World War II
Codes + Ciphers
Given at Scamp
1958.

Ladies and Gentlemen:

I am now about to begin the story of World War I and the cryptologic aspects of it. It broke out in August 1914 By that time Britain had become so dependent upon seaborne imports that its people couldn't live, let alone wage a war for more than four or five weeks after those sea lines of communication to the outer world were severed. Protection of these sea lines was Britain's Navy's principal task The Central Powers were not dependent upon seaborne imports and Navy's historic function of arresting enemy seaborne trade lapsed after German shipping found refuge in neutral ports British trade route protection was the responsibility of the Grand Fleet. A battle with the almost equally strong German Fleet would nullify this protection but the Germans were not inclined to risk their fleet. German hopes of quick victory were shattered when their armies were brought to a standstill in France and with each month it became more and more evident to Kaiser Wilhelm and his advisors that there could be no victory unless British seaborne trade was destroyed. Now the success of the German small submarine flotilla of 1914 pointed out a way of doing so without risking their fleet and therefore the highest priority was given to the construction and launching of submarines Now the rules of maritime warfare required that no merchant ship be sunk without warning and before the crew could take to the life boats. But observance of these rules severely reduced the destructive power of the submarines and their commanders were ordered to ignore them The British were unprepared for such an offensive and there came a time when the daily toll of ship losses was so heavy that unless something new was discovered or devised, there could be one

and only one end to the war and that would be soon The scientists and ship-builders and the sailors had their part to play and by tremendous exertion they enabled the British to turn the corner but it was not until early 1918 that a mastery over the submarine fleet was gained During the first year of submarine warfare, the German Government respected the rights of neutrals but faced with the prospect of losing the war unless all imports to Britain were stopped, they made the fateful decision--they ordered the submarines to sink at sight all ships encountered on the high seas In February 1917, they proclaimed that unrestricted submarine warfare would commence. Now the British expected the U S., already exasperated by activities of Gorman agents in America and by specious arguments by the German Government and excuses for sinking American ships, the British felt that the United States would soon join the Allies but President Wilson was determined to keep out of war and he tried most earnestly to keep neutrality, like Holland, like Denmark, like Norway and the other countries The South American Republics were not unsympathetic to Germany Spain was neutral but there was no lack of German sympathizers in Spain British and German agents conducted their own private warfare on Spanish soil The United States sympathies on the whole were with the Allies but there was alarge German-American population, powerful too and these had to be taken into account Even when British high-handed action every once in a while hurt their case, so the United States Government official position was very difficult President Wilson came to the time when he was hesitating on the brink of war, reluctant to plunge into it, clinging painfully

to the idea of strict neutrality which seemed to be almost a part of his religion. You remember the slogan for the Democrats for the second term for the President-- he kept us out of war. His statement, you will remember, "there is such a thing as being too proud to fight". This didn't set too well with the American people. For a large part of the United States, for the middle West and the far West, Southwest, the war in Europe was 3,000 miles across the Atlantic. It might just as well have been on another planet. Then came a cryptanalytic episode which entirely changed the picture and it did it almost overnight

The episode goes under the name "The Zimmermann Telegram". The interception and solution of this message by the British and the brilliant manner of its employment brought the United States into the war on the side of the Allies. Now I had decided to give a fairly detailed account of the Zimmermann Telegram episode and had ordered to be shipped out to SCAMP, the motion picture which you are about to hear. It is Walter Cronkhite's "You are There" and we are about to see a very well-done picture but just yesterday I received a letter from which I would like to read a few lines. I don't have time to request permission of its writer but I am sure my friend wouldn't object to my reading parts of his letter before this group. The letter is from Cmdr. A. G. Denniston who for a number of years before World War II was the head of the British cryptanalytic group and a short time after World War II began concentrated his attention upon the diplomatic, economic, political cyphers which were encountered A few weeks ago I was in London and I took the time to go down to the country and visit my old friend who has been retired for about a dozen

years I was very happy to do this I hope that when I get older and have to withdraw from active participation in this very interesting activity somebody will remember me and come around and talk over some interesting episodes. I wrote him a letter and note of thanks when I got home and my letter was dated the 26th of May and this letter in reply thereto is dated 19th of June.

"My dear Friedman. I found your letter of May 26th and its very interesting enclosure, sent thru Captain Currier, on my return from a visit to the North."

(What I sent him was a paper which I had written a number of years ago, before we became Allies with the British in this activity The paper dealt with the Zimmermann Telegram and certain questions were raised, the answers to which I needed some help in procuring I thought that Denniston could It turned out that the information in that paper I was told by the official custodians of the records and my friends at GCHQ, the contents of that paper, which by the way was written in collaboration with my late friend, Dr Charles J. Mendelsohn, who was Professor of Greek and German at the City College in New York, the contents of that paper according to them gave a more complete account of the Zimmermann Telegram from the cryptographic aspects than their own records But at any rate, I wanted Denniston's help I won't read anything more except I want to come to this place.)

"On the same day that you wrote your letter, the BBC on sound radio broadcast a version of the Zimmermann Telegram giving very full and accurate details of 40 OB and the methods employed and even the names of the actual performers I am trying to find out who is responsible but I suspect Admiral

James." So you see the Zimmermann Telegram, an episode which took place forty years ago is still a live subject.

Now I think we will start the film, we'll turn out the lights and we will listen to Walter Cronkhite's "You are There".

When the United States became one of the belligerents in World War I it entered into the war very illy equipped as far as cryptology is concerned. It had no organization whatever either for cryptography or for cryptanalysis. The Navy had a very small unit, called the Registered Publications Section and their job was to make the Naval codes which they did occasionally and revised them from time to time The Army had that wonderful piece of work, the War Department Telegraph/Code of 1915. There was in the United States a citizen whose name was Fabyan. He had a title--Colonel, Kentucky variety. He was a very wealthy man and he had a lovely estate about 35 miles west of Chicago and he conducted a number of curious activities on this estate. I came there in June 1915, in the middle of my work in the graduate school at Cornell University. I was trained as a geneticist. When I came I found on the place a division or department devoted to the study of acoustics, nothing much was known about acoustics in those days but Colonel Fabyan had gotten in touch with Professor Wallace Sabin of Harvard University who was the leading expert in the acoustics field in this country and Dr Sabin began to suggest certain things that Colonel Fabyan might do in the way of study of acoustics and he actually designed a building which was started and about one-fourth completed when Dr. [redacted] SABIN

died There was another division or department on the place besides my own, if you wish to call it that, devoted to the attempt to prove by means of cryptography that the works the world generally attributes to William Shakespeare are written by Francis Bacon and the attempt was underway with a number of young students under the leadership of a woman whose name was Elizabeth Wells Gallup. Riverbank Laboratories, or Riverbank, was a good distance from Chicago and in those days there weren't many young fellows who had sporty cars and I stuck pretty close to home and having an inquiring mind I wanted to know what was going on in the cipher department and besides a rather attractive young woman had come to join that organization about a year after I had started my genetics work From a casual interest in cryptography I came to have a deeper fix interest as Colonel Fabyan was a shrewd and far-sighted man came to believe that the United States would be drawn into the war sooner or later and that it would be a good thing if there were some people skilled in military cryptography. He suggested that I do some studying. I looked for texts, there was very little available certainly none in this small town of Geneva and the city of Chicago had little to offer I didn't realize at the time that there wasn't very much but at any rate I began studying with a manual that had been produced by the Army Signal School which was then at Fort Leavenworth and from the very small beginning grew an organization which was able to fill in the gap until the government could establish a real organization to deal with cryptology Now the first slide I want to show is one of, I think of, George Fabyan.

Colonel George Fabyan sitting in what we called the "hell chair". It is suspended you see on chains and which the chains were attached and when you were called upon the carpet you had to stand in front of him and he slowly swing back and forth and you caught hell!!

There is that War Department Telegraph Code of 1915 and soon after our entry into the war, our British Ally gentlyinformed the Military Intelligence Division of the War Department General Staff that its code was not safe. I think you can see the implications of that statement and I certainly wouldn't deny myself the benefit of reading the code of an Ally to be and I believe that they probably were reading a certain amount of Army traffic. There was somebody else who had very little confidence in the codes of the United States Government--President Wilson. There is a message which he was getting off in his own handwriting. Mrs. Wilson was his cryptographic expert--she put the message up in a special code. Where there was no word in the code or phrase and a name had to be given those words were left as they are That is the way the message was finally sent out from the White House to the Department of State for transmission and whether the message was super-encoded by State Department code, I don't remember at this time.

Some shorthand written by President Wilson--a memorandum for himself which he then typed out and you will see that it's in a code made up not of groups of numbers or letters but a word code--the old-fashioned type. Someday I am going to try to find that code. I think it would be a good souvenir to have And the plain text of that shorthand note is down here. Now I said that

we began studying, I say "we" because it was not only myself but by that time Elizebeth Smith had become Mrs Friedman and we studied together and the manual that we had was the manual for the solution of military ciphers--this is it and this is the very copy that she used--her own copy That had been written by Parker Hitt, then a Captain of the Infantry, but stationed at Leavenworth, the Signal School for a brief period and it was a good manual, very succinct and I learnt the basic principles. Colonel Hitt became the Chief Signal Officer of the ADF and did a fine job and after, shortly after, the end of World War I retired I believe he is still living

We also studied a manual, a little brochure

Question:

Yes, an advanced problem. The problem was the PLAYFAIR cypher--the cypher which I think anyone of you could solve now with one hand tied behind you in twenty minutes but in those days it was considered quite a feat. As a matter of fact the PLAYFAIR cipher was the field cipher used by the British in World War I and to a certain degree by our own field forces This is the picture of Mauborgne, the author of that treatise He later became Chief Signal Officer He took a deep interest in cryptography I suppose that my continuance in the cryptologic field I owe to him. We studied ciphers and since there was no department in the government that was devoted to that sort of business, Colonel Fabyan got in touch with the authorities in Washington and pretty soon we were being given messages to solve The messages were mostly those that were surreptiously obtained by the Department of Justice

passing between points in the United States including Washington and Mexico. If you will remember in those days, 1915, 1916 we were in continual difficulty with our Southern neighbor so it was necessary to know as much as possible what was going on and we got these messages and had good fortune--we were able to read everything that the Mexican Government sent--the ciphers were not very complex We also taught classes in cryptography to the classes of officers sent out by the Adjutant General, few from Navy, when the government began to see that it was necessary to do some training in this field It was while we were studying ciphers there that I had my first contact with Francis Bacon's bi-literary alphabet, bi-literal cipher, so called and there is the alphabet and this I believe, gentlemen, is one of the very earliest examples of binary code By means of that alphabet you could indicate thoughts, sentences, so on, very simply This is an example, a fantastic picture of a castle Some of the bricks are shaded, some are plain and if you start in at the upper most tier of bricks, assign them to a or b according to that binary system, your message that is spelled out is the following It was prepared by a physician friend of Colonel Fabyans "My business is to write prescriptions and then to see my doses taken but now I find I spend my time endeavoring to out-Bacon Bacon." Many years later, desirous of giving a picturesque example of Bacon's bi-literal cipher in one of my Army texts, but thinking that a picture of a holy castle of this sort might not set well with the authorities, I had to put in a different type of cipher and there it is. You will note the footnote which calls attention to the fact that

there is a cipher in that paragraph Even so, the number of students who have found the secret message is very low If there had been no footnote, I don't think it would ever have been found Anybody want to try to find it now?

Well, we built up a cryptanalytic organization and we did a job that had to be done until the government did organize its facilities, mainly, under the Military Intelligence Division of the War Department General Staff The Navy did not go in for cryptanalysis at that time. We were called in occasionally to help out and this slide will give an example of the type of letter which occasionally was sent to us by the Department of Justice This was one page of a seven-page letter sent by a Hindu in New York City who was reporting to his superior in Geneva, Switzerland The Hindus, financed by the Germans, were trying to stir up a rebellion in India The purpose being to cause enough of a disturbance so that the British would have to withdraw troops from the Western Front and send them to India The Hindus in this country were buying arms and ammunition and trying to ship them to India. Since the United States was neutral, this could not be allowed and when the British turned over these messages, how they got them I do not know--I suppose they had their own secret agents, we were asked to take a look and this particular letter was solved in its entirety You will notice that it's a page line and letter in the line system. The reason that we were able to solve it was that this Hindu was a lazy fellow and instead of jumping all over the book, he took sequent letters in many cases and he used the same page and sometimes the same line for a good many different spellings so that with the

plain language interspersed you would get a clue, some idea, as to what might be in here. This might be a name, you see Well my assuming names and words between the places where there was plain language, we could begin to reconstruct the book from which the key letters came . For example, there was a place in the text where it said

fitted in right by it

you will see if you replace these letters - you can build up words in that text. This gave some idea as to the nature of the book. It dealt with ~~his~~ political economy or history of Germany and I found the book It was Price Colliers' Germany in the Germans. The Hindus had two other systems. This is one of them, one of the two other ones It was a monoalphabet sort of thing key numbers of the key word lamp. They had a trial in Chicago of these Hindus and they were found guilty and then they had a bigger trial in San Francisco and there were about 102 or 103 Hindus on trial simultaneously. I went out as government expert to testify on some of these messages and the trial wound up in a very dramatic fashion. These Hindus were quartered in a hotel and everyday before they were led into the courtroom they were searched for weapons. One day one Hindu managed to secret a gun and in the midst of the proceedings, he drew the gun and shot the Hindu who had turned State's evidence dead on the spot The idea being that ~~the~~ this dead Hindu I suppose was the one that gave away the key to the ciphers, you see. Whereupon the United States Marshal, who was a man about six feet three, standing in the rear of the court room drew his gun and shot over the heads of

the spectators and the second Hindu was dead and the whole business within one minute I was glad I was not in the line of fire. Now, in due course, the Military Intelligence Division built an organization around a young man whose picture is shown, Yardley, Herbert O. Yardley, a first Lieutenant at the time. He had been a telegraph operator in the State Department and had taken an interest in cryptography and he knew more about ciphers, I suppose, from what little he had done with the State Department codes than most other people in Washington so when they needed somebody, they commissioned Yardley and he began building the organization. I will have something to say about Yardley a little later on

This picture shows, save for Yardley who was abroad at the time, the entire officer staff of the cryptologic division of the War Department General Staff in World War I. Some of them attained positions of distinction. This gentleman was already a distinguished man at the time--that's John Manly who was Head of the Department of English at the University of Chicago and this is David Stevens who became Head of the Humanities Division of the Rockefeller Institution. And everyone of them was a scholar of some sort so one must see that at least Yardley and his associates above him understood from the beginning that cryptologic work required a little bit more than the ordinary run of mine brains. Now some of the things that Military Intelligence worked on I think should be mentioned Of course they had postal censorship and there is a picture post card and there is the back of the postcard with a message which is unintelligible-- it is German but it is unintelligible. It was prepared by means of a grille which would be applied to the card on which you were going to do the writing.

That's the front side of the grille. that's the back side so you had two positions--in all you had four positions But from the first position you get the words: Lever, Charles and so forth, you can read that in plain language So for the rest of the thing, you just put the words in as you apply the grille to the basic card on which you are writing There is one more position and then we are finished with that--a rather easy thing to reconstruct. Music--real music, the writing which you see in between here is in secret ink. That was one of the methods the spies and secret agents used. The gentlemean who used this one was a German spy. He was caught in England and was sentenced to life imprisonment. Here is an example of phoney music, usually detected by any musician I should modify that to say except/for perhaps those who are addicted to modern music. A very simple expedient, what we call a concealment system--every fourth word in this message is significant, the rest is padding. Another example, well, there is the text of that one. Another example. In this case every sixth word in lines containing an even number of words--in this case we have a message indicated by heavy shading of letters. This message in fact got by the German censors, you see the censors mark at the top. MI-8 worked on sabotage messages, this doesn't happen to be one that they worked on themselves but I show it for its interest. This was solved by the British organization and if you read the text, you will see that they were, the Germans were bent on raising as much hell as they could by means of sabotage and some of you are old enough to remember a great disaster on the Eastern Seaboard, the Black Tom explosion and the Kingsland fires where millions of dollars worth of property damage was done to munitions

going to England. The trial of certain suspects went on for years and the German-American Mixed Claims Division dealt with it for years and finally the German Government gave in and admitted that the things had been done by some of their agents.

That is the original German plaintext message of the previous one in cipher. I got that from German records after World War II. There is the second page with all the authenticating signatures. This was no fly-by-night action on the part of anybody, this was the German Government setting out the sabotage arrangements.

Next we have, that is a page from Blue Book magazine with secret ink writing that was a part of the testimony or exhibits in the Mixed Claims Commission study of the case.

I have here now a message which was found on the person of a man who was caught crossing the border from Mexico into Texas. That was a chap named, Paablo Viversky. The message was solved and there you see at the bottom how dangerous it is to be a spy and carry anything on you.

the bearer of this is the subject of the Empire as a Russian under the name of Paablo Viversky etc. He was tried by court martial, sentenced to death--the sentence was commuted to life imprisonment by President Wilson and the gentleman was out of the hoosegow in within a year.

Question:

No it is not really a double transposition It's a queer kind of transposition which I think I will take up later

Well, we continued to work at Riverbank on various messages that were sent to us but as the organization in Washington grew we were gradually being contracted and devoted our attention then more to running some of these instructional courses and this is a picture of one of those classes. This is the largest class we had. Colonel Fabyan paid for all the instructional work, the rooms and facilities at a hotel in Aurora adjacent to Geneva. This picture contains ciphers. It's binary alphabetic. You will see some of the officers are standing looking straightforward, some are looking one way or another so you have a binary system. This chap took me too literally by the way and is smack in the middle. There's myself, you see. But the message as you start off abaab abbaa, etc-- knowledge is power.

Question:

I don't know whether ~~xxxxxxx~~ I would consider him a garble but that picture was reproduced in an issue of Time magazine about 1956, summer of 1956, when the government was rather nice to me and some letters came into the editor objecting to the fact that there was one character missing--one of the five units, the last one was missing. Well if you had any sense at all, you would know that you could fill that in. If you got knowledge is powe, you should know what the last letter is.

After this class was over, I was commissioned and went directly to France where I became a member of the German Code and Cipher Solving Section of the Military Intelligence Staff. That is Colonel Mauborgne, who was my chief. Now at that time I learnt something about the kinds of codes and ciphers in use by the various belligerents. That is the cipher system used by the Russians. This is

A simple modification of the system It happens to have a key of 2 - 4 - 6 - 8 positions and there is the decipherment. They were very inept at it, by the way, and I could talk for a whole hour on the causes for the terrible defeat of the Russians forces at Tannenberg and the collapse of the Russian military effort because of their ineptitude in cryptography. They couldn't even use that simple system and many times they had to resort to plain language. It was easy for Ludendorf and Hiddenburg to make up their operations based upon their knowledge of where the Russian forces were.

This is a cipher system used by the French Army. It is a transposition with keying for the columns but with a little querk in it by diagonals--I won't take the time to go into that

This is a cipher used by the Italians, a variation of the Viginere Square and this is the great German General Staff high-level cipher, called the ADFGVX, because the cipher text was composed of those five letters, six letters at the latter part of the war, a matrix with the letters ADFGVX, coordinates, these in mixed arrangements, generally a keyword arrangement in here The plain text of your message requests etc , the substituted equivalents diagraphic, the substituted equivalents used now is again a diagram, transposition diagram with a key to determine the order which you take your letters out of the columns so here is the first message. You begin abaff and so on. The ADFGVX cipher for that period was a very secure system but we read 95% of all the messages that were transmitted. This cipher is susceptible of solution in three ways. First, if you have two messages which begin with the same

words. Second, if you have two messages which end with the same words. Third, if you have a number of messages, which are of identical lengths. In those days we had not worked out a general solution but after the war when we had a little more time to devote to theoretical studies, a couple of my associates worked out a general solution and this cipher now would not be at all secure under heavy use. Incidentally, I might say that by following the ebb and flow of traffic in the ADFGVX cipher we gained a great deal of information because it was the high command cipher.

Next I show you the PLAYFAIR cipher which is composed of a matrix, 25 characters, 5 X 5, the letters I and J are considered the same and you take them by pairs. For example if you want to encipher EH, well they happen to be on the same line, you take the letters to the right HW. EK would be enciphered by the letters standing at the other diagonal, AU and so on. Incidentally that cipher goes by the name of PLAYFAIR, Lord Playfair, Leon Playfair is his name but it was actually invented by Sir Charles Wheatstone who tried to get it introduced into the Foreign Office but had no luck and he thought that maybe his friend Playfair would be able to impress the officials in the Foreign Office but he didn't have too much luck either but during World War I, the PLAYFAIR cipher was used.

Another system that was used was the double transposition. Perhaps later on I will give you an illustration of that.

We come now to code systems of World War I. I hardly have to tell you what a code is. You see there an example a page from a, a couple pages

from a commercial code. Those code words, five letter groups, all differ from each other by a minimum of two letters, the purpose being that if a single error is made in transmission or reception and generally an operator will not make more than one error, you can detect that there is something wrong by the fact that the group will not be in the book. This two letter differential was a very important piece of business for commercial codes. Oh, this one was a code and somewhat specialized. You know there are people who believe that illness is all in the mind and so can be treated by mental processes and this was a code gotten up by a practitioner of that art who wanted to have a holiday now and then and he also wanted to be able to treat his patients at a distance but he realized that he had to be a bit careful because of errors, the likelihood of errors, so that he had not a two letter differential but a three letter differential. You will see that if a patient were complaining of constipation, he might get treated for diarrhea unless there was a three letter differential of some sort.

Chinese telegraph codes. I have here a couple of these. They are interesting to look at. This is the official code of the Chinese Telegraph Ministry. There is nothing secret about it. They can't send characters so they send numbers to represent the characters and the characters are all disposed on pages 10 X 10 so that it is a very simple matter, if you can read Chinese, to pick out the numbers and send it. Now prior to World War I, it was considered impractical to use codes in the field but the Germans initiated the use of codes in the field and I show you a picture of one of their so-called KRUSA codes, because the code words began with those letters. You will see

variants, it's not a bad code at all.

The French had a code. In this case it was not only a--I think this one is a two-part code, yes, two-part code and then on top of that they super-enciphered.

This one is an extract. I am sorry I can't give you an actual facsimile of a British field code. Our British allies were particularly cagey about letting us have any of their codes so we did the best we could. We photographed, we copied a page from one they had lent us for an hour. The AEF went into the war very very poorly prepared. This, believe it or not, is authentic. I have the thing in my own collection. I don't know, maybe there are one or two who remember these gentlemen: Johnson,

But we caught up pretty quickly and that is a fascimile of a couple of pages from the American field code called the Champlain We had for the First Army a river series; the Allegheny, the Potomac, etc. and for the Second Army, a lake series. After we really got started we were the wonder boys of France because who but the Americans would have an Adjutant General with a van and a printing plant so that we could get up a new edition of a code of this sort every five or six days so we were pretty secure with those codes.

Now American successes in cryptanalytic work in the ADF xx World War I were not remarkable especially as regards the solution of codes because we were assigned to a quiet sector and there was very little traffic. We had fair success with the cipher traffic and in this we collaborated very closely with our French and British allies. The best results that we had in regard to codes

were with the low echelon three-digit codes and often we got tactical useful information by working on those. By the way, I remember how we used to get information when a code changed, when a German code changed, by a very simple subterfuge. The Germans are very very methodical and if they didn't have anything to report, they reported "nothing to report" and this happened thousands of times in World War I and several hundred thousands in World War II. If you have good reason to suspect that on the hour from a certain station, where there has been quiet, there will be a report, it will be "nothing to report" so you have a very excellent crib. We also had another crib. They had an inspector who used to go around to see to it that the men were following the code instructions to the letter and so we could follow this chap around on his rounds because he did the unpardonable thing of signing his messages and he had a long German name and this had to be spelled out so every time the code changed we looked for this - - - - - .

Here is an example of the worksheet that confronted us every morning. We had scads of them facing us when we came in and all you had to do was to fill in the meanings, very simple.

This is an example of the sort of information that was put out from the ADFGVX cipher. This is a particularly good one. It was, I don't know, a 12 or 15 part message after the armistice when McKenson's army was withdrawing and we followed them and were able to tell everything that was going on. Every message of McKenson's was solved.

Now I mentioned that we got a certain amount of information by watching

the ebb and flow of traffic in the ADFGVX cipher. This, I believe, is the first example of what later became the art or science of traffic analysis. When there was a peak, we could expect in four or five days action in the vicinity of where that traffic was going or coming from. After the war, I was demobilized and I went back to Riverbank and stayed for a year. The government wanted me back. I was asked, urgently asked, to come into the Regular Army. I was urged by Colonel Fabyan to do this--he had a special motive of his own. So I went and took the examination. I flunked miserably. They said I had heart disease--that was 38 years ago and I'm still alive. Now, I think this is a good place to stop. I will resume on Monday with what happened in Washington--I think I can finish this, it will only take a moment or two.

I went back to Washington, not as an officer but as a civilian and I had charge of the code compilation division in the Office of the Chief Signal Officer. At that time, the cryptologic work in the Army was in somewhat chaotic state. The Signal Corps had responsibility for the compilation and the revision of the codes and ciphers. The Adjutant General had responsibility for storage and issue of the codes and ciphers and their printing. The Director of Intelligence, G-2, had charge of cryptanalytic work and there was no contact between the code compilers and in the Chief Signal Office and the code solvers in G-2. Yardley had gone to New York and had established what was later termed the American Black Chamber and I will have something to say about that later on.

There came a time when a Colonal Albright came to duty in the General Staff and he didn't like this arrangement of division of responsibility and he made a study of the situation and came up with the report that recommended that the work be integrated under the Chief Signal Officer so that the work that was conducted under Yardley in New York, in great secrecy, came back to Washington, or what there was left of it and Yardley proceeded to publish a book. This book was called "The American Black Chamber" and I have a copy of it here, it's a first edition. It raised quite a commotion, 30,000 copies of it were sold in Tokyo within three weeks of a Japanese edition. It almost got us into a war right there and then because you see Yardley tells in his book xxxx about how we were reading their messages between Tokyo and Washington at the time of the disarmament conference and how Mr. Hughes, who was the Secretary of State at the time, and was Chairman of the U.S. delegation and at the time this book was written was Chief Justice of the United States Supreme Court--this didn't look very nice. Well, there was nothing that could be done to Yardley for his indiscretions All I can say is that the publication of this book cost the government of the United States hundreds of millions of dollars and thousands and thousands of lives because until this book was published, the Japanese were children cryptologically speaking, children. After the book was published, they began to study. They improved their ciphers There was only a small amount of money that could be devoted to cryptologic work in the Army and what little we had had to be concentrated on one thing or another. The concentration was on Japanese diplomatic ciphers. We had no money, no people to study military ciphers. As a consequence, the

very simple types of ciphers that the Army and military attaches were using up until the time this book was published, became replaced by much more difficult systems and we did not read a single Army message from December 7, 1941 until about the 1st of April 1943. This was a very unfortunate thing. Had we been able to read the military messages, we might have done some good with what little forces we had and prevented the Japanese from their onward rush into Southeast Asia.

During the time that I was working in the Office of the Chief Signal Officer and studying ciphers and revising and compiling, I also did a number of brochures. These were published and I show you one of them, I think the title page of one. 1923--this was the first document that the government of the United States printed officially on cryptology. I show it because I have here a photostatic copy of it. This photostatic copy we captured from the Germans and the Germans captured it from the French. It is now liberated and belongs in the Friedman Collection. I would like any of you who want to see it to come up and see it.

Now I think this is-- one last slide. This is a picture of the entire cryptanalytic group under me in the year 1935 We had two rooms This outer room, where people are standing, I think everyone of these people in the picture are still in the business except this one lady who has several children-- she may be a grandma by this time The secret work was conducted inside a vault--we actually got locked in The funny part of it is, you won't believe this, but whatever results we put out in the way of decodes and decrypts, nobody ever saw. Our instructions were to put them on a hook--this was hot

stuff, it was too dangerous to handle, it was illegal. I think with that we will bring this period to a close and will resume on Monday. Thank you very much.