N THESE RECORDS WILL BE D FOR OFFICIAL PURPOSES DO NOT REMOVE PAPERS FINAL CONTENTS TO UNAUTHORIZED PERSON(S)

RECORDS CHARGE-OUT

5223

DATE OF REQUEST	SUSPENSE DATE
25 Mar '60	

FILE OR SERIAL NUMBER AND SUBJECT	From the Files of the Special Consultant - Friedman) Final Version of Lecture No. 1 - 24 pages (carbon copy), No. 2 - 24 pages, No. 3 - 19 pages and 1 page of notes. ~~CONFIDENTIAL~~ (All carbon copies)
TO	NAME AND EXTENSION OF PERSON REQUESTING FILE: Mr. William F. Friedman (Home) — ORGANIZATION, BUILDING, AND ROOM NUMBER: Special Consultant
RETURN TO	NSA Records Management Br, AG-24 - Christian — DATE RET'ND — INITIAL HERE
INSTRUCTIONS	WHEN TRANSFERRING FILE TO ANOTHER PERSON COMPLETE SELF-ADDRESSED TRANSFER COUPON BELOW, DETACH, STITCH TO BLANK LETTER-SIZE PAPER AND PLACE IN OUT-GOING MAIL SERVICE

2ND TRANSFER COUPON

5223

TO:

FILE (serial number and subject)

TRANSFERRED TO (name and extension)

ORGANIZATION, BUILDING, AND ROOM NUMBER

DATE | (sig) | (ext)

Final
Lecture . 1

LECTURE I

The objective of this series of lectures is to create an awareness of the background, development, and manner of employment of a science that is the basis of a vital military offensive and defensive weapon known as CRYPTOLOGY, a word that comes from the Greek kryptos, meaning secret or hidden, plus logos, meaning knowledge or learning. Cryptology will be specifically defined a little later; at the moment however, I'm sure you know that it has to do with secret communications.

Let me say at the outset of these lectures that I may from time to time touch upon matters which are perhaps essentially peripheral or even irrelevant to the main issues of cryptology, and if a defense is needed for such occasional browsing along the by-ways of the subject while travelling along the main highways of the science, I'll say that long preoccupation with any field of knowledge begets a curiosity the satisfaction of which is what distinguishes the dedicated professional from the person who merely works just to gain a livelihood in whatever field he happens to find himself a job. That's not much fun, I'm afraid. By the way, a British writer, James Agate, defines a professional as the man who can do his job even when he doesn't feel like doing it; an amateur, as a man who can't do his job even when he does feel like doing it. This is pretty tough on the gifted amateur and I for one won't go all the way with Agate's definition. There are plenty of instances where gifted amateurs have done and discovered things to the chagrin and red-facedness of the professionals.

Coming back now to the main thoroughfare after the foregoing brief jaunt along a by-way, I may well begin by telling you that the science of cryptology has not always been regarded as a vital military offensive and defensive weapon, or even as a weapon in the first place. Here I am reminded of a story in a very old book on cryptography. The story is probably apocryphal, but it's a bit amusing, and I give it for what it's worth.

It seems that about two thousand years ago there lived a Persian queen named Semiramis, who took an active 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 is reported that she met with 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 on the outside of which, on its front stone wall, there was to be graven a message, 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 inscription was a cryptogram, a jumble of letters without meaning or even pronounceability. For several hundred years the possibility of sudden wealth served as a lure to many experts who tried very hard to decipher the cryptogram. Thay were all without success, until

one day there appeared on the scene a long-haried, be-whiskered, and be-spectacled savant who, after working at the project for a considerable length of time, solved the cipher, which 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 several more cryptograms the last one of which may have involved finding the correct combination to a 5-tumbler combination lock--who knows? Well, he solved that one too, after a lot of work, and this enabled him to open the sarcophagus, inside which he found a box. In the box was a message, this time in plain language, and this is what it 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!

I'm frank to confess that many times during my 40-year preoccupation with cryptology, and generally near the middle and the end of each month, I felt that good old Queen Semiramis knew what she was talking about. However, earning money is only a part of the recompense for working in the cryptologic field, and I hope that most of you will find out sooner or later what some of these other recompenses are and what they can mean to you.

If Queen Semiramis thought there are other things to learn that are more useful than the art of deciphering, I suppose we'd have to agree, but we are warranted in saying, at least, that there isn't any question about the importance of the role that cryptology plays in modern times: all of

us are influenced and affected by it as I hope to show you in a few minutes.

I will begin by reading from a source which you'll all recognize--TIME magazine, the issue of 17 December 1945. I will preface the reading by reminding you that by that date World War II was all over--or at least V-E and V-J days had been celebrated some months before. Some of you may be old enough to remember very clearly the loud clamor on the part of certain vociferous members of Congress who had for years been insisting upon learning 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, for these Congressmen contended that the truth could no longer be hushed up or held back because of an alleged continuing need for military secrecy, as claimed by the Administration and by many Democratic senators and representatives. The war was over--wasn't it?--Republican senators and representatives insisted. There had been investigations--a half dozen of them, but all except one were TOP SECRET. The Republicans wanted, and at last they got what they desired--a grand finale Joint Congressional Investigation which would all be completely open to the public. No more secrets! It was spectacular! Not only did the Congressional Inquiry bring into the open every detail and exhibit uncovered by its own lengthy hearings, but it also disclosed to America and <u>to the whole world</u> everything that had been said and shown at all the previous Army and Navy investigations. Most of the

information that was thus disclosed had been and much of it was then still TOP SECRET; yet all of these precious secrets became matters of public information as a result of the Congressional Investigation.

There came a day in the Congressional Hearings when the Chief of Staff of the United States Army at the time of the Pearl Harbor Attack, 5-star General George C. Marshall, was called to the witness stand. He testified for several long, long days, eight of them in all. Toward the end of the second day of his 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. The letter was about codes. With frozen face, General Marshall balked at disclosing the whole letter. He pleaded most earnestly with the Committee not to force him to disclose certain of its contents, but to no avail. He had to bow to the will of the majority of the Committee. Here's a picture of General Marshall and Governor Dewey. I will now read from TIME a bit of information which may be new to many of my listeners, especially to those who were too young in December 1945 to be delving into periodical literature or to be reading any pages of the daily newspaper other than those on which the comics appear.

Said TIME, and I quote:

"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 had painstakingly constructed in a hidden room in Washington. With this machine, built after years of trial and error, of inference and deduction, cryptographers had 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, and had given ample warning of the Japs' sneak attack if only U.S. brass hats had been smart enough to realize it. Now, General Marshall continued the story of 'Magic's' magic.

1. "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.

2. "It had given the U.S. full advance information on the size of the Jap forces advancing on Midway, enabled our 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.

3. "It had directed U.S. submarines unerringly to the sea lanes where Japanese convoys would be passing.

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

TIME goes on to give more details of that story, to which I may later return but I can't leave this citation of what cryptology did toward our winning of World War II without telling you that the account given by TIME of the achievements of MAGIC makes it appear that all the secret intelligence gained from our reading Japanese messages was obtained by using that "harmless little machine" which TIME said was used in Tokyo by the Japanese Foreign Office. I must correct that error by telling you that the secret information we obtained that way had little to do with those portions of the MAGIC material which enabled our Navy to win such spectacular battles as those of the Coral Sea and Midway, and to waylay Japanese convoys. The naval parts of MAGIC were nearly all obtained from Japanese naval messages by our own very ingenious U.S. Navy cryptanalysts. At that time, I may tell those of you who are new, that the Army and Navy had separate but cooperating cryptologic agencies and activities; the United States Air Force was not yet in existence as an autonomous and separate component of the Armed Forces, and work on Japanese, German, and Italian air force communications was done by Army cryptanalysts admirably assisted by personnel of what was then known as the Army Air Corps.

It is hardly necessary to tell you how carefully the MAGIC of World War II was guarded before, during, and after the war until the Congressional Inquiry brought most of it out in the open. Some remaining parts of it are still very carefully guarded. Even the fact of the existence of MAGIC was

known to only a very few persons at the time of Pearl Harbor--and that is an important element in any attempt to explain why we were caught by surprise by the Japanese at Pearl Harbor in a devastating attack that crippled our Navy for many months. Let me read a bit from page 261 of the Report of the Majority of the Joint Congressional Investigation of the attack:

> "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 that the fact that 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 over-emphasize the importance of communications intelligence in World War II, but I think it warranted to read a bit more of what is said about its importance in the Report of the Majority. The following is 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 General MacArthur's operations officer, or G-3, throughout the war in the Pacific, has written: "The information G-2 that is, the intelligence staff, gave me in the Pacific Theater alone saved us many thousands of lives and shortened the war by no less than two years." We can't put a dollar-and-cents value on what our possession of COMINT meant in the way of saving lives; but we can make a dollar-and-cents estimate of what communications intelligence meant by shortening the war by two years, and the result of that estimate is that it appears that $1.00 spent for that sort of intelligence was worth $1,000 spent for other military activities and materials.

In short, when our commanders had that kind of intelligence 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, too,--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 this series of lectures, so let's get down to brass tacks. For those of you who come to the subject of cryptology for the first time, a few definitions will be useful, in order that what I shall be talking about

will be understood without question. Agreement on basic terminology is always desirable in tackling any new subject. In giving you the definitions there may be a bit of repetition because we will be looking at the same terms from somewhat different angles.

First, then, what is cryptology? Briefly, we may define it as the doctrine, theory, or branch of knowledge which treats of hidden, disguised, or secret communications. You won't find the word cryptology in a small dictionary. Even Webster's Unabridged defines it merely as "secret or enigmatical language"; and in its "Addenda Section", which presumably contains new or recently-coined words, it is defined merely as "the study of cryptography". Neither of these definitions is broad nor specific enough for those who are going to delve somewhat deeply into this science.

Cryptology has two main branches; the first is cryptography, or, very briefly, the science of preparing secret communications; and the second is cryptanalysis, or the science of solving secret communications. Let's take up cryptography first, because as a procedure it logically precedes cryptanalysis: before solving anything there must be something to solve.

Cryptography is that branch of cryptology which deals with the various means, methods, devices, and machines for converting messages in ordinary, or what we call plain language, into secret language, or what we call cryptograms. Here's a picture of one of the most famous cryptograms in history. It was the solution of this cryptogram which resulted in bringing America

into World War I on the side of the Allies on 6 April 1917, just about six weeks after it was solved. I'll tell you about it later in this series.

Cryptography also includes the business of reconverting the cryptograms into their original plain-language form, by a direct reversal of the steps followed in the original transformation. This implies that the persons involved in both of these bits of business, those at the enciphering and sending end, and those at the receiving and deciphering end, have some sort of understanding as to what procedures, devices, and so on, will be used and exactly how--down to the very last detail. The what and the how of the business constitutes what is generally referred to as the key. The key may consist of a set of rules, alphabets, procedures, and so on; it may also consist of an ordinary book which is used as a source of keys; or it may be a specialized book, called a code book. That cryptogram I just showed you was made by using a book--a German codebook.

To encrypt, is to convert or transform a plain-text message into a cryptogram by following certain rules, steps, or processes constituting the key or keys and agreed upon in advance by the correspondents, or furnished them by higher authority.

To decrypt is to reconvert or to transform a cryptogram into the original equivalent plain-text message by a direct reversal of the encrypting process, that is, by applying to the cryptogram the key or keys, usually in a reverse order, employed in producing the cryptogram.

A person who encrypts and decrypts messages by having in his possession the necessary keys, is called a cryptographer, or a cryptographic clerk.

Encrypting and decrypting are accomplished by means collectively designated as codes and ciphers. Such means are used for either or both of two purposes: (1) secrecy, and (2) economy. Secrecy usually is far more important in diplomatic and military cryptography than economy but it is possible to combine secrecy and economy in a single system. Persons technically unacquainted with cryptology often talk about "cipher codes", a term which I suppose came into use to differentiate the term "code" as used in cryptology from the same term as used in other connotations, as, for example, the Napoleonic Code, a traffic code, a building code, a code of ethics, and so on. Now, in cryptology, there is no such thing as a "cipher code". There are codes and there are ciphers, and we might as well learn right off the differences between them so that we get them straightened out in our minds before proceeding further.

In ciphers, or in cipher systems, cryptograms are produced by applying the cryptographic treatment to individual letters of the plain-text messages, whereas, in codes, or in code systems, cryptograms are produced by applying the cryptographic treatment generally to entire words, phrases, and sentences of the plain-text messages. More specialized meanings of the terms will be explained in detail later but in a moment I'll show you an example of a cryptogram in cipher and one in code.

A cryptogram produced by means of a cipher system is said to be in cipher and is called a cipher message, or sometimes, simply, a cipher. The act or operation of encrypting a cipher message is called enciphering, and the enciphered version of the plain text, as well as the act or process itself, is often referred to as the encipherment. A cryptographic clerk who performs the process serves as an encipherer. The corresponding terms applicable to decrypting cipher messages are deciphering, decipherment, and decipherer.

A cryptogram produced by means of a code system is said to be in code, and is called a code message. The text of the cryptogram is referred to as code text. This act or operation of encrypting is called encoding, and the encoded version of the plain text, as well as the act or process itself, is referred to as the encodement. The clerk who performs the process serves as an encoder. The corresponding terms applicable to the decrypting of code messages are decoding, decodement, and decoder. A clerk who encodes and decodes messages by having in his possession the pertinent code books is called a code clerk.

Technically, there are only two distinctly different types of treatment which may be applied to written plain text to convert it into a cipher, yielding two different classes of ciphers. In the first, called transposition, the letters of the plain text retain their original identities and merely undergo some change in their relative positions, with the result that the original text becomes unintelligible. Here's an authentic example of a

transposition cipher; I call it authentic because it was sent to President Roosevelt and the Secret Service asked me to decipher it. Imagine my chagrin when I had to report that it says "Did you ever bite a lemon?" In the second, called substitution, the letters of the plain text retain their original relative positions but are replaced by other letters with different sound values, by symbols of some sort so that the original text becomes unintelligible.

Nobody will quarrel with you very hard if you wish to say that a code system is nothing but a specialized form of substitution; but it's best to use the word code when a code book is involved, and to use substitution cipher when a literal system of substitution is used.

It is possible to encrypt a message by a substitution method and then to apply a transposition method to the substitution text, or vice versa. Combined transposition-substitution ciphers do not form a third class of ciphers; they are only occasionally encountered in military cryptography. Applying a cipher to code groups is a very frequently-used procedure and we'll see cases of that too.

Here's an example of a substitution cipher, and a very simple one. It was found on a German spy in World War II. Here's the cipher alphabet; here's the plain text which happened to be in German; and here's the cipher text or encipher ment.

Now for an example of a cryptogram in code. Here's a plain-text message in the handwriting of President Wilson, to his special emissary in London, Colonel House. Here's the cryptogram after the plain text was encoded, by Mrs. Wilson. The President then himself typed out the final message on his own typewriter, for transmission by the Department of State. It would appear that President Wilson lacked confidence in the security of the Department of State's methods--and maybe with good reason, as may be seen in the following extract from a letter dated 14 September 1914 from the President to Ambassador Page in London: "We have for some time been trying to trace the leaks, for they have occurred frequently, and we are now convinced that our code is in possession of persons at intermediary points. We are going to take thorough-going measures." Perhaps one of the measures was that the President got himself a code of his own. I must follow this up some day.

A cipher device is a relatively simple mechanical contrivance for encipherment and decipherment, usually "hand-operated", or manipulated by the fingers, as for example, a device with concentric rings of alphabets, manually powered. Here's an example--a cipher device with such rings. I'll tell you about it later. A cipher machine is a relatively complex apparatus or mechanism for encipherment and decipherment, usually equipped with a type-writer keyboard and generally requiring an external power source. Modern cryptology, following the trend in mechanization and automation in other fields, now deals largely with cipher machines, some highly complicated. Here's a picture of a modern cipher machine with keyboard and printing mechanism.

One of the expressions which uninformed laymen use but which you must never use is "the German code", or "the Japanese code", or "the Navy cipher", and the like. When you hear this sort of expression you may put the speaker down at once as a novice. There are literally hundreds of different codes and ciphers in simultaneous use by every large and important government or service, each suited to a special purpose; or where there is a multiplicity of systems of the same general nature, the object is to prevent a great deal of traffic being encrypted in the same key, thus overloading the system and making it vulnerable to attack by methods and procedures to be mentioned in broad terms in a few moments.

The need for secrecy in the conduct of important affairs has been recognized from time immemorial. In the case of diplomacy and organized warfare this need is especially important in regard to communications. However, when such communications are transmitted by electrical means, they can be heard or, as we say, intercepted, and copied by unauthorized persons, usually referred to collectively as the enemy. The protection resulting from all measures designed to deny to the enemy information of value which may be derived from the interception and study of such communications is called communication security, or, for short, COMSEC.

In theory, any cryptosystem except one, to be discussed in due time, can be attacked and "broken", i.e., solved, if enough time, labor, and skill are devoted to it, and if the volume of traffic in that system is large

enough. This can be done even if the general system and the specific key are unknown at the start. You will remember that I prefaced my statement that any cryptosystem can be solved by saying "in theory", because in military operations theoretical rules usually give way to practical considerations.

That branch of cryptology which deals with the principles, methods, and means employed in the solution or analysis of cryptosystems is called cryptanalytics. The steps and operations performed in applying the principles of cryptanalytics constitute cryptanalysis. To cryptanalyze a cryptogram is to solve it by cryptanalysis. A person skilled in the art of cryptanalysis is called a cryptanalyst, and a clerk who assists in such work is called a cryptanalytic clerk.

Information derived from the organized interception, study, and analysis of the enemy's communications is called communication intelligence, or, for short, COMINT. Let us take careful note that COMINT and COMSEC deal with communications. Although no phenomenon is more familiar to us than that of communication, the fact of the matter is that this magic word means many things to many people. A definition of communication that is broad enough for our purposes would be that communication deals with intelligent messages exchanged between intelligent beings. This implies that human beings, and human operators are involved in the preparation, encryption, transmission, reception, decryption, and recording of messages which at some stage or stages are in written form and in some stage or stages are in

electrical form as signals of one sort or another. But in recent years there have come into prominence and importance electrical signals which are not of the sort I've just indicated. They do not carry "messages" in the usual sense of the word; they do not convey from one human being to another an intelligible sequence of words and an intelligible sense. I refer here to electrical or electronic signals such as are employed in homing or directional beacons, in radar, in telemetering or recording data of an electrical or electronic nature at a distance, and so on. Information obtained from a study of enemy electronic emissions of these sorts is called electronic intelligence, or, for short, ELINT. The particular or specialized study of enemy radar signals is called RADINT. All these, COMINT, ELINT, RADINT comprise SIGINT, that is, signal intelligence. Cryptology is the science which is concerned with all these branches of secret signalling.

In this series of lectures we shall be concerned only with COMSEC and COMINT, leaving for others and for other times the subjects of ELINT, RADINT, and so on. This means that we shall deal with communications or messages.

Communication may be conducted by any means susceptible of ultimate interpretation by one of the five senses, but those most commonly used are seeing and hearing. Aside from the use of simple visual and auditory signals for communication over relatively short distances, the usual method of communication between or among individuals separated from one another by relatively long distances involves, at one stage or another, the act of writing or of speaking over a telephone.

Privacy or secrecy in communication by telephone can be obtained by using equipment which affects the electrical currents involved in telephony, so that the conversations can be understood only by persons provided with suitable equipment properly arranged for the purpose. The same thing is true in the case of facsimile transmission (i.e., the electrical transmission of ordinary writing, pictures, drawings, maps). Even today there are already simple forms of enciphered television transmissions. Enciphered facsimile is called CIFAX; enciphered telephony, CIPHONY; and enciphered television, CIVISION. However, these lectures will not deal with these electrically and cryptanalytically more complex forms of cryptology. We shall stick to enciphered or encrypted writing--which will be hard enough for most of us.

Writing may be either visible or invisible. In the former, the characters are inscribed with ordinary writing materials and can be seen with the naked eye; in the latter, the characters are inscribed by means or methods which make the writing invisible to the naked eye. Invisible writing can be prepared with certain chemicals called sympathetic or secret inks, and in order to "develop" such writing, that is, make it visible, special processes must usually be applied. Here's an interesting example--the developed secret-ink message that figured in an $80,000,000 suit won by two American firms against the German Government after World War I sabotage was proved. There are also methods of producing writing which is invisible to the naked eye because the characters are of microscopic size, thus

requiring special microscopic and photographic apparatus to enlarge such writing as to make it visible to the naked eye. Here's an example--a code message in a space not much larger than the head of a pin. A simple definition of secret writing would be to say that it comprises invisible writing and unintelligible visible writing.

There is one additional piece of basic information which it is wise to call to your attention before we proceed much further, and I'll begin by stating that the greatest and the most powerful instrument or weapon ever forged and improved by man in his long struggle for emancipation from utter dependence upon his own environment is the weapon of literacy--a mastery of reading and writing; and the most important invention, the one that made the weapon of literacy practical, was the invention of the alphabet. It is therefore a rather striking anomaly that we should now come to the study of another weapon--a counter-weapon to the weapon of literacy--the weapon of secrecy, the basic intent of which is to thwart the weapon that man struggled so long to forge. Secrecy is applied to make writing more difficult and the reading of the writing very difficult, if not impossible.

Perhaps this is a good place to do a bit of theorizing about this matter of secrecy and what it implies.

Every person who enciphers a piece of writing, a message, or a text of any kind, for the purpose of hiding something or of keeping something secret, does so with the idea that some other person, removed from him in distance,

or time, or both, is intended to decipher the writing or message and thus uncover the secret which was so hidden. A person may possess a certain piece of knowledge which he does not wish to forget but which he is nevertheless unwilling to commit to open writing, and therefore he may jot it down in cryptic form for himself to decipher later, when or if the information is needed. The most widely known example of such a cryptogram is found in Edgar Allan Poe's romantic tale The Gold Bug. That sort of usage of cryptography, however, is unusual. There are also examples of the use of cipher writing to establish priority of discovery, as did the astronomers Galileo and Huygens. Here's a slide which shows both examples. I suppose I should at least mention another sort of cryptic writing famous in literary history, the diaries of persons such as Samuel Pepys and William Byrd. These are commonly regarded as being "in cipher", but they were actually written in a more or less private shorthand and can easily be read without the help of cryptanalysis. Here's a picture of a page of Pepys diary.

Now there can be no logical reason, point, or purpose in taking the time and trouble to encipher anything unless it is expected that some other person is to decipher the cipher some time in the future. This means that there must exist some very direct, clear-cut and unambiguous relationship between the enciphering and deciphering operations. Just what such a relationship involves will be dealt with later but at this moment all that it is necessary to say is that in enciphering there must be rules that govern or

control the operations, that these rules must admit of no uncertainty or ambiguity and that they must be susceptible of being applied with undeviating precision, otherwise it will be difficult or perhaps impossible for the decipherer to obtain the correct answer when he reverses the processes or steps followed in the encipherment. This may be a good place to point out that a valid or authentic cryptanalytic solution cannot be considered as being merely what the cryptanalyst thinks or says he thinks the cryptogram means, nor does the solution represent an opinion of the cryptanalyst. Solutions are valid only insofar as they are objective and susceptible of demonstration or proof employing scientifically acceptable methods or procedures. It should hardly be necessary to indicate that the validity of the results achieved by cryptanalytic studies of authentic cryptograms rests upon the same sure and well-established scientific foundations, and are reached by the same sort of logic as are the discoveries, results, or "answers" achieved by any other scientific studies, namely, observation, hypothesis, deduction, induction, and confirmatory experiment. Implied in what I have just said is the tacitly understood and now rarely explicitly stated assumption that two, or more, equally competent and, if necessary, specially qualified investigators, each working independently upon the same material, will achieve identical or practically identical results.

Cryptology is usually and properly considered to be a branch of mathematics, although Francis Bacon considered it also a branch of grammar and

what we now call linguistics. Mathematical and statistical considerations play an ever-increasing and prominent role in practical cryptology, but don't let my statement of this point frighten those of you who have not had much formal instruction in these subjects. We have excellent cryptologists who have never studied more than arithmetic, and some of our best ones would hide if you were to go searching for mathematicians around here. What is needed is the ability to reason logically as the mathematician sometimes does and this ability is found in the most curious sorts of persons and places. So those of you who are frightened by the words mathematics and statistics take heart--you're not nearly so bad off as you may fear.

But now to return to the main theme as to the place mathematics occupies in cryptology, let me say that just as the solution of mathematical problems leaves no room for the exercise of divination or other mysterious mental or psychic powers, so a valid solution to a cryptogram must leave no room for the exercise of such powers. In cryptologic science there is one and only one valid solution to a cryptogram, just as there is but one correct solution or "solution set" to any problem in mathematics. But perhaps I've already dwelt on this point too long; in any case, we'll come back to it later, when we come to look at certain types of what we may call pseudo-ciphers.

In the next lecture I'm going to give you a brief glimpse into the background or history of cryptology, which makes a long and interesting story that has never been told accurately and in detail. The history of communications

security, that is, of cryptography, and the history of communications intelligence, that is, of cryptanalysis, which are but opposite faces of the same coin, deserve detailed treatment but I am dubious that this sort of history will ever be written because of the curtain of secrecy and silence which officially surrounds the whole field of cryptology. Authentic information on the background and development of these vital matters having to do with the security of a nation is understandably quite sparse.

But in the succeeding lectures I'll try my best to give you authentic information, and where there's conjecture or doubt I'll so indicate. I must add, however, that in this series I'm going to have to omit many highly-interesting episodes and bits of information not only because these lectures are of low classification but also because we won't and can't go beyond a certain period in cryptologic history for security considerations. Nevertheless, I hope you won't be disappointed and that you'll learn certain things of great interest and importance, things to remember if you wish to make cryptology your vocation in life.