	-	-	-	5	1	2	-	1	2	2	27
C	5	2	-	-	7	2	2	-	3	-	-	1	4	-	-	10	2	-	4	-	-	3	-	-	-	2	47
D	-	1	1	4	2	1	-	-	3	4	2	-	3	-	4	-	3	2	2	2	2	-	4	-	-	3	43
E	4	6	3	-	4	1	4	1	2	-	1	9	1	-	4	-	-	-	-	-	-	4	2	1	-	-	47
F	1	-	1	2	1	-	-	8	5	4	-	4	-	5	3	4	1	-	4	3	-	3	1	-	-	-	50
G	3	-	4	1	-	-	-	7	6	-	4	1	-	3	-	-	-	3	-	-	-	2	6	3	1	-	44
H	-	-	6	-	-	1	2	4	-	-	-	4	2	1	-	3	1	-	1	8	-	1	5	3	-	3	45
I	1	2	1	1	1	1	1	1	-	-	-	-	-	-	-	2	-	3	1	1	-	4	5	6	1	5	37
J	2	-	1	4	4	7	-	3	1	5	2	4	1	1	5	1	-	6	-	-	3	-	-	1	-	2	53
K	2	-	1	-	-	-	-	1	-	2	3	-	-	-	6	3	4	-	3	1	3	1	5	1	-	4	40
L	-	-	3	2	-	4	-	-	-	-	-	2	2	1	1	1	-	3	3	6	-	2	-	2	2	6	40
M	-	2	-	1	4	2	2	-	-	-	5	4	6	-	1	1	4	1	7	2	-	2	2	-	7	-	53
N	2	-	1	2	2	-	4	-	-	1	-	-	1	3	2	1	-	3	6	1	5	-	2	2	4	2	44
O	-	1	2	1	1	-	6	2	-	-	4	1	2	-	7	1	-	7	2	-	4	-	-	3	-	-	44
P	6	5	-	2	1	2	3	5	1	-	5	-	-	3	-	-	2	-	-	-	1	1	-	-	1	6	44
Q	-	-	7	3	1	1	5	3	2	1	1	1	-	2	1	-	5	-	-	2	-	1	2	-	2	-	40
R	1	-	1	1	3	1	-	-	1	4	2	3	-	3	1	3	1	5	-	1	2	2	-	2	-	1	38
S	3	-	3	-	3	2	1	-	1	6	4	-	4	-	-	2	-	-	1	-	5	1	-	-	3	2	41
T	-	5	1	-	1	-	1	1	-	-	-	3	-	8	6	1	-	-	1	2	-	4	-	-	13	1	48
U	3	-	1	2	-	2	2	-	5	-	-	-	-	-	-	1	1	-	1	-	6	5	1	-	3	-	33
V	-	1	1	-	1	6	5	2	-	5	-	1	1	6	1	-	6	3	-	2	-	-	-	-	-	2	43
W	-	6	1	4	-	4	1	-	6	3	-	3	-	-	-	-	-	-	1	2	2	-	-	3	3	4	43
X	-	3	1	8	-	4	-	3	3	5	2	-	7	4	-	3	-	-	3	-	-	2	3	1	1	-	53
Y	6	-	-	1	-	-	3	1	3	-	2	1	7	2	4	-	6	-	-	2	8	-	-	5	1	-	52
Z	1	5	3	-	-	-	-	1	-	-	1	-	3	1	-	1	6	3	3	-	-	1	2	3	2	-	36

Figure 10

A tabulation is now made of the rows in descending order of total number of tallies, as shown below:

53	52	50	49	48	47	45	44	43	41	40	38	37	36	33	27
J	Y	F	A	T	C	H	G	D	S	K	R	I	Z	U	B
M					E		N	V		L					
X							O	W		Q					
							P								

We begin by matching the heavy J and M rows, and we arrive at the highest ξ I.C., 1.89, for the following juxtaposition:

J [2 - 1 4 4 7 - 3 1 5 2 4 1 1 5 1 - 6 - - 3 - - 1 - 2
M - - - 5 4 6 - 1 1 4 1 7 2 - 2 2 - 7 -[- 2 - 1 4 2 2

The next three heavy distributions, X, Y, and F, are easily added, since the ξ I.C.'s with the J row yield 1.84, 1.82, and 1.83, respectively, for the best matches, as shown below, to-

gether with the columnar sums of the frequencies, labelled $\Sigma(\alpha)$. (The line at the top shows the relative placement of the five letters in the cipher component.)

	J			X															Y			M				F			
J	[2	-	1	4	4	7	-	3	1	5	2	4	1	1	5	1	-	6	-	-	3	-	-	1	-	2]
M	-	-	-	5	4	6	-	1	1	4	1	7	2	-	2	2	-	7	-	[-	2	-	1	4	2	2
X	1	-	[-	3	1	8	-	4	-	3	3	5	2	-	7	4	-	3	-	-	3	-	-	2	3	1
Y	-	2	1	7	2	4	-	6	-	-	2	8	-	-	5	1	-	[6	-	-	1	-	-	3	1	3
F	1	-	-	8	5	4	-	4	-	5	3	4	1	-	4	3	-	3	1	-	-	-	[1	-	1	2
$\Sigma(\alpha)$:	4	2	2	27	16	29	-	18	2	17	11	28	6	1	23	11	-	25	1	-	9	-	2	10	7	10

We now use the summation row, $\Sigma(\alpha)$, as a means of strengthening our results in matching the next five rows, yielding I.C.s of 1.71, 1.96, 1.92, 1.85, and 1.78 for the highest scores, and we obtain a new summation row which we label $\Sigma(\beta)$. This matching is shown below, with the letters in the top row representing, as before, the placement of the letters thus far recovered in the cipher component:

	J		X	E										A		T	Y	H	M			F			C
	4	2	2	27	16	29	-	18	2	17	11	28	6	1	23	11	-	25	1	-	9	-	2	10	7	10
A	1	2	-	6	2	3	-	3	-	2	3	7	-	-	[5	2	-	3	-	-	1	-	1	2	4	2
T	-	3	-	8	6	1	-	-	1	2	-	4	-	-	13	1	[-	5	1	-	1	-	1	1	-	-
C	2	-	-	7	2	2	-	3	-	-	1	4	-	-	10	2	-	4	-	-	3	-	-	-	2	[5
E	1	-	-	[4	6	3	-	4	1	4	1	2	-	1	9	1	-	4	-	-	-	-	-	-	4	2
H	-	-	-	4	2	1	-	3	1	-	1	8	-	1	5	3	-	3	[-	-	6	-	-	1	2	4
$\Sigma(\beta)$:	8	7	2	56	34	39	-	31	5	25	17	53	6	3	65	20	-	44	2	-	20	-	4	14	19	23

Using the $\Sigma(\beta)$ as a base, we are able to match correctly the remaining rows, with ξ I.C.s ranging between 1.64 and 2.13, being helped of course by the fact that no two rows may match flush. The final matching of all the rows is shown in Fig. 11, below. The cipher component as recovered is

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

but knowing that there is a decimation of 7 involved, we find that the original cipher component must have been

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

	J	Q	X	E	P	S	W	G	I	U	B	N	L	Z	A	K	T	Y	H	M	R	D	F	O	V	C
J	2	-	1	4	4	7	-	3	1	5	2	4	1	1	5	1	-	6	-	-	3	-	-	1	-	2
M	-	-	-	5	4	6	-	1	1	4	1	7	2	-	2	2	-	7	-	-	2	-	1	4	2	2
X	1	-	-	3	1	8	-	4	-	3	3	5	2	-	7	4	-	3	-	-	3	-	-	2	3	1
Y	-	2	1	7	2	4	-	6	-	-	2	8	-	-	5	1	-	6	-	-	1	-	-	3	1	3
F	1	-	-	8	5	4	-	4	-	5	3	4	1	-	4	3	-	3	1	-	-	-	1	-	1	2
A	1	2	-	6	2	3	-	3	-	2	3	7	-	-	5	2	-	3	-	-	1	-	1	2	4	2
T	-	3	-	8	6	1	-	-	1	2	-	4	-	-	13	1	-	5	1	-	1	-	1	1	-	-
C	2	-	-	7	2	2	-	3	-	-	1	4	-	-	10	2	-	4	-	-	3	-	-	-	2	5
E	1	-	-	4	6	3	-	4	1	4	1	2	-	1	9	1	-	4	-	-	-	-	-	-	4	2
H	-	-	-	4	2	1	-	3	1	-	1	8	-	1	5	3	-	3	-	-	6	-	-	1	2	4
G	-	-	2	6	3	1	-	3	-	4	1	-	-	-	7	6	-	4	1	-	3	-	-	-	3	-
N	1	-	3	6	1	5	-	2	2	4	2	2	-	1	2	2	-	4	-	-	1	-	-	1	3	2
O	1	1	-	6	2	-	-	4	1	2	-	7	1	-	7	2	-	4	-	-	3	-	-	-	1	2
P	-	-	1	6	6	5	-	2	1	2	3	5	1	-	5	-	-	3	-	-	2	-	-	-	1	1
D	1	-	-	3	4	2	-	3	-	4	-	3	2	2	2	2	-	4	-	-	3	-	1	1	4	2
V	1	-	1	6	5	2	-	5	-	1	1	6	1	-	6	3	-	2	-	-	-	-	-	-	2	-	1
W	2	-	-	3	3	4	-	6	1	4	-	4	1	-	6	3	-	3	-	-	-	-	-	-	-	1	2
S	1	-	-	3	2	3	-	3	-	3	2	1	-	1	6	4	-	4	-	-	2	-	-	1	-	5
K	-	-	-	6	3	4	-	3	1	3	1	5	1	-	4	2	-	1	-	-	-	-	1	-	2	3
L	1	1	-	3	3	6	-	2	-	2	2	6	-	-	3	2	-	4	-	-	-	-	-	2	2	1
Q	-	-	-	7	3	1	1	5	3	2	1	1	1	-	2	1	-	5	-	-	2	-	1	2	-	2
R	-	-	1	4	2	3	-	3	1	3	1	5	-	1	2	2	-	2	-	1	1	-	1	1	3	1
I	1	1	-	4	5	6	1	5	1	2	1	1	1	1	1	1	-	-	-	-	-	-	-	-	2	-	3
Z	1	-	1	6	3	3	-	-	1	2	3	2	-	1	5	3	-	-	-	-	1	-	-	1	-	3
U	-	1	-	6	5	1	-	3	-	3	-	1	2	-	2	2	-	5	-	-	-	-	-	-	1	1
B	-	-	-	5	1	2	-	1	2	2	-	3	-	-	6	1	-	-	-	1	1	-	1	-	-	1

Figure 11

Since we know both the cipher component and its motion, we are now able to reduce the cipher text to monoalphabetic terms, using an arbitrary A-Z sequence for the plain component at the initial setting as shown below:

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

The first cipher letter of the message, X_c, is deciphered as M_p; the second letter, Y_c, involves a shift of the cipher component of 6 positions to the left and is therefore deciphered as F_p; and so on for the reduction of the rest of the text. The reduction of the first 10 of the 67 lines of 17 letters is shown in Fig. 12, together with the distribution of the monoalphabetically converted text.

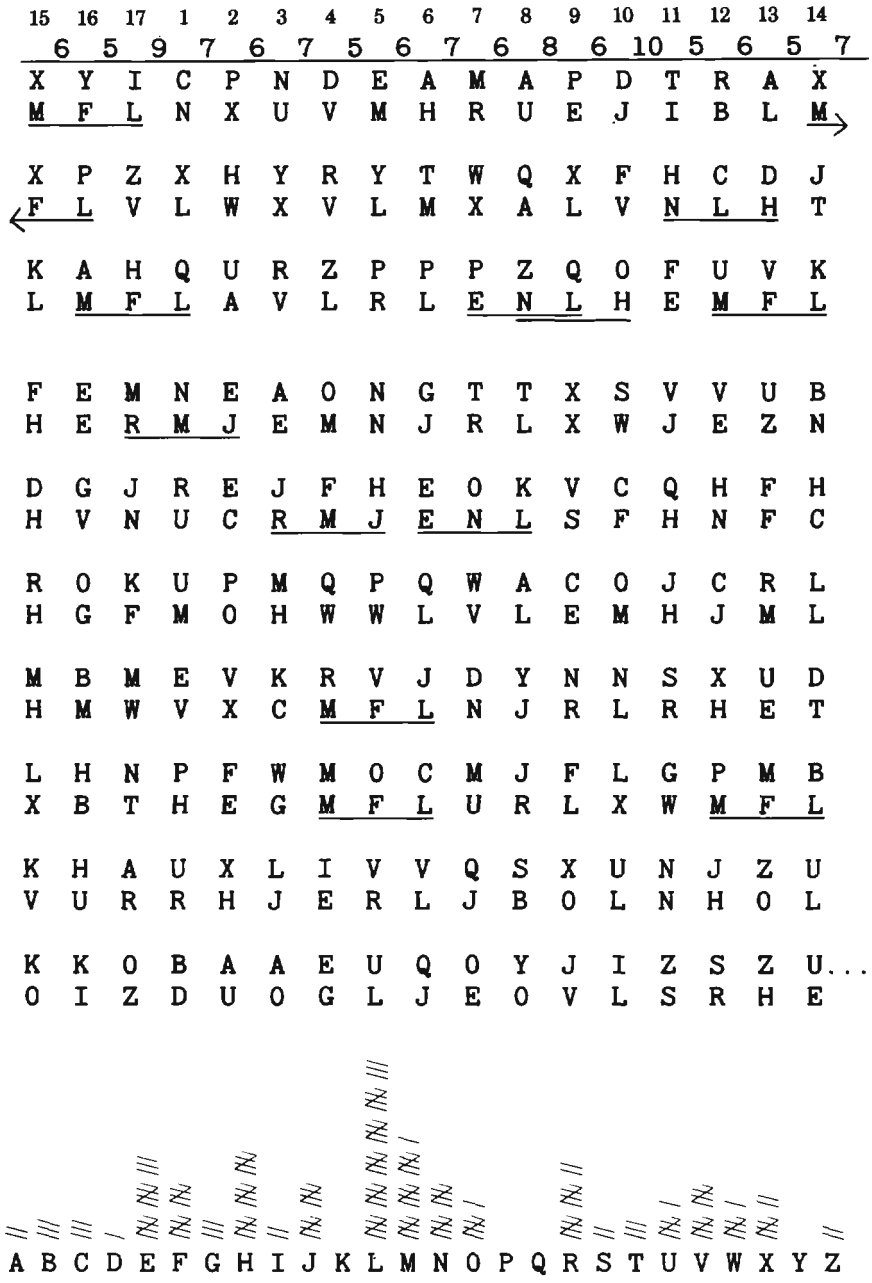

15 16 17 1 2 3 4 5 6 7 8 9 10 11 12 13 14
6 5 9 7 6 7 5 6 7 6 8 6 10 5 6 5 7
X Y I C P N D E A M A P D T R A X
M F L N X U V M H R U E J I B L M
X P Z X H Y R Y T W Q X F H C D J
F L V L W X V L M X A L V N L H T
K A H Q U R Z P P P Z Q O F U V K
L M F L A V L R L E N L H E M F L
F E M N E A O N G T T X S V V U B
H E R M J E M N J R L X W J E Z N
D G J R E J F H E O K V C Q H F H
H V N U C R M J E N L S F H N F C
R O K U P M Q P Q W A C O J C R L
H G F M O H W W L V L E M H J M L
M B M E V K R V J D Y N N S X U D
H M W V X C M F L N J R L R H E T
L H N P F W M O C M J F L G P M B
X B T H E G M F L U R L X W M F L
K H A U X L I V V Q S X U N J Z U
V U R R H J E R L J B O L N H O L
K K O B A A E U Q O Y J I Z S Z U...
O I Z D U O G L J E O V L S R H 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

Figure 12

The simple substitution is now easily solved, beginning with the identification of L_c of the converted text as E_p and the initial trigraph MFL_c as THE_p. The decipherment of the first two rows is shown in the fragment below:

15	16	17	1	2	3	4	5	6	7	8	9	10	11	12	13	14
	6	5	9	7	6	7	5	6	7	6	8	6	10	5	6	5	7
X	Y	I	C	P	N	D	E	A	M	A	P	D	T	R	A	X	
M	F	L	N	X	U	V	M	H	R	U	E	J	I	B	L	M	
T	H	E	C	O	U	R	T	I	S	U	N	A	B	L	E	T	
X	P	Z	X	H	Y	R	Y	T	W	Q	X	F	H	C	D	J...	
F	L	V	L	W	X	V	L	M	X	A	L	V	N	L	H	T	
H	E	R	E	F	O	R	E	T	O	P	E	R	C	E	I	V	

The recovered plain component, set in position against the cipher component for decipherment of the first letter of the text, is as follows:

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

Since the sequences were made up at random (but not too well at that) and since three letters did not occur in the first 170 letters of the plain text, we cannot be certain of the placement of the missing letters in the plain component. (Actually, X_p does occur at the 539th and 647th positions of the text, so this letter could be inserted in its proper place in the plain component, immediately to the left of the S.)

And all this in 2 hours and 41 minutes!