

Are We Giving Away Our Secrets

*A Cipher Expert's View of the Methods Used by the Government
in Its Diplomatic Correspondence*

By

HERBERT O. YARDLEY

(Reading time: 25 minutes 10 seconds.)

ONE of my deep regrets at the reception of my book, *The American Black Chamber*, is that it has been accepted as a story of romance, intrigue, and ingenuity in the tracking down of spies through secret inks and ciphers, and the uncovering of foreign machinations through the decipherment of diplomatic messages, instead of as an exposé of America's defenseless position in the field of cryptography.

I had hoped to bring home to my government and to the public the dangerous position that America holds by abolishing the Black Chamber and at the same time retaining antiquated codes to carry our diplomatic secrets. All great powers have their Black Chamber where the best cipher brains in the world puzzle out our codes.

I had begun to believe that no one cared to read between the lines of my book, when I received an offer from a national magazine, suggesting that I write an article describing in detail what sort of codes and ciphers our government should adopt. In this manner it was felt that the Department of State might be stung from its lethargy and indifference. In almost the same mail I received a letter from one of America's leaders.

"Is it really true," he wrote, "that we no longer intercept the telegrams of foreign governments and decipher them? Is it also true that the State Department still uses the type of codes that do not safeguard our secrets from foreign cryptographers?"

My answer was very short. "Yes," I replied. "Both statements are unfortunately true."

A few days later I received a letter from this man, asking me to come to see him and begging me to bring some material that he might learn more of the science of cryptography. He pledged himself to use his influence to force the State Department, by indirect means, sooner or later to adopt safe means of communication.

"Since we no longer have a Black Chamber to decipher the secret messages of foreign governments," he wrote, "it seems criminal to me for the United States to play into the hands of foreign governments. The least we can do is to protect our own communications."

I gathered a few typewritten brochures on the decipherment of various types of codes and ciphers—it was always the practice of the Black Chamber to put down on paper any new discovery—and caught a train.

When I was announced, he cleared his desk, told his secretary that he was not to be disturbed, and, turning to me, wrinkled his heavy eyebrows.

"I want you to explain one thing to me," he demanded. "You worked in the code room of the Department of State as a young telegrapher and code clerk for a number of years. You demonstrated, by actually deciphering their codes, that they were unsafe."

"You were later employed by them on secret pay roll to intercept and decipher the messages of foreign governments. You handed the Department of State over a period of twelve years some forty-five thousand deciphered messages. Now tell me this: Why, in God's name, if you tell them their codes are antiquated, don't they demand that you modernize them?"

I leaned back in my chair and smiled. "Perhaps the

Department has ordered thumbs down since I wrote *The American Black Chamber*."

"Thumbs down!" he exclaimed. "What have personalities to do with national danger? If I had been Secretary of State and read your statement that our codes were unsafe, after having employed you secretly to solve foreign codes, I would have demanded your presence in Washington to prove your statement."

I had not expected such an ardent supporter. "It's obvious," I said, "that you have never worked for the government."

He sat frowning. "Why don't you write the Secretary of State a letter offering to turn over to him without hope of remuneration the type of cipher you describe in your book—an instantaneous and indecipherable cipher?"

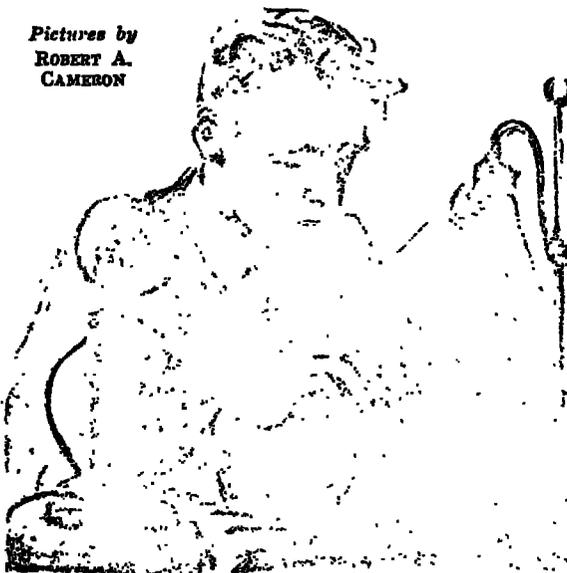
"A letter wouldn't do any good," I said. "Did you ever write the Department?"

THEN I told him of the letter I had received from a national magazine and that I planned to write a piece of exposition for it. He advised in justice to my government that I should first offer to turn over to the Department a memorandum of what form of secret communication they should use, with the provision that I be assured that the memorandum would be acted upon and not merely filed.

This I felt a waste of time and effort, and told him so. But he was so optimistic about the Department's reception of my letter, and so distressed at the idea of our secrets being read by other governments, that I agreed to follow his advice.

He gave me a stenographer. A while later I handed him the proposed letter, which read:

Pictures by
ROBERT A.
CAMERON



THE HONORABLE HENRY L. STIMSON
SECRETARY OF STATE,
STATE DEPARTMENT,
WASHINGTON, D. C.

MY DEAR SIR:

In Chapter XIX of my book, *The American Black Chamber*, a copy of which I am sending you, I have described a conversation I had with a member of the Department when he asked me to decipher the Department's code messages to determine if they were soluble. The conversation grew so interesting that the State Department had received a letter from the government was intercepting and deciphering diplomatic messages.

It is not necessary for me to describe the various positions I have in my book. Suffice it to say that I advised you that your codes were soluble by cryptographers; that it was not only the agents of foreign governments but also confidential code and cipher messages, but that they were undoubtedly doing so; that the methods used by the Department for encipherment were slow and cumbersome, being no greater



December 19, 1931

December 19, 1931

Liberty.

g Away Our State Secrets?

by the Government
e

THE HONORABLE HENRY L. STIMSON,
SECRETARY OF STATE,
STATE DEPARTMENT,
WASHINGTON, D. C.

JULY 11, 1931.

MY DEAR SIR:

In Chapter XIX of my book, *The American Black Chamber*, a copy of which I am sending you under separate cover, I have described a conversation I had with a responsible official of the Department when he asked me to analyze the State Department's code messages to determine whether or not they were soluble. The conversation grew from the fact that the State Department had received information that another government was intercepting and reading our diplomatic messages.

It is not necessary for me to detail here as I have in my book the various points discussed. Suffice it to say that I advised your official then that your codes were soluble by skilled cryptographers; that it was not only possible for the agents of foreign governments to read our confidential code and cipher messages, but that they were undoubtedly doing so; that the methods of the Department for encipherment were slow and cumbersome, being no great

improvement over those employed in the sixteenth century.

I was asked at that time whether it was possible to devise a system of encipherment which would render our messages indecipherable by even the most expert cryptographers of other governments. I assured your official then that it was possible to do this, but that it could only be done by a consideration of the fact that *no code or cipher is impregnable to attack unless it is insoluble by the inventor himself.*

All existing codes now employed are broken in the end by the fact that the inventor attempts to conceal repetitions. The only indecipherable means of communication is one in which there are no repetitions to conceal. The adoption of

[CONTINUED ON NEXT PAGE]

LEY

red thumbs down since I wrote *The Chamber.*

he exclaimed. "What have personal danger? If I had been Secretary your statement that our codes were employed you secretly to solve I have demanded your presence in your statement."

I such an ardent supporter. "It's at you have never worked for the

"Why don't you write the Secretary to turn over to him without hope type of cipher you describe in your us and indecipherable cipher?" do any good," I said. "Did you ever t?"

of the letter I had received from a and that I planned to write a piece of advised in justice to my government er to turn over to the Department a t form of secret communication they provision that I be assured that the be acted upon and not merely filed. e of time and effort, and told him so. stic about the Department's reception distressed at the idea of our secrets governments, that I agreed to follow

enographer. A while later I handed ter, which read:

"I SENT the code word meaning ten million dollars. Two letters were transposed, which changed it into the word meaning eleven million dollars!"



4. When the text letters are repeated, insert X, Y, or Z before enciphering; thus:

Change TT to TX TZ, which, enciphered, equal
ES BX (cipher).

Message: "Enemy retreating."

Divide into digraphs: en em yr et. re at in gx
Cipher: CT PD QZ PE PK SG BW TW

My friend examined the cipher for several moments.

"Note the lack of repetitions in the cipher for 'Enemy retreating,'" I said. "E is represented by C, P, and K.

"Before the war this cipher was considered indecipherable by the British. While I was in England studying cryptography under the British during the war, I asked Captain Hitchings, the great English cipher genius, if they still used the Playfair cipher. He smiled good-naturedly at me, and said, 'That was indecipherable once, but now we can solve it within thirty minutes.'

"AN example of the growth of the science as developed by our allies and the Black Chamber is the solution of the famous Bazeries cylindrical device. Here is a picture of it.

"The apparatus consists of twenty disks. Each disk is movable to any position and contains an alphabet of twenty-five letters, and each alphabet is different. The key is the order in which the disks are placed in the apparatus, which is so constructed as to permit the disks to revolve.

My friend was examining the cylinder intently. Suddenly his face lighted up. "I see the sentence, *Je suis indéchiffrable* [I am indecipherable] on the disks. How does one send this sentence?"

"By taking any one of the other twenty-four rows of letters. The sender may take the top line, GXYYSXDBRZZBGBBGSICU, or the bottom line, MUXRNPB RSRNMKKUDGFC, or any other row.

"Let us assume that the cipher message as received reads like the top line, GXYYSXDBRZZBGBBGSICU. The receiver, having first arranged the disks in the order of his key, moves each disk until he has these twenty letters in one row.

"He now searches the other twenty-four rows for something that makes sense. In this case he finds *Je suis indéchiffrable*.

"Commandant Bazeries, in describing his cipher, says that the possible combinations of the disks are approximately two quintillions [2,000,000,000,000,000], and, since each disk has twenty-five letters, the sentence *Je suis indéchiffrable* may be sent in as many different combinations as two quintillions raised to the twenty-fifth power!"

My friend blinked his eyes at this stupendous figure.

"Is what he says true?" he asked.

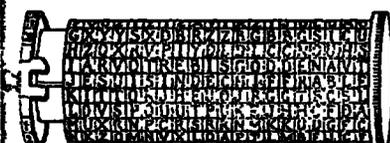
"What he says about the number of combinations is true," I replied, "but it is not true that the device is indecipherable. The Black Chamber developed a method of solution. To decipher a message in this system without knowledge of the key, we set up the message on twenty-four different disks and gave each letter a number based on its frequency in the English language. We then turned over the twenty-four disks to twenty-four clerks who began to add on adding machines the numbers we had given the letters. This gave us twenty-four charts of

statistics. These charts were then turned over to twenty-four cryptographers. After experimenting with these figures, one of the twenty-four cryptographers would find the correct solution."

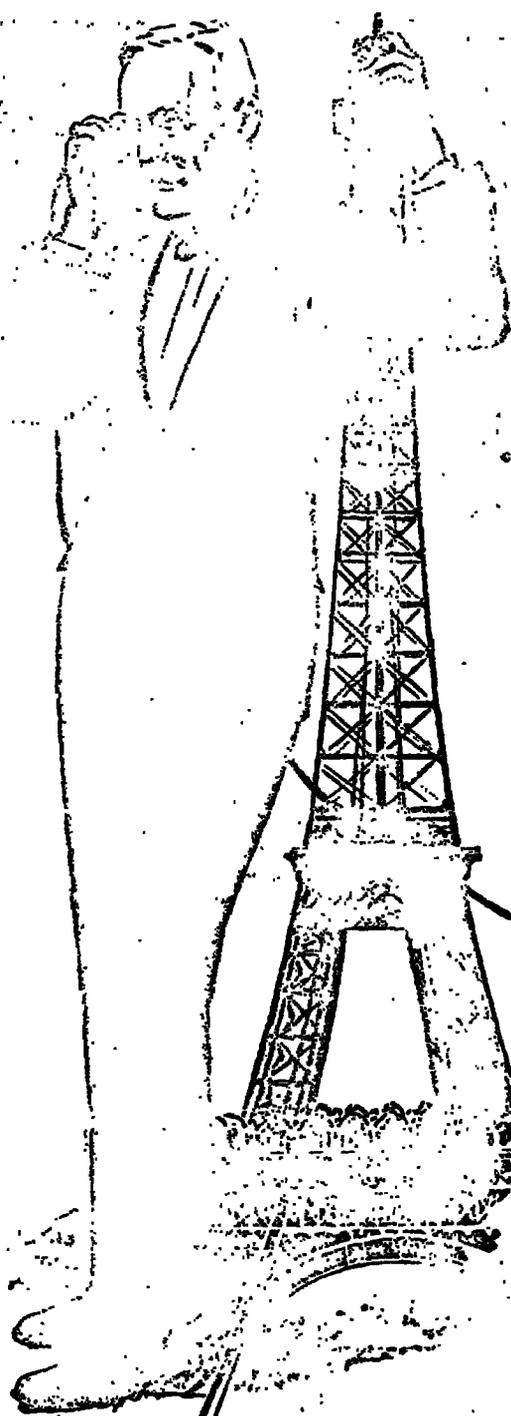
My friend shook his head doubtfully.

"There is nothing mysterious about this," I assured him, "and nothing particularly phenomenal. When a hundred or more men and women devote their entire time and minds to a problem, it is amazing the formulas they will discover for the solution of various types of codes and ciphers."

[CONTINUED ON NEXT PAGE]



The Bazeries cipher cylinder.



J
B
K
R
Z

that
lumn
to the

ngle.
er of

[ARE WE GIVING AWAY OUR STATE SECRETS?]
Continued from page eleven

"And the State Department has no one studying these problems?" he asked.

"No one," I answered. "The codes they now use are substantially the same as they were when I was a clerk in the code room."

"I think something will develop from your letter," he said hopefully.

I thought him a bit sanguine, but said nothing.

A week or so later I received an imposing envelope from the Department of State. This is what it contained:

THE DEPARTMENT OF STATE
WASHINGTON, D. C.

HERBERT O. YARDLEY, ESQUIRE,
WORTHINGTON, INDIANA.

July 14, 1931.

SIR: The Department has received your letter of July eleventh,

offering to turn over without charge or claim of any sort the information which in your judgment would improve the code and cipher service of the Government and guarantee complete secrecy for confidential messages, provided that the Department will satisfy you of its good faith in the matter, of its intention to give the suggestion fair and complete consideration, and that you shall also be satisfied that an examination will be given by a competent committee and the method you suggest adopted should the committee report favorably.

The Department would be very glad to receive from you or anyone else any information or suggestions designed to improve the efficiency of its communication service, but such information and suggestions must be tendered unconditionally, and the Department must be left free to decide the manner in which and the extent to which such information and suggestions may be employed. If you are willing to tender your suggestions on these conditions, the Department will be glad to receive them and give them such consideration as in its judgment may be merited.

Very truly yours,

For the Acting Secretary of State:
(Signed) WILBUR CARR,
Assistant Secretary.

This is, of course, what one might expect, but I had had a secret hope that it might be different. One would suppose from the letter that I was a stranger in the corridors of the State Department. One would never suspect that I had been employed there for ten years to turn over to the Department the secrets of the capitals of the world. Nor would one even suspect that I had ever seen a code book.

I very seriously doubt that the Department desires an improvement in the communication service, as Mr. Carr so diplomatically states; this entirely aside from unsafe codes. Any improvement requires investigation and change; investigation and change require thought and energy. In any case, let us go down to one of New York's greatest export and import companies and compare their communication service to that of the Department.

THE president of the Blank Exporting and Importing Corporation is a personal friend of mine. I sent in word that I had a strange request to make, and he consented to see me.

"I want to talk to one of your code clerks—not the chief of the code department, but someone you consider just an ordinary code clerk. I want to find out how much he knows."

He looked at me doubtfully, but told his secretary to send in Mr. Jones, who proved to be a thin, long-legged youngster, about seventeen. He stood nervously twisting his fingers.

"I'm down here to get some suggestions to improve the State Department's communication service," I told him. "But first tell me how long you have been encoding messages and what is your salary."

He looked at his employer, still uneasy. "I've been

here about a year," he finally said. "My salary is eighteen dollars a week."

"Eighteen dollars a week. Do you know much about codes and ciphers?"

"Not much," he replied.

"Well, if you don't mind, I want to ask you some questions, anyway. The State Department begins its messages something like this—" and I wrote down on a pad:

No. 648, July 28th. Reference your telegram No. 563, and our telegram No. 842.

"The telegram itself then begins in code," I said. "It takes the Department two and one-half cable words to send these references. How many words would it take you?"

The boy was now at his ease. He studied over the lines a few minutes, then said:

"I could encode that in one ten-letter word. We first encipher our telegram numbers and references in a figure table, then convert the figures into ten letters which are accepted by the cable companies as one chargeable word."

"That is a saving of two and one-half words per cable for most of the Department's messages," I told him. "But let us call it an average of two words. Now how long has this corporation been encoding telegram numbers and references in one word?"

HE was uncertain, but his employer said, since about 1905, when the new cable regulations permitting the use of ten arbitrary letters as one word went into effect.

I was figuring rapidly. From 1905 to 1931 is twenty-six years. When I was with the Department it averaged about 100 messages a day, taking into consideration the telegrams between other posts. For a period of twenty-six years this would be about 1,000,000 telegrams. Cable rates fluctuate, but conservatively the average cost over this period would easily be fifty cents a word. I scarcely believed my eyes. A saving of \$500,000!

"You make eighteen dollars a week?" I said. "Well, if you had been with the Department of State since 1905 and they had followed your system of enciphering references, you would have saved your government five hundred thousand dollars."

The boy's eyes grew as large as saucers.

The Department's codes are what we call "one-letter differential codes." That is, each code word differs from another by only one letter. I'll quote a few code words to illustrate this:

BABAB
BABAC
BABAD
BABAF

Now suppose that BABAB means *six-inch cruisers* and BABAC means *eight-inch cruisers*. The ambassador in London during the Armament Conference receives a long telegram from Washington which discusses the cruiser strength and ratio between England and America. In the telegram he finds the code word BABAB—six-inch cruisers. But Washington didn't send the code word BABAB. Washington sent BABAC—eight-inch cruisers, but in transmission across the Atlantic the code word became garbled, and upon reaching London read BABAB. So the ambassador rushes over to the Foreign Office and talks about six-inch cruisers instead of eight-inch cruisers.

In order to compare the Department's code words with those of the business world I asked this eighteen-dollar-a-week clerk what type of code words he used.

"Two-letter differential," he said without hesitation.

"Why?" I asked.

He asked to be excused, and within a few minutes came back with a standard commercial code book and opened it before me on the desk. These are two lines of the page he showed me:

AUWUS—buy as little as possible.
AUWYW—buy as much as possible.



December 19, 1931

Are We Giving Away Our State Secrets? — By Herbert O. Yardley

13

"I'll show you why we use a two-letter differential," he said. "Suppose the sender encodes 'buy as little as possible,' and sends AUWUS. It is garbled by the cable company, and when we receive the code word it reads AUWYS. The U has been changed to Y. We look for AUWYS in the code book, but, since each code word differs from all others by at least *two* letters, we cannot find the code word in our code book. This is a warning that an error has been made.

"Now suppose the code book had been constructed like this," he continued, and rapidly scribbled the following on a pad:

AUWUS—buy as little as possible.

AUWYS—buy as much as possible.

"With such a one-letter-difference code we would find AUWYS to mean 'buy as much as possible,' although our correspondent meant to tell us to buy as little as possible. Is that clear?" the boy asked me.

"Yes, it's clear enough, and especially interesting that a seventeen-year-old boy in the business world appreciates the importance of a two-letter differential."

I thanked him for his explanations. When he left the room his employer said, "If you are really interested in this sort of thing I can tell you something about code words. From bitter experience we not only insist upon a two-letter difference, but even refuse to use a code book

which contains code words which, when adjacent letters are transposed, are in the code book. Such a book once cost this firm a million dollars. We were bidding on a project in the Argentine and I cabled that we would increase our bid from nine millions to ten.

"I sent the code word meaning ten million dollars. When it reached the Argentine the last two letters had been transposed, which changed it into the word meaning eleven million dollars. Since that time you may be very sure that we not only use two-letter differentials, but we use code words that differ from each other even after adjacent letters have been transposed."

THERE seemed to me to be no reason for answering the State Department's letter. Had the Department seriously wished to improve its communication service it would have done so long years ago.

My friends agreed with me that the matter was closed so far as the Department was concerned, but advised answering the Department's letter and publishing the correspondence, which might awaken the Foreign Relations Committee to the serious situation.

The letter I finally sent follows:

July 25, 1931.

THE HONORABLE
THE SECRETARY OF STATE
WASHINGTON, D. C.

SIR:

I have a letter dated July 14 (A-C) signed by Mr. Carr, Assistant Secretary of State, in answer to my letter of July 11, offering the Department of State the indecipherable and instantaneous means of communication, without charge or claim of any sort, which I describe in Chapter XIX of my book, *The American Black Chamber*. Mr. Carr writes,

"The Department would be very glad to receive from you or anyone else any information or suggestions designed to improve the efficiency of its communication service, but such information and suggestions must be tendered unconditionally, and the Department must be left free to decide the manner in which and the extent to which such information and suggestions may be employed. If you are willing to tender your suggestions on these conditions, the Department will be glad to receive them and give them such consideration as in its judgment may be merited."

I must confess that I am bewildered by this reply. If Mr. Carr will search the archives of the Department he will find my memorandum written before the World War while I was a clerk in the Code Room giving a technical description of my method of breaking the Department's codes. Since Mr. Carr

was with the Department at this time this memorandum was handed my superior, Dr. Buck, then Chief of Archives, he is not only familiar with the type of codes then in use by the Department, but can appreciate the statement in my book that since then only one change has been made in the construction of the Department's codes. He must also be aware of the accuracy of the statement that those upon whose shoulders rests the responsibility of rendering our diplomatic secrets safe from foreign cryptographers have never had any experience in the solution of unknown codes and ciphers. And you must admit that unless one is qualified to "solve" codes one is scarcely qualified to determine the invulnerability of existing or proposed methods of secret communication.

I shall be very glad to tender unconditionally my instantaneous and indecipherable means of communication to a competent committee, but I must first be advised the names of the technical experts who would review my memorandum.

I feel sure you will agree with me, if you will investigate my history, that I am entitled to the assurance that my memorandum will be reviewed by men who have had long training and experience in the "solution" of codes and ciphers, and that you will agree with my statement that only an experienced solver of codes is competent to judge the indecipherability of secret means of communication.

For your information I should like to add that had the Department of State adopted

the secret means of communication I speak of it would not have been necessary for the President and Secretary Mellon, while using the telephone during the moratorium negotiations, to use slang, as the papers report, in an effort to keep secret from the French Government the nature of their conversations. With instantaneous and indecipherable means of communication in effect, the President could communicate with his Ministers without fear of being overheard.

If you will investigate the matter thoroughly I feel that you will also agree with me that in this mechanical age it would be difficult to defend the Department's present means of communication in which code clerks fumble around for hours turning the pages of antiquated codes.

Yours very truly,

(Signed) HERBERT O. YARDLEY.

I SHOULD like to have heard that conversation over the telephone!

I have seen and heard a lot of methods of secret communication, but the most delightful one is communication over the telephone by the use of American slang.

The incident reminds me of the attitude of a Signal Corps colonel in France during the World War. Headquarters had attempted to impress upon all commanders the vital necessity of the use of codes, for it was known that the Germans intercepted our wireless messages and attempted to read them. One day our own wireless intercepting station turned in a message that was in plain English, but divided into groups of five letters. The colonel who sent the message was ordered to headquarters to explain his action.

"What do you mean by sending messages in this fashion?" his superior officer demanded.

"There is no necessity for the use of codes," he replied. "The Germans are too dumb to read that message."

I presume that is the theory of our government. Foreign nations are too dumb either to understand slang or to decipher our messages, so why bother?

The whole trend of civilization is toward machinery. So the trend in cryptography should be toward machinery, which means, rapid, accurate, safe communication.

With machine ciphers in use, if Secretary Stimson wished to communicate with Ambassador Dawes in London, he could take the elevator to the code room and dictate his message to the cipher-machine operator, who, while writing the message on a typewriter, would at the same moment flash the message across the Atlantic. Should England listen in on the wire she would hear nothing but an indecipherable string of letters.

THE END

The first of a series of

Yardleygrams

puzzles in ciphers will

appear in

Next Week's LIBERTY