No 6

1st draft

INTRODUCTION TO CRYPTOLOGY-VI

~~Confidential~~

INTRODUCTION TO CRYPTOLOGY — VI

By William F. Friedman

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

Insert attached →

x x x x x

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

INSERT to p. 1 of handwritten ms after

Type this on legal size paper, original + one carbon, triple space. Number the sheets 1(a), 2(a), 3(a) etc on this set of pages. July

(2)

[New introduction for Lecture No 6]

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

It would be entirely too ambitious a project even to attempt to compress within a lecture of only 50 minutes all that should or could be told in that segment of our history of cryptology. In a nutshell, however, it can be said that the most significant and important events and developments during that quarter of a century were directly concerned or connected with the advances made in the production of more complex mechanical, electrical and electronic cryptographic apparatus, and with the concomitant advances in the production of more sophisticated mechanical, electrical and electronic apparatus for the solution of the messages produced by these increasingly complex cryptographic machines. These two phases are inter-related because, to use a sort of simple analogy, cryptography and cryptanalysis represent the two faces of a single coin.

It would be nice if I could go a

bit into detail in regard to these increasingly complex matters but security considerations prevent my doing so because the classification of these lectures, viz, CONFIDENTIAL, is the lowest one now possible. As to the advances in the development and use of more sophisticated cryptographic apparatus I will only note at this point a comment which General Omar Bradley makes in his quiet but very interesting book entitled A Soldier's Story:[1]

indent + single space

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

It is immodest for me to try to amend General Bradley's remark but this is how I wish he had worded it:

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

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

[1] New York: Henry Holt and Co., 1951, p. 474.

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 those are the ones which were so fully and disastrously disclosed by the various investigations conducted by the Army and Navy very secretly while World War II was still in progress and both secretly and openly after the close of hostilities. The investigations were intended to ascertain why our Army and Navy forces in Hawaii were caught by surprise by the sneak attack on Pearl Harbor by the Japanese on the morning of 7 December 1941. They were also intended to ascertain and pin the blame on whoever was responsible for the debacle. I don't think I should even attempt to give you my personal opinion on these complex questions, which were studied by seven different boards within the Services and finally by the Joint Congressional Committee on the Investigation of the Pearl Harbor Attack. I mentioned the latter investigation in my first lecture and now I must add to what I then said. The Committee published its findings conclusions and recommendations in 1946. It began its work in September 1945 with secret hearings but on 70 days subsequent to 15 November 1945 up to and including 31 May 1945 open hearings were conducted in the course of which some 15,000 pages of testimony were taken and a total of 183 exhibits received incident to an examination of 43 witnesses. The Committee put out a final Report of 580 pages to accompany a set of 39 volumes of testimony and exhibits. In the Report there was one by the Majority (signed by six Democratic ~~members~~ 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 who believe the attack was "engineered" by President Roosevelt.

For this history the interesting fact is 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 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]:

Indent + single space

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

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

2/ P.5 of NSA Technical Journal (Vol. + date), quoting from p. 232 of the Report of the Majority.

3/ p.514 of Report.

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, and that they be maintained in the work for an extended period of time in order that they may become steeped in the ramifications and refinements of their field and employ this reservoir of knowledge in evaluating material received. The assignment of an officer having an aptitude for such work should not impede his progress nor affect his promotions. Efficient intelligence services are just as essential in time of peace as in war, and this branch of our armed services must always be accorded the important role which it deserves.

indent & single space

[4] P. 253 of Report of the Majority.

recommendation
I assume that due note of this has been
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 army's long neglect of intelligence training was soon reflected by the ineptness of our initial undertakings. For too many years in the preparation of officers for command assignments, we had overlooked the need for specialization in such activities as intelligence. It is unrealistic to assume that every officer has the capacity and the inclination for field command. Many are uniquely qualified for staff-intelligence duties and indeed would prefer to devote their careers to those tasks. Yet instead of grooming qualified officers for intelligence assignments,

Indent + single space

[5] Op. cit., p. 33.

Indent & single space

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 the army, ours as well as in foreign armies, is called a "general officer" or "General"? It is because he is supposed to have learned something about everything connected with military operations — he is not a *specialist*. But how much can a general officer know about complexities of such very important areas of the military science and operations such as are involved in modern engineering, electrical communications, guided missiles, rockets, etc, etc.? How much can be learn without first-hand experience in the tricky business of ordinary military intelligence operations let alone the much more complicated business of cryptology as applied in modern military operations?

But let us leave these speculations, interesting as they may be, and continue with our history. Let us first dispose of certain comments in the COMINT area of that history.

However, there is one small but extremely significant piece of information involved in this matter and I will say a few words about it. You will recall that in the ~~very~~ 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 the late General George C. Marshall, ~~then~~ Chief of Staff of the U.S. Army, ~~from [illegible] to [illegible]~~ wrote to Governor Thomas E. Dewey, Republican candidate for President in the 1944 election campaign. In that letter, which was written on 27 Sept 1944, General Marshall practically begged Governor Dewey to say nothing during the campaign about a certain very vital piece of information which General Marshall had reason to believe ~~had~~ become known to ~~have been~~ 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 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 ~~that piece of~~ the information which had surreptitiously ~~been~~ been given to Governor Dewey true but 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. was still reading the secret communications in these systems as well as certain other enemy communications. Therefore, it was vital that Governor Dewey not use the information which had come into his possession as to our reading Japanese secret communications prior to the attack on Pearl Harbor. I said in that first lecture that I might later give further extracts from TIME's account and, ~~here they are~~ continuing the extracts printed on pages 3, 4, and 5 of the first lecture, here they are:

Copy material marked on accompanying photos in red

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,

~~but more importantly, the war was still in progress, the Japanese were still ... (and the U.S. were still reading ... 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 communications prior to the attack on Pearl Harbor. The letter is so important in cryptologic history that I feel the whole of it should be brought to your attention. When it was written it was,~~ of course, TOP SECRET and it was only under great pressure by certain members of the Joint Congressional Committee on the Investigation of the Attack on Pearl Harbor that General Marshall revealed the contents of the letter.[1] Thus the letter came into the public domain when the 40 volumes of the Hearings of that Committee were published, by authority of the Committee, and put on sale by the Superintendent of Documents of the Government Printing Office. The disclosure of the contents of the Marshall-Dewey were indeed such a sensation that LIFE magazine printed the whole of it in its issue of 17 December 1945, with the following introduction:

not only on the very day that General Marshall had to place it in evidence — the letter caused a great sensation in the newspapers — but also

copy from LIFE — p 19-21

1. 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 ~~Governor Dewey~~ as a patriotic citizen, acceded to General Marshall's request — the Gov's

made no use whatever of the vital secret information during the campaign, nor after it, so far as I am aware. TIME's account specifically states that Dewey "held his tongue. The War Department's most valuable secret was kept out of the campaign".

~~Except for a change in the first two and last paragraphs this letter is identical with the first letter. The chan~~

~~At the end of the Second letter as printed in LIFE there appears in parentheses and italics and the following:~~

~~(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. Perhaps it was simply for the sake of brevity, but this seems improbable.

~~There is no explanation for this omission: perhaps it was simply for the sake of brevity~~

In my first lecture (p. 4 of NSA Technical Journal No. ?, date?) I called attention to the fact that the account given in the TIME article gives credit to ~~the~~ Army cryptanalysts 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
the editors of
cryptanalysts. One cannot blame TIME for making
the source of the error may be traced directly to
such a bad error because ~~the letter which~~ General
letter itself. Several years
Marshall's ~~wrote contains that error~~ ago I asked
my friend had carried
Col. Clarke, who General Marshall's letter to
Governor Dewey and who was at the time a high
how such an error had crept into
level officer in G-2, ~~who had prepared the~~
General Marshall's letter, and I was told that the letter which
~~letter for General Marshall's signature. 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. Per-
haps that is how the error to which I have
referred crept into the letter. One could hardly
expect General Marshall to be entirely familiar with
in what he wanted to tell Governor Dewey;
the technical cryptanalytic details involved ~~and keep~~
nor should one criticize him for not being able
~~straight~~ in his very busy days and under very heavy
to bear in mind or even to know about
pressure of events, the differences between the enemy
respective and separate
systems worked upon by the Army and ~~by the~~ Navy
[Insert over]
cryptanalytic organizations.
period during which the ~~disclosures~~
Since the disclosures ~~made~~ ~~of~~ the Joint
were made, disclosures which were disastrous
Congressional Investigation, so far as concerns ~~what~~
the important accomplishments of
the two services ~~accomplished~~ before and after the

Insert

It is of course possible, indeed it may be probable, that certain COMINT regarding the Battles of the Coral Sea and of Midway, as well as other important naval operations, came from messages read by Army cryptanalysts, and this is what confused General Marshall.

Pearl Harbor attack, in the field of communications intelligence, much has been written and is now in the public domain regarding those accomplishments, but, fortunately, no ~~technical~~ details of significance have been disclosed. Hints here and there are in abundance in the many books and articles that have been published by U.S. writers since the end of World War II; but more than hints of the great part played by COMINT ~~was~~ in U.S. military and naval successes are to be found in books and articles published by American officers as well as by officers of the beaten Japanese, ~~and~~ German, and Italian armed forces. Time does not permit ~~any~~ citing in this lecture ~~any~~ ~~remaining~~ of these hints or definite statements, ~~but the following~~ two are of particular interest because they concern the ~~U.S. Navy~~ Battle of Midway, which is considered the one which turned the war in the Pacific from a possible Japanese victory to one of ignominious defeat:

indent + single space what is written over

see over

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 Japanese author is a bit too severe on the Japanese intelligence organization. I say

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

The distinguished American naval historian, Professor Samuel E. Morison, characterizes the victory of United States forces at Midway as "a victory of intelligence." In this judgment the author fully concurs, for it is beyond the slightest possibility of doubt that the advance discovery of the Japanese plan to attack was the foremost single and immediate cause of Japan's defeat. Viewed from the Japanese side, this success of the enemy's intelligence translates itself into a failure on our part — a failure to take adequate precautions for guarding the secrecy of our plans. Had the secret of our intent to invade Midway been concealed with the same thoroughness as the plan to attack Pearl Harbor, the outcome of this battle might well have been different. But it was a victory of American intelligence in a much broader sense than just this. Equally as important as the positive achievements of the enemy's intelligence on this occasion was the negatively bad and ineffective functioning of Japanese intelligence.[3]

[2] Midway, the battle that doomed Japan: The Japanese Navy's Story by Mitsuo Fuchida and Masatake Okumiya, 1955, pp. 131 and 232.

this because their cryptanalysts were up against much more sophisticated cryptosystems than they knew or were qualified to solve. In fact, even if they had been extremely adept 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 ~~subject~~ which is of highest importance — the phase which deals with communications security, or COMSEC, and I shall confine myself largely to its historical background in the U.S. Armed Forces. The background is a very broad one because it should include the background of the developments of each of the three components of COMSEC: cryptosecurity, transmission security, and 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 references to the history of the other two components. And even in limiting the data to cryptosecurity I will have opportunity only to give some of the highlights of the development of the items that comprise our cryptomaterials, omitting ~~leaving out~~ comments on the history of the development and inprovement of our techniques, procedures and practices, all of which are extremely important.

→ Move this down to p. 14 of this ms.

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 19th and~~ 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 with the need for greater and greater speed of cryptographic operations to match as much as possible the very great increase in the speed of communications brought about by inventions and improvements in electric telegraphy. The need for cryptographic apparatus and machines became quite obvious.

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

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

There are further definitions of the word but what I've given is sufficient for our purposes. But why define the word; 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 assistants, journeyed several times half-way around the world. He journeyed in safety — he met with no accident. On the other hand, in April 1943 Admiral Isoroku Yamamoto, Commander-in-Chief of the Combined Fleet, Japanese Navy started out on ~~what was~~ ~~intended to be~~ be just an ordinary inspection trip but it turned out to be a one-way trip for the Admiral. His death was announced in an official Japanese Navy communiqué stating that the Admiral

[Continue over]

had met a glorious end while directing operations in a naval engagement against ~~a~~ superior enemy forces. But we know that this was simply not true; Admiral Yamamoto "met with an accident." But some bright person, it was the late Jimmy Walker, when mayor of New York City, I think, who said that "accidents don't just happen — they are brought about." No; Admiral Yamamoto did not die simply by accident: he died because our Navy pin-pointed the schedule of his trip down to the last detail so that it was possible to set up an ambush with high degree of possible success. Here

Here's the story[3] as told in an interesting manner by Fleet Admiral William F. Halsey, USN:

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

Eighteen P-38's of the Army's 339th Fighter Squadron, based at Henderson Field, were

single space indent

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

single space indent

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 than did the tattletale; we continued to break their codes. ..

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

But lest you get the impression that enemy intelligence agencies had no success at all with ~~the~~ 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~~ disillusioning statement but I can say that as a general rule the successes were attributable ~~not~~ to technical weaknesses in U.S. cryptosystems but to their improper use, ~~in the case~~ of certain low-level ones, by unskilled, or improperly ~~insufficiently~~ trained cryptographic clerks. I may as well ~~tell you right now~~ ~~that this has been true for a great many years~~ ~~information obtainable by procedures not the~~ ~~direct result of cryptanalysis but by means~~ ~~and procedures~~ ~~connected with~~ ~~what we call~~ matter of fact, because as ~~for centuries as a~~ long ago as the year 1605 Francis Bacon, who wrote the first treatise in English on the subject of cryptology, said, in *The Advancement of Learning*:

indent + single space

> This Arte of Cypheringe, hath for Relative, an Art of Discypheringe; by supposition unprofitable; but, as things are, of great use. For suppose that Cyphers were well mannaged, there bee

indent + single space

Multitudes of them which exclude the Decypherer. But in regarde of the rawnesse and unskilfulnesse of the handes, through which they passe, the greatest Matters, are many times carryed in the weakest Cyphers.

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 intelligence can be gained merely from a study of the procedures used in transmission, the direction and flow of communications, the call signs of the transmitting and receiving stations, ~~stations~~ etc., all without solving the ~~crypto~~ communications even if they are in cryptic form. Following are a couple of extracts from a document entitled German Operational Intelligence, published in April 1946 by the German Military Document Section, a Combined British, Canadian, and U.S. Staff:

indent & single space

(P.8.) "Signal intelligence [etc. as per cards attached. ...

(P.8) "Most of their signal intercept success etc.

indent & single space

(P.22) "Importance of Signal Intelligence during the Normandy Invasion: During the invasion etc

A great many examples of intercepted messages of tactical content are cited in the above-mentioned document, which is replete with information of deep interest although the document was originally issued ~~as~~ 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.

Here insert matter on p. 8 of this mss.

REF ID:A62831

Continuation of Lecture No. 6 by f. mature
1st 14 pages have been typed

Here's a photo of Alberti's disk (Fig. 6) but I won't take the time to explain it, except to say that the digits 1, 2, 3, 4 were used to encipher code groups and that the letters of the cipher or revolving alphabet were in mixed order.

Until the advent of electronic cipher ~~cryptographic~~ machines most cryptographic apparatus and devices were built upon or around circular rotating members or cipher wheels, cipher disks, etc. The very earliest such disks or else the earliest picture of such disks appears in a treatise by an Italian cryptologist named Alberti whose Trattati in cifra was written in Rome about 1470. ~~and~~ It is the oldest tract on cryptography the world now possesses.) In Porta's book, first published in 1563 in Naples, there appear several cipher disks and in the copy which ~~I~~ was given me as a gift by

(45.1) Colonel Fabyan they are in working condition. Here is a picture of one of them. (Fig. 7). In this version the devices used symbols as cipher characters. And apparently nobody thought up anything much better for a long, long time. It seems, in fact, that not only did nobody ~~could they~~ ~~not~~ think up anything new or even some ~~any~~ improvements on the original Alberti or Porta disk 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 ~~time and again~~. For instance, in Lecture No. 4 of this series ~~I~~ you were shown a picture of a slight variation of the cipher disk "invented" by Major Albert Myer, the first Chief Signal Officer of the U.S. Army, who obtained a patent on his invention in 1865. [Insert over.]

(45.4) the Cipher Disk used by the Signal Corps of the U.S. Army in World War I was in theory but Porta's in essence.

We all know that it generally takes a pretty long time to get a patent through the complex workshops of the U.S. Patent Office, but in 1924 the ancient device

Insert to P15

Here's a picture of ~~the~~ disk (Fig. 8) and the explanation of it (Fig. 9).

And you will remember that ~~the one of the~~ Signal officers 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~~ period 1910 to 1920, that is, during the ~~period~~ including World War I, ~~(Fig. 10)~~ ~~it~~ was nothing but a white celluloid variation of the original Alberti 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 cipher alphabets are simple ~~plain~~ reversed standard sequences.

was patented in 1924 by S.H. Huntington (Fig. 11). Here you can see a great improvement over the Signal Corps version — a blank is added to both sequences so that the space between words could be enciphered. This, as you have learned, is a fatal weakness if seen in the cipher text; in the Huntington device the spaces between words would be enciphered ~~but~~ the cipher text would have space signs, although they would not correspond to the actual spaces between words in the plain text.

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

The first significant improvement on the old cipher disk was that made by Sir Charles Wheatstone, who some time before 1879 invented ~~and described~~ a cipher device which he called a cryptograph. He described it in a volume entitled The Scientific Papers of Sir Charles Wheatstone, published by the Physical Society of London. Here is a picture of Wheatstone's device which is in my private collection (Fig. 13). What Sir

Charles did was to make the outer circle of letters (for the plain text) comprise the 26 letters of the alphabet plus one additional character to represent "space". The inner circle, for cipher equivalents, contained only the 26 letters of the alphabet and these could be disarranged in a mixed sequence. Two hands, like the hour and minute hands of a clock, were provided, under control of a differential gear mechanism, so that as the long or "minute" hand is advanced to make a complete circuit of the letters on the outer circle of letters on the face of the cryptograph ~~makes~~ the short or "hour" hand advances one space or segment on ~~the letters on~~ the inner circle of letters on the face of the cryptograph. In Fig. 13, for example, the plain-text letter G is represented by the cipher letter A. 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. In encipherment the long hand is ~~plac~~ always moved in the same direction (clockwise, for example) and is placed over 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 at each encipherment.

In this way, ~~successive~~ identical letters of the plain text will be represented by different and varying letters in the cipher text, depending upon how many revolutions of the long hand intervene between the first and subsequent appearances of the same plain-text letter. Correspondents must naturally agree upon the mixed alphabet used in the inner circle and the ~~starting~~ initial positions of ~~each of~~ the two hands at the beginning of the encipherment of a message. In decipherment the operator moves the long hand counterclockwise, seeking the cipher letters in the inner circle and noting the plain-text letters to which the long hand points in the outer circle.

During World War I, some time in 1917, the British Army resuscitated Wheatstone's cryptograph and improved it both mechanically and cryptographically. ~~Here~~ 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 ~~can~~ simultaneously discloses both the plain-text and cipher letters. The ~~The same is. The~~ inner circle of segments is juxtaposed in an eccentric manner against the outer circle of segments,

~~The sequents~~ which are made of a substance upon which letters may be written in pencil or in ink. In this improvement on the original Wheatstone device both sequences of letters are now <u>mixed</u> 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 ~~for~~ assessment of these cryptologists was given me while I was still at the Riverbank Laboratories. I was able to show that the modified Wheatstone cryptograph was still insufficiently secure for ~~serious~~ 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 <u>Several Machine Ciphers and Methods for their Solution</u>, 1918. A better method of solution was devised by me some years later.

Many years later, and almost by sheer good fortune, I learned that a cipher machine was in the museum of a certain small town in Connecticut named Hampden. I was interested and wrote to the curator of the

1879
1817
62

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 sent me, and found a device, beautifully made and encased in a fine mahogany case, with its inventor's name, Decius Wadsworth, and the date, 1817, engraved on the face of the machine, which was nothing but another version of the Wheatstone Cryptograph. (Here's a picture of it (Fig. 15). I believe the model was made by Eli Whitney. ~~Mechanically~~ Mechanically it was similar to the British modification except that the outer sequence had 33 characters, the inner 26, so that the differential gear instead of operating on the ratio 27 to 26 was now on the ratio 33 to 26. ~~I forgot~~ Thus, Decius Wadsworth, an American Army Colonel, ~~and~~ our first Chief of Ordnance, and an associate of Eli Whitney, had anticipated Sir Charles Wheatstone by over 60 years in this invention. He also anticipated the British by a whole century in their modification of Wheatstone's original, because in the Wadsworth device there was only one hand and both alphabets could be made mixed sequences. This is very clearly shown in Fig. 16 as regards the outer sequence and I believe the inner one could also be disarranged but I am now not sure as to this point. I returned the device a good many years ago and it is now on display in the Eli Whitney Room of the New Haven Historical Society's Museum.

The next device I ~~will~~ bring to your ~~notice~~ attention is shown in Fig. 17, a device invented by a French Army reservist, Commandant Bazeries, who for some 10 years tried to get the French Army to adopt it. He was not successful and included a description of his device, which he called his "cryptographe cylindrique," in a book published in 1901 in Paris.[15] He had, however, 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 each~~ of which are differently mixed alphabets of 25 letters each. The disks are assembled on the shaft in some prearranged or key sequence. The first 20 letters of the plain text of a message are aligned, as seen in Fig. 17 (JE SUIS INDECHIFFRABLE="I am indecipherable") and as cipher text one may select any one of the other 24 lines of letters, which are recorded. Then the next set of 20 plain-text letters is aligned, etc. To decipher a

[15] Les chiffres secrets dévoilés.
[16] Comptes Rendus, Marseilles, Vol. XX, pp. 160-165.

~~indication that the letters on the outer sequence are inter-changeable, so that of Fig. 16 seems to indicate that those on the inner sequence are not, this may be an illusion.~~

message, one takes the first 20 cipher letters, aligns them on the device (the disks having been assembled on the shaft in accordance with the prearranged or key sequence) and then one turns the whole cylinder searching for a ~~line of plain~~ row of letters which form intelligible text. There will be only one such row, and the ~~letters~~ plaintext letters are recorded. Then the next 20 letters of cipher are aligned, etc.

In 1893 another French cryptologist, the Marquis de Viaris, 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 attempts to get the French Army to adopt his device. But in the U.S. there were apparently none who encountered either what Bazeries or de Viaris wrote on the subject. Capt. Parker Hitt, U.S. Army, whom I have mentioned in a previous lecture, in 1915 invented a device based upon the Bazeries principle but not in the form of disks mounted upon a central shaft. Instead of disks, Hitt's device used sliding strips and here is a picture of his very first model which he presented to me some time in 1923 or 1924 (Fig. 18). But I learned about his

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

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

Capt. Hitt brought his device to the attention of the then Major Mauborgne, whom I have also mentioned in a previous lecture and who was then on duty in the Office of the Chief Signal Officer in Washington. There is some question as to whether it was Hitt who 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 ~~its~~ disks instead of strips. I have that model, a present from General

Mauborgne many years later. It is made of brass, very heavy, on the peripheries of the disks of which he had engraved the letters of his own specially-devised alphabets. In 1919, after my return to Riverbank from my service in the AEF, Mauborgne sent Riverbank the first 25 letters of a set of some 25 or more ~~beginnings of~~ 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 Mauborgne told us that two consecutive words in one of the ~~test~~ challenge messages were the words "are you." Many years later I found ~~out the~~ reason for our complete lack of success, when I came across the plain texts of those messages in a dusty old file in the OC SigO. Here is a picture of the beginnings of the first six messages (Fig. 20). Mauborgne, when I chided him on the unfairness of his challenge messages, told me that he had not prepared them himself — he had an underling (Major Fowler was his name, I still remember it!) prepare them. In our struggles to solve the challenge messages 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 of it (Fig. 21). That device was standardized and used for at least 10 years in the Army and Navy.

In 1922, a war-time colleague, the late Capt. John M. Manly (Prof. and Head of the Department of English at the University of Chicago) brought to my attention a photostat of a holographic manuscript in the collection of Jefferson Papers in the Library of Congress. It consisted of two pages entitled "The Wheel Cypher," and here is a picture of the second page (Fig. 22) showing Jefferson's basis for calculating ~~of~~ 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!

It soon became apparent to both the Army and the Navy cryptologists that a great increase in cryptosecurity would be obtained if the alphabets of the M-94 device could be made variable instead being fixed. There began efforts in both services to develop a practical instrument based upon this principle. I won't take time to show all these developments but will show the final form of the Army Strip Cipher Device Type M-138-A (Fig. 23). This form used an aluminum base into which channels were cut ~~to~~ to hold paper cardboard strips of alphabets which could be slid easily within the channels. It may 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 a grooved device in quantity, Mrs. Friedman succeeded — on behalf of her own group in the U.S. Coast Guard. The aluminum Strip Cipher Device Type M-138-A was used from 1935 to 1940 or 1942 by the Army, the Navy, the Coast Guard, and the State Department. It was used as a back-up system even after the two services as well as the Department of State began employing ~~had jointly developed an~~ electrical cipher machines of high speed and security.

Thus far we have been dealing with cipher devices of the so-called "hand-operated" type. None of them can really be considered as being "machines", that is, apparatus employing mechanically-driven members upon which alphabetic sequences can be mounted so that a constantly-changing series of cipher alphabets are produced. We come now to a type of apparatus which can be called a machine, such as the one shown in Fig. 24, ~~It~~ is called the KRYHA, ~~after~~ the name of its German inventor, who unfortunately committed suicide a few years ago, perhaps because he failed to make a success of his invention. The Kryha has a fixed semi-circle of ~~letters~~; against which is juxtaposed a rotatable circle of letters ~~sequence~~. Both sequences of letters can be made mixed alphabets (the segments are removable and interchangeable on each sequence). The [illegible] handle at the right serves to wind a rather powerful coiled steel spring which drives the rotating member on which the letters of the inner circle are mounted. In Fig. 25 ~~which~~ can be seen something of the inner ~~work~~ mechanism. The large wheel at the right ~~is seen~~ has ~~apertures~~ segments ~~some of~~ 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

sequence are mounted. ~~A prearranged~~ The initial juxtaposition of the ~~two~~ inner or movable alphabet against the outer or fixed one, as well as the composition of these alphabets is governed by some key or ~~prearrange~~ by other prearrangement. ~~Upon enciphering (and recording) the equivalent of the~~ 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 ~~rotates~~ advances 1, 2, 3, 4... up to 7 ~~step one or more~~ steps, depending on the keys, and the next letter is enciphered, etc. The pictures I've shown you apply to the latest model of the Kryha; as regards the first model, which came on the market sometime in the 1920's, a German mathematician produced an impressive brochure showing how many different permutations and combinations the machine afforded. Here's a picture of a couple of pages of his dissertation (Fig. 26) but even in those days professional cryptanalysts were not too impressed by calculations of this sort. With modern electronic computers such calculations have become of even less significance.

Let us now proceed with some more

complex and more secure machines. In this next
machine which represents a
Slide (Fig. 27) you see a rather marked improvement
by a Swedish cryptographic firm
upon the ones shown thus far. It is mechanico-
machine designated as Cryptograph B211. ~~Here for~~
electrical ~~in character and moreover for~~ the first
machine provided with a
time you see a cryptographic ~~with a~~ keyboard similar
to that on an ordinary typewriter.
keyboard
Depressing a key on this 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
four front wheels
two rear wheels. The are the rotating elements
drive the two rear wheels; the latter are electrical commutators that
which ~~change~~ serve as connection-changers ~~and~~
to change the circuits
~~circuit changers~~ between the keys of the keyboard
and the lamps of the indicating board. There
isn't time to show you the internal works ~~of this~~
which control the rotating ~~elements~~ and ciphering wheels (you will see them later)
~~machine~~, but I must show you ~~about~~ the next
the improvement of such
step in cryptographic machines, which made it possible ~~was~~ to
eliminate the tedious job of recording by
hand on paper the results of encipherment or
This was done by means of
decipherment. ~~by~~ 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 typewriter,
modified to be actuated by impulses from the crypto-

graphic 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. 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 Fig. 27 are clearly seen. The slide-bar mechanism at the right controls the displacements of the printing wheel in front of the slide-bar mechanism and causes the proper letter to be printed upon the moving paper tape seen at the front of the machine.

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

At the left a switch button labelled "encipher", "decipher" or "neutral" positions: can be set to

(labelled I)

In Fig. 1 at the left is seen the machine with the top cover plate closed. At the front is the keyboard; above it the indicator board, consisting of lamps underneath glass disks upon which letters have been inscribed. Above the indicator board and to the left are seen the peripheries of four metal notched wheels (labelled II). At the right in Fig. 1, the top cover plate has been removed, exposing the internal ciphering mechanism. Three rotors or connection-changers "in cascade" can be seen, attached to notched rings. The rotors are rotatable and ~~which~~ 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 the rotor connect the contacts on the two faces, two by two, ~~to those on the right face~~ and these connections are arbitrarily made. The rotors have engraved or painted on their peripheries the 26 letters of the alphabet, which ~~these~~ letters can be seen through small windows in the cover plate, so that the rotors can be aligned to an initial key setting. I used the expression "in cascade" a moment ago, in referring to the rotors, which simply means that the current initiated by depressing ~~from~~ a key of the keyboard passes through the stator and then through all three rotors before reaching

At the left of the first rotor is a stator, on the periphery of which are also the 26 letters of the alphabet. [This stator is stationary.]

Insert

and the contacts are connected by 26 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.

also has a ~~~~ circle of 26 equally-spaced contacts, but these are only on its right face. But the stator is ~~also~~ rotatable and its position at any time can also be seen through a window (labeled 3 in Fig. 1(I), so that the initial setting of the 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.

a lamp of the indicator board. In the ENIGMA, when the current exits from the third, that is, the last rotor at the right and then 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 two by two by 13 internal wires. ~~13 of its contacts go to are connected to the other 13, contacts by wires passing through this stator.~~ This stator, called the reflector, serves to return the current, which exits from one of the 26 contacts on the right face of the third rotor, ~~back into one of the 25~~ to one of the remaining 25 contacts of the right face of that ~~third~~ rotor, ~~and thence back through~~ a contact on the left face of that rotor into a contact on the right face of the second or middle one of the rotors, etc., ~~to a contact on the right face of the left-hand~~ stator. ~~Thus~~ The circuitry in this machine insures that if, for example, $A_p = K_c$, 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, ~~itself~~ that is, A_p, for example, can never be represented by A_c, no matter what ~~at any~~ position of the three rotors and the left-hand stator happens to be. The same is true of all the other 25 letters of the alphabet. The three rotors are interchangeable, so that $3 \times 2 \times 1$ or six permutative arrangements of these rotors is the maximum possible, since in this construction the rotors cannot be inserted in an "upside-down" position. In other types of such machines the rotors are made so that they can be inserted in either a

6×4×2

Of course, if there are more than three rotors are available from which a selection of these can be made the possibilities increase very considerably.

"rightside-up" or "upside down" position. This makes possible a maximum of 6×4×2 or 48 permutations of the three rotatable rotors. The ~~left-hand~~ 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 cipher equivalent. I won't take the time to tell you about how the rotors are caused to advance so that ~~over~~ 17 thousand letters can be enciphered before the window settings of stator and rotors return to their initial alignment. (The total number is not in this case 26^3 or 17576 but 16,900 (26×25×26) for technical reasons which there isn't time to explain.) Power for the electrical circuits is provided by small dry cells in the box at the upper right in Fig. 31 (II).

The original ENIGMA enjoyed a fair degree of

On the other hand, in the case of the ENIGMA, the electrical currents made only one trip through the rotors; in Hebern's [illegible] the current went in one direction through the rotors and no displacement ~~[illegible]~~ goes through in the reverse direction.

success in sales but it was by no means spectacular. When Hitler came into power, further sales were prohibited, ~~for reasons that must be omitted in this lecture.~~ Suffice it to say that its ~~ENIGMA~~ became the basis for machines used by the German Armed Forces in World War II.

In the U.S. a California inventor named Hebern indepently conceived a machine which he called an "electric code". It is similar to the ENIGMA but with some important differences: the cipher alphabets produced by it were not reciprocal and, moreover, a plain-text letter could represent itself in the cipher text. Hebern managed to avoid these two weaknesses by incorporating a switch plate which could be set one way for enciphering another way ~~and~~ deciphering. Here is a slide (Fig. 33) which shows Hebern's very first model, which he constructed for communications of the Ku Klux Klan. You will note that ~~is~~ this model ~~[illegible]~~ has but one rotor; also, the cipher machine is connected to an electric typewriter so that hand recording of results was no longer necessary. [Insert over] Hebern interested our Navy in his machine and built the 5-rotor model which you see in this slide (Fig. 34). Their 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

One additional virtue of the Hebern machine was that the wirings in the rotor were variable, a feature not incorporated in the ENIGMA rotors.

0751-7

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 me. The rotor wirings 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.

machine. Power was furnished by the small dry cell seen at the upper left. The Navy was considering purchasing a rather number of these machines and Lieut. Strubel, then Chief of the Navy's Code and Signal Section of the Office of Naval Communications, asked me to study the machine for its cryptosecurity. After some ~~weeks~~ study I reported that in my opinion the security of the machine was not so great as Navy thought. The result was a challenge, which I accepted. Navy gave me ten messages put up on its machine and I was successful in solving them. There isn't time to go into the methods used but if you are interested you can find them described in my brochure entitled

Hebern built several more models for Navy and these had printing mechanisms associated with them, but Navy dropped negotiations with Hebern when it became obvious that he was not competent to build what Navy wanted and needed. Navy then established its own cryptographic research and development unit at what is now known as the Naval Weapons Plant in Washington.

Army developed at the Signal Corps Laboratories at Fort Monmouth a machine known as Converter M-134 and here's a slide (Fig. 35) showing what it looked like.

Army and Navy went their separate ways in such work for a number of years, but finally, in 1938 or 1939, close collaboration brought as a result ~~[illegible]~~ about an excellent machine which was developed ~~and~~ produced in quantity by the Teletype Corporation in Chicago. This machine was distributed and used very successfully by all our Armed Forces from 1940 to the end of World War II and for some years thereafter. This was a rather large ~~and~~ machine, requiring considerable amounts of electric power and hence unsuited for use ~~in~~ by small units in field operations. In the late 1930's the Army became interested in a small mechanical machine invented by a Swedish engineer named Hagelin. Modifications desired by Army were incorporated in the machine, which was called Converter M-209, and over 100,000 of them were manufactured in the years 1942-44 by the Smith-Corona Typewriter Co. at Groton, New York. Here's a slide (Fig. 36) showing Converter M-209, which was used by all our Armed Forces in World War II, and here is another (Fig. 37). When properly used it gave a high degree of security; when improperly used, as was often the case, its security was rather illusory. This machine operates on what is termed the key-generator principle and when two or more messages are enciphered by the same key stream or portions thereof, solution is relatively a simple matter but I cannot go into that now.

With the world-wide adoption of automatic printing telegraph or teleprinter communications the need became pressing for a reliable and practical cryptographic mechanism to be associated or integrated with the teleprinter. The first apparatus ~~development~~ of this sort in the U.S., ~~is~~ shown in this slide (Fig. 38), was that developed by the American 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 latter may be useful. It is based upon the use of what is called the "Baudot Code", that is, a system in which there are five elements of two different kinds to represent characters of the alphabet. These two elements may be positive and negative currents of electricity ~~impulses~~, or the "presence and absence of current." Here is a slide (Fig. 39) 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 holes and spaces or blanks appear. The letter A, for example, is represented by a hole in the 1st and 2nd levels, the 3rd, 4th and 5th levels are blanks; the letter I, by holes in positions 2 and 3, etc. Toward 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, or "lower" and "upper" case. When the "letters" key is depressed, the characters

Typist: continue after p. 30 of 1st draft, discarding old page 31 of 1st draft.

REF ID:A62831

This material is to be typed triple space, on legal size sheets 1 carbon copy

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 materiel are given ~~the~~ short titles ~~beginning~~ 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 single 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 have or even~~ to see the machine, let alone have it. In order to ~~pro~~ facilitate inter-communication between U.S. and British forces, an adaptor was developed so that, by ~~the~~ use of the latter in connection with the American ECM-SIGABA, messages could be exchanged ~~[illegible]~~ in cipher with the British units possessing ~~equipped with~~ a British machine called TYPEX, for which an ~~equipped with an equivalent~~ adaptor cryptographically equivalent to the American one had been developed. This system of inter-communication worked satisfactorily and securely.

[over]

Certain improvements in the method of usage and certain new 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 originally developed and produced became obsolete some years after the close of hostilities, ~~because~~ when newer machines, ~~[illegible]~~ developed by NSA cryptologists and engineers, replaced them, but not because ~~that~~ there were ever any indications 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 materials were housed, were stolen ~~from~~ during the night when parked ~~on the street~~ in front of the headquarters of the 28th Division during the Battle of the Bulge. A great search was instituted, 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 episode terminated in court-martial proceedings; 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 M-134 suitable, for reasons already indicated in connection with the SIGABA. The sum of $2000 was allotted by the Army to the Chief Signal Officer for the development of a suitable cipher machine small enough to be 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 proffered 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. ~~up all the funds allotted for the purpose.~~ 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 ignominious end to the SCL's development, brought about by the failure on the part of the military director of 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 out a development REF ID:A62821 technical guidance from the SIS. ~~First~~ It was about this time that ~~the~~ ~~development of~~ small mechanical machine which had been developed and produced in quantity in Stockholm by a Swedish engineer named Hagelin was brought ~~around~~ 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 ~~theoretical~~ cryptosecurity was theoretically quite good, it had a low degree of cryptosecurity ~~[illegible]~~ if improperly used — and practical experience had taught me that improper use could be expected to occur with ~~without fail~~ sufficient frequency to jeopardize the security of all messages enciphered by the same setting of the machine, whether correctly enciphered or not. [Insert attached] I tried to assure the CSO that my 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~~ anything that was better than the Hagelin machine, or even as good, ~~as it was~~ with all its mechanical ~~faults~~ deficiencies and cryptographic weaknesses taken into consideration. Accepting, though somewhat reluctantly, ~~as gracefully as possible~~ the well-considered directive of the CSO, the SIS pointed out where improvements could be made and the desired modifications were incorporated in the 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 slide (Fig. 36) showing the machine, which was extensively used by all our Armed Forces during World War II, and here's another (Fig. 37) 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 their 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 in-

defavorable comment by the military developers of the SCL.

Insert

This was because the Hagelin machine operates on what is termed the key-generator principle, so that when two or more messages are enciphered by the same key stream or portions thereof, solution of those messages 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 [over]

801

Dickens, Charles.

Excerpt from:
The Pickwick Papers, Chapter XI: "Involving another journey and an antiquarian discovery."

[Typescript of episode dealing with a fraudulent inscription.]

which have been correctly enciphered by the same key setting, thus making a whole day's traffic readable by the enemy. I cannot go into details in this regard in this lecture.

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, v. 1, NSA Technical Journal, Vol. V, No. 2, April 1960).

large machine requiring considerable amounts of electric power and hence unsuited for use by small units in field operations. In the late 1930's the Army became interested in a small mechanical machine invented by a Swedish engineer named Hagelin. Modifications desired by Army were incorporated in the machine, which was called Converter M-209 and over 100,000 of them were manufactured in the years 1942-1944 by the Smith-Corona Typewriter Co. at Groton, New York. Here's a slide (Fig. 36) showing Converter M-209, which was used by all our Armed Forces in World War II, and here is another (Fig. 37). When properly used it gave a high degree of security; when improperly used, as was often the case, its security was rather illusory. This machine operates on what is termed the "key-generator principle" and when two or more messages are enciphered by the same key stream or portions there of, solution is relatively a simple matter but I cannot go into that now.

Triple space on legal size paper 1 cc

With the introduction of ~~world-wide adoption of automatic~~ 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 teleprinter~~. The first apparatus of this sort in the U. S., shown in this photo ~~slide~~ (Fig. 38), was that developed by the American 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 modern teleprinter ~~the latter~~ may be useful. This principle employs ~~It is based upon~~ what is called the "Baudot Code", that is, a system in which permutations of two different elements taken in groups of five are employed ~~there are five elements of two different kinds~~ to represent characters of the alphabet. (In Bacon's "code" were a's and b's; he used but 24 of the 32 permutations available ($2^5=32$). For electrical communications the two elements) These 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 composed of "marking" and "spacing elements," respectively. Here is a slide (Fig. 39) 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 ~~holes and spaces or blanks~~ perforations appear. The letter A, for example, is represented by ~~a hole~~ perforations only on the 1st and 2nd levels, the 3rd, 4th and 5th levels remaining unperforated ~~are blanks~~; the letter I is represented by holes in positions 2 and 3, - no holes on the other three levels, etc. The English alphabet uses 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 ~~etc. Toward 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

26

printed are the 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 on 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; ~~the space~~ "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 ~~another~~ printing, nor is there any "stunt" functioning by the printer, but the tape merely advances. In modifying the standard printing telegraph machine to make it a printing telegraph cipher machine, or, to put the matter in a slightly different way, in developing the printing telegraph cipher machine the American Telephone and Telegraph Company ~~made good luck~~ was fortunate in having at its disposal the services of a ~~rather brilliant~~ communications engineer named Gilbert S. Vernam who ~~had~~ conceived a brilliant principle. That principle ~~It has~~ turned out to be so useful and valuable that it has come to bear his name and is often referred to as the "Vernam rule." Vernam saw that if in accordance with some general but invariable 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, ~~in the same system in accordance with some general rule~~ 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] the final resultant would be the original character. Vernam extended his idea to make it applicable to a cipher system for teleprinters and an application in Vernam's name was filed in the U.S. Patent Office on 13 September 1918, and Patent No. 1,310,719 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[21] written by one of the ~~other~~ 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:

Indent and single space | copy matter indicated on attached sheet → (R.D. Parker p.108)

Here is an extract from a paper prepared by Vernam himself which in simple language explains

Footnote: 21/ Parker, R.D. "Recollections Concerning the Birth of One-Time Tape and Printing-Telegraph Machine Cryptography", NSA Technical Journal, Vol. II, No. 2, July 1957, pp. 103-114.

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

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

indent + single space

The messages are first punched in a paper tape by means of the keyboard perforator (Fig. 38 of this lecture). ...

* * * * *

The cipher "key" may take the form of another tape [etc as indicated on attached sheets labeled p. 17-21-]

Material attached

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

REF ID:A628[illegible]

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 a rather warm argument conducted by letters exchanged between Colonel Fabyan, the Director of Military Intelligence and the War Department, the Chief Signal Officer, regarding the crypto-security of the cipher printing telegraph system as used by the Signal Corps. The argument ended by meeting successfully a test, which was tantamount to a challenge by the Signal Corps to prove Fabyan's contention, by solving the cipher tapes of 150 messages selected from one day's traffic in the system. The solution was accepted with mixed feelings in Washington, especially on the part of the Director of Military Intelligence who, having signed a letter to the Chief Signal Officer, prepared by Major Yardley, to the effect that the cipher system in question was "absolutely indecipherable," had then—

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 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.

~~exactly~~ how his invention and ~~the~~ system works:

indent & purple space

copy matter attached p.17

22

duty and courtesy of writing a congratulatory letter to Colonel Fabyan, dated 24 March 1920, the final paragraph of which is as follows:

indent + single space

> 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.

[Insert here matter on back of this sheet (p. 48a) also on sheet number 48b + 48c]

The A.T.&T. Company Printing Telegraph Cipher equipments purchased by the Signal Corps were withdrawn soon after Riverbank proved the double-key-tape system insecure. The machines went into storage, where in due course most of them were dismantled. But after I left Riverbank at the end of 1920 and had joined the Chief Signal Officer's staff in Washington, I induced the Chief Signal Officer to resuscitate two of the equipments. These I employed, believe it or not, in preparing the manuscripts for several editions of new ~~field~~ codes ~~for field use~~, 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, and 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 ~~the~~ Signal Corps communications engineers from 1920 until soon after Pearl Harbor. Although beginning about 1938 one of my associates, Mr. Frank B. Rowlett, and I kept urging that there was

Insert to p. 48 (on reverse side)

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

indent + single sp

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 ~~was~~ suggested had not only been done once, but twice. The first time was immediately after the solution, ~~and the~~ copies of the write-up mentioned on p. oo ~~which~~ 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 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. [Insert continued on attached sheet]

p. 48a

Continuing insert to p. 48

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 system, 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 ~~and his associates [illegible] felt that this~~ 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 ~~of~~ long tapes "while presenting a challenge, was not impractical." I am glad to admit that they were right, because ~~in~~ during World War II and for years afterward ~~even up to this~~ 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

[continued - 48b -] [over]

[Insert to p. 48a continued from other side]

proved practical, too, and aside from an occasional error involving the re-use of a once-used tape, ~~the system of~~ absolutely secure inter-communication was assured and was ~~used~~ between and by radio printing telegraphy among large headquarters where the volume of traffic justified the use of this equipment, ~~was assured~~. The principal advantage was the simplicity of crypto-operation — no rotors to be set, no settings of rotors to be enciphered, no checking of encipherment by deciphering the message before transmission, etc.

Insert

However, the leading members of the S.I.S. maintained a theoretical cryptanalytic interest in such equipment and in 193? 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 ~~investigate~~ study the machine 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. ~~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 none other than a retired officer of the Signal Corps and my old friend Colonel Hitt. ~~I was a bit embarrassed~~ to tell him about the results of our test, as he was ~~the first 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 ~~give up~~ neglect his technical studies because of the pressure of administrative duties, he ~~finds it hard~~ unfortunately finds it very difficult to keep abreast of new developments and progress in the field in which he was at one time an expert ~~of his technical cognizance~~. The I.T.&T. Company having spent a great deal of money on the development of a machine which hardly presented any room for improvement, because ~~the~~ principles underlying it were so faulty overall, ~~the Company~~ dropped ~~the~~ further work on it. Colonel Hitt, I am glad to say, ~~weathered~~ ~~survived the disappointment~~ and was well enough in 1942 to be able to

Returning 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.

[Insert matter on reverse side of this page]

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. ~~for such a project.~~ Our more or less sudden entry into World War II, after 7 December 1941, immediately brought a ~~great~~ need ~~pressure~~ for cipher printing telegraphy, especially for radio communication, 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 ~~they~~ S.I.S. did have drawings in readiness, and the development of the machines ~~was~~ was given as a priority task to the Teletype Corporation because ~~workmen~~ 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 because the use of ~~radio~~ 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 development thereof. The machines were produced with 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-888. Under heavy

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-~~apparatus~~ equipments, although the history of their development is rather fascinating and very important. But I must

use in service 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 ~~of ciphering~~, 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 operators' errors left messages open to solution, so that when the new cipher machines were ready they were placed into service as soon as possible, priority being given to circuits with heavy traffic.

~~Other types of cryptographic apparatus were developed during World War II. machines~~ called ~~CIFAX machines, for protecting facsimile transmissions; CIFAX machines~~ I cannot refrain from adding that in every case except one the apparatus produced by commercial research and development firms ~~that~~ without 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 SIGSALY. 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 SIGSALY principles and such equipments are bound to play extremely important roles in any ~~future~~ 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 ~~[illegible]~~ 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 begin ~~[illegible]~~. 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 ~~[illegible]~~ make 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 ~~at-hand~~ available to him instrumentalities that 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 ~~of the~~ sometimes astronomically large number of possibilities, i.e., permutations and combinations, must be tested one after the 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 ~~doesn't~~ 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 cryptanalytic aid made in the U.S. is the one shown in Fig. , which is a picture of what I made ~~called~~

529/607 Parker Hitt 0963 REF ID:A62831

19721 Box 884 Front Royal, Va.

~~A progenitor of [illegible] or [illegible] cryptologic history repeats itself. Dated 21 July 1948.~~

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~~ 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 (Army and Navy were not then sharing secrets) that the Navy Code and Signal Section had an IBM machine 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 subsistance for young men who could find no ~~work~~ 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 newfangled ideas of his predecessor and wanted to get rid of those nasty IBM machines. But the contract with IBM still had some months to ~~go~~ 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 and here's a picture of it (Fig.). I'll read you what it says:

Indent & single space

attached

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

[This belongs in envelope No 28]

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 <u>really</u> begin to do worthwhile <u>cryptanalytic</u> work.

F.

the emphasis upon the ~~bur~~ burden that would be lifted from cryptographic work, ~~the~~ 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 ~~studies~~ were at that time restricted purely to theoretical studies. Studies ~~on~~ or cryptanalytic work on foreign cryptosystems had been ~~was not~~ a responsibility of ~~the Signal Corps during peace time~~ G-2 of the General Staff until 1929, ~~but 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 ~~lim~~ restricted cryptanalytic operations on foreign communications to <u>war-time</u>. And, more to the point, was the fact that there was no material to work on even if funds were available, because the Army ~~we~~ 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 ~~proved~~ 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 a picture (Fig. 00) of one of two whole wings in one of our buildings at Arlington Hall filled with IBM machines — the biggest installation in the world at that 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 achievements 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 ~~de~~ computers are ~~so~~ highly useful in cryptologic work. For example, here is a paragraph (fig.) taken from a Russian book entitled

and ~~below~~ it is ~~the~~ 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 to be dull or tedious to the layman. But long consideration of the military ~~totality~~ importance of cryptography and communication security as against that of cryptanalysis and communication intelligence has induced me to formulate what I shall immodestly call Friedman's Law. It is ~~quite~~ simply stated. ~~You may~~ If ~~you~~ a commander keeps the cryptanalytic or COMINT face of ~~your~~ his cryptologic coin bright and shiny, he ~~stands~~ has a good chance of winning a battle even if his forces are inferior in size and ability compared with ~~to~~ those of his enemy; but if he lets ~~keep~~ the cryptographic or COMSEC face of ~~your coin~~ that coin become dull from neglect, ~~or~~ indifference, or carelessness he will almost ~~certainly~~ lose a battle even if his forces are superior in size and ability compared with those of his enemy.

With the foregoing statement of ~~my~~ an ~~well considered~~ opinion distilled founded upon a half century's devotion study and experience in/ to cryptology as a profession, I bring this series of lectures to an undramatic ~~close~~ but, I hope, meaningful close.