3rd DRAFT

~~CONFIDENTIAL~~

LECTURE NO. 6

This lecture, the last ~~fourth lecture~~ in the series, will be divided into two parts. The first ~~of which~~ will be devoted to a brief review of developments ~~certain bits and pieces of~~ in the field of communication security during the period between the end of World War I and the beginning of World War II, developments which played a ~~historical information which may not at first appear to you as having very~~ role of importance far greater than you might at first imagine. This because it is not so spectacular as the one played by communications intelligence, which ~~much to do with our main theme—the history of cryptology. But, as I~~ will be treated in the second part of this lecture. As I intimated in the first lecture of this series, I do not think it necessary to ~~shall not~~ apologize for making an occasional detour ~~and digressions~~ from our two main themes, because digressions may be ~~In my opinion they should be interesting and~~ technically useful to those of you who ~~hope to make cryptology a profession and therefore~~ aim to become professionals. In both the first and the second part of this lecture ~~we shall return to our main theme, the history~~ I shall have to omit a great many items of information which have an important bearing upon the history of American ~~of~~ progress in the development of new ideas and methods in cryptology, especially ~~as~~ such as have been made in recent years. I have to omit them for ~~manifested in the codes and ciphers used by each side in the War Between the States, better known to most of you, perhaps, as the Civil War.~~ the reason that the security classification of this lecture is only confidential and it is obvious that not enough time has elapsed to permit disclosing information, no matter how interesting, which is of a higher classification.

My first digression will be to return Edgar Allan Poe ~~whom~~ and specifically to something I said about him at the end of Lecture No. 3, which on re-reading left me with the feeling that I had been a bit too ~~extraordinarily imaginative American poet and writer, who was the inventor~~ severe in my criticism of him as a cryptologist. Poe, of course, was the inventor of the type of fiction now commonly called "The Whodunit". It was Poe who ~~and who~~ made at least

3rd DRAFT

one contribution to the science of cryptology which is notable in the
and for which I we must ~~in duty bound to~~ give him full credit.
history of the subject. Here's an excellent picture of Poe, probably made in 1849, only a few years after he had attained fame and found life's vicissitudes too much a burden.

Many Americans believe that cryptology in America was born when Poe's story of the "Gold Bug" and his important article "A Few Words on
and I am convinced that
Secret Writing" had been published, ~~but~~ such a belief is ~~un~~warranted.
It is true that
In a previous lecture I mentioned James Lovell and characterized him as the one-man NSA who served the Continental Congress as cryptologist. But
Lovell's work has thus far remained wholly
since ~~that lecture I've come across an episode which occurred over a half~~
unknown to all but a very, very few of the ~~cryptologic~~ cognoscenti
~~century before Poe's exploits in cryptology, an episode of the American~~
in the world of cryptology, as against the world-wide acclaim
~~Revolution in which the work of two or three cryptanalysts of that period~~
that has come to Poe in that field, I for one am quite eager to
~~had consequences of first importance. Their work was in connection with~~
acknowledge the indebtedness of the cryptologic world to
~~uncovering the traiterious conduct of an American occupying a very prominent~~
Poe for a dictum of highest importance in the science.
~~position not only in the Continental hierarchy, as a member of the~~
~~Massachusetts Provincial Congress, but also in the hierarchy of the young~~
~~American Army. The traitor was Dr. Benjamin Church, Jr., who was Surgeon~~

3rd DRAFT

General in the Army and whose official title in the Army was that of Director-General of the Hospital and the respective Regimental Surgeons". As a British agent, Dr. Church was indiscreet: he used a cipher that was readily solved by a Reverend West, of Dartmouth, Massachusetts, and by two others, Elbridge Gerry, of the Committee of Safety, and Colonel Elisha Porter, of the Massachusetts Militia. The Church episode is exceedingly interesting but too long to tell in this lecture, so I'll reserve it for a future opportunity.

~~But now let's go back to Poe and see what he wrote~~ what did Poe write aside from The Gold Bug which makes his name notable in the history of cryptology?

First, how did Poe become interested in cryptology? It appears that in 1821 the interception by French security police of certain correspondence broke up a conspiracy to return the Bourbons to the throne which they had lost to the rival House of Orleans. The correspondence, which was between the Legitimist Duchesse de Berry and her conspirators in Paris, was in cipher but of a rather simple sort; it was monoalphabetic,

3rd DRAFT

with a modification that made solution a bit tricky. A French orator named Berryer solved the correspondence and the solution, as well as the whole affair, attracted a certain amount of interest in the world. In particular, the story attracted the attention of Poe whose natural inclination toward the obscure, the mysterious, and the enigmatical, led toward a reaction that could easily be anticipated: Poe became interested in cryptology. Now, it is quite likely that on first contact with the subject he was entirely self-taught, but it wasn't very long before he sought out what could be found in America on the subject, including what there was in at least three encyclopaedias, the Britannica, the Americana, and Abraham Rees' Cyclopaedia. There wasn't much in those three sources, ~~although it is true that, in the last named source, the article on "Cipher," by William Blair, was then the second most complete treatise in English to be found on the subject, the first being a little book by James Falconer, entitled Cryptomenysis patefacta, or the art of secret information, published in London in 1685. The rules for solving ciphers, as set forth in the reference works mentioned above would have taught Poe little that his own first-class intellect had not already discovered.~~ Poe was impressed by the

3rd DRAFT

paucity of information on the subject, ~~of cryptography (he didn't know about the writings of Falconer and Babin)~~ and at the end of the first installment of his four-part article entitled " A Few Words on Secret Writing," published in Graham's Magazine (July, August, October, December, 1841) he notes this fact and says:

> "If, however, there should be sought in these disquisitions--or in any--rules for the solution of cipher, the seeker will be disappointed. Beyond some hints in regard to the general structure of language, and some minute exercises in their practical application, he will find nothing upon record which he does not in his own intellect possess."

Note carefully that final remark that a person seeking ~~I think that Poe's comment on what can usually be found in the~~ information on the subject "will find nothing upon record which ~~literature available to the general public is still valid in large measure.~~ he does not in his own intellect possess". There ~~So, as I've already remarked, there~~ wasn't much information readily at hand in America on the subject of cryptology in Poe's time, but what there was Poe quickly absorbed and thus he became an expert--or so he thought. Perhaps I was a bit severe on him in ~~my~~ a preceding lecture when I said that Poe appears to have sincerely believed that any cryptogram he couldn't solve was not a valid cipher, and I cited a little ditty reflecting on such a naive belief. So now I'll try to make it up to those of you who happen

3rd DRAFT

to be Poe idolators by telling you some details about a cryptologic dictum he enunciated, a dictum which has become world famous in cryptologic tradition and which those of you who aim to become professionals in the field of cryptology should ponder over from time to time.

In a previous lecture it was pointed out that cryptanalysis is really a quite ancient art or science, but it seems clear that it was Poe who was the first to contend that there was no such thing as a cipher which can't be solved. Poe didn't say it quite that simply and baldly, as some people seem to think. Let's see exactly what he did say.

The very first time Poe wrote about cryptography, which was in a brief article that appeared on 18 December 1839, in a journal called "Alexander's Weekly Messenger," he said, with reference to the solution of enigmas and conundrums, that "...rules really exist, by means of which it is easy to decipher any species of hieroglyphical writing--that is to say writing where, in place of alphabetical letters, any kind of marks are made use of at random." At the end of this statement there is an asterisk calling attention to a footnote which appears at the end of the article.

3rd DRAFT

The footnote says:

> "For example--in place of A put † [a dagger] or any other arbitrary character--in place of B, a * [an asterisk] etc. etc. Let an entire alphabet be made in this manner, and then let this alphabet be used in any piece of writing. This writing can be read by means of a proper method. Let this be put to the test. Let any one address us a letter in this way, and we pledge ourselves to read it forthwith--however unusual or arbitrary may be the characters employed."

Several weeks later, on 15 January 1840, under the heading "ENIGMATICAL," the first response to this challenge appeared. Before giving the cryptogram, and its solution, Poe wrote:

> "Some weeks since, in an editorial article under this head [ENIGMATICAL], we mentioned that, with a proper method, it would be easy to decipher any piece of writing in which arbitrary signs were made use of in place of proper alphabetical characters--pledging ourselves, at the same time, to read any thing which should be sent to us thus written."

These two statements contain the germ of the idea which later was elaborated into what has come to be known as Poe's ~~world-famous~~ dictum. Let us see exactly how, a year and a half later, this germ of the idea was elaborated upon in his very first formal statement of his dictum, which appeared in the 25 March 1840 issue of "Alexander's Weekly Messenger." Here is what he wrote:

> "We assert roundly, and in general terms, that human ingenuity cannot concoct a proper cypher which we cannot resolve."

3rd DRAFT

Note carefully that word "We"--it undoubtedly is an editorial pronoun. It is almost absolutely certain that it could only refer to Poe himself, because no other person connected with "Alexander's Weekly Messenger" has ever been discovered to have dabbled in cryptography. Now why, let us ask, did Poe insert the word "proper" before the word "cypher" in this first formal statement of his dictum? The answer must be that he felt that in making his challenge he had to be careful to set up certain limitations upon the kind of ciphers he would undertake to solve, namely, simple ciphers, or what we now call monoalphabetic substitution ciphers, in which one and only one substitution alphabet is involved. By inserting that word "proper," with the connotation I have here elucidated, Poe must have felt that he had protected himself against any charge of fraud, because, as you all are or should by this time be fully aware, practically every monoalphabetic substitution cipher can be solved, no matter what characters are used in the cipher text, provided only that the original plaintext message is in an alphabetical language, is of sufficient length, say 25 or more characters, and you know a bit about the language involved. This is

3rd DRAFT

true even of the sort of "crypts" which appear in many of our daily newspapers, ciphers which are made difficult by the use of outlandish words and outrageous diction so as to suppress the normal frequencies of the letters of the English language, as exemplified in the following specimen:

Jmoud vag, Mhev gipsy, stalk mohr nth time. Mpongwe gunboy aims nickt khnum. Unfed, knab jhum, ngapi.

If you think I m trying to put over a fast one on you, or that there are typographical errors in this example, consult your Webster's unabridged English dictionary. You'll find every one of those words in it and what the message says makes sense — sort of sense, that is.

By setting up the limitation of monoalphabeticity Poe made certain that he could solve any challenge cryptogram; if he couldn't, then it meant that the challenge cryptogram was fraudulent, so far as he was concerned.

In the 22 April 1840 issue of "Burton's Gentlemen's Magazine," which

3rd DRAFT

was merely a continuation of "Alexander's Weekly Messenger" under a different name, Poe wrote at the end of one of his solutions: "We say again deliberately that human ingenuity cannot concoct a cypher which human ingenuity cannot resolve." Note, now, a simple but quite significant change in this, the second statement of his dictum. In the first version he equated "human ingenuity" with his own ingenuity--the two apparently were, in his opinion, equivalent. But in the second version he substituted for the "We" in the first version the phrase "human ingenuity.' Let's place the two versions side by side for comparison:

1) "We assert roundly, and in general terms, that human ingenuity cannot concoct a proper cypher which <u>we</u> cannot resolve."

2) "We say again deliberately that human ingenuity cannot concoct a cypher which <u>human ingenuity</u> cannot resolve."

(My emphasis)

Well, here you can easily see how these two statements or versions of Poe's dictum differ. In the first, Poe placed himself upon a very tall pedestal of cryptanalytic capability; in the second he becomes more modest and leaves room for other aspirants to the accolade. But I'm sorry to have to tell you that only a bit later, in a letter to a man named Frailey, whose challenge cipher message he'd just solved (it was the most

3rd DRAFT

difficult which he ever solved), he wrote: "Nothing intelligible can be written which, with time, I cannot decipher." Poe was rather jubilant about his solution of the Frailey cryptogram and perhaps he was justified--it was a very early, if not the earliest, case of the use of outrageous diction, such as is found in the modern "crypts" for the purpose of thwarting the would-be cryptanalyst. In Fig. 00 you see it just as Poe published it. In Fig. 00 you see the cryptogram with an inter-linear decipherment which you can easily read, and in Fig. 00 you see Poe's own interlinear decipherment of it.

PHOTO
FIG. 00

PHOTO
FIG. 00

PHOTO
FIG. 00

~~If you want to know more about this episode in Poe's cryptanalytic divertisments I suggest you read Prof. W. K. Wimsatt's illuminating article "What Poe knew about cryptography" in the September 1943 issue of the Publications of the Modern Language Association of America, or my own essay on Poe in the Signal Corps Bulletin, Nos. 97, 98 and 99, reprinted in [illegible]~~

3rd DRAFT

~~Cryptography and Cryptanalysis, Washington: Government Printing Office, 1942~~. I wish that Poe had never written that flamboyant sentence "Nothing intelligible can be written which, in time, I cannot decipher," because of its unbecoming immodesty, especially in view of his real lack of professional experience. It seems that Poe had reason to regret having made such a bold and bald claim, because, as you will soon see, in the third and final statement of his dictum, he once more modified it. This time his dictum becomes more consistent with reality and with the modesty that we like to see ~~is becoming~~ in the writings of one of the greatest literary figures of modern times.

Let us see how Poe worded the dictum in his third and final attempt to put his idea across. It is found in his short story "The Gold Bug." I've mentioned that tale twice already, but I'll now add that those of you who haven't read that story should do so before letting another day go by, for it is a fascinating one. It is told with an adroitness and perspicacity which nobody else in the world before or after him has surpassed or even equalled. In that tale Poe's dictum is stated when the hero says: "It

3rd DRAFT

may well be doubted whether human ingenuity can construct an enigma of the kind [such as the cryptogram in "The Gold Bug"] which human ingenuity may not, by proper application, resolve." In this form Poe neatly puts the matter in a manner that aptly expresses what professional cryptologists believe to be true today, save for one exception about which I hope you'll learn something in due time. [Insert attached] ~~But don't forget this: it was Poe who first formulated the dictum and~~ for this he deserves to be remembered for all time by all professional cryptologists. I would like to conclude this digression about Poe by quoting a paragraph which I have taken from Fletcher Pratt's Secret and Urgent and which I think quite interesting:

> "Poe has an important niche in the history of cryptography although he brought little or nothing new to the art but his taste for it and a natural skill in decipherment. He made it briefly popular in Philadelphia in the 1840's, but what was a great deal more important he attracted literary interest to the subject, particularly in France, where his works were received so much more enthusiastically than in his own country. The Gold Bug had numerous imitators there. Jules Verne three times introduced cryptograms and their solution as important elements of his stories, and Balzac found the mania for ciphers in fiction so widespread that he was moved to put a cryptogram three pages long into La Physiologie du Mariage. It must have amused the last writer greatly to discover that for years after there was hardly a writer on ciphers in any country who did not attempt to solve the Physiologie du Mariage cryptogram and fail in the attempt. Commandant Bazeries, the same who broke the Great

Insert to p.13

I have something to add now which ~~possibly~~ will seem a bit ~~so~~ anti-climactic ~~to~~ after what I've told you of the background of Poe's dictum. I came across it only quite recently in looking up a certain question in an old book on cryptology. Listen now to these words:

We are now attempting an arduous and difficult task; for all cryptologists have hitherto considered this method of writing [the writer here refers to what we now call the ~~repeating key~~ multiple alphabet system a repeating key] not merely extremely difficult ~~but~~ actually impossible to solve. I have always believed, however, that anything locked up by the use of a system may be opened by using the same system."

Who wrote this pearl of cryptologic wisdom? One of the master cryptologists of the Renaissance, none other than the Italian mathematician and physicist I mentioned several times before, namely, Giovanni Baptista Porta. The statement appears in the second edition of his De Furtivis Literarum Notis (Naples, 1602, Book IV, Chapter XVI, p. 119.) But let us note, too, that what Porta says on this question is certainly not quite the same as Poe's dictum. In fact, Porta's dictum ~~states~~ required ~~employs~~ the use of the same system to unlock a cryptogram that was used in locking it; that is, it implies that the ~~unlocker must use the key to unlock~~ only way to unlock a door is to use the same key that was used to lock the door — and we know that this is not true either of locks or of cryptograms. Hence, Poe's statement still stands as the very earliest expression of the basic dictum of ~~great importance~~ cryptology and therefore I say that for this alone Poe deserves to be remembered for all time by ~~all~~ cryptologists ~~all~~ the world over.

There are several more historical items I'd like to present by way of digressions from our main themes in this lecture. For instance, I'd like to tell you why Francis Bacon, the father of British cryptology, deserves credit for an invention which is not only basic in the science of electrical telegraphy, both the Morse dot and dash system and the Baudot or printing-telegraph system, but also is basic in modern electronic digit computer technology. But there just isn't time for any more detours. Let's get on with our history of inventions and developments in communication security and see how Poe's dictum fits into that picture.

3rd DRAFT

> Cipher of Louis XIV, finally spoiled the sport with an analytical essay demonstrating that the message was an elaborate fake, almost as carefully composed as a genuine cipher, and arranged to have a number of almost-clues."

If you'll take the trouble to look up what Bazeries says about this famous and unsolved Balzac cryptogram you'll find something interesting. Pratt says that Bazeries "finally spoiled the sport with an analytical essay demonstrating that the [Balzac] message was an elaborate fake." And so Bazeries does say. But one can only smile at the manner in which Bazeries demonstrated that the Balzac message is a fake. First he "demonstrates" that it can't be monalphabetic--and his reasoning leaves much to be desired. In fact, it is fallacious. Then he says that it can't be a system of transposition, which we may grant without argument. Bazeries then closes his reasoning by a simple denial that it is an encipherment of the genus of the cipher square [Vigenère]--but he doesn't even attempt to substantiate that opinion. Bazeries concludes:

> "Balzac, having wished to say that the question of the confessor and the lover was an indecipherable question, without doubt left two or three pages blank in his manuscript, and said to his editor: 'Fill this up as you please, with capital letters, small letters, figures, punctuation marks, etc, putting some of them right side

3rd DRAFT

up, some upside down, in a way that will form a ~~jumble mixture~~ sort of confusing intricacy which nobody will understand.'

"That's what he did.

"Thus the Balzac cryptogram is simply a facetiousness on the part of the author and is not the result of any cryptographic system whatever."

How like Poe! What Bazeries couldn't solve was not a valid cryptogram. Maybe he's right--I haven't tried to solve the Balzac cryptogram, so I don't know. Why don't some of you try it. ~~Here it is:~~ But be sure you get the correct version, which I believe is only to be found in the first edition of the Balzac work. There are other versions, I understand, made up exactly in the manner Bazeries claims the first one was composed.

~~So much for Edgar Allan Poe, the man who may be regarded as the~~ popular founder of American cryptologic doctrine and practice, although the technical accomplishments of James Lovell, whom I mentioned in a preceding lecture, were far better. But then Lovell remained unheard of as a cryptologist until quite recent times, when his achievements were turned up in the musty files of the Clinton Papers in the Clements Library, at Ann Arbor. ~~Some day I hope to tell you more about the incredible James Lovell, who is to be regarded as the real father of U. S. cryptology, not Edgar Allan Poe.~~

3rd DRAFT

Now we must go on with our story of the developments in the history of cryptology after Poe's time, that is, after the 1840's. It will be useful at this point to say a few words about the role played by the invention of electric telegraphy and by the rather rapid developments and improvements in electrical communications, for they brought about equally rapid developments and improvements in cryptographic communications and, as a concomitant, in cryptanalytic technology. And here I begin my second diregression from our main theme.

Of course, there can be no single and simple explanation for the rather rapid developments and improvements in cryptologic technology that began about the middle of the nineteenth century. It would be incorrect to ascribe them solely to the invention and development of the electric telegraph, but it is valid to assume that telegraphy, that is, electric telegraphy, now began to play the major role. I refer here particularly to that type of electric telegraphy which was invented and developed by Samuel F. B. Morse. Morse was primarily an American portrait painter but

3rd DRAFT

he had a good background of education in electrical studies. Aboard the packet-ship "Sully" in October 1832, returning from Europe, Morse developed plans for a telegraph recording instrument and laid down the principles for the first practical system of electric telegraphy. Morse's system was based upon a rather simple scheme and it was because of its simplicity that electric telegraphy became practical: short and long pulses of current in an electrical circuit, separated by intervals during which no current flows. The short and long pulses of current are termed respectively dots and dashes, so that people generally refer to the scheme as "The Morse dot and dash code." It will be well to stop right here and emphasize that the word "code" in this context does not have by connotation

3rd draft

of "secrecy" because there is not, and there never has been, anything secret about "The Morse Code." The word as used in this context simply means a "convention," "agreement," "set of rules," etc., as in the expressions "the Napoleonic Code," or a "building code," and the like. The Morse Code is merely a set of conventional equivalents for the 26 letters of the English alphabet, plus some additional ones for the 10 digits, and a few more for punctuation signs, such as comma, period, question mark, etc. Its usage in telegraphy spread very rapidly and soon it became famous throughout the entire civilized world. Basically, what were (or are) these equivalents? The answer is very simple: they are combinations and permutations of two simple elements: periods when a current of electricity flows in a circuit, separated by intervals during which no current flows. In other words, the Morse Code is a way of representing a set of about 40 elements (26 letters, 10 digits, plus several signs of punctuation) by combinations and permutations of only two elements--periods of current and periods of no current. It is true, however, that within each of these two periods, the "length" or rather the duration of the differentiating signals is variable, but the ratios between the shortest signal and the others are more or less fixed, since in manual operation the duration of the shortest signal and in turn the speed in words per minute depends upon the skill of the operator. When current is flowing, for instance, the duration of the flow is variable, the shortest, about 1/24th of a second, for a moderate word speed, representing a dot (E = 1 unit); the next in length, about 3/24ths of a second, representing a dash (T = 3 units); the next in length being a long dash, about 5/24ths of a second, representing the letter L (= 5 units); and the longest, being a dash of seven units in duration, representing the digit zero. These lengths are a bit theoretical. Likewise, the duration of the spaces, that is, the periods of no-current, are also variable in length: the space between the dot-dash components of a letter equals the length of one dot, (= 1 unit), except in certain dot letters (C, O, R, Y, Z) in American Morse, which contain a space equal in length of that of two dots. The space between the letters of a word is equal to three dots, and the space between words is equal to six dots. (Again, these lengths are a bit theoretical.) It is clear, therefore, that the Morse code is by no means one which is composed of but two elements, dots and dashes; and this is true also of the International Morse Code where there are no letters in which the dots are separated by spaces equal to two dots, nor are there letters with spaces longer than the length of three dots. It isn't even true that the Morse code is composed of permutations of three elements, dots dashes, and spaces, because, as indicated, the dashes are of several lengths and so are the spaces.

Morse was quite logical and clever when he devised his set of dot-dash-space equivalents for the letters of our alphabet, because from the very first he composed those equivalents in accordance with the normal frequencies of letters in English. To the letter E he assigned a single dot; to the letter T a single dash the shortest dash; to the letter I, he assigned two dots; to the letter A a dot followed by a dash etc. A few years later as Morse telegraphy spread all over the world, some modifications were made in Morse's original code when by international agreement a set of equivalents was adopted for international telegraphy, although in the United States the American Morse continued, and still continues, to be used, because of its supposedly greater efficiency. Both codes are shown below.

(Enc Brit Vol 21, p.883 (Enc Brit Vol 21, p. 883, 14th Ed.

<u>Photograph Morse Code</u>

3rd draft

I think that most of you, when you read or learn something about the Morse Code, probably hear, in your imagination, the "clatter-clatter" of a telegraph instrument representing dots and dashes. And when you listen to certain programs on your radio you hear the short and long high-pitched squeals of radio-telegraphy, representing the dots and dashes of the Morse Code sent at high speed. But Morse's first model of his telegraph system was a recording instrument--dots and dashes, separated by spaces, were recorded, that is, printed or indicated, upon a moving paper tape. Here's a picture of it. (Britannica, Vol. 15, p. 828) In April 1844, Alfred Vail, one of Morse's associates, made the important discovery that it was possible to read messages by sound. He noted that as a dot or dash is being recorded on the moving tape the printing lever makes two distinct sounds, one as it strikes against the stop limiting its motion in one direction and again in retreating, as it strikes, against the stop limiting its motion in the other direction. He noted that when a dot or a short dash is recorded the interval is shorter than when a long dash is recorded, and he found that signals could thus be read by the length of the intervals between sounds. Thus was born "the sounder." Because of its simplicity "sound" telegraphy spread like wild-fire; but, unfortunately, it retarded the development, or rather the re-birth, of "recording" telegraphy for many years. Nowadays, one seldom sees or hears the "clatter-clatter" of the Morse Sounder, for sound telegraphy suffered a lingering death when modern printing telegraphy was invented, developed and perfected. Today, in America, there are only a very few working veterans of the Morse sound telegraphy; progress has passed them by and soon there will be none remaining, except those few "old-timers" you may still see behind the ticket windows of railroad station offices in the country, in very small towns and hamlets. In international commercial radio-telegraph communications you can still hear the rapidly-interrupted whine of the Morse Code dots and dashes, although even in that field radio-printing telegraphy is rapidly expanding in usage.

If question be raised at this point as to why this lecture devotes so much time to "codes" such as the American and the International Morse Codes, which have little to do specifically with secrecy or cryptology, I can only say that in practical work the professional cryptologist uses his knowledge of these types of "codes" to good advantage, when he must straighten out errors or "garbles" or the like made in telegraphic transmission or reception. The information is therefore quite relevant and is sufficiently important in the cryptologic study of electrical communications to warrant the presentation of additional information of interest and pertinence.

Before passing on to my next digression, I think you will be interested in seeing the title page of what is believed to be the very first codebook which addressed itself specifically to the new technology introduced by Morse's electric telegraphy. Here it is. Note the date of publication, 1845, which was just one year after the first telegraph line in America, the one between Washington and Baltimore, was put into public use. As you can see, the codebook was produced by Francis O. J. Smith, one of Morse's partners, and it is dedicated to "Professor Samuel F. B. Morse", Inventor of the American Electro-Magnetic Telegraph." I said that that first telegraph line was put into public use in 1844 for originally it was built for experimental use, $30,000 having been appropriated by Congress in 1843 for this purpose five years after Morse had demonstrated his telegraph before President Van Buren and his cabinet early in 1838. You'll be amused to learn that soon after his telegraph had proved to be a great success, Morse offered his system and patents to the Government for

3rd draft

$100,000, but the offer was refused upon the recommendation of the Postmaster General, who reported that he was "uncertain that the revenues could be made equal to the expenditures"--this, after the immense value of the telegraph to the Government had became fully apparent. But perhaps the refusal was best after all, for had the offer been accepted the chances are good that the telegraph would have become a governmental monopoly, as is the case in every country except Canada and the United States. When Morse was turned down, he enlisted private capital, and in 1844 a company was organized to erect a telegraph live between New York, Baltimore and Washington. Ten years later, there were more than 50 telegraph companies in the United States using Morse patents, but now 100 years later, by act of Congress, there is only one company in the United States, the Western Union, which offers to the general public a domestic telegraph service wherein a message may be handed in "over-the-counter" or telephoned in for transmission. Western Union accepts overseas messages but transmits them via cable. On the other hand, radio-telegraph companies such as the Radio Corporation of America, the International Telegraph and Telephone Company, etc., cannot accept messages to be transmitted within the United States, but only overseas.

So much for the second diversion from my main theme. I have but one more, which I hope will be interesting and will give you some useful information.

Nowadays we see many references to certain relatively new machines called electronic digital computers, and "data-processing machines." These machines constitute a post-World War II innovation which offers a means to increase man's productivity in many different ways and at ever-increasing speeds--wherever large-scale, repetitive clerical and computational tasks can be mechanized, or wherever there is a possibility of speeding up operations, or of saving time, labor and money in processing large amounts of data. They can be "instructed" or "programmed" of great assistance wherever a great deal of information is needed to manage enterprises, run institutions, direct research, and plan endeavors. They are even being developed or modified to perform, or to assist in the performance of, large-scale language translation projects, in mathematical research, biological investigations, etc., etc. These machines are so versatile because they can deal with all such problems in one and always the same very simple way: they function according to one or the other of two and only two states or ways which may be termed "yes" or "no", the equivalents of which, in the language of electricity, are the conditions called "current-on" or "current-off", just as is the case in an ordinary electric-bulb in your home--the light is either "on" or "off", depending upon the position of the switchvwhich controls the flow of current to it. Because these two conditions can be changed electrically within the components of the computer, it can perform its operations at great speed, electronic speed in fact, and that's why such machines are called "electronic computers." But why are they called "electronic digital computers?" It is because they employ circuitry and mechanisms which function in what is termed the "binary mode", that is, according to a system that operates under one or the other of two and only two conditions representable by two and only two different symbols or digits which may be extended to denote all numbers or quantities no matter how large. The method is commonly called "the binary-digit system." The expression "binary digit" gave rise to the abbreviation or rather contraction "bit", coined by one of NSA's associates, Dr. John Tukey, of Princeton and the Bell Telephone Laboratories, by simply joining the first two and the last two letters of the expression. It is easy to understand that one could use any two symbols or digits but it is common nowadays to use "0" and "I", i. e., the first two of our ordinary series of digits 0, 1,...9. It is possible to represent or "encode" any sort of message--a printed page, a musical composition, a photograph, etc., etc.--by using only this pair of digits. To summarize, electronic digital computers operate on a method of notation or counting based upon the "binary scale," and a bit of explanation as to how they are able to count according to that scale will be useful if you are to understand certain fundamental principles underlying the functions and manner of operation of these computers.

In everyday life nowadays we add, subtract, multiply and divide according to a system of counting that is based upon the decimal or denary system, in which arithmetic notation is based upon "decades." Let me explain the idea in simple language. In our system of notation there is a sequence of ten symbols or numbers called "digits", namely, 6,7,8,9, and they have what is called "positional value," that is, the numerical value of a digit in a number consisting of two or more digits depends upon the position of that digit in the number under consideration. A digit at the extreme right in the number has a unitary value, that is, it represents as many units as the digit indicates. In a compound number the value of a digit to the left,of it has a value 10 times as large as that of the one to the right of it. The positions from right to left have these values:

10x 10 x 10 x 10 x 10,	10x10x10x10,	10x10x10,	10x10	10	1
or	or	or	or		
100,000	10,000	1,000	100	10	1

The foregoing simple presentation of the matter makes it clear that next to the left or "hundreds" position, and so on. Although we write numbers consisting of two or more digits from left to right, the numerical values of the individual digits composing the number increase from right to left by the successive powers of 10. The number 1796, for instance, represents one thousand seven hundred and ninety-six units of something being counted, weighed, or measured, that is, $10^3+(7\times10^2)+(9\times10^1)+6$, or $1000+700+90+6$,.

TheThe foregoing rather lengthy explanation may seem superfluous; in fact, it appears hardly worth so many words of exposition, because the matter to be (and it really is) very obvious to us now. But it took thousands of years of progress in civilization to invent or develop the very simple system of notation which we call the decimal or denary system. It is perhaps astonishing that none of the ancient civilizations of Africa or Europe had such a simple system. Let me remind you that in the Roman system of notation, which was based upon strokes, probably representations of fingers, there were separate symbols for numbers. "One" was represented by a single stroke (I); "five" (V), "ten" (X); "fifty" (L), "hundred" (C), "five hundred" (D), and "thousand" (M). The number 1848 was represented by eleven letters--MDCCCXLVIII. Later, by subtraction, 4 was written as IV; 9, as IX; 40, as XL. Sometimes a bar over a symbol multiplied its value by 1,000; thus $\bar{x}$ = 10,000; $\bar{C}$ = 100,000; $\bar{M}$ = 1,000,000. How would you like to find the square of the number 1796 using Roman notation? Many ancient civilizations used systems of notation similar to that of the Romans, and they were all rather cumbersome, compared to our present system. It is hardly a curious fact that practically the world over systems of numeration were based upon counting by tens--because fingers were (and still are) used in counting and we have ten of them. (The word "digit" comes from "digitus" and means "finger" or "toe", although nowadays we say that our hand comprises four fingers and a thumb.) The denary system

-3rd draft

including both the idea of the positional value of notation and the idea of a having a symbol for zero, was invented in India, and was brought to Europe by the Arabs.

But there are systems of counting other than by tens. Man has five fingers on each of two hands, and five toes on each of two feet. He thus has a counting "abacus" arrangeable on a scale or radix of 5, 10 or 20. Systems based upon radix 10 are very convenient, as, for example, in our American currency system: 10 cents make a "dime," 10 "dimes" make a dollar, etc. But a scale of 12 is also very convenient, the number 12 being divisable by 2,3,4, and 6. In matters other than financial or currency we still in the United States use the British system of counting; we use their system of linear measurement which is based upon 12 inches to the foot, their system of weight measurement, which is based upon 12 ounces to the pound, and so on.

But I now wish to say a few words about a system of counting based upon the radix 20, the so-called vigesimal system, which is the one that was used by the Celts in Europe 2000 years ago and by the ancient civilizations of Central America. Consider, for instance, the mathematical system of the ancient Maya of Yucatan, who thousands of years ago were great astronomers. Inde-

3rd draft

pendently of the Hindus of India, or of the Arabs, or of the Europeans, and probably much earlier than them, the Maya invented or discovered two ideas of first importance in any efficient system of enumeration: they had a symbol for "zero" and their symbols had positional value, just as do the digits in our present-day denary system. A symbol or unit in the last (or units) place in the Maya system had the value "1"; it took 20 such units to make a unit in the next-to-last place, and so on, so that in their system the positional values of the symbols went thus:

6th Position	5th Position	4th Position	3rd Position	2nd Position	1st Pos.
20^6	20^5	20^4	20^3	20^2	20^1
20x20x20x20x20x20	20x20x20x20x20	20x20x20x20	20x20x20	20x20	20
64,000,000	3,200,000	160,000	8,000	400	

Such a system made it easy for the Maya astronomers to represent very high numbers with great economy in the use of symbols. In practice, the Maya wrote their numbers vertically (not horizontally, as we do), the units position being the bottom one. They also had special symbols for the multiples 20, 400, 8000, etc. It is an astonishing fact that the great mathematicians of neither ancient Greece nor of ancient Rome seemed to have any inkling of either the concept of "zero" or that of the positional value of symbols in numeration.

Once you have these two ideas, problems of arithmetic become much easier than in the case of Egyptian, Greek or Roman numeration. One more curious fact: Greenlanders use the counting system based upon radix 20 and some people wonder if this a bit of evidence of the tropical origin of the Greenlanders.

We come now to the binary scale used in electronic digital computers. In the binary scale, the binary digits, or "bits", also have positional value, proceeding from right to left, as in the denary system, but, as already mentioned, only two digits or symbols are involved in the binary system. Only one of them has a value, and that value progresses from right to left according to the scale 1, 2, 4, 8, 16, 32, 64, 128,..., that is, on the progression of the powers of 2. This can be seen in Figure wherein are set down the binary equivalents for the decimal numbers 0, 1, 2, 3, ...31.

3rd draft

Column No.	5	4	3	2	1		
Binary value	16	8	4	2	1		
Binary equiv.	0	0	0	0	0	=	0
" "	0	0	0	0	1	=	1
" "	0	0	0	1	0	=	2
" "	0	0	0	1	1	=	3
" "	0	0	1	0	0	=	4
" "	0	0	1	0	1	=	5
" "	0	0	1	1	0	=	6
" "	0	0	1	1	1	=	7
" "	0	1	0	0	0	=	8
" "	0	1	0	0	1	=	9
" "	0	1	0	1	0	=	10
" "	0	1	0	1	1	=	11
" "	0	1	1	0	0	=	12
" "	0	1	1	0	1	=	13
" "	0	1	1	1	0	=	14
" "	0	1	1	1	1	=	15
" "	1	0	0	0	0	=	16
" "	1	0	0	0	1	=	17
" "	1	0	0	1	0	=	18
" "	1	0	0	1	1	=	19
" "	1	0	1	0	0	=	20
" "	1	0	1	0	1	=	21
" "	1	0	1	1	0	=	22
" "	1	0	1	1	1	=	23
" "	1	1	0	0	0	=	24
" "	1	1	0	0	1	=	25
" "	1	1	0	1	0	=	26
" "	1	1	0	1	1	=	27
" "	1	1	1	0	0	=	28
" "	1	1	1	0	1	=	29
" "	1	1	1	1	0	=	30
" "	1	1	1	1	1	=	31

Figure 1 - Binary representation of decimal values 0 - 31

Note the neat and orderly manner in which the 0's and 1's are arranged within columns from right to left: single alternations in the last column on the right.

alternations of pairs in the 2nd column from the right, alternations of sets of 4's in the 3rd column, of sets of 8's in the 4th column, and alternations of sets of 16's in the 5th column.

In Figure 00 are shown only the first 32 permutations of the binary digits 0 and 1. And the reason for stopping with these 32 permutations is that I wish to demonstrate an interesting if not an astonishing fact, namely, that Francis Bacon, whose biliteral cipher system, invented in 1583, was explained in detail in the second lecture of this series, was really the first inventor of the principle underlying the pure binary scale! Whereas Bacon assigned the letter equivalents A, B, C, ... Z to systematically-arranged permutations of the two elements of his binary scale, composed of "a's" and "b's", in computer technology these very same permutations (but of "0's" and "1's" instead of "a's" and "b's") are used to represent the numbers of the sequence 0, 1, 2, 3, ... But the fundamental principle is unquestionably the same, as can be seen by placing the first 24 permutations of "0's" and "1's" of the modern binary scale alongside the sequence of "a" and "b" equivalents Bacon established for the letters of the alphabet as used in the days of Elizabeth I (Figure 2). The coincidence is quite remarkable.

Column No.	5	4	3	2	1	Decimal Value
Binary value	16	8	4	2	1	
Binary equiv.	0	0	0	0	0	= 0
" "	0	0	0	0	1	= 1
" "	0	0	0	1	0	= 2
" "	0	0	0	1	1	= 3
" "	0	0	1	0	0	= 4
" "	0	0	1	0	1	= 5
" "	0	0	1	1	0	= 6
" "	0	0	1	1	1	= 7
" "	0	1	0	0	0	= 8
" "	0	1	0	0	1	= 9
" "	0	1	0	1	0	= 10
" "	0	1	0	1	1	= 11
" "	0	1	1	0	0	= 12
" "	0	1	1	0	1	= 13
" "	0	1	1	1	0	= 14
" "	0	1	1	1	1	= 15
" "	1	0	0	0	0	= 16
" "	1	0	0	0	1	= 17
" "	1	0	0	1	0	= 18
" "	1	0	0	1	1	= 19
" "	1	0	1	0	0	= 20
" "	1	0	1	0	1	= 21
" "	1	0	1	1	0	= 22
" "	1	0	1	1	1	= 23

Bacon's Biliteral Alphabet					
Letter	Permutation				
A	a	a	a	a	a
B	a	a	a	a	b
C	a	a	a	b	a
D	a	a	a	b	b
E	a	a	b	a	a
F	a	a	b	a	b
G	a	a	b	b	a
H	a	a	b	b	b
I - J	a	b	a	a	a
K	a	b	a	a	b
L	a	b	a	b	a
M	a	b	a	b	b
N	a	b	b	a	a
O	a	b	b	a	b
P	a	b	b	b	a
Q	a	b	b	b	b
R	b	a	a	a	a
S	b	a	a	a	b
T	b	a	a	b	a
U - V	b	a	a	b	b
W	b	a	b	a	a
X	b	a	b	a	b
Y	b	a	b	b	a
Z	b	a	b	b	b

Fig. 00. - Computer binary equivalents and Bacon's biliteral alphabet.

I add now another curious and quite interesting fact.

When Bacon enunciated his biliteral alphabet, composed of permutations of two things through five places, nobody had yet conceived of such a thing as electric telegraphy. But Bacon's "code" of a's and b's came to enjoy its birthright several hundred years after he devised it, when electric printing telegraphy came into use. It is rather astonishing to note that

Bacon's "code" of permutations of two different signs taken in sets of five (of which he used only 24 out of the possible total of 32 permutations) is now actually employed in its entirety the world over in practical electrical printing telegraph systems! In the latter, however, the permutations, although the same as those used in Bacon's "code", are assigned alphabetic equivalents different from those Bacon had assigned them. For instance, in Bacon's system, the first permutation, aaaaa, represented A; aaaab, the next permutation, represented B, and so on, in a neat, orderly sequence, as seen in Figure OO. But in a practical system of electric printing telegraphy the assignment of characters and functions to the successive permutations was dictated by two factors: (1), economy in the use of electrical energy and (2), reduction to a minimum of wear and tear on the mechanical apparatus. We come now to a consideration of the first of these factors, viz., economy in the use of electrical energy, and in such consideration we shall take a good look at the "code" used for modern printing telegraphy.

One of the most widely used systems of printing telegraphy systems is that in which there is for each character a "start" impulse at the beginning of the set of five signals for a character, and a "stop" impulse at the end of the set. This system is commonly referred to as the "5-unit code, start-stop" printing telegraph system. In this system, there is, as in Bacon's system, a "code" based upon the permutations of two things taken in sets of five; in this case the two things are "current" and "no current," or "positive current" and "negative current." Thus, if we use "+" and "-" as symbols to represent the two electrical states involved, Bacon's aaaaa = A could be represented as +++++; B could be represented ++++-, and so on. But in printing telegraph systems the assignment of the permutations of "+'s" and "-'s" to represent the characters to be transmitted are made according to a scheme which takes into consideration something other than a desire to make the alternations of the "+'s" and "-'s" conform to the neat sequential or systematic pattern of Bacon's biliteral alphabet. Thus, if "+" represents "current" and "-" represents "no current," it is obvious that the greatest efficiency and economy in the use of electrical energy and the least wear and tear on mechanical parts would be obtained by assigning the permutations in accordance with the normal frequencies of letters and punctuation signs. And, as for the second of the two factors mentioned above, it is obvious that here again such assignments would result in the least amount of wear and tear on mechanical or moving parts. Thus, the letter E is assigned the permutation /----; the letter T, ----/; the space between words, --/--, etc., since in each of these permutations there is but one instant in the cycle of five time periods when current is flowing. A "code" of this type was designed many years ago by a French inventor and engineer named Baudot, and the "code" is now generally referred to as the Baudot Code. The unit expressing speed in electric signalling, the baud, is named in his honor.

In Fig. 00 the Baudot Code is presented in the form of a picture of a piece of perforated tape for a controlling a printing telegraph system. Each character is represented by one or more "character holes" which may be punched in five different positions or "levels" across the tape, i.e., transversely to its length. Since in each of these five levels a hole may be present or absent, there are 2^5 or 32 possible permutations, of which 26 are used to represent characters, and 5 are used to control certain functions of the printing mechanism, viz., "space," "carriage return," "line feed", "figure-shift", and "letter-shift", leaving one permutation (no hole in any level) which is the "blank" or "idling" signal. The "letter-shift" and "figure-shift" permutations permit doubling the number of characters that can be represented. When the "letter-shift" precedes a section of tape, the punch-permutations that follow are interpreted as alphabetic characters; if "figure-shift" precedes, the punch-permutations that follow are interpreted as numeric or special characters.

Careful scrutiny of Fig. 3 will confirm what has been said about the assignment of punch-permutations on the basis of statistical considerations, for purpose of economy and efficiency in the use of electric power and wear and tear on the apparatus. The most frequently used letters (or functions) are represented by punch-permutations having the fewest holes; the least-frequently used letters (or functions) are represented by permutations having the most holes. Thus, "line feed," "carriage return," "space," and the letter E are represented by one-hole punch-permutations; the letters T, R, I, N, O, A, ..., are represented by two-hole punch-permutations, etc. In referring to a hole or a blank (or no-hole) one often says "a hole (or perforation) in the 1st (or the 2nd, 3rd, 4th, or 5th level"), or "a blank in the ... level."