BLACK CHAMBER

WITH

WM FRIEDMAN'S COMMENTS

"Omnes Homo Mendax"

a J. Mc

F.W. 119.25/765

The American Black Chamber

By

HERBERT O. YARDLEY

Illustrated

THE BOBBS-MERRILL COMPANY
PUBLISHERS INDIANAPOLIS

Printed in the United States of America

PRESS OF
BRAUNWORTH & CO. INC.
BOOK MANUFACTURERS
BROOKLYN N Y

The Personnel of MI-8 c

Our Ski
The Fore
Who still remain behind

umes of copies of telegrams to read there the authentic record of his machinations. There too I found the thrilling stories of the seizure of the Panama Canal, the Venezuelan incident when America was on the verge of war with England, and other great moments of American nationalism. I was again sitting on a flour barrel in the village bakery, listening to intrigues of the vivid past as recited by the baker, an exiled German nobleman.

Were our diplomatic codes safe from prying eyes? Who knew? From the pages of history I had had glimpses of the decipherer who could unravel military and diplomatic cipher telegrams. Other countries must have cryptographers. Why did America have no bureau for the reading of secret diplomatic code and cipher telegrams of foreign governments?

As I asked myself this question I knew that I had the answer to my eager young mind which was searching for a purpose in life. I would devote my life to cryptography. Perhaps I too, like the foreign cryptographer, could open the secrets of the capitals of the world. I now began a methodical plan to prepare myself.

I quickly devoured all the books on cryptography that could be found in the Congressional Library. These were interesting but of no practical value. Next I searched Edgar Allan Poe's letters for a glimpse of the scientific treatment of cryptography. These were full of vague boasts of his skill—nothing more. To-day, looking at cryptography from a scientific point of view, for the American Black Chamber has never had an equal,

I know that Poe merely floundered around in the dark and did not understand the great underlying principles.

At last I found the American Army pamphlet on the solution of military ciphers. This pamphlet was used as a text-book for a course in cipher solution at the Signal Corps School at Fort Leavenworth. The book was full of methods for the solution of various types. The only trouble was that the types of cipher it explained were so simple that any bright schoolboy could solve them without a book of instructions. I was at the end of the trail.

It was obvious I would have to do my own pioneer work. I began at once. Due to friendly connections previously established, I had no difficulty in obtaining copies of code and cipher communications dispatched by various embassies in Washington. Progress was slow, for the clerical work incidental to the solution of messages is enormous. (Later I was to have fifty typists busy making elaborate frequency tables.) Some I solved and some I did not. But I was learning a new science, with no beaten path to follow.

One night, business being quiet, I was working on the solution of a cipher when I heard the cable office in New York tell the White House telegraph operator (we used the same wire to New York) that he had five hundred code words from Colonel House to the President. As the telegram flashed over the wire I made a copy. This would be good material to work on, for surely the President and his trusted agent would be using a difficult code.

Imagine my amazement when I was able to solve the

World War, the President sent a mission into Russia, headed by another of his favorites, George Creel. By this time all code messages filed with the cable companies came to me in a routine manner, and so simple to solve were the American Mission's secret dispatches that they were used as elementary examples in the training of student cryptographers.

For months now, I had been working on the solution of the American diplomatic code, which progressed slowly but surely. The clerical work incidental to its solution was uninspiring but unfortunately necessary. Aside from this I was making notes as I slowly chiseled out words here and there, for it was my aim to write an exhaustive treatise on this problem and hand it to my superior. I shall not explain my methods. To do so would reveal the character of the State Department code book which of course can not be done. Further on we shall follow the scientific analysis and solution of the codes and ciphers of foreign governments.

During these years from 1913 to 1917 many faces passed before me. Among them Mr. Lansing, who was later Secretary of State, stands out vividly. Immaculately dressed, gray hair, a short mustache, and the blank face of a faro dealer. In a deuces-wild poker game, I mused, he should hold his own with even Mont Mull, or at least with Salty East, our two village poker sharks. Had Secretary Lansing not been tied to a tyrant schoolmaster and represented in London by an Anglophile, history might well have been changed.

This was a beginners cipher with the key "CORN BREAD." C J m

distinguished audience present, I requested, in the name of the State Department, that the wire from Galveston, Texas, the cable from Galveston to Vera Cruz, the telegraph wire from Vera Cruz to Mexico City, be held open. A few minutes after seven the operator at Galveston said, "Here you are, forty words from Mexico City."

"What is it?" demanded Daniels.

"The message you are waiting for," I replied and turned to my typewriter, beginning to copy.

As the sounder spelled out the code words, Secretary Daniels began in a solemn voice, "Gentlemen, we are now receiving the most vital message ever confronted by this Administration."

I deciphered the message and handed it to them. Mexico refused. They actually turned pale, but had the good sense to run to the President.

All this time my work on the decipherment of the American diplomatic code was slowly progressing. At last I laid some one hundred pages of typewritten exposition before my immediate superior.

"What's this?" he asked.

"Exposition on the 'Solution of American Diplomatic Codes,'" I replied.

"You wrote it?"

"Yes."

"You mean to say our codes are not safe?" He turned to me. "I don't believe it."

"Very well," I answered. "This memorandum repre-

sents over one thou
and tedious detailed
years. I merely ask

As I left him he
for he had compile
secret communicati

Aside from this
mysterious trick, an
some occult power.
the combination of t
and as he did so h
Saturday, and I w
failed to tell me t
him for it.

All this I realize
morning. He had
permit us to carry
pockets. Instead,
telephone figures
book, anagrammed
resented the combi

Interested in sub
would be great fun
phoning for the c
the telephone woul
change the combin

I sat down and t
laughing about wh
before? He must

when I was in London studying cryptography with the British, an English Colonel told me that Captain Hitchings, their most brilliant cryptographer, was worth four divisions to the British Army.

Judging from the letters I found in the files of the War College, nearly every one in the United States had dabbled in ciphers. The authors of these letters were either offering their services, or had a new and indecipherable cipher that the government should immediately purchase.

From among the former I quickly selected a few scholars who appeared to have a superficial knowledge of ciphers, and ordered them commissioned.

!! first? A second lieutenant "orders them commissioned"

The spectacle of an eager thin-faced lieutenant, surrounded by a group of scholarly captains, was indeed a noteworthy sight, and I was obliged to submit to a great deal of good-natured raillery. However, they seemed to enjoy my energetic illiteracy, which they kindly termed "native intelligence," and I was amused at their eagerness to master the principles of cryptography. Here was a problem not found in the classroom, and not many of them would succeed. Scholarship, I suddenly discovered, was nothing more than the capacity to absorb learning. These scholars were faced with a quite different problem, for there was not a great deal of learning to absorb. They would be obliged to make their own discoveries. For this reason most of them were dismal failures.

The first of these captains to arrive was Dr. John M.

United States and England, pass these secret messages. Close by this cable, at the bottom of the Atlantic, lay German submarines. The cables can not be tapped, but by stretching other wires alongside for a distance of several hundred feet telegraph operators stationed in the submarines can copy the passing messages by induction.

No wonder the memorandum from the Assistant Secretary of State frightened the War Department! The Chief of Staff made a personal request for a prompt report.

Upon investigation, I learned that a copy of the War Department code book had been stolen in Mexico during our punitive expedition in 1916 and that a photograph of this was reported to be in the hands of the German Government. Furthermore, I discovered from actual tests that because of the technical construction of the code, it could be solved within a short time by the interceptors even though they were not in possession of the book.

I prepared my memorandum after this investigation, but I doubt that it was taken very seriously. However, the opinion of the British Government was held in respect and inasmuch as England had reported the unsafety of communications which *must* be kept secret, I was ordered to drop everything and revise the entire system of War Department codes and ciphers.

I promptly chose a man in the State Department Code Room whom I considered best qualified to follow my

directions, and tempted him with a commission. I wished him to take immediate charge of a subsection which would compile codes and ciphers. I had no intention of being overwhelmed with the details of this work for I had much else before me. In a very short time the subsection was efficiently functioning with ten clerks assisting the man who had been put in charge. The arrangement was wholly satisfactory for the work was being done well, and I needed to devote no more than an hour each day to reviewing some of the more important details.

This subsection prepared codes, ciphers, tables, etc., for communication with Military Intelligence officers, special agents, Ordnance Department agents, military attachés, General Bliss of the Supreme War Council, the commanding officer of American Forces in London, and General Pershing.

The compilation of codes and ciphers was, by General Orders, a Signal Corps function, but the war revealed the unpreparedness of this department in the United States. How much so is indicated by a talk I had with a higher officer of the Signal Corps who had just been appointed a military attaché to an Allied country. It was not intended that attachés should actually encode and decode their own telegrams, but as part of an intelligence course they were required to have a superficial knowledge of both processes in order that they might appreciate the importance of certain precautions enforced in safeguarding our communications.

When the new attaché, a veteran of the old Army, appeared, I handed him a brochure and rapidly went over some of our methods of secret communication. To appreciate his attitude, the reader should understand that the so-called additive or subtractive method for garbling a code telegram (used during the Spanish-American War) is about as effective for maintaining secrecy as the simple substitution cipher which as children we read in Poe's *The Gold Bug*.

He listened impatiently, then growled: "That's a lot of nonsense. Whoever heard of going to all that trouble? During the Spanish-American War we didn't do all those things. We just added the figure 1898 to all our figure code words, and the Spaniards never did find out about it."

He outranked me greatly or I might have added that we were not at war with medieval Spain but with twentieth-century Germany, who had gathered the brains of her empire behind the greatest war machine the world had ever seen.

Amazing as it may seem, his attitude was characteristic, even at the Front. One of the young officers whom we had trained confirmed this when he arrived at General Headquarters in France. He had received his instruction and practical experience in my bureau. Having observed the necessity for revising the War Department's communications in this country, he was eager to learn whether the codes and ciphers of General Pershing in use at the Front were safe.

The first thing which this young officer did after arriving in France was to induce his superiors to intercept by wireless our own radio code and cipher messages along the American sector. These codes and ciphers were used to transmit the most secret and important messages and by those who employed them they were considered safe.

Without any knowledge of the American method of encipherment, the young officer solved these messages within a few hours. The system was wholly inadequate and as a means of insuring secrecy was little more than a farce.

Through decipherments of German intercepted cipher messages, our Cipher Bureau in France knew that the enemy maintained a large staff of skilled cryptographers. All radio messages of the Allies and of the Americans were intercepted and sent to the German Cipher Bureau for attack. If this young American officer, who was still merely a student cryptographer, could solve these messages, the German cryptographers, with their long experience of code and cipher solution, without question had also solved and read these telegrams even more quickly than he. And once the system was broken, the enemy could solve every message as easily as the person to whom it was addressed.

As it happened, the contents of this particular decipherment were so important and their secrecy so imperative that the young officer's memorandum on the matter threw the General Staff into a panic of confusion. From these wireless intercepts he learned the disposition

of troops along the St. Mihiel salient, the number and names of our divisions, and, finally, the actual hour at which the great American offensive would be launched. This, then, the enemy knew!

The herculean effort of flattening out the salient, which for four years had formed a huge "pocket" inside the French lines, cutting off communication and stopping railways between Verdun and Toul, was the task of the Americans. And by reading the intercepts, the Germans had already learned in detail, just as easily as this young officer had learned, plans and preparations for the great American offensive. Incredible! No wonder the General Staff was in a panic. In these messages were contained some of the most important stratagems of the World War.

The Germans considered their position in the salient impregnable. General Pershing knew that the enemy had several lines of defense, the second known as the Schroeter Zone, another as the Hindenburg Line or Kriemhilde Position. What was to happen to the great American offensive of 1918 if the enemy was prepared for it? Or, if the defenses were not considered strong enough now to meet the offensive, was the enemy, warned by our messages, withdrawing?

The latter was the case. Our young officer had shown the General Staff the leak in the offensive, but it was too late to swoop down upon the Germans in a surprise attack. The messages were already in their possession and a retreat had begun. The American offensive

of September 12, 1918,
it represents only a smal
tremendous story in the
mans not been forewarn
in inadequate code and
at the Front. The enen
American confidence, th
munications. It was n
achieved. Pershing pur
and entered St. Mihiel
salient was broken, but t
pass. Too many staff
authorities in Washingt
trust in any encipherme
sight.

Seldom are the curta
tricate secret plots, da
known. In a history of
story of this amazed yo
formative generalization
cipher systems were inad
reveal his findings and gi
The story of his revelatic
enacted behind a curtain
was too late to undo the
had revealed the inadeq
Of this whole episode w
tory of the World War:

of September 12, 1918, was considered a triumph, but it represents only a small part of what might have been a tremendous story in the annals of warfare, had the Germans not been forewarned. The stubborn trust placed in inadequate code and cipher systems had taken its toll at the Front. The enemy had actually been taken into American confidence, through the non-secrecy of communications. It was not a surprise attack which was achieved. Pershing pursued an already retreating horde and entered St. Mihiel on September thirteenth. The salient was broken, but the surprise attack never came to pass. Too many staff officers in France had, like our authorities in Washington, placed a childish unfounded trust in any encipherment which could not be read at sight.

Seldom are the curtains drawn back so that the intricate secret plots, dangers and discoveries may be known. In a history of the World War, one reads the story of this amazed young officer, in some short uninformative generalization. He knew that the code and cipher systems were inadequate; but all he could do was reveal his findings and give warning to the General Staff. The story of his revelation is one which, like many others enacted behind a curtain of warfare, is seldom told. It was too late to undo the damage after the young officer had revealed the inadequacy of the codes and ciphers. Of this whole episode we read but one sentence in a history of the World War:

Despite all Pershing's precautions for secrecy in the St. Mihiel sector, the Germans expected attack and began to withdraw.

By reading contemporary history of the World War we are led to believe that inefficiency was found on this side of the Atlantic only. Such is not the case. In fact, the foregoing incident is but one of the tragedies of the American Expeditionary Forces, led by General Pershing. The Signal Corps in France was using inexpert and ineffective codes and ciphers to carry over the wireless the secret orders of the General Staff in France.

We have now seen the ridiculous spectacle of President Wilson, Colonel House, the Department of State, George Creel, the War Department, and General Pershing in France attempting to conduct successful diplomacy and warfare with schoolboy codes and ciphers. Later on, as late as 1929, we shall hear something of a novice on whose shoulders rests the responsibility of maintaining inviolate the diplomatic secrets of the United States Government.

The Code and Cipher Compilation Subsection in America won a great deal of praise from the War Department in the form of letters of congratulation. One letter directed me to inform all the officers and clerks who had contributed to the preparation of the new codes that the ingenuity, skill and painstaking labor involved in their conception and execution were thoroughly appreci-

seemed obvious that a Military Intelligence should control its own communications if it were to be held responsible for its vital secrets.

Therefore I commissioned another man from the Department of State Code Room, drew up a plan of organization, cut in direct wires to the cable points, employed a corps of code clerks and telegraph operators and within a few weeks we had a subsection which rivaled, in speed, accuracy and economy of transmission of cables, that of the Associated Press. It was also the duty of this subsection to train clerks for our agencies abroad and to instruct the numerous Military Intelligence agents who passed through MI-8, in the use of codes and ciphers.

Although I had already surrounded myself with men and women who were interested in codes and ciphers, and had drawn up a course of instruction, it began to look as if the war had converted me into an executive instead of a cryptographer.

As I turned my attention once more to the organization of the Code and Cipher Solution Subsection, I was seriously interrupted by a curious document which came from the Department of Justice. (See facing page.)

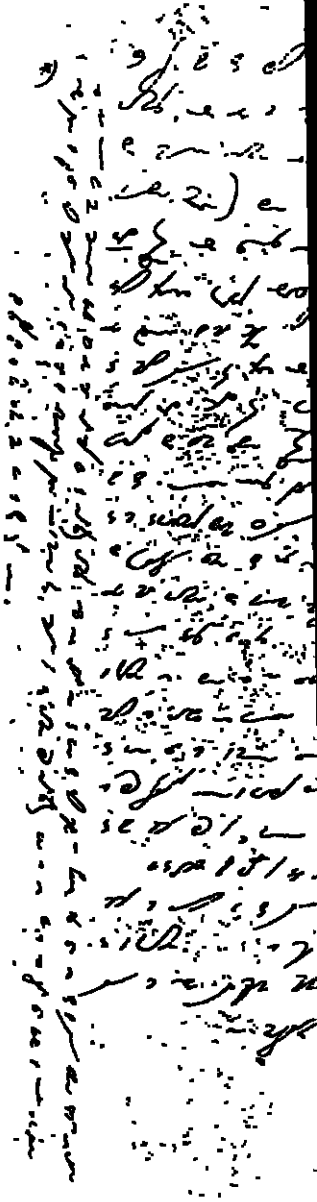
Colonel Van Deman called me to his office and handed me this strange letter. There were several pages.

"What's this, Yardley? Cipher?"

I looked the letter over very carefully.

"Looks like shorthand to me."

"I've already showed it to my secretary. She says it isn't Gregg or Pitman."



Page of Werner Tismer, pris

CHAPTER III

Secret Inks

The Code and Cipher Compilation Subsection, the Communications Subsection and the Shorthand Subsection were all necessary. But the really exciting activities came through actual contact with German-spy cipher and secret-ink documents. If I had never dreamed that the organization of the three foregoing subsections would fall to my lot, as a cryptographer, the final surprise came when Van Deman called me to his office and handed me a folded sheet of ordinary blank writing-paper.

I unfolded it and held it up to the light. There was not a trace of writing. I wondered what the next mystery would be, for a Department of Justice agent had just brought me a dead carrier-pigeon and wanted me to determine whether or not its perforated feathers carried a hidden message. There seemed no limit to the variety of problems which I was called on to solve. I wondered if this sheet of blank paper, like the dead pigeon, was but a mistake, a false alarm, and whether or not I could determine its meaning so readily. For I had, after examining the pigeon carefully, plucked several of the unperforated feathers and placed them in my desk drawer for examination the following day. But upon taking them out again, to make this inquiry,

covered secret inks for the use of their spies which could not be developed by heat or any other known chemical reagent. But perhaps these new major inks had not yet reached German agents operating in Mexico and the United States.

I immediately telephoned the National Research Council which kept a list of scientists, and asked them for the name of the most skilful chemist in Washington. Within an hour he was in my office. ?

After I had handed him the sheet of blank paper and told him my story, he said, "I am a chemist but I know nothing of secret writing. Why don't you send this to the British laboratory in England?"

"That would take three weeks. Van Deman wants quick action. Why not subject a small portion of the paper to heat? I'm afraid to try it myself; afraid I'll scorch or seriously burn the paper. You can do this, can't you?"

"Yes, I can apply heat without injuring the paper."

"Suppose we go down in the basement and try it." I suggested. "Would a lighted candle do? Or a hot iron?"

He told me he had what he wanted in his laboratory, and I suggested he write a note for delivery to his assistant.

Immediately I sent a messenger to get the equipment he needed, and within a half-hour we were buried in the basement. There, in our improvised secret-ink laboratory, the experiments began.

I believe J. M. Manly developed this letter.
Mc Hurd

I watched him carefully as he took the paper in his skilful fingers and passed a small portion of it back and forth over the heat. Again and again he did this, but the endeavor seemed to be useless. The page remained blank.

I had given up all hope of developing the writing, if it contained writing, with heat. Suddenly I heard him exclaim:

"Here are traces of writing!"

He lowered the paper closer to the lamp, then held it under the light while we both studied the curious characters which had appeared as though by magic. But despite our encouragement only small portions of writing were visible and these were too faint to be made out. It had been impossible to anticipate in what language the message might be written although we had expected German, Spanish or English. We continued to study the faint traces of what was revealed to us thus far. Perhaps it was cipher. Then suddenly, as I bent over, studying the characters, my heart stood still.

"The writing is fading away!" I cried.

But the chemist, sure of his ground now, laughed at my distress.

"Heat will bring it back again," he assured me. "Have you a photostat-room here?"

"Yes."

"Have them get a camera ready. We will have to photostat this writing after I apply more heat."

I hurried back to him after arranging for the photo-

stats, wondering ho
velopments had take
to his assertion, fade
Or had the continued
message clearly?

As I bent over the
was true. Distinctly
which had been, jus
blank paper, were the
of the message.

We rushed it to th
"It's written in Gr
camera ready?"

"Yes," I said exci
"I don't know," he
Greek scholar."

A few moments lat
the color of death un
photostat-room, hande
rious message. (See i

After the seemingly
feat of producing visi
paper had been accor
Greek scholar was neg
a translation of the me
and within a few hou
me the mysterious pa
the solution of the pro

Mr. ——,
San Antonio, Texas.

I beg you to betake yourself quickly to Galveston, in order that the representative of —— may deliver to you the $119,000 which you ask for in your letter of 5-8.

There is no need of your having trouble (disputes) with the I.W.W.

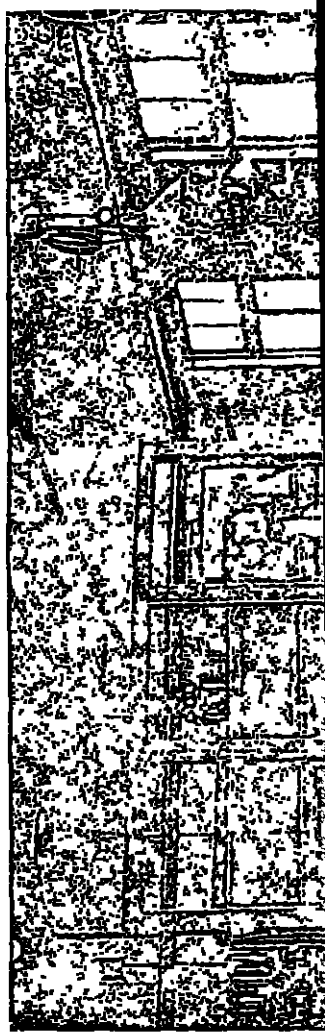
Your friend,
L. de R.

In the excitement which followed, I returned to my office and drafted a cable, for Van Deman's signature, to our Military Attaché in London, requesting that the British Government cable full instructions regarding necessary equipment and personnel for a secret-ink laboratory. The message also urged that they send at once one of their best chemists to the United States to act as an instructor.

We received an immediate reply, stating that ~~Dr.~~ Mr. S. W. Collins, England's foremost secret-ink chemist, would sail as soon as possible. The answer also gave us specific instruction for the organization of a secret-ink laboratory. I therefore immediately ordered commissioned several of our most brilliant chemists and instructed them to set up a laboratory according to the plan outlined in the cable from England.

Again!

While awaiting the arrival of Doctor Collins these chemists scoured the country for scientific information on the subject of secret ink. But as all had suspected, almost nothing was known in America on this subject. With the exception of a few scattered references in the



him, convinced now that he was well fitted to instruct them in the intricacies of this scientific battle of wits.

"There are many ingenious ways of carrying secret inks," he continued, "so as not to arouse suspicion. In one case, because of the discovery of forged passports, we carefully examined the belongings of two suspects who had just arrived in England and finally concluded that they had no secret ink in their possession, although our authorities were certain of their respective missions. But at the last moment, we discovered the ingenuity of the agents. Had they carried cobalt salts, potassium ferrocyanide or other secret-ink materials with them openly, we would have seized them without delay. But the spies had brought them in concentrated form. One spy had cleverly concealed potassium ferrocyanide in a tube of toothpaste. The other German agent carried his supply in a cake of soap.

"This discovery of ingenious concealment led immediately to the institution of more thorough search of suspected persons, and this, in turn, led to amazing discoveries. The German system of secret writing was based on carefully considered chemical reactions, but it was also based on practicability. In every possible case German chemists labored to devise an ink which could pass as something else if discovered. ~~Some~~ One of their inks reach a concentration so low that only a spectroscopic analysis can detect the presence of silver in them. Among the seized possessions of one agent the ink was in a scent bottle. The container concealed fifteen cubic centimeters

disgrace that I was utterly unable to defend myself properly. I feel that only my mother's plea to Theodore Roosevelt and that grand old lion's insistence on clemency, together with the good heartedness of the British, made the continuance of life on this planet possible for me.

I thought you might be interested in hearing from one of the leading characters in your story. It has created great interest here and I find myself a sort of local historical character, for the time being—a somewhat sinister historical character, however.

Cordially,
(Signed) GEORGE VAUX BACON

Doctor Collins suggested that we now take up the problems already before MI-8, but we begged him first to tell us about other secret-ink spy cases. He smiled good-humoredly and continued:

"There is an earlier case of Pickard, a German spy. This man carried the first example of a really clever secret ink. Before his time the enemy had relied on simple processes such as lemon juice, potassium ferrocyanide and alum, as in the case told me by Captain Yardley in which he developed by heat secret writing in a sheet of blank paper which a woman had concealed in the heel of her shoe. Pickard was convicted of espionage and condemned to death by court martial in September, 1916. He carried his ink in a bottle which also contained a small quantity of alcohol and perfume, hoping that the scent would be a protection.

"Alfred Hagn, like Pickard, carried the same ink. He possessed two bottles of this, one bearing the label

See page 57 — he says the most distinguished chemist in Washington opened this letter

Thus

this secret formula for developing all kinds of inks, the life of every one of our spies who uses secret writing hangs by a thread. In this respect we are helpless. It is useless for us to develop new inks. But once we discover this general reagent, we doubtless will discover a defense against its successful use.

"The last words of my superiors just before I sailed, were: 'For God's sake, find this general reagent. Beg America to join us in our researches.'"

La Fayette — we are here.

CHAPTER IV

Patricia

I left these chemists with their strange tubes and chemicals and returned to my office to draw up plans for a direct liaison between our laboratory and those of the French and British.

Our group of scientists was now divided into two sections: one, for research for the great discovery; the other, for technical study under Doctor Collins, which included the restoration of secret inks after development, opening and resealing of letters, forging of letters and diplomatic seals, photography, duplication of paper and envelopes in cases where they were injured, duplication of post-marks, replacing or duplicating seals, etc. Some of these duties required the employment of America's most adept criminals, skilled in forgery and counterfeiting.

The problem of discovering a general reagent for which the United Allied scientists struggled was finally limited to one field: if the Germans could develop a letter written in clear water, their reagent obviously was not based upon chemical reactions. Was water used merely to keep the pen from scratching the paper? Or was there another purpose? Would not any fluid which touched paper disturb the fibers of the surface? These premises seemed sound enough. Elaborate apparatus

were therefore installed for photographing and enlarging letters written with distilled water. Though it seemed obvious to all that the fiber had been disturbed by the water, photography brought no results.

For months chemists and photographers worked over this problem, for they were convinced that whatever form a general reagent might take, it would inevitably be one which revealed these disturbed fibers of the paper.

And then overnight the discovery! Credit for this discovery which revolutionized the technique of secret-ink laboratories is hard to place. There was such a close liaison between the scientists of all Allied laboratories, as each idea was flashed back and forth by cable, that I hesitate to mention one man or one nation. Suffice it to say that the long-dreamed-of general reagent was discovered. And like all great discoveries, it was so obvious, so simple that it left all the chemists dazed, wondering why they had not thought of it before.

A glass case; an iodine vapor! Nothing more!

Insert a secret-ink letter in a glass case and shoot in a thin vapor of iodine. This vapor gradually settles into all the tiny crevices of the paper, all the tissues that had been disturbed by pen and water. Even to the naked eye there forms a clear outline of writing.

No longer did it matter at all what secret inks enemy spies used. An iodine-vapor bath—and, like magic, appeared secret writing!

There was rejoicing throughout the American and Allied espionage circles. Our chemists had now caught

up with those of our enemies. But we must surpass them. Germany too knew of the iodine vapor or some similar treatment and, as Doctor Collins had pointed out, could develop the secret letters of the Allied spies. Many of these spies had been captured and condemned to death. The lives of others were in the hands of Providence. Our chemists must discover a formula of invisible writing that defied iodine vapor or any similar process.

While engaged in this worthy cause our scientists received a most disconcerting blow. It seemed incredible, but we were faced with the facts. Our examiners reported that iodine vapor no longer revealed secret writing even in cases where invisible writing was absolutely known to exist—known to exist from unimpeachable sources of information! What did this mean? It meant but one thing. Our great discovery had reached the ears of enemy spy headquarters in Germany. And with true genius in chemistry German scientists had quickly discovered a method of secret writing in which the iodine-vapor treatment was not effective—a method for which Allied chemists had been feverishly searching. German chemists were still one step ahead of us!

It may seem incredible that the iodine-vapor discovery was so quickly known by the enemies and a preventive method devised. To understand this rapid transmission of secret discovery to German headquarters, it is necessary to keep in mind constantly the intricacy and subtlety of the espionage system.

were the French to know that there was not, even in the uniform of an American Intelligence officer, a German spy to send back to enemy headquarters the sensational outline of French espionage which had been given? This story of the indiscreet liaison officer serves to illustrate the secret and rapid transmission of news, and by keeping it in mind we can better grasp the whole problem of secrecy. No wonder the triumph of our Secret-Ink Laboratory was discovered!

Now our scientists had to begin all over again. What had the Germans done to prevent the success of iodine tests? What made iodine-vapor tests possible? Disturbed tissues of the paper—disturbed by the pen or fluid. How could this disturbance be prevented?

After over one hundred experiments American chemists discovered that if a letter is written in secret ink, dried, dampened lightly by a brush dipped in distilled water, then dried again and pressed with an iron—the secret ink can not be developed by an iodine-vapor bath. Why? Because the dampening process disturbs *all* the fibers of the paper. Since the original crevices formed by pen and water were now destroyed, the iodine vapor settled on the entire surface of the letter but revealed no outline of secret writing.

This was a long-sought-for discovery. Germany could no longer develop the secret-ink letters of our own spies. Nor could we develop those of our enemy!

The development of secret writing was now at a standstill on both sides. We had at last caught up with the

Collins was sure about my wicked discoveries must have happened very rapidly in those days Mrs

Germans. Would we surpass them? There was now no known process of developing ink without knowing the reagent, provided the letter had first been dampened. In other words we were right back where we had been when Doctor Collins arrived.

An English discovery

We were engaged in a deadlock with the Germans except for one thing. We suddenly made another important discovery. We found a method of streaking suspected letters with two different chemicals—*and if these two streaks ran together it proved that the letter had been dampened.* And who would ever think of dampening a letter except a spy? Whether we could develop the ink or not, a dampened letter was sufficient proof that we were dealing with a spy message. not quite true

It does not mean such a method

But this was not enough. Our scientists must discover a reagent to develop *all secret-ink letters even though the letters were dampened.*

Inevitably in the battle of wits came this startling and greatest of all triumphs, a triumph that marked a new and final epoch in the achievements of secret-ink chemistry—the infallible reagent that revealed secret-ink writing under any and all conditions.

This secret was of such vital importance to successful espionage and was so jealously guarded—I doubt if a dozen men know of its existence—that it did not find its way to enemy ears. Even here it would be unethical to reveal the nature of this scientific formula, which came only after repeated discouragements and after long months of experiments by all the Allied chemists.

× Of course they did not.

× unethical? It is 5 laughs

Publish the unveiled lie! + comma + total.

Tabriz my capitalistic writers, you know how you hate boasting. You would to us

Picked up on San Francisco Censorship

Shortly after our chemists made this discovery our censor on the ~~Mexican border~~ intercepted the letter facing pages 82 and 83—because of the hieroglyphics on pages 2 and 4. This letter was addressed to Pardee Sanchez, a cover for Cabanne

The character of the secret ink and the importance of the plan revealed by the secret-ink writing indicate that this letter is from an important spy.

The secret ink as developed reads:

> I wrote you about the incarceration of the trio, etc.

This must refer to three suspects that have been arrested—spies are often vague in their secret-ink letters.

> Let me know as soon as you can about the boys going to France. If of no use in France they are preparing to flee.

Our department had already uncovered information that German agents planned to have at least one spy in each regiment. Patricia, who signs the letter, obviously is asking her superior how these boys are to operate when they reach France. There is more on this subject.

> I'm wondering if this ink is good. Let me know if those boys would be of any use to you in France.
>
> Preparations are being made for training and drilling in use of big guns in U. S. Officers returning from France for that purpose.

I regret to say that "Patricia" was never captured.

The letter was sent to Code & Cipher Sec. G's people could make nothing out & sent and turned it over to me. The message was in a ink. The paper was not dampened A. J. McGrail

Pages two and three of the "Patricia" spy letter. The mysterious symbols have never been deciphered

This was due to over-zealousness on the part of our agents on the west coast. I also regret that we were never able to decipher the hieroglyphics. They certainly contain a hidden meaning, for, as any one knows, the scansion of the two lines of poetry is ridiculous. The first line, "A thing of beauty is a joy forever," is the opening line of Keats' *Endymion;* and the second, "Of man's first disobedience and the fruit," is the opening line of Milton's *Paradise Lost.* In scanning poetry, each syllable, or each word of one syllable, takes but one mark, either accented or unaccented. The words *first* and *and* each have two marks, and rather curious ones at that. Perhaps the reader can decipher these cryptic signs. Or perhaps Patricia, if she sees this, will tell us all about them!

Patricia also writes that she is sending fashion sheets and face creams. Fashion sheets suggest nothing; however, secret ink was often sent in face creams by spies. "Cephalic index" is clear enough, but the diagrams below these words are a complete mystery.

There is one thing about the "open" letter that is reminiscent—the name Hopkinson-Smith. A red-haired young lady, obviously a German agent, once made the statement to one of my cryptographers, "You and I must work for the same cause." She gave her name as Smith-Hopkinson and her address in care of a certain bank in Los Angeles, which is not so very far from San Francisco where this letter was mailed.

Is Patricia, who writes of Hopkinson-Smith, the red-

blade carefully between the flap and cover, we raised the flap without much difficulty.

After photographing the contents, we resoftened the remaining gum on the envelope flap by the steam method and if sufficient gum did not remain, rubbed the edge against the moistened gummed edge of an unused envelope. This was better than application of glue for it assured the adherence of just the right quantity. Otherwise, an oversupply might ruin the job by making it sticky and splotched. In case any gum marks showed after the letter was resealed, we brushed the cover lightly with moistened blotting paper, followed by blotting with similar dry material. In cases where the seams were obviously affected by this steam process, we pressed them out with a hot iron and removed all traces of our work.

Replacing or duplicating seals was a much more difficult task than that of opening and resealing envelopes. The operation required more skill, and the process sometimes depended upon the nature of the seal. For a rough small seal, we used a thin sheet of lead with a backing of india-rubber placed on it and screwed down under a writing press. This took only a few seconds and any impressions which were made on the envelope during the process could be ironed out satisfactorily. For a perfect large seal, the operation was much more complicated.

We first dusted it with French chalk. Then we placed a piece of gutta-percha, slightly mixed with oil and

Usually Dentists modeling wax

I wonder where this process was carried out. I never saw it done. Mcf

heated with hot water, over the seal. This we put under pressure until the gutta-percha became firm and cold. Then, with another piece of gutta-percha, similarly heated, we made a second impression from the cold material after it had been covered with graphite and put under pressure as in the first operation. After taking the second impression, and after again thoroughly graphitizing, we put it in a copper-plating bath and started an electric current. Depending on the amount of current we could force, the process of obtaining our copper deposit took from twenty minutes to an hour or more. When we broke away the copper deposit from the gutta-percha we had a perfect seal. The back we then filled in with ordinary solder and supplied a handle.

Even more difficult than constructing a mold, was the process of getting the original seal off the diplomatic letter. We heated the wax to a certain temperature by a small electric hot-plate. Our success depended on applying just the correct amount of heat to the seal. At the proper stage we scraped the wax from the envelope with a small scraper. With this old wax, in case the seal was broken, we made a duplicate with the mold already described.

Thus did

Such tasks as these scarcely came within the duties of the chemists. It was obvious that specialists in this particular science must be added to the American Secret-Ink Laboratory. Thus two of the most adept criminals who had been convicted for forgery and counterfeiting were sought out and their particular skill incorporated

This is a lie I tried to that the English used two pointed fingers. We did not have such aids

mcf

with that of th

There was one

me. ? We were as

tents of a letter a

dent of Mexico.

terfeiter made a c

letter, photograph

velope, we discov

been made was to

loss to know what

us that he could

engraving a seal.

he made a closer e

seal and discover

made with an old

fied a distressing

necessary to obtai

collector to make

Note: The official hi

Report of the Chief of S

Code and Cipher S

this section concerned

war with Germany was

or to the Government

developed this section co

Secret-Ink Bureau.

Intelligence Services, thi

ing this hitherto little-

dangerous. Over 50 imp

led to many arrests an

lifting of the postal cen

were tested for secret i

It is not recall th

It may have been ad

Carrie and I worked

was the card used.

About December 15

with that of the Secret-Ink Subsection of MI-8.

There was one case in particular that always amused me. We were asked to open and photograph the contents of a letter addressed to General Carranza, President of Mexico. Before opening this letter, our counterfeiter made a copy of the seal, but after opening the letter, photographing the contents, and resealing the envelope, we discovered that the duplicate seal which had been made was too defective to be used. We were at a loss to know what to do. Finally the counterfeiter told us that he could perhaps approximate the original by engraving a seal. While this move was under discussion, he made a closer examination of a portion of the original seal and discovered, happily enough, that it had been made with an old and rare MEXICAN coin. This simplified a distressing problem in engraving, for it was only necessary to obtain one of these coins from an obliging collector to make a perfect seal.

Note: The official history of this bureau will be found on page 99 in *Report of the Chief of Staff U. S Army to the Secretary of War, 1919.*

Code and Cipher Section (MI-8)—Codes and Ciphers—The work of this section concerned an important field of endeavor which before the war with Germany was almost entirely unknown to the War Department or to the Government of the United States as a whole. . . . As finally developed this section comprised five bureaus, as follows:

. . . . .

Secret-Ink Bureau.—By direct liaison with the French and British Intelligence Services, this bureau built up a useful fund of knowledge covering this hitherto little-known science which is at once so useful and so dangerous. Over 50 important secret-ink spy letters were discovered which led to many arrests and prevented much enemy activity. Prior to the lifting of the postal censorship an average of over 2,000 letters per week were tested for secret inks.

I do not recall that this letter was addressed to Carranza. It may have been addressed to the Mexican Ambassador in Washington and I envisaged it this way. I found out that a Mexican coin was the one used. Yardley was in Europe at the time — Washington November 15th 1918

McG

I suggest that you check the story with the
DOJ and the Federal District Attorney NYC
Mcf

CHAPTER V

Madame Maria de Victorica

A great deal of romance has been written about the famous German spy, Madame Maria de Victorica, alias Marie de Vussière, the "beautiful blonde woman of Antwerp," but the authentic story of her activities, detection and arrest has never been told. Though she had been sought by the British Secret Service since 1914, it was the Secret-Ink Bureau of MI-8 that finally proved her nemesis.

Madame de Victorica was the most daring and dangerous spy encountered in American history. Her activities in this country between her arrival and arrest comprise a story of ruthless espionage and wholesale destruction that surpasses the wildest fantasies of our most imaginative fictionists. But like many other German spies, Madame Victorica did not reckon with our skilled chemists, whose glass test-tubes and varicolored liquids at last undid her.

On November 5, 1917, the British authorities gave us information, which, though it had no direct bearing on Madame Victorica, finally led indirectly to her identity. We were informed that a German agent of unknown name and nationality had recently left Spain for the United States with instructions to pay ten thousand

dress on the envelope is D. Crain, 932 E. 108th Street, New York;* and the letter itself begins, "Dear Mrs. Gerhardt." Here are enough discrepancies to awaken the suspicions of any novice.

"Have you investigated Crain at 932 E. 108th Street?" our chemist inquired. "That is the return address on the envelope."

"The report that came with the letter said that he was being investigated and promised to telephone in any information that was picked up."

"Be sure to tell me the moment it comes in. It might help us with our secret-ink tests."

As the iodine-vapor test had not yet been discovered, there was nothing to do but to test the letter with the reagents already known to be in use by German agents. Our chief chemist unfolded the letter and with deft fingers rapidly drew a line with a brush dipped in chemicals crosswise on the paper. When no visible writing appeared, he took up another brush dipped in another bottle and drew another line. At the third attempt faint traces of invisible writing appeared.

"It's written in 'F' ink—here's secret writing," he exclaimed; "in German script!"

"How long will it take to develop all the letter?"

"It may take all night. This is an important spy letter and we will have to work carefully in order not to injure the paper. We may wish to restore the secret writing." The secret agent turned to go, but was called

*Name and address have been changed.

Years of constantly facing the danger of detection had taken its toll even of this handsome and clever woman. Like so many other successful spies, Madame Victorica was of necessity a drug addict.

On June 7, 1918, the Federal Grand Jury found an indictment against her for conspiracy to commit espionage in time of war. She was never brought to trial, and though treated with every consideration, for the American authorities held her in the highest esteem, she aged rapidly behind prison bars.

Finally, a pitiable, broken creature, her beauty and charm gone, her spirit crushed, she died on August 12, 1920, and was buried at Kensico, New York, in the Gates of Heaven Cemetery.

Madame Maria de Victorica, who had cleverly escaped detection since 1914, was but the victim of coincidence and the Secret-Ink Section of MI-8. Though a pathetic figure in death, may she remain immortal in the annals of espionage.

I believe Victorica came clear with the Federal authorities in Newyork and furnished them inside information.

It is my impression that Victorica was captured by the Dept of Justice, and that the cipher stuff came as a consequence of the capture, not the capture as a consequence of the cipher stuff. U. Investigation could throw light on this.

Cf. time which chapter it was necessary to say this! The distinction was made in M.I.8 by the name? Whatever! A mere matter of getting the destinary and reading the messages! Cut it!

CHAPTER VI

Two German Wireless Intercepts

By January, 1918, the Code and Cipher Solution Subsection of MI-8 had grown to ambitious proportions. We not only had to train students for our own use, but were also required to teach recruits for General Pershing's Cryptographic Bureau in France. This double function severely handicapped us, for we felt that in justice to the American Expeditionary Forces we should send abroad the students who showed the greatest promise for successful code and cipher attack. I regret to say that not more than two of all those we sent to France distinguished themselves, but this was not the fault of MI-8.

The successful cryptographer requires a type of mind difficult to describe. The work is absolutely foreign to anything he has ever done. To excel, he not only needs years of experience but great originality and imagination of a particular type. We call it "cipher brains." I know of no better description. We were never able to formulate an intelligence test that would indicate the future of a student. The most successful students, when put on their own responsibility were, more often than not, utterly worthless, except for clerical work. I was later to have the unusual opportunity of studying under the British, French and Italians. I learned that they too

had the same experience. In the combined Cipher Bureaus of England, France, Italy and America there were thousands of men and women devoting their lives to this science, but among these thousands there were no more than a dozen who had "cipher brains."

By tracing the actual decipherment of a code message, the reader may be better able to appreciate the type of mind required for successful code attack. The following two code messages, destined to make history, are especially adapted for this purpose. The column of letters at the left are not a part of the telegrams. They are added for reference purposes.

Code Message No. 1 "G"

(A)	49138	27141	51636	02062	49140	41845
(B)	42635	02306	12201	15726	27918	30348
(C)	53825	46020	40429	87112	48001	88219
(D)	50015	43827	50015	04628	01315	55331
(E)	20514	87803	19707	33104	33951	29240
(F)	02062	42749	38951	40252	88608	14918
(G)	33446	16329	55936	24909	27143	01158
(H)	42635	01806	09501	49718	55927	50112
(I)	13747	24255	27143	02803	24909	15742
(J)	49513	22810	16733	41362	24909	17256
(K)	19707	49419	30408	19801	34011	06386
(L)	15726	47289	29901	37018	42635	19707
(M)	42022	80334	06733	04156	39501	03237
(N)	14521	87320	18508	42635	33951	29901
(O)	49117	46633	02062	16636	19707	01426
(P)	11511	42635	11239	04156	02914	12201
(Q)	28145	55381	49423	08455	12201	80205
(R)	88951	88219	50015	04156	43827	06420
(S)	28309	19707	33104	42635	00308	29240

resentatives in Europe for that purpose. Foreign Office Busshe. Machinery plans for rifle manufactory can be put at disposal. Details of machinery, technical staff, and engineer for aircraft could be arranged here with the authorized man of president [Mexico] to be sent by him for negotiations about loan. We agree purchase arranged by Craft (Kraft) in Japan of ten thousand rifles, etc., wished by president. General Staff Political Section number (?)

There was general excitement in Washington when these two messages were deciphered, for this would obviously open a new avenue to the United States for information of not only the intrigues of Germany, but also of the true aims and intentions of Mexico and, perhaps, Japan. What would the decipherment of further messages reveal? A hundred instruments tuned in on the powerful Nauen wireless station in order to intercept the next messages that would surely follow.

But Nauen was now suddenly silent. Why? Because news of our success had been flashed back to Berlin? There can be no other reason, for when Nauen finally again begins to send out messages their system of encoding has changed. MI-8, with all its care in the selection of its personnel, has a German spy within its doors. A finger of suspicion now points at every cryptographer.

Interrogative never returns to the 'finger of suspicion.'
Pure Guide. - I remember that about June 1919 I read some Berlin-Mex messages in 260 46 - They asked me to take a copy to Major (?) So and So & to say that when German messages to Mex had last been read some one (the implication was clearly some one not in the M.I.D.) had revealed the fact the code had been changed, the German [illegible] that the same thing had just happened again [illegible]

Of the Wabarski message it is merely necessary to say that Manly deciphered it and at once took them both to Yardley, with the other messages, for Yardley had given it up. There is nothing startling about the solution.

See notes Page 165

CHAPTER VII

Pablo Waberski

Early in February, 1918, Colonel Van Deman buzzed for me on the inter-office dictograph and asked that I come to his office at once.

He motioned to me to sit down beside him and without comment handed me a sheet of ordinary writing paper on which was typed the following series of letters:

15-1-18

scofnatupk	asiheihbbn	uersdausnn
lrseggiesn	nkleznsimn	ehneshmppb
asueasriht	htcurmvnsm	caincouasi
insnrnvegd	esnbtnnrcn	dtdrzbemuk
kolselzdnn	auebfkbpsa	tasecisdgt
ihuktnaeie	tiebacuera	thnoicaeen
hsdaeniakn	ethnnneecd	ckdkonesdu
eszadehpca	bbilsesooe	etnouzkdml
neuiiurmrn	zwhneegver	eodhicsiac
nnusnrdnso	drgsurriec	egrcsuassp
eatgrsheho	etruscelca	umtpaatlee
cicxrnprga	awsutcmair	nasnutedea
errreoheim	eahktmuhdt	cokdtgceio
eefighihre	litfiueunl	eelserunma
znai		

There was no address or signature—nothing but a jumble of letters, bearing the date January 15, 1918.

I had been with the War Department now for nearly eight months, and though thousands of code and cipher documents as well as secret-ink letters had passed

ary necessary to
to have him three
dley had given at
about the solution.

II

KI

el Van Deman buzzed
ph and asked that I

beside him and with-
of ordinary writing
wing series of letters:

15-1-18
uersdausnn
ehneshmppb
eaincouasi
dtdrzbemuk
tasecisdgt
thnoieaeen
ckdkonesdu
etnouzkdml
eodhicsiac
egrcsuassp
umtpaatlee
nasnutedea
cokdtgceio
eelserunma

ature—nothing but a
January 15, 1918.
rtment now for nearly
ids of code and cipher
k letters had passed

through my hands, I still felt a thrill at the mystery of the unknown when a jumble of letters met my eye. And aside from this I well knew that Colonel Van Deman did not ask me to see him personally unless he had something out of the ordinary to discuss.

I took it for granted that this was an important cipher, but I could not know that I was holding in my hand a document that would lead to one of the most extraordinary cases in American history—a document that would be responsible for the death sentence of a daring German spy.

"What do you make of it?" Van Deman asked.

"It looks like cipher and not code to me," I replied. "There are long sequences of consonants such as *shmppb* in the second line, and *snbtnnrcndtdrzb* in the fourth line. Usually, code groups are formed by combinations of vowels and consonants. Yes, I'm quite sure this is cipher. Would you mind telling me its source—where it came from?"

"Have you ever heard of Lather Witcke, alias Pablo Waberski?" he asked.

"Not a great deal—nothing except that he is suspected of being one of the most dangerous and unscrupulous German spies operating across the Mexican border."

"Well, we arrested him on the border a few days ago. Nothing was found on his person but this slip of paper. And since he is traveling on a Russian passport, we shall be unable to hold him even though we know that he is not so. He had at least a dozen papers of various sorts including a list of code words and their meanings.

7.

a German spy unless this cipher contains incriminating evidence." He paused and looked me squarely in the eyes. "Yardley, I want this message deciphered," he said in his incisive voice. "I want to know what it says. I am depending upon the cleverness and ingenuity of MI-8. Don't come back until you can bring me the decipherment." And he curtly dismissed me.

On only one other occasion had I seen Van Deman, usually even-tempered, so exercised over a cipher message. Several months earlier he had given me a spy message and almost demanded a decipherment by the next morning. I had worked on it all night and, basing my opinion on scientific analysis, had told him the document was not a cipher but a fraud, or, as we called it, a fake cipher. Van Deman was very impatient at my report, but in the face of criticism I maintained that the message was a pure fraud and had been constructed by some one who simply sat before a typewriter and pecked out a jumble of letters.

Van Deman's secret operator was plainly disgusted with both me and my report, but at my insistence consented to give the two principals in the case a severe cross-examination. As a result they confessed that they had made up the cipher out of pure malice in order to implicate a third person. The suspect was released from jail, and from that day no report from MI-8 was ever questioned.

Experiences of this type, however, led to one very grave difficulty—it soon became a tradition that MI-8

Note how closely these two tables resemble each other. Such a close resemblance would indicate that there is no doubt about this being a German transposition cipher.

How does one go about deciphering a transposition cipher? If in the spring of 1918 you had searched the libraries of the world you would not have discovered so much as one word that would give you the least idea how to attack such a problem. Even the pamphlet used by the United States Army for instruction in codes and ciphers would have given you no clues. This is what I meant earlier when I made the statement that the cryptographer in order to be successful must make his own discoveries; there is no beaten path to follow.

Now in German the letter *c* is always followed by the letter *h* or *k*, except in a few rare words and proper names. If you first write a message in German and then disarrange the letters by a formula, it follows that the letters of all the digraphs *ch* or *ck* are disturbed or disarranged in the same manner. And if you can discover a method for matching up correctly all the *c*'s with their affinity *h* or *k*, you have made long strides in the solution of the message.

The scientific method as developed by MI-8 for such a problem is first the tabulating of the number of letters in the cipher message that separate each *c* and each *h* or *k*. The message therefore was turned over to clerks to compile these statistics.

Was it possible, I wondered, that German cryptographers had not made this discovery? Evidently not,

German reservists who fled across the border at the declaration of war were recruiting and drilling Mexican troops; that high German officials, such as Jahnke (Chief of German Secret Service), Von Eckhardt (the German Minister), and the German Consul-General to Mexico were extremely friendly and operated openly with President Carranza.

Our agents reported that German spy plans were of a most ambitious nature: destruction at the opportune moment of the Tampico oil fields; establishment of a wireless station for direct communication with Berlin with the knowledge and cooperation of General Carranza (a most flagrant violation of neutrality—see Chapter VI); stirring up strikes in the United States through the I. W. W.; fomenting discontent among the negroes in the South, who, at the proper moment, were to start a series of massacres; destruction of war industries in the United States; and every other conceivable phase of war-time espionage.

We were of course deciphering all of the Mexican Government's diplomatic cipher telegrams which gave us a fair picture of the attitude of General Carranza toward the United States.

That our own spies were not exaggerating matters may be gleaned from the Nauen messages. See Chapter VI.

That Von Eckhardt, the Consul-General, and Jahnke were not only ambitious but ruthless in their activities may be surmised from the following which is a trans-

sceefaonen ehsmnrgoot erzruierne
incneinfee etkstnbika zeugdednkr
ibhideeree aeuneinzet dendaoeres
ighueuoanu uzasruoddi eeemcutiee
teanchchdd igrrrrrrnso esiereerde
emiehdeade nhdthmnosm elolmeennd
rhktendend uockehaete cresfjhouk
fhbmkttemn ledsetuehl enimliaern
ehzeuesesg snmeuhaimd rrcnsshikh
rahdbennjh osesedfhin meerneaseh
udzsgifmri uoisoehsna deitfeebsa
ekamhceant eaoabeunou flrnneizua
nfphhmnfon gusdiporth fhrsmdndrl
tmaurrwini ulnezsknts hdrsdbbnip
osedlsuctb ctidafsaue ttunwirhbr
ngnedumiis veurakklne enrcmtdtes
nsinleimgr iehnlemnlg gkhegdatee
eaacegtero arusrelari graenuinbi
eeikdnspni ribhhpkuze tkfseshdne
haravntsee ipreicseuu emozusmudh
ipitnndark nalccssgle ursttrlecp
irbdnsaend recoeteian mdtnnheamt
ntzeomtier nukwmtteke ucebdihtnf
cswgowgeen notzreasnu caahnbgeil
ceernsnrta lgghcue*

Translation of Decipherment

[Addressed to all German Consuls in Mexico]

Please carefully and immediately burn without remainder, and destroy the ashes of, all papers connected with the war, the preservation of which is not absolutely necessary, espe-

*After reading the decipherment of the Waberski document, the reader may wish to attempt to decipher this. The translation of the German decipherment follows.

The decipherment of PQR was, in the main, the work of Capt Stevens. I finished entering it

C J M

always maintained. He instructed me to give a copy of the letter to each officer and clerk who had contributed to the decipherment.

This German cipher message, officially designated PQR, is without question the frankest and most open document treating on the subject of espionage, excepting the Soviet spy document in Chapter XIII, that I have ever seen. I am always amused at the frankness with which diplomats express themselves in secret code telegrams, and their childlike faith that a cipher or a code can keep their utmost secrets from prying eyes. Diplomats, as we read more of them later on, are almost as naïve as children.

In retrospect, it is no wonder that my superiors were concerned about the cipher document found on Pablo Waberski, for Mexico was full of spies operating across the border and, so the reports read, Pablo Waberski was the most dangerous of them all. There were even reports from the British who suspected him of being responsible for the Black Tom explosion in New York Harbor in July, 1916.

Pablo Waberski, so the reports stated, entered the United States at Nogales, Arizona, on February 1, 1918, traveling on a Russian passport. He was not aware that our secret agents in Mexico had reported his activities and was surprised when arrested as he crossed the border.

He was rushed to the Military Intelligence Officer at the camp of the 35th Infantry and searched. Nothing

but a sheet of writing-paper containing a series of ten-letter groups was found on his person. However, since our authorities already had reports of his activities, he was kept under close guard.

I returned to MI-8 with no small concern, for I understood better the importance of the Waberski document. Van Deman had placed the issue squarely in the hands of MI-8. Would we be able to outwit the German cryptographers? Was our skill greater than theirs?

When I returned a great deal of progress had already been made. All the necessary statistics had been prepared and several cryptographers, under the direction of Captain Manly, were busily engaged in piecing the message together.

The Waberski cipher had been retyped and each letter given a number; thus,

s e o f n á t u p k etc., etc.
1 2 3 4 5 6 7 8 9 10

Our frequency table already tells us that there are 15 *c*'s and 20 *h*'s. All the *c*'s were underlined in red and all the *h*'s in blue, so that the eye could readily find them. They were then typed on another sheet of paper together with their letter-numbers; thus,

H	H	H	H	H	H	H	H	H	H
14	17	52	56	69	71	152	172	181	193
H	H	H	H	H	H	H	H	H	H
217	253	264	307	309	367	373	378	396	398

C	C								
85	109								
C	C								
294	319								

Now, as al
mathematical
arranging the
the letter *c* is
the digraph *c*
analysis of *ck*
letter-number
all the *h*'s, we
cipher is a gri

Let us, the
the resultant
dealing with.
be graphically
numbers in a
letter-number
paper. By
column from
arrive at the
each *c* and e
smaller than t
424, the numb
ber before sub
424 equals H-

The followi

C	C	C	C	C	C	C	C	C
85	100	145	199	201	259	266	270	290
C	C	C	C	C	C			
294	319	331	333	381	387			

Now, as already explained, our problem is to find the mathematical formula that the Germans used in disarranging the original text. And since in pure German the letter *c* is nearly always followed by *h* or *k* (only the digraph *ch* will be considered in this problem, as the analysis of *ck* will not be necessary), if we subtract the letter-numbers of all the *c*'s from the letter-numbers of all the *h*'s, we should find a common factor, unless the cipher is a grille or double transposition.

Let us, therefore, take this first step and see whether the resultant figures indicate the type of cipher we are dealing with. The distances between the *c*'s and *h*'s can be graphically shown by writing the *h*'s and their letter-numbers in a horizontal column, and the *c*'s with their letter-numbers in a vertical column, on cross-section paper. By subtracting each figure in the vertical column from each figure in the horizontal column we arrive at the distance, or number of letters, between each *c* and each *h*. In cases where the *h* number is smaller than the *c* number it will first be necessary to add 424, the number of letters in the message, to the *h* number before subtracting; thus, in the first case H-14 plus 424 equals H-438 minus C-85 equals 353.

The following figure shows the result of this process:

it is difficult to believe that MI-8 is cleverer than the German cryptographers who obviously have not discovered a method for solving transposition ciphers or they would never have recommended such a system. Let us be fair to the German cryptographers. Perhaps German officials are like our own and do not take the recommendation of cryptographers as seriously as they should.

We have already noted that 8 of our 15 *c*'s are properly placed, or at least they are followed by *h*. Let us see if we can place the remaining 7 *c*'s.

C, line 50, is followed by *k*; *ck* is a very common German digraph.

C, line 78, is followed by *i* in the four-letter group *n a c i*. This is most unusual because in pure German the letter *i* never follows *c*. Have we made an error? Perhaps the copyist has made an error, or the German who enciphered the message. If not, and we are on the right track, *n a c i* must be a group of letters from a foreign word. We have already noted the Spanish word *peso*. Perhaps *naci* is the beginning of the Spanish word *nacional—national*. This seems reasonable for in line 86 we find *onal*.

C-319, line 103, is the final letter of the trigraph *nec*. This *c* is apparently also not followed by *h*, for a reference to Figure 4 shows a question mark. As *nec* suggests no word, let us pass to the next *c*.

C-331, line 7, and *c*-381, line 57, have question marks after them in Figure 4. They either are not followed by *h* or the technical construction of the table used by the

The sequence in each of the above lines is 16-8-2-3-8-12-8-11.

After dividing Figure 9 into German words, it reads:

Decipherment

An die Kaiserlichen Konsular-Behoerden in der Republic Mexiko Punkt.

Strenggeheim Ausrufungszeichen!)

Der Inhaber dieses ist ein Reichsangehæriger der unter dem namen Pablo Waberski als Russe reist punkt Er ist deutscher geheimagent punkt Absatz ich bitte ihm auf ansuchen schutz und Beistand zu gewæhren komma ihm auch auf, Verlangen bis zu ein tausend pesos oro nacional vorzuschiessen und seine Codetelegramme an diese Gesandtschaft als konsularamtliche Depeschen abzusenden punkt

VON ECKARDT

It was daylight before the message was completely deciphered and translated. It was too late to telephone Van Deman. Aside from this I hesitated to telephone the fact that the Waberski document had been deciphered. Since it was Sunday, he would not be at the office before ten o'clock. The message had produced too much excitement for sleep; so there seemed nothing to do but wait for him.

I tried to appear calm when Colonel Van Deman entered his office. He seemed a bit surprised when he found me waiting.

"What's on your mind, Yardley?" he asked as he sat down at his desk.

Lather Witcke, a
durin

a German transposition cipher. The address, signature and the message itself were first written in German and then by a prearranged diagram the letters were mixed up. Our problem was to discover the formula by which the letters were disarranged."

"Have you discovered the diagram?"

"Yes."

"Please offer my sincere congratulations to the personnel of MI-8," he said. "If for no other reason, the decipherment of this document justifies your bureau."

For an hour or more we discussed the decipherment of the Waberski document, and the feasibility, now that we had discovered the German espionage method of identifying their secret agents, of drafting identification ciphers along the line of the Waberski cipher for use by our own agents in Mexico, so that they could pose as German spies.

On February sixteenth Pablo Waberski, manacled and under heavy guard, was taken by train to San Antonio, and from there to the military prison at Fort Sam Houston. Though carefully guarded while incarcerated here and awaiting trial, Waberski composed a cipher message and attempted to have it smuggled out of prison. It was intercepted and sent to MI-8 for decipherment. *

It was addressed to Señor K. Tanusch, Calle Tacuba 81, Mexico, D. F. The translation reads:

> Need my note-book which I left in Mr. Paglasch's safe. Very necessary. The address,

Señor Jesus A
is absolutely s
in secret. I h
addresses whi
people here th

Waberski obvi
desperate position
In the hope of i
mailed the cipher
Finally in Aug
name was Lathe
court. He was ch
trial lasted two d
court sentenced hi

The failure of
other spies, was d
increased, our po
to affect the life o
the decisions of g

* Sentenced - yes
commuted sentence
see June 4, 19 = 0

But he was l
Germany, and
was alive a

yes, Waberski
and released
on condition
Lost paid hi

Señor Jesus Andrada, Box 681, San Antonio, is absolutely safe and it will be delivered to me in secret. I have forgotten certain names and addresses which I need in order to show the people here that I am innocent. Need money.

Waberski obviously recognized that he was in a desperate position.

In the hope of intercepting the reply, our authorities mailed the cipher message. But no answer ever came.

Finally in August, 1918, Pablo Waberski, whose real name was Lather Witcke, was tried before military court. He was charged with being a German spy. The trial lasted two days. He was found guilty, and the court sentenced him to be hanged by the neck until dead.+

The failure of Pablo Waberski, like that of many other spies, was due to the skill of MI-8. As our skill increased, our power as an organization was not only to affect the life of a single person but was also to shape the decisions of governments.

+ Sentence - yes - but President Wilson commuted sentence to life imprisonment on June 4, 1920.

But he was later pardoned and sent back to Germany, and at last reports in the press was alive and well.

Yes, Waberski (or rather Witzke) was pardoned and released from Leavenworth Dec 21-1923, on condition he left U.S. at once. The German Govt paid his passage.

Of the Spanish codes much could be said, but cannot here be indicated. All this showed the Mexican 9.51/ Victoriano Huerta gave us the Spanish diplomatic codes! —
See p. 218

CHAPTER VIII

A Stolen Code

One morning my correspondent at the Department of State called me on the telephone and asked me to come over as soon as possible. The whole Department of State is controlled by a small clique in the diplomatic corps, and this man was considered one of its most brilliant leaders. He was a staunch supporter of MI-8 and dealt directly with the Secretary of State.

He was positively the most mysterious and secretive man I have ever known in my sixteen years of experience with the United States Government. Although I dealt personally with him for several years, I know less about the man now than I did the first day I saw him. He was almost a human sphinx and when he did talk his voice was so low that I had to strain my ears to catch the words.

He offered me a cigarette without any greeting and lighted one himself. A good minute passed before he spoke. Being accustomed to this procedure, I always forced him to open the conversation. Sometimes several minutes passed.

"The Spanish code?" he almost whispered.

By this he meant when were we going to be able to read Spanish diplomatic messages. Our powerful wireless station on the coast of Maine was intercepting hun-

"What has the Captain told you, Miss Abbott?"* I began.

"Nothing, except a very amusing story," she said.

I felt a certain reluctance about taking her into my confidence, not because her report was by any means discouraging, but because I had heard so many stories of the failures of women agents. But there was always the chance of success; and even if she did tip off our hand, all that she could disclose would be the fact that the United States Government was making an effort to solve the Spanish Government's codes. Should Spain learn of this it would mean a change of codes. We had already made a great deal of progress and I knew I would have to impress this on Miss Abbott.

"You have no idea why you were asked to come here?" I began again.

"No. Mrs. Blakeslee telephoned me that I was wanted here. She gave no reason. She was very mysterious about the matter, but she always is."

"You know the Spanish Ambassador?" I asked her.

"Yes."

"Any of the Embassy staff?"

"Slightly."

Perhaps, I thought, the best plan would be to tell her as little as possible until I had an opportunity to judge her character and discretion.

"You could cultivate a better acquaintance with some of these men?"

*For obvious reasons the correct name can not be given.

CJM tells me this was Miss Willard. See entries on p 191-3

lowing, apparently an innocent cablegram from Germany," I said, and showed it to him:

From Germany
To Schmidt & Holtz, New York

Give Victorica following message from her lawyers lower terms impossible will give further instruction earliest and leave nothing untried very poor market will quote however soonest our terms want meanwhile bond have already obtained license.

Disconto

"This cablegram appears on its face to be harmless," I said, "and seems to concern a lawsuit or a sale. In any case, it readily escaped the British Censor for Victorica was unknown at that time."

I now pulled out another document. "Here," I said, "is a photograph of the letter containing instructions for decoding cables of this type. You can see the secret writing as developed in our laboratory.

"The first consonant of each word in a clear text message stands for a figure. In the case of this particular cable the equivalents are:

1 = d t
2 = y n z y
3 = m w
4 = q r
5 = s sh
6 = b p
7 = v f ph
8 = h ch j
9 = g k x
0 = l c

Victorica may have given this to the Federal people in New York may

I don't know why Zimmerman did with this but it was not worked out by them. Probably the story was captured

If Boyd could only get a copy of one of these codes, and if this girl could find out whether or not the others were secondary copies, we need only discover the system, or if there was no system, the mere fact that there were primary and secondary codes would aid us. Negative information is often as valuable as positive.

"I think I should like to study cryptography," she said.

"All right. I'll give you a copy of our short course of instruction. But don't clutter up your mind with this. After all, one cryptographer can't do very much. If you can pick up odd scraps of information for us you will be much more valuable. Suppose you cultivate Mr. Gomez. If you succeed in this task you will be our best cryptographer."

"I'll try," she said.

And one had only to look at her to know that she would succeed. I must confess that I felt rather sorry for Mr. Gomez.

The girl prepared to leave, and I turned to her.

"Communicate with me at once if you learn anything. Of course I should warn you to be discreet and all that sort of thing, but I don't think it is necessary."

"It isn't," she said simply. Then she flashed a reassuring smile at me and was gone.

Boyd left Washington for the Panama Canal Zone a few days later, and it was not long before I received an inquiry from him requesting me to cable him at once

The account of the stealing of the code in the Canal Zone is correct, but the rest of the description of the breaking of the Spanish codes is fiction. While I was abroad, the British gave me copies of two of the Spanish codes. From these two the system

several copies of different Spanish diplomatic messages. In response to my inquiries about his success, I had only the laconic reply that he was progressing satisfactorily.

Then came a message requesting funds on the Royal Bank of Canada with the urgent demand for quick execution. And then he seemed doubtful about the code he was preparing to photograph. He did not seem sure that it was the code we desired.

Boyd had stolen into the Consulate at night, opened the steel safe which protected the diplomatic code, but had been unable to decipher the messages which we had cabled. For this reason he doubted that he had discovered the correct code. Boyd also explained that only a few pages of this book could be photographed each night and to make a photograph of each page, with the facilities he had available in his secret proceedings, would require time.

We were not surprised that the book Boyd found would not decode telegrams passing between Spain, America and Germany. Miss Abbott had already supplied us with detailed reports regarding all phases of the Spanish diplomatic codes. There was an amazing network of codes within codes.

According to Miss Abbott's reports, and of course confirmed by cryptographic analysis, the Spanish Government was using in all twenty-five codes. Each message was prefaced with an "indicator," a special number indicating the particular code which was used to encode the message. The complete list, so far as we were able

and instructed me to show him about. I was not particularly pleased when I was instructed to tell this officer our secrets. But in order that the reader may appreciate my point of view it will be necessary to digress.

MI-8 had been on good terms with the Navy Signal Office which compiled naval codes and ciphers. In fact this office had submitted several messages encoded in their battle codes and asked if, in our opinion, their methods were safe. When the Navy Signal Office transmitted their first problem to me, they remarked, facetiously, that they wished me luck, for they thought I would need it.

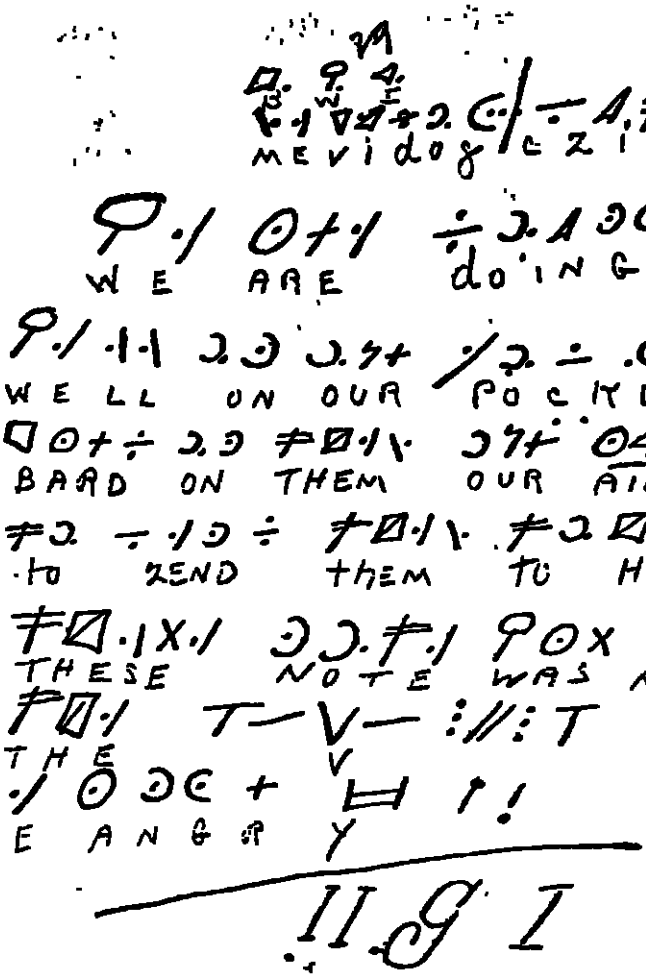
The American and British fleets maintained close liaison, for it was necessary for them to communicate with each other during operations. The Navy Department methods for secret communication had been submitted to British cryptographers who had pronounced them indecipherable. Because of this, I was especially anxious to demonstrate our skill.

The Navy system was a most elaborate one, and at first it looked as if I would need a great deal of luck. But after several clerks had compiled elaborate statistics which required thirteen hundred pages and six hundred and fifty thousand entries, the messages were readily solved. Thirteen hundred pages and six hundred and fifty thousand entries, merely to prove that the United States Navy was still controlled by amateur cryptographers! x

x yes, quite readily. By means of the code. It was merely a question of breaking down the encipherment which he also was told

7

could now read documents in nearly any language in thirty different shorthand systems; and our Secret-Ink Subsection was examining two thousand letters a week, and had developed over fifty important spy secret-ink letters.



Example of personal cipher turned over to MI-8 by censor. The reader may wish to try his hand at decipherment.

breaking enemy cipher and code messages, being represented in their office by a Liaison Officer who looks after the interests of the Navy."

For once, the Navy Department, ever jealous of its prestige, admitted failure.

Cryptography seems to do queer things to people. On several occasions I had been obliged to let persons resign on account of shattered nerves. I too felt the strain and though I said nothing about it for several weeks, in July I suddenly knew that I was close to a breakdown and asked to be relieved.

General Churchill was sympathetic, but refused to accept my resignation. Instead he asked that I draw up plans for a Cipher Bureau for the Expeditionary Forces to Siberia which was then being formed. Papers were drawn up ordering me to Siberia with a selected personnel, when a cable came from General Pershing, asking that I be sent to France.

Although I felt some pride in General Pershing's request for my services in France, I was too ill to take a great deal of interest in what was going on. I had nothing to do with the plans that were made for me, but it seems that after an exchange of several cables it was decided that I should go abroad on temporary duty to establish liaison between Allied and American Cipher Bureaus, and to obtain certain information from our Allies on the subject of codes and ciphers.

deal of tea and drank quantities of whisky and soda with various officers in the War Office. They were affable enough and invited me to their clubs. But I received no information.

I was at a distinct disadvantage for I did not dare communicate with Washington, since the British would decode every word I sent. Not having anticipated that I should find a British subject in possession of our secret codes, I had brought with me no special means of enciphering my cablegrams.

While playing a waiting game with the War Office I quietly investigated the situation in the Military Attaché's office, and finally took a chance on transmitting a secret cable to Washington by a method that I felt certain the British would be unable to decipher. This method, I am sure, is worth describing.

Several months previously the Mexican Government had changed their diplomatic ciphers, and the small group of cryptographers who specialized in MI-8 on Mexican telegrams was unable to break into the new system. Although they had been able to discover the type or method under study, and had followed the usual analysis necessary for the solution of such ciphers, the messages resisted successful attack.

Finally, when I saw that these cryptographers were merely going around in circles, I took a summary of their statistics and analyses home where I could work undisturbed. The analyses before me showed clearly that the messages were enciphered with a mixed alphabet,

one but MI-8 would be able to read my dispatch, despite the fact that the British must have by now photostated our codes.

I went on to describe the exact situation in the Military Attaché's office. I did this with some trepidation, for although General Churchill had told me to report anything I considered of interest, I still felt some misgivings as to his attitude toward my meddling in affairs foreign to my mission. I doubt if I would have had the courage to draft the cable, had it not been for the fact that Colonel Tolbert told me that the British had made repeated efforts to plant British agents in his office in Copenhagen.

Still I reasoned that as long as we granted British subjects access to our secret means of communication, even in one office, nothing but stupidity could prevent them from reading every message sent and received by our military attachés throughout the world. Sooner or later peace would be declared. There would be a squabble among the powers for the spoils of war. We would be helpless in our negotiations with our communications compromised.

In order to save my face, I suggested that Van Deman be ordered to make an investigation. After all, I was nothing more than a Captain.

I managed to escape the scandal my report produced, for Washington was horrified when it learned that our Military Attaché's office in London was full of British subjects. An investigation was made in every Military

Attaché's office in the world to the end that all foreigners were discharged and replaced with Americans trained in Washington.

But this did not assist me in my mission, though I did receive the thanks of General Churchill. Discouraged with the British refusal to all my requests, I cabled for permission to proceed to Paris. The matter was taken up with the State Department and I was instructed that they advised that I not try to press the British, but that I should gain their confidence by my silence and discretion, and should establish pleasant personal relations. They told me that the English were cautious about giving confidence until fully convinced of one's trustworthiness and discretion.

This was sound advice but scarcely helpful. Our relations seemed pleasant enough. At least they gave me enough whisky and food to keep me dizzy nearly every night. Perhaps I couldn't drink enough.

Finally Captain Brook-Hunt of the British War Office submitted to me for examination a combination substitution and transposition cipher. The British Army planned to adopt this cipher for the transmission of telegrams along the Western Front. Since such messages carried definite information, such as the disposition of troops and the hour of attack along different sectors, it was vital to the lives of the troops engaged that the messages be indecipherable, for German wireless stations intercepted all telegrams that passed through the air and passed them on to the German Cryptographic Bureau at

German headquarters for solution. Readers who are old enough will remember the laconic bulletins issued by the War Offices, such as:

> Our troops made surprise attack on —— sector, but were repulsed by superior forces.

Surprise indeed! More likely than not the enemy knew the hour of attack and strength of the forces engaged by the decipherment of wireless intercepts. How many men died for this reason no one knows.

If I could break this cipher the British were about to adopt, and demonstrate that it was suicide to use it for front-line military messages, all my trouble with the War Office would be over. Such an accomplishment would establish me on a professional basis that could not be denied. With these thoughts in mind I asked the Military Attaché for a room where I could study undisturbed. Here for several days I pored over the sample messages that Captain Brook-Hunt had given to me, striving for a solution. Suddenly the whole structure of the messages fell apart and I rushed with my solution to the War Office.

Its doors were now open to me; I could have anything I wanted. That evening I cabled Washington that I was on extremely good terms with the British War Office, due to my lucky decipherment of a double substitution and transposition cipher which they had recommended for use at the Front.

who cabled it to the Secretary of State, who in turn gave it to the President. Diplomatic procedure would require that such sensational information be transmitted by the Foreign Office to Ambassador Page, but Admiral Hall did as he pleased. It is no wonder then that he was feared by the Foreign Office.

Edward Bell was on extremely good terms with Admiral Hall, and the little success I had with the Admiralty was due almost entirely to his good offices. The Admiral had been informed by Colonel French of my mission in London and was prepared to give me as little information as possible. He made it clear that he absolutely would not deal officially with the United States Government. He insisted that everything be transacted on a personal basis, and though he remained firm in his refusal to give me any information about the German diplomatic codes used for wireless messages between Berlin and Madrid, he finally consented to give me, personally, several copies of a certain neutral government's diplomatic codes and a copy of a German Naval code in two volumes.

The naval codes he gave me under the most mysterious instructions. He promised to forward them to Washington but they absolutely were not to be turned over to the United States Government. Upon my return to Washington they would be handed to me personally. These codes, so I learned, had been photographed from the original by an English spy within the German Admiralty.

Is this a slam at Uncle Sam?

Spain Cypher See p 172

* Hall naturally would be reluctant to be placed in the position of having caused the British government to commit an unfriendly act against a neutral friendly government, Spain – if he should later be found out.

being deciphered and *the undeniable fact that the French Ambassador in Washington, since my first visit to Mordacq, had transmitted to our State Department information these messages contained.*

Two days before this Washington had asked me whether I thought it advisable to ask Colonel House to help, but when I cabled Warburton's interview with Clemenceau and Cartier, they readily saw how hopeless it would be to ask Colonel House to use his influence, for it was by now obvious to every one that France had no intention of permitting me to have even a peek into *La Chambre Noire.* Later, when the reader sees some of the diplomatic messages deciphered by our own Black Chamber, he will better appreciate the impossibility of my entering the doors of the diplomatic Code and Cipher Bureau of a foreign government. However, my negotiations were not wholly in vain, for my failure impressed upon American officials the absolute necessity for an American Black Chamber even in peace times, if the United States hoped to thwart the machinations of other governments.

That Washington was planning for the future I was assured by General Churchill's frequent letters, telling me that he was sure that, with my added knowledge of codes and ciphers obtained abroad, MI-8 would have no equal in the science of cryptography.

How so ? ? ?
He learned very little from the British, nothing at all from the French (after some admissions) so where did he get the "added knowledge" ?

share of glory in the part that the American Expeditionary Forces played in the winning of the war.

While at Chaumont I received orders from Washington to report to General Bliss, for "special duty at the Peace Conference." I cabled for further details and was instructed that my special duty was to organize code and cipher communications between the Peace Conference and the Military Intelligence Division at Washington. I was told that my status and allowances as Military Observer ceased when I reported to General Bliss, but that General Churchill, who would soon arrive in Paris, would provide an allowance from special funds.

I immediately left for Versailles and reported to General Bliss in person. He gave me a letter to Colonel Van Deman, who had been appointed Director of Intelligence at the Peace Conference, authorizing anything he considered necessary for establishing a Code Bureau in Paris. Van Deman in turn gave me the same authorization.

I immediately telegraphed General Headquarters for several particular officers and field clerks, demanded two rooms at 4 Place de la Concorde—the general offices of the Peace Conference—and within a short time was well organized. As it was difficult to anticipate my duties, I prepared for both a Communication and a Deciphering Bureau. Eventually we handled the messages of General Bliss, the Secretary of War and Military Intelligence; deciphered intercepted wireless messages of the Entente; and devised codes and ciphers

The M.A.'s code bureau handled the telegrams of all M.A.'s in Europe and M.I.D. coming to the Peace Conference as well as all of Sec Baker's messages when he was in Europe in 1919. We sent coded messages for Yardley & Mr Friedman Mr Friedman was in charge of this bureau +

began to write on the package, Goelet edged closer and watched him slowly spell out the address for which Van Deman had searched in vain!

If I was unprepared for the sort of espionage that engages women to attempt to influence the decisions of our Peace Commissioners (though one should never be amazed at what occurs either during a war, or at the division of the spoils), the reader may well appreciate the shock I received as I deciphered a telegram which reported an Entente plot to assassinate President Wilson either by administering a slow poison or by giving him the influenza in ice. Our informant, in whom we had the greatest confidence, begged the authorities for God's sake to warn the President.

I have no way of knowing whether this plot had any truth in fact, and if it had, whether it succeeded. But there are these undeniable facts: *President Wilson's first sign of illness occurred while he was in Paris, and he was soon to die a lingering death.*

After the President arrived and the excitement subsided, there was not a great deal to do. In fact, except for a few overworked clerks, and the Commissioners themselves, the whole Peace Conference now developed into one grand cocktail party. Every one with the Mission received stacks of tea and dinner invitations. And in typical American fashion it was the general custom to blackball any French host or hostess who failed to serve champagne. No wonder the French dislike our manners!

Messages trickled in now and then from Washington about the status of MI-8. We were all dreaming now of a powerful peace-time Cipher Bureau, and at last, late in March, when it was obvious that MI-8 was rapidly disintegrating, General Churchill ordered me to proceed to Rome to see what information I could pick up there about codes and ciphers, and then to hurry to Washington to draw up plans for a peace-time organization.

In Rome I learned very little. The Italians were reported to be clever at cryptography, but I soon was convinced that they were not to be classed with the French and British.

The day I sailed for the United States from Genoa, a cable was forwarded to me from The Hague, stating that the German diplomatic codes I had failed to obtain from the British and French could be purchased there from a German for six thousand dollars. The Military Attaché had cabled me after I left Paris requesting that I proceed to The Hague in order to have the benefit of my judgment. As this would delay my arrival in Washington, it was finally decided that I proceed at once and send some one else to examine the codes.

When finally reached Washington, then I the Berlin Madrid codes had been bought three during my absence. It would have taken three days of toil to mention this

C J M

gsemi	fnrui	rnths	ngtno	aeviu	lheru
nitte	agnhu	icggh	nruar	hddgr	tnuev
thort	aencl	oylms	maera	nnnke	efnre
rlgmf	hleln	hkonw	nslhl	snedu	ntatt
gltmh	ihmln	gukra	hciea	tgeut	tseal
nwttb	neent	iatri	eane		

"I was instructed to tell you that the State Department wanted a decipherment at the earliest possible moment," he said.

"Yes! How do you suppose we go about deciphering a jumble of letters like this?"

"I haven't the faintest idea," he admitted. "I'm only repeating my instructions."

"You fellows in Washington are always in a terrible rush to know the contents of a secret document. We'll do our best, but don't give them the idea that all we have to do is to go into a trance to reveal hidden secrets."

I showed him about the place, and got rid of him, for I was myself anxious to see what the messages said.

The Latvian Government, I later learned, had tried to decipher these messages and, after failing, had asked the American Consul at Riga to send them to the United States in order to see what the American cryptographers could do with them.

By the same analysis as that followed in the decipherment of the Waberski document we discovered that these ciphers were transposition, and written in German. I shall not go into the details of decipherment, for I am not sure that all readers will care to follow the method. However, for those who wish to try their hand at cryp-

I claim I have read Soviet messages enciphered by some in Russia. These common transposition ciphers were the only messages upon which I was in a position to work. I have no reason to suppose Soviet Virginia - but they were simply ciphered in transposition in German.

ALSKI arrived here with money on his way to America. German Government permits exchange of journalists from here. The "Frankfurter Zeitung" is taking advantage of the opportunity. Urgently needed capable talent.

These messages created a sensation among officials in Washington, for they were the first authentic documents that came into the government's possession dealing with international Soviet activities.

MI-8 also received original telegrams that Lenin sent to Bela Kun during the White revolution in Hungary. But these are too long to publish here.

There is one Soviet document, however, that is too revealing to pass over. I have always regretted that I was not employed by a government, such as the Soviet Government, that understood and practised espionage in the same ruthless and intelligent manner.

The following document to me is unique. Although espionage as practised by the Great Powers is no different from this, it is seldom that one comes into possession of a document that is so clear and frank in its instructions to secret agents.

Instructions to Agents for Hiring Spies in Legations.

Instructions

When enlisting the Chinese servants and employees in the legations of Japan, England and America you must pay the utmost attention to the following subjects:

will recognize it; and having recognized it, will know that I must also possess other Soviet documents of a more sensational character. For instance, instructions for the massacre of foreign nationals, etc.*

What? Not!

* *Soviet agents, please note.* Yes, I once had copies of these documents, but I don't care to have my throat cut and do not plan to publish them. In fact they have been destroyed. So be reasonable.

Weisband confirms my impression that the deciphered Soviet messages of this chapter were read by means of keys recovered from the outside

CJ

During my absence abroad several unsuccessful attempts had been made to decipher these messages, and although I always have assumed that any code or cipher can be solved, during the next five months I was to regret many times that I had been so sanguine in my promise to reach a solution within one year. Since my return to the United States I had worked over these messages at odd moments, but it was not until July that I began a serious and methodical analysis.

I shall not of course attempt to give all the details of the decipherment of the Japanese codes, for these would be of interest only to the cryptographer, but when I tell the reader that the Black Chamber sent to Washington, during the Washington Armament Conference held two years later, some five thousand deciphered Japanese messages which contained the secret instructions of the Japanese Delegates, I am sure he will wish to know how it was possible for the Black Chamber to take such an important part in the making of history. Let the reader therefore, for the moment at least, put aside his natural desire to listen to the whisperings of foreign diplomats as they lean closer together to reveal their secrets, and I shall try to tell a few of the tremendous discouragements that I had to overcome in the decipherment of this code, written in the most difficult of all languages, Japanese.

At the time I began this enormous task I knew nothing about the Japanese language. Before we begin to analyze these code telegrams, let us therefore see just how the Japanese language is formed.

Japanese differs in grammar and in vocabulary in its spoken and written forms, but here we have to deal with the written form only. From about the ninth century on, the classical language was expressed by the use of Chinese ideographs. These we have all seen on Chinese laundry slips, which we reluctantly accept as a receipt, wondering at the time if the Chinaman will be able to find our shirts and collars with the aid of these mystic signs. These ideographs, as of course the reader knows, are either pictorial or arbitrary symbols. We might call ⊙ a pictorial ideograph, which, though expressing no sound, might symbolize and be pronounced *sun* in our language, while in another the sound would be quite different, the idea *sun* however remaining the same. In our language we have such symbols as *1, 2, 3, ?, /,* etc. Though pronounced differently in other languages they mean the same thing.

The method adopted by the Japanese of expressing their language in Chinese ideographs proved very cumbersome, and in the course of time it became necessary to resort to abbreviations which finally took the form of *kana*. The *kana* which might be termed the Japanese alphabet or syllabary is expressed in seventy-three or more ideographs representing Japanese and Chinese sounds. Later, in order to express Japanese in Roman letters, these ideographs were Romanized.

The *kana* ideographs and the Romanized *kana* are both given on the following page.

seen how I proved that Japanese has its peculiar letter, syllable and word behaviors just as any other language has. Of course, without the assistance of a corps of typists this work would have been too enormous even to contemplate.

But what about the *code* telegrams!

Let the reader again examine the code message on page 251. Now that we have our Japanese language charts, how shall we go about deciphering these telegrams? How indeed! Since April, and this was now July, I had pored over these code messages at odd moments trying to discover what type of code or cipher the Japanese were using. I finally made up my mind that these messages were encoded with a two-letter code. If I should go into the labyrinth of analytical details showing why I finally arrived at this opinion, I am afraid that we should never get to the Washington Armament Conference, or at least not in this book.

Whether right or wrong I had to start at some point. I turned the telegrams over to my typists with instructions to divide the ten-letter code words into two-letter groups and copy them in the same manner as they had the Japanese language telegrams. They selected approximately 10,000 two-letter groups and carded each group on a separate card, showing the four-code-group-prefix and the four-code-group-suffix, just as they had done with the Japanese *kana*. These cards were sorted according to prefix and copied on sheets, then sorted according to suffix and again copied. I now had before

I always calls this a code. But Technically the Japanese messages were in cipher.

7.

...e not only 20,000 lines of Japanese language data, but also 20,000 lines of code data

The typing and indexing, the retyping and reindexing, in all 60,000 lines, as well as the compilation of reduced statistical charts, together with other miscellaneous data—all this work, done by a corps of typists, is the background of the scientific cryptographer. The reader will now better appreciate the difficulties I experienced as a clerk back in the State Department when I was deciphering our own diplomatic codes, for, since I was working alone, I was obliged to do all this drudgery.

As I had anticipated, the indexing of these code words both by their prefix and suffix, revealed in graphic form repetitions of varied lengths. My first step then was to go through all the messages and underline in different colored pencil all the repetitions of four or more letters. This work I did myself, in order to familiarize myself with the text. My typists also compiled tables of these repetitions, taking great pains to add the references (page and line) so that I could instantly refer to the exact position in which they occurred in the messages.

One of the most striking points that these charts revealed was that the code group *en* occurred only 11 times, and that its position was, in most cases, in the last ten-letter code group of the messages. Now one of the reasons that I had been uncertain of the possibility of a two-letter code was the fact that the last code word *always* contained 10 letters. As the reader can see, in

> have made so promising a beginning. . . . The agreements you found are very striking . . . your method is fine and your results are probably right . . . there isn't one chance in ten thousand that you haven't hit the meaning of the differential group. . . . How I wish I were with you. . . .

And how I wished he were with me! These letters kept up my courage though I still worked mostly in circles. Finally I made several trips down to the Japanese Consulate in New York to look the ground over and make up my mind as to the possibilities of getting into the Consulate's safe for a peep at his code book. If I could only be *sure* that I was on the right track. But this would be too dangerous to try in New York. Why not try it in some other country, where, if caught, we would not be suspected! I must see Blank about this, and get his opinion. One thing was certain. Washington had given me a job to do—the decipherment of the Japanese codes. If I couldn't do it one way, I'd have to do it in another.

I took up again the history of the decipherment of the Rosetta Stone, which led to the reading of the Egyptian hieroglyphics on the ancient monuments of Egypt. The problem here was not unlike my own, but the method of attack used by scholars was so primitive and elementary that I did not get much encouragement. Their idea as to what constitutes evidence in the correct identification of any given ideograph was so vague that for centuries they had published solutions that later proved

* Poor Champollion! Another idea shattered!! I never knew that the Cretan and Mayan inscriptions are still unread - but to mention the Egyptian is one.

C.J.M.

San Francisco on November first, is urgently requested.'

"The ideal repetition is one where the difference is between similar beginnings and endings. Can't you see how simple it would be for me to find these names in the code message? I'm sure a telegram along these lines would enable me to break into the code. Do you think a bona fide case can be found?"

This idea intrigued Churchill for he was born for espionage. Later, however, he told me that they had been unable to find a real case that would fit. It might take some time; we must make no error that would lead the Japanese to believe that they were being duped.

General Churchill, in my opinion, was the greatest executive produced by the General Staff during the war. He knew what he wanted; but when he told his subordinates to do a job he was ready at all times to lend them any aid at his command.

The reader must not get the impression that I had given up all hope of deciphering the Japanese codes without aid. I had not. Nor were any of my plans fulfilled, for as we shall soon see I had no need of them. But I was preparing myself for failure. I *might* need assistance.

By now I had worked so long with these code telegrams that every telegram, every line, even every code word was indelibly printed in my brain. I could lie awake in bed and in the darkness make my investigations—trial and error, trial and error, over and over again.

Finally one night I wakened at midnight, for I had retired early, and out of the darkness came the conviction that a certain series of two-letter code words absolutely *must* equal *Airurando* (Ireland). Then other words danced before me in rapid succession: *dokuritsu* (independence), *Doitsu* (Germany), *owari* (stop). At last the great discovery! My heart stood still, and I dared not move. Was I dreaming? Was I awake? Was I losing my mind? A solution? At last—and after all these months!

I slipped out of bed and in my eagerness, for I knew I was awake now, I almost fell down the stairs. With trembling fingers I spun the dial and opened the safe. I grabbed my file of papers and rapidly began to make notes.

WI	UB	PO	MO	IL	RE	(code)
a	i	ru	ra	n	do	(Ireland)

The word *independence* should follow Ireland, for Ireland was then fighting for her freedom.

WI	UB	PO	MO	IL	RE	RE	OS	OK	BO	(code)
a	i	ru	ra	n	do	do	ku	ri	tsu	(Ireland independence)

The only proof here of a correct solution is the repetition *re re.*

do do

Now, one of the frequent repetitions in the code mes-

Even this small chart convinces me that I am on the right track. For an hour I filled in these and other identifications until they had all been proved to my satisfaction.

Of course, I have identified only part of the *kana*—that is, the alphabet. Most of the code is devoted to complete words, but these too will be easy enough once all the *kana* are properly filled in.

The impossible had been accomplished! I felt a terrible mental let-down. I was very tired.

I finally placed my papers in the safe, locked it and leaned back in my chair, checking up my blunders, and at the same time wondering what this would mean to the United States Government. What secrets did these messages hold? Churchill would want to know of my accomplishment. Should I telephone him at this hour? No, I would wait and dictate a letter.

I was unbelievably tired, and wearily climbed the stairs. My wife was awake.

"What's the matter?" she asked.

"I've done it," I replied.

"I knew you would."

"Yes, I suppose so."

"You look dead."

"I am. Get on your rags. Let's go get drunk. We haven't been out of this prison in months."

CHAPTER XV

A Missionary Cryptographer

The next morning, or rather the same, I dictated a long letter to Churchill, outlining in detail what the reader already knows. I did this for two reasons. General Churchill was always interested in the details of my bureau, and besides I had no small measure of pride in having solved the Japanese codes and wished a record in the War Department files. Churchill had been especially anxious to have a few Japanese telegrams in his possession when we went to Congress for the Military Intelligence appropriation. These I promised him in ample time.

I shouldn't wonder but that this letter sounded a bit youthful. Even yet, the memory of those exciting days thrills me.

When General Churchill received my letter he did not wait to write, but telephoned his congratulations, and told me that those in authority would hear of the new success of my bureau. Judging by the tenor of his voice and words, he was more excited than we were.

After dictating the letter I instructed my secretary to tell my cleverest cryptographer, Charles Mundy (I shall call him this for want of a better name, for he now holds a position that might be jeopardized were his past history known) that I wanted to see him.

When he came in I knew by the expression of his small eyes that looked at me through thick lenses that he already knew of the breaking of the Japanese diplomatic codes. In fact I had sensed an air of excitement throughout the office. Every one had anxiously been awaiting the breaking of this code and no doubt had guessed of my success by my manner.

When I showed him a part of my analysis, he smiled his pleasure.

"How are the Russian codes progressing?" I asked.

"We're still working on the manuscript," he said. "The code doesn't look very difficult."

"I may be wrong," I told him. "But I have the feeling that these Japanese codes will make history. I need a Japanese scholar to read them. I have already canvassed the United States for one without success. I'll find one somehow or other. But you know how translators are. It's one chance in a thousand that he will ever develop cipher brains. In my opinion it may be easier for a cryptographer to learn Japanese than for a Japanese student to learn cryptography. I'm going to give some one here an opportunity to study Japanese. I'll give him a year, or two years if necessary, to learn the language. I'll get a fund from Washington for this purpose. Now the person I select for this job need no longer have any strings attached to him. He need report to me but once a month to convince me of his progress."

I could see his little eyes burn with desire. I have

All this looked rather hopeless, but I kept at it and finally discovered a retired missionary of some sixty years of age who I was told was one of America's best Japanese scholars. I paid his expenses to New York and after sizing the man up put all my cards on the table and tried to intrigue his mind with the mystery of codes and ciphers.

He demurred at first and I thought he was afraid to attach himself to an under-cover organization that was prying into the affairs of foreign governments. But I suddenly learned that he was just a good horse-trader and was holding out for more money than I had at first offered. We finally came to an agreement, and he immediately moved his family to New York.

I now regrouped my cryptographers, and selected the most rapid and accurate clerks (accuracy on the part of clerks will often save months of futile investigations in the decipherment of a code) for the Japanese Department.

I selected the largest room available, placed our long whiskered missionary and thick-spectacled cryptographer at adjacent desks, and changed the locks and keys.

The Black Chamber, housing as it did so many persons of queer sorts, seemed almost like a menagerie, but I never failed to laugh to myself every time I went into the Japanese Department and saw this benevolent-faced, whiskered, old missionary as he puzzled over Japanese words, *kana* and code groups. He was instantly the

favorite of the whole office. He was so gentle and so very frightened at the mystery and secrecy. I had never expected to live to see a missionary engaged in espionage. I don't think he ever quite realized what he was doing.

However he was a good translator and in February, 1920. I sent to Washington the first translations of Japanese decipherments. When General Churchill received these messages he took them at once to the Chief of Staff and to officials of the State Department, and told me personally that he considered their decipherment the most remarkable accomplishment in the history of code and cipher work in the United States. He told me to extend to my assistants his personal regards and official congratulations.

I do not make these statements to magnify the accomplishments of the American Black Chamber. History alone will decide those things. I cite them as a tribute to the fine general officer under whom we served. He knew and understood that men and women to succeed at cryptography must be inspired both by a passion for the science and by sympathetic leadership. Certainly, no human being would burn up his heart and brain without the latter.

On June 12, 1920, our missionary made the following translation of a Japanese code message from the Japanese Foreign Office in Tokio to the Japanese Ambassadors to Washington and London. The italics are mine.

A cabinet council has decided on a partial evacuation of the Japanese army from districts

did not disturb the steady flow of Japanese translations, for in six months Mundy had accomplished the unheard-of thing of mastering the reading of the Japanese language. He had done well in six months what it takes army officers in Japan three years to do poorly. He had the greatest capacity for languages of any one I have ever known. Even back in 1917 when he came to MI-8, he had this facility, but cryptography had sharpened his intellect. He had no originality of mind as a cryptographer, however, and needed assistance when a new cipher problem confronted him; but as a sponge for absorbing languages he had no equal.

The code I had broken, I designated *Ja* for reference purposes—the *J* standing for Japanese, the *a* an arbitrary designation. The next code we solved would be termed *Jb*, the next *Jc*, etc.

Now the Japanese had no intention of permitting us to rest on our laurels, for from 1919 until the spring of 1920 they introduced eleven different codes.

We learned that they had employed a Polish cipher expert to revise their code and cipher systems. It took all our skill to break the new codes that this man produced, but by now we had developed a technique for the solution of Japanese codes that could read anything. Theoretically the Japanese codes were now more scientifically constructed; practically they were easier to solve than the first code, although some of them contained as many as twenty-five thousand *kana*, syllables and words.

The Polish cryptographer seemed to specialize on

army codes, for the Japanese Military Attaché's codes suddenly became more difficult than those of any other branch of the Japanese Government. This new system was elaborate and required ten different codes. The Japanese would first encode a few words of their message in one code, then by the use of an "indicator" jump to another code and encode a few words, then to still another code, until all ten had been used in the encoding of a single message.

An ancient scheme, I.

Messages encoded in this manner produced a most puzzling problem, but after several months of careful analysis, I discovered the fact that the messages were encoded in ten different systems. Having made this discovery, I quickly identified all the "indicators." From this point on it was not difficult to arrive at a solution.

The Japanese Government must have received information of our successes, because they not only employed a Polish cryptographer to revise their codes, but also began a series of well-planned and secret inquiries at the Cable Companies as to whether it was possible for the United States to obtain copies of their code telegrams after they had been filed for dispatch.

Information of this type always reached me, for as Chief of the Black Chamber, I was not only executive and cryptographer, but was obliged to maintain my own espionage system as well.

Early in 1921 there were rumblings of an Armament Conference for the limitation or reduction of arms. No doubt anticipating this, the Japanese again launched a

structed new codes, but had adopted a new principle in their construction. We all dropped everything we were doing and concentrated on its solution.

Our difficulty in breaking this code was due to its scientific construction. Although the code messages were on their face the same as others (they were all in groups of ten letters) we could not discover the real length of the code words. Heretofore the code words had been of two-letter and four-letter length. We divided the ten-letter groups of these messages in all their various combinations without success.

Finally we discovered that three-letter code words were interspersed throughout the messages. The code words in all other codes had been divisible by two. This new element of three so confused us that we could not even set about solving the code.

However, once we had discovered the three-letter elements, we quickly solved the messages, and within forty days after their receipt were reading current telegrams almost as rapidly as the Japanese themselves. Momentarily, at least, all those in the Black Chamber gave a sigh of relief. This new code we designated as *Jp*, the sixteenth code we had broken since my original solution.

It is of interest to note that Japan and the Soviet Union are the only nations which attempt to take advantage of the construction of code words of uneven lengths. It is a powerful weapon with which to confuse the cryptographer, and I have repeatedly urged this upon our own government, with not a great deal of success, I am sorry to say.

Is this principle so good, how is it that you were able to break three ciphers [illegible] ?
F.

I mentioned this to me Jones + sent a memo. He never urged and the principle is open to question.

> that it would be a good plan to move at frequent intervals so that people in the neighborhood would not get wise to our activities. I explained to him that I felt sure that no one in our neighborhood suspected the nature of our work, especially in view of the fact that there are almost a half-dozen other offices in the same block in private homes conducted in the same manner as this office.
> . . . He asked whether I would experience any difficulty in cashing checks during your absence. I told him there would be no trouble at all.

In June, 1922, I returned from Arizona in excellent health, but found my most valuable assistant in a frightful condition. He had been working sixteen hours a day for so long that he talked incoherently, with a strange light in his eyes. I kept close watch over him for a week or more, for cryptography steals into the blood stream and does curious things to people.

I myself had already had trouble in this respect. Then there were the cases of two girls who were near a nervous breakdown and asked that I let them resign. One dreamed constantly that a bulldog was loose in her room. For hours she chased it under and over the bed, behind the chair, under the dresser, and finally when she caught it, she found written on its side the word *code*. The other girl dreamed each night of walking along a lonely beach, weighed down by an enormous sackful of pebbles. She struggled along for miles with this heavy burden on her back, searching for pebbles that matched those in the

* Finney laughed when I told him about y's description of him. "That dunce" he said.

7.

bag. When she found one that exactly matched she could take the duplicate from the bag and cast it into the sea. This was her only method of lightening the burden that weighed so heavily upon her shoulders.

It was therefore with some concern that I observed my assistant. Finally he came to me of his own accord and told me he was becoming afraid of himself. I told him to go away for a couple of months and try to forget codes and ciphers. Upon his return he said that he wished to give up cryptography and try something else. We finally found a good position for him in another field. I suspect that he does not now regret his step.

Not long after I returned from Arizona I was ordered to Washington for a conference with Colonel Heintzelman. He had just been promoted to a Brigadier-General and would shortly be relieved, because the Director of Military Intelligence is not a general officer. When a Director is promoted to a General he is relieved by a Colonel. Colonel Nolan had been relieved because he too had been promoted to a Brigadier-General.

"Yardley," General Heintzelman began, "I have talked about you to the Chief of Staff, General Pershing, and the Secretary of War. You are to receive the Distinguished Service Medal."

I could only connect this in my own mind with the part played by the Black Chamber during the Armament Conference. It was a surprise to me, for no matter

what may be said about my organization, it can never be charged that any of us ever played politics, either for promotions or for honors. In fact, we were happy to remain unknown, hidden behind curtains, as long as our work was useful to the United States Government.

The patriot speaks

I thanked him for his interest in my behalf. It is not too much to say that in my opinion the Black Chamber had a great deal to do with the promotions of both Nolan and Heintzelman to general officers, for it was well known that the Chief of Staff and the Secretary of War were vitally interested in the translations from the Black Chamber, and both officers were in a measure responsible for our successes.

"In awarding you the D. S. M.," the General began again, "we find it difficult to draft a citation that will describe your distinguished services, and at the same time keep the nature of your activities secret, for of course all citations are published. Have you any suggestions?"

"I naturally have never given the matter any thought."

"Well, we'll draft something, so that your successes will not be revealed. The only regret is that the real reason for conferring the D. S. M. can not be given."

We were of course well aware that if our activities were discovered there would be no protest from foreign governments, for we knew that all the Great Powers maintained Cipher Bureaus for the solution of diplomatic telegrams. This was a sort of gentlemen's agreement. Just as in warfare armies do not attempt to bomb

each other's headquarters, so also in diplomacy statesmen do not protest against the solution of each other's messages. However, if foreign governments learned that we were *successful* they would immediately change their codes, and we would be obliged after years of struggle to begin all over again. For this reason the War Department would need to draft the wording of my citation in a manner that would not lead foreign governments to suspect the skill of the Black Chamber.

After discussing with him some of the new problems of my office, I returned to New York, and within a few weeks was again ordered to Washington.

I was to appear before Secretary of War Weeks at two P.M. to receive the D. S. M. On the way to his office I asked General Heintzelman if Secretary Weeks really knew why I was being awarded the D. S. M. He assured me that the Secretary was one of the most ardent supporters of the Black Chamber.

I felt rather silly standing before the Secretary of War, as he read my citation that seemed to have very little to do with the breaking of codes of foreign governments, but I was relieved when he pinned the medal on my lapel, for with a twinkle in his eye he winked at me. The wink pleased me immensely.

The vague phraseology of my citation and the note from my secretary to me while I was in Arizona gave some idea of the fear on the part of Washington that our activities would be discovered. We were not only asked to move our office from time to time, but many other so-

called precautions were taken to keep our identity secret. As Chief of MI-8 my name was known in every corner of the earth, for I had to sign all letters dealing with codes and ciphers. Aside from this I was well known to English, French and Italian cryptographers during the war, as the Chief of MI-8. If a foreign government wished to find out whether the United States still maintained a Cipher Bureau, the first thing their secret agents would do would be to locate me, and of course my address was on file with the Adjutant-General of the Army.

It was really useless to attempt to hide my whereabouts, but as the attempt seemed to please Washington, I made no protests. My name was not permitted in the telephone book, mail addressed to me was through a cover-address, etc.

Washington was especially concerned that I keep away from congressional investigations. During the investigation of Secretary of Interior Fall, my correspondent in Washington telephoned me for God's sake to lie low for if I was called upon to decipher the Fall messages we would be ruined.

During the Senate's investigations of the authenticity of the Mexican cipher telegrams published in the Hearst papers that produced such a scandal, I was in Washington and had a good laugh with one of my minor correspondents. Why, I do not know, unless the Navy still advertised itself as it did during the war, but in any case the Senate appealed to the Navy for its opinion as to the genuineness of these Mexican cipher

messages. We in New York had already analyzed the telegrams and could, at a moment's notice, have given an incontestable opinion as to their authenticity, for we had deciphered thousands of Mexican code and cipher diplomatic and consular messages. The Navy, however, came around to my correspondent for his opinion, but was told that the War Department had no Cipher Bureau, and did not know a thing about the subject! The situation was especially ludicrous, for the Naval officer knew that my correspondent was lying, but there was nothing he could do about it.

It certainly amused us both to see so-called Naval experts give their opinion about the Hearst documents. How did they become expert? The last I had seen of a Navy Cryptographic Bureau was when they closed up their office and placed a liaison officer in MI-8 because of their failure to decipher a single message.

This morning, and I am now writing of February, 1931, I was informed by a friend just back from Washington that the committee investigating Soviet activities had one thousand Soviet code messages which had been turned over to "Government experts" to decipher, but they couldn't be solved by these experts. This was very enlightening, for it had been my impression that the Black Chamber had a monopoly on experienced cryptographers, and the Black Chamber had long ago been closed by the government.

In spite of all the precautions to maintain secrecy regarding our activities, we were once nearly given away

through our kindness in giving a helping hand to Bruce Bielaski while he was conducting under-cover investigations of rum-runners off the Atlantic coast.

He was intercepting by wireless a great number of cipher messages to "mother" ships along the coast, which lay beyond the twelve-mile limit, waiting for opportune moments to discharge their cargoes of fine wines and liquors to rum-runners. Bielaski, with whom I was closely associated during the war when I was Chief of MI-8 and he Chief of Investigations of the Department of Justice, knew of my present activities and asked if I minded if one of my assistants deciphered these messages. I said no, so long as it did not interfere with our work. He gave my cryptographer two hundred dollars per month for this, and often when the latter needed help I assisted in the decipherment of these bootleg cipher messages.

Finally Bielaski decided he could win a case for conspiracy by presenting as evidence several messages we had deciphered that showed conclusively the nature of the activity of a mother ship off the coast of Atlantic City. He sent his coast guard out to haul in the vessel, which, as I remember, contained about a half-million-dollar cargo.

He was all ready for the trial, and called me up to tell me that he would need expert testimony on the decipherment of the messages. I nearly dropped dead when he made this request, and told him emphatically that I could permit no one connected with my office

all stuff in a great pile to me x,

2

1 Weisberg told me he mentioned this to Bielaski, and Biel said "I think I met y. twice." c f m

2 Weisberg says y never helped him c f m

to give such testimony. To do so would disclose our secret activities. The newspapers would be full of the activities of the Black Chamber. Foreign governments would change all their codes and years of labor would be erased. Needless to say, this ended our connection with bootleg cipher messages.

Despite all our precautions, however, some one, or some government suddenly became interested in our secret activities and went about learning what they could in the manner I knew they would follow, for I had not been connected with espionage all these years for nothing.

For several weeks now I had known I was under observation. Whenever I ventured on the street, which was no more than once or twice a day, I sensed this shadow behind me. But to make certain I employed a private investigator. After this when I appeared my unwelcome friend sprang from nowhere and strolled along well behind me, and behind him too ambled my investigator. We were of course now certain that I was being watched. For what purpose? My man endeavored to discover this by following my shadow after I returned to the office, but he was too clever. He also sensed that he was covered and at the proper moment eluded pursuit.

Nearly every day late in the afternoon I dropped in at a speakeasy in the West Forties for a cocktail or two before dinner. As the bar was always jammed, more often than not one engaged a stranger in conversa-

cab. From the mail-box in the vestibule I learned the location of her apartment and helped her as best I could up the first flight of stairs. I fumbled for her key, and in another moment we were in a beautifully furnished two-room apartment. Once inside she lay down on the couch and instantly fell into a deep labored sleep.

I quickly searched the apartment and discovered what I was looking for in the handkerchief drawer of her dressing-table. It was a typewritten note that must have been delivered by messenger the day before. It read:

> Have tried to reach you all day by telephone. See mutual friend at first opportunity. Important you get us information at once.

The message was unsigned, unaddressed.

I bent over to see if she was still asleep, gently took off her slippers, covered her with a blanket and quietly let myself out.

The next day she disappeared and left no trace of her whereabouts. Who employed her, just what information her employers wanted I have no way of knowing. However, whatever they wanted they must have wanted badly, for the next night the office door was forced, cabinets rifled, and papers scattered all over the place. I took it for granted that they had photographed the important documents which they required.

Quoting Treishoff: "It's a damned lie! All that was taken were a couple of bottles of booze. It was my booze and I think he took it "himself"!
Two pmm C.J.M.
F.

CHAPTER XVIII

The Secretary Sees the President

The Black Chamber did not deal solely with the diplomatic codes of Japan. We solved over forty-five thousand cryptograms from 1917 to 1929, and at one time or another, we broke the codes of Argentine, Brazil, Chile, China, Costa Rica,* Cuba, England, France, Germany, Japan, Liberia, Mexico, Nicaragua, Panama, Peru, Russia, San Salvador, Santo Domingo, Soviet Union* and Spain.*

We also made preliminary analyses of the codes of many other governments. This we did because we never knew at what moment a crisis would arise which would require quick solution of a particular government's diplomatic telegrams. Our personnel was limited and we could not hope to read the telegrams of all nations. But we drew up plans for an offensive, in the form of code analyses, even though we anticipated no crisis. We never knew at what moment to expect a telephone call or an urgent letter demanding a prompt solution of messages which we had never dreamed would interest the Department of State.

Among these preliminary studies were the code telegrams of the Vatican. But our analysis of the Vatican code nearly got me into trouble, and was abandoned under rather rare circumstances.

Quite an impressive list - but he is discreetly silent as to which were given him already solved, or stolen! Current belong.

+ Costa Rica code was furnished by ex-officials of Government.

* Soviet Union - No code message of Russian Foreign Office was ever solved by M.I.8

* Copy of Spanish code furnished by British.

A new Director—I shall not give his name—had been appointed, and I was ordered to Washington to outline the history of the activities and accomplishments of the Black Chamber, and to give him my plans for the future.

The new Director, his executive officer and I were lunching at the Army and Navy Club, when the Director asked:

"Yardley, what code do you plan to solve next?"

"I don't know, but the Vatican code telegrams rather intrigue me. Our preliminary analysis shows that they can be read. . . ."

I noticed with amazement that the Director's face went very white. At the same moment the executive officer gave me a vicious kick under the table. It scarcely needed the injury to my shins to make me realize that the Director was a Catholic, but it gave me an opportunity to cover up my confusion.

My voice was a bit tremulous, but I began again:

"Our preliminary analysis shows that they can be read, but I personally feel that it is unethical for us to inquire into the Vatican secrets. I hope you concur with my view."

The word unethical sounded a bit strange in its association with the activities of the Black Chamber, but in this case it was effective, for the blood slowly returned to the Director's face.

"You are quite right, Yardley," he said. "I wouldn't bother with the Vatican code telegrams. I'm glad to

* I am quite sure this was Gen Nolan & told me of this incident. F.

see that you recognize that there are certain limits that we can not exceed in the espionage necessary for the successful operation of your bureau."

Though the Black Chamber made preliminary analyses of many codes that it was never called on to solve, it was on the other hand required to solve all the codes of certain countries even though they gave our government no information of any value, since at the moment there were no important questions being discussed. This was done of course with only a few governments, and was necessary, for only by continuity is it possible to keep up with the changes that the codes of all governments gradually undergo. In fact the success of a Cipher Bureau in breaking new codes is often dependent on continuity. If we read a particular government's messages over a period of years, when the code is suddenly changed, it is less difficult to break the new one, because, having observed this government make slight improvements from year to year, we are familiar with the line of reasoning of the expert who is compiling the codes. Each government has pet theories about codes and ciphers, and as long as the same man compiles them, we assume, when confronted with a new code or cipher, that we are dealing with his particular type.

Let us take the Mexican Government as an example. In 1917 they enciphered their messages in simple substitution ciphers, of the *Gold Bug* type. Shortly afterward their cryptographer evidently thought these unsafe, for he adopted multiple substitution ciphers.

code words and the plain text words for which they stood was thoroughly mixed. In Chapter VIII there is quoted a page from a German trench code that shows how a thoroughly disarranged code is constructed. The illustration facing page 313 also shows a thoroughly mixed code in use by the British Foreign Office during the Washington Armament Conference. The latter is what we call a "skeleton code." At this stage about thirty-five hundred words had been identified, The British Government seemed to prefer small codes of only ten thousand words and phrases.

We have now watched the slow development of Mexican means for the encipherment of their diplomatic messages. They had started with simple single substitution ciphers and had gradually reached the stage of the disarranged code. It was by continuity that we were able to solve them so readily. Over a period of years we learned not only their pet theories on so-called indecipherable codes and ciphers, which assisted us immeasurably, but also became familiar with their stock expressions or phraseology. No cryptographer can hope for rapid solutions unless he has this background to assist him. Aside from this, if no attempt is made to decipher messages during quiet periods when there seems to be no likelihood of important issues arising, the true aims and intentions of a government can not possibly be ascertained. One never knows at what moment another government will start a movement prejudicial to our interests.

the analysis of the solution of this message, but he was now frowning at me again.

"Now, Yardley, I have a most unusual story to tell you. Yesterday morning, a few moments after this message arrived, the Secretary took it over to show it to the President. The President glanced at your decipherment, then, handing it back to the Secretary, said, 'Yes, the Attorney-General showed that to me a few moments ago. He just left.'"

He paused and eyed me furtively. He waited for some comment. I made none, for I knew now what was coming.

At last he said very slowly and deliberately:

"Now, tell me if you can, *how did the Attorney-General get a copy of this message?*" He said this as if he were exploding a bomb.

Some one, perhaps the Secretary, had tramped on his toes, for he was very angry by now.

"That's easily explained," I answered, "though you may not yourself appreciate the explanation. You see, during the war the department that I organized was the central Code and Cipher and Secret-Ink Bureau for the War, Navy, State and Justice Departments. At that time the Department of Justice had on their pay-roll an agent who had dabbled in ciphers. The Department of Justice contributed his services when we asked for him. He became expert. So after the war, when we moved to New York and organized as a civilian bureau on secret pay-roll, though we severed

entire message before me, I could see at a glance many other repetitions of several five-figure code words. The fourth group NCOTRAL was probably cipher and spelled a place or a name not in the code book.

I immediately put through a call to Washington:

"Just got your note. The message is in code and I suppose we can read it, but why all the mystery?"

"I don't know a thing, Yardley."

"Well, you know where you got it, don't you? You can give us a clue as to the language it is in."

"I haven't the least idea of the language. S. D. gave the message to me under the most secretive conditions, but told me to impress on you the importance of a quick solution. Be sure to let me know what progress you make, no matter how slight."

"All right," I answered, and hung up.

By S. D. he meant the State Department. This was just another one of those problems of opening a safe without the combination. If the Department of State was interested it must be a diplomatic message. The only important controversy at the time was the Tacna-Arica case in which the United States was acting as umpire. This disputed territory had nearly led to war between Chile and Peru, and the United States was attempting to get them to settle their dispute without resorting to arms. The message, then, so I reasoned, must be either Peruvian or Chilean. I had been surprised that the State Department had not asked us to furnish decipherments of both countries' telegrams during this

This is pure Sherlock Holmes stuff. Cut

"The memo that accompanied this telegram stated that the conference was between Mr Ellis, Mr Stasher, and the Secy of State!" — From an unofficial report by H O Y

W++

controversy, but I was long past attempting to anticipate the Department's vagaries.

We maintained a clipping bureau of our own, and indexed all articles in the *New York Times* and a few other papers regarding any international controversy, so that we could review what had been mentioned in the newspapers without any research. A perusal of the clippings regarding this controversy showed that one of the questions was the disposition of the City of Arica. We reasoned therefore that the phrase *ciudad de Arica* should occur at least once.

As we had deciphered the Chilean and Peruvian codes during the war and were familiar with their construction, we assumed that this message was encoded in an alphabetical system; that is, one in which the words retain their alphabetical sequence and the code words their numerical order. The codes we had solved during the war were, however, five-letter code words instead of five figures.

Our analysis told us that the code word occurring most frequently was 36166, which we assumed as *de* and inserted this meaning throughout the message. As *ciudad de Arica* should occur, we began to look for a word that followed *de* that would fit for Arica—the code word for Arica should begin with 00 . . . since Arica would occur early in the code book itself. After several hours' search we gave up 36166 as meaning *de* and filled it in as *en*.

As *en* brought no results, we temporarily abandoned the solution of 36166.

We now selected 27359, another high-frequency group, to mean *de*, and again began our search for *ciudad de Arica*, which we finally tentatively identified.

In this manner after the first day we filled in only such words as *de, en, el, que, y, a,* etc., and were rather doubtful of a quick solution, for the problem now, of course, became a great deal more complex, since about 250 out of a total of 390 code words in the message occurred only once.

The next morning, however, we fortunately identified the words *Secretary of State,* and such phrases, translated, as *the Secretary of State said,* etc.

When we made this discovery, I picked up the telephone and told my correspondent in Washington to inform the Department of State that the message was from either the Chilean or Peruvian Ambassador, and that the message reported a conversation with the Secretary of State about the Tacna-Arica controversy. Also that if they wanted a quick solution he should send us a résumé of this conversation. It was the Secretary's custom to dictate résumés of conversations immediately after a conference with a representative of another government. These were often sent to us and were invaluable in the solution of new codes.

The résumé arrived the next morning, and within a few days we had deciphered the entire message, which turned out to be from the Peruvian Ambassador to his home government in Lima. A part of the translation is quoted:

and sat smoking while he made up his mind to tell me, in his secretive way, what was on his mind.

"Yardley," he finally began, "I have wondered for a long time whether our own codes are safe." Another long pause. "It may be possible for me to get copies of some of our coded messages so that your office can see

Plett's Cipher Machine, a modification of the famous Wheatstone cryptograph. The inner disk contains twenty-six spaces, the outer twenty-seven. The machine is so constructed that with each revolution of the inner disk it changes its position one space. The alphabet may be changed at will.

between these two machines tapped the wire, he would have intercepted nothing but a jumble of letters. In cases where instantaneous transmission and decipherment was not practicable the operator first enciphered the message by striking the letters on the keyboard and turned the resultant cipher message over to the cable company. When the cipher telegram reached the addressee, he adjusted his machine, struck the cipher letters on the keyboard and the original telegram appeared before him.

"This machine filled every requirement of simplicity of operation, speed and accuracy. *But it was not indecipherable.*

"There have been many cipher machines invented. One in particular was so ingeniously contrived that there is no repetition for four billion letters. Or at least that is what the inventor thinks; for you see, there again you have the amateur attempting to escape repetitions by a series of disks, tapes, electric impulses, etc. These machines fill your needs in simplicity, speed and accuracy, and if you adopted them, you could discharge ninety per cent. of your code clerks, but all these machines are invented by people who haven't as yet grasped the fact that there is no method of avoiding repetitions. To the eye these machines, as well as innumerable other ciphers and types of codes, do escape repetitions, but mathematical formula will reveal them."

"If this is true, and I am ready to admit anything you tell me, how is it possible to construct any practicable

means of secret communication that is indecipherable?"

"There is no way as long as the attempt is made to avoid repetitions. *The only indecipherable cipher is one in which there are no repetitions to conceal.* Therefore no need to attempt to escape them."

"There is such a method?"

"Yes."

"It can be made practicable by some such machine as the American Telephone and Telegraph machine that you described?"

"Yes, though for small offices the machine need be no larger than a typewriter. If and when the Government of the United States adopts such a system, and not until then, may they have absolute certainty that their messages will never be read by a cryptographer. Sooner or later all governments, all wireless companies, will adopt some such system. And when they do, cryptography, as a profession, will die.

"I hope you now understand why I prefer not to write a memorandum for your Code Bureau. Even with all my experience, I wouldn't know how to go about compiling an indecipherable code or cipher along the conventional lines. There is only one indecipherable means of communication, and its adoption would require the Department to revolutionize its antiquated methods. I'm afraid there is nothing that either you or I can do about it.

"What I have said might have seemed disrespectful to the Department, but I'm sure you appreciate my

There are only a few inaccuracies in this chapter.

CHAPTER XX

The Black Chamber Is Destroyed

In the latter part of 1928 the newspapers were full of the Anglo-American naval race. The British in 1927 had walked out on Hugh Gibson at the conference at Geneva, but when President Coolidge recommended the fifteen-cruiser bill which would bring us to parity with England, the British statesmen suddenly changed their tone and decided after all that perhaps it might be well to enter an agreement with America on limitation of cruisers.

Everything pointed definitely to a conference in 1929. We therefore set about to prepare ourselves to play an important part, as we had done in 1921-22 at the Washington Armament Conference.

This was not a simple matter. The Black Chamber had entered a critical period of its history. It became increasingly difficult to obtain copies of the code telegrams of foreign governments, and we were forced to adopt rather subtle methods. Our superiors did not always assist us in the measures necessary to maintain the flow of telegrams into the Black Chamber.

I envied the foreign cryptographer, for he had no such problem to worry over. All coded messages were turned over to him as a matter of routine, as they were to us during the war. In fact England, in her license con-

ants, I studied it a long while in silence before I had the courage to open it.

Finally I ripped it open. The first words spelled our doom. The letter was almost illegible, full of exclamations, and what-not. I put in a telephone call for more details.

My informant told me that the messages I had sent down were given to the Secretary, who wished to know how they were obtained. When informed of the Black Chamber he had totally disapproved of our activities and ordered that all State Department funds be withdrawn from our support, and that the State Department have absolutely nothing to do with our organization. He took the position that we should not supervise the telegrams of foreign governments. This of course spelled the doom of the Black Chamber which was now supported almost totally by State Department funds.

I slowly hung up the receiver and turned to my secretary, who had been with me for ten years. She had gathered the meaning of the conversation. Her face was as white as death.

"I'm sorry," I said inanely. "I guess we'd better call in the others."

When I told them the decision at Washington, they all stared at me with uncomprehending eyes. Most of them had devoted many years to cryptography, working secretively, not even their most intimate friends being aware of their real accomplishments. That

The reasons obviously exist as to the transfer of the files from MID to the Signal Corps, April-May, 1929, just before this episode. HOY's Black Chamber was doomed when this transfer was made.