

NO 6  
2d Draft

INTRODUCTION TO CRYPTOLOGY VI

Confidential

*Richard Cowie*  
*Anthony Chief*  
*Security*  
*Form*  
~~*Edward*~~  
~~*John*~~  
~~*194*~~

INTRODUCTION TO CRYPTOLOGY - VI

by

By (WILLIAM F. FRIEDMAN



This lecture, the sixth and last in this series, deals with cryptology in the period from the end of World War I to the end of World War II (Unclassified material only). The emphasis in this lecture is upon communications security (COMSEC) not only because in the five preceding lectures the emphasis was placed very largely upon communications intelligence (COMINT) but also because although not as spectacular as COMINT, (COMSEC) in the final analysis, is really more vital to National Security than COMINT.

*Insert here the matter of pages 1a-1e then continue with*

\* \* \* \* \*

You will perhaps recall that in the very first lecture in this series reference was made to the role that COMINT (or "Magic") played not only in the events preceding the Japanese sneak attack on Pearl Harbor but also in the military, naval, and air operations which followed that attack. This is not the place nor is there time to go into the complex problems involved in an attempt to ascertain the names of the persons and to fix upon them the blame for being caught by surprise. Millions of words have been published on this subject and I do not propose to add to that voluminous literature whatever thoughts I may have thereon.

~~However, there is one small but extremely significant piece of information involved in this matter and I will say a few words about it.~~

P

*in the 17 December 1945 issue of TIME magazine,*  
 the first lecture I called to your attention an article which appeared and which was based upon a letter <sup>that</sup> the late General George C. Marshall, then Chief of Staff of the

Army, wrote to Governor Thomas E. Dewey, Republican candidate for President in the 1944 election campaign. *Here is a picture showing how the two principals looked at that time (Fig. 1)* In that letter which was written on 27 Sept. 1944, General Marshall practically begged Governor Dewey to say nothing during the campaign about a certain piece of very vital information which General Marshall had reason to believe

*(continue with matter on p. 2 etc.)*

This, the sixth and final lecture in this series on the history of cryptology, will be devoted to a presentation of <sup>the</sup> events and developments of significance or importance in that history from the end of World War I to the end of World War II.

It would be entirely too ambitious a project even to attempt to compress within a lecture of only 50 minutes all that should or could be told in that segment of our history of cryptology. In a nutshell, however, it can be said that the most significant and important events and developments during that quarter of a century were directly concerned or connected with the advances made in the

production of more complex mechanical, electrical, and electronic cryptographic apparatus <sup>in order to increase or to facilitate greater cryptosecurity of our own cryptos</sup> and with the concomitant advances in the production of more

sophisticated mechanical, electrical and electronic <sup>cryptanalytic</sup> apparatus <sup>in order to speed up</sup> ~~for the~~ <sup>or to</sup> make possible the solution of enemy communications ~~solutions of the messages~~ produced by their increasingly complex cryptographic

machines. These two phases are inter-related because, to use a sort of simple analogy, cryptography and cryptanalysis represent the <sup>obverse and reverse</sup> ~~two~~ faces of a single coin, and it

<sup>some</sup> would be nice if I could go ~~into~~ <sup>into</sup> detail in regard to these increasingly complex matters but security considerations prevent my doing so.

~~because the classification of these lectures, via, CONFIDENTIAL, is the lowest~~

~~one now possible.~~ <sup>P</sup> As to ~~the~~ advances in the development and use of more complex or more

sophisticated cryptographic apparatus I will only note at this point a comment which General Omar Bradley makes in his quiet but very interesting book entitled

A Soldier's Story: ✓

✓ New York: Henry Holt and Co., 1951, page 474.

Signal Corps officers like to remind us that "although Congress can make a general, it takes communications to make him a commander."

It is <sup>presumptuous</sup> ~~immodest for me to try~~ to amend General Bradley's remark but this

is how I wish he had worded it:

Signal Corps officers like to remind us that "although Congress can make a general, it takes rapid and secure communications to make him a good commander."

This will in fact be the keynote of this lecture. In other words, communications security, or COMSEC, will be its main theme and the one I wish to emphasize.

But before coming to that part of our history perhaps a bit more attention must be devoted to events and developments of cryptanalytic significance or importance during the period 1918 to 1946. By far the most spectacular and interesting of these are the one which were so fully and disastrously disclosed by the various investigations conducted by the Army and Navy very secretly while World War II was still in progress, and both secretly and openly after the close of hostilities. The investigations were intended to ascertain why our Army and Navy forces in Hawaii were caught by surprise by the sneak attack on Pearl Harbor by the Japanese on the morning of 7 December 1941. They were also intended to ascertain and pin the blame on whoever was responsible for the debacle. I don't think I should even attempt to give you my personal opinion on these complex questions, which were studied by seven different boards within the Services and finally by the Joint Congressional Committee on the Investigation of the Pearl Harbor Attack. I mentioned the latter investigation in my first lecture and now <sup>will</sup> ~~must~~ add to what I then said. ~~The committee published its findings, conclusions and recommendations in 1946.~~ <sup>early</sup> ~~It~~ began its work in September 1945 with secret hearings, but on 70 days subsequent to 15 November 1945 up to and including 31 May 1945 open hearings were conducted, in the course of which some

15,000 pages of testimony were taken and a total of 183 exhibits received

*In July 1946*

incident to an examination of 43 witnesses. The Committee put out a final

*containing its findings, conclusions and recommendations. The Report*

Report of 580 pages, *to accompany* a set of 39 volumes of testimony and exhibits.

*was accompanied by*

*was really not a single report:*

The Report there was one by the Majority (signed by six Democratic and two Republican members), and one by the Minority (signed by two Republican members).

The Minority Report was not nearly as long as that of the Majority but it

brought into focus certain troublesome points which still form the subject of

*by those*

acrimonious discussions and writings who believe the attack was "engineered" by

President Roosevelt, and that certain authorities in Washington were as culpable as were certain commanders in the Army and in the Navy in Hawaii.

For this history an interesting fact is that both the Majority and Minority *reports, however, it is*

Reports contain glowing tributes to the role played by COMINT before and during

*(NSA Technical Journal, Vol. IV, No. 4, Oct 1953, p. 5),*

our participation in World War II. In my first lecture, I presented a brief

extract in this regard taken from the Majority Report; but here is what the

*to/*

Minority Report says on the subject:

*Underline - all in italics*

6. Through the Army and Navy intelligence services extensive information was secured respecting Japanese war plans and designs, by intercepted and decoded Japanese secret messages, which indicated the growing danger of war and increasingly after November 26 the imminence of a Japanese attack.

With extraordinary skill, zeal, and watchfulness the intelligence services of the Army Signal Corps and Navy Office of Naval Communications broke Japanese codes and intercepted messages between the Japanese Government and its spies and agents and ambassadors in all parts of the world and supplied the high authorities in Washington reliable secret information respecting Japanese designs, decisions, and operations at home, in the United States, and in other countries. Although there were delays in the translations of many intercepts, the intelligence services had furnished to those high authorities a large number of Japanese messages which clearly indicated the growing resolve of the Japanese Government on war before December 7, 1941.

Page 5 of NSA Technical Journal (Vol. 4 - later), quoting from page 232 of the Report of the Majority, 79th Congress, 2d Session, Senate Document No. 244, Washington: Government Printing Office, 1946, p. 232.  
3. Page 514 of Report.  
Ibid, p. 514.

The Majority Report made five main recommendations, of which the second is of special interest:<sup>4</sup>

That there be a complete integration of Army and Navy intelligence agencies in order to avoid the pitfalls of divided responsibility which experience has made so abundantly apparent; that upon effecting a unified intelligence, officers be selected for intelligence work who possess the background, penchant, and capacity for such work for an extended period of time in order that they may become steeped in the ramifications and refinements of their field and employ this reservoir of knowledge in evaluating material received. The assignment of an officer having an aptitude for such work should not impede his progress nor affect his promotions. Efficient intelligence services are just as essential in time of peace as in war, and this branch of our armed services must always be accorded the important role which it deserves.

I assume that due note of this recommendation has been <sup>taken</sup> by the services but how far it has been possible and practicable to insure that the recommendations has been carried out or will be I do not know. In this connection I think it may be of interest to cite what the distinguished commander whom I have already mentioned, General Omar Bradley, has to say on this point:<sup>5</sup>

In their intelligence activities at Allied Forces Headquarters, the British easily outstripped their American colleagues. The tedious years of prewar studies the British had devoted to areas throughout the world gave them a vast advantage which we never overcame. The American Army's long neglect of intelligence training was soon reflected by the ineptness of our initial undertakings. For too many years in the preparation of officers for command assignments, we had overlooked the need for specialization in such activities as intelligence. It is unrealistic to assume that every officer has the capacity and the inclination for field command. Many are uniquely qualified for staff intelligence duties and indeed would prefer to denote their careers to those tasks. Yet instead of grooming qualified officers for intelligence assignments, we rotated them through conventional duty tours, making correspondingly little use of their special talents. Misfits frequently found themselves assigned to intelligence duties. And in some stations G-2 became a dumping ground for officers ill suited to line command. I recall how scrupulously I avoided the branding that came with an intelligence assignment in my own career. Had it not been for the uniquely qualified reservists who so capably filled so many of our intelligence jobs throughout the war, the army would have found itself badly pressed for competent intelligence personnel.

Have some of you pondered over the reason why an officer who reaches the highest level of command in an army, ours as well as in foreign armies, is called a "general officer" or "General"? It is because he is supposed to have

✓ Page 253 of Report of the Majority.  
Said, p. 253.

✓ Op. Cit., page 33

11/2/46

by diligent study and first-hand experience

high-level

learned something about everything connected with military operations. But a generalist is not a specialist in all the areas of operations <sup>within his cognizance and under his responsibility</sup>. As a field commander the generalist could conduct his operations satisfactorily, ~~even brilliantly~~, without being a specialist in all the phases of warfare before the latter became so complex as it has become in modern times. He can perform satisfactorily, even brilliantly, even now, provided he has competent specialists to assist him. And it is in the ~~are involved in modern engineering, electrical communications, guided missiles,~~ very important areas of cryptology, in COMINT and COMSEC, for military, naval, and air operations and services that you, if you become ~~rockets, etc. etc?~~ How much can he learn without first-hand experience in the real specialists, can be of utmost assistance to field commanders, the generalists. That is where you come into the picture - as their ~~tricky business of ordinary military intelligence operations, let alone the much~~ responsible and qualified specialists in the quite complex operations of ~~more complicated business of cryptology as applied in modern military operations~~ <sup>possible</sup> ~~warfare~~.

as to the applications of cryptology in modern fare <sup>in the future</sup>  
But let us leave these speculations, interesting as they may be, and  
of such applications in the past.

continue with our history. Let us first dispose of certain comments in the

COMINT area of that history, and specifically to the role that COMINT (or "Magic") played, not only in the events preceding the attack on Pearl Harbor, but also in the military, naval, and air operations ~~conducted~~, not only in the Pacific but also in the European Theatre.

had become known to Governor Dewey, it having been "leaked" to him by persons not authorized to disclose it. The information dealt with the fact that the U. S. had been reading <sup>certain high-level</sup> Japanese codes and cipher even before the attack on Pearl Harbor. The vital point which General Marshall wanted to convey to Governor Dewey was that not only was the information which had surreptitiously been given to Governor Dewey true but more important were the <sup>following</sup> facts, <sup>viz,</sup> that (1) the war was still in progress; (2) the Japanese were still using certain of the pre-Pearl Harbor cryptosystems; and (3) the U. S. was still reading the secret communications in these systems as well as certain other enemy communications. Therefore, it was vital that Governor Dewey

not use the information which had come into his possession as to our reading Japanese secret communications prior to the attack on Pearl Harbor. I said in that

first lecture that I might later give further extracts from TIME's account and, <sup>to</sup>

continue <sup>e</sup> the extracts <sup>from that account,</sup> ~~printed on pages 3, 4, and 5 of the first lecture,~~ here

they are:

General Marshall had a long series of bad moments after U. S. flyers, showing a suspicious amount of foresight, shot down Admiral Yamamoto's plane at Bougainville in 1943. Gossip rustled through the Pacific and into Washington cocktail parties; General Marshall got to the point of asking the FBI to find an officer "who could be made an example of." (The FBI, fearful of looking like a Gestapo, refused).

Once a decoder was caught in Boston trying to sell the secret. Once, well-meaning agents of the Office of Strategic Services ransacked the Japanese Embassy in Lisbon, whereupon the Japs adopted a new code for military attaches. This code remained unbroken more than a year later. The worst scare of all came during the 1944 presidential campaign, when George Marshall heard that Thomas E. Dewey knew the secret and might refer to it in speeches.

Yet for all these fears, the Japs never discovered that the U. S. was decoding their messages. Even after the surrender, the Army still used Magic as a guide to occupation moves; though it had once been planned to send a whole army into Korea, Magic showed that a single regiment would be enough.

SECRET KEPT

The letter, on stationery of the Chief of Staff's Office, bore a bold heading: TOP SECRET, FOR MR. DEWEY'S EYES ONLY. Candidate Thomas E. Dewey, his curiosity piqued, read rapidly through the first two paragraphs:

*If I ever learned about the Boston incident, I have forgotten all about it. But I shall never forget about the Lisbon episode. — W.F.F.*

*underline*

I am writing you without the knowledge of any other person except Admiral King (who concurs) because we are approaching a grave dilemma in the political reactions of Congress regarding Pearl Harbor.

*underline*

What I have to tell you below is of such a highly secret nature that I feel compelled to ask you either to accept it on the basis of your not communicating its contents to any other person and returning this letter or not reading any further and returning the letter to the bearer.

Tom Dewey looked up from the typewritten page. As he did the word cryptograph, a few paragraphs below, flashed into his vision like a red traffic light. He made his decision quickly, folded the letter, handed it back. Colonel Carter W. Clarke (in mufti), who had flown from Washington to Tulsa to catch up with Tom Dewey's campaign, went back, his mission uncompleted. *Here's a picture of Colonel Clarke (Fig. 2). Judging by the*

*Account on this page the photographs may have been taken on the return from his first visit to the Governor.*

"YOU HAVE MY WORD." It was September 1944. The campaign train rolled up through the Midwest, returned to Albany. A few days later Tom Dewey received another visit from Colonel Clarke.

The Colonel, again in civilian clothes handed over another letter from General Marshall. The General had changed his mind somewhat:

"I am quite willing to have you read what comes hereafter with the understanding that you are bound not to communicate to any other person any portions on which you do not now have or later receive factual knowledge from some other source than myself . . . You have my word that neither the Secretary of War nor the President has any intimation whatsoever that such a letter has been addressed to you . . ."

THE LOCKED FILE. This time Tom Dewey read on. As he turned the pages, he became the first man outside the high command to know the full story of "Magic" and what it was accomplishing in the War against the Japs (see above). The letter closed with a plea:

"I am presenting this matter to you, for your secret information, in the hope that you will see your way clear to avoid the tragic results with which we are now threatened in the present political campaign."

Tom Dewey locked the letter in his files, went back to his electioneering. Though he had known before that the U. S. had cracked the Jap code, had suspected that this information cast grave doubts on Franklin Roosevelt's role before Pearl Harbor, he held his tongue. The War Department's most valuable secret was kept out of the campaign.

MEETING AT A FUNERAL. Recounting this story at the Pearl Harbor hearing last week, General Marshall recalled that he and Tom Dewey never discussed the matter in person until they met at Franklin Roosevelt's funeral last April; "I asked Mr. Dewey to come with me to the War Department and I showed him current Magic showing Japanese movements. His attitude was friendly and gracious."

Had Marshall ever told Franklin Roosevelt of the letters to Dewey? Said Marshall: "The President died without knowledge of it."

## SECRET LOST

The Pearl Harbor Committee blithely tossed away one still-secret U. S. Government weapon. George Marshall's letters to Governor Dewey (see above) mentioned that the U. S., with the help of the British, had decoded German as well as Japanese messages, George Marshall begged the Committee to cut out these references. The Committee refused.

Publication of the letters thus gave the Germans their first knowledge that their code had been broken. It was also a breach of diplomatic confidence with the British, who had let the U. S. in on the secret on the understanding that it would be kept.

*✓ "A few days later . . ." But note that the first letter is dated 25 September 1944, the second letter, dated 27 September. It is possible that Colonel Clarke was unable to deliver the letter immediately but my recollection is that he did deliver it the next day. — W.F.F.*

The Marshall-Dewey correspondence is so important in cryptologic history that

I feel that the whole of it should be included even in this brief history. When

the letter was written it was, of course, TOP SECRET and it was only under great

pressure <sup>from</sup> ~~by~~ certain members of the Joint Congressional Committee ~~on the Investiga-~~  
~~tion of the Attack on Pearl Harbor~~ that General Marshall revealed <sup>its</sup> ~~the~~ contents <sup>of</sup>

~~no P~~ ~~the letter.~~ Thus, <sup>it</sup> ~~the~~ letter came into the public domain not only on the very day  
 that General Marshall <sup>was forced</sup> ~~had~~ to place it in evidence — <sup>its publication</sup> ~~the letter~~ caused a great sen-

sation in the newspapers — but also when the 40 volumes of the Hearings of that

Committee were published ~~by authority of the Committee~~ and put on sale by the Super-

intendent of Documents of the Government Printing Office. The disclosure of the

contents of the Marshall-Dewey correspondence was indeed such a sensation that

LIFE magazine printed the whole of it in its issue of 17 December, 1945, with the

following introduction:

**“MARSHALL-DEWEY LETTERS”**

**GENERAL TOLD CANDIDATE WE HAD BROKEN JAP CODE**

2/ During the 1944 election campaign General George C. Marshall wrote two letters to Republican Candidate Thomas E. Dewey, telling him that Army cryptographers had broken the Japanese "ultra" code. This fact was first revealed in a story by LIFE Editor, John Chamberlain, which appeared in LIFE, Sept. 24. Marshall's purpose, Chamberlain wrote, was to forestall Dewey's revelation of that fact in a possible attack on the Roosevelt administration's Japanese policy before Pearl Harbor. The actual text of the letters remained secret until last week, when General Marshall appeared before the Congressional Committee investigating Pearl Harbor and made the letters public. They appear below.

When he had finished reading the first two paragraphs of the first letter, Governor Dewey stopped because, as the Chamberlain article reported, "the letter might possibly contain material which had already come from other sources, and that anyway, a candidate for President was in no position to make blind promises." General Marshall sent the letter back again with an introduction which relieved the governor of binding conditions. This time Dewey read the letter and after much thought and discussion decided not to make use during the campaign of any information he previously had.

3/ So far as I am aware it has neither been ascertained nor disclosed, if known, who gave Governor Dewey the information. But it is a fact that as a patriotic citizen, he acceded to General Marshall's request — he made no use whatever of the vital secret information during the campaign or after it. TIME's account specifically states that Dewey "held his tongue. The War Department's most valuable secret was kept out of the campaign." *I know this to be true. — W. F. F.*

## FIRST LETTER

~~TOP SECRET~~  
(FOR MR. DEWEY'S EYES ONLY)

25 September 1944

My Dear Governor:

I am writing you without the knowledge of any other person except Admiral King (who concurs) because we are approaching a grave dilemma in the political reactions of Congress regarding Pearl Harbor.

What I have to tell you below is of such a highly secret nature that I feel compelled to ask you either to accept it on the basis of your not communicating its contents to any other person and returning the letter or not reading any further and returning the letter to the bearer.

I should have preferred to talk to you in person but I could not devise a method that would not be subject to press and radio reactions as to why the Chief of Staff of the Army would be seeking an interview with you at this particular moment. Therefore, I have turned to the method of this letter, to be delivered by hand to you by Colonel Carter Clarke who has charge of the most secret documents of the War and Navy Departments.

In brief, the military dilemma resulting from Congressional political battles of the political campaign is this:

The most vital evidence in the Pearl Harbor matter consists of our intercepts of the Japanese diplomatic communications. Over a period of years our cryptograph people analyzed the character of the machine the Japanese are using for encoding their diplomatic messages. Based on this, a corresponding machine was built by us which deciphers their messages.

Therefore, we possessed a wealth of information regarding their moves in the Pacific which in turn was furnished the State Department - rather than, as is popularly supposed, the State Department providing us with information - but which unfortunately made no reference whatever to intentions toward Hawaii until the last message before Dec. 7, which did not reach our hands until the following day, Dec. 8.

Now the point to the present dilemma is that we have gone ahead with this business of deciphering their codes until we possess other codes, German as well as Japanese, but our main basis of information regarding Hitler's intentions in Europe is obtained from Baron Oshima's messages from Berlin reporting his interviews with Hitler and other officials to the Japanese Government. These are still in the codes involved in the Pearl Harbor events.

To explain further the critical nature of this set-up which would be wiped out almost in an instant if the least suspicion were aroused regarding it, the Battle of the Coral Sea was based on deciphered messages and therefore our few ships were in the right place at the right time. Further, we were able to concentrate on our limited forces to meet their advances on Midway when otherwise we almost certainly would have been some 3,000 miles out of place.

We had full information of the strength of their forces in that advance and also of the smaller force directed against the Aleutians which finally landed troops on Attu and Kiska.

Operations in the Pacific are largely guided by the information we obtain of Japanese deployments. We know their strength in various garrisons, the rations and other stores continuing available to them and what is of vast importance, we check their fleet movements and the movements of their convoys.

The heavy losses reported from time to time which they sustain by reason of our submarine action largely results from the fact that

✓ In regard to this and the succeeding four paragraphs, see my comment below (p. 00). - W.F.F.

we know the sailing dates and the routes of their convoys and can notify our submarines to lie in wait at the proper point.

The current raids by Admiral Halsey's carrier forces on Japanese shipping in Manila Bay and elsewhere were largely based in timing on the known movements of Japanese convoys, two of which were caught, as anticipated, in his destructive attacks.

You will understand from the foregoing the utter tragic consequences if the present political debates regarding Pearl Harbor disclose to the enemy, German or Jap, any suspicion of the vital sources of information we now possess.

The Roberts' report on Pearl Harbor had to have withdrawn from it all reference to this highly secret matter, therefore in portions it necessarily appeared incomplete. The same reason which dictated that course is even more important today because our sources have been greatly elaborated.

As a further example of the delicacy of the situation, some of Donovan's people (the OSS), without telling us, instituted a secret search of the Japanese Embassy offices in Portugal. As a result the entire military attaché Japanese code all over the world was changed, and though this occurred over a year ago, we have not yet been able to break the new code and have thus lost this invaluable information source, particularly regarding the European situation.

A recent speech in Congress by Representative Harness would clearly suggest to the Japanese that we have been reading their codes, though Mr. Harness and the American public would probably not draw any such conclusion.

The conduct of General Eisenhower's campaign and of all operations in the Pacific are closely related in conception and timing to the information we secretly obtain through these intercepted codes. They contribute greatly to the victory and tremendously to the savings of American lives, both in the conduct of current operations and in looking toward the early termination of the war.

I am presenting this matter to you, for your secret information, in the hope that you will see your way clear to avoid the tragic results with which we are now threatened in the present political campaign. I might add that the recent action of Congress in requiring Army and Navy investigations for action before certain dates has compelled me to bring back the corps commander, General Gerow, whose troops are fighting at Trier, to testify here while the Germans are counterattacking his forces there. This, however, is a very minor matter compared to the loss of our code information. ✓

Please return this letter by bearer, I will hold it in my secret file subject to your reference should you so desire.

Faithfully yours,  
G. C. Marshall

SECOND LETTER

~~TOP SECRET~~  
(FOR MR. DEWEY'S EYES ONLY)

27 September, 1944

Mr Dear Governor:

Colonel Clark, my messenger to you of yesterday, Sept. 26, has reported the result of his delivery of my letter dated Sept. 25. As I understand him you (A) were unwilling to commit yourself to any agreement regarding "not communicating its contents to any other person" in view of the fact that you felt you already knew certain of the things

✓ The last two sentences in this paragraph were omitted from the Second Letter. See footnote 11 below. — W.F.F.



in G-2, how such an error had crept into General Marshall's letter, and was told that the letter which had been prepared for General Marshall's signature did not meet with the General's whole-hearted approval and that the General himself had modified it. Perhaps that is how the error to which I have referred crept into it.

*no 7* ~~the letter~~. One could hardly expect General Marshall to be entirely familiar with the technical cryptanalytic details involved in what he wanted to tell Governor Dewey, nor should one criticize him for not being able, in his very busy days and under very heavy pressure of events, to bear in mind or even to know about the differences between the enemy systems worked upon by the respective and separate Army and Navy cryptanalytic organizations. It is of course possible, indeed it may be

~~probable, that certain COMINT regarding the Battles of the Coral Sea and of Midway~~

*that in the case of certain valuable COMINT*  
~~as well as other~~ important naval operations <sup>A</sup> came from messages read by Army crypt-

*analysts, and this <sup>maybe</sup> is what confused General Marshall, in implying that all the credit belonged to them because of their solution of the Japanese highest-level diplomatic cryptosystem, the one that used the so-called "Purple Code", which wasn't a "code" but*  
 Since the period during which the disclosures of the Joint Congressional In-

vestigation were made, disclosures which were disastrous so far as concerns the important accomplishments of the two services before and after the Pearl Harbor

*7* attack in the field of communications intelligence, and much less has been written

and is now in the public domain regarding those accomplishments, but fortunately

no technical details of significance have been disclosed. Hints here and there

are in abundance in the many books and articles that have been published by U. S.

writers since the end of World War II; but more than hints of the great part played

by COMINT in U. S. military and naval successes are to be found in books and articles

published by American officers as well as by officers of the beaten Japanese, Ger-

man, and Italian armed forces. Time does not permit citing in this lecture many

of these hints or definite statements, but the following two are of particular interest because they concern the Battle of Midway, which is considered the one which turned the war in the Pacific from a possible Japanese victory to one of ignominious defeat:

[Fig. 3]

If Admiral Yamamoto and his staff were vaguely disturbed by the persistent bad weather and by lack of information concerning the doings of the enemy, they would have been truly dismayed had they known the actual enemy situation. Post-war American accounts make it clear that the United States Pacific Fleet knew of the Japanese plan to invade Midway even before our forces had sortied from home waters. As a result of some amazing achievements by American intelligence, the enemy had succeeded in breaking the principal code then in use by the Japanese Navy. In this way the enemy was able to learn of our intentions almost as quickly as we had determined them ourselves. <sup>2</sup>

\* \* \* \* \*

The distinguished American Naval historian, Professor Samuel E. Morison, characterizes the victory of United States forces at Midway as "a victory of intelligence." In this judgment the author fully concurs, for it is beyond the slightest possibility of doubt that the advance discovery of the Japanese plan to attack was the foremost single and immediate cause of Japan's defeat. Viewed from the Japanese side, this success of the enemy's intelligence translates itself into a failure on our part - a failure to take adequate precautions for guarding the secrecy of our plans. Had the secret of our intent to invade Midway been concealed with the same thoroughness as the plan to attack Pearl Harbor, the outcome of this battle might well have been different. But it was a victory of American intelligence in a much broader sense than just this. Equally as important as the positive advancements of the enemy's intelligence on this occasion was the negatively bad and ineffective functioning of Japanese intelligence. <sup>12</sup>

It is the second extract above which is of special interest to us at the moment, and, in particular, the portion which refers to "the negatively bad and ineffective functioning of Japanese intelligence." <sup>I think,</sup> The ~~Japanese~~ author is, <sup>a</sup> bit too severe on the Japanese intelligence organization. I say this because their cryptanalysts were up against much more sophisticated cryptosystems than they <sup>dreamt of</sup> knew or were qualified to solve. In fact, even if they had been extremely adapt in cryptanalysis it would have been of no avail - U. S. high-level communications were protected by cryptosystems of very great security.

<sup>12</sup> Midway, The Battle that Doomed Japan: The Japanese Navy's Story, by Matsuo Fuchida and Matasake Okumiya, 1955, pp. 131 and 232, translated by U.S. Naval Institute Publication, Annapolis, 1955, pp. 131 and 232. Admiral Morison actually wrote: "Midway was a victory of intelligence bravely and wisely applied." See ~~the~~ Vol. IV of His History of U.S. Navy Operations in the Pacific: Coral Sea, Midway and Submarine Actions, May - August 1942. New York: Little Brown, 1944, p. 158.

This brings us to a phase of cryptology which is of highest importance - the phase which deals with communications security, or COMSEC, and I shall confine myself largely to its <sup>development and</sup> historical background in <sup>our</sup> ~~the~~ U.S. Armed Forces. The background is a very broad one because it should include the background of the developments of each of the three components of COMSEC, <sup>(1)</sup> cryptosecurity, <sup>(2)</sup> transmission security, and <sup>(3)</sup> physical security of cryptomaterials. But since time is limited and because I think you would be more interested in the phases pertaining to cryptosecurity, I will omit <sup>or to the history of their development.</sup> further references to the ~~history of the~~ other two components. And even in limiting the data to cryptosecurity, I will have opportunity only to give some of the highlights of the development of the items that comprise our <sup>present</sup> cryptomaterials, omitting comments on the history of the development and improvement of our techniques, procedures and practices, all of which are extremely important.

I shall begin the story with a definition which you will find in any good English dictionary, a definition of the word "accident." You will get the point of what may seem to you right now to be merely another of my frequent digressions from the main theme, but if it be a digression I think you will nevertheless find it of interest. The word "accident" in Webster's Unabridged Dictionary is defined as follows:

1. Literally, a befalling.

- a. An event that takes place without one's foresight or expectation; an undesigned, sudden, and unexpected event.
- b. Hence, often, an undesigned and unforeseen occurrence of an afflictive or unfortunate character; a mishap resulting in injury to a person or damage to a thing; a casualty; as, to die by an accident.

There are further definitions of the word but what I've given is sufficient for our purposes. But why define the word? <sup>What</sup> what has it to do with COMSEC?

During our participation in World War II, the President of the United States, accom-

Here's a picture taken at the Casablanca Conference in January 1943 (Fig. 4). Imagine the disaster it would have been if the photo showing this distinguished group had been shot down and lost over the Atlantic or the Mediterranean.

military, naval, and civilian

panied by many of his highest-level assistants, journeyed several times half-way

and they

neither he nor they

around the world. He journeyed in safety — ~~he~~ met with ~~no~~ "accident." On the other

hand, in April 1943, Admiral Isoroku Yamamoto, Commander in Chief of the Combined

Imperial

to be

Fleet of the Japanese Navy started out on what was just an ordinary inspection trip

but it turned out to be a one-way trip for ~~the Admiral~~ <sup>him.</sup> ~~His death was announced in~~ (Fig. 5), who was the architect of the attack on Pearl Harbor. His death was announced in an official Japanese Navy communiqué stating that the Admiral "had met a glorious end

while directing operations in a naval engagement against superior enemy forces."

But we know that this was simply not true; Admiral Yamamoto "met with an accident" <sup>to</sup>

— I think

But some bright person, it was the late Jimmy Walker, when Mayor of New York City —

~~I think~~ who said that "accidents don't just happen — they are brought about." <sup>Jimmy</sup> Walker's comment was true in this case at least:

Admiral Yamamoto did not die ~~simply~~ by accident; he died because our Navy knew the

schedule of his trip down to the <sup>very</sup> last detail so that it was possible to set up an

ambush with high degree of ~~possible~~ success. Here is the story as told in an inter-

esting manner by Fleet Admiral William F. Halsey, U. S. N., in his book entitled Admiral Halsey's Story:<sup>13</sup>

I returned to Nouméa in time to sit in on an operation that was smaller but extremely gratifying. The Navy's code experts had hit a jack pot; they had discovered that Admiral Isoroku Yamamoto, The Commander in Chief of the Imperial Japanese Navy, was about to visit the Solomons. In fact, he was due to arrive at Ballale Island, just south of Bougainville, precisely at 0945 on April 18. Yamamoto, who had conceived and proposed the Pearl Harbor attack, had also been widely quoted as saying that he was "looking forward to dictating peace in the White House at Washington." I believe that this statement was subsequently proved a canard, but we accepted its authenticity then, and it was an additional reason for his being No. 3 on my private list of public enemies, closely trailing Hirohito and Tojo.

Eighteen P-38's of the Army's 339th Fighter Squadron, based at Henderson Field, were assigned to make the interception over Buin, 35 miles short of Ballale. Yamamoto's plane, a Betty, accompanied by another Betty and covered by six Zekes, hove in sight exactly on schedule, and Lt. Col. Thomas G. Lamphier, Jr., dove on it and shot it down in flames. The other Betty was also shot down for good measure, plus one of the Zekes. . . . We bottled up the story, of course. One obvious reason was that we didn't want the Japs to know that we

<sup>13</sup> Admiral Halsey's Story, McGraw-Hill, New York, 1947, pp. 155-157.

had broken their code. . . . Unfortunately, somebody took the story to Australia, whence it leaked into the papers, and no doubt eventually into Japan . . . . But the Japs evidently did not realize the implication any more than did the tattletale; we continued to break their codes.

Admiral Halsey's Story contains a good many more instances of cryptologic significance and interest to us. Other authors, both American and Japanese cite similar instances. One Japanese author states in categorical language that Japan was defeated because of poor COMSEC on the part of the Japanese Navy and good COMINT on the part of the American Navy.

But lest you get the impression that enemy intelligence agencies had no success at all with secret communications of U. S. Armed Forces, let me tell you that they did have some success and in certain instances, very significant success.

There is not time to go into this somewhat disappointing or dissillu<sup>o</sup>inating statement but I can say that as a general rule the successes were attributable not to technical weaknesses in U. S. cryptosystems but to their improper use<sup>o</sup> of certain low-level ones, by unskilled, <sup>and</sup> ~~or~~ improperly or insufficiently trained cryptographic clerks. I may as well tell you right now that this has been true for a great many years, for centuries as a matter of fact, because as long ago as the year 1605

Francis Bacon, who wrote the first treatise in English on the subject of cryptology, made the following comment: <sup>✓</sup>  
~~said~~ in the Advancement of Learning

This Arte of Cyphering, hath for Relative, an Art of Discyphering; by supposition unprofitable; but, as things are, of great use. For suppose that Cyphars were well managed, there bee Multitudes of them which exclude the Discypherer. But in regarde of the rawnesse and unskillfulnesse of the handes, through which they passe, the greatest Matters, are many times carried in the weakest Cyphars.

When electrical and particularly radio transmission entered into the picture additional hazards to communications security had to be taken into account, but

<sup>valuable</sup>  
 many commanders have failed to realize how much intelligence can be gained merely  
 ✓ The Two Bookes of the proficience and advancement of Learning, London, 1605, p.61. This book is commonly known as The Advancement of Learning. Some 18 years later Bacon saw no reason to change his comment in his De Augmentis Scientiarum, London, 1623. In fact, he strengthened it by making it read: " . . . but the rawnesse and unskillfulnesse of Secretaries, and Clerks in the Cowits of Princes, is such that many times the greatest matters are committed to futile and weak Cyphers." <sup>✓</sup>  
 (Gilbert Wake Translation, 1640, p.270.)

of messages as well as from a study of  
 the  
 from a study of the procedures used in transmission, the direction and flow of  
 radio traffic,  
 communications, the call signs of the transmitting and receiving stations, etc.,

all without solving the communications even if they were in cryptic form. Follow-

ing are <sup>these paragraphs</sup> a couple of extracts from a document entitled German Operational Intelligence, published in April 1946 by the German Military Document Section, a Combined British, Canadian, and U. S. Staff:

[i.e., communications intelligence or COMINT]

Signal intelligence was a chief source of information in the German Army. In the eastern theater, where there was offensive warfare primarily, the signal intelligence service was well-organized with well-defined purposes, efficient personnel, and adequate equipment. In the course of the campaign, it was reorganized to exploit to the fullest the success already experienced, and, by 1943, there existed a complete and smoothly functioning machine sufficient to meet all demands." (p. 8)

Most of their signal intercept success came from low echelon traffic. Armored and artillery radio nets passing operational traffic were followed closely and were one of the chief sources of signal intelligence. Artillery radio nets were given first coverage priority. Apart from messages intercepted in code or in clear, signal procedure, peculiarities of transmitting, and characteristics of Allied radio operators provided enormous assistance in helping to evaluate signal information. The Germans noticed that call signs were often the same for a unit over long periods and that even frequencies remained unchanged for weeks at a time. (p. 8)

omit  
 Much tactically important information was drawn from the enemy Air Force liaison net. It was assumed that an independent net served all Air Force liaison officers attached to the various headquarters and once one of these stations had been picked up and identified, it could be used to trace all other stations over a considerable area. Air Force traffic dealing with bombing targets was intercepted by Air Force units, and was sent through liaison channels to Western Theater Command. From here, over a network going down to divisions, the information would be flashed to all Army formation headquarters. Receiving sets at all levels, including division, were tuned in continually to this broadcast frequency." (p. 8)

Importance of Signal Intelligence During the Normandy Invasion:

During the invasion, the G-2s in the West drew about 60 per cent of the operationally important information from signal intelligence. The remaining 40 percent was derived from all other fields of intelligence. The amount of information decreased during the months of mobile warfare. During the retreat, although the possibilities of obtaining information became less frequent, the amount of information from signal intelligence remained high. Most of the information was deduced from the organization of enemy radio traffic networks, from decoded messages, and from the radio nets of the enemy Air Force liaison officers who were attached to ground troops. Based upon this information the evaluation center of signal intelligence often came to conclusions which, at first, sounded hypothetical to the operational command and were therefore doubted. In 90 percent of all these cases the events verified the signal intelligence information so that eventually more credence was given to its conclusions." (p. 22)

A great many examples of intercepted messages of tactical content are cited in the aforementioned document, which is replete with information of deep interest although the document was originally issued with the lowest security classification then in use (U. S. "Restricted"; British-Canadian "For official use only".) I wish there were time to quote at greater length from this useful brochure.

Coming directly now to the history of the development of our cryptomaterials themselves, I hardly need reiterate what was pointed out in previous lectures as to the profound effect of the advances in the science and art of electrical communications in the 20th Century. Those advances had a direct effect upon military communications and an indirect effect upon military cryptology. Hand-operated ciphers

and, of course, codebooks became almost obsolete <sup>because</sup> with the need for <sup>and greater</sup> greater speed of cryptographic operations <sup>became obvious in order</sup> to match as much as possible the very great increase in

the speed of communications brought about by inventions and improvements in electric wire and radio-

telegraphy. The need for cryptographic apparatus and machines <sup>thus very soon</sup> became quite obvious but it took quite some time to satisfy that need in a manner that could be considered to give adequate security for military communications.

The history of the invention and development of cryptographic devices, machines and associated apparatus and material is long and interesting. Let us begin with a résumé of the earliest items of importance in that history.

Until the advent of electronic cipher machines most cryptographic apparatus and devices were built upon or around <sup>concentric</sup> circular rotating members <sup>such as</sup> cipher wheels, cipher disks, etc. <sup>A very early, perhaps</sup> ~~The very earliest of~~ the earliest picture of <sup>a device</sup> such disks appears in a treatise by an Italian cryptologist named Alberti whose Treatati in Cifra was written in Rome about 1470. It is the oldest tract on cryptography the world now possesses. Here's a photo of Alberti's disk (Fig. 6), but I won't take the time to explain it except to say that the digits 1, 2, 3, 4 <sup>to call your attention to the fact</sup> were used to encipher code groups and <sup>that</sup> the letters of the cipher or revolving <sup>or</sup> alphabet were in mixed order. In Porta's book, first published in 1563 in Naples, there appear several cipher disks; ~~and~~ in the copy which was given me as a gift by Colonel Fabyan they are <sup>still</sup> in working condition. Here is a picture of one of them (Fig. 7). In this version the device used symbols as cipher characters. And apparently nobody thought up anything much better for a long, long time. It seems, in fact, that not only did nobody think <sup>up</sup> anything new or even some improvements on the original Alberti or Porta disks <sup>but</sup> those who did any thinking at all on the subject merely "invented" or "re-invented" the same thing again, and that happened repeatedly in successive generations. For instance, in Lecture No. <sup>IV</sup> of this series you were shown a picture of the cipher disk "invented" by Major Albert Myer, the first Chief Signal Officer of the U. S. Army, who obtained a patent on his invention in 1865. Here's a picture of the patented disk (Fig. 8) and the explanation of <sup>the invention</sup> it (Fig. 9). <sup>may also</sup> ~~And~~ you ~~will~~ remember that signalmen of the Confederate Signal Corps mechanized the old Vigenere Square and put it out in the form of a cylinder (see Figs. 13, 14 and 15 of Lecture No. IV). The cipher disk used by the Signal Corps of the U. S. Army during the decade <sup>our participation as a belligerent in</sup> 1910 to 1920, that is, during the period including <sup>World War I,</sup> was nothing but

white celluloid <sup>v</sup>variation of the original Alberti disk of the vintage of 1470  
 (except that it was even simpler than <sup>a</sup>its progenitor, because in the latter the  
 cipher alphabets produced were mixed alphabets whereas, in the Signal Corps  
 disk, the cipher alphabets are simple reversed standard sequences. We all know  
 that it generally takes a pretty long time to get a patent through the complex  
~~workshops of~~ the U. S. Patent Office, but in 1924 the ancient device was  
 patented in 1924 by S. H. Huntington (Fig. 11). Here you can see a great  
 improvement over the Signal Corps version--a blank is added to both sequences so  
 that the space between words could be enciphered. <sup>Indication of word space</sup> ~~This~~, as you have learned, is  
 a fatal weakness if seen in the cipher text; in the Huntington device the spaces  
 between words would be enciphered but the cipher text would have space signs,  
 although they would not correspond to the actual spaces between words in the plain  
 text. *In the Huntington device, the space signs in the cipher text would be a  
 bit misleading, but not to an experienced cryptanalyst, who would soon  
 realize that they do not actually represent "word space" in the plain text.*  
 It is interesting to note that in Austria in 1936, during the days when the  
 German National Socialists were banned as an organization, the Nazis used this  
 variation of the old disk--it had the 10 digits on both the outer and the inner  
 sequences for enciphering digits (Fig. 12).

The first significant improvement on the old cipher disk was that made by  
 Sir Charles Wheatstone, who ~~invented~~ <sup>invented</sup> some time before 1879 a cipher device which  
 he called a <sup>The</sup> Cryptograph. He described it in a volume entitled The Scientific  
Papers of Sir Charles Wheatstone, published by the Physical Society of London.

Here is a picture of Wheatstone's device, which is in my private collection (Fig. 13).

What Sir Charles did was to make the outer circle of letters (for the plain text) comprise the 26 letters of the alphabet, plus one additional character to

represent "space." The inner circle, for cipher equivalents, contains only

the 26 letters of the alphabet and these <sup>can</sup> ~~could~~ be disarranged in a mixed sequence.

Two hands, like the hour and minute hands of a clock, were provided, <sup>and they are</sup> under control

of a differential gear mechanism, so that <sup>when</sup> ~~as~~ the long or "minute" hand is advanced

to make a complete circuit of the letters on the outer circle ~~of letters on the~~

~~face of the cryptograph~~ the short or "hour" hand advances one space or segment

on the inner circle ~~of letters on the face of the cryptograph~~. In Fig. 13, for

example, the plain text letter G is represented by the cipher letter A, <sup>that is,  $G_p = A_c$</sup>  If

the long hand is now advanced in a clockwise direction for one revolution,  $G_p$

<sup>the letter immediately to the right of  $A_c$  on the inner circle.</sup> will be represented no longer by  $A_c$  but by  $G_c$ . In encipherment the long hand is

always moved in the same direction (clockwise, for example) and <sup>its aperture</sup> is placed <sup>successively</sup> over letters on the outer circle according to the ~~the~~ successive letters of the ~~plain~~ text message, the cipher equivalents being

recorded by hand to correspond with the letters to which the short hand points <sup>on</sup>

each encipherment. In this way, identical letters of the plain text will be

represented by different and varying letters in the cipher text, depending upon

how many revolutions of the long hand intervene between the first and subsequent

appearances of the same plain-text letter. Correspondents must naturally agree

upon the mixed alphabet used in the inner circle and the initial positions of the

two hands at the beginning of the encipherment of a message. In decipherment, the

operator moves the long hand, <sup>again</sup> ~~counterclockwise~~, <sup>until the hour hand points to</sup> seeking the cipher letter ~~in the~~

inner circle, <sup>then notes</sup> ~~and noting~~ the plain-text letter <sup>which is seen through the aperture at the end of</sup> to which the long hand points

<sup>on</sup> ~~to~~ the outer circle. Thus, in the case of the example given above, the cipher letters XZ AABGQAM will be found to represent the word REFERENCE.

During World War I, some time in 1917, the British Army resuscitated

Shows, with the alphabets shown in Fig. 13, and with the initial setting  $G_p = A_c$ , the word "reference" would be represented in cipher as follows: REFERENCE XZ AABGQAM in which it will be seen that repeated letters in the plain text are represented by different letters in the cipher text.

Wheatstone's cryptograph and improved it both mechanically and cryptographically.

Here's a picture of the device (Fig. 14), in which it will be seen that there are

now no longer the "minute" and "hour" hands but a single hand with an opening

or window that simultaneously discloses both the plain text and cipher letters.

*When the single hand is turned, the inner circle of segments is advanced eccentrically and a similarly-made outer*

~~is juxtaposed in an eccentric manner against the outer~~

circle of segments, which are made of a substance upon which letters may be

written in pencil or in ink, In this improvement on the original Wheatstone device

both sequences of letters are now mixed sequences. Making the outer circle

also a mixed sequence added a considerable degree of security to the cipher.

When it was proposed that all the Allied armies use this device for field communications and its security had been approved by British, French, and

American cryptologists (both at GHQ-AEF and at Washington) an opportunity to

agree or disagree with the assessment of these cryptologists was given me while

~~was~~ still at the Riverbank Laboratories. I was able to show that the modified

Wheatstone cryptograph was still insufficiently secure for military purposes

and the devices, thousands of which had been manufactured and issued, were

withdrawn. If you are interested in the method of solution I used you will find

it in Riverbank Publication No. 20, entitled Several Machine Ciphers and Methods

for their Solution, 1918. A better method of solution was devised by me ~~some~~ <sup>about 1923.</sup>

~~years later.~~

<sup>Some</sup> ~~many~~ years later, and almost by sheer good fortune, I learned that a cipher machine was in the museum of a ~~certain~~ small town in Connecticut named

Hamden. I was interested and wrote to the <sup>t</sup>curator of the museum, requesting

that he lend the device for a short period to me as principal cryptanalyst of

the War Department. Imagine my astonishment and pleasure when I unpacked the

<sup>upon its receipt</sup> box ~~sent me~~, and found a device, beautifully made and encased in a fine mahogany

case, with its inventor's name, Decius Wadsworth, and the date, 1817, engraved on the face of the machine, which was nothing but another version of the Wheatstone Cryptograph. Here's a picture of it (Fig. 15). <sup>There are good reasons to believe that</sup> ~~I believe~~ the model was made by Eli Whitney. Mechanically it was similar to the British modification, except that the outer sequence had 33 characters, the inner 26, so that the differential gear instead of operating on the ratio 27 to 26 was now on the ratio 33 to 26.

Thus, <sup>Colonel</sup> Decius Wadsworth, <sup>who was then</sup> ~~an American Army Colonel~~ <sup>the</sup> first Chief of Ordnance <sup>of the U.S. Army</sup>, ~~and an associate of Eli Whitney,~~ had anticipated ~~Sir Charles~~ Wheatstone by over 60 years in this invention. He also anticipated the British <sup>Army cryptologists</sup> by a whole century in their modification of Wheatstone's original, because in the Wadsworth device, too, there was only one hand and both alphabets could be made mixed sequences. This is very clearly shown in Fig. 16 as regards to the outer sequence, and I believe <sup>the picture does not clearly show this to be the case, so that</sup> the inner one could also be disarranged but, I am now not sure as to this point.

I returned the device a good many years ago and it is now on display in the Eli Whitney Room of the New Haven Historical Society's Museum.

The next device I bring to your attention is shown in Fig. 17, a device invented by a French Army reservist, Commandant Bazeries, who for some 10 years <sup>valiantly but unsuccessfully</sup> tried to get the French Army to adopt it. ~~He was not successful and~~ <sup>He</sup> included a description of his device, which he called his <sup>"Cryptographe Cylindrique" or</sup> "cryptographic cylinder," in a book published in 1901 in Paris. <sup>15</sup> He had, however, <sup>previously</sup> described his device in an article entitled "Cryptographe à 20 rondelles--alphabets (25 lettres par <sup>tr</sup> alphabet)," published in 1891. <sup>16</sup> In this device there is a central shaft on which

<sup>15</sup> Les chiffres secrets dévoilés.

<sup>16</sup> Comptes Rendus, Marseilles, Vol. XX, pp. 160-165.

can be mounted 20 numbered disks on the peripheries of which are differently mixed

alphabets of 25 letters each. The disks <sup>can be</sup> are assembled ~~on the shaft~~ in some <sup>extreme</sup> and then locked into position on the shaft by pushing in the locking disk at the prearranged or key sequence. The first 20 letters of the plain text of a message

<sup>first</sup> are aligned, as seen in Fig. 17 (JE SUIS INDECHIFFRABLE = "I am indecipherable"); the disks are then locked into position so that the whole assembly can be turned; and as cipher text one may select any one of the other 24 <sup>rows</sup> ~~rows~~ of letters,

<sup>then by hand on paper</sup> which are recorded. Then the next ~~20~~ 20 plain-text letters <sup>is</sup> aligned, etc. <sup>are one of the other 24 rows of letters selected and recorded</sup>

To decipher a message, one takes the first 20 cipher letters, <sup>and then locks</sup> aligns them

<sup>into position</sup>

on the device, the disks having been assembled on the shaft in accordance with

the prearranged or key sequence and then ~~one~~ turns the whole cylinder, searching

for a row of letters which form intelligible text. There will be <sup>one and</sup> only one such

row, and the plain-text letters are recorded. Then the next 20 letters of cipher

are aligned, etc.

~~In 1893~~ <sup>soon</sup> Another French cryptologist, the Marquis de Viaris, showed how

messages prepared by means of the Bazeries cylindrical cipher could be solved.<sup>17</sup>

Maybe that is why Bazeries wasn't too successful in his attempts to get the

French Army to adopt his device. But in the U. S. there were apparently none

who encountered either what Bazeries or de Viaris wrote on the subject. Capt. Parker

Hitt, U. S. Army, whom I have mentioned in a previous lecture, in 1915 invented

a device based upon the Bazeries principle but not in the form of disks mounted

upon a central shaft. Instead of disks, Hitt's device used sliding strips and here

(Fig. 18),

is a picture of his very first model, which he presented to me some time in 1923

or 1924 (Fig. 18). But I learned about his device some time in 1917 while still

at Riverbank, and solved one challenge message put up by Mrs. Hitt, a Riverbank

guest for a day. <sup>In meeting, the challenge successfully (which brought a box of chocolates</sup> I didn't use anything like what I could or might have learned

<sup>17</sup> L'Art de chiffrer et de déchiffrer les dépêches secrètes, Paris, 1893, p 100.

from de Viaris, ~~in accomplishing the solution (which brought a box of chocolates to Mrs. Friedman)~~ because at that time I hadn't yet come across the de Viaris book. I solved the message by guessing the key Mrs. Hitt employed to arrange her strip alphabets. She wasn't wise to the quirks of inexperienced cryptographic clerks; she used RIVERBANK LABORATORIES as the key, just as I suspected she would. The device she brought with her was an improved model: the alphabets *and the letters were* were on paper strips <sup>^</sup>glued to strips of wood, as seen in Fig. 19.

Capt. Hitt brought his device to the attention of the then Major Mauborgne, whom I have also mentioned in a previous lecture and who was then on duty in the Office of the Chief Signal Officer in Washington. There is some question as to whether it was Hitt who <sup>first</sup> <sup>^</sup>brought his device to Mauborgne's attention; Mauborgne later told me that he had independently conceived the invention and, moreover, had made a model using disks instead of strips. I have that model, a present from General Mauborgne many years later, <sup>brass disks</sup>. It is made of ~~brass~~, very heavy <sup>^</sup>on the peripheries of ~~the disks of~~ which he had engraved the letters of his own specially-devised alphabets. In 1919, after my return to Riverbank from my service in the AEF, Mauborgne sent Riverbank the <sup>beginnings (the</sup> <sup>^</sup>first 25 letters) of a set of ~~some 25 or~~ ~~more~~ messages enciphered by his device and alphabets. He also sent the same data to Major Yardley, in G-2. Nobody even solved the messages, even after a good deal of work and even after Mauborgne told us that two consecutive words in one of the challenge messages were the words "are you." Many years later I found the reason for our complete lack of success, when I came across the plain texts of those messages in a dusty old file in <sup>one of the rooms occupied in the old Munitions Building by</sup> <sup>^</sup>the Office of Chief Signal Officer. Here is a picture of the beginnings of the first six messages (Fig. 20). Mauborgne, when I chided him on the unfairness of his challenge messages, told me that he had not prepared them himself--he had an ~~understanding~~ <sup>understanding</sup> (Major Fowler was his name, I still

remember it!) prepare them. In our struggles to solve the challenge messages ~~we~~ had assumed that they would contain the usual sorts of words found as the initial words of military messages. It was the complete failure by Riverbank and G-2 to solve the challenge messages that induced Mauborgne<sup>n</sup> to go ahead with the development of his device. It culminated in what became known as Cipher Device, Type M-94. Here is a picture of it (Fig. 21). That device was standardized and

used for at least 10 years in the <sup>U.S. by the</sup> Army, ~~the~~ Navy, the Marine Corps, the Coast Guard, the Intelligence Agencies of the Treasury Department, and perhaps by other agencies.

In 1922, a war-time colleague, the late Capt. John M. Manly (Prof. and Head of the Department of English at the University of Chicago) brought to my attention a photostat of a holographic manuscript in the <sup>large</sup> collection of Jefferson Papers in the Library of Congress. It consisted of two pages entitled "The Wheel Cypher" and here is a picture of the second page (Fig. 22) showing Jefferson's basis for calculating the number of permutations afforded by the set of 36 wheels of his device. He didn't ~~attempt to make the~~ multiplication; he didn't have an electronic digital computer--for the total number is astronomical in size.

Jefferson anticipated Bazeries by over a century, and the Hitt-Mauborgne combination by almost a century and a half.

It soon became apparent to both ~~the~~ Army and ~~the~~ Navy cryptologists that a great increase in cryptosecurity would be obtained if the alphabets of the M-94 device could be made <sup>nt</sup> ~~variable~~ <sup>of invariant.</sup> instead ~~being fixed.~~ There began efforts in both services to develop a practical instrument based upon this principle. I won't take time to show all these developments but <sup>only</sup> ~~will~~ show the final form of the Army Strip Cipher Device Type, M-138-A (Fig. 23.). This form used an aluminum base into which channels were cut to hold ~~paper~~ cardboard strips of alphabets <sup>w</sup> ~~which~~ could be <sup>be</sup> slideeasily within the channels. It may <sup>be</sup> of interest to you to learn that

REF ID: A62832  
And that's how the first models of strip cipher devices made of aluminum by the extrusion process came to be. And how the U.S. Army, by administrative cooperation on an inter-service level and technical cooperation on a marital level, found it practical to develop and produce in quantity its

after I had given up in my attempts to find a firm which would or could make aluminum by womanly wiles and cajolery, on such grooved devices in quantity, Mrs. Friedman, ~~succeeded~~ on behalf of her own succeeded in ~~persuading~~ inducing or enticing one firm to make them for her group in the U. S. Coast Guard. ~~The aluminum Strip Cipher Device, Type M-138-A, was~~

This was the Marine Corps, used from 1935 to 1940 or 1942 by the Army, the Navy, the Coast Guard, and the et al, including the Armed State Department. It was used as a back-up system even after the ~~two~~ Services as well as the Department of State began employing ~~electrical~~ much better and more sophisticated cipher machines of high speed and security.

Thus far we have been dealing with cipher devices of the so-called "hand-operated" type. None of them can really be considered as being "machines," that is apparatus employing mechanically-driven members upon which alphabetic sequences can be mounted so that ~~a~~ constantly-changing <sup>sequences</sup> series of cipher alphabets are produced. We come now to ~~a~~ types of apparatus which can be called machines, and one machine is such ~~as the one~~ shown in Fig. 24. It is called the KRYHA, the name of its

German inventor, who unfortunately committed suicide a few years ago, perhaps the last model of his improved machine failed to impress professional cryptologists. because ~~he failed to make a success of his invention.~~ The Kryha has a fixed semi-circle of letters against which is juxtaposed a rotatable circle of letters. Both sequences of letters can be made mixed alphabets (the segments are removable and interchangeable on each sequence). The handle at the right serves to wind a rather powerful ~~coiled~~ <sup>clock</sup> steel spring which drives the rotating member on which the letters of the inner circle are mounted. In Fig. 25 can be seen something of the inner mechanism. The large wheel at the right has segments which are open or closed, depending upon the "setting" or key. This wheel controls the angular displacement or "stepping" of the circular rotating platform upon which the letters of the cipher sequence are mounted. The initial juxtaposition of the

of the inner or moveable alphabet against the outer or fixed one as well as the composition of these alphabets is governed by some key or other prearrangement. The cipher equivalents must be recorded by hand. After each encipherment, the button you saw in the center of the panel in (the preceding) Fig. 24) is pushed down, the inner wheel <sup>is</sup> advanced 1, 2, 3, 4 . . . ~~steps~~ steps, depending on the key, and the next letter is enciphered, etc. The pictures I've shown you apply to the latest model of the Kryha; as regards the first model, which came on the market sometime in the 1920's, a German mathematician produced an impressive brochure showing how many different permutations and combinations the machine afforded. Here's a picture of a couple of pages of his dissertation (Fig. 26) but even in those days professional cryptanalysts were not too impressed by calculations of this sort. With modern electronic computers such calculations have become of even less significance.

Let us now proceed with some more complex and more secure machines. In this next slide (Fig. 27) you see a machine which represents a rather marked improvement by a Swedish cryptographic firm upon the ones shown thus far. It is a mechanico-electrical machine designated as Cryptographe B-211. Here for the first time you see a cryptographic machine provided with a keyboard similar to that on an ordinary typewriter. Depressing a key on this keyboard causes a lamp to light under one of the letters on the indicating bank above the keyboard. At the top of this machine can be seen four wheels in front of two rear wheels. The four front wheels are the rotating elements which drive the two rear wheels; the latter are electrical commutators that serve as connection-changers to change the circuits between the keys of the keyboard and the lamps of the indicating board. There isn't time to show you the internal works which control the rotating

elements and ciphering wheels (you will see them later) but I must show you the next step in the improvement of such cryptographic machines, which made it possible to eliminate the tedious job of recording, <sup>by</sup> ~~hand~~ hand on paper, the results of encipherment or decipherment. This was done by means of a printing mechanism which was associated with the cryptographic machine. Here is a slide (Fig. 28) which shows the assembly--the B-211 connected to a Remington <sup>electric</sup> typewriter, modified to be actuated by impulses from the cryptographic machine. Of course, it was natural that/ the next step would be to make the recording mechanism an integral part of the cryptographic machine~~s~~. This you can see in the next slide (Fig. 30), in which the four rotating members referred to in connection with Fig. 27 and which control the two commutators also mentioned in connection with <sup>that figure</sup> Fig. 27 are clearly seen. The slide-bar mechanism at the right, <sup>called the "barrel" or "cage,"</sup> controls the displacements of the printing wheel in front of <sup>it</sup> ~~the slide-bar mechanism~~ and causes the proper letter to be printed upon the moving paper tape seen at the front of the machine.

Now we come to the next and a very important development, one first conceived by a European inventor, <sup>who</sup> ~~he~~ was followed soon thereafter, but independently, by an American inventor. <sup>✓</sup> In this advance the circuits between the keys of the keyboard and the lamps of the indicating board are varied by electrical circuit changers called "rotors," which rotate between <sup>fixed</sup> ~~rotating~~ members called "stators". In Europe the first of such machines put upon the market for purchase by anyone desiring one is shown in the next slide (Fig. 31). The machine was appropriately named the ENIGMA--for solution of messages enciphered by its means was believed to be impossible, or nearly so.

*I have some doubts on this question of priority of invention in this case. Hebern began working on his first model in 1910 or 1911, although his first application was filed on <sup>the date of conception in</sup> ~~be earlier than~~ 1910. I do not know what it was. The date on which the application for a patent on a rotor machine was filed in Europe is <sup>by a Danish inventor named</sup> ~~is~~   
 -26 -*

In Fig. 1 at the left (labeled I) is seen the machine with the top cover plate closed. At the front is the keyboard; above it the indicator board, consisting of lamps underneath glass disks upon which letters have been inscribed. Above the indicator board and to the left are seen the peripheries of four metal notched wheels, at the left a switch button which can be set to "encipher", "decipher" or "neutral" positions.

At the right in Fig. 1 (labeled II), the top cover plate has been removed, exposing the internal ciphering mechanism. Three rotors or connection changers "in cascade" can be seen attached to notched rings. The rotors ~~are rotatable and~~ serve to change the circuits between the keys of the keyboard to the lamps of the indicator board.

In such a rotor there is a circle of 26 equally-spaced contacts on the left face and a similar circle of contacts on the right face; wires passing through to rotor connect the contacts on the two faces, two by two, and these connections are arbitrarily made.

The rotors have engraved or painted on their peripheries the 26 letters of the alphabet which letters can be seen through small windows in the cover plate, so that the rotors can be aligned to the initial key setting. At the left of the first rotor is a <sup>stator</sup> ~~stator~~, on the periphery of which are also 26 letters of the alphabet. This <sup>stator</sup> ~~starter~~ also has a circle of 26 equally-spaced contacts, but / these are only on its right face and the contacts are connected by wires to 26 double-pole, double-throw switches operated by and associated with the 26 keys of the keyboard. The connections between the 26 contacts on the <sup>stator</sup> ~~starter~~ and the 26 switches of the keyboard are fixed.

But the <sup>stator</sup> ~~starter~~ is rotatable and its position at any time can also be seen through a window, labeled 3 in Fig. 1 (I), so that the initial setting of the <sup>stator</sup> ~~starter~~ and the three rotors can be seen through the four windows. The initial settings of these four elements constitute the key for the starting point in ciphering operations.

I used the expression "in cascade" a moment ago, in referring to the rotors, which

simply means that the current initiated by depressing a key of the keyboard passes through the stator and then through all three rotors before reaching a lamp of the indicator board. In the ENIGMA, when the current exits from the third <sup>rotor,</sup> that is, the last rotor at the right, <sup>it</sup> ~~and then~~ enters into another stator also having a circle of 26 contacts, but these are only its left face. This stator is fixed, ~~or~~ non-rotatable, and its contacts are connected, two by two, by 13 internal wires. This stator, called a reflector, serves to return the current, which exits from one of the 26 contacts on the right face of the third rotor, back into one of the <sup>25 other</sup> ~~25~~ contacts on the right face of that rotor, thence back through <sup>a</sup> contact on the left face of that rotor into a contact on the right face of the second or middle <sup>rotor, thence through the first rotor,</sup> ~~one of the rotors, etc.,~~ to a contact on the right face of <sup>the</sup> ~~that~~ left-hand stator. The <sup>circuity</sup> in this machine insures that if  $A_p = K_c$ , for example, then  $K_p = A_c$ , in the same position of the rotors, that is, the cipher process is reciprocal in nature. The circuitry can be seen in Fig. 32. It also has <sup>as</sup> a consequence that no letter can encipher itself that is,  $A_p$ , for example, can never be represented by  $A_c$ , no matter what position of the three rotors and the left-hand stator happens to be. <sup>C</sup> The same is true of all the other 25 letters of the alphabet. The three rotors are interchangeable, so that  $3 \times 2 \times 1$  or six permutative arrangements of these rotors is the maximum possible, since in this construction the rotors cannot be inserted in an "upside-down" position. In other types of such machines the rotors are made so that they can be inserted in either a "rightside-~~up~~" l.c. or <sup>in an</sup> "upside-down" position. This makes possible a maximum of  $6 \times 4 \times 2$  or 48 permutations of the three ~~rotors~~ rotors. Of course, if ~~there are~~ more than three rotors are available, from which a selection of three can be made, the possibilities increase very considerably. The stator at the left can be moved only by hand; the reflector at the right is fixed in this model of the ENIGMA. Depressing a key of the keyboard causes the first rotor to advance one step, thus changing the

circuit from the left-hand stator, thence through the rotors to the reflector, thence back through the rotors to the left-hand stator thus causing a second depression of the same key to produce a different equivalent. I won't take the time to tell you about how the rotors are caused to advance so that <sup>almost 17,000</sup> ~~over 17 thousand~~ letters can be enciphered before the window settings of stator and rotors return to their initial alignment. [The total number is not in this case  $26^3$  or 17576 but 16,900 ( $26 \times 25 \times 26$ ) for technical reasons which there isn't time to explain.] Power for the electrical circuits is provided by small dry cells in the box at the upper right in Fig. 31 (II).

The original ENIGMA enjoyed a fair degree of success in sales but it was by no means spectacular. When Hitler came into power, further sales were prohibited.

Suffice it to say that it became <sup>the</sup> ~~the~~ basis for machines used by the German Armed Forces in World War II.

In the U. S. <sup>in about 1910,</sup> a California inventor named <sup>made</sup> Hebern independently conceived a machine which he called an "electric code". <sup>Hebern's first patent application is dated ? and covered a</sup> ~~It was~~ similar to the ENIGMA but with some important differences: the cipher alphabets produced by it were not reciprocal and, moreover, a plain-text letter could represent itself in the cipher text. Hebern managed to avoid these two weaknesses by incorporating a switch plate which could be set one way for enciphering and deciphering another way. On the other hand, not as is the case of the

ENIGMA, the electrical currents made only one <sup>traverse</sup> ~~traverse~~ through the rotors <sup>rather than</sup> ~~rather than~~ <sup>traverse</sup> ~~traverse~~ into the rotors <sup>via one circuit</sup> ~~via one direction~~ and back through them <sup>via another circuit,</sup> ~~via another direction,~~ as is <sup>two,</sup> ~~two,~~ in encipherment the current went in one direction through the rotors and in <sup>via the same path.</sup> ~~in~~ decipherment in the reverse direction.

Here is a slide (Fig. 33) which shows Hebern's very first model, which he constructed for communications of the Ku Klux Klan. You will note that this model has but one rotor; also, the cipher machine is connected to an electric typewriter so that hand recording of results was no longer necessary. One additional virtue of the Hebern machine was that the wirings in the rotor were variable, a feature not incorporated in the ENIGMA rotors. Hebern interested our Navy in his

original patent application for Hebern's machine, in the Hebern, etc.

machine and built the 5-rotor model which you see in this slide (Fig. 34). The rotors are interchangeable and can be inserted "rightside-up" or "upside-down"; the internal

wiring could be readily changed. But this was not a printing machine. Power was

furnished by the small drycell seen at the upper left. The Navy was considering <sup>placed a purchase order for two such machines on 30 July 1924 and</sup>

purchasing a rather <sup>large</sup> number of <sup>them later,</sup> ~~these machines~~ and Lieut. Strubel, the Chief of the

Navy's Code and Signal Section of the Office of Naval Communications, asked me to

study the machine for its cryptosecurity. Navy had but two machines, neither of which

could be made available, so I induced the Chief / Signal Officer to buy a couple of them, <sup>for Army study. The order</sup>

<sup>was placed on 7 October 1924.</sup>

<sup>of the Army's</sup> ~~for me~~ The rotor wirings <sup>of the machines</sup> were altogether different from those of the Navy, a fact which

I discovered simply by asking Strubel to encipher a few letters on his machine, using

settings I specified. After some study I reported that in my opinion the security of the

machine was not as great as Navy thought. The result was a challenge, which I accepted.

Navy gave me ten messages put up on its machine and I was successful in solving them.

There isn't time to go into the methods used, but if you are interested you can find

them described in my brochure entitled \_\_\_\_\_.

Hebern built several more models for Navy and these had printing mechanisms associated

with them, but Navy dropped negotiations with Hebern when it became obvious that he

was not competent to build what Navy wanted and needed. Navy then established its own

cryptographic research and development unit at what is now known as the Naval Weapons

Plant in Washington. Army developed at the Signal Corps Laboratories at Fort Mammouth

a machine known as Converter M-134, and ~~there's~~ a slide (Fig. 35) showing what it

looked like. Army and Navy went separate ways in such work for a number of years but

finally, in 1938 or 1939, close collaborating brought as a result an excellent machine

which was developed and produced in quantity by the Teletype Corporation in Chicago.

This machine was distributed and used very successfully by all our Armed Forces from

1940 to the end of World War II and for some years thereafter. This was a rather