Corrections for draft
No. 2. Made in two copies.
When General Turing invited me to address the staff and students of the Senior School of the Marine Corps on the subject "Communications Intelligence and Security" I accepted the invitation because, amongst other things, that I accepted the invitation because, amongst other things, the objective of my address is to give you awareness of the role that these two branches of the science of cryptology have been employed as a vital military weapon, and will continue to be employed as such in the future. The science of cryptology, a specialty that I will give you something about how it developed, must now indicate the manner in which it operated first some presentation of the historical background of cryptology. Next will come a presentation of the manner and 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, is obtained, how unrivalled it may be properly modernly used and safeguarded, and its utility 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.
Soon after the close of World War II,

the Commandant of the various service

schools began to ask the cryptographic authorities of the

Naval Forces for information to explain to their student

officers something about our wartime code

cryptologic activities during the war. There was at

first question as to the advisability of drafting the

security and sufficient to permit discussion of the

subject. The official record of the Naval War College

on the matter was stated in a letter from the then President of

the College, Admiral R.A. Spruance, to the

Chief of Naval Communications, Admiral F.E. Stope.

In commenting upon the free presentation made by a

certain speaker, Admiral Spruance said:

\[ \text{Signature} \]

The treatment of the subject of Alice was to be continued on the next to last page.
language, and this is what it said:

O, thou vile and insatiable monster! To disturb these poor bones!
If thou hadst learned something more useful than the art of
deciphering,
Thou wouldst 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
endorsement to her basic communication, the single word "Concur." MAXIMUM

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
by that date all
reminding you that/the war was/over--or at least V-E and V-J days had been

some months before You'll remember the
celebrated/quirkiness 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 those the Japanese had inflicted upon us
at Pearl. This clamor had to be met; the matter could no longer be hushed up,

they contended, by the need for military secrecy. Sometimes were investigations--
of them, and now there was to be a
a half dozen or more/quirkiness grand finale Joint Congressional Invest-
igations into the Attack on Pearl Harbor. It was this investigation which not

only itself brought into the open every detail and exhibit uncovered by mvv
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.

Now, because of the secrecy or cloak of silence which officially surrounds the whole field of cryptology and especially cryptanalytics, it is obvious that authentic information with reference to the background and development of the science in foreign countries is quite sparse; and although after World War II we learned much regarding the accomplishments in this field of work by our enemies, security rules prevent my saying very much in detail about how good or bad they were in comparison with us. Suffice it to say that we looked pretty good in cryptologic affairs; together with our principal ally, Britain, we cryptologists naturally think we won the war, though others seem to have mislaid the peace somewhere.

I can only give a fairly good account of U.S. cryptologic activities up to a certain point of time, and even then I will not be able to say very much about them simply because the story is too long to give in a lecture or even a series of talks. In the course of my talk I will present a number of illustrations of
cryptography and cryptanalysis, some of which form part of my own experience. Modesty would dictate their omission, but because of their possible interest I will use them and will here and now make a general apology for the use of the personal pronoun.

Now may we have the first slide, please. Cryptography and cryptanalysis go back to the dawn of the invention of writing, and here I show an instance of cipher in the Bible. In Jeremiah 25:26 occurs the expression "And the king of Sheshhah shall drink after them." Also in Jeremiah 31:14: "How is Sheshhah taken?" Well, for many, many years that name "Sheshhah" remained a mystery. There was no such place. But then somebody discovered that if you write the twenty-two letters of the Hebrew alphabet in two rows, eleven and eleven, like this, you set up a substitution alphabet whereby you can replace the letters by those standing opposite them. For example, "Shin," is represented by "Beth" or vice versa, so that "Sheshhah" translates "Babel," or "Babylon." The vowels had to be supplied. Incidentally, mentioning the Bible, one might say that was an early but not the first in the Bible—Daniel, who was/first psychoanalyst, was also the first cryptanalyst. I say psychoanalyst, because you remember how he interpreted Nebuchadnezzar's dreams.
remember it, but it's a part of your job to find that out and then interpret it."

That was a pretty stiff assignment, and they failed to make good, which irked

Nebuchadnezzar no end. Kings had a nasty habit of chopping your head off in

these days if you failed, so in this case it comes as no surprise to learn that

Nebuchadnezzar passed the word along to destroy all the wise men of Babylonia,

including Daniel. Well, when the King's guard came to get Daniel, Daniel asked

that he be given a bit of time. Then, by some hocus-pocus the record simply

says that the secret was revealed to Daniel in a night vision. Daniel was able

to remember the dream and then interpret it. Some years later, Nebuchadnezzar's son, Belshazzar, was giving a feast, and during the course of the feast the fingers of a man's hand appeared on the wall behind the candlestick and wrote

a secret message; Belshazzar was very much upset and called for his soothsayers,

Chaldean sorcerers, magicians and so on, but they couldn't read the message--
apparently they couldn't even read the cipher characters! Well, Daniel was

called in and succeeded not only in reading the writing on the wall: "Mene,

in deciphering mene, tekel, upharsin", but also the meaning of the words. His interpretation was "Mene" -- God hath numbered thy kingdom and finished it. "Tekel" -- Thou

art weighed in the balances and found wanting. "Upharsin", or rather "Peres",

(apparently the chap who did the handwriting on the wall knew a thing or two

about cryptography, because he used "variants") -- Thy kingdom shall be divided

and given to the Medes and Persians."
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 the ancient Egyptian hieroglyphic writing was sometimes enciphered. But we pass over the history of the early days of cryptography with the foregoing brief mention. There is, however, that history which is writing of special notoriety which is the pot-hall, the ancient cipher device.
Greek. They had a 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 cylinder, 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 Tuscan 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 the princes and chancellories in the Papal states, about 1496. 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
Retyped pages—extra copy if needed—and obsolete pages from original draft 2 copy.
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. H. 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 periods, 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.
language, and this is what is said:

O, thou vile and insatiable monster! To disturb these poor bones!
If thou hadst learned something more useful than the art of
deciphering,
Thou wouldst 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
endorsement 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 be 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
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 fore-
going 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 Lacedemonians 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 cylinder, 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 Tironian 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 1485. 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
When General Twining invited me to address the staff and students of the Senior School of the Marine Corps on the subject "Communications Intelligence and Security" it was with pleasure that I accepted the invitation because I assumed that the objective of such an address is to give you some background information about the field to which those two subjects belong, namely, the science of cryptology. Suppose I propose to tell you something about that science, namely how it developed, and how to indicate the manner in which it can and has been employed as a vital military weapon.

My talk being divided into three parts or periods, I will give you first some of the historical background of cryptology. Next will come a presentation of the manner and instrumentalities 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 or SIGINT, in British terminology, whereby Communications Intelligence, or, for short, COMINT is obtained, how the function properly used and safeguarded, and its utility shown 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.
language, and this is what it said:

O, thou vile and insatiable monster! To disturb these poor bones! If thou hast learned something more useful than the art of deciphering, Thou wouldst 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 the war was over--or at least V-E and V-J days had been some months before. You'll remember the celebrated/controversial 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 and calamity as the Japanese had inflicted upon us at Pearl. This clamor had to be met; the matter could no longer be buried up, they contended, by the need for military secrecy. So there were investigations--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...
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.

Now, because of the secrecy or cloak of silence which officially surrounds the whole field of cryptology and especially cryptanalytics, it is obvious that authentic information with reference to the background and development of the science in foreign countries is quite sparse, and although after World War II we learned much regarding the accomplishments in this field of work by our enemies, security rules prevent my saying very much in detail about how good or bad they were in comparison with us. Suffice it to say that we looked pretty good in cryptologic affairs, together with our principal ally, Britain, we cryptologists naturally think we won the war, though others seem to have mislaid the peace somewhere.

I can only give a fairly good account of U.S. cryptologic activities up to a certain point of time, and even then I will not be able to say very much about them simply because the story is too long to give in a lecture or even a series of talks. In the course of my talk I will present a number of illustrations of
cryptography and cryptanalysis, some of which form part of my own experience. Modesty would dictate their omission, but because of their possible interest I will use them and will here and now make a general apology for the use of the personal pronoun.

Now may we have the first slide, please. Cryptography and cryptanalysis go back to the dawn of the invention of writing, and here I show an instance of cipher in the Bible. In Jeremiah 25:26 occurs the expression "And the king of Sheshakh shall drink after them." Also in Jeremiah 51:41: "How is Sheshakh taken!" Well, for many, many years that name "Sheshakh" remained a mystery. There was no such place. But then somebody discovered that if you write the twenty-two letters of the Hebrew alphabet in two rows, eleven and eleven, like this, you set up a substitution alphabet whereby you can replace the letters by those standing opposite them. For example, "Shin," is represented by "Beth" or vice versa, so that "Sheshakh" translates "Babel", or "Babylon." The vowels had to be supplied. Incidentally, mentioning the Bible, one might say that an early but not the first in the Bible--Daniel, who was psychoanalyst, was the first cryptanalyst. I say psychoanalyst, because you remember how he interpreted Nebuchadnezzar's dreams.
Some years later, Nebuchadnezzar's son, Belshazzar, was giving a feast, and during the course of the feast the fingers of a man's hand appeared on the wall behind the candlestick and wrote a secret message; Belshazzar was very much upset and called for his soothsayers, Chaldean sorcerers, magicians and so on, but they couldn't read the message—apparently they couldn't even read the cipher characters! Well, Daniel was called in and succeeded not only in reading the writing on the wall: "Mene, mene, tekel, upharsin", but also the meaning of the words. His interpretation was "Mene" -- God hath numbered they kingdom and finished it. "Tekel" -- Thou art weighed in the balances and found wanting. "Upharsin", or rather "Peres", (apparently the chap who did the handwriting on the wall knew a thing or two about cryptography, because he used "variants"!) -- Thy kingdom shall be divided and given to the Medes and Persians."
The next is an illustration of the earliest cipher device history records, a device which was called a *scytale*, used by the ancient Lacedemonians or Greeks. They had a 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-dimensional cylinder, 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 his story 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 Tironian notes, as they are called.

The beginning 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 the princes and chanceries in the Papal states, about 1486. 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