A preceding chapter I have referred to Rutherford's achievement in 1919 of splitting an atom for the first time. In the preceding year, 1918, I had discovered a method of doing something to the written word, in any language, which affected that written word so as to result in its chaotic disruption. In two respects my method for achieving the complete annihilation of order and design in written language is more noteworthy than the method for the disruption of the atom. First, because my method for splitting the word is so simple that it could be performed by any normal ten-year-old school child, and second, because, unlike any other process of explosion or disruption, my method of disrupting the written words is identical and simultaneous with the complete restoration of order and design in the same written words.

Down through the ages, it has been the aim and desire of human beings to be able, on occasion, to write their thoughts in such a way as to be wholly unintelligible to anyone except the person to whom these thoughts were intended to be exclusively addressed. Of course, I could remark here with more truth than flippancy that a great many writers have found no difficulty in presenting their "thoughts" in gobbledegook language which nobody at all can understand, but with that kind of thing I am not concerned.

While it has always been the aim and hope of many to be able at times to express themselves in indecipherable script, the inherent difficulty of doing just that had never yet been overcome; and, indeed, the impossibility of doing it has been universally declared by all students of the subject.

Edgar Allan Poe was a most ardent and, to take him at his own word, a very capable cryptanalyst, and in two of his works he gives utterance to his conviction that all cipher is decipherable. In his well-known story "The Gold Bug" he states, "It may well be doubted whether human ingenuity can construct an enigma of the kind which human ingenuity may not, by proper application, resolve" and in his less known essay on "Cryptography" he declares, "It may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve" and in this same essay he goes on to say that "The reader should bear in mind that the basis of the whole art of solution, as far as regards these matters, is found in the general principles of the formation of language itself, and thus is altogether independent of the particular laws which govern any cipher, or the construction of its key.

My reason for quoting Poe here in this way is because of all the writers on the subject, he has expressed himself the most succinctly. So far as the accuracy of his observations is concerned I will only remark that Poe was far less cautious than he should have been when he uttered that dictum beginning with, "It may be roundly asserted . . ."

When I discovered my method for the utter disruption of the written word, or, to express this differently, my method for writing a cipher which would, in fact, be absolutely indecipherable, I discovered something which was just as accessible to Poe as it was to me. The ancient Egyptians and Babylonians could have been completely familiar with the principle, a fact which is readily deducible from a treatise on mathematics written by Hero of Alexandria in the second century B.C. The point I am making is that during the past two thousand years and more anyone could have had access to my method for the chaoticification of language. The first device, or machine, which I constructed, solely for the purpose of demonstrating a principle, was a little model, constructed in an empty cigar box which, when full, had contained fifty small Havana cigars. I made this model myself, and to say that it was a crude affair would be only to describe it accurately.

Let me state simply what I claim to have accomplished in this connection: First, I formulated a principle for the development of a cipher which would be materially and mathematically in-
decipherable, and, second, I built the little model, of which I have spoken, for the purpose of demonstrating this principle. With these two things, my device and my principle, any person, anywhere, writing any language, could by applying my principle and using my device transcribe his written words into a script which would be absolutely indecipherable by anyone except the persons for whom the message is intended; and be it remembered that while possession of my device together with knowledge of my principle, would enable any person to write a script which would be absolutely indecipherable by anyone except the person or persons for and to whom the script was written and addressed, yet possession of my device together with knowledge of the general principle involved, would not enable any person to decipher any messages whatever written by anyone else and not intended for him.

In all my efforts to locate backing for my idea and device, I have found it practically impossible to make people understand exactly the import of what I have just written in the preceding paragraph. For this reason, I repeat, that if every person on earth were in possession of my device and applied my principle, he or she could encipher a message, in any language, and this message would be absolutely indecipherable by anyone except the person for whom it was intended. Moreover, if every person on earth were to encipher the same message, say for instance, this paragraph of which this sentence is a part, no two of the resultant encipherments would be alike.

In June, 1919, I went to Washington to consult with the then famous attorney, Marcellus Bailey, with whom I had arranged an appointment. When I arrived at his office I was informed that he was at home ill, but that he would see me there. At his almost palatial residence I was ushered into the aged attorney's bedroom, and there, sitting on the side of his bed, I demonstrated my principle on my little cigar box device. Marcellus appeared intensely interested during my full three-hour demonstration and at the end of that time he said, "Well, Mr. Byrne, you certainly have succeeded in scrambling your eggs; but my advice to you now is not to enter the patent office with that little device, for, after all, it is scarcely more than a toy. When you go into the patent office, go into it with your better foot foremost. You say you intend to collaborate with an expert draftsman in producing

the blueprints of a readily operable machine, and my professional opinion is that you ought to wait until you have your blueprints ready."

It was only comparatively recently that I realized how I missed my cue at that interview with Marcellus Bailey. He had told me that my little device was "scarcely more than a toy"—and what I should have done was to enter it in the patent office as just that; for in this way, the device would have come into general use, and its ability in enabling anyone to write an indecipherable cipher would have soon become a universally recognized fact.

But what I did then was to spend six months working with a first-rate draftsman, and at the end of this time I wrote to Marcellus Bailey who replied to me in part as follows:

Marcellus Bailey,
Attorney at Law & Solicitor of Patents,
Washington, D.C.

501 F Street, N.W.

January 24, 1920

My dear Mr. Byrne:

I am in receipt of your letter of the 20th instant and I congratulate you on having at last the finished drawings of the Cipher Machine developed from the device which you exhibited to me on June 10 last. It must have been some job . . . ."

Marcellus had more to say in his letter, but the point he evidently desired most to emphasize at that time was in going on record as to the exact date upon which I exhibited my device to him.

I then approached several machine makers asking for an estimate of the cost of making my machine, and from not one of them could I get anything approaching a firm bid, everyone of them was vague, and the best I could get by way of an estimate was that it would not be less than $5,000 and might run to $20,000 or more; so my blueprints are still gradually returning into the dust which is the ultimate destination of all things, including ourselves.

It would be impracticable and fruitless here to give a detailed account of my experiences in connection with my efforts trying to
"put across" my cipher idea, efforts which entailed my expenditure of thousands of dollars and countless unrewarded days of time. So I shall do no more than tell briefly, and with occasionally necessary reserve, a few of the outstanding facts and incidents.

But before proceeding further with my story, let me make it clear that my discovery was not fortuitous. During many years previous to it, I had often questioned casually the accuracy of the universal consensus regarding the impossibility of constructing an indecipherable cipher; but it was not until the autumn of 1918 that I gave serious thought to the subject. Reading at that time a detective story in a well-known magazine, I came to a reference to a cipher message which the detective hero had little difficulty in deciphering because, as he was made to comment laconically, "all such communications yield to methodic and scientific analysis"—instantly I felt, as it were, my mind bristling, and I asked myself the question: Is it really a fact that all ciphers must yield to methodic and scientific analysis? The expert cryptanalyst's answer to this question is a categorical "Yes"; and he bases his "Yes" as Poe did, on "the general principles of the formation of language itself."

In his essay on "Cryptography" Poe states that some months previously he had "ventured to assert" that he would be able to resolve any cipher "of the character specified." This challenge, Poe asserts, resulted in letters being "poured in" on him "from all parts of the country"; and he continues: "Out of, perhaps, one hundred ciphers altogether received, there was only one which we did not immediately succeed in resolving. This one we demonstrated [italics are Poe's] to be an imposition—that is to say, we fully proved it a jargon of random characters, having no meaning whatever."

The foregoing statement by Poe is one of the most surprising and self-revealing declarations ever uttered by anyone; and it also furnishes a most beautiful example of a "non sequitur." Poe says he "fully proved" the submitted "cipher" to be "a jargon of random characters." This, of course, I admit Poe could prove to his heart's content, but why, I ask, why in the name of common sense did he go on to assume from the fact that it was "a jargon of random characters," that it had "no meaning whatever"?

I grant freely that Poe was almost certainly correct in saying that the "cipher" he was referring to had "no meaning whatever." The important point here, however, is that Poe did not perceive the non sequitur of his deduction—that he did not perceive that if "human ingenuity" were to aim at concocting a cipher which "human ingenuity" would not be able to resolve, that cipher would have to be "a jargon of random characters."

Almost twenty years ago a pretentious book written by one Herbert Yardley, and bearing the title of The American Black Chamber, achieved considerable popularity and notoriety. In this book there is a chapter devoted to "A Word with the State Department" and in this chapter the author refers to the actual, or potential, existence of an indecipherable cipher which is such because the cipher has no repetitions to conceal. And then the author proceeds to ramble incoherently about the pride he would feel if he were able to give to the United States an impenetrable and permanent cipher which would preserve its secrecy forever. Just what Mr. Yardley was trying to say in this chapter remains obscure, but it is a fact that years before it was written I had given a demonstration to the War Department in Washington of my first crude cipher machine. The persons to whom I demonstrated my "machine" were Major Frank Moorman, of the General Staff, referred to in Chapter XI of Yardley's book, and Mr. W. F. Friedman, cryptanalyst; and this demonstration was given by me in July 1922, some nine years before Yardley's American Black Chamber was published.

It is interesting to note that in his book Yardley displays the same ignorance that Poe did—and that everyone else does—regarding the essential character of an indecipherable cipher; for, in reference to such a demand made on him by Colonel Van Deman for the decipherment of a certain message, Yardley told the Colonel that he had worked on the message all night, and, basing his opinion on "Scientific Analysis," declared the document was not a cipher but a fraud and a fake, put together by someone who had picked out a jumble of letters on a typewriter.

Let us consider here what kind of cipher script could properly be described as a jargon of random characters. Suppose you were to get a revolving drum and put into it twenty-six marbles, similar in size and weight, but each one designating a different letter of the alphabet; and then suppose you were to dictate,
letter by letter, a piece containing, say, one thousand words to someone who would take at random a marble out of the drum each time you called out a letter, and then replace that marble in the revolving drum before the next draw; and all the while write down every letter in the sequence as they were fortuitously drawn from the drum—what would the resultant script written by this haphazard method be like? Would it not best be described as a "jargon of random characters?" Yes, it would. But does it necessarily follow that this "jargon of random characters" has "no meaning whatever"? No, it does not.

If it be agreed that this script, resulting from the casual drawing of a marble from a rotating drum for each letter in a piece of plain text containing one thousand words, could best be described as a "jargon of random characters," may we not ask how the script, resulting from the casual drawing of marbles from a rotating drum for every letter in a piece of plain text containing one million words, or one quintillion words—or, indeed words ad infinitum—could best be described? Is it not obvious that this resultant script would continue to be—ad infinitum—a "jargon of random characters?"

It should be obvious to anyone, as it should have been clear to Major Yardley, that the only cipher which would be materially and mathematically indecipherable is one which would present no feature other than that of having been drawn inconsequentially from a rotating drum, or pecked haphazardly on a typewriter—a cipher which would be devoid of discernible order, or design, a cipher which would, in actual fact, possess no order or design, a cipher which could only be adequately described as a "jargon of random characters."

When I first set out to discover a system for concocting an indecipherable cipher, I had it clearly in mind that such a system would and should be universally available. I had no thought of devising a system which would be available, say, for the War Department, or for the Navy, or for the State Department. What I had in mind, I repeat, was a system available for everybody; and I fully believed—and am convinced—that the really big market for my system would be in the commercial, general correspondence, and literary fields. I aimed at supplying for one and all a method and a means for conveying his or her thoughts in such a way that he or she could be absolutely assured that only the intended recipient would be able to read them. I envisioned, for instance, the utilization of my method and machine by business men for business communications, and by brotherhoods and social and religious institutions. I believe that my method and machine would be an invaluable asset to big religious institutions as for example the Catholic Church with its world-wide ramifications. I had, and still have in mind the universal use of my machine and method by husband, wife, or lover. My machine would be on hire, as typewriting machines now are, in hotels, steamships, and, maybe even on trains and airliners, available for anyone anywhere and at any time. And I believe, too, that the time will come—and come soon—when my system will be used in the publication of pamphlets and books written in cipher which will be unreadable except by those who are specially initiated.

I have an acquaintance whose grandfather was a close friend and an admirer of Alexander Graham Bell. Towards the end of 1876, Bell demonstrated his crude telephone to the grandfather I am speaking about, and, having done so, asked him whether he would care to invest $3,000 in its commercialization. "Oh, no, Alec," the grandfather replied laughingly to Bell, "don't ask me to invest in a thing like that—why, man, it's just a toy! But let me tell you, Alec, if that you need the $3,000 for yourself, either as a loan or a gift, you can have the money with pleasure."

"It's just a toy!" That's what the grandfather said to Alec Bell; and that's what Marcellus Bailey said to me about my crude device. And the "toy" that was Alec Bell's brainchild grew up, and up, and up, till it is even now the fundamental base of the largest corporate organization on earth—The American Tel. and Tel.

In 1920 a friend of mine, a New York lawyer, who was also a friend and former law associate of Bainbridge Colby, suggested to me that I sound out the State Department in Washington on the availability to it of my cipher system. Colby was then Secretary of State; and I approached him by letter, enclosing a personal introduction to him written by our mutual friend. About three weeks later I received a surprising letter, written on the stationery of The Secretary of State, and here reproduced in part.
THE SECRETARY OF STATE
WASHINGTON

My dear Sir:

The Secretary desires me to acknowledge the receipt of your letter of the twenty-sixth regarding a cipher machine concerning which you wrote to him on September thirtieth. . . .

The Department has examined with interest the plan which you submitted, but it does not feel that it can undertake to pass upon the value of an invention of this sort.

I am returning to you herewith the papers which you sent to the Department.

Yours very truly,
G. Howland Shaw
Executive Assistant.

In the following year, 1921, there was a new President in Washington, and also a new Secretary of State, the great Charles Evans Hughes. Years before that time I had been introduced to Mr. Hughes, and I held him, as I still hold his memory, in high esteem. So once again I decided to approach the State Department in regard to the availability of my cipher. But before doing this I thought it would be advisable to seek an opinion regarding my cipher system from a person qualified to give an opinion about it, so shortly after Harding’s inauguration, I got in touch with Colonel Parker Hitt, who had authored a little booklet which had been published officially in Fort Leavenworth, Kansas, bearing the title, *Manual for the Solution of Military Ciphers*. During the succeeding months, I heard several times from Colonel Hitt anent my cipher system, and I knew from him that he was vastly interested in it. But it was not until August 3, 1921 that he wrote me a definitive and formal letter about my system. It would not now be wise for me to give this letter in full, but in it he wrote in part as follows:

HEADQUARTERS 2ND CORPS AREA
Governors Island, New York City.
August 5, 1921

My dear Mr. Byrne:

I am returning to you herewith the machine and the accompanying papers which you let me have in connection with it. It has been impossible for me to do any connected work with it for many weeks, on account of the pressure of official business and the various things which I have to take care of. I am now about to leave for Washington for permanent station and we might as well call it a day.

As to the principle of the machine, it is undoubtedly a most ingenious and effective device. . . .

. . . but I have attempted to formulate a plan for breaking down this system of yours and so far have not been able to do it successfully.

I feel that you could safely go ahead with the commercial exploitation of the machine with confidence in the practical indecipherability of the product.

I regret that I have not been able to handle this matter with the care and deliberation which I like to give these things, but I assure you of my interest in it and I want to thank you for having let me see it and for your courtesy in putting the cards on the table for me.

Yours sincerely,
Parker Hitt

When I read Colonel Hitt’s letter, it was clear to me that he had not at all fully apprehended the principle of my “machine,” as he called it. But I was glad, however, to know that he was aware of the fact that “commercial exploitation” of my system and machine was the object I had in view.

Having received this letter from Colonel Hitt, I immediately communicated with the State Department, being ignorantly hopeful that Secretary Hughes would give me some encouragement. But in a few days I got one more shock of disappointment in the form of the letter, here reproduced:
DEPARTMENT OF STATE
WASHINGTON
September 2, 1921

In reply refer to
IB 119.25/360
Mr. J. F. Byrne,
70 Wilson Street,
Brooklyn, New York.

Dear Sir:

Receipt is acknowledged of your letter of the 29th ultimo with regard to a cipher machine invented by you and which you desire to demonstrate to the Department.

In reply I beg to inform you that while the Department appreciates your courtesy in bringing this matter to its attention, the codes and ciphers now used are adequate to its needs.

I am, Sir,

Your obedient servant,
For the Secretary of State:
Harry P. Fletcher
Under Secretary

Be it remembered that the foregoing letter, a paragon of smugness, was written to me twenty-nine years ago by the State Department of these United States; and then compare this fact with the fact that Robert E. Sherwood was reported only a little more than a year ago in all our newspapers as declaring that high Government officials, including the late Harry Hopkins, believed that the State Department code was "very vulnerable" as far back as 1941. And on December 8, 1948, Under Secretary Robert A. Lovett, talking about the Chambers-Hiss affair at a Washington news conference, assured the news gatherers that the State Department's diplomatic "codes" had been made as secure against espionage as it was "humanly possible" to make them—and this "new security," Mr. Lovett explained, had been achieved during the last ten years by steadily improved peace and wartime procedures and devices. But at the same time Mr. Lovett was reported as "conceding" that "great aid" to spies in cracking the old codes could be found in documents involved in the Chambers-Hiss case.

THE WAR COLLEGE
WASHINGTON
7 March, 1922

My Dear Mr. Byrne,

But, if you come to Washington or want to correspond with the right man here about your machine, I will be glad to put you in touch with Major Frank Moorman, General Staff, Room 2648, Munitions Building, who handles these matters (in connection with the Signal Corps) and who is a personal friend and cipher pupil of mine.

As for the last paragraph of your letter, I deeply appreciate your offer but turn it down in the interest of my own liberty of action. I am a free lance at this game and expect to remain one. For that reason, I am returning your letter in order that we may consider it as never written.

Yours truly,
Parker Hitt

In the week after receipt of this letter, I arrived once more with my first model in Washington, where I was met on March 17, 1922, by Colonel Hitt, who immediately escorted me in person to give me a glowing introduction to both Major Moorman, and Mr. W. F. Friedman, Cryptanalyst.

Nearly five months later I wrote to Major Moorman and received the following reply:

MILITARY INTELLIGENCE DIVISION
WAR DEPARTMENT
OFFICE OF THE CHIEF OF STAFF
WASHINGTON
August 26, 1922
Mr. J. F. Byrne,
70 Wilson Street,
Brooklyn, N.Y.

Dear Sir,—

I have for acknowledgement your letter of August 21st and wish to assure you that I have not forgotten the profitable hour we spent together. I am sending a letter to Mr. Friedman with request that he communicate with you with reference to your cipher device.

Very sincerely yours,
Frank Moorman
Major, General Staff

And a few days afterwards I received by parcel post from Washington a package containing my cipher model smashed into smithereens.

When I was devising my cipher system, I worked neither with model nor with diagram. I solved my problem in a short period of delicious mental concentration and exhilaration. In fact, I worked out the problem blindfold, as I would have worked out a chess problem; and I entertained the erroneous belief that merely to narrate and describe my system to a serious and disinterested student of Cryptography, or to any person of unbiased intelligence, would be sufficient to evoke his assent to the validity of my claims in its regard. This is where I made a big mistake; and this is what I had in mind in a preceding chapter of this book when I referred to the harmful consequences which might ensue from indulging in blindfold chess play.

A result of this mistake was that when I constructed my cigar-box model in 1918, I had in mind only the construction of a model on which I could demonstrate a principle. My cousin Mary Fleming was charmed with the resultant "toy"—it looked so simple and colorful; and when I told her the purpose for which it was intended and explained its operation, she was entranced with the idea which she grasped quickly and clearly. And very earnestly she said to me, "That will surely bring you a Nobel Prize." At that time all I replied was, "Well it certainly is a strange thing that, being so simple as it is, no one ever thought of it before." And since that time I have seen many a Nobel Prize awarded for lesser achievements.

After my experience with the War and State Departments, I felt that it was, and would remain, quite useless to attempt to get anywhere with any department of the United States Government. In this opinion I abided for a full fifteen years; and then, in a weak moment, I fell for an item which appeared in the newspapers in 1937. This item was to the effect that Rear Admiral Harold G. Bowen had requested a congressional appropriation "for the development of a system of Cryptography by which warships can transmit signals to another vessel in the fleet which cannot be deciphered (sic) by an enemy vessel."

On reading this news item, I decided to construct a working model on which I could do extended encipherments and decipherments, and on which I could with some freedom put my principle into operation. Working through the summer and fall of 1937, I made my model and prepared on and by it, a document which I intended for submission to the Navy Department—this document being composed as a concrete example of the kind of work which one could accomplish on my model. After some hard labor in producing the cipher, I found even harder labor ahead of me in trying to find a printer who would be able to turn out the kind of job I wanted. Finally I did locate a printer who was willing to tackle the work, and who did turn out an excellent job. He printed for me five hundred copies. And they cost me plenty—both in time and money.

On November 18, 1937, I wrote my first letter to the Navy Department, addressing it to Admiral Bowen, who has since retired, and has become Executive Director for the Thomas Alva Edison Foundation of which Charles F. Kettering is President. In my letter to Admiral Bowen I told him of my device and system, stressing their universal availability. I enclosed also some copies of my document, Chaocipher—The Ultimate Elusion.

I never had any reply from Admiral Bowen himself; but a couple of weeks later, on December 7, 1937, I had the following letter from a Captain J. M. Irish, who was Assistant to the Chief of the Bureau of Engineering.
Sir:

Receipt of your letter of 18 November 1937 is acknowledged herewith.

This Bureau regrets very much that its limited personnel does not permit deciphering the material enclosed with your letter. However, the Bureau would be very pleased to examine fully a detailed description of your general system and of the mechanical means used for obtaining the cipher.

Your courtesy in according the Bureau an opportunity of examining your system is very much appreciated.

Very respectfully,

J. M. Irish
Assistant to Bureau

On the following January 15, I wrote a further explanatory letter, this one to Captain Irish, with another marked copy of my ten-page cipher booklet, entitled *Chaocipher: The Ultimate Elusion*. In this letter I said in part:

"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."

The plain text of each of the 100 lines on pages 1, 2, 3, and 4 reads thus:

ALLGO OD, QU ICKBR OWNFO XESJU MPOVE RLASY DOGTO SAVET HEIRP ARTY

"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 Indepen-
thing like $1 a year), provided that I were allowed to develop
the commercial exploitation of my system. In one of my first le-
ters to the Navy Department in 1938, I made this point clear;
and in a letter to me written on March 12, 1938, Captain Irish wrote:

"Referring to the questions raised in your letter, the Bureau
is unable to state at this time whether or not, in event of adop-
tion of your system, it would elect to purchase your invention
or merely to right to use same for Governmental purposes leav-
ing all other rights to you. It is probable, however, that the former
course of action would be taken for reasons of secrecy."

In using these four words "for reasons of secrecy," Captain Irish
made it clear that he did not grasp my claim regarding the uni-
versal availability and indecipherability of my system.

Let me return now to the subject of that Washington news
conference on December 8, 1949. At that conference it was re-
vealed that Whittaker Chambers had produced stolen documents,
the theft of which, according to Assistant Secretary of State John
E. Peurifoy, meant that "our codes were being read by foreign
nations" during a long period. And at this conference Under
Secretary Robert A. Lovett stated that he "knew the State De-
partment's code work now is completely secure—both against
code-solving and theft of its documents." And then a few seconds
later at this same conference Mr. Lovett added that "the State
Department has been told by cryptographic experts its code work
is as secure as any material of that nature can be."

When such statements or elucidations as the one made by Mr.
Lovett are to be imparted to the public, why should such an
onerous job be loaded on the back of a high official like Mr.
Lovett? Where were the "cryptographic experts" who reportedly
"told" the State Department about the security of its "codes,
and why were not these "experts," or at least one of them called
upon to give at first hand to the public the assurances on which
Mr. Lovett based his claim about the "security" of the "codes"?

Finally, may I ask Mr. Lovett, or anyone now in the State
Department—or in any other Government Department—who or
what is a "cryptographic expert"? I have a clear notion of the
connotation of the title "cryptanalytic expert"; but I never heard
any such expert—save one—express the opinion, or even concede
the possibility, that any indecipherable script could ever be con-
coected. And in this connection I express here my belief that the
persons who were dubbed by Mr. Lovett "cryptographic experts"
were, in fact, "cryptanalytic experts," who would themselves un-
hesitatingly express their conviction that there never was—and
that there never will be—a "cryptographic expert." These "crypt-
analytic experts" are precisely the kind of persons who would give
the most positive assurance to the head officials in any Department
that "its code work is as secure as any material of that nature
can be."

"The most fitting comment on the last preceding sentence is,
"A word to the wise is sufficient."

But much more recently, and more dramatically, the spotlight
of publicity was brilliantly directed to the subject of what Mr.
Lovett called the security of this nation's "code work." In the
days when, after his recall from Korea, General of the Army
Douglas MacArthur was testifying before the Senate Committee
in Washington, the gist of some messages that had been sent to
him in cipher was submitted to the committee, but always with
the explanation that this gist was a carefully paraphrased version
of the original plain text of the cipher messages. And the ex-
planation offered for submitting such paraphrased versions was
that this was done to protect this government's cipher system
from being "broken" or "cracked."

In this connection, referring to a document that had been sent
on January 15, 1951, Secretary Marshall testified: "It's been
declassified with the approval of the President, and in a manner that
we do not think discloses any cryptographic information and
things of that sort."

At the time that General Marshall uttered that insidious, cau-
tious, and hedging pronouncement, he was the top man of the
Armed Forces of these United States; and the plain inference
from his pronouncement is that the highest ranking government
officials of this country not only admit, but assert, that their cipher
systems are defective and vulnerable and decipherrable. Indeed,
this inference would have been justified even if General Marshall
had not uttered that wobbly, "We do not think . . . ." For from
this mere fact alone that it was found necessary to issue "precise
instructions for paraphrasing" the plain texts, the deduction is
inescapable that the highest officials in this country are fully aware
of the insecurity of its "code work."
In this connection, I assert and claim that the publication of the plain text of a trillion documents enciphered by my cipher system would not be of the least use or assistance to anyone attempting to cryptanalyze the cipher product of my system.

Let me repeat here that any person on earth using a device similar to my own home-made contraption, could produce a cipher message which would be indecipherable by any other person except the one to whom the message is directed. And let me add that devices far more operable than my crude model could be mass-produced to sell at ten dollars each.

I reproduce, herewith, four cipher exhibits, together with their plain text equivalents—which are given verbatim et literatim.

The first and longest of these exhibits is the one entitled Chaocipher—The Ultimate Elusion, which was prepared by me for presentation to the Navy Department. As a matter of fact, several more copies of this document are, or were, in the various departments of the United States Government. Although I have already given the general schema of this ten-page document, let me repeat that the first four pages are devoted to the encipherment of an identical line which reads:

ALLGO ODQ QU CKBR OWINF OXESJU MPOVE RLAYZ DOGTO SAVETH ERPR ARTY

There was really no need for the two punctuation marks, the comma and the period, represented respectively by a free Q and a free W. They are just an illustrative embellishment. On page 5 of this document, lines 101 to part of 105 are devoted to a few introductory words to the two great historic documents that follow: These being the “Declaration of Independence,” which begins at the third letter in the ninth group on line 105, and ends at the fifth letter in the fourth group on line 237; and the “Gettysburg Speech,” which begins at the first letter in the fifth group on line 227, and ends at the third letter in the third group on line 238. In both the cipher and plain texts of the Gettysburg speech, there was an error of omission at the fourth character in the eighth group of five letters in line 239. At this point 95 characters were left out, these being a comma followed by the words “but it can never forget what they did here.”

The second exhibit reproduced is an encipherment of four short passages from the first three chapters of Caesar’s De Bello Gallico, with the exact plain text in Latin; and the reader will note the frequency of the recurrence in the cipher script of both the letters W and K, notwithstanding that the letter W does not occur at all in Latin, and the letter K is extremely rare in that language.

The third exhibit reproduced here is one which speaks for itself, and will, I fancy, be of some interest to a certain person in Washington.

I call the fourth exhibit reproduced “A Glimpse of Chaos.” This is the encipherment, with exact plain text, of a portion of the memorable speech made by General of the Army, Douglas MacArthur, before the joint session of Congress after his recall from Korea. This encipherment is distinguished from the other three in that it bears within itself full and complete instructions to an initiate for its decipherment.

In regard to the first of these four exhibits, I have already said that several copies of this document were submitted to Washington, together with an abortive demonstration. Moreover, a formal demonstration of my chaocipher system, together with a decipherment of this exhibit, were given by me to the American Tel. & Tel. Company through some top officials of the Bell Laboratories, these including Mr. Ramond D. Parker, a former Telegraph Development Director for that organization. I cannot, therefore, issue a categorical challenge to everyone to decipher this document.

But in regard to the other three exhibits, I do challenge any person or group of persons—including the Bell Laboratories and the American Tel. & Tel.—to decipher these documents.

Now seeing that in the case of documents two and three I give the exact plain text equivalents, verbatim et literatim, of their cipher text, I can envision the possibility that some wags or wiseacres may claim decipherment of these two documents by simply copying the plain texts as given. For this reason I issue a further and more specific challenge in regard to exhibit four, this challenge being as follows: In the last two lines of the cipher text of the number four exhibit, namely lines 34 and 55, a little over a dozen words, with punctuation marks, of the plain text as I have given it have been re-enciphered. Now, to the first person, or group of persons, who within three months after date of publication of this book succeeds in deciphering this number four exhibit, I shall give ($5,000) five thousand dollars—this sum to be
Ye know on earth, and all ye need to know,

O, then afford a friend to whom thou art

Tell you all that remain, in midst of other woes,

Ye know in truth, and that is all.
The Declaration of Independence begins with the "H" in "JSHVI."
131 XYRUIW MBTXF HYVNG ZLXEL VTZDC QMVFPL CBYKX BMESG HSOEP SPKKE WMGEQW
132 COINQ URHIG BQNGQ AAPXFQ TICWVNZ ZIEXL BETQG LQEOS DNEBQ MBTBY DIAKE
133 FHHMNX LQOLKF MLNZQ QLAXE UQCWZ PXXOQ ACFNP MRUIN YQDHJ BGUSD GBAHL
134 EPFKEQ CVTID XJQSO UYYHN KYPEB JYDMQ OKSWL OTPOD LILSV SPTYX
135 DNWTH QWVTU FRBHG DTWZ ADLAM KOMBB GMHAN GSCHA OCUZA OYQGB VYWKT
136 GNYAJ MAGYS KHOQSA RQWVZ PODRM CNYGQ MSHKE KHIQK GFJRW MFPOK MDYUT
137 JWTAH YOLIX RKKJW BALQV AMLVY ZGDAF BIEKV BUXEC AUCRP PKKQY DPUBL
138 TSNWQ XKNDC RHECG JLDGM MZWFK GPMKY VIISO QCXVP BKXBY LXSHP YZNLK
139 YRMSH DOSGC ZS9GD VRSWR QWHSC HXOSQ XSJXQG MISSEH OBSEUG LGANB AWEVY XCMXK
140 ADMYX DNMWE FWXZF RFRPO DRUUX AXUFG IMHAG KEXQI DULBU ABFHX JXZEX
141 HADCV SXXOJ ULPGT 1KQGO YXVDP DGRFQ EYLYS QXFTQG JYPRH TLWNZ JCTYQ
142 QOXHZ SYFPL APZWO HSCQG UYJCG YOOGH JAHAB HQYSG NISSC HGBVD BFBWE ZYQGZ
143 SITLX CGPJK JYKXW TUEQP SFJQS YWNEQ JYFPO GDXXU QXZAY QMGRK HXHZJ
144 RLYTVS NTNDL TZXNA UGUFU LIARP VXWFX ADACK QICHH IMQBX IYQPS MHGFL
145 NNRQV NTOHP QHYQT YXUBM JUMQV MDGOS QNPKH USKQO BYESA QBERP WJGRM
146 BMIELC PLBEO UADYT JHEDU GFHNA WXIXH BEMTH WTVVK WLYJW CDOWN YRRAT
147 YUGGQ UUBLG NUVZQ YCQZT ILAQQ PGSTK XKWCO YQFDU ZGUGY BCPUL KHTYV
148 TXXQYM YMZHV QYESL KBMPS GQFFD QOIRX KWWJQ JDWJS LNSPM KTSCP XSVSD
149 ISACT JNGYU YLZGO BCBPO RLXEP SQMWW PBKTY NEMRY XKXXU DURWH ZNSGY
150 MNNWUL SMXXM ZIDBO MLDPN NLCDR BRKQZ EFGQF SCTKM VYDOL ONJXS
151 NOCPN CORXN OKEWO JFRBO RAUDI JERSP WWXQR EKXZU OXQXU KHRWV YPVFG
152 VUENV NJHWW QNXSR JQXOW BZQHJ QOCWQ CROJW MURGK VYBHJ NDKXZ EJNER
153 YOAYO QLGYB CZKTD QCIOV RAUCQ ZIUTS JRJWJ EMQWE PUPFB QKQEB OTROM
154 ADSEP ZWFWU QOXLH ZOGSR BEHYT QPHOK OSHTO LHJTR BIYAS TKCTW ZBJSF
155 NENLD PJJMD ZCICO JHQIN JLYPKA HNHRO KSTFX IHPQI AMOQJ UFQFP TQFPM
156 KSQDS GDZKO RWJUV DCTOU SBEPP SNLUT YQIVW ALADD PFFGH IDQZL BVKXJ
157 KXHBEJ PAJPA HORDP JXEMR ZVQWO TKIEI IRORC AUJWQ KDUZJ KBLWH IRTOC

158 NEKNC MRMCT KGUVU EYXJY WITSN LQFYH JZJNX JDAT HKVATQ VQXST QXBAJF
159 GQCAK KEPFF KXCMW NZZWQ FQIYK JPKSSX WTVYL NDDCL MPMIZ HESBP CGATU
160 TSJKQ PZZHC AMWXM ZEBQX FQKBY UYHVF ZPKJ JQMLO QXQSR DQGGY GPXAD
161 YOPON TWAEE SVEBS BHYHJ KYZCR WDLIK XOTXX OMBNK UXIQY GPGLP RMDRK
162 YKQGE QDPJL FXALE PTLJU QGPRN DBAZC VQXSM GRTXJ JXCHV MCTQI QKBXR
163 QGQPX RDQSU LTPTH MNDQX VQUBN LGNST SQETQ MZGQY MREVD QWWEB
164 DHONG XZVDR NHQXG AQMSS CMCYD KIHXJ QXFTK WCEBG UQJLA UPDCQ XPYAB
165 DSZMM UVCCO EJGSR LBKQI FQZDN FQHAT QDLBK FQXBO RESDS FQZQR FQZQR
166 PPUSC UYFCM ENJSL TYPQF KBFEP YFJNU ZBYLO EBSNV VSTDH XISWZ TXUVO
167 PRHQC BTLVJ PHPFF YEHRN SVEYU NEFVS WGHZS KIEMK TCLBD MVRTH SFKHE
168 LDZAU FLZGC PAFPO DHDDR FUNKT FPRSC SXXQR CTQTV KZCQP FBAAN ZLYSC
169 NAXGT FXIKI SOZAD NWZQQ IHMUF UPEFB JQPEL SHAOW NZGKX NTFAQ FCQQT
170 PIMTX BMPLR KYKRD KCOQV NGBHH PRYNW KZHYR FSTXL ZQHKQ YQIQS MKRLF
171 HMNFK ZTUZF FEVQJ IFWAV LXTLB PBJDN BDMOS ULYNQ VTVGR VGLEB
172 BUXYD QSCGD WTQKO BYDPO PPHEG FOWLQ MUIQML AAMAP PORAQ EJBAU
173 AGAOL SNBBH QZKMB GJXTH OHSDU WFLBZ XYPEX WYJPX WISTQ IDEDP GBQMU
174 XYHNL UXBAY HNRSR DBEGO ZOHSX HFCOA VTQED KTHRV MYYUJ KXVGN TZMYX
175 PTCTM UXBAY HNRSR DBEGO ZOHSX HFCOA VTQED KTHRV MYYUJ KXVGN TZMYX
176 NLIWT WWFPK FYQXK DXGQF XOPAF YQUTE VVODS PGJTF LMJAN CAYLY QAQGC
177 SQUGS DLTVF PNHGQ DHZDD QHNDH FQWMH DFHIV LIDLG MBPZB WILYW NOMRY
178 TPEZH HGDZQ LQGIP WEDOL PPLXJ DAZYT MDPVY TDQPY NUFUX WUHTA RZJBR
179 ITGFG WTVAG TNYWK MLDHQ LQGCF WWYVS KDXTY CGMKL SARCOO VXNNX PKJPF
180 BSGXU DEQFL TFAPO BDYPO HZBES NQTFP GBJBG BJVFK NGBXN BZXMS NWSLG
181 BEXKL BYAOB BWVIS GBHRS TQKRV HNENY VQAXBV QBARV QVSEQ FABTO
182 AENUL LGJLZ XBRKV GPMWK RGFLT EOBST NHQPS QHGBX XXQAX KVERO LKQSV
183 TTQSH LFCGQ MSCOD OOCCA FWYAB GDFXG RYXEN WWSIC JFJWX QMVX EYMMM
184 DZGCN HCFPI BHOLQ NZETM WADER BSTWA LGEBI OSAEC LAVRD WAQGO XZCQM
CHAO CIPHER

EXHIBIT I

Plain text (in groups of five letters) of Declaration of Independence and Lincoln’s Gettysburg Speech, as enciphered in the document entitled “Chao cipher—the Ultimate Elusion.”

105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139

WHB9 NINTH ECOU
SE0FH UMANE VENTS QITRE COMES NEEEE SARYF ORONE POOLE ETODI SSOLV
ETHEP OLIIT CALBA NSSSH TIOHIA VECOQ NSCCT DTHEM WITHA NQTHS RGAND
TOASS UMEAM ONSOA RPOWE ROQFT HEEAR THHE SEPAR TATEAN DEQUA LSTRAT
INTO WHICH THAQA WERNF AUREO ANDOF NATUR EKSSO DENTU TLTHM RGAND
BOSB RSEPP OTOO HOFSN NSMNS OFMA NINDR EKBH ESSA THERT SHOUH
DBRGL ARTHB EBAUS KSSHI CHIMP RTHHE MTCHT ESEP AATATI NNESS OLTH
BSTHR UTHST ODEBS LITFV IDENT QTHAT ALME NAREC RASTE DEQUA LQTH

† Gettysburg Address ends with “T” in “RDIUY.”
CHAOIPHER
Exhibit 2

PLAIN TEXT IN LATIN OF EXCERPT IN CIPHER FROM
De BELLO GALLICO

GALLII AESTO MINDS IVISA INPAR TESSTR ESWW W HORUM ONMIU MPORT ISSIM
ISUNT BRELO BYPLO PTERT AQUOD ACULT UATQU EHUMA NITAT RTPRO INCA
ELONG ISSIM SABIU NITMI NMBEQ UARAD OSMER ESSAB BPECM MEANT
ATQUB RAQOA RABEFP FEMIN ANDOS ANIMO SPERT INENT IMPOR TANTY PROXI
MIQUE SUNTG ERMAN ISYQU TTRAN SHEN UMINC OLMINT YQTIB USCUM CONTI
NENTRE UBERL UMEYR UMTWQ UADEC UASA ELVEL LIQUO QUEREB LIQUO SGALL
OSYR TUPET RACEE DUNIO QUDIF ERBOO TTIDIA NISPR ORLEI SCIEU ERHAN
ISCON TENDU NTYCU MAUTS ULESI NIBUS EOSPR CIESB NTYAU TIPSIC ENVOR
UMPIN IUSBUS ELLUM GRTENN TITWHR ISRBB USFTIE RATUET EMINU UUSLAV EVAGA
REENT USTREM INOF ACTIE FINIT IMSIB ELLUM INFER REPSO SENTY QAEX
PARGET HOMIN BSEL LONDI CAPIF TMAQ ODOLO READP ICIEBE ANTUR WPROM
UETIT UDIEN AUREM HOMIN UMTFO ROGLO RITABE RUPFO RINU TINDI
ANGUS TOSSK FINES HABER EARBI TRABA NTQUIN QUBRI LONGI TUDIN EMMIL
IAPAS SUMOC GXYLI MLATTI TUDIN EMCLX XXPAT EBANT WWWAD EASBE SCOTF
ICEN DABSI ENNUT MSTBI SATTIS BSSBD UXERO NTYIN TETRI UMANN UMPRO
FECTI ONEMD ERGEO NFIRM ANTRA DRELB ESEO FICEF NDASO RTEST RIXDE
LIGIT UWRIS SIBIR EGIATI ONEMY DOOV TATES SUSCE PITTUE NEQUB INERE
persu ABETT ASRICT OCYAT AMANT AORED ISFIL IOLVE QUANO YCUUJU SPATE
RREGN UMINS EJITAN TSMUL TOSAN NOSOBI TINUE RATER ASENZ UPOP UURO
MANTIA MIGUS APPEL ATUSE RATUZ TRXXN UMINC IVITA TESUA QGCUB ARETY
QUOOP ATERA NTBHA BERRA WWATH ACORA TIONE ADDUC TIINT HRESP IDMEM
TUUSJ URAND UMADN YETTR EGNIO COUPA TOPER TRESP OTITD ISSIM OSAFC
IRMIS SIMOS PEPOL OSTOP IUSGA GLIAE SEESEP OTIRI POSSE SPREA NTW
EXACT PLAIN TEXT OF ENCIIPHERED EXCERPT FROM
CONGRESSIONAL SPEECH BY GENERAL OF THE
ARMY DOUGLAS MACARTHUR

Beyond pointing out these general truisms, I shall confine my
discussion to the general areas of Asia. Before one may objec-
tively assess the situation now existing there, he must comprehend
something of Asia's past and the evolutionary changes which
have marked her course up to the present.

Long exploited by the so-called colonial powers, with little op-
portunity to achieve any degree of social justice, individual
dignity, or a higher standard of life such as guided our own noble
administration in the Philippines, the peoples of Asia found their
opportunity in the war just past to throw off the shackles of colo-
nialism, and now see the dawn of new opportunity, a heretofore
unfelt dignity, and the self-respect of political freedom.

MusterIng half of the earth's population and sixty per cent of
its natural resources, these peoples are rapidly consolidating a new
force, both moral and material, with which to raise the living
standard and erect adaptations of the design of modern progress
to their own distinct cultural environments.

Whether one adheres to the concept of colonization or not, this
is the direction of Asian progress and it may not be stopped. It is a
corollary to the shift of world economic frontiers, as the whole
epicenter of world affairs rotates back toward the era whence it
started.

In the situation it becomes vital that our own country orient its
policy in consonance with this basic evolutionary condition rather
than pursue a course blind to the reality that the colonial era is
now passed and the Asian peoples have the right to shape their
own destiny. What they seek now is friendly guidance and support
not imperious direction.

The dignity of equality and not the shame of subjugation.
Their prewar standard of life, pitifully low, is infinitely lower
now in the devastation left in war's wake.

World ideologies play little part in Asian thinking and are lit-
tle understood. What the people strive for is the opportunity for
a little more food in their stomachs, a little better clothing on
their backs, a little firmer roof over their heads, and the realiza-
tion of the normal nationalist urge for political freedom.
ENCIPHERED EXCERPT FROM SPEECH MADE BEFORE BOTH HOUSES BY GENERAL OF THE ARMY DOUGLAS MacARTHUR

A Glimpse of Chaos

506