MASSACHUSETTS INSTITUTE OF TECHNOLOGY
CAMBRIDGE 39, MASS.

DEPARTMENT OF MATHEMATICS

Dear Major Grosjean,

I have written RAND concerning the machine description. This was handwritten and was sent to NSA late last spring, I believe, or sent to someone there. Essentially the same machine description was sent to a Navy communication center in Washington, I think.

I have discussed the general machine and ~~theo~~ exponential conjecture with R.C. Blanchfield and A.M. Gleason who have worked for NSA. Recently a conversation with Prof. Hoffman here indicated that he has recently been working on ~~wa~~ a machine with similar objectives. Since he will be consulting for NSA I shall discuss my ideas with him. He has developed minimal redundancy coding methods.

I hope my handwriting, etc. do not give the impression I am just a crank or circle-squarer. My position here is Assist. Prof. of math. My best known work ~~is~~ is in game theory (reprint sent separately). I mention these things only in the interest of securing a most careful consideration of the machine and ideas by your most competent associates.

If the machine description does not turn up. I will prepare another. Also I shall be happy to provide any additional information or answer any queries to the best of my ability.

With <u>many</u> thanks for your prompt reply, I am

Sincerely Yours,

John Nash

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
CAMBRIDGE 39, MASS.

DEPARTMENT OF MATHEMATICS

letter concerns
ENCIPHERING

Dear Sirs:

An enciphering-deciphering machine (in general outline) of my invention has been sent to ~~your~~ your organization by way of the RAND corporation. In this letter I make some remarks on a general principle relevant to enciphering in general and to my machine in particular. This principle seems quite important to me, and I have some reason to believe you may not be fully aware of it.

Consider an enciphering process with a finite "key", operating on binary messages. Specifically, we can assume the process described by a function

$$y_i = F(\alpha_1, \alpha_2, \dots \alpha_r; x_i, x_{i-1}, x_{i-2}, \dots x_{i-n})$$

where the α's, x's, and y's are mod 2 and where if x_i is changed, with the other x's and α's left fixed then y_i is changed.

The x's denote the "key" containing r bits of information. n is the ~~spa~~ maximum span of the "memory" of the process. If n were ∞ the arguments given below would not be basically altered.

To consider the resistance of an enciphering process to being broken we should assume that at same times the enemy knows everything but the key being used and to break it need only discover the key from this information.

We see immediately that ~~at~~ in principle the enemy needs very little information to begin to break down the process. Essentially, as soon as r bits of enciphered message have been transmitted the key is about determined. This is no security, for a practical key should not be too long. But this does not consider how easy or difficult it is for the enemy to make the computation determining the key. If this computation

, although possible in principle, were sufficiently long at best then the process could still be secure in a ~~pract~~ practical ~~se~~ sense.

The most direct computation proceedure would be for the enemy to try all 2^s possible keys, one by one. Obviously this is easily made impractical for the enemy by simply choosing s large enough.

In many cruder types of enciphering, particulary those which are not auto-coding, such as substitution ciphers [letter for letter, letter pair for letter pair, triple for triple..] shorter means for computing the key are feasible, essentially because the key can be determined piece meal, one substitution at a time.

So ~~the~~ a logical way to classify enciphering processes is by the way in which the computation ~~length~~ length for the computation of the key increases with increasing ~~length~~ length of the key. This is at best exponential and at worst probably a relatively small power of r, ar^2 or ar^3, as in substitution ciphers.

Now my general conjecture is as follows: For almost all sufficiently complex types of enciphering, especially ~~to~~ where the ~~information~~ instructions given by different portions of the key interact complexly with each other in the determination of their ultimate effects on the ~~enc~~ enciphering, the mean key computation length increases exponentially with the length of the key, or in other words, with the information content of the key.

The significance of this general conjecture, assuming its truth, is easy to see. It means that it is quite feasible to design ciphers that are effectively unbreakable. ~~and~~ As ciphers become more sophisticated the game of cipher breaking by skilled teams, etc., should become a thing of the past.

The nature of this conjecture is such that I cannot <u>prove</u> it, even for a special type of cipher. Nor do I expect it to be proven. But this does not destroy its signifance. The probability of the truth of the conjecture can be guessed at on the basis of experience with enciphering and deciphering.

If qualified opinions incline to believe in the exponential conjecture then I think we (the U.S.) can not afford not to make use of it. Also we should try to keep track of the progess of foreign nations towards "unbreakable" types of ciphers.

Since the U.S. presumably does not want other nations to use ciphers we cannot expect to break, this general principle should probably be studied but kept secret.

I believe the enciphering-deciphering machine I invented and had transmitted to the N.S.A. via RAND has this "unbreakable" property. In addition it has several other advantages in that the same physical machine would function both for ciphering and deciphering and that it is auto-synchronizing and recovers after isolated errors in transmission. These properties are not typical of enciphering systems which are auto-coding. Also it is suitable for an all electronic, ultra rapid, embodyment.

~

I do not expect any informative answer to this letter, yet it would be nice to have some sort of answer. I would be happy to explain more fully anything which is not clear in my letter, or to amplify on it.

I have been treating my ideas as information deserving some secrecy precautions, yet I feel it is important to communicate them to the right people. I hope the material in this letter can obtain prompt consideration by very highly competent men, versed in the field.

Sincerely,
John Nash
John Nash
Asst. Prof. Math.

Serial: 531
25 JAN 1955

Mr. John Nash
Department of Mathematics
Massachusetts Institute of Technology
Cambridge 39, Massachusetts

Dear Mr. Nash:

Your recent letter, received ~~**~~ 18 January 1955, is noted. Technicans at this Agency recall a very interesting discussion with you which took place approximately four years ago, and will welcome the opportunity to examine your ideas on the subject of cryptography.

A check within this Agency has, unfortunately, disclosed no information on your machine. A description of the principles involved will be appreciated.

Sincerely,

E. M. Gibson
Lt. Col., AGC
Assistant Adj. Gen.

cc: AG
C/S
COMSEC (3)
412

M/R: In Jan 1955, Mr. Nash offered general remarks on cryptography and requested evaluation of descriptive material which he had forwarded through Rand Corp. NSA Ser 236, 12 Jan 55 informed Mr. Nash that the material had not arrived. Mr. Nash in letter rec'd 18 Jan 55 states the material was sent to NSA and to a Navy Communication Center in Wash. late last spring. A check of Agency records and discussions with various individuals (R/D mathematicians and persons who might have had contact with Rand Corp.) within the Agency has uncovered nothing concerning the system. This correspondence requests a description of the machine.

In 1950 Mr. Nash submitted material, in interview, which was evaluated by NSA as not suitable.

M. A. Lyons, 4128, 60372, in

3 C/Sec 2-2

Serial: 236
12 JAN 1955

Mr. John Nash
Department of Mathematics
Massachusetts Institute of Technology
Cambridge 39, Massachusetts

Dear Mr. Nash:

Reference is made to your recent letter concerning enciphering processes. The information regarding the general principles has been noted with interest. It will be considered fully, and particularly in connection with your enciphering-deciphering machine.

The description of your machine has not yet been received from the Rand Corporation. As soon as details are received, the machine will be studied to determine whether it is of interest to the Government.

The presentation for appraisal of your ideas for safeguarding communications security is very much appreciated.

Sincerely,

D.M. GROSJEAN
MAJOR WAC
Actg. Asst. Adjutant General

cc: AG
C/S
COMSEC (3)
412

M/R: Mr. Nash offers remarks on a general principle relevant to enciphering in general and to his machine in particular. The machine, which he is sending via the Rand Corporation, has not yet been received.

This letter informs Mr. Nash that his remarks are being noted and that the machine will be studied as soon as details are received. This reply coordinated with Mr. M. M. Mathews, NSA-31. This is an interim reply.

M. A. Lyons
M. A. Lyons, 4128, 60372, in

2

C/SEC 2-2

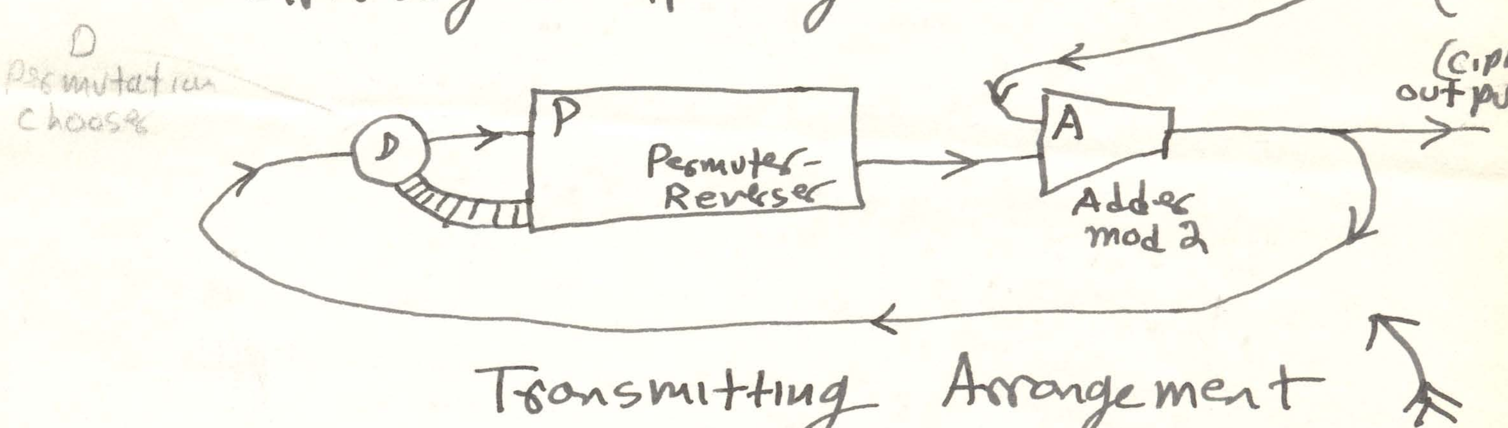
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
CAMBRIDGE 39, MASS.

DEPARTMENT OF MATHEMATICS

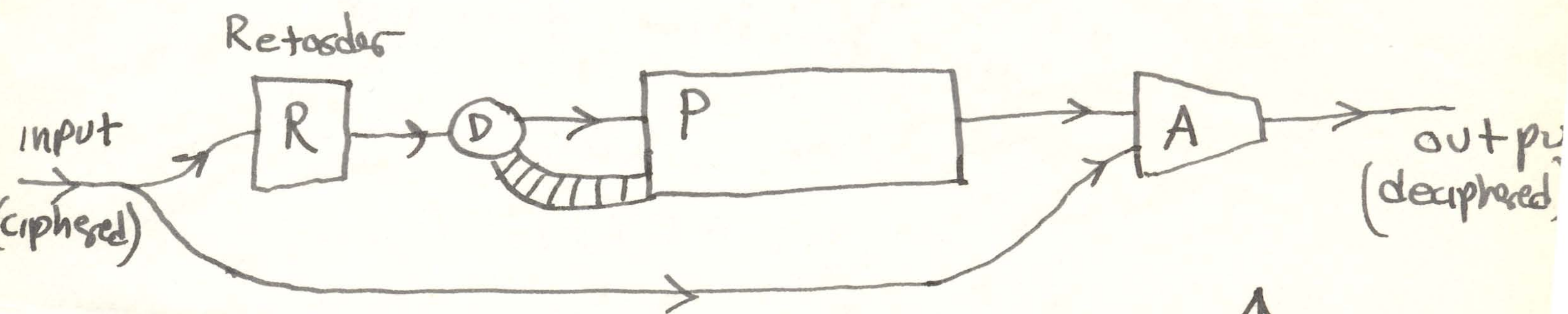
E.M. Gibson, Lt. Col., AGC, Asst. Adj. Gen.

Dear Sir:

Here is a description of my enciphering-deciphering machine.



Transmitting Arrangement



Receiving Arrangement

In the receiving arrangement the same components are used except for the addition of the retorder, which is a one-unit delay. The messages are to be sequences of binary digits (numbers mod 2). The machines work on a cycling basis, performing certain operations during each cycle.

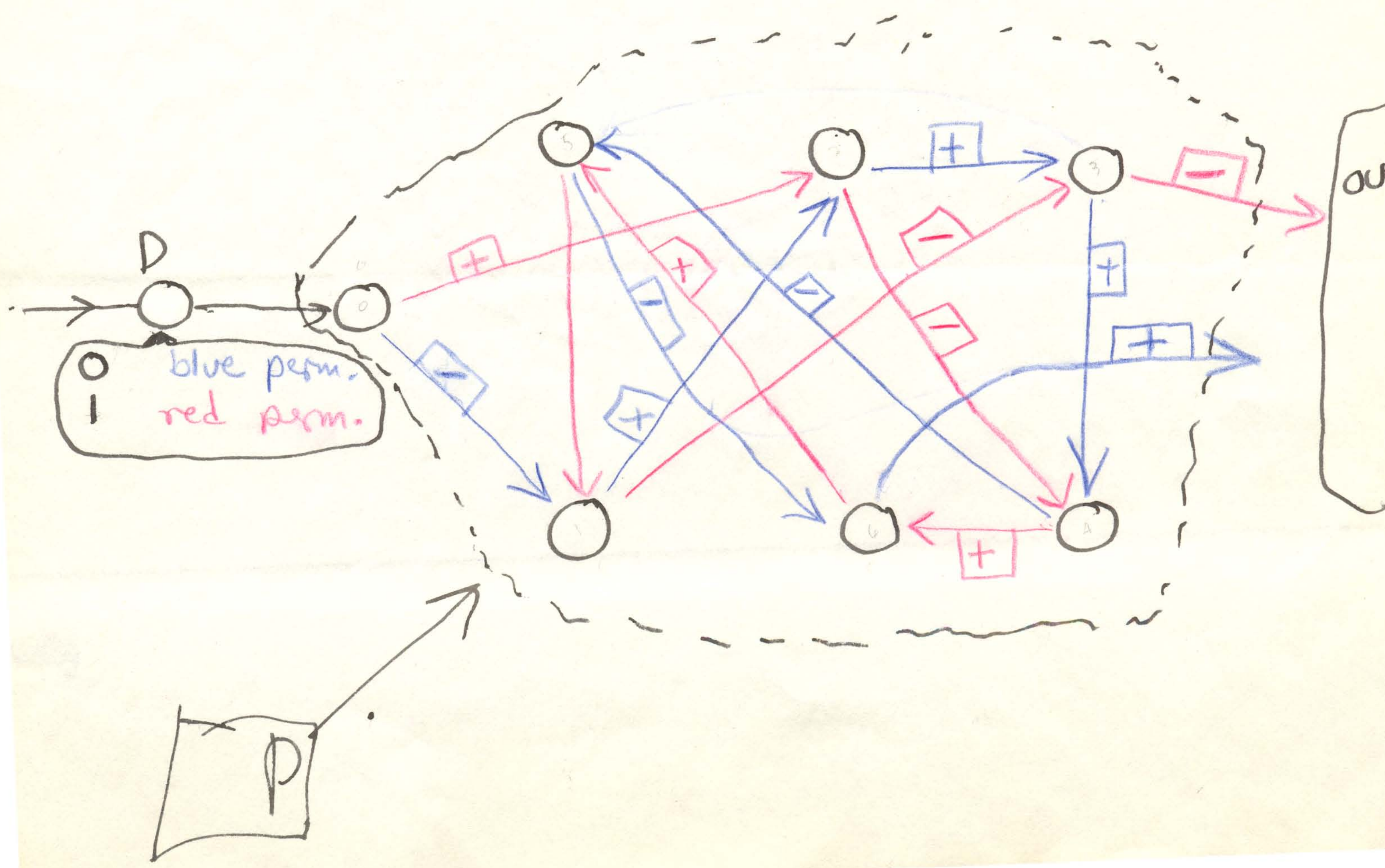
During each cycle the adder, A, takes in two digits and adds them and sends on the sum obtained from the previous addition. The delay in this addition necessitates the retarder, R, in the receiving circuit.

The permuter will be described in more detail below. It takes in a digit from D during each cycle and also puts out a number. What it does, which is the choice between two permutations is determined by what digit (1 or 0) is in D at the time. The permuter always has a number of digits remembered within it. Each cycle it shuffles them around, changing some 1's to zeros, sends one digit on, and takes in a digit from D.

In operation the input of the receiver is the output of the transmitter. So the input to R is the same as the input to D in the transmitter. Hence the output of P in the receiver is the same as the out-put of P in the transmitter, except for a one-unit lag.

So the adder A in the receiver gets: (1) the output of A in the transmitter, and (2) the <u>previous</u> input from $P_{(trans.)}$ to $A_{(trans)}$. Now since binary addition is the same as binary subtraction (i.e. + & − mod 2 are the same) the output of $A_{(receiv.)}$ will be the previous input to $A_{(trans.)}$ from the input to the transmitter, i.e., it will be the clear or unciphered message.

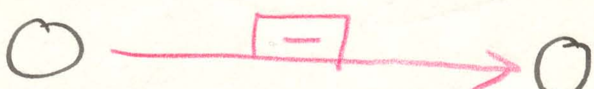
The permuter, P, and "decider", D, work as follows, illustrated by example:



The circles represent places where a digit can be stored. During each cycle either the red permutation of digits or the blue takes place. This is decided by the digit in D at the beginning of the cycle. The D digit moves to the first circle or storage place in P during the cycle after it has determined the choice of the permutation.

Both permutations should cycle through all the places in P, so that a digit would be carried ~~tot~~ through all of them and out under its action alone.

In addition to moving digits around the permutations can change ~~on~~ 1's to 0's and v.v. For example



represents a shift of the digit in the left circle to the right with this change

$\boxed{-}$ $\begin{matrix} 1 \to 0 \\ 0 \to 1 \end{matrix}$.

(For $\boxed{+}$ $\begin{matrix} 1 \to 1 \\ 0 \to 0 \end{matrix}$)

The "key" for the enciphering machine is the choice of the permutations. If there are n storage points in P, not counting the first one, which receives the digit from D, then there are

$$[n!\,2^{n+1}]^2$$ possible keys.

I guess I can rely on your people to check on the possession of this machine of the various properties I claimed for it in a previous letter. I hope the correspondence I have sent in receives careful attention from the most qualified people, because I think the basic points involved are very important.

Sincerely,

John Nash

Assist. Prof. Math.

P.S. Various devices could be added to the machine, but I think it would generally be better to enlarge the permuter than to add anything. Of course error ~~cor~~ correcting coding could occasionally be a useful adjunct.

file

2065

Serial: 1358
3 MAR 1955

Mr. John Nash
Department of Mathematics
Massachusetts Institute of Technology
Cambridge 39, Massachusetts

Dear Mr. Nash:

Reference is made to your letter received in this Agency on 17 February 1955.

The system which you describe has been very carefully examined for possible application to military and other government use. It has been found that the cryptographic principles involved in your system, although ingenious, do not meet the necessary security requirements for official application.

Unfortunately it is impossible to discuss any details in this letter. Perhaps in the future another opportunity will arise for discussion of your ideas on the subject of cryptography.

Although your system cannot be adopted, its presentation for appraisal and your generosity in offering it for official use are very much appreciated.

It is regretted that a more favorable reply cannot be given.

Sincerely,

E.M. Gibson
Lt. Col., AGC
Assistant Adj. Gen.

cc: AG
C/S
COMSEC (3)
412

(M/R ATTACHED)

C/Sec 2-2.

13

M/R: In Jan 55 Mr. Nash offered general remarks on cryptography and requested evaluation of descriptive material which he had forwarded through Rand Corp. The material was not received from Rand Corp. Dr. Campaigne received a letter from Mr. Nash inclosing a copy of the letter (5 Apr 54) from Rand which transmitted this material to NSA. This material was found in R/D files. In the meantime Mr. Nash sent a handwritten description of his enciphering-deciphering machine.

Mr. Nash proposes a permuting cipher-text auto-key principle which has many of the desirable features of a good auto-key system; but it affords only limited security, and requires a comparatively large amount of equipment. The principle would not be used alone in its present form and suitable modification or extension is considered unlikely, unless it could be used in conjunction with other good auto-key principles.

This correspondence informs Mr. Nash that his system does not meet necessary security requirements; and expresses pleasure at the thought of an opportunity to discuss Mr. Nash's ideas on cryptography again. Such a discussion took place in 1950 when Mr. Nash submitted material, in interview, which was evaluated by NSA as unsuitable.

An interesting pamphlet on Non-Cooperative Games, written by Mr. Nash was also sent to this Agency by the author for our information.

Dr. Campaigne has been informed that the reply has been written and is not interested in further coordination.

M A Lyons
MALyons, 4128/60372/rwb