Massachusetts institute of technology
cambridge 39, mass.
department of mathematics

letter concerns enciphering

Dear Sirs:

An encipher-deciphering machine (in general outline) of my invention has been sent to 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

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

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

The α's denote the "key" containing r bits of information. n is the 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 some 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 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 practical sense.

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

In many cruder types of enciphering, particularly those which are not autocoding, 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 a logical way to classify enciphering processes is by the way in which the computation length for the computation of the key increases with increasing 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 where the instructions given by different portions of the key interact complexly with each other in the determination of their ultimate effects on the 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. 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 prove it, even for a special type of cipher. Nor do I expect it to be proven. But this does not destroy its significance. 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 a afford not to make use of it. Also we should try to keep track of the progress 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
Asst. Prof. Math.