Nº 6

FINAL

# INTRODUCTION TO CRYPTOLOGY - VI

William F. Friedman

Space

<u>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, in the final analysis, COMSEC is really more vital to National Security than COMINT.</u>

This, the sixth and final lecture in this series on the history of cryptology, will be devoted to a presentation of the 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 firstly with the advances made in the production of more complex mechanical, electrical, and electronic cryptographic apparatus in order to increase or to facilitate greater cryptosecurity of our own cryptocommunications; and secondly with the concomitant advances in the production of more sophisticated mechanical, electrical and electronic cryptanalytic apparatus in order to speed up or to make possible the solution of enemy communications produced by these their increasingly complex cryptographic machines. These two phases are inter-related because, to use a short of simple analogy, cryptography and cryptanalysis represent the obverse and reverse faces of a single coin, and it would be nice if I could go into some detail in regard to these increasingly complex matters but security considerations prevent my doing so.

As to 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 quite but very interesting book entitled <u>A Soldier's Story</u>:[1]

[1] 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 presumptuous to amend General Bradley's remark butthis 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 histilities. 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 will add to what I then said. The committee began its work early 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 incident to an examination of 43 witnesses. In July 1946 the committee put out a final Report of 580 pages containing its findings, conclusions and recommendations. The Report was accompanied by a set of 39 volumes of testimony and exhibits. The Report was really not a single 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 acrimonious discussions and writings by those 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 lecture, however, it is an interesting fact that both the Majority and Minority Reports contain glowing tributes to the role played by COMINT before and during our participation in World War II. In my first lecture, (NSA Technical Journal, Vol. IV, No. 4, Oct 1959, p. 5), I presented a brief extract in this regard, taken from the Majority Report[2]; but here is what the Minority Report says on the subject:[3]

> 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 translati[redacted]pts, the i[redacted] furnished to those high [redacted] number of [redacted] which clearly indicated the growing resolve of the Japanese [redacted] on war before December 7, 1941.

Although references to COMINT abound in the Report of the Majority as well as in the Report of the Minority, there are also many references having to do with COMSEC in both Reports, as well as in the 39 accompanying volumes of testimony and exhibits. Some technical misconceptions with regard to those subjects are there, too, and I will only comment that it is quite comprehensible that there should be some on the part of laymen, but to encounter a serious one in a book by an experienced high-level commander in World War II is a bit disconcerting. Listen to this paragraph from a recent book by one such commander:[4]

> The argument has been made that we could not afford to let the Japanese know we had broken their code. But this argument against a Presidential warning does not hold water. It was not a mere matter of having broken a specific code; what we had done was to devise a machine which could break any (author's emphasis) code provided it was fed the right combinations by our extremely able and gifted cryptographers. The Japanese kept changing their codes throughout the war anyway. And we kept breaking them almost as a matter of routine.

I don't know where General Wedemeyer obtained his information about that wonderful machine he mentions. I imagine that there are many other persons who think there is such a machine because of all they hear and see about those marvelous "electronic brains" which are capable of performing such amazing feats in solving all kinds of problems, including mathematical ones. I daresay I won't be wrong in assuming that many of you do indeed wish there were such a machine [redacted]hat mentioned by General Wedemeyer. Nobody doubts that electronic digital computers can do lots of things in cryptologic research, and many persons entertain speculations as to the role they may play in their possible applications in connection with such research in future wars. But let's leave such speculations, interesting as they may be, and continue with our history of past applications. Let's first dispose of some comments in the COMINT area of that history not only on the events preceding the Pearl Harbor attack, but also on the ~~history~~ military, naval and air operations which ensued in the Pacific as well as in the European Theatres.

You will recall that in my first lecture I called to your attention an article which appeared in the 17 December 1945 issue of TIME magazine, and which was based upon a letter that the late General Marshall wrote to Governor Dewey, Republican candidate for President in the 1944 campaign. Here's how the two principals looked at the[redacted]r. 1). In the letter, which [redacted]n

Fig. 1

[2] The 79th Congress, 2nd Session, Senate Document No. 244, Washington: The Government Printing Office, 1946, p. 232.

[3] Ibid, page 514.

[4] Wedemeyer, General Albert C. Wedemeyer Reports, New York: Henry Holt and Company, 1958, p. 430.

27 September 1944, and was hand-carried by Colonel Carter W. Clarke, a high-level officer in Army G-2, to Governor Dewey, General Marshall begged the Governor to say nothing during the campaign about a certain piece of very vital information which had become known to the Governor, it having been "leaked" to him by persons unknown and unauthorized to disclose it. The information dealt with the fact that U. S. Government authorities had been reading Ja panese codes and ciphers before the attack on Pearl Harbor. The points which General Marshall wanted to convey were that not only was the "leaked" information true, but much more important were the facts 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. Government was still reading highly-secret Japanese messages in those systems, as well as highly-secret messages of other enemy governments. Therefore, it was absolutely vital that Governor Dewey not use the top secret information as political ammunition in his campaign.

After merely glancing over the first two paragraphs of the letter, Governor Dewey handed it back to Colonel Clarke with the comment that he did not wish to read any further, whereupon there was nothing for Colonel Clarke to do but return immediately to Washington. Here's a photograph of the Colonel (Fig. 2). Judging by the scowl on his handsome countenance I think it's possible that the picture was taken when he got back to his desk in the Pentagon. Well, General Marshall made certain changes in the opening paragraphs of the letter and again Colonel Clarke hand-carried it to the Governor, who then read the whole of it. In my first lecture I said that I might later give further extracts from TIME's account of this episode but there isn't time. Cap. Instead, however, I've put the whole account in an appendix to the present lecture. The Marshall-Dewey correspondence is so important in cryptologic history that I have deemed it useful to put the whole of it also in the Appendix.[6]

The information disclosed during the various official investigations of the attack on Pearl Harbor, so far as concerns the important COMINT achievements of the Army and the Navy before and after that attack, was classified information of the very highest security level, and the disclosures were therefore highly detrimental to our national security. Much has been written about them since the end of hostilities and although all that formerly top secret information is now in the public domain, fortunately very few details of technical

[6] See p. 00 [illegible]

significance or value can be found therein. Hints and even blunt statements about the great role played by COMINT in U. S. military, naval and air operations are found in books and articles published by U. S. Government officials and American officers, as well as by officers of the beaten Japanese, German, and Italian armed forces. Time at my disposal permits citing only a few examples.[6]

As regards disclosures by U.S. Government officials and officers, I can begin with those of the late Mr. Cordell Hull, who was Secretary of State at the time of the Pearl Harbor attack. In his memoirs are many references (over a dozen ~~dozen~~) to the contents of intercepted and solved Japanese Foreign Office messages.[7] The late Mr. Henry L. Stimson, Secretary of War at that time, makes clear references in his autobiography to COMINT successes and our failure to use them prior to the attack.[8] Dr. Herbert Feis, who was Mr. Hull's adviser on international economic affairs from 1937 to 1943,aand from 1944 to 1946 was Mr. Stimson's Special Consultant, has a good deal to say abtut the role played by "Magic" in a book written as a member of the Institute for Advanced Study, at Princeton.[9] Admiral Kimmel, one of the two commanders in Hawaii at the time of the attack, in defending himself in his book, cites many "Magic" messages.[10] And Major General Sherman Miles, head of G-2 at the time of the attack, has much to say about "Magic" in an article published in 1948.[11] As regards disclosures by former enemy officers, the following are of particular interest because they concern the Battle of Midway, which is considered the one that turned the tide of war in the Pacific from a possible Japanese victory to one of ignominious defeat:

[6] A good bibligraphical survey of items concerning the attack up to the year 1955 will be found in the following: Morton, Louis. "Pearl Harbor in Perspective," U.S. Naval Institute Proceedings, Vol. 81, No. 4, Whole No. 626, April 1955, pp.461-8.

[7] The Memoirs Of Cordell Hull, New York: The MacMillan Co., 1948, Vol. II, pp. 998,1013, 1035, 1055, 1056-7, 1060, 1065, 1068, 1074, 1077, 1087, 1092, 1095, 1096, 1099-1100.

[8] Stimson, Henry L., and McGeorge Bundy, On Active Service in Peace and War, New York: Harper & Brothers, 1947, pp. 391-4, 454-5.

[9] Feis, Herbert, The Road to Pearl Harbor, Princeton: The Princeton University Press, 1950, p. vii, and pp. 219-340, passim. (See index under "Magic" on p.350.)

[10] Kimmel, Husband E., Admiral Kimmel's Story, Chicago: Henry Regnery Co., 1954.

[11] Miles, Sherman, "Pearl Harbor in Retrospect," The Atlantic Monthly, Vol. 182, No. 1, July 1948, pp. 65-72.

If Admiral Yamamoto and his staff [Fig. 3] 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 [redacted]e United States [redacted]new of [redacted]o i[redacted]dway even be[redacted] sortie[redacted] A[redacted] 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.[12]

* * * * *

The distinguished American Naval historian, Professor Samuel E. Morison, characterized the victory of United States forces at Midway as "a victory of intelligence." In this judgement the author fully concurs, for it is beyond the slightest possibility of doubtthat 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. [redacted] [redacted]

¶ But it was a victory of American intelligence in a much broader sense than just this. Equally as important as the positive ~~advancements~~ achievements of the enemy's intelligence on this occasion was the negatively bad and ineffective functioning of Japanese intelligence.[12]

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." The author is, I think, a bit too severe on the Japanese intelligence organization. I say this because their cryptanalysts were up against much more sophisticated cryptosystems than they dreamt of, 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.

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 development and historical background in our 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, viz, (1) cryptosecurity, (2) transmission security, and (3) 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 further references to the other two components, or to the history of their development. 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 present 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: [redacted] [redacted]

[12] Midway, The Battle that Doomed Japan: The Japanese Navy's Story, by Matsuo Fuchida and Matasake Okumiya, U. S. Naval Institute Publication, Annapolis, 1955, pp. 131/and 232. Admiral Morison actually wrote: "Midway was a victory of intelligence breavely and wisely applied." See Vol. IV of his History of U. S. Navy Operations in the Pacific:" Coral Sea, Midway and Submarine Actions, May [redacted]t 1942." New York: [redacted]944, pa[redacted] [redacted]

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 occurence 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? What has it to do with COMSEC?

During our participation in World War II, the President of the United States, accompanied by many of his highest-level military, naval and civilian assistants, journeyed several times half-way around the world. He and they journeyed in safety--neither he nor they met with an "accident". Here's a Fig. 4 picture taken at the Casablanca Conference in January 1943 (Fig. 4). Imagine the disaster it would have been if the plane carrying this distinguished group had been shot down and lost in the Atlantic or the Mediterranean. On the other hand, in April 1943, Admiral Isoroku Yamamoto, Commander in Chief of the Combined Fleet of the Japanese Imperial Navy started out on what was to be just an ordinary inspection trip but turned out to be a one-way trip for him. Here's Fig. 5 a good picture of the Admiral (Fig. 5), who was the architect of the attack on Pearl Harbor. His death was announced in an official Japanese Navy communique 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." But some bright person--I think it was the late Jimmy Walker, when Mayor of New York City--who said that "accidents don't just happen--they are brought about." Jimmy Walker's comment was true in this case at least: Admiral Yamamoto did not die by accident; he died because our Navy knew the schedule of his trip down to the very last detail so that it was possible to set up an ambush with high degree of success. Here is the story as told in an interesting manner by Fleet Admiral William F. Halsey, U.S.N., in his book entitled Admiral Halsey's Story:[13]

> Q c I returned to Noumea 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.

[13] Admiral Halsey's Story, McGraw-Hill, New York, 1947, pp. 155-157.

> 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 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 then 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.]

Omit?

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 disillusioning statement but I can say that as a general rule the successes were attributable not to technical weakness in U. S. cryptosystems but to their improper use in the case of certain low-level ones, by unskilled, and improperly or insufficiently trained cryptographic clerks. I may as well tell you right now that this weakness in cryptocommunications 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:[14]

> This Arte of Cypheringe, hath for Relative, an Art of Discypheringe; by supposition unprofitable; but, as things are of great use. For suppose that Cyphars were well mannaged, there bee Multitudes of them which exclude the Discypherer. But in regarde of the rawnesse and unskillfulness of the handes, through which they passe, the greatest Matters, are many times carryed 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 many commanders have failed to realize how much valuable intelligence can be obtained and used from a study of the procedures used in the transmission of messages as well as from a study of the direction and flow of radio traffic, the call signs

[14] The Twoo 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 Clarks, in the Courts of Princess, is such that many times the greatest matters are committed to futile and weake Cyphers." (Gilbert Wats' translation, 1640, p. 270.)

of the transmitting and receiving stations, etc., all without solving the communications even if they were in cryptic form. Following are two paragraphs extracted 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:

German Army.) In the eastern theater, where there was offensive

l.c.

> Signal intelligence (i.e., communications intelligence or COMINT) was a chief source of information in the 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)

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 because the need for greater and greater speed of cryptographic operations became obvious in order 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 thus very soon 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 concentric circular rotating members such as cipher wheels, cipher disks, etc. A very early, perhaps the earliest picture of such a device appears in a treatise by an Italian cryptologist named Alberti, whose Trattati 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 (Fig. 6), but I won't take the time to explain it except to say that the digits 1, 2, 3, 4 were used to encipher code groups and to call your attention to the fact that the letters of the cipher or revolving alphabet were in mixed order. In Porta's book, first published in 1563 in Naples, there appear several cipher disks; in the copy which was given me as a gift by Colonel Fabyan, they are still in working condition. Here is a picture of one of them (Fig. 7). In this version the device uses 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 up anything new or even some improvements on the original Alberti or Porta disks but 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. IV of this series you were shown a picture of the cipher disk "invented" by Major Alber 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 (Fig. 8) and the explanation of the invention (Fig. 9). You may also remember Fig 9 that signalmen of the Confederate Signal Corps mechanized the old Vigenère 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 1910 to 1920, that is, during the period including our participation as a belligerent in World War I, was nothing but a white celluloid variation of the original Alberti parchment disk of the vintage of 1470 (except that it was even simpler than its progenitor, because in the latter the cipher alphabets produced were mixed alphabets whereas, in the Signal Corps disk, the Fig. 10 cipher alphabets are simple ~~reversed~~ standard sequences (Fig. 10). We all know that it generally takes a pretty long time to get a patent through the U. S. Patent Office, but ~~in 1924~~ the ancient device was patented in 1924 by S. H. Huntington Fig. 11 (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. Indication of word space, 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 sp" in the plain text.

It is interesting to note that in 1936, during the days when the German National Socialists were banned as an organization in Austria, the Nazis used this variation of the old disk--it had 10 digits on both the outer and the inner sequences for enciphering digits (Fig. 12). Fig. 12 2d ed p 298

The first significant improvement on the old cipher disk was that made by Sir Charles Wheatstone, in 1867, when he ~~who some time before 1879~~ invented a cipher device which he called The Cryptograph. He described it in a volume entitled The Scientific Papers of Sir Charles Wheatstone, published in 1879 by the Physical Society of London. Here is a picture of the Wheatstone~~'s~~ device ~~which is~~ in my private collection (Fig. 13). 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 can be disarranged in a mixed sequence. Two hands, like the hour and minute hands of a clock, were provided and they are under control of a differential gear mechanism, so that when the long or "minute hand" is advanced to make a complete circuit of the letters on the outer circle the short or "hour hand" advances one space or segment on the inner circle. In Fig. 13, for example, the plain-text letter G is represented by the cipher letter A, that is, $G_p = A_c$. If the long hand is now advanced in a clockwise direction for one revolution, $G_p$ will be represented no longer by $A_c$ but by $G_c$, the letter immediately to the right of $A_c$ on the inner circle. In encipherment the long hand is always moved in the same direction (clockwise, for example) and its aperture is placed successively over the letters on the outer circle according to 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 on 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. Thus, 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:

R E F E R E N C E
X Z Z Z B G Q A M, in which it will be seen that repeated letters in the plain text are represented by different letters in the cipher text. 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 again clockwise, until the hour hand points to the cipher letter in the plain-text letter which is seen through the aperture at the end of the long hand on the outer circle. Thus, in the case of the example given above the cipher letters XZAABGQAM will be found to represent the word (REFERENCE.)

During World War I, some time in 1917, the British Army rescuscitated 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 and the cipher letters. ~~simultaneously~~ When the single hand is turned, the inner circle of segments, which are made of a substance upon which letters may be written in pencil or in ink is advanced eccentrically and against a similarly-made outer circle of segments. 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 cryptocommunications 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 still at Riverbank. 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 about 1923.

Fig. 14

Some years later, and almost by sheer good fortune, I learned that a cipher machine was in the museum of small town in Connecticut named Hamden. I was interested and wrote to the 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 box upon its receipt and found a device, beautifully made and encased in a fine mahogany C maghony 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). There are good reasons to believe that 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 of 27 to 26 was now on the ratio 33 to 26. Thus, Colonel Decius Wadsworth, who was then the first Chief of Ordnance of the U. S. Army, had anticipated Wheatstone by over 60 years in this invention. He also anticipated the British Army cryptologists as World War 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 ~~the~~ the outer sequence, and I believe the inner one could also be disarranged but the picture does not clearly show this to be the case, so that I am 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.

Fig. 15

Fig 17

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 valiantly but unsuccessfully tried to get the French Army to adopt it. He included a description of his device, which he called his "Cryptographe Cylindrique" or "cryptographic cylinder," in a book published in 1901 in Paris.[15] He had, however, previously described his device in an article entitled "Cryptographe à 20 rondelles--alphabets (25 lettres par alphabet)," published in 1891.[16] In this device there is a central shaft on which can be mounted 20 numbered disks on the peripheries of which are differently mixed alphabets of 25 letters each. The disks can be assembled in some prearranged or key sequence on the shaft, from left to right, but they can be revolved thereon and then locked into position on the shaft by pushing in the locking disk at the extreme left. The first 20 letters of the plain text of a message are first aligned, as seen in Fig. 17 (JE SUIS INDÉCHIFFRABLE = "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 rows of letters, which are recorded then by hand on paper

[15] Les Chiffres secrets dévoilés.

[16] Comptes Rendus, Marseilles, Vol. XX, pp. 160-165.

Then the next 20 plain-text letters are aligned, one of the other 24 rows of letters selected and recorded, etc. To decipher a message, the disks having been assembled on the shaft in accordance with the prearranged or key sequence, one takes the first 20 cipher letters, aligns and then locks them into position ~~on the device~~, and then turns the whole cylinder, searching for a row of letters which form intelligible text. There will be one and only one such row, and the plain-text letters are recorded. Then the next 20 letters of cipher are aligned, etc.

Another French cryptologist, the Marquis de Viaris, soon showed how messages prepared by means of the Bazeries cylindrical cipher could be solved.[17] Maybe that is why Bazeries wasn't too successful in his attempt 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 is a picture of his very first model (Fig. 18), which he presented to me some time in 1923 or 1924. ~~(Fig. 18)~~. But I first 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. In meeting the challenge successfully (which brought a box of chocolates for Mrs. Friedman from Mrs. Hitt) I didn't use anything like what I could or might have learned

no space

a/R.c

[17] L'Art de chiffrer et de déchiffrer les dépêches secrètes, Paris, 1893, p. 100.

from de Viaris, 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 were on paper strips and the latter were glued to strips of wood, as seen in Fig. 19. 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 first 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. It is made of very heavy brass disks on the peripheries 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 beginnings (the first 25 letters) of a set of 25 messages enciphered by his device and alphabets. He also sent the same data to Major Yardley, in G-2. Nobody ever solved the messages, even after a good deal of work and even after Maugorgne 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 one of the rooms occupied in the old Munitions Building by the Office of Chief Signal Officer. Here is a picture of the beginnings Fig. 20 of the first six messages (Fig. 20). Mauborgne, when I chided him in the unfairness of his challenge messages, told me that he had not prepared them himself--he had an underling (Major Fowler was his name, I still remember it!) prepared 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 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 Fig 21 of it (Fig. 21). That device was standardized and used for at least 10 years in the U. S. by the 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 two pages of a holographic manuscript in the large collection of Jefferson Papers in the Library of Congress. It described his invention ~~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. Fig 22

It soon became apparent to both Army and Navy cryptologists that a great increase in cryptosecurity would be obtained if the alphabets of the M-94 device could be made variant instead of invariant. 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 only the final form of the one adopted by the Army, Strip Cipher Device Type, M-138-A (Fig. 23). This form used an aluminum base into which channels with overhanging edges were cut to hold cardboard strips of alphabets which could be slid easily within the channels. It may be of interest to you to learn that after I had given up in my attempts to find a firm which would or could make such aluminum grooved devices in quantity, Mrs. Friedman, by womanly wiles and cajolery on behalf of her own group in the U. S. Coast Guard succeeded in inducing or enticing one firm to make them for her. And that's how the first models of strip cipher devices made of aluminum by the extrusion process came about, and how the U. S. Army, by administrative cooperation on and inter-Service level and technical cooperation on a marital level, found it practical to develop and produce in quantity its Strip Cipher Device, Type M-138-A. This was used from 1935 to 1941 or 1942 by the Army, the Navy, the Marine Corps, the Coast Guard, et al, including the Treasury and State Departments. It was used as a back-up system even after the Arme-Services as well as the Department of State began employing much better and more sophisticated cipher machines of high speed and security. Fig. 23

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

inventor, who unfortunately committed sucide a few years ago, perhaps because the last model of his improved machine failed to impress professional cryptologists. 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 steel clock spring which drives the ~~rotating~~ rotatable platform 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 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 is advanced 1, 2, 3, 4 . . . 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 dessertation (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.

Fig 26

Tape at 102 //

Fig. 27

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-21. 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 discuss in detail the internal works which control the rotating elements and ciphering wheels, of which you(ll see a glimpse later, but I must show you the next step in the improvement of such apparatus, which made it possible to eliminate the really tedious job of recording, by hand on paper, the results of operation. This was done by means of associating a typewriter with the Fig. 28 crypto-component. Here is a picture (Fig. 28) which shows the assembly — the B-21 connected to a Remington electric typewriter, modified to be actuated by impulses from the crypto-machine. Of cour~~s~~se, it was natural that the next step would be to make the recording mechanism an integral part of the crypto-Fig. 29-A machine. This you can see in the next picture (Fig. 29-A), in which the four rotating members referred to in connection with Fig. 27 and which control the two commutators also mentioned in connection with [illegible] that figure are seen. The slide-bar mechanism in Fig. 29-B, at the right, is called the "cage" or "Barrel," and controls the displacements of the printing wheel, causing the proper letter to be printed upon the moving tape seen at the front of the machine.

Now we come to some very important new types of electric cipher machines first conceived and developed in Europe, but very soon thereafter, and probably independently, also in the U. S. In the crypto-component of these machines, the electrical paths between the elements representing the plain-text characters and those representing their cipher equivalents are constantly varied by multiple connection-changers within the crypto-component. In early European models of this type of machine the connection-changers consisted of a frame upon which insulated wires were mounted to connect in an arbitrary manner a series of contacts on one side of the frame to a similar number of contacts on the other side of the frame. This frame was slid between two fixed contact-bearing members, one on each side of the frame. By sliding the frame between the two fixed members, the paths between the opposite contacts on the latter could be varied as a whole set with a single movement of the sliding frame. A connection-changer Fig. 30-A of this sort is shown in schematic form in Fig. 30-A, where the sliding member 10, slides between fixed members 11 and 12, thus changing the electrical paths between the keyboard and the printing mechanism. The connection-changer 10 is moved to the left or right 1,2,3, ... positions, as determined by a cam mechanism. We won't go into this type of machine any further because it wasn't long before inventors saw the advantages of using,instead of slidable connection-changers, mechanisms performing a similar function but of a rotatable nature which we now call "electric rotors," and which rotate, usually step-by-step, between circular, fixed, contact-bearing members called "stators." Rotors and stators of this type are shown in schematic form in Fig. 30-B, there being a left-hand stator labeled 1, three rotors labelled 2a, 2b, 2c, and a right-hand stator labeled 3. The connections leading away from stator 1 toward the left go to the keys of the keyboard; those leading away from rotor 3 toward the right go to the magnets of the printer. About these elements we shall explain some details presently.

Fig 30-B

In Europe, the first machine using rotors and stators was that developed by a German firm, the Cipher-machine Compnay of Berlin, and was appropriately named the ENIGMA. Here's a picture of ~~It~~, Fig. 30-C, in which you see a keyboard, a set of eight rotors juxtaposed in line, or, as we now generally say, "juxtaposed in cascade," and a printer. This machine was apparently too complicated for practical usage and was superseded by a second model, which also printed and was also unsuccessful. One of the difficulties with these two models was that a multiple switch with many contacts to be made simultaneously was required in order to establish an operative encipher-decipher relationship, so that if in enciphering the letter $D_p$, for example, and the corresponding key on the keyboard is depressed, a cipher letter, say $F_c$, is printed, then on deciphering the letter $F_c$, and the corresponding key on the typewriter is depressed, the plain-text letter ~~D~~$_p$ will be printed. In this machine this could only be done by making the current for decipherment traverse exactly the same path through the rotors and stators that it had traversed in encipherment. This was the function of the multiple switch shown schematically in Fig. 30-D, in which a machine with only six characters (A to F) is depicted. In the left-hand circuit diagram, $D_p$ is being enciphered and produces $F_c$; in the right-hand circuit diagram $F_c$ produces $D_p$. But the switching mechanisms 4 and 4' in Fig. 30-D make things a bit complicated because they are within one switching member that operates in one of two positions, one for encipherment, the other for decipherment, and many contacts must be established in one fell swoop so to speak. I won't go into further details as to its construction because a clever inventor of that German firm came up with a new idea which greatly simplified matters, not only in regard to the crypto-component but also in regard to the indicating mechanism. We may quickly explain how the matter of ~~eliminating~~ simplifying the indicating mechanism was accomplished, namely, by eliminating the printer altogether and replacing it with a simple bank of flashlight type lamps. We'll

tr/

Fig 30-C

Fig 30-D

skip the third model of the ENIGMA, which was only a slightly simpler version of the fourth model, which is shown in Fig. 31-A. This one comprised a keyboard, a bank of indicating lamps, and a set of rotors and stators, but no printer.

Fig 31-A

In Fig. 31-A is seen the machine with its cover-plate down. At the front is the keyboard; above it, the indicator board, consisting of 26 lamps beneath glass disks upon which letters have been inscribed. Above the indicator board are seen four oval apertures with covers, through which letters can be seen. To the right of each aperture can be seen the peripheries of four metal scalloped wheels, the first being unmarked but the next three being labeled 1. A switch lever seen at the right can be set to encipher, decipher, or neutral positions. In Fig. 31-B is seen the machine with the cover-plate removed, exposing the internal crypto-component. Three rotors, labeled 4 in this figure, are seen, and affixed to them are the scalloped metal rings, which are not labeled. A fourth scalloped ring, labeled 11 in Fig. 31-B, is affixed to another rotor-like member labeled 8 in that figure. This member looks like an ordinary rotor in this picture but is really a stator of special construction to be described presently. Perhaps it would be useful at this point to show you what an ENIGMA rotor looks like and this can be seen in Fig. 31-C. In each of these rotors there is a circle of 26 equally-spaced contact pins on one face of the rotor (Fig. 31-C-I) and a circle of 26 equally-spaced contact surfaces on the other face (Fig. 31-C-II). Insulated wires connect the contact pins on one face to the contact surfaces on the other face, these connections being made in an arbitrary, systematic, or unsystematic manner, depending on certain circumstances into which we need not go. When the rotors are juxtaposed as seen in Fig. 31-C-III, the contact pins on one rotor are brought against the contact surfaces on the adjacent rotor, so that an electric current will traverse all three rotors via a certain path. The large scalloped rings are for setting the rotors in alignment manually when they are juxtaposed and rotated to form a portion of the key-setting (see E*Z*R in Fig. 31-C-III). The toothed metal ring seen in Fig. 31-C-I is associated with a cam mechanism so that ~~a~~ the rotor (I) will be advanced one step ~~when~~ the preceding rotor (II) has made a sufficient number of steps to permit a cam to fall into a notch at B in the top smooth ring of the rotor II. Sometimes a complete revolution will be necessary before this happens, depending upon the initial key-setting. The first rotor immediately to the left of the stator at the extreme right in

Fig 31-B

Fig 31-C

Fig

Fig. 31-B, however, always makes one step with each depression of the key on the keyboard. The advance of the rotors is similar to that of the wheels of a counter like that of the odometer on your automobile.

We come now to the matter of simplifying the crypto-component of the ENIGMA shown in Fig. 31-B to eliminate the multiple switching mechanism shown in Fig.30-B, without much loss in security (or so it would seem, at least). Let us see how this simplification was accomplished in the ENIGMA, by showing Fig. 31-D, in connection with the first ENIGMA model. For this purpose I show you now Fig. 31-D, in which the encipher-decipher circuitry is clearly seen in a machine having, for illustrative purposes, only three rotors, labeled 1,2,3, rotatable between two stators, the one on the left labeled 4, that on the right labeled 5. Stator $\overset{5}{4}$ is fixed or non-rotatable in this model, and it has 26 contacts on its left face, only two of which are shown. These contacts are connected fixedly to the keys of the keyboard and to the lamps of the lamp-board. Stator $\overset{4}{5}$ is rotatable, bu' only manually, and it has 26 contact surfaces on its right face, only two of which are shown. But in this stator 4 the 26 contact surfaces are inter-connected in pairs by 13 insulated wires passing through the member. Thus, a current entering one of the 26 contact surfaces on the right face of 4 goes through the stator and returns to one of the remaining 25 contact surfaces on the right face of 4. For this reason it is called a "reflector," and serves to return a current that has come from one of the 26 contacts on the fixed stator at the extreme right, then through the rotors and into the reflector via one path, returns through the rotors and back into the stator 5 via a different path, emerging at one of the 25 other contacts on the left face of the stator at the extreme right. This circuitry assures that in a particular setting of the machine, if $Y_p = Z_c$, for example, then $Z_p = Y_c$, that is, the cipher is reciprocal in nature. It also has as a consequence that no letter can be enciphered by itself, that is, $Y_p$, for example, cannot be represented by $Y_c$, no matter what the setting of the crypto-component is and this is true of all the other letters of the alphabet with regard to the ENIGMA.

If you like you may trace the path traversed by the current in Fig.31-D in encipherment and decipherment, where $Z_p = Y_c$ and $Y_p = Z_p$, but $Z_p$ cannot be represented by $Z_c$, nor can $Y_p$ be represented by $Y_c$. I have already told you briefly about how the rotors are advanced. In the ENIGMA shown, the total number of encipherments that can be made before the key-setting of the machine returns to its original setting, as seen through the windows I referred to a few moments ago when showing you the first picture of the fourth model ENIGMA, is 16,900, viz., $26^3 - 26^2$, and not $26^3$, for technical reasons I won't go into now.

Power for the electrical circuits is provided by small dry cells in the machine. This model enjoyed a fair degree of financial success, but when Hitler came into power further promotion and sales of the ENIGMA were prohibited. Suffice it to say that it became the basis for machines used by the German Armed Forces in World War II.

In the United States, in about the year 1910, a California inventor named Edward H. Hebern (Fig. 32) began to develop cipher machines but he was merely traveling along roads that had thus far led other inventors nowhere. In about the year 1918 he struck out along a new path in America. I don't know whether he independently conceived the idea of a machine using an electric rotor or had, in his research come across patents covering very recently invented European electrical cipher machines. At any rate, Hebern's first application for a patent covering a rotor machine which he called an "electric code," was filed on March 31, 1921, and a patent was issued on 30 September 1924. Here is a picture (Fig. 33-A) which shows the machine that he himself told me once many years ago he'd built for the Ku Klux Klan. You will note that the crypto-component had but one rotor, and like the early models of the ENIGMA it was associated with a printing mechanism, a typewriter operated electrically. Hebern's cipher system was also similar in nature with that of the first two ENIGMA models — a full reversing switch was essential since the electric current had to traverse exactly the same path in decipherment as it had in encipherment. I don't think that he ever conceived the idea of using a reflector; perhaps he was too late. At any rate, he never incorporated that idea in any of his machines. Moreover, I don't think he had any idea as to the cryptologic advantages and disadvantages of a crypto-component using a "single traverse" or "straight through" system of rotors, as compared ~~it~~ with one using a "double-traverse" or "twice-through" system of rotors with a reflector. But we won't go into that here, for it's a pretty involved piece of business.

32

Fig 33-A

But Hebern's rotors had a virtue not possessed by those of the ENIGMA machines, and not incorporated in the rotors of the latter, namely, the wirings of the rotors could readily be changed by the user of the Hebern machine, a feature of great importance in crypto-security. Fig. 33-B Hebern interested our Navy

Fig. 33-B

33-C in his ~~machine~~ 3-rotor model (Fig. 33-C), and as a result of conferences with Navy cryptanalysts he built the 5-rotor model which is seen is Fig. 34. Another very important security feature I have thus far failed to mention as regards the Hebern rotors was that they could be inserted in a "right-side up" or in an "upside-down" position in the machine, which could not be done with the ENIGMA rotors. The Navy liked the 5-rotor model, even though it was not a printing machine, assuming properly that this [redacted] added later on. Therefore, the Navy placed a purchase order for two such [redacted] in [illegible] July 1921 and [illegible] considering purchasing a rather large number of them later. Lieutenant Strubel, then Chief of the Navy's Code and Signal Section of the Office of Naval Communications, but now a retired Vice-Admiral, 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 for Army study. The order was placed on 7 October 1924. The rotor wirings of the Army's machines 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 Analysis of a mechanico-electrical cryptograph, Pt. I (1934), Pt. II (1935).

Tape at 1120, 1140

¶ 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 here's a 35 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 Forced from 1940 to the end of World War II and for some years thereafter. ~~This was a rather~~ In accordance with Navy nomenclature, it was designated as the ECM Mark II, ECM standing for "electric cipher machine;" in the Army it was designated as the SIGABA, in accordance with a nomenclature in which items of Signal Corps cryptographic material ~~are~~ were then given short titles with the initial trigraph SIG.

The ECM-SIGABA is a rather large machine requiring a considerable amount of electric power and much too heavy to be carried about by a signal operator performing field service. It was safeguarded with extreme care and under strictest security regulations during the whole period of World War II operations. None of our Allies were permitted even to see the machine, let alone have it. The British had their own electric cipher machine, which they called TYPEX. In order to facilitate inter-communication between U. S. and British forces, ~~an~~ adaptors ~~was~~ were developed so that, by use of the latter ~~in connection with the American ECM-SIGABA,~~ messages could be exchanged in cipher ~~with~~ between American and British units. ~~possessing a British machine called TYPEX, for which an adaptor cryptographically equivalent to the American one had been developed.~~ This system of inter-communication worked satisfactorily and securely.

Certain improvements in the method of usage and ~~certain~~ the development of special components, to be associated with the ECM-SIGABA for automatic decipherment by perforated tapes, were introduced during the war-time employment of these machines. But the SIGABA-ECM as orginally developed and produced became obsolete some years after the close of hostilities ~~where~~ when newer and better machines developed by NSA cryptologists and engineers replaced them, but not because there were ever any indications that messages enciphered on the machine had been deciphered by the enemy. As a matter of historical fact it may be stated that all enemy efforts to solve such messages were fruitless, and it is also a fact that no machines were ever captured by the enemy; nor were there ever any suspicions that a machine had been exposed to enemy inspection at any time. Once and only once were there any apprehensions in this regard, when, through a careless disregard of specific instructions, a truck and an attached trailer, in which this machine and associated material were housed, were stolen during the night when parked in front of the no headquarters of the 28th Division during the Battle of the Bulge. [Road blocks were immediately placed around the area and a great search was instituted by U.S. Army Engineers, during the course of which a river was diverted ~~and~~ the trailer, with all its contents intact, was found resting on the former bed of the diverted stream. The cipher, however, was not found; it had been "liberated". The episode terminated in court-martial proceedings with serious consequences to certain derelict commanders. It's hardly necessary to add and there were no further incidents of this sort.

Let me add that such apprehensions as were entertained at the time of this temporary loss of custody of the machine were based not upon the possibility that its usefulness was at an end but upon the fear that the Germans would make "Chinese copies" of it and thus be in a position to turn our very valuable weapon against us.

About five years before the SIGABA was put into service the Army's need for a small cipher machine for field use became obvious. The strip cipher system was not suitable for this purpose, nor was the Army's first keyboard operated electrical rotor ~~electrical~~ machine, Converter M-134, suitable, for reasons already indicated in connection with the SIGABA. The sum of $2,000 was allotted by the Army to the Chief Signal Officer for the development of a cipher machine small enough to be suitable for field usage but also affording adequate security. The funds were naturally turned over to the Signal Corps Laboratories at Fort Monmouth, New Jersey, for this development. The military director of the laboratories, spurning all proferred technical guidance or assistance from the Signal Intelligence Service and deciding that his staff had sufficient know-how without outside assistance, developed a machine which required no electricity, being all-mechanical. On its completion the model was sent to the Signal Intelligence Service for a cryptosecurity test. Two short messages were enciphered by the Chief of the SIS, using settings of his own selection. He then handed the messages and the model over to me as technical director and I turned them over to two of my assistants. The reason for turning over the model with the messages was that it must be assumed that under field conditions machines will be captured. One of the two test messages was solved in about 20 minutes; the other took longer - 35 minutes. This test brought an igominious end to the SCL development, brought about by the failure on the

part of the military Director of the SCL to recognize that cryptographic invention
must be guided by technically qualified cryptanalytic personnel. Unfortunately, all
the available funds had been expended on this unsuccessful attempt; none was left for
a fresh start on a development with technical guidance from the SIS. It was about
this time that a small mechanical machine which had been developed and produced in
quantity by a Swedish engineer in Stockholm named Hagelin was brought to the attention
of the Chief Signal Officer of the U. S. Army by a representative of the Hagelin firm.
The SIS was asked to look into it and as technical director I turned in an unfavorable
report on the machine for the reason that although its cryptosecurity was

if properly used,

theoretically quite good, it had a low degree of cryptosecurity if improperly used -

in cryptocommunications has demonstrated time and again of crypto material may

and practical experience had taught me that improper use ~~could~~ be expected to occur

now + then in the heat of battle. even with well-trained personnel, with insufficiently trained or careless

inexperienced [illegible] improper usage can occur

with sufficient frequency to jeopardize the security of ~~all~~ other messages enciphered by ~~the~~

a cipher

This is because the keying elements may be reconstructed

same setting of the machine whether correctly enciphered or not. This was because

from the solution of one or two improperly - enciphered messages and once reconstructed those elements may be employed

to decipher correctly enciphered one. This is particularly true of that category of cipher machine

the Hagelin machine operates on what is termed the key-generator principle; ~~so that~~ which

that is, such machines produce a long stream of keying characters, and

when two or more messages are enciphered by the same key stream or portions thereof,

In the case of the Hagelin machine, which from a key-generator

solution of those messages ~~is~~ is a relatively simple matter. Such solution permits

recovery of the settings of the keying elements so that the whole stream can be
produced and used to solve messages which have been correctly enciphered by the same

using the same key stream

key settings, thus making a whole day's traffic readable by the enemy. I cannot go
into details in this regard in this lecture. I tried to assure the CSO that my

rejection of the H machine (not was law) military

opinion was not motivated by "the NIH factor" but was over-ruled by my military
superiors, and properly so, because neither the SIS nor the SCL had developed anything
that was better than the Hagelin machine, or even as good, with all its mechanical
deficiences and cryptographic weaknesses taken into consideration. Accepting, though
somewhat reluctantly, the well-considered directive of the CSO, the SIS pointed out
where improvements could be made and the desired modifications were incorporated in the

[illegible] window [illegible] the key wheel

machine, which became known as Converter M-209. Over 100,000 of them were manufactured in 1942-1944 by the Smith-Corona Typewriter Company, at Groton, New York. Here's a
36-B slide (Fig. 36-B) showing the machine, which was extensively used by all our Armed
36-C Forces during World War II, and here's another (Fig. 36-C) showing its internal mechanism. It turned out that under field conditions the fears upon which I had based my personal rejection of the Hagelin machine proved to be fully justified - a great deal of traffic in it was solved by the Germans, Italians, and Japanese. If I was chagrined or suffered any remorse when I learned about the enemy successful attacks on M-209 traffic, those feelings were generated by my sense of having failed myself to think up something better than the M-209 despite the short-sighted attitude ~~undefensible conduct~~ of the military director of the SCL.

With the introduction of printing telegraph or teleprinting machines for electrical communications the need became pressing for a reliable and practical cryptographic mechanism to be associated or integrated with such machines. The first apparatus of
37 this sort in the U. S., shown in this photo (Fig. 37), was that developed by the American Telegraph and Telephone Co., in 1918, as a more or less simple but ingenious modification of its ordinary printing telegraph. First, a few explanatory words about the basic principles of the modern teleprinter may be useful. This principle employs what is called the "Baudot Code", that is, a system in which permutations of two different elements taken in groups of five are employed to represent characters of the alphabet. Curiously enough, Francis Bacon was the first to employ such a "code" way back in the early 17th Century, and I showed you the one he used, in Lecture No. 2. (see Fig. 25, p. 42, of NSA Technical Journal, Vol. V, No. 2, April 1960). These two elements in Bacon's "code" were <u>a</u>'s and <u>b</u>'s; he used but 24 of the 32 permutations available ($2^5=32$). For electrical communications the two elements may be positive and negative currents of electricity, or the presence and absence of current, the latter system being often ~~referred to as being~~

referred to as being composed of "marking" and "spacing" elements, respectively.

38 Here is a slide (Fig. 38) which depicts the Baudot or "5-unit code" in the form of a paper tape in which there are holes in certain positions transversely to the length of the tape. The holes are produced by a perforating mechanism; the small holes running the length of the tape are "feed-holes" by means of which the tape is advanced step by step. You will note that there are five levels on which the perforations appear. The letter A, for example, is represented by a perforation only on the 1st and 2nd levels, the 3rd, 4th and 5th levels remaining unperforated; the letter I is represented by holes in positions 2 and 3, no holes on the other three levels, etc. The English alphabet uses was 26 of the 32 permutations; the remaining 6 permutations are used to represent the so-called "stunt characters," which I will now explain. The third and fourth characters from the right-hand end of the tape are two permutations labeled "letters" and figures," respectively. These are equivalent to the "shift" and "unshift" keys on a typewriter keyboard, for "lower" and "upper" case. When the "letters" key is depressed, the characters printed are the 26 letters of the alphabet (all capital letters); when the "figures" key is depressed the characters represented are similar to those printed on a typewriter when the "shift" key is depressed. The second, third, and fourth permutations at the left-hand end of the tape are also stunt characters and represent "line feed", "space," and "carriage return," and they perform electrically in a teleprinter what is done by hand on a typewriter: "line feed" causes the paper on which the message is printed to advance to the next line; "space" does exactly what depressing the space bar on a typewriter does, etc; When there are no holes anywhere across the tape, the character is called a "blank" or "idling" character - nothing happens; the printer does no printing, nor is there any "stunt" fuctioning by the printer, but the tape merely advances.

In modifying the standard printing telegraph machine to make it a printing
the matter in a slightly different way, modify
telegraph cipher machine, or, to put the printing telegraph cipher machine the
American Telephone and Telegraph Company was fortunate in having at its disposal
23-year old (Fig. 39)
39 the services of a communications engineer named Gilbert S. Vernam, who conceived
and an automatic method for ciphering teleprinter communications. The principle and method
a brilliant principle. ~~That principle~~ turned out to be so useful and valuable, not only
in the U.S. but also internationally "Vernam principle," the
that it has come to bear his name and is ofte~~r~~n referred to as the "Vernam rule."
"Vernam, mod-2 addition," etc.
Vernam saw that if in accordance with some general but invariant rule the marking and spacing elements of a 5-unit code group were combined one by one with those of another 5-unit code group, which would serve as a keying group, and the resultant 5-unit group transmitted over a circuit and combined at the receiver with the same keying group in accordance with the same general rule, ~~20~~ 20 the final
conceived the idea early in 1918, or
resultant would be the original character. Vernam ~~extended his idea to make it~~
perhaps in late 1917. I have a copy of Vernam's circuit diagram dated and witnessed on 27 Feb 1918,
~~applicable to a cipher system for teleprinters and an application in Vernam's name~~
but the application for a patent thereon, with his name as inventor,
was filed in the U. S. Patent Office on 13 September 1918, and Patent No. 1,310,719
22 July 1919, covering
was granted on the invention entitled a "Secret Signaling System." ~~on 22 July 1919~~.

The following more detailed description of Vernam's patent on the foregoing cipher system is extracted from a paper written by one of the A. T. & T Company's engineers who was associated with Mr. Vernam at the time the invention was conceived and who a few years after retirement from that company, became one of NSA's consultants:

> This patent describes an "on-line" system, each character being enciphered, immediately transmitted, and in turn deciphered without delay at the receiving terminal. Thus, characters of a message in perforated tape form are automatically combined with other or key characters, "preferably selected at random," also in perforated tape form, and used only once to produce a third group of characters which are transmitted over the circuit. At the receiver an identical group of key characters is used to provide signals for combination with the arriving signals, character by character, to produce the original message. The combining rule for these operations disclosed in the patent was one in which like code elements produced "spaces" and unlike elements "marks", as shown below.

20 - In this system which uses only two different symbols or elements, the so-called "binary code," the combining rule is its own inverse.

[illegible] - Parker, L. D. "Recollections Concerning the Birth of One-Time Tape and Printing-Telegraph Machine Cryptography." NSA Technical Journal, Vol. I, No. 2, July 1956, pp. 103-114.

| | |
|---|---|
| Message character | + + - - - |
| Key | + - - + + |
| Cipher Character | - + - + + |
| Key | + - - + + |
| Deciphered Character | + + - - - |

It was, however, recognized that the opposite rule would work equally well, two like elements when combined giving a mark and two dissimilar elements a space, thus:

| | |
|---|---|
| Message Character | + + - - - |
| Key | + - - + + |
| Cipher Character | + - + - - |
| Key | + - - + + |
| Deciphered Character | + + - - - |

Other patent applications filed and later granted described the corresponding - "off-line" - method, where the encipherment is recorded in punched tape form for later transmission, but a single one-time random key-tape is used; the simultaneous use of of two endless key tapes, as described below; a scheme for eliminating "stunt" combinations - "bells", "line-shift" and the like - and many other ideas and devices in this field.

Here is an extract from a paper by Vernam himself, which in simple language explains how his invention worked in a system developed during World War I for use of the Signal Corps, U. S. Army:[22]

CIPHER MACHINE - METHOD OF OPERATION

The messages are first punched in a paper tape by means of the keyboard perforator [Fig. 39 of this lecture]. . . .

The cipher "key" may take the form of another tape of similar form having characters punched in it at random and with every tenth character numbered, so that the tape may be set to any designated starting position. The key tapes are prepared in advance, the original key being perforated by hand, as by working the keyboard at random, additional copies being made automatically by the machine.

The message tape is passed through a unit known as a transmitter, where the holes in the tape serve to control the positions of five contact levers, each of which makes contact with either of two bus bars. The key tape controls the contacts of a second tape transmitter. The contacts of the two transmitters are connected to a set of five magnets or relays as shown in Figure 9 [Fig. 40 in this lecture]. Each magnet will be energized if the correspondingly numbered contacts of the two transmitters are against opposite bus bars, but not if they are making contact with similar bus bars. In the diagram, contacts 1 and 2 of the messgge transmitter, are against the left or positive bus bar, this setting representing the letter "A". Contacts 1, 4 and 5 of the key transmitter are against the positive bus bar, representing the letter "B" in the printer code. This will energize magnets 2, 4 and 5, which combination represents the letter "G".

Fig. 40

All of the possible combinations resulting from various characters in the two tapes might be shown in a cipher square which would have 32 characters on a side instead of 26 [as in the case of the ordinary Vigenère Square].

See/

The characters of the cipher messages, formed in this way, may be recorded as perforations in a third tape. For this purpose a "machine perforator" is used. This device is similar in many respects to a keyboard perforator and is shown in Figure 10 [Fig. 41 in this lecture]. The tape, from a reel on the top of the machine, passes through the punch block at the front left corner or the machine. Here it passes under a die plate and over a group of six punches, which may be forced up through the tape by the action of an electromagnetic hammer. Five of these punches are too short to be acted on directly by the hammer and are pushed through the tape only when an individual "selecting finger" is interposed between the punch and hammer. The five selecting fingers are actuated by five magnets which may be controlled by the relays shown in Figure 9 [40]. A ratchet-operated star-wheel feeds the tape forward after each character has been punched.

[22] Vernam, Gilbert S. "Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraph Communications," a paper presented at the Midwinter Convention of the A. I. E. E., New York City, 8 - 11 February 1926.

| | |
|---|---|
| Message character | + + - - - |
| Key | + - - + + |
| Cipher Character | - + - + + |
| Key | + - - + + |
| Deciphered Character | + + - - - |

It was, however, recognized that the opposite rule would work equally well, two like elements when combined giving a mark and two dissimilar elements a space, thus:

| | |
|---|---|
| Message Character | + + - - - |
| Key | + - - + + |
| Cipher Character | + - + - - |
| Key | + - - + + |
| Deciphered Character | + + - - - |

Other patent applications filed and later granted described the corresponding - "off-line" - method, where the encipherment is recorded in punched tape form for later transmission, but a single one-time random key-tape is used; the simultaneous use of two endless key tapes, as described below; a scheme for eliminating "stunt" combinations - "bells", "line-shift" and the like - and many other ideas and devices in this field.

Here is an extract from a paper by Vernam himself, which in simple language explains how his invention worked in a system developed during World War I for use of the Signal Corps, U. S. Army:[22]

CIPHER MACHINE - METHOD OF OPERATION

The messages are first punched in a paper tape by means of the keyboard perforator [Fig. 37 of this lecture]. . . .

The cipher "key" may take the form of another tape of similar form having characters punched in it at random and with every tenth character numbered, so that the tape may be set to any designated starting position. The key tapes are prepared in advance, the original key being perforated by hand, as by working the keyboard at random, additional copies being made automatically by the machine.

The message tape is passed through a unit known as a transmitter, where the holes in the tape serve to control the positions of five contact levers, each of which makes contact with either of two bus bars. The key tape controls the contacts of a second tape transmitter. The contacts of the two transmitters are connected to a set of five magnets or relays as shown in Figure 9 (Fig. 40 in this lecture). Each magnet will be energized if the correspondingly numbered contacts of the two transmitters are against opposite bus bars, but not if they are making contact with similar bus bars. In the diagram, contacts 1 and 2 of the message transmitter, are against the left or positive bus bar, this setting representing the letter "A". Contacts 1, 4 and 5 of the key transmitter are against the positive bus bar, representing the letter "B" in the printer code. This will energize magnets 2, 4 and 5, which combination represents the letter "G".

40
Fig 9 of Vernam
my Fig. 40 here

All of the possible combinations resulting from various characters in the two tapes might be shown in a cipher square which would have 32 characters on a side instead of 26 (as in the case of the ordinary Vigenère Square).

The characters of the cipher messages, formed in this way, may be recorded as perforations in a third tape. For this purpose a "machine perforator" is used. This device is similar in many respects to a keyboard perforator and is shown in Figure 10 (Fig. 37 in this lecture). The tape, from a reel on the top of the machine, passes through the punch block at the front left corner of the machine. Here it passes under a die plate and over a group of six punches, which may be forced up through the tape by the action of an electromagnetic hammer. Five of these punches are too short to be acted on directly by the hammer and are pushed through the tape only when an individual "selecting finger" is interposed between the punch and hammer. The five selecting fingers are actuated by five magnets which may be controlled by the relays shown in Figure 9 (40). A ratchet-operated star-wheel feeds the tape forward after each character has been punched.

See

[22] Vernam, Gilbert S. "Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraph Communications," a paper presented at the Midwinter Convention of the A. I. E. E., New York City, 8 - 11 February 1926.

The cipher tape prepared in this way is unintelligible in form and may be ~~sent to the receiving~~ station by messenger or by mail, or if desired, it may be transmitted by wire or radio and reproduced by another machine perforator at the receiving point. The cipher tape is there run through the message transmitter, where its characters combine with those of a duplicate key tape to reproduce the original message, which will be printed out in page form ~~and in~~ plain text".

[redacted]

## LENGTH OF KEY TAPE

[redacted]

With the system as described above, the key tape must be at least as long as the sum of all the message tapes used with it, as the messages will lose their secrecy to some extent if the key tape is used repeatedly. The use of a short repeating key may give sufficient secrecy for some uses, however.

A roll of tape 8 inches in diameter contains about 900 feet of tape and would serve to encipher about 18,000 words counting five printed characters and a space per word, without repeating the key. If sent at an average speed of 45 words per minute this number of words would require 400 minutes or nearly 7 hours to transmit.

In order to reduce the amount of key tape required for handling large amounts of traffic, the "double key" system was devised.[23] In this system two key tapes are used, the ends of each tape being glued together to form a loop preferably about seven feet in circumference. The tapes should differ in length by one character or by some number which is not a factor of the number of characters in either tape. A separate transmitter is used for each tape, and the characters of the two key tapes are combined, by a method similar to that shown in Figure 9, with those of the message tape to form the cipher message. [40]

The result is the same as though the two key tapes were first combined to produce a long single non-repeating key, which was later combined with the message tape. This long, single key is not, strictly speaking, a purely random key throughout its length as it is made up of combinations of the two original and comparatively short key tapes. The characters in this key do not repeat in the same sequence at comparatively short regular intervals, however, as would be the case if only one key tape loop were used.

The number of characters in this equivalent single key is equal to the product of the number of characters in the two tape loops, and may easily exceed 600,000 before any part of the key begins to repeat. If proper care is taken to use the system so as to avoid giving information to the enemy regarding the lengths of the two key tape loops or their initial settings and to avoid the possibility of ever re-using any part of the resultant single key, this system is extremely difficult to break even by an expert cryptanalyst having a large number of messages and full knowledge of the construction of the machine and its method of operation.

The foregoing double-key-tape system was placed into operation in 1918, on three start-stop circuits which were used for intercommunication among four stations serving Washington, New York, Hoboken and Norfolk, and which according to Parker [see footnote 21 above] "continued in operation for many months, even after the end of the war." In addition, a Signal Corps Company was organized to go to Europe with new equipment for installation of printing-telegraph circuits in France. This Signal Company was about ready to sail when the Armistice was signed November 11, 1918.

Upon my return to Riverbank in April 1919, after being demobilized, I became an interested party in an rather warm argument conducted by letters exchanged between Colonel Fabyan, the Chief Signal Officer, the Director of Military Intelligence, and the War Department, regarding the cryptosecurity of the cipher printing telegraph system as used by the Signal Corps. The argument ended by meeting successfully

[23] By L. F Morehouse, an AT&T Co. equipment engineer. See U.S. Patent No. 1,356,546, "Ciphering System," granted 26 October 1920. —W.F.F

~~[illegible] tantamount to~~ a challenge by the Signal Corps to prove Fabyan's contention. The challenge consisted in sending Fabyan, on 6 October 1919, and requesting him to solve ~~by solving~~ the cipher tapes of about 150 messages selected from one day's traffic in the system. On 8 December 1919 Fabyan sent a telegram to the Chief Signal Officer notifying him that solution had been accomplished. In order to prove that this was true I sent I wrote a monograph on the solution, consisting of a basic paper of 21 typewritten pages, an Addendum 1 of 10 pages, ~~and~~ Addendum 2 of 25 pages and an Addendum 3 of six pages; a copy of each of these was sent to Washington, ~~together~~ ~~with~~ a perforated cipher-message tape to each of the offices named above. In order to decipher these messages the Chief Signal Officer had to use his own key tapes, thus proving that not only had Riverbank solved the system but had recovered both key tapes which had been employed in enciphering the challenge messages, so that Riverbank was in a position to produce the plain text of any of the latter on request, if further proof of solution was needed or desired. The solution was accepted with mixed feelings in Washington, especially on the part of Brigadier General Marlborough Churchill, the Director of Military Intelligence, who had ~~hastily~~ signed a letter to the Chief Signal Officer, dated 8 August 1918 and prepared by ~~Major~~ Capt. Yardley, to the effect that the cipher system in question ~~was~~ "is considered by this office to be "absolutely indecipherable."[22] General Churchill had the duty and courtesy ~~of writing~~ to write a congratulatory letter to Colonel Fabyan, dated 24 March 1920, the final paragraph of which is as follows:

> Your very brilliant scientific achievement reflects great credit upon you and your whole personnel. It would be impossible to exaggerate in paying you and Riverbank the deserved tribute for this very scholarly accomplishment.

The paper by Mr. Parker (see footnote 21) closes with the following final paragraph:

> Perhaps some day Mr. Friedman will tell of the part that he and the Riverbank Laboratories played in the cryptanalytic phase of this development.

Mr. Parker was not aware of the fact that what he suggested had not only been done once, but twice. The first time was immediately after the solution, and copies of the write-up mentioned on page 00 had been sent to Washington but they had met the fate that often happens to documents of limited or special technical interest--complete disappearance in the voluminous files of bureaucracy. The second time was soon after the

[22]

22

The letter states: "The mechanical means of enciphering messages with an arbitrary, meaningless running key of 999,000 letters, provided no two messages are enciphered at the same point on the tape as explained to Major Mauborgne, Signal Corps, and Captain Yardley, Military Intelligence Branch, by officials of the American Telegraph and Telephone Company [sic! The name is the American Telephone & Telegraph Company.], is considered by this office to be absolutely indecipherable."

end of hostilities of World War II, when it was discovered that a certain outfit I won't name was using the double-tape keying system for its teleprinter communications. I rummaged through my own files and uncovered the handwritten manuscript of certain parts of what I had written at the close of the successful solution of that system while at Riverbank. My second write-up is a classified document, dated 21 July 1948 the sub-title of which is "Can Cryptologic history repeat itself?" It is possible that this write-up can be made available to those of you who are interested in reading it, if proper authority grants permission.

Mr. Parker's paper (see footnote 21 above) devotes a good deal of space to the contention that the only reason why the double-tape keying method was adopted was that the Signal Corps and specifically its representative, Colonel Mauborgne, "complained about the difficulties that might be experienced in the preparation and distribution of one-time random key tapes, and seemed inclined to disapprove of the proposed system because of these difficulties. Since the systems, when properly used, seemed obviously to be one which gave absolute secrecy, a discussion arose on the value of the system and on methods which might be devised for the production and distribution of long one-time key tapes having characters arranged at random." Parker points out that the original method of use contemplated the use of long tapes of this nature and that he and his associates felt that the problem of producing and distributing long tapes "while presenting a challenge, was not impractical." I am glad to admit that they were right, because during World War II and for years afterward tapes of this nature were produced by special machinery (in some cases as many as five copies being perforated and the sections numbered automatically in a single operation). Distribution of and accounting for the tapes proved practical, too, and aside from an occasional error involving the re-use of a once-used tape, absolutely secure inter-communication by radio printing telegraphy was assured and was used between and among large headquarters where the volume of traffic justified the use of this equipment. The principal advantage was the simplicity of crypto-operations--no rotors to be set, no settup of rotors to be enciphered, no checking of encipherment by deciphering the message before transmission, etc.

The A.T. & T. Company Printing Telegraph Cipher equipment; purchased by the Signal Corps were withdrawn soon after Riverbank proved the double-key-tape system insecure. The machines went into storage, when in due course most of them were dismantled. But after I left Riverbank at the end of 1920 and had joined the Chief Signal Officers' staff in Washington, I induced the Chief Signal Officer to rescusitate two of equipments. These I employed, believe it or not, in compiling codes, called Division Field Codes, for use in training or in emergency. I won't undertake to explain how I performed this stunt, for it was a stunt, but it worked very successfully. The codes were duly printed, issued and used until there was no longer any need for codes of this type.

Cipher printing telegraphy was placed upon the shelf and more or less forgotten by Signal Corps communications engineers from 1920 until soon after Pearl Harbor. Although beginning about 1938, Mr. Frank B. Rowlett, one of my associates, and I kept urging that there was or would be real need for new and improved machines for protecting teleprinter communications, there was not only a complete lack of interest in such apparatus, but what was perhaps a more important factor in the failure to continue work in this field was the lack of Signal Corps funds for research and development for such work. However, the leading members of the S. I. S. maintained a theoretical cryptanalytic interest in such equipment and in 1937 there came an opportunity to test such theories as were developed by them when a machine produced by the International Telephone and Telegraph Company evoked the interest of the Department of State as a possible answer to the needs of that Department for rapid and secure cryptocommunications by radio. The Secretary of State requested the Secretary of War to study the machine, which ~~was to be associated with a standard teleprinter, and to study it only~~ had to be used with a standard teleprinter, and to study it only from the point of view of security. For this purpose messages enciphered by the Chief of the Communications and Records Division of the Department of State were provided. 41-A 41-B ~~Here are two pictures of the teleprinter attachment, Fig. 41-A, and 41-B.~~ Here are two pictures of the teleprinter attachment, Fig. 41-A, a general view and Fig. 41-B, an internal view of its mechanism. It is a source of satisfaction to be able to tell you that the S. I. S. quickly solved the test messages and therefore reported that the machine was quite insecure; but it is with much regret that I must now tell you who invented and developed the machine. It was a retired officer of the Signal Corps and none other than my old friend Colonel Hitt. I was as embarrassed to tell him about the results of our test as he was to force himself to listen to what I had to say about the inadequacies of his brain child. As is so often the case, when a competent technician has to neglect his technical studies because of the pressure of administrative duties, he unfortunately finds it very difficult to keep abreast of new developments and progress in a field in which he was at one time an expert. The I. T. & T. Company having spent a great deal of money on the development of a machine which hardly presented any room at all for improvement, because the principles underlying it were so faulty, dropped further work on it. Colonel Hitt, I am glad to say, readily survived the disappointment and was well enough in 1942 to be able to return to active duty during World War II and retired a second time at the end of hostilities. He lives a quiet life now, on a small farm near Front Royal, Virginia.

Our more or less sudden entry into World War II, after 7 December 1941, immediately brought a great need for cipher printing telegraphy, especially for radiocommunication but there was no apparatus for it whatever--not a single one of those A. T. & T. Company machines of 1918-1920 was in existence. But the S.I.S. did have drawings in readiness, and the development of the machines was given as a priority task to the Teletype Corporation, because that firm had proved that it had the necessary know-how when it produced the SIGABA-ECM's for us. Navy had less need for cipher printing telegraphy than Army becuase the use of printing telegraphy by radio was then not practicable for ships at sea. However, Navy did have a need for such apparatus for its land communications and joined Army in the procurement ~~development~~ thereof. The machines were produced with ~~a~~ remarkable speed by the Teletype Corporation. Most of them were allotted to Army, a few to NAvy. The Army called the machine the SIGCUM; the Navy called it CSP-1515. Under heavy use in servie e, improvements were made both in regard to mechanical and electrical features and in regard to methods of keying, the use of indicators, etc. But I must tell you that before those machines became available in quantity there was only one recourse: we went back to the use of the double-key-tape method using standard teletype apparatus. The cipher was practically the same as it was in 1920 but we had safer methods of key-tape production and indicators for their use. The S.I.S. and the equivalent unit in Navy were not happy because operator's errors left messages open to solution, so that when the new cipher machines were ready they were pleased into service as soon as possible, priority being given to circuits with heavy traffic.

Cryptographic equipments of the foregoing type fall in the category of apparatus for protecting LITERAL cryptocommunications because the latter employ letters of the alphabet; but apparatus for protecting CIFAX transmissions, that is, picture or facsimile transmissions, and apparatus for protecting CIPHONY transmissions, that is, telephonic communications, were also developed. But there isn't time to go into details with regard to machines and apparatus for these last two categories of crypto-equipments although the history of their development is rather fascinating and very important. But I just cannot refrain from adding that in every case except one the apparatus was produced by commercial research and development firms with~~out~~ direct guidance from the cryptologists of the Army and the Navy. The one exception is, I believe, in the case of the extremely high security ciphony system and equipment developed and built by the A. T. & T. Company. It was called SIGSALLY. There were six terminals, each of which cost over $1,000,000. But NSA cryptologists and engineers have produced smaller and better equipments based upon SIGSALLY principles and such equipments are bound to play extremely important roles in any wars in the future.

So much for the history of the developments and progress in cryptographic apparatus at this point. I shall return to that phase of cryptologic history before the close of this lecture. Right now I shall say a few words about the history of the developments and progress in cryptanalytic apparatus.

The solution of modern crypto-communication systems has been facilitated and, in some cases, made possible only by the invention, development, and application of highly specialized cryptanalytic machinery, including apparatus for intercepting and recording certain types of transmissions before cryptanalysis can even be undertaken. One must understand the basic nature of the problem which confronts the cryptanalyst when he attempts to solve one of these modern, very complex cryptosystems. First of all he must be given the crypto-communications in a form which makes them visible for inspection and study. Usually they are characters (letters or numbers) in the case of literal communications, or they are electrical signals of a recordable type in the case of cifax or ciphony communications. Next he must have available to him instrumentalities tht will assist him in his analytical work, such as machinery for making frequency counts, comparisons of sequences, etc., and this, in the case of complex systems, must be done at high speed. Cryptanalysis of modern cryptosystems requires testing a very great number of assumptions and hypotheses because sometimes astronomically large number of possibilities, i.e., permutations and combinations must be tested one after the ~~cipher~~ other until the correct answer is found. Since the advent of high-speed machinery for such purposes, including electronic digital computers about which so much is being heard and read nowadays, the cryptanalyst isn't discouraged by these astronomically great numbers of possibilities.

Perhaps long before my time cryptanalysts in Europe discovered that the use of sliding strips of paper could sometimes facilitate reaching a solution to a cryptanalytic problem, but so far as I am aware the very first cryptanaltyic aid made in 42 the U. S. is the one shown in Fig. 42 , which is a picture of what I made at Riverbank and which I called the Polyalphabet. It was useful in solving ciphers which today are regarded as being of the very simplest types. When I came to Washington after leaving Riverbank I wasn't troubled by a plethora of ideas for cryptanalytic aids--I was pre-occupied with devising and inventing cryptographic aids and machines. But I did now and then develop and try out certain ideas for cryptanalytic aids, frequency counters, comparison or coincidence machinery, and the like. Why didn't I think of IBM machines? I did, but what good did that do? Did the Signal Office have any such machines--or even one dollar for their rental? You know the answer to that without my spelling it out. There wasn't any use even in suggesting that IBM machines could be of assistance to me--remember, now, that I'm talking about the years from 1921 to 1933, and in the last-named year we were in the depths of a great economic depression. But one day in the summer of 1934 I learned by a devious route ~~that~~ (Army and Navy were not then sharing secrets) that the Navy Code and Signal Section had some IBM machines or two, and my chagrin was almost unbearable. Not long afterwards I learned that a certain division of the Office of the Quartermaster General in the Munitions Building had an IBM installation which had been used for accounting purposes in connection with the C.C.C--the Civilian Conservation Corps, established to provide work and subsistence for young men who could find no jobs in the depression. I also learned that a new officer had just been assigned to head that particular division--

and that he just had no use for the new-fangled ideas of his predecessor and wanted to get rid of those nasty IBM machines. But the contract with IBM still had some months to run before the lease expired and either the machines would sit idle or the Government would lose money by terminating the contract before the due date of expiration. This annoyed me, but it also gave me an idea. I wrote a memorandum

43 and here's a picture of it (Fig.43). I'll read you what it says:

30 October 1934

> Major Akin: In many years service here I have never once "set my heart on" getting something I felt desirable. But in this case I have set my heart on the matter because of the tremendous load it would lift off all our backs.
>
> The basic idea of using machinery for code compilation is mine and is of several year's standing. The details of the proposed system were developed in collaboration with Mr. Case, of the Int. Bus. Machines Corp.
>
> I regard this as one of my most valuable contributions to the promotion of the work for which we are responsible.
>
> Please do your utmost to put this across for me. If you do, we can really begin to do worthwhile cryptanalytic work.

Attached to the memo was a brief explanation amounting to what I've told you about that IBM installation in the Office of the Quartermaster General. Note that I placed the emphasis upon the burden that would be lifted from cryptographic work by using the IBM machinery, thus leaving more time for cryptanalytic work. This was because the responsibilities of the S.I.S. for cryptanalytic operations were at that time restricted purely to theoretical studies. Studies on cryptanalytic work on foreign cryptosystems had been a responsibility of G-2 of the General Staff until 1929, when that responsibility had been transferred to the Chief Signal Officer and the Signal Corps in the year named. But the Chief Signal Officer had very little money to use for that purpose, and, besides that, the Army Regulation applicable thereto specifically restricted cryptanalytic operations on foreign communications to wartime. And, more to the point, was the fact that there was no material to work on even if funds were available, because the Army had at that time no intercept stations whatever, anywhere in or outside the U. S. But that's another story and I'll proceed to the next point, which is that my memo to Major Akin produced results. Just a half √ √ month after I wrote and put it in his "In" basket I got the machines moved from the Office of the Quartermaster General to my own warren in the Office of the Chief Signal Officer! That memo must have been potent magic.

Once having demonstrated their utility to the Chief Signal Officer the almost prematurely terminated contract with IBM was renewed--and soon expanded. I don't know how we could have managed without such machines during World War II. Here's 44 a picture (Fig.44) of one of two whole wings in one of our buildings at Arlington Hall filled with IBM machines--the biggest installation in the world atthat time.

We built or had built for us by IBM and other concerns adaptors to work with standard IBM machines; we constructed or had constructed for us by commercial firms highly specialized cryptanalytic apparatus, machines and complex assemblies of components. Under war-time pressures fantastic things were accomplished and many were the thrills of gratifying achievement when things that just couldn't be done were done--and were of high importance in military, naval and air operations against the enemy.

Even were time available I couldn't show you pictures of some of the high-class gadgets we used; neither is it permissible to say more than I have already said about them, even though it is no longer a deep secret that electronic computers are highly useful in cryptologic work. For example, here is a paragraph (Fig. ) taken from a Russian book entitled

and below it is what it says in English.

To the layman the exploits of professional cryptanalysts, when those exploits come to light as, for example, in the various investigations of the attack on Pearl Harbor, are much more fascinating than those of cryptographers, whose achievements in their field appear in comparison to be dull or tedious to thelayman. But long consideration of the military importance of COMSEC as against COMINT leads me to return to something I mentioned at the very beginning of this lecture, when I made a statement to the effect that cryptography and cryptanalysis represent the obverse and reverse faces of the same single coin. In closing this lecture I will expand that statement a bit, and in so doing perhaps formulate a dictum which we may call the law governing the minting and usage of the cryptologic combat coin. It would run something like this:

When an officer is selected to command a fighting unit, an efficient appointing authority gives him and entrusts into his care a top secret, magic talisman of great potency, a coin which is called his cryptologic combat coin, and which, as is usual in the case of all but trick coins, has two faces, a COMINT face and a COMSEC face. When given to him that coin should be in mint condition, it should be bright and shiny on both faces, and he should strive his utmost to keep them both that way. If, to begin with, he is given a coin that is tarnished a bit on both faces, he is really starting out with a great handicap, no matter how good he and his forces are in respect to size, equipment, training and ability. If he keeps only the COMINT face bright and shiny, he stands a good chance of winning a battle even if his forces are inferior in size, etc., compared with those of the enemy. But if he lets the COMSEC face of his coin become dull from indifference, carelessness, or ignorance, he will almost surely lose the battle, even if his forces are superior in size, etc., compared with those of the enemy.

As a remarkable example of the validity of the foregoing dictum, an example that comes directly from the two Japanese Navy officers who wrote Midway: The Battle that Doomed Japan (see footnote 12 above)let me quote the initial paragraphs of the Preface to their book (p. xiii) :

> For Japan, the Battle of Midway was indeed a tragic defeat. The Japanese Combined Fleet, placing its faith in "quality rather than quantity," had long trained and prepared ~~for~~ to defeat a numerically superior enemy. Yet at Midway a stronger Japanese force went down to defeat before a weaker enemy.
>
> Not only were our participating surface forces far superior in number to those of the enemy, but the initiative was in our hands. Nor were we inferior, qualitatively, in the crucial element of air strength, which played the major role throughout the Pacific War. In spite of this we suffered a decisive defeat such as the modern Japanese Navy had never before experienced or even dreamed possible.

Earlier in this lecture (see p. ), I quoted two other paragraphs from this same book, in which the Japanese authors make it perfectly clear the reasons for the loss of the Battle of Midway, reasons which have also been stated by other writers. The cryptologic combat coin our Navy entrusted to Admiral Nimitz was highly polished and bright on both sides; the one the Japanese Navy entrusted to Admiral Yamamoto was dull on both sides to begin with. Admiral Yamamoto not only didn't even know how tarnished it was; he lost his life because of his ignorance a couple of years later. Neither he nor his superiors had the experience and knowledge that were necessary to polish up that coin. It took almost ten years for the truth of that dictum I formulated for you a moment or two ago to become clear to the Japanese Navy. Had they taken quick and full advantage of the unfortunate leakage of the vital COMINT facts ~~soon~~ after the Battle of Midway, they could and perhaps would have come to the proper conclusions long before they did. Who knows what the results might have been, and the effect thereof on the outcome of the war in the Pacific?

~~Considering that~~ H[redacted] [redacted]ance in the c[redacted] battles of World War II escaped the attention of Winston Churchill, who ~~have~~ even, way back in 1915, when he was First Sea Lord of the British Navy in World War I, had ~~taken~~ a great interest in cryptology. He made the following ~~his~~ final comment on the Battle of Midway, a comment that is impressive in its guarded revelations and in its restraint:[23]

> One other lesson stands out. The American Intelligence system succeeded in penetrating the enemy's most closely guarded secrets well in advance of events. Thus Admiral Nimitz, albeit the weaker, was twice able to concentrate all the forces he had in sufficient strength at the right time and place. When the hour struck this proved decisive. The importance of secrecy and the consequences of leakage of information are here proclaimed.

It will probably seem to many of my listeners and readers that I have paid more tributes to the achievements of our Navy cryptanalysts in World War II than to those of ~~our~~ their Army and Air Force opposite numbers. If I have done so, I can only say in extenuation of what may appear to be favoritism toward Navy and neglect toward Army and Air Force, that three factors are here involved. First, as regards my apparent overlooking the contributions of the USAF, I need but remind you that it wasn't until after the war was all over that the Army Air Corps became autonomous; before then the technical achievements of cryptanalysts of that Corps were merged with those of the Army. Second, as a member of the Army's Signal Intelligence Service, and then the Army Security Agency during World War II, it is fitting that somebody other than I blow the trumpets in celebration of our Army's cryptanalytic achievements. All I will say is that they were as important as those of our Navy, but for various reasons they have not received much publicity, which is just as well from the point of view of National Security. As a matter of fact, the publicity regarding our Navy's cryptologic successes comes very largely from former enemy officers and from the various official investigations into the attack on Pearl Harbor, and not from any U.S. Navy personnel.. Third, there has been very little leakage with regard to Army's cryptanalytic successes except such as can also be traced back to those Pearl Harbor investigations. General Eisenhower's Crusade in Europe has not one word to say on the subjects of signal intelligence, cryptanalysis, codes, ciphers, or signal security, etc., although he does make a few rather caustic remarks about the failures and errors of his own intelligence staff. General Bradley's

[23] The Hinge of Fate. Vol. IV. Boston: Heughton Mifflin Co., 1950, p.252-3.

book is equally reticent on these subjects but I cannot refrain from quoting one rather amusing episode having to do with COMSEC:

> To identify hills, road junctions, and towns without our giving our plans away in the event of an enemy tap on the wire, I had key features numbered on my war map and gave copies of those numbers to the division commanders. It was a makeshift private code, lax enough to cause Dickson[Bradley's G-2]worry over the security of our plans.
>
> One morning when I called mMajor-General Terry Allen, he referred to an obscure cross-road by its number in this private code.
>
> "Just a minute, Terry," I said. "I can't find that number on my map."
>
> "Well, listen carefully, Brad," he said. "The enemy may be listening in. I'll say the name of the place as fast as I can."
>
> Dickson overheard this conversation and threw up his hands. "Security wouldn't be much of a problem," he said, "if only there were fewer generals in the army."

General Hap Arnold's book I've mentioned before, and have taken one extract from it. There are several others I might have used, but they are not too significant in revelations. One volume of the history of the U.S. Army in World War II, entitled "The Signal Corps" contains a few references to the achievements of the Signal Intelligence Service, but these, too, are not very illuminating. In only one book by a former U.S. Army officer, Col. Robert S. Allen, entitled Lucky Forward: The history of Patton's Third Army,[24] do I find a specific reference to the help the SIS gave Patton. In telling about Patton's signal officer, Colonel Hammand, Allen writes:

> One of his ace units was the SIS. A radio-interception agency, commanded by Major Charles Flint, a young, trigger-smart expert, it worked closely with G-2 on a dual mission: maintaining a vigilant security check on friendly communications and intercepting enemy messages. The unit performed outstandingly in both fields.
>
> Its reports plugged up an unwitting leak from a Mechanized Cavalry source, capable of revealing important troop-movement information to the enemy. And at a critical period in the Battle of Bastogne, the unit broke a German coded message that enabled heavy losses to be inflicted upon the redoubtable 5 Para Division. The SIS was particularly fruitful in breakthroughs and fluid situations when the enemy was on the run and had to use radio.

The foregoing extract is, of course, far from spectacular. Indeed, I imagine that it will hardly bring forth more than a polite yawn from many members of an audience that has already learned about the sensational revelations made during the various PearlHarbor investigations, and about those famous letters that General Marshall wrote to Governor Dewey. But

[24] New York: The Vanguard Press, Inc., 1957, p. [illegible]. The author makes some quite caustic comments about the failure of the intelligence staffs to make use of the intelligence they were furnished. They are worth reading.

there remains this much more to be said: the achievements of our Army's cryptologic units both in Washington and in the field, as well as certain still undisclosed top secret successes of our Navy's units ashore and afloat, are locked away in archives where they will probably remain for a long, long time. More than this I am not at liberty to tell you in this lecture.

With this statement I bring this series to a rather undramatic but I hope meaningful close. I will wind it up by paraphrasing the last sentence of the Introduction to that important book The Battle of Midway from which I have quoted at some length. The Introduction was written by Admiral Nobutake Kondo, the senior living commander of the former Imperial Navy, who participated in that battle. I close this series with the hope that my lectures will serve as material for criticism and reflection.

Thank you very much for your kind attention!

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 placed a purchase order for two such machines on 30 July 1924 and was considering purchasing a rather large number of them later. ~~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 for Army study. The order was placed on 7 October 1934. ~~for me.~~ The rotor wirings of the Army's machines were altogether different from those of the Navy, a fact which I discovered simply by asking Strubel to encipher~~d~~ 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 classified brochure entitled Analysis of a mechanico-electrical cryptograph, Part I. Washington: Government Printing Office, 1934. ?

Hebern built several more models for Navy and these had printing mechanisms associated with them, but Navy dropped negotiations with Hebern in 1934, when it became obvious that he was not competent to build what Navy wanted and needed. Soon after the close of hostilities in World War II Hebern brought a suit in the U.S. Court of Claims for $50,000,000, alleging that the government had used his inventions in the cryptographic machines without paying any of royalties to him. He died before the case could be settled, as it finally was in 1956 or 57, at which time his estate was awarded $35,000. The settlement was made out of court between counsel. That amount was merely as a token [illegible] services he had rendered in his long & continued efforts to produce a satisfactory machine for the Navy, and not as redress for alleged infringement of his patents. 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 collaborati~~ng~~on brought as a result an excellent machine which was developed and produced in quantity by the Teletype Corporation of ~~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. In the Navy it was ~~This was a rather~~

Now we come to some very important new types of electric cipher machines first conceived and developed in Europe, but very soon thereafter and probably independently conceived and developed also in the U.S. In the crypto-component of these machines the electrical paths between the elements representing the plain-text characters and those representing the cipher equivalents are constantly varied by multiple connection-changers within the crypto-component. In early European models of this type of machine the connection-changers consisted of a frame upon which insulated wires were mounted to connect in an arbitrary manner a series of contacts on one side of the frame to a similar number of contacts on the other side of the frame. This frame was slid between two fixed contact-bearing members, one on each side of the frame. By sliding the frame between the two fixed members the paths between the opposite contacts on the latter could be varied as a whole set with a single movement of the sliding frame. A connection-changer of this sort is shown in schematic form in Fig. 30-A, where the sliding member 10, slides between fixed members 11 and 12, thus changing the electrical paths between ~~contacts on~~ the keyboard and the printing mechanism

The connection-changer, 10, is moved to the left or right 1, 2, 3, ... positions, as determined by a cam mechanism but we won't go into this type of machine any further because it wasn't long before inventors saw the advantages of using, instead of slidable connection-changers, mechanisms performing a similar function but of a rotatable nature which we now call "electric rotors," and which rotate, usually step-by-step, between fixed, contact-bearing members called "stators." Rotors and stators of this type are shown in schematic form in Fig. 30-B, there being a left-hand stator, labeled 1, three rotors labeled 2a, 2b, 2c, and a right-hand stator, labeled 3. The connections leading away from stator 1 toward the left go to the keys of the keyboard; those leading away from rotor 3 toward the right go to the magnets of the printer. A bit later we shall explain these elements in more detail.

In Europe, the first machine using rotors and stators was that developed by a German firm and appropriately named the ENIGMA. Here's a picture of it, Fig. 30-C, in which you see a keyboard, a set of eight rotors juxtaposed in a line, or, as we generally say, "in cascade", and a printer. This machine was apparently too complicated for practical usage and was superseded by a second model which also printed and was also unsuccessful. One of the difficulties with these two models was that a multiple switch with many contacts to be made simultaneously was required in order to establish an operative encipher-decipher relationship, so that if in enciphering the letter $D_p$, for example, and the corresponding key on the keyboard is depressed, a cipher letter, say $F_c$, is printed, then on deciphering the letter $F_c$ and the corresponding key on the keyboard is depressed, the plain-text letter $D_p$ will be printed. In this machine this could only be done by making the current for decipherment ~~and~~ ~~decipherment~~ traverse exactly the same path through the rotors and stators that it had traversed in encipherment. This was the function of the multiple switch shown schematically in Fig. 30-D, in which a machine with only six characters (A to F) is depicted. In the left-hand circuit diagram $D_p$ is being enciphered and produces $F_c$; in the right-hand circuit diagram $F_c$ produces $D_p$. But the switching mechanisms 4 and 4' in Fig. 30-D make things a bit complicated because they are within one switching member that operates in one of two positions, one for encipherment, the other for decipherment. I won't go into further details as to its construction because a clever — inventor ~~member~~ of the German firm came up with a new idea which greatly simplified matters not only in regard to the crypto-component of the ENIGMA but also in regard to the indicating mechanism. We may quickly explain how the matter of simplifying the indicating mechanism was accomplished, namely, by eliminating the printer entirely and replacing it with a simple bank of flashlight type lamps. We'll skip the third model, which was only a simpler version of ~~pattern as~~ the fourth model of ENIGMA, seen in Fig. 31-A. This model comprised a keyboard, a bank of indicating lamps and a set of rotors and stators, but no printer. ~~come now to the matter of simplifying the crypto-component to eliminate the multiple switching mechanism shown in Fig. 30-D without loss in security (or so it would seem). Perhaps we would do well to show what the regular rotor looks like. Fig. 30-E~~

Insert over

~~1/ The third model was very similar to the fourth but had one less rotor.~~

Insert

In Fig. 31-A is seen the machine with the cover plate down. At the front is the keyboard; above it, the indicator board, consisting of lamps beneath glass disks upon which letters have been inscribed. Above the indicator board are seen four oval apertures with cover plates through which letters can be seen through holes in these plates. To the right of each aperture can be seen the peripheries of four metal notched wheels, the first one not being labeled ~~but the~~ next three being labeled 1. A switch lever, seen at the right side, can be set to "encipher", "decipher," and "neutral" positions. In Fig. 31-B is shown the machine with the ~~top~~ cover plate ~~off~~ removed, exposing the internal crypto-component. Three rotors, labeled 4 in this figure, are seen and ~~attached~~ affixed to them are the notched metal rings; ~~the fourth notched ring, labeled 11, is affixed to another rotor-like~~ member ~~body labeled 8. This member looks like a rotor but it is really a stator of a peculiar construction and it is this which brings no~~

~~Insert~~ contd. on p. 4c . . . ~~Perhaps it would be a good idea to show you what an ENIGMA rotor looks like and for these can be seen in Fig. 31-B-A~~

Insert to p. 4 contd

ks

which are not labeled. Perhaps it would be a good idea to show you what an ENIGMA rotor looks like and this can be seen in Fig. 31-C. In each of these rotors there is a circle of 26 equally-spaced contact pins on one face of the rotor (Fig. 31-C-I) and a circle of 26 equally-spaced contact surfaces on the other face (Fig. 31-C-II). Insulated wires connect the contact pins on one face in an arbitrary manner to the contact surfaces on the other face. When the rotors are juxtaposed as seen in Fig. 31-C-III, the contact pins on one rotor are brought up against the contact surfaces on the adjacent rotor, so that an electric current will traverse all three rotors along a certain path. The large notched rings are for rotating the rotors manually when they are juxtaposed and aligned to form a portion of the key setting (see E-Z-R in Fig. 31-C-III). The toothed metal ring seen in Fig. 31-C-I is associated with a cam mechanism so that a rotor will be advanced ~~stepped~~ one position when the preceding rotor has made a complete revolution. The first rotor, ~~however~~, immediately to the left of the stator at the right (Fig. 31-B), however, always makes one step with each depression of a key."

A fourth notched ring, labeled 11 in Fig. 31-B, is affixed to another rotor-like member labeled 8 in that figure. This member looks like (a rotor in this picture but it is really a stator of a special construction to be described presently.

We come now to the matter of simplifying the crypto-component of Fig. 31-B to eliminate the multiple pinwheel mechanism shown in Fig. 30-D without much loss in security (or at least so it would seem).

Let us see how this simplification was accomplished in the model depicted ~~shown~~ in Figs. 31-A and B, by showing Fig. 31-D. In the latter, the encipher-decipher circuitry is clearly shown in a machine having, for illustrative purposes, three rotors, labeled 1, 2, 3, rotatable, between two stators, the one on the left labeled 4, that on the right labeled 5. Stator 4 is fixed or non-rotatable and it has 26 contacts on its left face, only two of which are shown. These contacts are connected fixedly to the keys and lamps. Stator 5 is rotatable (but only manually) and it has 26 contact surfaces ~~but only~~ on its right face, only two of which are shown. But in this stator the 26 contact surfaces are inter-connected in pairs by 13 ~~by~~ insulated wires passing through the member. Thus, a current entering one of the 26 contact surfaces goes through the rotor and returns to one of the remaining 25 contact surfaces. For this reason it is called a "reflector", and serves to return a current that has come from one of the 26 contacts on the fixed stator and then through the rotors and into the reflector, via one path, back through the rotors and back into the stator, via a different path, emerging at one of the 25 other contacts of the stator. This assures that in a similar setting of the machine, if $Y_p = Z_c$, for example, then $Z_p = Y_c$, that is, the cipher is reciprocal in nature. It also has as a consequence that no letter can be enciphered by itself, that is, $Y_p$, for example, cannot be represented

[over]

by $Y_c$, no matter what the setting of the ~~cipher~~ crypto-component is and this is true of all the other letters of the alphabet.

If you like you may trace the path traversed by the current in Fig. 31-D in encipherment ~~(where $Z_p = Y_c$) and [illegible]~~ and decipherment, (where $Z_p = Y_c$ ~~[illegible]~~ and $Y_p = Z_c$, but $Z_p$ cannot be represented by $Z_c$, nor can $Y_p$ be represented by $Y_c$.

I won't take the time to tell you about how the rotors are caused to advance in a manner somewhat similar to that in which the wheels of an automobile odometer are advanced. In the case of the ENIGMA shown the total number of encipherments before the key-setting of the machine returns to its original setting is not 26 x 26 x 26 but 26 x 25 x 26, or 16,900. Power for the electrical currents is provided by small dry cells in the box at the upper right in Fig. 31-A. This model enjoyed a fair degree of financial success but when Hitler came into power further sales were prohibited. Suffice it to say that it became the basis for machines used by the German Armed Forces in World War II.

~~tell you~~ discuss in detail ~~about~~ ~~show you~~ the internal works which control the rotating elements and ciphering wheels (you will see have a glimpse of 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, by hand on paper, the results of encipherment or decipherment. This was done by means of a printing mechanism which was associated with the crypto component of ~~cryptographic~~ machine. Here is a slide (Fig. 28) which shows the assembly—the B-211 connected to a Remington electric typewriter, modified to be actuated by impulses from the cryptographic elements ~~machine~~. Of course, it was natural that the next step would be to make the recording mechanism an integral part of the cryptographic machine. This you can see in the next slide (Fig. 29-A ~~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 that figure are clearly seen. The slide-bar mechanism in Fig. 29-B at the right, called the "barrel" or "cage", controls the displacements of the printing wheel in front of it 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, who was followed soon thereafter, but independently, by an American inventor.[18] 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 fixed 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.~~

31/ In Fig.31-A Roman letter ~~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 four openings in the cover plates through which letters can be seen the peirpheries of four metal notched wheels, three labeled 1, the one at the extreme left being unlabeled. ~~at the left A~~ switch lever ~~button~~ which can be set to "encipher", "decipher" or "neutral" positions is shown. ~~At the right~~ In Fig.31-B Roman letter ~~(labeled II)~~, the top cover plate has been removed, exposing the internal ciphering mechanism. Three

[18] I have some doubts on this question of priority of invention in this case. Hebern began working on cipher apparatus ~~his first model~~ in 1910 or 1911, although his first U. S. application on a true electrical rotor machine was filed on 13 March 1921. The date of conception may be much earlier than 1921, I do not know what it was. The date on which the application for a patent on a simpler type of rotor machine was filed in Europe in Germany, by an ~~Danish~~ inventor named Arthur Scherbius on 11 February 1922.

show you the internal works which control the rotating elements and ciphering wheels ~~(you will see them later)~~ but will pass on to ~~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, by 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 electric 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. This you can see in the next slide (Fig. 29-A 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 that figure are clearly seen. The slide-bar mechanism at the right, called the "barrel" or "cage", controls the displacements of the printing wheel in front of it 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, ~~who was~~ followed soon thereafter, but independently, by an American inventor.[18] 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 fixed members called "stators". In Europe the first application for a [illegible] on such a machine was filed in Germany, ~~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.~~

on 23 Feb 1918 and the [illegible]

31 In Fig.31 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 peirpheries 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

[18] I have some doubts on this question of priority of invention in this case. Hebern began working on ~~his first model~~ cipher apparatus in 1910 or 1911, although his first U. S. application on a true electrical rotor machine was filed on 13 March 1921. The date of conception may be much earlier than 1921; I do not know what it was. The date on which the application for a patent on a similar to the rotor ~~machine~~ machine was filed in Europe in Germany, by a ~~Danish~~ inventor named Arthur Scherbius on 11 Feb 1922.

rotors or connection changers "in cascade" can be seen attached to notched rings.
The rotors 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 window~~s~~s 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 stator, on the
periphery of which are also 26 letters of the alphabet. This stator 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 stator and the 26 switches of the keyboard are
fixed. But the stator is rotatable and its position at any time can also be seen
31 through a window, labeled 3 in Fig.31 (I), so that the initial setting of the
stator 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 refering
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 be-
fore reaching a lamp of the indicator board. In the FNIGMA, when the current
✓ exi~~s~~ts from the third rotor, that is, the last rotor at the right, it enters
✓ into another stator also having a circle of 26 contacts, but these are only on its
left face. This stator is fixed, or non-rotatable, and its contacts are connected,
Tr. two by two, by 13 internal wires. This stator, called a "reflector", serves to
✓ return the current, which exi~~s~~ts from one of the 26 contacts on the right face
of the third rotor, back into one of the 25 other contacts on the right face of
that rotor, thence back through a contact on the left face of that rotor into a
contact on the right face of the second or middle rotor, thence through the first
rotor to a contact on the right face of the left-hand stator. The circuitry 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 as a consequence that no letter can encipher
itself/that is, $A_p$, for example, can never be represented by $A_c$, no matter what

~~[illegible]~~ figures initial

rotors ~~or connection changers~~ "in cascade" can be seen attached to notched rings. A fixed notched ring is also seen & it will be described presently.

~~The rotors serve to change the circuits between the keys of the keyboard to the lamps of the indicator board.~~ In ~~such a~~ each of these rotor; there is a circle of 26 equally-spaced contacts on ~~the left~~ each face; ~~and a similar circle of contacts on the right face;~~ insulated wires passing through ~~to~~ the rotor connect the contacts on one face to those on the other and ~~the two faces, two by two, and~~ these connections are made in an arbitrar~~ily~~ manner ~~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~~ an initial key setting. At the ~~left~~ right of the ~~first~~ third from the key rotor is a stator with 26 contacts and the ~~on the periphery of which are also 26 letters of the alphabet.~~ This stator also has a circle of 26 equally-spaced contacts, but these are only on its ~~right~~ left 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 and with 26 lamps in a permanent manner. [The connections between the 26 contacts on the right face of the stator and the 26 switches of the keyboard are fixed.] But the stator is fixed (now) ~~rotatable~~ and its position at any time can also be seen through a window, labeled 3 in Fig.31 (I), ~~so that the initial setting of the stator and the three rotors~~ and their rotatory position at any given moment can be seen through the ~~four~~ windows. The initial settings of these four elements constitute the key for the starting point in ciphering operations.

to the individual keys of the keyboard & to the lamps of the indicating board. a current enters in this stator at one of the 26 contacts

[I used the expression "in cascade" a moment ago, in refering to the rotors, which simply means that the current initiated by depressing a key of the keyboard passes ~~through~~ into the right-hand stator and then through all three rotors before reaching ~~a lamp of the indicator board.~~ the stator at the left. This stator is different from the one on the right from the keyboard] In the ENIGMA, when the current enters ~~exists from~~ the ~~third~~ first rotor, that is, the ~~last~~ first rotor at the ~~right~~ left, it enters into ~~another~~ this second stator also having a circle of 26 contacts, but these are only on its ~~left~~ right 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 ~~exists~~ enters it from one of the 26 contacts on the ~~right~~ left face [of the third rotor, back into one of the 25 other contacts on the right face of that rotor, thence back through a contact on the left face of [~~that rotor~~ the 2d or middle] ~~into a contact on the right face of~~ [the second or middle] rotor, thence ~~through the first rotor~~ to a contact on the ~~right~~ left face of ~~the left-hand~~ stator. The circuitry 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.~~ 31-B It also has as a consequence that no letter can encipher itself that is, $A_p$, for example, can never be represented by $A_c$, no matter what

goes through the stator and exits the [illegible] that

thence through the rotor to that

into the contact on the left face of this 3d rotor (the one at the extreme right) goes through that

the stator & into one of 26 contacts of a stator

31 ✓

In the U.S., in about the year 1910, a California inventor named Edward H. Hebern (Fig. 32), ~~who~~ began ~~[illegible]~~ to try to develop a ~~mechanical~~ cipher machine but, he was merely ~~along mechanical~~ traveling along a well-traveled road that thus far had led ~~to see~~ nowhere. In about the year 1918 he ~~began~~ struck out along a new path. I don't know whether he independently conceived the idea of a machine using an electric rotor or had, in ~~heard of such a machine or searched through~~ his search in the files of the U.S. Patent Office, come across patents covering very recently conceived European electrical cipher machines. At any rate Hebern's first application for a patent covering a machine which he called an "electric code" was filed on 31 March 1921 and a patent was issued to him on 30 September 1924. Here's a picture (Fig. 33) which shows the machine that he himself once told me he'd built for the Ku Klux Klan. You will note that the crypto-component had but one rotor but, ~~his machine~~ like the early models of the ENIGMA, it was associated with a printing mechanism, a Remington electrically controlled typewriter, so that hand recording of the results of operating the keyboard of the cipher part of the machine was not necessary. Hebern's cipher system was also similar in basic nature with that of the first two ENIGMA models — a reversing switch was essential since the electric current had to traverse exactly the same path in decipherment that it had in encipherment. I don't think that Hebern ever thought of the idea of using a stator which also served as a reflector; at any rate he never incorporated that idea in any of his machines. Moreover, I don't think that he had any idea as to the comparative cryptologic advantages and disadvantages of a crypto-component using a "single traverse" or ~~with~~ "straight-through" system of rotors as compared with ~~that~~ one using a ~~reflector~~ "double-traverse" or "twice-through" system of rotors ~~and~~ with a reflector. But we won't go into that here, for its pretty involved.

But ~~there was one~~ Hebern's ~~stuff~~ rotors ~~was~~ had a virtue not possessed by the ENIGMA, ~~namely~~, their wirings could readily be varied, a ~~changed, which was a principle advantage~~ crypto-security of very great importance, ~~and which was not true of Enigma rotors and~~

in his machine and built the 5-rotor model which is seen in Fig. 34. Another very important security feature of the Hebern rotors, I ~~forgot~~ not mentioned, was that they could be used in a "right-side up" or "upside down" position, which ~~could~~ not be done with Enigma rotors. The Navy placed position of the three rotors and the left-hand stator happens to be. The same is true of all the other 26 letters of the alphabet. The three rotors are interchangeable, so that 3x2x1 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 but not in the E the rotors are made so that they can be inserted in either a "rightside-up" or in an "upside-down" position. This makes possible a maximum of 6x4x2 or 48 permutations of the three rotors. Of course, if 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 almost 17,000 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 17,576, but 16,900 ($26^3 - 26^2$ or 26x25x26), 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 the basis for machines used by the German Armed Forces in World War II.

✓ In the U. S., ~~in about 1920~~, a California inventor named Hebern independently conceived a machine which he called an "electric code". Hebern's first patent application covering a one-rotor machine is dated 13 March 1921 and on 20 November 1923 he applied for a patent covering a ~~covers a~~ machine somewhat similar to the ENIGMA in regard to juxtaposing rotors in cascade, 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.[18] Hebern ~~managed to~~ avoided these two weaknesses by incorporating a multiple switch plate which could be set ~~one way~~ in one position for enciphering and in another position for deciphering, ~~another way~~ thus avoiding reciprocal alphabets; ~~On the other hand, not~~ as is the case of the ENIGMA. In the ENIGMA the electrical currents ~~made only one~~ make two traverses through the rotors in encipherment and decipherment: in encipherment the current from a point on the left-hand stator enters and goes ~~rather than two traverses, into the~~ through the three rotors via one ~~circuit and back through them~~ path to the reflector, and then back from the reflector and again through the rotors via another circuit, ~~as is the case in the ENIGMA.~~ In the HEBERN, in encipherment the current ~~went~~ goes in one direction and via one path through the stators and rotors; ~~and~~ in decipherment, it goes in the reverse direction via the same path.

[18] The reciprocal nature of the equivalents and the fact that no letter can be represented by itself is a concomitant of the use of a stator which serves as a reflector and ~~[illegible]~~ these are important weaknesses in the ENIGMA. It is a curious fact that in the earlier German rotor machine there was no reflector — the circuits went straight through.

position of the three rotors and the reflector left-hand stator happens to be. The same is true of all the other 26 letters of the alphabet. The three rotors are interchangeable, so that 3X2X1 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" or in an "upside-down" position. This makes possible a maximum of 6x4x2 or 48 permutations of the three rotors. Of course, if more than three rotors are available, from which a selection of three can be made, the possibilities increase very considerably. The stator at the right is fixed left can be moved only by hand; the reflector at the left right is fixed in this model of the ENIGMA. Depressing a key of the keyboard alongside causes the first rotor adjacent to the fixed stator to advance one step, thus changing the circuit from the right 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 in a manner somewhat similar to the manner in which the wheels in an odometer are advanced so that almost 17,000 letters can be enciphered before the window settings of stator and rotors and the reflector return to their initial alignment. (The total number is not in this case $26^3$ or 17,576, but 16,900 (26x25x26), 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 three rotors are [illegible] a [illegible]

This model of the 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 the basis for machines used by the German Armed Forces in World War II.

In the U. S., in about 1920, a California inventor named Hebern independently conceived a machine which he called an "electric code". Hebern's first patent application is dated 13 March 1921 and covers a machine somewhat similar to the ENIGMA but with some important differences; the cipher alphabets produced by it the Hebern 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 in [illegible] for deciphering another way. On the other hand, not as is the Hebern the case of the ENIGMA, the electrical currents made only one traverse through the rotors, rather than two traverses: into the rotors via one circuit and back through them via another circuit, as is the case in the ENIGMA. In the HEBERN, in encipherment the current went in one direction through the rotors and in decipherment in the reverse direction via the same path.

# APPENDIX TO LECTURE VI

I. The story in TIME magazine of 17 December 1945:

Matter attached
(photos)

II The Marshall - Dewey letters of 25 and 27 September 1944.

Matter attached
(Typed pages)

II

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 from certain members of the Joint Congressional Committee that General Marshall revealed its contents.[8] Thus, it came into the public domain not only on the very day that General Marshall was forced to place it in evidence--its publication caused a great sensation in the newspapers--but also when the 40 volumes of the Hearings of that Committee were published and put on sale by the Superintendent 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

> 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 'ast 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.

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.

[8] 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 valualbe secret was kept out of the campaign." I know this to be true.---WFF

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 you 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 campagin 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 message 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.9

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 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 on timing on the known movements on Japanese convoys, tw. of which were caught, as anticipated, in his destructive attacks.

9 In regard to this and the succeeding four paragraphs, see my comment bwlow (P. 00)--WFF

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 Robert's 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 attache' 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 Europeen 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 threatended 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.[10]

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

Faithfully yours,
G. C. Marshall

SECOND LETTER

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

27 September 1944

My Dear Governor:

Colonel Clarke, 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 probably already referred to in the letter, as suggested to you by seeing the word "cryptograph," and (B) you could not feel that such a letter as this to a Presidential candidate could have been addressed to you by an officer in my position without the knowledge of the President.

[10] The last two sentences in this paragraph were omitted from the Second Letter. See footnote 11 below.---WFF

> As to (A) above 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. As to (B) above 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 or that the preparation or sending of such a communication was being considered.
>
> I assure you that the only persons who saw or know of the existence of either this letter of my letter to you dated Sept. 25 are Admiral King, seven key officers responsible for security of military communications any my secretary who typed these letters.
>
> I am trying my best to make plain to you that this letter is being addressed to you solely on my initiative, Admiral King having been consulted only after the letter was drafter, and I am persisting in the matter because the military hazards involved are so serious that I feel some action is necessary to protect the interests of our armed forces.
>
> (The second letter then repeated substantially the text of the first letter except for the first two paragraphs).

LIFE failed to note that the last two sentences in the penultimate paragraph of the "First Letter" were omitted from that paragraph in the "Second Letter," but there is no explanation for the omission.[11] Perhaps it was simply for the sake of brevity, but this seems improbable.

In my first lecture I called attention to the fact that the account given in the TIME article gives credit to Army cryptanalysis for providing the secret communications intelligence "which enabled our Navy to win such spectacular battles as those of the Coral Sea and Midway, and to waylay Japanese convoys," whereas the credit for the communications intelligence which enabled our Navy to win these battles was produced by Navy cryptanalysts. One cannot blame the editors of TIME for making such a bad error because the source of the error can be traced directly to General Marshall's letter itself. Several years ago I asked my freind Colonel Clarke, who had carried General Marshall's letter to Governor Dewey and who was at the time a high level officer 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. 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 critisize him for not being able, in his very busy days and

[11] The sentence beginning "I might add. . ." and the one beginning "This, however is . . ." were omitted.---WFF

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 that in the cases of certain important naval operations valuable COMINT came from messages read by Army cryptanalysts and this may be what confused General Marshall in implying that all the credit belonged to them because of their solution of the Japanese highest-level diplomatic cryptosystems, the one that used the so-called "Purple Code," which wasn't a "code" but a cipher machine.

Since the period during which the disclosures of the Joint Congressional Investigation were made, disclosures which were disastrous so far as concerns the important accomplishments of the two services before and after the Pearl Harbor 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

The Majority Report made five main recommendations, of which the second is of special interest;[4]

> 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 entended period of time in order that they may become steeped in the ramifications and refinements of their field and employ this reservior 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 taken by the services but how far it has been possible and practicable to insure that the recommendation 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:[5]

> 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

[2] 79th Congress, 2nd Session, Senate Document No. 244, Washington: Government Printing Office, 1946, p. 232.

[3] *Ibid*, page 514.

[4] *Ibid*, page 253.

[5] *Op. Cit.*, page 33.

Army's long neglect of intelligence training was seeon 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 any army, ours as well as in foreign armies, is called a "general officer" or "General?" It is because he is supposed to have by diligent study and first-hand experience learned something about everything connected with military operations. But a high-level generalist is not a specialist in all the operations under his cognizance and responsibility. As a field commander the generalist could conduct his operations satisfactorily 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 very important areas of cryptology, in COMINT and COMSEC for military, naval and air operations and services that you; if you become real specialists, can be of utmost assistance to field commanders, the generalists, That is where you come into the picture--as their responsible and qualified specialists in the quite complex operations of cryptology as applied in modern warfare.

But let us leave speculations as to the possible applications of cryptology in modern warfare in the future, interesting as they may be, and continue with our history of such applications in the past. 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 which ensued, not only in the Pacific but also in the European Theatre.

You will recall that in the first lecture I called to your attention an article which appeared in the 17 December 1945 issue of TIME magazine, and which was based upon a letter that 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 principles looked at that time (Fig. 1). In that letter, which was written on

al/

> Army's long neglect of intelligence training was seeon 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 intelligense 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 capebly 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 any army, ours as well as in foreign armies, is called a "general officer" or "General?" It is because he is supposed to have by diligent study and first-hand experience learned something about everything connected with military operations. But a high-level generalist is not a specialist in all the operations under his cognizance and responsibility. As a field commander the generalist could conduct his operations satisfactorily 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 very important areas of cryptology, in COMINT and COMSEC for military, naval and air operations and services that you, if you become real specialists, can be of utmost assistance to field commanders, the generalists. That is where you come into the picture--as their responsible and qualified specialists in the quite complex operations of cryptology as applied in modern warfare.

But let us leave speculations as to the possible applications of cryptology in modern war/ fare in the future, interesting as they may be, and continue with our history of such applications in the past. Let us first dispose of certain comments in the COMINT area of that history, and specifically to the role that COMINT (or "Magic") ital played, not only in the events preceding the attack on Pearl Harbor but also in the military, naval and air operations which ensued, and; not only in the Pacific but also in the European Theatre.

You will recall that in the first lecture I called to your attention an article which appeared in the 17 December 1945 issue of TIME magazine, and which was based upon a letter that 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 principles al looked at that time (Fig. 1). In that letter, which was written on

27 September 1944, General Marshall practically begged Governor Dewey to say nothing during the campaign about a certain peice of very vital information which General Marshall had reason to believe 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 certain high-level Japanese codes and ciphers 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 surreptitously been given to Governor Dewey true, but more important were the following facts viz, 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 Japanese 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 and that he not use as political ammunition the unproved assumption, or even if the assumption were true; that the attack should not have caught us by surprise. I said in that first lecture that I might later give further extracts from TIME's account and, to continue the extracts from that account, here they are:

> General Marshall had a long series of bad moments after U. S. flyers, showing a suspicious amont of foresight, shot down Admiral Yamaoto'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 attachés. This code remained unbroken more than a year later.[6] 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.
>
> Bold face
>
> **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.

[6] If I ever learned about the Boston incident, I have forgotten all about it. But I shall never forget about the Lisbon episode. --WFF

27 September 1944, General Marshall practically begged Governor Dewey to say nothing during the campaign about a certain peice of very vital information which General Marshall had reason to believe 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 certain high-level Japanese codes and ciphers 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 surreptitously been given to Governor Dewey true, but more important were the following facts viz, 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 Japanese communications in these systems, as well as certain other enemy communications. Therefore, it was vital that Governor Dewey not use the information as political ammunition in his campaign ~~which had come into his possession as to our reading Japanese secret communications prior to the attack on Pearl Harbor and that he not use as political ammunition the unproved assumption, or even if the assumption were true, that the attack should not have caught us by surprise.~~ I said in that first lecture that I might later give further extracts from TIME's account and, to continue the extracts from that account, here they are: These will be found in App. 1 to this lec.

> 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 attachés. This code remained unbroken more than a year later.[6] 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.
>
> Bold face
>
> 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.

[6] If I ever learned about the Boston incident, I have forgotten all about it. But I shall never forget about the Lisbon episode. --WFF

6 See Appendix ?

Ital

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.

Ital

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 scowl on his face the photograph may have been taken on the return from his first visit to the Governor]

Bold? face

"You have my word." It was September 1944. The campaign train rolled up throught the Midwest, returned to Albany. A few days later Tom Dewey received another visit from Colonel Clarke.7

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

Ital

> "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 how 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. ..."

Bold face

l.c.

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:

Ital

> "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.

Bold

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 knowlegge of it."

Bold + l.c.

SECRET LOST

The Pearl Harbor committee blithely tossedaway 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.

e/

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

7/ "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---WFF

> 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.

Italics

> 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 scowl on his face the photograph may have been taken on the return from his first visit to the Governor.]

Caps.

"You have my word." It was September 1944. The campaign train rolled up throught the Midwest, returned to Albany. A few days later Tom Dewey received another visit from Colonel Clarke.7/

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

Ital

> "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 how 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. ..."

l.c. bold

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:

Ital

> "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 knowlegge 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 branch of diplomatic cofidence with the British who had let the U. S. in on the secret on the understanding that it would be kept.

7/ "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---WFF