#11

record taken from USPF's home

1) MARINE CORPS
LECTURE SERIES
11 December 1958

2) Presentation as modified and delivered on 26 April 1960, before Staff and Student Officers of Advanced Officers Course, USMC, Quantico, Va

Unclassified Lecture AS&C 1958

In inviting me to address the staff and students of the Senior School of the Marine Corps on the subject of "Communications Intelligence and Communication Security" I assume that General Twining's objective is to make you aware of the role that these two branches of the science of cryptology have played in the past and can in the future again play as a vital military weapon.

Soon after the close of World War II, the commandants of our various service schools began to ask the cryptologic agencies of the Armed Forces for lecturers to tell their student officers something about our cryptologic activities during the war. There was at first serious question as to the advisability of lifting the security veil sufficiently to permit discussion of the subject, but in time an affirmative decision was made. The official views of the Naval War College on the matter were stated in a letter dated 5 February 1946, from the then President of the College, Admiral R. A. Spruance, to the Chief of Naval Communications, Admiral E. E. Stone. In commenting upon the fine presentation made by a certain speaker, Admiral Spruance said:

> "His treatment of the subject matter emphasized the value of communication intelligence to naval commanders, the vital importance of maintaining the security of our own communication intelligence activities, and the necessity for observing the principles of communication security in defense against enemy communication intelligence. I consider that the value to be derived from the indoctrination of senior officers of the Navy in these principles far outweighs any possible loss of security resulting from a partial revelation of our activities in the past war, particularly in view of the disclosures which have been made in the press.

"It appears axiomatic that the full benefit of communication intelligence can be obtained only when all senior officers realize its potentialities for winning and losing battles and wars, and when their actions are tempered by complete knowledge of the elements of communication intelligence, rather than by incomplete and inaccurate information obtained through the channels of gossip."

My talk being divided into three period, I will give you first some of the historical background of cryptology. Next will come a presentation of the manner and the apparatus whereby Communication Security, or for short, COMSEC, is established and maintained; and finally will come a presentation of the basic principles, procedures, machinery, and organization whereby Communications Intelligence, or, for short, COMINT or SIGINT, in British terminology, is obtained, how it may be properly used and safeguarded, and its unrivalled utility as an intelligence weapon in the conduct of modern warfare.

First, then, for historical background.

I opened my remarks by referring to the science of cryptology as a vital military weapon, but it has not always been regarded as a weapon, let alone a vital weapon. I am here reminded at this point of a story that I came across in an old book on cryptology, a story which is probably apocryphal but which I give for what it may be worth.

It seems that about two thousand years ago there lived a Persian queen named Semiramis, who took an interest in cryptology. Whether it was because of that interest or for other unnatural reasons, such as curiosity about what people call secrets, the record doesn't say, but anyhow it was reported that she met an untimely death. Presumably she went to Heaven, or perhaps to the other place, but she left instructions that her earthly remains were to be placed in a golden sarcophagus within an imposing mausoleum which, on the outside of its front wall, there was carved a message, to be saying:

Stay, weary traveller!
If thou art footsore, hungry, or in need of money-
Unlock the riddle of the cipher graven below-
And you will be led to riches beyond all dreams of avarice!

Below this curious message was a cryptogram and for several hundred years the possibility of sudden wealth served as a lure to many experts who tried their hands at deciphering the message. They tried without success, until one day along came a long-haired, be-whiskered, and bespectacled savant who, after working at the project for a considerable length of time, solved the cipher. It gave him detailed instructions for finding a secret entry into the tomb. When he got inside he found an instruction to open the sarcophagus, but he had to solve another message in order to do so. Possibly it involved finding the correct combination to a 5-tumbler lock! Well, he solved that one too, after a lot of work, and this enabled him to open the sarcophagus, in which he found a box. In the box was a message in plain

language, and this is what is said:

> O, thou vile and insatiable monster! To disturb these poor bones!
> If thou had'st learned something more useful than the art of deciphering,
> Thou would'st not be footsore, hungry, or in need of money!

Many times in the course of the past forty years I've had occasion to wish that I knew the old gal's address so that I could write her, as a first indorsement to her basic communication, the single word "Concur."

This being a TOP SECRET lecture it will appear a bit incongruous that I should begin by reading from a source which you'll all recognize--TIME magazine. I'll read from the 17 December 1945 issue and I will preface the reading by reminding you that by that date the war was all over--or at least V-E and V-J days had been celebrated some months before. You'll remember the loud clamor on the part of certain vociferous members of Congress who had for years been insisting upon learning and disclosing to the people of the United States the reasons why we had been caught by surprise in such a disastrous defeat as the Japanese had inflicted upon us at Pearl. This clamor had to be met; the matter could not longer the hushed up, they contended, by the need for military secrecy. There had been and still were investigations--a half dozen or more of them--and now there was to be a grand finale Joint Congressional Investigation into the Attack on Pearl Harbor. It was this investigation which not only itself brought into the open every detail and exhibit uncovered by

its own lengthy investigation and hearings but, it also disclosed to America and to the whole world everything that had been said and shown at all the previous Army and Navy investigations--about a half dozen of them.

There came a day in the Congressional Hearings when the 5-star General George C. Marshall, Chief of Staff/ U.S. Army at the time of the Pearl Harbor Attack,/was called to the witness stand. He testified for several long, long days. Toward the end of the ordeal he was questioned about a letter it had been rumored he'd written to Governor Dewey in the Autumn of 1944, during the Presidential Campaign. General Marshall balked. He pleaded/most earnestly with the Committee not to force him to disclose the letter or its contents, but to no avail. He had to bow to the will of the/Committee. I now read:

'U.S. citizens discovered last week that perhaps their most potent secret weapon of World War II was not radar, not the VT fuse, not the atom bomb, but a harmless little machine which cryptographers painstakingly constructed in a hidden room in Fort Washington. With this machine, built after years of trial and error, of inference and deduction, cryptographers have duplicated the decoding devices used in Tokyo. Testimony before the Pearl Harbor Committee had already shown that the machine known as 'Magic' was in use long before December 7, 1941, had given ample warning of the Japs' sneak attack if only U.S. brass hats had been smart enough to realize it (TIME - Dec. 18). Now General Marshall continued the story of "Magic's" magic. It had:

"Enabled a relatively small U.S. force to intercept a Jap invasion fleet, win a decisive victory in the Battle of the Coral Sea, thus saving Australia and New Zealand.

"Given the U.S. full advance information on the size of the Jap forces advancing on Midway, enabled the Navy to concentrate ships which otherwise might have been 3,000 miles away, thus set up an ambush which proved to be the turning-point victory of the Pacific war.

"Directed U.S. submarines unerringly to the sea lanes where Japanese convoys would be passing.

"By decoding messages from Japan's Ambassador Oshima in Berlin, often reporting interviews with Hitler, given our forces invaluable information on German war plans."

And then TIME goes on to give more details of that story. We shall return to it later in this talk.

It is hardly necessary to tell you how carefully Magic was guarded before, during, and after the war. It is still very carefully guarded. Even the fact of its existence was known to only a very few persons at the time of Pearl Harbor--that is an important element in any attempt to explain why we were caught in such a devasting surprise attack. Let me read you a bit from page 261 of the Report of the Majority in the Joint Congressional Investigation of the attack: [redacted]

"The Magic intelligence was pre-eminently important and the necessity for keeping it confidential cannot be overestimated. However, so closely held and top secret was this intelligence that it appears the fact the Japanese codes had been broken was regarded as of more importance than the information obtained from decoded traffic."

TIME says, in connection with this phase of the story of Magic during World War II:

"So priceless a possession was Magic that the U.S. high command lived in constant fear that the Japs would discover the secret, change their code machinery, force U.S. cryptographers to start all over again."

Now I don't want to seem to over-emphasize the importance of COMINT in the Pearl Harbor affair but I think it warranted to read you what the Majority said about it in its Report. The following comes from p. 232:

"... all witnesses familiar with MAGIC material throughout the war have testified that it contributed enormously to the defeat of the enemy, greatly shortened the war, and saved many thousands of lives."

General Chamberlin, who was MacArthur's G-3 throughout the war in the Pacific, has written: "The information G-2 gave G-3 in the Pacific Theater alone saved us many thousands of lives and shortened the war by no less than two years." I hardly need say that we can't put a dollar-and-cents value of COMINT in the saving of lives; but we can make an estimate of what COMINT meant in the way of shortening the war by two years means. I made a calculation and found that $1.$$ spent for COMINT is worth $1,$$$ spent for other activities and materials.

In short, when our commanders had COMINT in World War II they were able to put what small forces they had at the right place, at the right time. But when they didn't have it--and this happened several times--their forces often took a beating. Later on we'll note instances of each type.

I hope I've not tried your patience by such a lengthy preface to the real substance of my talk, so let's get down to brass tacks, and since a bit of history is always useful in introducing a subject belonging to a special and not-to-well-known field, I'll begin by giving you some historical information about cryptology, which comprises two related sciences, that of cryptography, and the other of cryptanalysis. They are but opposite faces of the same coin, for progress in one inevitably leads to progress in the other.

If time permitted we could go far back into history to see the earliest beginnings of secret communications and this might take us to the very dawn of the art of writing because there is room to wonder which came first, ordinary, intelligible writing or unintelligible, that is, secret writing. Instances of cipher are found in the Bible, for instance, and we now know that some of the ancient Egyptian hieroglyphic writing was sometimes enciphered. But we must quickly pass over the history of the early days of cryptology with the foregoing brief mention. There is, however, one item in that history which is worthy of special notice, the scytale, which is the earliest cipher device history records and which was used by the ancient Lacedaemonians or Greeks. They had a

(2) wooden cylinder of specific dimensions, around which they wrapped spirally a

piece of parchment; they then wrote the message across the edges of the parchment, unwound it, and sent it to its destination, where the recipient would wind the parchment around an identically-dimensioned bylinder, and thus bring together properly the bits of letters representing the message. This diagram, incidentally, is not correct. The writing was done along the edges of the parchment, as I said before, and not as shown in this picture. And, by the way, the baton which the European field marshal still carries as one of the insignia of his high office derives from this very instrument.

Caesar, of course, is well known in history to have used cryptography--a very simple method, obviously, because all he did was to replace each letter by the one that was fourth from it in the alphabet. Cicero was one of the inventors of what is *now* called shorthand. He had a slave by the name of Tiro who wrote for Cicero his records and so on, in shorthand or Tironean notes, as they are called.

The beginnings of modern cryptology can be traced back to the days of the early years of the 15th Century, when the science was extensively employed by
(4.18) the princes and chanceries in the Papal states, about 1400. I show next an alphabet of that period which is interesting merely because it shows that in those early days they already had a recognition of the basic weakness of what we call

single or monoalphabetic substitution. Solution of this type of cipher, as you all know, is accomplished by using data based upon frequencies. I don't have to go into that because all of you, at some time or other, have read "The Gold Bug", and understand that sort of analysis. But this slide shows that the early Italian cryptographers introduced a method of disturbing the normal frequencies, by having the high-frequency letters represented by more than a single character. I will add that the earliest tract that the world possesses on the subject of cryptography, or for that matter, cryptanalysis, is that which was written in 1474 by a Neapolitan, whose name was Sicco Simonetta. He sets forth the principles and methods of solving ciphers--simple ciphers no doubt, but he describes them and their solution in a very clear and concise form. The first book or extensive treatise on cryptography is that by a German abbot named
(245.2) Trithemius, who wrote his monumental work in 1531. He planned to write four volumes, but he quit with the third one because he wrote so obscurely and made such fantastic claims that he got charged with being in league with the Devil. They burned his books, as a matter of fact. This may be a good place to present
(151) (242) a slide which shows that the necessity for secrecy in this business was recognized from the very earliest days of cryptology.

We are going to jump a ways now to some examples from the more recent
(3.5) history. This slide shows a cipher alphabet and system used by Mary, Queen of Scots, in the period 1545, or thereabouts. There was an Italian cryptographer whose name was Porta and who wrote a book, published in 1563, in which he showed certain types of alphabets that have come down in history and are known now as

(6) Porta's Alphabets. Here's an example of the Porta Table, showing one alphabet with key letters A or B, another alphabet with key letters C or D, and so on. I don't want to go into exactly how those key letters are used, but it is sufficient to say that even to this day cryptograms using the Porta alphabets are occasionally encountered. Incidentally, Porta was quite a fellow. There are lots of people who refer to his book but have never read it. I took the trouble to have it translated to see just what he did say, and he was, in my opinion, the greatest of the old cryptographers. Incidentally, also he was the inventor of what we know as the camera obscura, the progenitor of our modern cameras. I think also he was one of the earliest of cryptanalysts able to solve a system of keyed substitution, that is, where the key is changing consistently as the message undergoes encipherment. Porta's table was actually used in

(6.1) official correspondence. Here is a picture of a table that was found among the state papers of Queen Elizabeth's time, used for communicating with the English Ambassador to Spain. It used Porta's alphabets.

(5) The next slide I show is a picture of what cryptographers usually call the Vigenère Square or Vigenère Table; a set of twenty-six alphabets successively displaced one letter per row, with the plain-text letters at the top of the square and the key-letters at the side. The method of using the table is to agree upon a key word, which causes the equivalents of the plain-text letters to change according to the manner in which the key changes. Now, Vigenère also has an interest to me because although he is commonly credited with having invented

that square, he really didn't and, what's more, never said he did. Here's a
(5.1) picture of it as it appears in his own book. It goes considerably beyond what the ordinary references say about his table, but I won't go into those differences because they're technical and perhaps of no great interest to you today.

The next cryptographer I wish to mention is a Frenchman, Francois Vieta, an eminent mathematician, founder of modern algebra. In 1589 he became Councellor of Parliament at Tours and then Privy Counselor. While in that job he solved a Spanish cipher system using more than 5## characters, so that all the Spanish dispatches falling into French hands were easily read. Phillip II of Spain was so convinced of the safety of his cipher that when he found the French were aware of the contents of his letters to the Netherlands, he complained to
(5.2) the Pope that the French were using sorcery against him. Here's a slide that shows one of the hundreds of ciphers the Court of Spain was then using Vieta was called on the carpet and made to explain how he'd solved the ciphers. Here is another example of another old official cipher. Here are the alphabets; and
(3.7) a sliding card, which could be shifted up and down, was used for changing the
(3.8) key, or as a means of changing the key. Here is another, called the "two-square cipher", or "two-alphabet cipher"; it involves coordinates: here is one complete alphabet and here is another one, the coordinates are used to represent the letters. That was actually used in Charles I's time, 1627, in communicating with France and Flanders.

I want to jump now to the period of the American Revolution, in U.S. history. The systems used by the Americans and by the British were almost identical! In one case, in fact, they used the same code book! Here's a list:

Ciphers

American:
a. Simple monoalphabetic substitution.
b. Monoalphabetic with variants by use of long key sentence ala Franklin.
c. Vigenere with repeating key.

British:
a. Monoalphabetic substitution.
b. Vigenere with repeating key.
c. Grilles.

Codes

a. Dictionaries.
b. Keybook using words.
c. Syllabaries.

a. Dictionaries.
   1. Entick's
   2. Bailey's
b. Small alphabetic 1-part codes of 6##-7## items and code names.
c. Ordinary book such as Blackstone - page, line, no. of words in line.

Miscellaneous

a. Secret inks.
b. Grilles
c. Various concealment methods.

In addition, code or conventional words were used to represent the names of persons and places. The British used code names:

American Generals - Names of the Apostles:
Washington = James
Sullivan = Matthew

Philadelphia	-	Jerusalem
Detroit	-	Alexandria
Delaware	-	Red Sea
Susquehanna	-	Jordan
Indians	-	Pharisees
Congress	-	Synagogue

I know that there was an American who seems to have been the Revolution's one-man NSA, for he was the cipher expert to Congress, and, it is claimed, he managed to decipher nearly all, if not all, of the British code messages intercepted by the Americans. Of course, the only way in which enemy messages were obtained

in those days was to seize couriers, knock them out or off, and take the messages from them. Rough stuff compared to getting the material by radio

(6.31) intercept The next chart shows a picture of a code or "syllabary", as we call it, used by Thomas Jefferson. This syllabary is constructed on the so-called two-part principle. This is a portion of the decoding section. You will note that the numerical groups are in consecutive order but their meanings are at random. They have no alphabetical order at all. It simply means that you have to have another section, the encoding section, in which the words are in alphabetical order, and their equivalents are in random order. This sort of system even today is in extensive use. Jefferson was an all-around genius, and I shall have something to say about him and cryptography a little bit later on, I hope.

I'm sure you've learned as school children all about the ~~despicable and~~ treasonable conduct of Benedict Arnold when he was the Commanding General of the American Forces at West Point, but you probably don't know that practically all his exchanges of communications with Sir Henry Clinton, Commander of the British Forces in America, were in cipher, or in invisible inks. He even used one trick that was quite similar to one used as recently as in 1957 by the Russian spy Colonel Abel who was arrested in New York in June 1957, tried and convicted, and is still languishing in a Federal prison. The trick was to inclose bits of writing in specially-constructed hollow bullets. Here's an interesting slide showing one of Arnold's cipher messages, in which he offers to give up West

it off post haste to London for solution. But, of course, Clinton knew it was going to take a lot of time for the message to get to London, be solved and returned to America--and he couldn't afford to wait that long. Now it happened that in his command there were one or two officers who fancied themselves to be cryptologists and they undertook to solve the message, a copy of which had been made before sending the original off to London. Well, they gave Sir Henry their solution--which happened to be wrong and Clinton's operation turned out to be rather a dismal failure. The record doesn't say what Clinton did to the two amateur cryptologists when the correct solution arrived from London weeks later. By the way, you may be interested in learning that the British have operated a cryptanalytic bureau ever since the year 1540, save for a few years from about 1850 to 1914.

There's also an episode I learned about only very recently, which is so amusing I ought to share it with you. It seems that a certain British secret agent was sent a message in plain English giving him instructions from his superior. But the poor fellow was illiterate and had to call upon the good offices of a friend to read it to him. What he didn't know, however, was that his friend was one of Washington's secret agents!

If interest in cryptology in America wasn't very great, if it existed at all after the Revolution, this was not the case in Europe Books on the subject were written, not by professionals perhaps, but by learned amateurs Here's a picture of the frontispiece to a book in French dealing with espionage and counter-espionage, and it has a section dealing with cryptology.

way, of course, and makes no sense, but if you read it backwards it makes excellent sense: "If I should be in a boat off Aquia Creek at dark tomorrow, Wednesday evening, could you without inconvenience meet me and pass an hour or two with me? (Signed) A. Lincoln." I think the President was kidding a bit, but he may have lacked confidence in the official cryptosystems in the same way that President Wilson lacked confidence in the codes of the State Department, as can be seen in the slides which I now show. (Nos.

Twenty-five years later, in the days just before Pearl Harbor, certain high-level officers in our Army lacked confidence in the Army's highest level cryptosystems and preferred those of the Navy--at least, that's what one of them said during the Congressional Hearings on Pearl Harbor. What these officers forgot by the time of the investigation, if they'd ever known it to begin with, was that the Army and the Navy were both using the very same machine, one based upon cryptoprinciples ~~suggested~~ invented by Army cryptographers, but built/under direction of Jointly Army and Navy cryptographers.

This is a photograph of a page or two from the code book and cipher system used by the Federal Army. They had what is called "route ciphers", that is, a matrix with indications of route to be followed in inscribing and transcribing the words of the message. Here's how you write the message in: the first word, second, third, fourth, fifth, sixth and so forth; then you take them out according to another route. And here the thing is complicated by the use of arbitrary equivalents for the names of important people.

"President of the U.S " is represented by "Adam" or "Asia". It had two equivalents, you see. Here are some of the names of famous or well-known officers of that period. I have with me today the complete set of cipher books used by the Federal Army during that period, and after my talk those of you who wish may come up and examine them, together with certain other exhibits. The next slide is a picture of a message sent to General Grant in one of those route ciphers. I shall not take time to read it.

[redacted]

After the Civil War, or War Between the States, the use of cryptography in United States military affairs went into a decline for a long period of peace [redacted] broken only briefly by the Spanish-American War. In 1885 the War Department published a code called "Code to Insure Secrecy of Telegrams". It is a cryptographic curiosity and no tribute to the imagination of the officer who was responsible for its production because he copied almost word for word the title page, the instructions for use, and the arrangement of contents from

then Captain Parker Hitt; and the title page of a small brochure by the then Lieut. J. O. Mauborgne. But these were almost private ventures; officially, as regards cryptographic preparations, no new codes were in preparation in either Service; no new ciphers were being dreamed up; no cipher devices or cipher machines were being investigated or invented in either Service. As for cryptanalytic operations--well, there just were none whatever in either Service, and, for that matter, in the whole government. A private research institution near Chicago, the Riverbank Laboratories, of which I happened to be a member, working in a totally different field of science, began studying cryptology and soon certain members of the staff were working on messages sent to the laboratories for study, messages which were furnished us by various government departments and agencies in Washington. Most of these messages were solved and returned to Washington, and the staff became more and more adept. But mind you this was not even a quasi-governmental agency, it was operated as a patriotic gesture and at his own expense by the man who, in 1915-1916, as an astute and wealthy business-man, Colonel George Fabyan, foresaw the inevitable entry of the U.S. into the war, wholly unprepared for any cryptologic work. The Colonel was right, for on 6 April 1917 the U.S., almost suddenly it seemed, declared war on Germany. How did this come about? It came about <u>when</u> it did as the result of a nice piece of cryptanalytic work by the British cryptanalytic experts in London. The message first came from the German Foreign Minister in Berlin to the German Ambassador in Washington; it was then sent on to the German Minister in Mexico City. Here's the message in the form in which it was transmitted to Mexico. I won't go into the story about how the British solved it, for this involved the reconstruction of two rather large codes

and represented a first-class piece of work. But I do want to say a few words about the political effects of the solution, and about British cleverness in the handling of the case, because it is a good illustration of how astute, diplomatically, they are, As I have already said, it resulted in bring us into the war on their side. Here is the translation of the thing. It was important because the message said the Germans were going to resume unrestricted submarine warfare and this part, here, dealing with a proposal to be made to Mexico, was the straw that broke the camel's back. People in the Middle West had been very lukewarm toward the idea of our getting into the War--on either side--but when the Germans began talking about returning Texas, New Mexico and Arizona to Mexico, that was something else again. So, we got into the war within a couple of weeks after the British gave us and we had established the authenticity of the translation of "the Zimmermann Telegram". A year or so ago the telegram and episode was the subject of one of the series of Walter Cronkhite's "You Are There" television programs. And a book of almost 250 pages, dealing only with that telegram and episode, was published just about six weeks ago. I brought a copy with me for you to look at later.

Well, as I said a few minutes ago, on 6 April 1917 we were in the war as a belligerent and things began popping, especially in my own little world at the Riverbank Laboratories, We began training more people and doing more solution work--all paid for by Colonel Fabyan. We had messages to solve that dealt with our neighbor on our southern border as well as messages that dealt with the activities of enemy agents

There was one rather interesting case, in which I happened to play a minor role. In 1916-17 the Germans financed a large number of Hindus in their attempts to stir up a rebellion in India, the idea being to cause so much trouble in India that the British would be forced to withdraw troops from the Western Front to quell disturbances in India. These Hindus were negotiating for the purchase of arms and ammunition in the United States and sending them over to India. Since the U.S. was neutral, it was against our own laws to permit such undertakings against a friendly nation. So the business had to be conducted secretly and that is how cryptograms entered into the picture. Here

is one page of a long, seven or eight-page letter that was intercepted between the top Hindu agent in the United States and his chief in Switzerland. The latter consisted of groups of figures, in which were interspersed some plain-text words. I recognized pretty quickly that the letters of the secret text had been replaced by numbers which indicated specific letters in a book. Each group of numbers represented the page number, the line number, and the position number in the line of the letter. All I needed was the book, but unfortunately the Hindu failed to tell me what the book was, so I had to go ahead and try to solve the message without it. It was solved, and I'll show you very briefly the method. As I said, there were words, plain-text words, interspersed throughout the cipher text, and I would make a guess at what the numerical group before or after a plain-text word represented. Here, for example: "Formed something, with something". I assumed that this first "something" would be the word "committee", and that meant that on page 65, the fourth line, the second letter in the line was a C; the third to be O; the fourth M; the fifth another M, but the sixth letter in that line was not indicated. Instead, the next group jumped to another page, from which the letters I, T, T, and so on were taken. Well, by substituting some of these guesses in their proper positions and making tabulations of this sort, I assumed that the first five letters of this word "committee" came from the word "communication" on page 65, line 4; the next three, from a word having "TTE" in it, such as "attention"; but the last letter, E, came from another page altogether and I could only add more data before making any guess as to what the word on page 72, line 2,

various belligerents because, these were used, especially for tactical purposes, in preference to codes and code systems, which came as a later development. Here's a picture of the cipher system used and misused by the Russians. You will note that it is nothing but the old Vigenere principle all over again, using numbers instead of letters. It represents a case involving only a set of 7 or 8 alphabets used repetitively, by a key number, for substitution. This was the deciphering table. Russian ineptitude in communications and especially in cryptography cost them the Battle of Tannenberg and contributed to their being knocked out of the war. The next slide is a picture of a front-line cipher system used by the French. It was a transposition system, the columns being here transcribed according to the columnar key; in addition, certain disturbing elements came into the method by taking off the letters in diagonals. And here is a picture of the system used by the Italian Army in World War I. Again, it is only a variation of the old Vigenere system. Here is a system used by the Germans; it was invented by them, or, I should say, it was a clever combination of two methods. We called it the ADFGVX cipher because the cipher text consisted exclusively of those letters. An alphabet in here, arranged according to some pre-arranged plan, with the coordinates ADFGVX; the letters of the message were then replaced by pairs of coordinates; for example, the letter R is represented by AG, and so forth. Then a numerical key, developed from a key word, is written over the X's, A's and so forth, and the letters are then taken out in columns according to the key order. That system was a brand new thing in military cryptography and caused no end of

headaches for the Allied cryptanalysts until it was discovered just how a solution could be achieved. The solution was not a general one but depended upon special cases; however, these happened so often that we could bank on them occurring practically every day. That cipher system was used by the German high command and consequently someone soon discovered that if you made a chart based upon just the number of ADFGVX messages transmitted why you could discover certain things about the tactical situation and, more important, you could, with some degree of assurance, predict what might happen in three or four days at a certain sector of the front. Here is an example of such a chart based upon the ADFGVX intercepts. This, gentlemen, is the first illustration that I know of in history of one of the basic principles of what we call traffic analysis and traffic intelligence (Explain chart.) The next slide gives a picture of the sort of "communiques" we issued, "Bulletins" we called them, that we put out when the ADFGVX messages were read. Here is one of a set of messages, dated November 2#, 1918; of course the war was over by that date, but this gave very detailed and very important information about the withdrawal of Mackensen's army in Roumania. There is the German text and there is the translation, an interesting and authentic message.

For tactical messages the British and Americans in World War I used a method known as the Playfair Cipher, allegedly invented by Lord Lyon Playfair, but he didn't invent it--Sir Charles Wheatstone invented it. By the way, Wheatstone, who is credited with inventing the electrical bridge that is known by his name, didn't invent that bridge--a chap named Christy really did. The