Reference - S 67/68 (11-18-W9)

VF 108-15

1647 Macomb's Road
Bronx, New York, N.Y.
January 15, 1938

Sir:

With this letter I am forwarding a set of blueprints, consisting of five sheets. I want to impress on you the advisability, for your own sake, of handling these blueprints tenderly, because they are rather venerable with age.

I am also sending you another copy of my booklet, "Chaocipher - The Ultimate Elusion." You will observe that on this copy I have written in, over the corresponding cipher, the plain text of the first hundred lines. But since each of the first hundred lines, (covering pages 1, 2, 3, and 4), is identical in meaning with the other ninety-nine, I have written the plain text only over the top line on the first four pages.

On page 5 I have written in the plain text of the first eight lines of the Declaration of Independence; and on page 10 I have written in the plain text of the last line of the Declaration of Independence, together with the plain text of the first line of the Gettysburg Speech and the last line of the same.

I am sending you also the full text of the Declaration of Independence and the Gettysburg Speech written exactly as enciphered. The text which I used, of both these historic documents, is as printed, paragraphed, and punctuated in the World Almanac. For punctuation marks I have used letter equivalents. These, of course, are purely arbitrary, and would be largely unnecessary - except where a very high degree of literary precision is desired.

The punctuation marks I have employed, with their letter equivalents, are as follow:

Paragraph	**********	Z
Period	**********	W
Colon	**********	V
Comma	**********	Q
Semi-colon	**********	U (Also QQ, this latter being used only once - in 11th word in Line 112)
Hyphen	**********	J
Apostrophe	**********	X

May I respectfully suggest to you, Sir, that this exhibit which I am presenting be subjected to the most exhaustive scrutiny by the Navy Department; and if you feel that the Navy Department, owing to its "limited personnel," is unable to do this adequately, then may I further suggest that you enlist any and every resource available to any and every department of the United States government for this purpose.

Such a rigorous scrutiny as I suggest will demonstrate to you that this stuff I have submitted is materially and mathematically indecipherable. Indeed, the mathematical examination will establish the utter fortuity of the cipher; for in my cipher system it is impossible to predict what letter of the 26 in the alphabet will represent any given letter in the text to be enciphered. Mathematically, my cipher system will produce exactly the same result as would follow from picking, each time at random, one out of 26 letters tossed together in a hat.

As your mathematicians will be able to verify, here is, in effect, the way the thing works out: when a letter in the given text is to be enciphered, you pick a letter at random out of 26 in the hat; then you throw back that letter into the hat; shake it up, and pick another one to represent the next letter in the text.

And there is this proviso: Whenever a doublet occurs in the text, you pick a letter out of the hat to represent the first letter in the doublet; then you don't replace the letter in the hat, but you pick another one out of the 25 remaining in the hat to represent the second letter of the doublet in the text. Similarly, whenever a triplet occurs in the text (as in the 11th word in Line 238, where the group LLL occurs) the letter representing the first L is - metaphorically speaking of course - taken out of the hat; then this letter, which in this instance happens, as you can see, to be G, is not replaced in the hat, but a letter to represent the second L is drawn from the remaining 25; this letter, as you can see, being O. Now, both the G and the O are kept out of the hat and a letter is drawn from the 24 remaining in it to represent the third L; this letter, as again you can see, being P. Now all three letters are put back in the hat; and to represent the next letter in the text, one is picked from the full 26.

May I once more remind you, Sir, that all this is metaphorical. As a matter of actual fact, of course, there is no such operation as drawing letters "at random" out of any receptacle - much less a hat. But I want to emphasize the fact that the principal of my cipher system produces a result which is - or would be - mathematically identical with the result produced by drawing letters at random.

As a corollary to the foregoing, you will note that whenever a letter in the text happens to be repeated two or three or more times, such repetition cannot occur in the cipher equivalent; and, in accord with this, you will note that when a letter is repeated two or three or more times in the cipher, then the letters in such a repeated group have not the same meaning.

In this connection, there is an interesting coincidence to be observed: I have been discussing the group LLL which appears in the 11th word in Line 238 of the original text; you will note that in the very same Line 238, of the cipher, there is a group LLL in the 9th and 10th words, the textual equivalent for these three L's being EWO.

The process of encipherment in my system is undeviating and unvarying. It is a process which, because of its incessant monotony, is preeminently adapted to a machine. A child could operate my model; and if the finished machine were to be developed as I envision, it could be operated by any child who had outgrown his infancy.

In the actual process of encipherment, there is no discretion required on the part of the operator. The operator is required to do the same thing over and over again. It is the principle of the system which does the work - the work which I have described as being identical with picking letters at random. And this random process goes on, without guidance or interference, forever. There is no such thing as periods or cycles in my system; and if you were to use it to encipher all the words that have ever been, or ever will be, written or spoken by man, it would forever continue to be the same old process of picking a letter at random out of a hat.

Adverting now to the development of my principle in a machine, you are aware, of course, that radio control of distant alphabetical groupings or keyboards, is now an accomplished fact. I am referring to this not because I am making any claim along such a line, but because a radio controlled keyboard would be the ideal auxiliary for the transmission of my cipher. If used in this way, the operators at both the transmitting and receiving ends would be relieved of all trouble so far as the cipher is concerned. In fact, neither of them would have anything to do with it. If you will permit me to digress here for a moment, I shall come back to this subject later.

The blueprints of a machine which I am sending you were done for me many years ago by a first rate man who was at that time Chief Draftsman of the Intertype Corporation. I am frank to say that this machine as blueprinted would, I feel sure, be largely outmoded now. Mechanical developments, particularly in the electrical field, have made enormous strides since it was designed. Besides, it carried a keyboard for 36 letters and symbols, including numerals and punctuation marks. These last named numbers and punctuation marks I have eliminated, as you will see from my booklet, in which I have employed only 26 letters of the alphabet as I am convinced that these 26 letters will be found ample in actual practice for all purposes.

However, my machine as blueprinted should be extremely useful in that it could be developed as an elaborate working model to furnish base for further development along mechanical and electrical lines. This blueprint machine has two cylinders in a make-and-break connection. When a message was to be enciphered on this machine, the operator would have nothing to do but play the letters of the original text on the keyboard, and then perform a couple of simple lever operations after typing each letter. At the back of this machine there are two cylinders, each of which is to carry a roll of paper like that carried in the broadsheet ticker. Then as each letter would be tapped on the keyboard, the original message would appear on cylinder A, and the cipher equivalent simultaneously on Cylinder B.

Harking back now to radio control; suppose the Navy Department wants to send a cipher message; it could be done by simply turning over the text to an operator, who would tap this message on his keyboard. The machine would automatically encipher the message, and transmit only the indecipherable cipher symbols, which, at the receiving end, would be automatically transformed into the symbols of the original text.

So far as I and my claims are concerned, I am not a mechanic, nor an electrician - no more than I am a carpenter. But I am familiar with recent mechanical and electrical developments, and I am therefore able to say that there isn't a doubt of the feasibility of complete mechanization of my cipher system.

And now I come to the nub of this whole subject: Even as a youth, I was deeply interested in the subject of cryptography; and I remember being struck by a sentence in Edgar Allan Poe's "Gold Bug," and also in his Essay on Cryptography, in both of which he says, "It may be roundly asserted that human ingenuity cannot concoct an enigma which human ingenuity cannot resolve." Many years ago, I set out to accept this challenge; and as a result I evolved my system.

From the outset, I had in mind only one primary purpose - and that was to achieve a system the product of which would be absolutely indecipherable. Of course, I did keep in mind the ultimate mechanization of my scheme, but I cannot too forcibly stress the fact that my primary purpose was to devise a system by means of which one could continue forever to "concoct enigmas which human ingenuity cannot resolve."

And this I claim to have accomplished - and in support of my claim I have submitted to you the example of my Chaocipher. This sample, I repeat, is not decipherable. I am submitting it to you with the complete translation (verbatim et literatim), of 98% of it; and I assert that even with this translation it cannot be deciphered. And I challenge the Navy Department, and anyone else in the world, to show how this cipher was constructed and to send me the decipherment of the untranslated words in Lines 101 to 105; and in Line 248 - all these words having been produced in precisely the same manner as all the other words in the document, and being an integral part of it.

Therefore, Sir, I suggest to you that you subject this document to a thorough examination; and in view of the fullness of information which I am giving you about it, I believe you ought to be able speedily to send me your report.

I am convinced that this is obviously the best and most expeditious procedure: You go ahead and scrutinize this document, the cipher of which is identical in character with any cipher my system may produce. And when you find out for yourself that you cannot contest my claim as to its indecipherability, you can get in touch with me and we can arrange for a demonstration on my model. And, speaking for myself, the sooner this takes place the better.

Simple as my principle is, it would be quite impractical for me to put you au fait with it without demonstrations on my model - in which, by the way, I am sure you will be much more interested than in the blueprints. And I promise you that if and when I have given you a full demonstration of my principle, you will be just as helpless - even with my model - to decipher my booklet as you are now.

Let me remind you that I have no patent on my system or devices; and I assure you that no one on earth, except some members of my own immediate family, ever had a demonstration of my cipher principle as it is illustrated in the booklets I have sent you.

During the past couple of years I have been a few times in touch with International Business Machines, where I was frankly told by some of its officers that they are looking for, and have been for a long time trying to develop, a cipher machine. Before the I.B.M. people would consider my scheme, they asked me to sign the Waiver which I enclose. Needless to say, I did not sign it. And all I have to add here and now on this subject is that there is little wonder that I.B.M. is able to pay a "salary" of $342,008 a year to its President, Mr. "Tom" Watson, as disclosed Sunday last in the official report of the House Ways and Means Committee.

Finally, please accept my apologies for this long letter. But I wanted to cover as much of the ground as is at present possible.

May I ask you kindly to acknowledge by return mail receipt of this with enclosures. And, subsequently, when you have had time to digest the full matter of my communication, I shall be glad to hear from you as fully and frankly as you wish.

Very respectfully,

J.F. BYRNE

Captain J. M. Irish
Assistant to Bureau of Engineering
Navy Department
Washington, D.C.

JFB:gr

VF110-1

/

JOHN BYRNE
DESIGN CONSULTANT
P. O. Box 1075
EAST CORINTH, VERMONT 05040 • 802-439-6173

Dear Greg, I re-read this letter and find that it sounds snotty — this was not my intent! Best, John

February 8 1981

Dear Greg,

Along with my apologies for not writing to you sooner I believe that I should offer some sort of explanation.

Your paper " J.F. Byrne and the Chaocipher Work in Progress" aroused several intense reactions in me:

- To respond paragraph by paragraph; to explain, clarify, expostulate, and justify.
- To ignore the whole thing as I really don't want to rake it all up.
- To say something appropriatly enigmatic and let you and your associates stew in it or not as you chose.

Your own statement that "... my interest has been in the chase and not in the kill." is finally wat deterred me from responding at all. This proved to be no solution. Your letters and paper have been sitting on my desk for time enough and time will eventually have its way. I have to answer, which means I want to.

I don't know how far you have progressed with this work since last we were in touch, but here are a few items that might be of some interest to you or to others.

I truly admire (ameven amazed by) your work even in those areas with which I cannot,or just don't,agree.

For reasons I can not honestly define I am not yet prepared to show you or anyone else the blueprints of my father's "device".

The infamous cigar box was "lost stolen, or strayed" before my memory but it was NOT "non functional".

The model my father, mother, and I worked on was destroyed by me shortly after my father's death.

Remember blindfold chess and all those other mental gymnastics ? My father hardly ever used "pencil and paper" except for making rare notes for others to read. (More's the pity.)

The "operations" could not have been performed with pencil and paper to any practical extent.

Dad foresaw the advent of a computer technology and predicted that one day the use of his system would be as "simple as using a typewriter."

(Back to the cigar box)... It was not at all a lesser contrivance in terms of its capacity to perform the full function(s) of the envisioned final device. Mr father's phrase "some freedom" refers to facility not to function. You may be sure that he was always precise... including his assertions concerning the encipherment and, as I prefer to call it, the "resolution".

Forget about Euclid, Heron, Joyce, and all those others. Use your own head. you obviously have a damn good one.

Finally, and as far as I will go right now there is the matter of FEACE and RENEFITS. I have been at some expenditure of time to check available carbon copies of the original manuscript against the galley proofs. I can assure you that to the best of my knowledge you should use the correct plain text spelling PEACE and BENEFITS for all applications. I am astounded that these typos got past our attention. I remember helping my mother and father check the galley proofs letter by damnable letter. We quite naturally concentrated on the cipher text to assure its absolut accuracy. Apparently the plain text did not receive the same "devoted" attention.

I can concieve of no way that these printing errors can reflect errors in the encipherment. Both my father's working notes and the available manuscript copies substantiate this judgement.

I have neither sought nor found any explanation whatsoever for VAGAREENTUR. I don't know whose Calico Belly my father was enjoying at that time. Sometime I'll look into it.

Speaking of "sometime"... Anent the Cryptogram (enclosed) you tod me that you would like to see it again some time. Please excuse my temporal irreverance.

One last note before closing. I must admit to that which you already suspect. The copies of Cryptogram and Cryptologia which you so kindly sent served only to turn me off. I truly am not sure that I have anything to contribute to the meetings... and I don't think I dig the lingo.

If you are of a mind, please write again.
Sincerely, and with best regards

John Byrne