

Chaocipher-Related Material

From J. F. Byrne's
"Silent Years: An Autobiography with Memoirs of James Joyce and Our Ireland"

February 2009

This document contains Chaocipher-related material found in J. F. Byrne's autobiography "Silent Years: An Autobiography with Memoirs of James Joyce and Our Ireland", published in 1953.

Chapter 21 recapitulates the story of his cryptographic invention he called "Chaocipher". The chapter tells the history of his invention, his attempts to interest numerous organizations in the cipher, and concludes with 23 pages of corresponding plaintext and ciphertext enciphered using the Chaocipher system.

The chapter concludes by betting \$5,000 or the total royalties of the first three months after publication of the book that no one would be able to solve the enciphered passages at the end of the chapter.

This document was produced from Albert Einstein's personal copy of "Silent Years", (currently in the Hebrew University in Jerusalem, Israel) sent to him by the author himself. Notice the red markings Einstein penciled in regarding paragraphs that interested him (e.g., pages 264, 266, 267).

p/

בית הספרים
הלחמי והחוניברסיטאי
ירושלם

JEWISH NATIONAL
AND UNIVERSITY LIBRARY
JERUSALEM

FROM THE LIBRARY OF THE LATE

PROF. ALBERT M. EINSTEIN

1955

1114 New York Ave.
Brooklyn 3, N.Y.
June 30, 1954

Dear Professor Einstein:

Although I do not presume to hope that you will read this book, yet there are a few subjects in it, especially the chapter on Chaocipher, which might be of scientific interest to the Institute for Advanced Studies at Princeton.

Cordially,

J. F. Byrne
J.F. Byrne

*In melancholy mood I wandered forth
Alone.
For I had left the fetich of life behind,
And in the darkness stumbled wearily on,
Going I knew not whither. Things I did
That to myself seemed strange and meaningless,
But still pursued my erring, lonely way.
Much did I yearn to know—nor got reply.
So, worse than sad, I felt that I had dreamed,
Was dreaming, and would dream till the end of all—
If end there be.
Just then I sat me down awhile to rest;
And with my heavy eyes I vainly sought
A refuge from the gloom, but all was dark.
Despairingly I turned and looked behind,
The way that I had come, and there beheld
A bower illumined with soft, rosy light.
Instinctively I knew it was the home
Of living love; and thither I resolved
To wend my way.
Whilst thinking thus I heard the heart-born sigh
Of one approaching slowly through the night,
Seeking, like me, the distant bower of love.
Weary she was; so having come quite near,
She sat beside me, and in sympathy
I took her hand, but spoke not any word,
For ours was sorrow kindred. She but came
Nearer to me, until with joy I felt
Her loosened tresses fluttering at my cheek—
Then did I boldly take YOU in my arms,
And kiss your yielding lips; whereat behold,
WE stood illumined in soft rosy light!
Wonderingly we saw, till that we gazed
Each in the other's eyes; then we both knew
That HERE was LOVE.*

J. F. BYRNE

Written August 1898 after visiting
Lugnaquilla and Vinegar Hill

CONTENTS

<i>One</i>	ANNA LIFFEY—I "WOKE ON ITS BREAST"	1
<i>Two</i>	"HOW MUCH ARE YOUR PENNY ORANGES?"	12
<i>Three</i>	IVANHOE—MY GOD—A NOVEL	21
<i>Four</i>	THE WHITE BISHOP	33
<i>Five</i>	CONGRESS V. HOUSE OF COMMONS AT CHESS	48
<i>Six</i>	"DISEASES OF THE OX"	58
<i>Seven</i>	"GHOSTS" IN HOUSE ON CORK HILL	67
<i>Eight</i>	"PRODIGAL MEDICAL STEW-GENTS"	74
<i>Nine</i>	I LEAVE NO. 7 ECCLES STREET	89
<i>Ten</i>	THE IRISH GRIEVANCE	102
<i>Eleven</i>	CONTINUATION OF "IRISH GRIEVANCE"	123
<i>Twelve</i>	APPEAL TO END CIVIL WAR IN IRELAND	134
<i>Thirteen</i>	I VISIT JAMES JOYCE IN PARIS, 1927	144
<i>Fourteen</i>	JOYCE WITH ME IN NO. 7 ECCLES STREET	153
<i>Fifteen</i>	MIDNIGHT IN THE HELL FIRE CLUB	172
<i>Sixteen</i>	I LECTURE ON SPINOZA	178
<i>Seventeen</i>	COUNTRY LIFE IN WICKLOW	192
<i>Eighteen</i>	INTRODUCTION TO "A PARABLE IN GOLD"	222 X
<i>Nineteen</i>	"A PARABLE IN GOLD"	238 X
<i>Twenty</i>	INTRODUCTION TO "THRONE OF CHAOS"	248
<i>Twenty-one</i>	CHIAOCIPHER	264 X X

CHAPTER TWENTY-ONE

Chaocipher

IN 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 or persons 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 the 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 chaotification 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 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, that if 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

October 28, 1920.

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 3, 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.

Before the end of this chapter I will consider further the general subject of Mr. Lovett's remarks, but right now I want to get on with my story.

During many months after receipt of the foregoing letter I succeeded in achieving nothing, and then in the following year, 1922, I got in touch again with Colonel Hitt at the War College in Washington, and he wrote me in part:

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.

ADDRESS BUREAU OF ENGINEERING, NAVY DEPARTMENT
AND REFER TO NO. S67/68 (11-18-W9)

NAVY DEPARTMENT
BUREAU OF ENGINEERING
WASHINGTON, D.C.

7, Dec. 1937

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 RLAZY
DOGT0 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 In-

dependence, 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 follows:

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	
Dash	H"	

My correspondence with the Navy Department continued for several months; and, by appointment, I went to Washington for a preliminary conference on April 4, 1938, and a few weeks later, on May 3, I returned again to Washington to give a demonstration of my device and principle—a demonstration which was not even begun before it ended abruptly.

At the proposed demonstration there were three Commanders—one a senior officer to preside; and two younger Commanders, whose names were Wagner and Tucker, as assayers. Wagner being a cipher "expert" while Tucker was an expert in radio and electronics. I can only say about this "conference" that it ended before it began with Commander Tucker sagely suggesting to me that I should take my device and system either to the War Department or to the State Department.

For the record, let me say that since 1920 I have consistently offered my cipher system to the various departments of the United States Government for a "nominal" remuneration (some-

|| thing like \$1 a year), provided that I were allowed to develop the commercial exploitation of my system. In one of my first letters 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 adoption of your system, it would elect to purchase your invention or merely the right to use same for Governmental purposes leaving 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 universal 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 revealed 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 Department'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-

cocted. 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 unhesitatingly express their conviction that there never was—and that there never will be—a "cryptographic expert." These "cryptanalytic 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 explanation 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 13, 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 insipid, cautious, 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 decipherable. 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 OD,QU ICKBR OWNFO XESJU MPOVE RLAZY
DOGTO SAVET HEIRP 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 227; 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 248. 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 35 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. Ralzemond 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 35, 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

paid by me out of the royalties accruing to me from *Silent Years* during the said three months. And if the royalties accruing to me during these three months do not amount to \$5,000, I shall give all the royalties that shall accrue to me during that period.

To the first person, or persons who may send me identification of the re-enciphered words in lines 34 and 35 I shall give credit for having submitted prima facie evidence of being able to decipher the whole of the number four exhibit; and such person or persons can then at any time, within the given three month period, give proof of being able to decipher this whole number four exhibit. Let me make it explicit here that anyone who *really can* identify and decipher the dozen or so specified words, must, *ipso facto*, be able to decipher the whole of this exhibit, because it is all of a piece.

And to all "cryptanalytic and cryptographic experts," including the Major Yardleys, I give cordial invitation to accept the challenge I make here. This invitation is extended also to the members—both individually and as a group—of the American Cryptogram Association, and its local affiliate, The New York Cipher Society. And finally, I issue to the believers in the wonderful capabilities of electronic calculating machines, a warm invitation to take up my challenge. Perhaps the genial-looking Professor Norbert Wiener of the Massachusetts Institute of Technology would like to embark on these waters of chaos in the hope that his cybernetical pilot might, by the exercise of super-human navigatory prowess, be able to steer him to some port.

One final plea I make to all my readers in regard to these dozen or so re-enciphered words in exhibit four: Please do not send me guesses—they will do you no good.

Chaociphering is not guesswork. There *never was*—and there *never will be*—anything requiring a higher degree of exactitude and truth. Often when I look at the crude model on which I have done my work I feel as our beloved Keats felt when he apostrophized "The Grecian Urn":

"Thou shalt remain, in midst of other woe
Than ours, a friend to man to whom thou say'st
'Beauty is truth, truth beauty,'—that is all
Ye know on earth, and all ye need to know."

CHAO CIPHER--THE ULTIMATE ELUSION

EXHIBIT 1

1	ALLGO	OD,QU	ICKBR	OWNFO	XESJU	MPOVE	RLAZY	DOGTO	SAVET	HEIRP	ARTY.
2	CLYTZ	PNZKL	DDQGF	BOOTY	SNEPU	ACKIU	NKNCR	INRCV	KJNHT	QAFQP	DPNCV
3	LTVFI	COTSS	LWYFI	HBICF	UTHXN	UVKGI	MVEZY	WSTHE	PIEWX	NNGFT	OGHSR
4	TBZXT	MVGLT	JXCSQ	XLNJT	ENCSV	LCWRT	BENZL	SUVYI	DAXLA	FATQS	RNZOP
5	HKYGQ	JTOGY	SDBNV	DJOWH	KECRM	LYWIQ	IFIKS	CYJGC	VXNSK	YHRYV	YEDSZ
6	RIFFZ	AQNHS	OMJPO	RWTJO	IJIPK	VHZGP	WQKRX	DMAUE	FFXIA	CFLOZ	MAFZS
7	JEOZI	FKJCF	METES	YHZU	VLFFU	RRHRI	IFFDZ	MTTOV	KLZOV	LPVPP	GVGEW
8	WEFRF	YHKXO	PKXRQ	SZKLC	ZKHZW	XRJXL	MVFGG	FGYIF	DAEIN	IWPOM	OUVRF
9	BUZLA	GDBCU	AMFQL	ACRWW	TUGSM	PFZBR	FASRO	YIRCA	GVEYN	SRTQ	TDLFJ
10	RUTKF	KASGV	LVYVF	VRAIY	NIVJK	IUWPF	ZBVRU	EOTEJ	GLCGY	SSNHH	QTIQW
11	UKQAS	XKGSP	WHRYM	TQSOQ	BAMAP	FQRLI	IUGTI	VBEBY	XFBIU	SEYHM	LKGOE
12	CSWUH	TBIZZ	HLBND	IWTQA	MAZBM	YMBEK	LUYRE	UGSKT	IMDWR	RNONJ	KDPTC
13	EBVUJ	EQIAE	MOHTG	FHFFI	DIQQJ	UAWDH	WQDE	RERHL	XWAMY	LRVPR	JFHRA
14	JDCJN	BVEOU	TWXOF	GRXND	KITNL	OXSLZ	ADDQC	BZWK	NPJAX	BYUKI	JGVUC
15	SDJWW	OIWEV	AVMRR	NLRJM	IFDHH	PFQRI	YCLLZ	YILTW	JBPAF	LPOIO	ZTBPI
16	ACJHF	XRALO	VRLZU	VANAB	NZDZT	NYEGS	ZWGUR	IFIPW	UMTLJ	YVYNE	ACGJX
17	USRXC	DCITE	EKMJB	HPPYO	UFFXC	PBWYQ	PHMTA	XNROB	ASQRZ	YVJXO	HUXFP
18	QPDLA	BSYMU	DOKYD	WRXCJ	WRXCJ	WRXCJ	WRXCJ	WRXCJ	WRXCJ	WRXCJ	WRXCJ
19	BIHGG	PKRFD	MWTOT	MKBOL	BRNO	CHWLQ	DVNEE	VXBNE	GHJQQ	CVIEF	YMEQR
20	XSYEW	VJZTQ	XDEWK	WSWIE	EHDNS	RHRCV	DUYOG	NGVDP	RHUTY	KPRAO	IVCUJ
21	DYVLO	WBMGS	TFTXU	VOXGZ	ZUIIR	YXSAY	EPRWP	KQJMS	VGYBN	ECJOK	CNMFP
22	GPHLK	QQMBS	LPMAC	OZCNB	RYAUO	HNHBE	SMIZT	CEOBF	KWXCE	IOXZX	EEIVJ
23	HGLQP	QHMMF	HXETY	YPEAQ	BUDWK	NDXDZ	BSLXX	XCTLH	CIWBI	QHXHN	YFYNH
24	NHYXA	RKZMC	RNZTO	NKZKO	SGNWF	KJXRP	QZIBR	CPXCW	FCCIM	EKLBA	BSHYA
	EYGFQ	DVTSD	RQBSV	RFKQG	UQVTK	CBERO	IETFA	TNGHQ	OAHBA	MSXAK	VKBSY

25	LRORO	IXQEZ	APHAF	CFFQW	OZJUL	UZBEQ	AGYIP	ZPHAB	QQRIX	IHRMS	LJTSB
26	HHCVA	HUPWS	FMHVH	JTRHA	FDJFW	CLEWE	KUMFJ	INAYG	KRSLH	NJFXV	THFPU
27	PHULQ	IZGLQ	IMGWB	EAVTJ	AAPUM	PYEMG	DMUAG	MAMZO	TIRTT	OWFVN	KCYAQ
28	GZRFQ	XMBAV	IXJCW	NLIEP	ENPVK	IMNSS	QWFR	UMWEG	GJUNR	QXTAT	EBLDI
29	UEZTE	XHZYV	WGXSQ	JGQHZ	VPPAW	LFSHD	USONO	QORTC	MRNCE	SRVXQ	QWLJV
30	ISRPS	BHJDV	YSROS	REHED	DEBAW	PDOGJ	MXAVJ	KETMA	PTTKR	HQZAN	XNGLM
31	QWJDT	CQCYO	UEYYC	DNCPS	HDRPG	VNEAL	LJJMG	HGAOQ	GRRHN	CARAI	QUKXS
32	IFUTU	TEQMB	JAYYP	XCUTT	NGFPX	NWFOZ	YSETA	ZWVZZ	LWPNL	MCQNP	PQCEL
33	ZMUEL	JYAJC	PMLNT	GDWEL	PNEQX	SVMXU	AMSJI	MTJIB	YNXTE	FYBNO	ESLMN
34	VFYNP	QHMMN	IDEIH	ISTYQ	QVDRN	ZIBXA	IKSXO	KESPN	XIMTE	KILQX	OPONS
35	NZPWQ	ZEPOY	CYCXJ	FACZA	EBXXG	MPQDH	NQTPP	WXKIM	ASNMO	LVCVT	OPYVM
36	SESPC	SSLSG	PFQZW	PBIJO	CZIPA	FAPFP	GSMOG	UFPME	BYEAL	EIOEH	VKJVV
37	SYSOC	EAGXA	SVYZE	DCJRJ	TIYBD	INAOB	YBGLP	BRXZA	NBCHF	DZTNJ	IGPFC
38	UUTKM	GSURU	LBJCM	NIQKC	XBJIX	OIZHT	ACVDK	ITWPH	XZCPM	UEDBI	TSTCK
39	VCPUF	YHIOW	BSBKF	ZGRBE	YVGSQ	YCNVT	ORGVO	FRYFJ	JEHTB	WYAKI	MMZQR
40	LQYMR	QOSGK	CVVEL	TCYSV	LLYHS	HMAZC	XCQNK	KTCBH	ZNOMM	PTKKW	QYSFM
41	OIQKK	ELZNC	XVBRZ	GGOKS	CGPBP	LARQL	RTVYO	XMZCW	EYBIH	OZMSW	XCIBO
42	USEYC	YDPVG	BPCUG	DVEVC	GKCAU	PYZIT	DITNZ	XVKPY	JROJI	DQHIN	BWCVV
43	FDEVG	HWWYX	LKKKF	IHIIZ	AXOPI	DHUWQ	XNWLM	YVDDH	GOIAZ	SCCQF	ZULJA
44	OOLCM	ADUWY	TLYVT	QWQTG	HENGO	ORMJW	ZOEWT	QLJCF	BUGAI	EUMRT	DKALN
45	VVOON	ASBIN	QWRPB	FCGWZ	KNVXG	QTXJB	IQZYO	XCFKU	SOTXN	NYRNV	YOHDO
46	AXDDA	CDLRC	VKOMS	XIHQI	TUNOM	AXDMI	SISFS	MBYTL	SAFEI	PGCNH	FMLFE
47	AEXFA	UPOKM	SBMNZ	YUHEM	ZLBQM	ROIUH	KECCE	IXDAR	VFAEV	WDHPS	GYTTA
48	ZRNTO	WRSTD	YOKCW	NQUIS	WEFIF	LFFZQ	BSDCS	CBNRQ	SZLXB	BRICQ	CLSCB
49	INRYO	RGNZE	GCIYAW	PMCQL	CGBMX	BBUBO	NQOZZ	OFNQR	YMZWA	CDMGX	NAIRA
50	ABKCI	OWTGT	CTOOK	MFRPG	XADLN	AAJSU	BMTIQ	VHOUZ	TBCZA	LEOPO	YVEWO
51	USDUN	TZTJT	YXUIG	OZQFS	VDDSR	JWUFH	FGIZS	ORJTB	IVSKB	BHMPQ	NXMKW

52	AGSNT	KJWOX	HALOV	WEXTS	VKIYF	ADOMO	NPZCZ	FZROC	BIRWP	UNTAX	WXSER
53	PGPPU	RINGD	CGFDG	ZALDT	NXPUG	EPQSU	ZVKDO	TXTEN	MUQAS	ZKIGH	WQRQI
54	DWXA	TYXBQ	QCJWF	YGNZE	FMABH	SBFPX	RCYGT	EQOTR	OFXXH	XEJYD	QLKIL
55	KRNXC	HWTWL	EYFHB	TUZXZ	JKVSC	VOYKJ	NRCLO	OZARV	LBSZG	TYHGU	JZHZV
56	WTWCP	CJURA	BTHXC	NSUHC	GQYEA	LLUPI	CHXEU	STQXX	VTPBN	SSGFH	XJKGA
57	MXECP	QSVIN	ZQFVE	MKKQU	EMQJA	ZQVST	GBCZN	VIMZK	OTWVY	AMIBJ	ATZCJ
58	WMDTM	ZJFMZ	ZNCCD	OVLZF	ALKUV	ABWMM	QXEGF	UCTNG	CFZKU	BACBI	URQBB
59	JUYTY	JGBIJ	LFUFI	PPIUW	JMSYK	WUPMY	DEJOP	RCGAU	OWGLU	BCHIK	DMTWK
60	WBSIA	VNKOQ	GSPYV	NYUZY	RPBHG	ZXIRA	GIGFN	XGZFM	WOCGL	XMGDK	RNQQB
61	XTVGN	LEOWT	SQJXC	OXMKB	BQXBC	HLWRI	BDKLZ	CXZBE	MNYUJ	BAJLP	BSGQD
62	SSAZB	DBXTS	WDJBS	REUJB	ZXBPC	ACTVN	NPJNH	FZDQC	YCHMM	FKHUS	RNTKW
63	COTOX	GXTBU	KDRBC	ZYZNC	YXLCA	KQMIM	NPJNH	OPAJN	VBWWF	SZKXD	RGSNR
64	XNIEK	GFHYJ	LIORG	OFSPJ	HBHWD	MIOCW	OHZCD	LYSSP	XUZTK	SMMCG	EAUMT
65	MQRVY	WLJFB	VVJFN	LIKIB	USXXT	HOKZO	USRWR	UHUEV	JKTUZ	UVJKJ	MZJYU
66	HLWJA	VTYTH	RCXTI	ZHDCM	KTWFT	JISPR	CENFT	OXOFK	QCRUB	NGLZG	XRPMT
67	PEDGQ	DKKHQ	AYWRK	AQQXR	SVEFE	OAXQU	LXYUB	ZOPBK	MKQLM	MZABC	THZKR
68	JAZJW	DLNAA	PMJHG	WMXBM	UPULD	BRDJK	FFZYW	KCENN	EQZQL	KEAKL	AJMPT
69	IBWGB	UATXC	YUTKB	NPWTO	QRIGB	NFTZF	TIGSV	WHEQG	DECFG	VHOFM	AIIRP
70	NXQRE	FBYCB	EDDZM	RVSIE	DYDI	BVGRP	SBTFE	WLVGX	GUZMK	YSYVL	LODQP
71	STZRN	JTINY	WRAWA	NCJQS	BLXNE	MEHFB	CIWHC	ODUJF	LXHLV	KASTO	VPPEV
72	UGBMC	UVYXX	HNBMZ	MEYNE	LCINY	VBVVB	VCMAJ	DIJIM	ZDWOU	YLGFO	VTXXG
73	CDYCG	TQFTF	KXSPI	CISAG	WAJBK	ANRVK	HGLMK	JFDPE	BJLGS	IIYAH	GPRAC
74	YCGTM	QXEHV	UFDJG	YHPZD	RQNJQ	COEBJ	IFECA	EUDCP	AIDUK	NBGTU	OJGJV
75	LQFSV	UTZAS	CQDQB	GDJBN	ZOATI	TQEVJ	XXNBE	ICFPE	WJCYI	RFYHA	UDTSC
76	DBCYC	LYMRD	QMFYT	GVOJE	AYVDY	XLBBT	WROYW	YVPCZ	SYTMM	QYCPG	JZJXT
77	QZAPN	PHRAQ	XIORJ	HZAZA	CYQDQ	FKEHG	UTNFV	TEUOQ	KIIHF	AFUAF	WHOFS
78	HJBIN	HFRBF	XAZMI	CUKWE	GFQRT	FNKYQ	LJYES	IAAFR	RKCQN	LFERD	FKDKS

79	MQUON	OYXGH	PITVG	MOQDE	GYGKU	BXWNT	TKNBF	BPWQD	IMTIV	ZWWMO	IOJZQ
80	MOWLH	YHDWQ	JADWC	JCZZT	TYAUW	UJRFK	SLXXM	VEUVH	TWUUP	XVRHK	PCHSM
81	WLPLQ	TBJON	YVEITM	MFFGH	VEJEP	IFSTY	NCLUY	IYOYC	SYDUO	QXHYD	GSYMB
82	XGWBG	NWDFY	TLEEK	DJUJ	XZRTC	SZEJR	FXLNQ	QYLPN	NWARU	CLRHS	BOMOE
83	OAIQL	IXYNS	AVDAC	EIBKU	DKADM	YPRMY	TQAWH	AVTXO	OPBFY	SZDYK	BGSJD
84	FCNLQ	NWAOG	NTQIV	JZRV	IACOO	KEYIN	OZBNP	KEGHF	JFASY	SDIFB	NXNXF
85	JPSAM	RVBQG	XNIZB	MVGUV	VNFMU	FJXEL	BZLTP	IFIWB	LBXPB	QDXAW	FRHBF
86	QPDQM	OXOSU	MMERK	QNMVF	YKDOC	BOXIY	SPLGV	PBLNG	NKTAK	YNGBX	MIPOM
87	RIDCL	TCIBZ	HFLDV	RXBKF	LPRKM	CQHEY	RAAVH	XAYDH	NNNUN	JCINA	RAEXP
88	UAQRP	RUDMO	OHOOM	EMGUP	IEEIX	AQTLU	PETXI	BQEPN	IWBRE	BNSEQ	RDUGG
89	TGWUR	QRJRL	XGRDP	MJPD	TSDBG	YYQDR	DQYSZ	GLXDR	IDLYX	FIVSQ	WZVQG
90	QRLN	LELGT	EGHVN	ZXRFN	HFQOW	XIXBE	ULILO	MRXQO	GJXRC	JOUZH	OTJAK
91	DMFER	TTWFO	XVGVE	UIBDG	WUGTF	HBNXM	EZNHB	COGDE	BBOPZ	ZWMTR	YRSDX
92	CUTFL	PHZYV	HTOTI	JOPJP	QTPMU	ZJYLU	FPULW	LWQOI	AMJRS	RAWNQ	THMOW
93	LHUGS	XSNKF	LAUOT	UMXYT	OFRYZ	IRIDT	ESKKM	OGJHL	BBDOD	RLSWZ	RRGVA
94	VOGEN	KOOZX	MGWQS	TUGJS	WSOEU	CIOYT	IZYSE	WUWWL	PXMF	RRRPV	PHVAC
95	KESYK	WKPJI	FOJEQ	LZZOK	RMBSG	LQYMR	GAPCT	ZJGHG	GRCLY	XPHXY	LBKIH
96	NSOZO	MTAOE	YJCBY	IXDVZ	VFENU	DIUTJ	GGPTE	REYHK	QLDCR	UMBKN	RSXQT
97	CVXTB	WQXZK	QOSIM	ELPDR	OVWTR	PITOO	NSRUF	PGQVS	YBQDK	OLCBV	NXBUC
98	GZMMW	IKOWW	ZEZFF	DWSLY	UTGXP	LMDUF	ESIHP	KUCXM	MFQQM	QIOPA	LOFBF
99	PWSDP	SMDZL	ZOWOB	IVZFK	NEUBS	AAIZY	XOKGP	VQCHE	QUHGV	OFZZJ	DNSTP
100	VWSYQ	SSYNT	HGBTW	ZBKGL	IDSAF	ARCJB	WJDOQ	GGOQO	DVRHK	OBYTI	KGNSS
101	NVCCP	HCZQV	AWFWI	GMMMB	TZPTG	AIYZV	PZDYR	HJVJT	BPTPJ	ADLWD	XOGUL
102	WVDGK	FGETB	BOHDT	JVYTD	IFHXX	VPLUM	SZBMA	VKUDL	ORYBW	YQVIN	UMUSC
103	HQQBD	XIDWX	DPZDW	PDCHC	BNOAT	WYDCG	QXBUB	JVAGG	OSQBB	GVOCY	YPIBA
104	QBLLB	BBDCS	LZEMS	TUWJV	WLZRO	FVMXS	LAITG	BHPEK	SIIEF	LKULQ	WRMPX

105	TUUXW	AIHAC	SMFKU	GSKFZ	JWBJZ	RPZEA	RIQLG	ZUUHW	JSHVI*AIYVI	GOVDD
106	RNFIW	XEKM	RKBSC	WEKEX	NXXQL	JJKPD	REZEI	ZAMOO	VHOEH	CKCES
107	AKDFL	FDDPJ	MSBLU	FXUIN	MDKID	WCRVA	WMXEE	SIKVS	ZTAOE	POMRV
108	LYMNQ	FIZIL	XCHYH	HKEMO	IMRCK	NDXDM	MZEPI	FUMKG	DGFFQ	BVLDY
109	LBAOW	LOZSD	YZFQE	CGTAT	TDSEX	FVKJA	YIVNU	QWYZX	XDYL	VXZPX
110	BZNM	FFWNU	CTFXK	VFBSP	UMEMJ	SAEVB	PKLBQ	OYMJR	XQJQG	RHSQK
111	ZUOEE	DCYRQ	PHZJC	DIRIK	QFRLT	OBPLD	BOLWB	VLJHJ	NRJUY	YFPUO
112	BIHKW	FFWUP	OKOOK	HZMPR	OKWET	WJWRZ	IDQYD	EJWYT	RVVPK	IHKTR
113	LOFRS	OEYMQ	MHSLF	GVGAH	EOOGW	JOJNM	CCNDS	DRGJA	BJYOL	QAQMC
114	FASLV	SVWCV	OAQRT	XCBJJ	YMRKH	ZOVAD	BWJFH	YVTJX	MLSQT	VZBYJ
115	EPQJS	CELSV	VXCKB	OYRTN	WICAI	ILULK	JZYIY	OBUDE	TKCCS	GRFJC
116	VZDUJ	KISDE	QFIMN	GRYMB	JZKUW	EMFHV	KNDZB	OIXDV	ISKUH	HGDGO
117	PCQZY	EXMWI	MOLSF	PDZPQ	XLBMK	YFUOM	FRWFL	RKBMP	TKLUR	OLYKZ
118	EYIHE	SPUOH	BNPSM	UQOAG	FVSAL	RFLYO	VMBTM	NNYQY	UQXGG	HWUTZ
119	SPDIX	EUYCN	YCEXU	JPMPP	THBGQ	HWBKD	VUHCF	NAQJM	OBZER	ITGEQ
120	ZCZHW	RWRRR	OHNTZ	GMQIU	TSPHS	ULCFT	MUGLD	GHVDS	UJURN	VXLIS
121	DBPOO	ESCJM	ROFLJ	BEDGI	UVAJK	OYSQJ	EUNJL	YMCUW	IVRWU	BKJXI
122	DOWJT	UFHZZ	HBWLG	PDNMZ	NNFPQ	DVBNG	TXXAC	NCEBM	QRCGQ	ZMBYS
123	OWRCJ	PZSME	NEJJE	OMQMI	IZEUZ	GXDQR	WBKZS	EXSEP	WWNON	ODUVL
124	VNHMX	VAQLH	JHQLW	QJYSM	VUYGW	ODMEH	NUPWV	NDWTT	EZUDQ	PJXOT
125	JEHAJ	HRIOF	QXIIH	SELSF	RAXFN	PIRCA	SKNRB	ZTHQK	AFBMS	ICTDB
126	PMDDT	GCWOR	SDAXB	FMKIU	ZMMKM	KRIYQ	NQFLG	QVBVD	XESGN	HIOCV
127	HBGNN	PQNNJ	WSDUD	HUAWG	VNWIK	MJRHX	NNMMN	BOIAW	DYDDK	AMZJF
128	JKKBX	OFRET	EAMRP	GAOMR	CDOFK	BQRAJ	CSIBX	XVDDK	ZZINP	OJPKW
129	EHZRL	XNCAE	RWAZZ	GCQPN	BQKPS	NSPLO	HLZEP	JJYQY	YFJA	MLZHS
130	ZNEXA	WPTZF	PTGYP	AVQTE	FZZZV	JHTTT	ICXNA	QASEE	MBDMK	WKNMH

• The Declaration of Independence begins with the "H" in "JSHVI."

131	XYRUW	MBTXT	HYVNG	ZLXL	VTZDC	QMVFL	CBBYK	BMESG	HSOEP	SKPKE	WMEQW
132	COQNB	URIIQ	BNQOG	AAXPE	ITCWN	ZJKXL	EKTTQ	LQEOS	NDBQF	MBYIV	DIAKZ
133	FHMBX	LQOLK	MLNLZ	QLAXE	UQOWZ	PDOXX	ACNFR	RUCIN	YQDHJ	BCTUD	GBLAI
134	EPPKO	DVITL	XJSOC	UZYHN	KVEGP	NJROY	YDKIM	OKSWL	OPTOD	ILTSV	SFYXC
135	DNMTH	QVWTU	FETHE	DTIWZ	ADLAH	KOMBR	GEMAH	GSCHA	OCUZA	OYQGB	YWKMT
136	GWYAJ	MAGYS	KHOSA	RGVWZ	PODNM	OZNGY	MEYAK	KIKMQ	GFJIW	EFAOK	MDUYT
137	JWWAH	YOIIX	REKWJ	BALQV	AMTJS	ZGDAF	BIEXV	BVUEC	AUCRP	PJKQY	DPBUL
138	TZNWQ	KRXDC	EHROQ	JLDGM	MTWFK	GFMK	XOXSQ	MHSSH	OEEUG	LGNAE	AWELV
139	YEMBH	DOSGC	ZSGDC	VRZWR	QWHSC	AXUPG	IMAHG	KEQXI	DULBU	APBXH	JEZXXZ
140	ADMYX	DNMKW	FWXZF	RFLFO	DTJCX	DGPRQ	ECYAZ	XQTFG	JPYHH	TLWNJ	ICYTQ
141	HGDCI	SOXXL	ULFGI	IKQGO	YXDVP	JOAHS	SVQYG	NISSC	GNEVD	BFBWY	ZLOYB
142	QOXHZ	DYFXO	APZHU	HSCWQ	UGCYI	YWNEG	JYPND	GXYTU	KEXAE	QWLWD	XIGYA
143	SSTXJ	CEPKR	JKYVW	TUEFQ	SFKJY	LIARF	ADAKK	QICHV	IMXQE	LYQPZ	MHKGf
144	RLTYS	NDFAL	TTZNA	UGFUF	QVGFH	MDUOS	QNZDK	USKOQ	YBZJA	QBONF	WJRUW
145	NRQVN	TOTHF	QQVTH	OYBUM	GFHEA	TZIXH	LBITH	IWVVK	WVLNJ	CDUWN	YRRAI
146	BMELC	PLFEO	UADYT	JHDEU	IIAWQ	PGSTK	KKWOO	YFQDU	ZGUGY	ECVTL	KHVTs
147	YUGCG	UBLQU	NJKZZ	VOZZI	GBQFF	OXISR	KVWJC	JDWIN	IXNSF	XTCRP	XSVSD
148	TXQYM	YMZHV	QYSLT	EHMFC	RLEPY	SQMWQ	FBKTY	NEXRY	KSXUY	DURWH	ZNOSV
149	ISACT	JNGYI	IYZGO	BBCFO	GBQFF	CBRGD	ERKZQ	ZEFQJ	SYCMK	IVDOH	ONJSX
150	MNWUL	STMXX	ZIDBQ	MAETF	NLDHV	RAUDD	DJESF	WXQQR	EXSUZ	OXXUA	KWREW
151	NCUPN	COREF	OKHOW	FILBO	EBMVZ	CRJOW	MUCRU	VEYFH	NOKGN	IDYZP	ZENEA
152	VUENV	INHkW	GENDP	QWXSE	RAUCG	ZUIVB	JRJOW	EMQWE	PPUBF	KQOEB	OITOM
153	YOAYO	LCYQB	CKZTD	QCIOV	EEHIV	OPKHO	OTSTO	LHJTR	BIVAS	TKCWT	ZBIJP
154	ATEPE	ZWFJU	GQXLH	ZOZSR	YLFXA	BHWRO	KSTFX	IPTQC	AMOOJ	BIYTU	FGFPM
155	NZNLD	PJNJD	ZSIOH	JNIHQ	SNLFY	JIVQW	ALDDE	PFFQH	IDOZL	BKVHJ	
156	KSQDS	GDZXO	RWJJV	DTOYU	SBBPZ	TIKIE	IRORC	AUIWP	KDUYZ	KBLWH	IRYCZ
157	KXHBj	PAJPA	HCRDF	JEMUE	ZVWQO						

158	NBKN	MRMCT	KQUVU	JEYIJ	WITSN	LQFHY	JZJNX	JYDAT	KVAYQ	VXSQT	XEAJP
159	GQCAC	KZFFF	XKCMW	NZWWE	GPIKY	KPJ SX	WTVYL	NCDDL	MFMoz	HSGBF	CCATU
160	ISKLQ	PZZHC	AWMHX	ZBKXG	FYZBV	IUVRW	ZRPKJ	JQMLQ	QXQSR	DFGYI	GFXAD
161	YPCPN	TWARE	SPVRE	BIHYH	KZVCR	WDLMK	KTXOX	OMBNK	UXIQV	GFLPG	RMDRK
162	YKQOE	QDPLJ	FXALE	PTALU	GQPRN	DBAZC	QXEUK	GRIIX	JBCHV	MZCTI	QBXWR
163	OQOKP	RDQSU	LPIYH	GXXLL	NDOCC	VKUBN	LGNST	SHQYE	MTDGG	MREVD	QJWEB
164	SGNQS	XVZJR	NHQGK	AQNSD	CMKDY	IKHDJ	QXKPT	WKBZG	ULOJA	UFDCO	TPYAB
165	DHZVM	UTCCC	AIGGR	LBKOI	MXDUT	DJSRS	MDPRR	OMMSU	YJVHI	FFZDA	IZHYK
166	PPUCS	YCFMO	EJSDL	IYFQE	KBBCF	VPNJU	BZVLO	EZSNV	VBTRD	XYSWZ	TXUVO
167	PRHCQ	BTLVJ	PHPFT	YEENN	SVEYU	NEPVS	WGHZZ	KMVMs	TZLBD	MVRTA	SFIKE
168	LDZAU	FLZIC	PAFNC	OHENR	PUMTA	EFASX	CYTUY	OCTVJ	KZCFF	PWAAN	ZLVSb
169	NAWGT	PXTIK	SCZAD	NWYZT	IHMUF	UIPEW	JQPEL	SHAOW	NZGKX	NYFRQ	OCOQT
170	PTBTX	BMFLR	KYDKE	KCOVQ	NGBHH	PEYNW	KZYHR	FETXL	CQUHO	YQQIS	MBLFL
171	HMEFK	NUZTF	FEVCJ	IFSAF	IWNUX	XTLPB	PBJDN	MMSOZ	UVIJN	VIGFR	VGLBS
172	BVXVD	QSCGD	UAOHT	WTQKE	BOYDV	PHPPG	FCLWI	MUQML	AACAM	POROA	EJAUM
173	AOAOI	SNBHS	QKZMB	GJJTH	OHSD E	WFLBZ	YXPEN	WYFJF	WISTG	IDEDP	GBGMU
174	XYEHL	UNAER	XTBJV	DHPHD	UMIIE	QEJOB	TPTAP	TEYJR	KFLMC	JZPZA	UUFcy
175	PTCTM	UXBAV	HNSRN	IEEEQ	ZOHXJ	HHFCA	VVBOW	KTHRv	MYUUI	KVEGN	TZYMY
176	ZEVLt	WWPQZ	FYOFX	DXZGP	XOUQF	OYUTE	VVODS	PGJYF	IJMAN	CALYW	QACQQ
177	SQUSE	DTRFK	GIEVN	GPOGR	NZUHN	QODCF	PWURI	DILGP	MWPBZ	WLIWR	NOMYH
178	TFZZH	HGZDH	LQGIF	WEDOL	PPXJX	DAZVT	MPDYE	TDPTY	NUFUX	WUvLA	RZBJR
179	ITGPW	WKVAG	TWNWQ	MLOHB	LQSJF	WVVSr	XDTYV	CGNMK	SREOO	VZNXY	PJKPV
180	ESXNU	DEPQL	TFAPQ	BYDFO	HBEBS	NGTFP	GFJBG	BJVFK	NYGBX	BZXMS	NWSLG
181	BXHQL	BAYOB	BWVIS	MEHNB	TAYTV	THNVX	KCITU	XAEHC	UKZOO	MVTXK	PLVNR
182	AENJU	IJAZR	XBBKV	CPMWK	NGFIQ	EQEIT	NQINH	QPOPG	XVEXQ	HHISC	LBMHS
183	TTQSH	IPCSG	MSCOD	OOCCA	FWYAB	GGFMX	RYXZN	WWSIC	JFBXN	CVMYX	MYGMM
184	DZGCN	HCFFI	BGHLQ	ZNEVM	WADER	DSTWA	LZGDI	CEAEC	IAVRD	WALQS	XZCCM

185	DTZWK	CRMOT	QFGNO	UMCAJ	SDTPK	RASVL	UXXTV	AQFKU	YKVN	ULZQD	AFHDS
186	YQILZ	TJLFN	DIUVR	SQIGG	NGHIA	HPEAG	IQXAN	WTNMM	WICCN	HVMFN	PJMD
187	INWWP	WLCLB	GNYCV	RUBAO	WZVYS	YWEXB	XKDXB	HABNP	LPCEL	RCEAV	VUSWO
188	JBHTG	YQHJB	NTYWQ	YXHVL	AUNMX	OCBPW	PCAE	ZOANW	XDGGY	LUPHB	XXEDO
189	XALNK	ZWQPF	PICTD	AQBRH	TPHIR	IBFYF	BDCPW	IIWVE	GOYTL	PBMJP	MFJSC
190	LISAP	RFIAG	LCUWW	SCKRH	MGRZB	GYORE	YWUVM	EFKBW	SIGHL	VDARC	ORNF
191	ZENKM	KNKQU	TLGRS	FUPIX	OILPP	NPQFU	QNCNS	VBQLF	GZFEJ	SLFHP	PFKYJ
192	KERHY	OQOYJ	VZCTT	JJESR	RDOAX	TEHDK	XOROR	SITEQ	CBBFY	KRZJX	FUEPT
193	NWDT	MFNTH	QVRVP	SIXKR	CVVPM	ZXIHM	DMJQL	FRWYZ	VOXQL	DQGLD	BAMLR
194	KVTHZ	KHXCS	YUJDC	KWRQC	AIMBO	QBGSF	YKQIA	BJEPB	VTSMA	PMPRQ	ZCOOJ
195	LCYKO	MZXL	ZLTRD	KMQPY	RMGUJ	EFUSM	DEJCL	ZLZEH	WJJPA	NKTSW	KUQHR
196	REIUO	HXSMD	CZDRN	JBPPE	TQORV	ZNNHG	GTXYB	DIWOD	GQZID	VURZZ	ZENTT
197	CWFZP	QVGIF	WBXXI	HYXKE	DNGPK	ANACB	SQRYJ	QQHVA	KHJUL	OQZPK	LDIJO
198	ORXKZ	LQURZ	YZDYM	IPYBM	PHPGY	YHIUJ	TGMHL	ELBSE	THIUN	ETKLO	YFRVS
199	CBCUS	HEAPT	LNZMJ	UVWEZ	HDNNE	BKKVY	RLDUP	ANUCN	HXAGG	LPUAN	SVMUP
200	MJDBT	NGRJK	ZPPXC	IYMKJ	VUUYK	AUHCM	ENHFM	BJZYM	WHRZN	DMSBA	USASZ
201	HXVTZ	RZZXN	LVMYJ	AHMUG	RNSUQ	JDDXO	GWZUF	EEJPN	ALZRC	GOSDN	UPXQG
202	VXZXX	KROKU	NOETO	SXKWR	JLRHI	EYKJM	LSYYP	RVCBH	HKEIS	OTXIN	NOVQJ
203	IGGZZ	AWYHD	RCEBJ	JUITF	YRRWN	LLPWG	HQDTZ	NHHRW	LAFHB	BNXUN	IWZGS
204	FEJEL	XXAWD	SOVDH	DKAUY	CHPLL	IGNNU	KTQKU	BCMSJ	UVLOP	KBXFA	UWFJH
205	EDVLH	SNAVU	DIHJH	YEGVP	QLJDQ	LBUVK	LFJVI	OVIOW	ODECM	XXTFO	OLGVV
206	HFPQR	DQCPD	PZGOB	ZMSTC	FTBXU	GDESR	YEPFG	IFRLA	OZROA	RZLRI	GAVVX
207	IGYKF	RHTLJ	LOCCS	TTWCI	KEZWK	MLMBF	XPCWF	IMXKU	LTUNE	KMQZU	MEATP
208	OBLAL	HVUIU	SQUQF	ZYKFS	JIXYA	SNULA	FACYX	RDZWD	GPBKB	XRKCS	QGRFT
209	LIPSL	GHIGX	YAYFG	SDHVQ	GFOFQ	DYSZO	OJRV	COGNJ	VJVHQ	KXTDJ	JBZEX
210	LHINQ	IMCZX	BUTLX	ROLQM	QBLLN	ETTFJ	ZDEC	CLKYS	UCWU	JTWN	CCIHK
211	VGHSU	DZOAE	UUGXL	VAROJ	LYGBJ	GIDUW	CUJAK	SIGVL	YPNOY	JATNX	JRCGJ

212	DAQP	HGXB	UMSEA	EPEGI	TCOVM	SGLIW	FLDKK	NXEND	XGYDU	OKYAX	IMAQM
213	NBET	OXASS	YZPTF	IBIUU	UMDFO	MWSWE	IEDJL	PUNOO	MXEVY	KNWWE	PLKQR
214	AAICA	ILRPT	ESDRY	NDENI	YAHCE	POXED	QVHKK	KRUDY	MNLJA	GZBWA	EYNTM
215	LEMRRP	HWZQD	COVEG	ZVPXF	AOQAW	YYPZV	WVULH	HGYWF	PYMER	DCQZO	LRXFC
216	UKKEW	NOEUY	IQRJU	NAARY	XNRWW	FQCLY	XLIPC	TGQKY	UZHVB	CWJML	GDUAL
217	ATITJ	HMING	DXRLY	PHZXN	ZJWON	FFHGC	QCWBB	DCBOO	PVSLI	SHHMW	CUGYS
218	JBJIZ	NBKPD	WTSKI	SAMHI	XKFOZ	KYZIG	MPSVY	VDWXS	POLFE	AIVPZ	UUWBY
219	GWDPD	XOXXL	SKPFM	IPOOS	JUGYC	VVNPS	NAKTO	VLVVU	EXSID	LCIFH	QAJYW
220	IZQCN	ESQBJ	ETMYN	PIBYX	FOHMS	MMUVJ	KOMEL	GTBPD	BAOKN	LLYVB	ODUXA
221	UHNIC	MGCRP	FAUBQ	JCGOG	DNGDD	IPQWU	MERFH	FLFLQ	XNYPV	ZACYW	KAZKC
222	MZCDN	MIESE	QFMSI	WFNGN	LMSNH	LSDDJO	FVIDK	YQCHB	KJRPD	AFNAS	TOTOX
223	BIQKI	JVYAY	XHEBI	AYVSY	VRKNQ	CRSLP	SSXYI	GOYRX	UQMAL	ZCTMC	TZKGN
224	EWWDN	GTNZH	FNRXP	MVENL	WUGVR	SWUNK	OXOCU	JBOPO	BTEBN	SKSFK	IYBVF
225	RYHRB	ATZBE	TFIPA	QSCITL	JXEIL	REYBH	BPDIZ	AMQOO	IAVEU	RQQUP	IYPDE
226	NHVCH	GXIFM	GPICA	YNYJO	QHUSG	ORFNG	SCGOM	PBXDV	CWSAQ	UOWTA	DUJNT
227	JPUIS	DCCGJ	ENGJT	QMKSD*	EIRKP†	GPEBA	ZATPW	CFYKI	BDHFK	XYDRN	UKNEW
228	BOCTW	PPAFD	NYUHF	GMAYY	NCLLF	IQFVU	MSTEX	TKBEP	HXZEQ	NYZFO	OTPCU
229	BUSWZ	RONJC	QVMOH	LGKPM	XWYPJ	YETIN	GHRRO	LNIWG	EDXGE	PQMCC	IZJNU
230	LJPNR	YHIWP	XVZZK	KQEOC	ACTCL	RAPDO	SPMRA	JNGYG	ANPUL	NMPPG	RVDRB
231	MLBW	XJSIE	ZCEBB	JMGSD	YFRDC	TGBDV	KNMBP	PQXVS	NGJXI	GWKKJ	ARLZQ
232	XQHPO	OHAWY	KJYOH	PBHWI	FDAFH	JJAFQ	GSFBR	XTYMJ	EFJFS	CBMQV	IQIJX
233	LTPJO	KFQTS	VZKKM	YFKKX	CBBLR	IOYNF	TKKMO	OFUDP	PXCFC	EVWUO	ADGPB
234	NWBJJ	NPNCW	SOTTO	IBBMN	ZTKFM	BMTWP	RHJZG	WFARD	JCDCE	KLPLY	DUHMX
235	ANKKG	NQPJQ	NAAZD	WVELQ	NISRH	KRLLR	ZPPCQ	DNHRZ	OHXJH	MXKOL	OBIXW
236	EBSFE	ISOTJ	MDBID	VMHWR	WOAKK	QQZCJ	ERRHO	KNQVE	GICDO	CMOYE	ZNASK

* The Declaration of Independence ends with the "D" in "QMKSD."

† Gettysburg Address begins immediately afterward.

237 SJTGN NCJJI CIEVR PEJKK UHIRM BTAXT TREXT IBKCS IDGAO KRWX NPOGD
 238 NMAKN SRTNJ DEAGO YTDGM MOUWP KZGCC FASXQ MMHPK PWYLL LPVHX IGOPF
 239 YWCHS HERBY NYLYI TINMU GSJAS KITWE SSIIO EECIN YDGHU IYARA WPKJV
 240 CAWIU EXDVM AUBXV TZFSK OWETO SXYNW SLYYS XWJUI YWYUY UUDNH CHEUF
 241 FVWYD VLSYF NVOND DQVLJ RPACI PLKXE FSYIA UQABT DOSVC HDPKF UPIUV
 242 XFQIE TXUWG RUPXM ZNZWD HSSPE FUGNU XQCIM LRPOP CRIMV KPFWI EUORK
 243 XVSXK ONBZV LNAGB JLHZZ WMNCR GRYNL FHECD JHGUS QWUIQ ZYRRP HATER
 244 UPQDW ODTWH MOIDF HHCFF GJUKX VNZBK CJPDP TGDYW AUJGP XGAJF DZTYH
 245 HZAYT PIVWN QCVJR ITRKE ZGJSP IAOXM HAUPA MPNKV VHTMH SOPFP VATIU
 246 PFMUE QQDGS QPXQH TFGHD BIJJQ AZRND EMKVQ AKZGK ABHEJ EMFXQ ZRYOE
 247 UYYJI UNCUL GVTQV MQUJQ PXTAW ZYLVR AZVFZ IQSEN MNFJD RPFSSR MFXQU
 248 OOSJA VAVIA RDIUY†NQBAK ANNBS FEXTI

CHAOICIPHER

EXHIBIT 1

Plain text (in groups of five letters) of Declaration of Independence and Lincoln's Gettysburg Speech, as enciphered in the document entitled "Chaocipher—the Ultimate Elusion."

105 WHE NINTH ECOUR
 106 SEOFH UMANE VENTS QITBE COMES NECES SARYF ORONE PEOPLE ETODI SSOLV
 107 ETHEP OLITI CALBA NDSWH ICHHA VECON NECTE DTHEM WITHA NOTHE RQAND
 108 TOASS UMEAM ONGTH EPOWE RSOFT HEEAR THTHE SEPAR ATEAN DEQUA LSTAT
 109 IONTO WHICH THELA WSOFN ATURE ANDOF NATUR EXSGO DENTI TLETH EMQAD
 110 ECENT RESPE CTTOT HEOPI NIONS OFMAN KINDR EQUIR ESTHA TTHEY SHOUL
 111 DDECL ARETH ECAUS ESWHI CHIMP ELTHE MTOTH ESEPA RATIO NZWEH OLDTH
 112 ESETR UTHST OBESE LFJEV IDENT QTHAT ALLME NAREC REATE DEQUA LQQTH

† Gettysburg Address ends with "I" in "RDIUY."

113	ATTHE	YAREE	NDOWE	DBYTH	EIRCR	EATOR	WITHC	ERTAI	NUNAL	IENAB	LERIG
114	HTSQT	HATAM	ONGTH	ESEAR	ELIFE	LIBER	TYAND	THEPU	RSUIT	OFHAP	PINES
115	SWTHA	TTOSE	CURET	HESER	IGHTS	QGOVE	RNMEN	TSARE	INSTI	TUTED	AMONG
116	MENQD	ERIVI	NGTHE	IRJUS	TPOWE	RSFRO	MTHC	ONSEN	TOFTH	EGOVE	RNEDW
117	THATW	HENEV	ERANY	FORMO	FGOVE	RNMEN	TBECO	MESDE	STRUC	TIVEO	FTHES
118	EENDS	QITIS	THERI	GHTOF	THEPE	OPLET	OALTE	RORTO	ABOLI	SHITQ	ANDTO
119	INSTI	TUTEN	EWGOV	ERNME	NTQLA	YINGI	TSFOU	NDATI	ONONS	UCHPR	INCIP
120	LESAN	DORGA	NIZIN	GITSP	OWERS	INSUC	HFORM	QASTO	THEMS	HALLS	EEMMO
121	STLIK	ELYTO	EFFEC	TTHEI	RSAFE	TYAND	HAPPI	NESSW	PRUDE	NCEQI	NDEED
122	QWILL	DICTA	TETHA	TGOVE	RNMEN	TSLON	GESTA	BLISH	EDSHO	ULDNO	TBECH
123	ANGED	FORLI	GHTAN	DTRAN	SIENT	CAUSE	SQAND	ACCOR	DINGL	YALLE	XPERI
124	ENCEH	ATHSH	EWNTH	ATMAN	KINDA	REMOR	EDISP	OSED	OSUFF	ERQWH	ILEEV
125	ILSAR	ESUFF	ERABL	EQTHA	NTORI	GHTTH	EMSEL	VESBY	ABOLI	SHING	THEFO
126	RMSTO	WHICH	THEYA	REACC	USTOM	EDWBU	TWHEN	ALONG	TRAIN	OFABU	SESAN
127	DUSUR	PATIO	NSQPU	RSUIN	GINVA	RIABL	YTHES	AMEOB	JECTE	VINCE	SADES
128	IGNTO	REDUC	ETHEM	UNDER	ABSOL	UTEDE	SPOTI	SMQIT	ISTHE	IRRIG	HTQIT
129	ISTHE	IRDUT	YQTOT	HROWO	FFSUC	HGOVE	RNMEN	TQAND	TOPRO	VIDEN	EWGUA
130	RDSFO	RTHEI	RFUTU	RESEC	URITY	WSUCH	HASBE	ENTHE	PATIE	NTSUF	FERAN
131	CEOFT	HESEC	OLONI	ESUAN	DSUCH	ISNOW	THERE	CESSI	TYWHI	CHCON	STRAI
132	NSTHE	MTOAL	TERTH	EIRFO	RMERS	YSTEM	SOFGO	VERNM	ENTWT	HEHIS	TORYO
133	FTHEP	RESEN	TKING	OFGRE	ATBRI	TAINI	SAHIS	TORYO	FREPE	ATEDI	NJURI
134	ESAND	USURP	ATION	SQALL	HAVIN	GINDI	RECTO	BJECT	THEES	TABLI	SHMEN
135	TOFAN	ABSOL	UTETY	RANNY	OVERT	HESES	TATES	WTOPR	OVETH	ISQLE	TFACT
136	SBESU	BMITT	EDTOA	CANDI	DWORL	DWZHE	HASRE	FUSED	HISAS	SENTT	OLAWS
137	QTHEM	OSTWH	OLESO	MEAND	NECES	SARYF	ORTHE	PUBLI	CGOOD	ZHEHA	SFORB
138	IDDEN	HISGO	VERNO	RSTOP	ASSLA	WSOFI	MMEDI	ATEAN	DPRES	SINGI	MPORT
139	ANCEQ	UNLES	SSUSP	ENDED	INTHE	IROPE	RATIO	NTILL	HISAS	SENTS	HOULD

140	BEGBT	AINED	QANDW	HENSO	SUSPE	NDEDQ	HEHAS	UTTER	LYNEG	LECTE	DTOAT
141	TENDT	OTHEM	ZHEHA	SREFU	SEDTO	PASSO	THERL	AWSFO	RTHEA	CCOMO	DATIO
142	NOFLA	RGEDI	STRIC	TSOFF	EOPLE	QUNLE	SSTHO	SEPEO	PLEWO	ULDRE	LINQU
143	ISHTH	ERIGH	TOFRE	PRESE	NTATI	ONINT	HELEG	ISLAT	UREQA	RIGHT	INEST
144	IMABL	ETOTH	EMAND	FORMI	DABLE	TOTYR	ANTSO	NLYZH	EHASC	ALLED	TOGET
145	HERLE	GISLA	TIVEB	ODIES	ATPLA	CESUN	USUAL	QUNCO	MFORT	ABLEQ	ANDDI
146	STANT	FROMT	HEDEP	OSITO	RYOFT	HEIRP	UBLIC	RECOR	DSQFO	RTHES	OLEPU
147	RPOSE	OFFAT	IGUIN	GTHEM	INTOC	OMPLI	ANCEW	ITHHI	SMEAS	URESZ	HEHAS
148	DISSO	LVEDR	EPRES	ENTAT	IVEHO	USES	EPEAT	EDLYQ	FOROP	POSIN	GWITH
149	MANLY	FIRMN	ESSHI	SINVA	SIONS	ONTHE	RIGHT	SOFTH	EPEOP	LEZHE	HASRE
150	FUSED	FORAL	ONGTI	MEQAF	TERSU	CHDIS	SOLUT	IONSQ	TOCAU	SEOTH	ERSTO
151	BEELE	CTEDU	WHERE	BYTHE	LEGIS	LATIV	EPOWE	RSQIN	CAPAB	LEOFA	NNIHI
152	LATIO	NQHAV	ERETU	RNEDT	OTHEP	EOPLE	ATLAR	GEFOR	THEIR	EXERC	ISEUT
153	HESTA	TEREM	AININ	GINTH	EMEAN	TIMEE	XPOSE	DTOAL	LTHED	ANGER	SOFIN
154	VASIO	NFROM	WITHO	UTAND	CONVU	LSION	SWITH	INZHE	HASEN	DEAVO	URED
155	OPHEV	ENTTH	EPOPU	LATIO	NORTH	ESEST	ATESU	FORTH	ATPUR	POSEO	BSTRU
156	CTING	THELA	WSFOR	NATUR	ALIZA	TIONO	FFORE	IGNER	SUREF	USING	TOPAS
157	SOTHE	RSTOE	NCOUR	AGETH	EIRMI	GRATI	ONSHI	THERQ	ANDRA	ISING	THECO
158	NDITI	ONSOF	NEWAP	PROPR	IATIO	NSOFL	ANDSZ	HEHAS	OBSTR	UCTED	THEAD
159	MINIS	TRATI	ONOFJ	USTIC	EQBYR	EFUSI	NGHIS	ASSEN	TTOLA	WSFOR	ESTAB
160	LISHI	NGJUD	ICIAR	YPOWE	RSZHE	HASMA	DEJUD	GESDE	PENDE	NTONH	ISWIL
161	LALON	EQFOR	THETE	NUREO	FTHEI	ROFFI	CESQA	NDTHE	AMOUN	TANDP	AYMEN
162	TOFTH	EIRSA	LARIE	SZHEH	ASERE	CTEDA	MULTI	TUDEO	FNEWO	FFICE	SQAND
163	SENTH	ITHER	SWARM	SOFOF	FICER	STOHA	RASSO	URPEO	PLEQA	NDEAT	OUTTH
164	EIRSU	BSTAN	CEZHE	HASKE	PTAMO	NGUSQ	INTIM	ESOFF	EACEQ	STAND	INGAR
165	MIESQ	WITHO	UTTHE	CONSE	NTOFO	URLEG	ISLAT	URESZ	HEHAS	AFPEC	TEDTO
166	RENDE	RTHEM	ILITA	RYIND	EPEND	ENTOF	ANDSU	PERIO	RTOTH	ECIVI	LPOWE

167	RZHEH	ASCOM	BINED	WITHO	THERS	TOSUB	JECTU	STOAJ	URISD	ICTIO	NFORE
168	IGNTO	OURCO	NSTIT	UTION	ANDUN	ACKNO	WLEDG	EDBYO	URLAW	SUGIV	INGHI
169	SASSE	NTTOT	HEIRA	CTSOE	PRETE	NDEDL	EGISL	ATION	VFORQ	UARTE	RINGL
170	ARGE	ODIES	OFARM	EDTRO	OPSAM	ONGUS	VFORP	ROTEC	TINGT	HEMBY	AMOCK
171	TRIAL	FROMP	UNISH	MENTF	ORANY	MURDE	RSWHI	CHTHE	YSHOU	LDCOM	MITON
172	THEIN	HABIT	ANTSO	FTHES	ESTAT	ESVFO	RCUTT	INGOF	FOURT	RADEW	ITHAL
173	LPART	SOPTH	EWORL	DVFOR	IMPOS	INGTA	XESON	USWIT	HOUTO	URCON	SENTV
174	FORDE	PRIVI	NGUSI	NMANY	CASES	OFTHE	RENEF	ITSOE	TRIAL	BYJUR	YVFOR
175	TRANS	PORTI	NGUSB	EYOND	SEAST	OBETR	IEDFO	RPRET	ENDED	OFFEN	CESVF
176	ORABO	LISHI	NGTHE	FREES	YSTEM	OFENG	LISHL	AWSIN	ANEIG	HBOUR	INGPR
177	OVINC	EQUEST	ABLIS	HINGT	HEREI	NANAR	BITRA	RYGOV	ERNME	NTQAN	DENLA
178	RGING	ITSBO	UNDAR	IESSO	ASTOR	ENDER	ITATO	NCEAN	EXAMP	LEAND	FITIN
179	STRUM	ENTFO	RINTR	ODUCI	NGTHE	SAMEA	BSOLU	TERUL	EINTO	THESE	COLON
180	IESVF	ORTAK	INGAW	AYOUR	CHART	ERSQA	BOLIS	HINGO	URMOS	TVALU	ABLEL
181	AWSAN	DALTE	RINGF	UNDAM	ENTAL	LYTHE	FORMS	OFOUR	GOVER	NMENT	SVFOR
182	SUSPE	NDING	OUROW	NLEGI	SLATU	RESQA	NDDEC	LARIN	GTHEM	SELVE	SINVE
183	STEDW	ITHPO	WERTO	LEGIS	LATEF	ORUSI	NALLC	ASESW	HATSO	EVERZ	HEHAS
184	ABDIC	ATEDG	OVERN	MENTH	EREBY	DECLA	RINGU	SOUTO	PHISP	ROTEC	TIONA
185	NDWAG	INGWA	RAGAI	NSTUS	ZHEHA	SPLUN	DERED	COURSE	ASQRA	VAGED	OURCO
186	ASTSQ	BURNT	OURTO	WNSQA	NDDDES	TROYE	DTHEL	IVESO	FOURP	EOPLE	ZHEIS
187	ATTHI	STIME	TRANS	PORTI	NGLAR	GEARM	IESOF	FOREI	GNMER	CENAR	iesto
188	COMPL	ETETH	EWOK	SOEDE	ATHQD	ESOLA	TIONA	NDTYR	ANNYQ	ALREA	DYBEG
189	UNWIT	HCIRC	UMSTA	NCESO	FORUE	LYTAN	DPERF	IDYSC	ARCEL	YPARA	LLELE
190	DINTH	EMOST	BARBA	ROUSA	GESQA	NDTOT	ALLYU	NWORT	HYTHE	HEADO	FACIV
191	ILIZE	DNATI	ONZHE	HASCO	NSTRA	INEDO	URFEL	LOWCI	TIZEN	STAKE	NCAPT
192	IVEON	THEHI	GHSEA	STOBE	ARARM	SAGAI	NSTTH	EIRCO	UNTRY	QTOBE	COMET
193	HEEXE	CUTIO	NERSO	FTHEI	RFRIE	NDSAN	DBRET	HRENQ	ORTOF	ALLTH	EMSEL

194	VESBY	THEIR	HANDS	ZHEHA	SEXCI	TEDDO	MESTI	CINSU	RRECT	IONSA	MONGS
195	TUSQA	NDHAS	ENDEA	VOURE	DTOBR	INGON	THEIN	HABIT	ANTSO	FOURF	RONTI
196	ERSQT	HEMER	CILES	SINDI	ANSAY	AGESQ	WHOSE	KNOWN	RULEO	FWARF	AREIS
197	ANUND	ISTIN	GUISH	EDDES	TRUCT	IONOF	ALLAG	ESQSE	XESAN	DCOND	ITION
198	SWINE	VERYS	TAGEO	FTHES	EOPPR	ESSIO	NSWEH	AVEPE	TITIO	NEDFO	RREDR
199	ESSIN	THEMO	STHUM	BLETE	RMSWO	URREP	EATED	PETIT	IONSH	AVEBE	ENANS
200	WERED	ONLYB	YREPE	ATEDI	NJURY	WAPRI	NCEQW	HOSEC	HARAC	TERIS	THUSM
201	ARKED	BYEVE	RYACT	WHICH	MAYDE	FINEA	TYRAN	TQISU	NFITT	OBETH	ERULE
202	ROFAF	REEPE	OPLEW	NORHA	VEWEB	EENWA	NTING	INATT	ENTIO	NSTOO	URBRI
203	TISHB	RETHR	ENWWE	HAVEW	ARNED	THEMF	ROMTI	METOT	IMEOF	ATTEM	PTSBY
204	THEIR	LEGIS	LATUR	ETOEX	TENDA	NUNWA	RRANT	ABLEJ	URISD	ICTIO	NOVER
205	USWWE	HAYER	EMIND	EDTHE	MOFTH	ECIRC	UMSTA	NCESO	FOURE	MIGRA	TIONA
206	NDSET	TLEME	NTHER	EWWEH	AVEAP	PEALE	DTOTH	EIRNA	TIVEJ	USTIC	EANDM
207	AGNAN	IMITY	QANDW	EHAVE	CONJU	REDTH	EMBYT	HETIE	SOFU	RCOMM	ONKIN
208	DREDT	ODISA	VOWTH	ESEUS	URPAT	IONSQ	WHICH	WOULD	INEVI	TABLY	INTER
209	RUPTO	URCON	NECTI	ONSAN	DCORR	ESPON	DENCE	WTHEY	TOOHA	VEBEE	NDEAF
210	TOTHE	VOICE	OFJUS	TICEA	NDOFC	ONSAN	GUINI	TYWWE	MUSTQ	THERE	FOREQ
211	ACQUI	ESCEI	NTHEN	ECESS	ITYQW	HICHD	ENOUN	CESOU	RSEPA	RATIO	NQAND
212	HOLDT	HEMQA	SWEHO	LDTHE	RESTO	FMANK	INDQE	NEMIE	SINWA	RQINP	EACEF
213	RIEND	SZWEQ	THERE	FOREQ	THERE	PRESE	NTATI	VESOF	THEUN	ITEDS	TATES
214	OFAME	RICAAQ	INGEN	ERALC	ONGRE	SSQAS	SEMBL	EDQAP	PEALI	NGTOT	HESUP
215	REMEJ	UDGEO	FTHEW	ORLDF	ORTHE	RECTI	TUDEO	FOURI	NTENT	IONSQ	DOQIN
216	THENA	MEQAN	DBYAU	THORI	TYOFT	HEGOO	DPEOP	LEOFT	HESEC	OLONI	ESQSO
217	LEMNL	YPUBL	ISHAN	DDECL	AREVT	HATH	ESEUN	ITEDC	OLONI	ESARE	QANDO
218	FRIGH	TOUGH	TOBE	FREEA	NDIND	EPEND	ENTST	ATESU	THATT	HEYAR	EABSO
219	LVEDF	ROMAL	LALLE	GIANC	ETOTH	EBRIT	ISHCR	OWNQA	NDTHA	TALLP	OLITI
220	CALCO	NNECT	IONBE	TWEEN	THEMA	NDTHE	STATE	OFGRE	ATBRI	TAINI	SANDO

221	UGHTT	OBETO	TALLY	DISSO	LVEDU	ANDTH	ATASF	REEAN	DINDE	PENDE	NTSTA
222	TESQT	HEYHA	VEFUL	LPOWE	RTOLE	VYWAR	QCONC	LUDEP	EACEQ	CONTR	ACTAL
223	LIANC	ESQES	TABLI	SHCOM	MERCE	QANDT	ODOAL	LOTHE	RACTS	ANDTH	INGSW
224	HICHI	NDEPE	NDENT	STATE	SMAYO	FRIGH	TDOWA	NDFOR	THESU	PPORT	OFTHI
225	SDECL	ARATI	ONQWI	THAFI	RMREL	IANCE	ONTHE	PROTE	CTION	OFDIV	INEPR
226	OVIDE	NCEQW	EMUTU	ALLYP	LEDGE	TOEAC	HOTHE	ROURL	IVESQ	OURFO	RTUNE
227	SQAND	OURSA	CREDH	ONCRZ	FOURS	COREA	NDSEV	ENYEA	RSAGO	OURFA	THERS
228	BROUG	HTFOR	THONT	HISCO	NTINE	NTANE	WNATI	ONQCO	NCEIV	EDINL	IBERT
229	YANDD	EDICA	TEDTO	THEPR	OPOSI	TIONT	HATAL	LMENA	RECRE	ATEDE	QUALZ
230	NOWWE	AREEN	GAGED	INAGR	EATCI	VILWA	RQTES	TINGW	HETHE	RTHAT	NATIO
231	NORAN	YNATI	ONSOC	ONCEI	VEDAN	DSODE	DICAT	EDCAN	LONGE	NDURE	WWEAR
232	EMETO	NAGRE	ATBAT	TLEFI	ELDOF	THATW	ARWE	HAVEC	OMETO	DEDIC	ATEAP
233	ORTIO	NORTH	ATFIE	LDQAS	AFINA	LREST	INGJP	LACEO	FTHOS	EWHOH	EREGA
234	VETHE	IRLIV	ESTHA	TTHAT	NATIO	NMIGH	TLIVE	WITIS	ALTOG	ETHER	FITTI
235	NGAND	PROPE	RTHAT	WESHO	ULDDO	THISZ	BUTQI	NALAR	GERSE	NSEQW	ECANN
236	OTDED	ICATE	HWECA	NNOTC	ONSEC	RATEH	WECAN	NOTHA	LLOWH	THISG	ROUND
237	WTHEB	RAVEM	ENQLI	VINGA	NDDEA	DQWHO	STRUG	GLEDH	EREQH	AVECO	NSECR
238	ATEDI	TFARA	BOVEO	URPOO	RPOWE	RTOAD	DORDE	TRACT	WTHEW	ORLDW	ILLI
239	TTLEN	OTEQN	ORLON	GREME	MBERQ	WHATW	ESAYH	EREWI	TISFO	RUSTH	ELIVI
240	NGQRA	THERQ	TOBED	EDICA	TEDHE	RETOT	HEUNF	INISH	EDWOR	KWHIC	HTHEY
241	WHOFO	UGHTH	EREHA	VE THU	SFARS	ONOB	YADVA	NCEDW	ITISR	ATHER	FORUS
242	TOBEH	EREDE	DICAT	EDTOT	HEGRE	ATTAS	KREMA	INING	BEFOR	EUSHT	HATFR
243	OMTHE	SEHON	OREDD	EADWE	TAKEI	NCREA	SEDDE	VOTIO	NTOTH	ATCAU	SEFOR
244	WHICH	THEYG	AVETH	ELAST	FULLM	EASUR	EOFDE	VOTIO	NHTHA	TWEHE	REHIG
245	HLYRE	SOLVE	THATT	HESED	EADSH	ALLNO	THAVE	DIEDI	NVAIN	HTHAT	THISN
246	ATION	QUNDE	RGODQ	SHALL	HAVEA	NEWBI	RTHOF	FREED	OMHAN	DTHAT	GOVER
247	NMENT	OF THE	PEOPL	EQBYT	HEPEO	PLEQF	ORTHE	PEOPL	ESHAL	LNOTP	ERISH
248	FROMT	HEEAR	THZ								

CHAOCIPHER

EXHIBIT 2

EXCERPT FROM DE BELLO GALLICO IN CHAOCIPHER

TLXWF WYHBI COJSP URTJM FDKTJ BFAEF GBRJO SISVK RGRPK OKXZQ BXHSY
 NZRXD YXZDX BDAGA LVCYG CMXEQ ISZIT MNICJ QHQXJ JUMSA GESXW FJUAK
 JWURE KMUIX YMFAJ CVURV AECLA KDWJB HBSJD WRQOP HUHPF GDONU PWDIY
 VDRSE SXPNR NSZMC XIYSO XBZPD SKBFS QXSYP DEGSJ USNXB JMVVW AVDPZ
 ILECG XBKKN FKVOX VKTBE QSCNK HDYQR YNNHN HQPJW XVUGW DGUWN DOIU
 HKWWJ MXXEG XITIK KTAXW LZREB QFVEI VWMRX OBIFN PQDMP YUARZ ELHDK
 DSCEK ACMDZ ZBGSU FMZRC LQUSI CSRVS FHHKH HPVIB CCNZJ HCRTU ZUOCC
 LWDWI EWBGF YJPQN NHTNN IBTLY WZAQS DHBOR BKHCH FBBZH ZHQXU BURTI
 EYELG DOFLB SVOEM GBFUC DLJDD RGGIO JVGJT ZXSRQ DGIKW IDKZP XFDCZ
 WODHB WMRCV KJQRZ FRJGF CTCLY XTIMN IXCKO KWXXD RQMHL QWUAC SYWKE
 VFSUG XNBCU ZJVKL SDLUP YVVIV HDZSY AXDAX LTPRP TCWQD XECKJ OQAEK
 SKWNA TLVZU WZUDQ AHZCR OYIMC ENWQM YMJDH KAORT NPOAW NASLV HGOUS
 WHLRF ROBQI SVRMT DOQPG BLITU PZXBV PDWVX UOBRE DOLFA CGKRK KGMBY
 HDGOD KQRAZ HNULW BEJQK FSPXJ SXJQB OHYSR JXNCN IASEX DXUJY HJHLU
 PIQTV PCWWJ IJQPP EKKTG CPVUA LISGU HVUMX XDIVX MMYHQ WZWIY UMHUA
 QSMND BKJGN RJYSG CUVRS PNSYE GDSMI WKPPE QKSJY BKNPC SWGSF XGMLW
 PSYWY RDKYS WMQET OPMQB GYLHO QRZCG MIBFH SAMQI WDIPA XWDUW SUNAR
 TTJIP AHILZ SSQFV QNIYC ZKTJI VUVQA LFOET QWKTU FEWDS HOWGX FIQHU JOQIG
 MELCN ZDABW WNFSP OKCSC ACGWZ TXJTT WEKUD HRKUH YPWRR HXWBQ DGNTU JIUEL
 LLNLJ OJHKE SRNHP ROEUF LKFJX HNJNT NTYHN VZJTO INEVB QNCVS OAXUO
 DMIEH ALHGW FNXGU GGLTM TJ SMA KMIBW OVGCI KKJLQ TYZJQ VPOWR RNLGF SFLT
 ZRVHD HZJNH LVOFU RIYJP KMBW OVGCI KKJLQ TYZJQ VPOWR RNLGF SFLT
 BCSCS UOZJZ NWTQS BECOE VXFJ WEQSX SFYNS QRFJP INAPK GFNOJ CRK
 S.V.B.E.E.V.
 C.J.C.

CHAO CIPHER

EXHIBIT 2

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

GALLI	AESTO	MNISD	IVISA	INPAR	TESTR	ESWW	HORUM	OMNIU	MFORT	ISSIM
ISUNT	BELGA	EYPRO	PTERE	AQUOD	ACULT	UATQU	EHUMA	NITAT	EPROV	INCIA
ELONG	ISSIM	EABSU	NTYMI	NIMEQ	UEADE	OSMER	CATOR	ESSAE	PECOM	MEANT
ATQUE	EAQUA	EADDEF	FEMIN	ANDOS	ANIMO	SPERT	INENT	IMPOR	TANTY	PROXI
MIQUE	SUNTG	ERMAN	ISYQU	ITRAN	SRHEN	UMINC	OLUNT	YQUIB	USCUM	CONTI
NENTE	RBELL	UMGER	UNTWQ	UADEC	AUSAH	ELVET	IIQUO	QUERE	LIQUO	SGALL
OSVIR	TUTEF	RAECE	DUNTY	QUODF	ERECO	TIDIA	NISPR	OELII	SCUMG	ERMAN
ISCON	TENDU	NTYCU	MAUTS	UISFI	NIBUS	EOSPR	OHIBE	NTYAU	TIPSI	INEOR
UMFIN	IBUSB	ELLUM	GERUN	TWWWH	ISREB	USFIE	BATUT	ETMIN	USLAT	EVAGA
REENT	URETM	INUSF	ACILE	FINIT	IMISB	ELLUM	INFER	REPOS	SENTY	QUAEX
PARTI	HOMIN	ESBEL	LANDI	CUPID	IMAGN	ODOLO	READF	ICIEB	ANTUR	WPROM
ULTIT	UDINE	AUTEM	HOMIN	UMETP	ROGLO	RIABE	LLIAT	QUEFO	RTITU	DINIS
ANGUS	TOSSE	FINES	HABER	EARBI	TRABA	NTURY	QUINN	LONGI	TUDIN	EMMIL
IAPAS	SUUMC	CXLYI	NLATI	TUDIN	EMCLX	XXPAT	EBANT	WWWAD	EASRE	SCONF
ICIEN	DASBI	ENNIU	MSIBI	SATIS	ESSED	UXERU	NTYIN	TERTI	UMANN	UMPRO
FECTI	ONEML	EGECO	NFIRM	ANTWA	DEASR	ESCON	FICIE	NDASO	RGETO	RIXDE
LIGIT	URWIS	SIBIL	EGATI	ONEMA	DCIVI	TATES	SUSCE	PITWI	NEOIT	INERE
PERSU	ADETC	ASTIC	OYCAT	AMANT	ALOED	ISFIL	IOYSE	QUANO	YCUJU	SPATE
PREGN	UMINS	EQUAN	ISMUL	TOSAN	NOSOB	TINUE	RATET	ASENA	TUPOP	ULIRO
MANIA	MICUS	APPEL	ATUSE	RATYU	TREGN	UMINC	IVITA	TESUA	OCCUP	ARETY
QUODP	ATERA	NTEHA	BUERA	TWWWH	ACORA	TIONE	ADDUC	TIINT	ERSEF	IDEME
TJUSJ	URAND	UMDAN	TYETR	EGNOO	CCUPA	TOPER	TRESP	OTENT	ISSIM	OSACF
IRMIS	SIMOS	POPUL	OSTOT	IUSGA	LLIAE	SESEP	OTIRI	POSSE	SPERA	NTW

CHAOCIPHER

Exhibit 3

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

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

N O F D I S P A T C H E S A N D O R D E R S W R I T
O N X X Q H R T V N H N C O X O Q Q L O U N F B W D

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

T E D I N D E F E A T A N D D I S A S T E R F O R T
B N N A Y B Y G M N U I U E X T N V I J D L B Q T I

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

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

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

C A S I O N S W H E R E T H E I N T E R C E P T I O
V B Q S V K V L P G B E V O Q K P N V L L W A B X R

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

T E N I N P L A I N L A N G U A G E H A S R E S U L
C M V T E F E N S R X Y T O L P L E G G R Z R T N F

T E D I N D E F E A T A N D D I S A S T E R F O R T
O G G A B N L V A K M S K P K T D I B F T W D F R E

HE FORCE WHOSE INTENTIONS THUS
W O S U A B U Y I G R S U Q C A I N G K S B R K W Y

BECAME KNOWN AT ONCE TO THE ENEM
V V S Q L F G G M G V J M D F A Z D F Q X M S E G I

THE HISTORY OF WARTEEMS WITH HO C
V V V Q M D W H F J P W A G P A M A N H S F Y Y L F

CASIONS WHERE THE INTERCEPTIO
Y B F I X Q L H T F K K E F V E A K U I X M S X S Z

NO DISPATCHES AND ORDERS WRIT
Q N P L D V P H A F L Q N Z R X G R H X Z E B W Q P

TEN IN PLAIN LANGUAGE HAS RESUL
Y H I S N Y T L F U H F S M K P O W D G F D L Y Q R

TED IN DEFEAT AND DISASTER FOR T
H I V V U J H F B I S O P F K K L Z T A Y Y V A G N

HE FORCE WHOSE INTENTIONS THUS
T Q Q E C S F D B V T T M A P O M F N S F L T N M U

BECAME KNOWN AT ONCE TO THE ENEM
P T U H J P U O R Z T I S Y C M Q X E P T K F B S X

THE HISTORY OF WARTEEMS WITH HO C
U J A A P G Z N O R Y X N U G T U E S B A B J Z V T

CASIONS WHERE THE INTERCEPTIO
M D L R Y U P S A W C U Q X P W E I Y G F C C P Y N

NO DISPATCHES AND ORDERS WRIT
L R P M Y Z S L M H A R O C P Y F N Q D D V L E G P

T E N I N P L A I N L A N G U A G E H A S R E S U L
I S K X A S B H M L A N C J A U K M Y W R S U W N R

T E D I N D E F E A T A N D D I S A S T E R F O R T
I O C H Z T X E G W W O R O P G J Q I G N H J L W D

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

B E C A M E K N O W N A T O N C E T O T H E E N E M
A O B N X X U C J G V J E I Z C P G E K W H G U K V

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

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

N O F D I S P A T C H E S A N D O R D E R S W R I T
E P N Q O W R Q F B S K K Y C J O Y F C P R V J B Y

T E N I N P L A I N L A N G U A G E H A S R E S U L
Y G F S B Q E U K I Y J E L J Z K P H H L S X K N H

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

H E F O R C E W H O S E I N T E N T I O N S T H U S
S V N I X P B J C S U U O U D S W A G O D E X P B X

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

CHAOCIPHER

EXHIBIT 4

EXACT PLAIN TEXT OF ENCIPHERED 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 objectively 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 opportunity 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 colonialism, 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 little 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 realization of the normal nationalist urge for political freedom. * * *

CHAOICIPHER

EXHIBIT 4

ENCIPHERED EXCERPT FROM SPEECH MADE BEFORE BOTH HOUSES BY
GENERAL OF THE ARMY DOUGLAS MACARTHUR

A Glimpse of Chaos

1	PMRGA	HTMRZ	ABMGA	KMAAC	VEHRN	WQSJL	DIWLU	KKTGY	RVSAE	BPWFN	RKPDP
2	QTQJT	HQEME	ANFNV	PMKRZ	MIGRF	MGBOS	WPDYK	WQDWO	HCFYL	CIJVV	KXURX
3	ICFAP	QVZIA	GEPYK	IKOPJ	LJVUW	WXKSN	SYBOB	RDTJF	LDNNS	BMSMR	JDIMJ
4	FOHKZ	IZADR	JICVQ	QYJTT	MUZUN	UQJNK	BVWCU	MSNSA	VNRPB	YBJLS	WRUEH
5	KMGQF	UOIID	MZCPT	URRKX	IICXO	AIYIE	CNQYK	GOZOT	SFDYS	ZVREC	ATJRO
6	ONGEE	WBQZQ	CYCYU	WFCZC	DQTOK	ZUIEZ	PUTLW	ZMQNJ	FRIKF	ZHBAK	ALXKY
7	FCLVW	XXXFZ	BMOPO	ESYXE	FCZBW	NQKTC	YFBQY	JCUTP	RHOPC	ASGUK	YRHVX
8	CBPGF	KTXKC	QHUUU	WAZKO	GZCOK	GLEUP	DUBAN	VDZAE	VOAKW	IFHZE	RGPSR
9	NHCKB	EVEFR	AOMFA	BMQDT	VWBRL	RQUQE	RRGEG	ALISY	EMBDU	KVIVV	OXMED
10	BWXZV	OIVGF	HKDJQ	LVWFY	JOLKH	VHKYP	PIDKI	GNYRE	XDOGV	SPETT	SQWNZ
11	WLJOA	EIFBK	YHNOF	BARDI	EPCHV	HGONV	JHLZH	DRYVF	UXJSZ	DSWIK	REUIV
12	CTVOP	POWWD	KDIFD	YBCEK	LOPMF	SUTRD	ASFCS	EDKDH	BSTKH	PGETY	EOCES
13	NTEXD	AOFPJ	AWPYT	ZXZAD	CQZSQ	BQVHI	GMMOI	YFKQF	HFNNE	ADKGU	KIEIH
14	EAVST	HORHC	UPQHE	FVXRT	LYBZZ	CMHDV	VBXFT	WCSHK	IWAGT	VJVUR	ACNLP
15	IWDVS	BJIVG	UXDPJ	HLVCB	RGJMD	MLOHX	KQQLO	YTQLL	FQMGD	TWFBP	NLPXQ
16	PMQQM	FVLIN	GEPQK	STYHI	TVSGO	EOVZH	RKFZE	TVMSY	XRNIW	NDQRI	NTNYQ

17 OJSCB XAQUU MZRUM KLMMV XXFPX WZOLL QUSVV OGCUB YIECW WRSTC LYURR
 18 DZDGX XLKYJ OOIQY GQMQI SKIPV NAMSU HTVE TFWZO FPDAL TEAPD AUIOS
 19 LRMCA SIWHU GKHSI BRLPY PZDAX GFAKC QGJPW ZSNAV AZTLQ WJTFV HRVRM
 20 BVBBC XARBV BALLYB ZXSEO OLXJP NTFPQ QQOIX DIAHS TRNZK TYVQT WQSTT KRKPR
 21 OFMDN NQTIU UVKCC ZGPYX BUNSQ PDTXC GBQYY ZHHFR WHJYC SJHLE TKBBC YSMFT
 22 OULYP BRJTL ZGPYX BUNSQ PDTXC GBQYY ZHHFR WHJYC SJHLE TKBBC YSMFT
 23 SCVYJ YQAAA HBFHD TTCYJ ZCGLS SAWIF ZGRZS OEJDJ YVDXQ WSRIE NBJYP
 24 SQPPG KZUZZ HMTWT GLMED JLISA USBLZ XRLXI MPRJU ZVBLR HKOKW VZUWY
 25 HBKIS MAAOV FGPTH XQDIN WKESQ HETCI JHWHM AJPAN YDMFR QPZKG CKZED
 26 DOXDV DEHQV LJDUD SIVFE NYKGV ETOFX SDCBF XTESJ MUXEW TDWGX TRYLR
 27 RMJMM PGHHL SGVDV IJQPZ SDZJR TZVGM APFWD JBANS QVJZL NLMZN RHSXI
 28 PPXJL BXBVB ALYZY IAJIV KSQMX PDZNT ZPCFS TZOFI HADTY QAAVI
 29 YIOMW XYQHP GXTVO FXXHB NOFWL NKEFG JUWWP MHSMY DHHAJ ARKZJ DVJYO
 30 MAEZR GSSTD CUOCE PBVIL UOGBT VHDNR BNIDM GUHWE HZAGR QKOTC QEASC
 31 VDECN EPLGG NWTRH XVVHL YLUQL IKHSZ OJEIX BHWPS TAWCE VDYDW ATGQS
 32 YRULL WLQZG RHRZC XDLRV YIAKL DVKKA YNBSJ GBFCZ ERWFS NTCWZ AGSLC
 33 HPGVC PXRKI IUMPB CTPER JQXKI WRRXI SUAPW SQWIK VEFBS NCHOT ZBFSE
 34 HCXYR XRZWN TXOAI MOWEK PSIXP CPOLZ JJMXS CYLRF UKMYF DPRCO ARREU
 35 DGYQH TQCFJ NGNQA DTLBU MYVDM ULXIW XNVHG OIK

