~~TOP SECRET~~

MR. FRIEDMAN'S RECORDED LECTURE

The talk today is to give you a bit of background -- historical background -- of a very old subject - cryptography and cryptanalysis. To give you an idea of how ancient this study is, I would like to tell you a little story which I came across in an old book on cryptography. I don't know how true it is, but it is a good story and I would like to tell it.

There was, it seems, an old queen in Persia about 2,000 years before Christ. Her name was Samarimus. She died and presumably went to heaven. She had had a great interest in cryptography, and at the end of her days she caused her remains to be entombed in a beautiful sarcophagus. On the outside of the tomb she had caused to be engraved a cipher message and above the cipher message she had put the following legend: "O weary traveler, if thou art footsore, hungry or in need of money, unlock the riddle contained in the cipher message below and you will be lead to riches beyond all dreams of avarice".

For many, many years the cipher message remained unread until one day along came a bewhiskered professor, I presume, who after much labor succeeded in unlocking the riddle. It gave him directions for entering the tomb and he got inside, and when he did so he found a box; inside the box was another box and inside the second box a third; and so on, until he came to a tiny box inside of which was a piece of parchment. And

this was what was written on the parchment, "O, vile monster, to disturb these weary bones. If thou hadst learnt something more useful than the art of deciphering - thou wouldst not be hungry, footsore or in need of money".

And I presume that every so often each of you, when you come to examine your accounts probably think that the old gal had something. Now we will proceed with the slides:

Slide 1

Here is a slide which gives you a rebus. Those of you as children, remember how you would be interested in this form of secret writing: "Good reader as you older grow, you see that is an old chair, you will learn what now you," etc. Now the alphabet and cryptography, I believe, came from this very early form of rebus writing.

Slide 2

In the Bible we find at least two instances of cipher writing: In Jeremiah, 25th Chapter, Verse 26, there occurs the expression: "and the king of Shashak shall drink after them". And again in Jeremiah: "How is Shashak taken". Now for many, many years this name "Shashak" was unknown, and not so long ago it was discovered that if you take the 22 letters of the Hebrew alphabet and write the first 11 on one line and the second 11 on the line below you have set up a reciprocal alphabet for substitution; so that "Shashak", you will see,

translates BBL, Babel, Babylon. In those days, of course, Hebrew writing didn't have the vowels, those had to be supplied, and so we see that "Shashak" stands for Babylon. Below, I have a representation of another ancient form of cipher writing among the Jews - the form which is now known as "Masonic writing". The angles formed by the lines are used to represent the various letters of the alphabet. So, as you see, in the lower left hand corner, the angle opening toward the right stands for "A", or "1" and with the dot in it stands for "I" or "10", and so on. As children, no doubt, you made use of a similiar type of design.

Slide 3

Among the ancient Greeks and Lacedemonians, there was in use a device known as the scytale. The device is pictured on this slide, but is not correct. It really should terminate in a point instead of being strictly with parallel sides. The way in which they used the device was this: When the commander of the field forces left for his command he was given a scytale of certain dimensions and an identical scytale was retained at the war office. When they wanted to send a message to the commander they wrapped a piece of parchment spirally around the scytale, and wrote along the edges of the parchment, and not as is shown on this slide; so that in order to read the writing, theoretically, you would have to have an identically dimensioned scytale on which you would wrap the parchment,

thus bringing together the bits of lines which go to make up the letters. It is interesting to note that the baton which the field marshal today carries around as one of the insignia of his high office, is derived from the scytale.

Slide 4

There are two forms --basic forms -- of cipher writing; one known as substitution, in which you replace the letters of the plain text with other letters or characters; and in the second form you transpose or re-arrange the letters. Here is a simple example of a substitution type of cryptography. This, I took from a Christmas card which was sent to me a number of years ago from one of the Signal Corps units. You will see the top line has three characters. It is in the "wigwag" code as it was called. T-H-E, and the next line reads, "season's"; "The Season's Greetings - etc". A very simple example of cipher writing.

Slide 5

In the next slide I have some examples of quite old forms of cipher writing. The top one is an alphabet which was used by Charlemagne. There are numerous examples underneath but I won't have time to go into these, because I think I have some better examples later on.

Slide 6

Sir Thomas More in his book about Utopia included at the end the type of writing which he called the "Utopian Alphabet"

and I thought it was interesting to show you what it looked like. I took this from a book which was published in 1524.

Slide 7

A number of years ago they came across a papyrus in Egypt which was very mysterious. The professors couldn't make out whether it was in Egyptian writing or some other form of ancient writing, and for many years the significance of this parchment was unknown. Not long ago a young man without the wide background that the professors who had studied the parchment were fortunate to possess, came across this manuscript, and applying the principles of simple substitution cipher finally succeeded in deciphering the writing. It turned out to be the formula used by a gentleman who apparently specialized in beauty work. That is, he was an ancient beautician, I suppose.

Slide 8

Now as old as that form of simple substitution is, nevertheless, even today, we come across examples of it every now and then. You will remember only two or three years ago, there was a sergeant in the United States Army who was arrested for being connected with a spy ring, and this is the type of cipher that was used by this group -- simple substitution. You will notice the characters are inter-lined with their equivalent plain text in German, and then the translation in English.

Slide 9

The idea of having multiple substitution came very early in the art. As you will see here, in 1401, there was used an aplhabet that had multiple representation for the high frequency letters. You see four characters to represent "a" and four to represent "e" and so on. This is the earliest known example of that type of substitution.

Slide 10

It was indeed used by Mary, Queen of Scots, and this is an example of one of the alphabets used by her in certain correspondence. You will notice that there are two or three equivalents for some of the high frequency letters.

Slide 11

The "Porta Alphabets" are well-known in the art of cryptography. They were invented and described by an Italian cryptographer named Porta, in 1563. This slide is a modern representation of those alphabets. You will see that there are reciprocal alphabets in the top section. The key letters "a" and "b" will represent that particular alphabet wherein "a" is represented by "n" or "n" is represented by "a" and in the next section the key letters "c" and "d" will represent the keys where "a" is represented by "z" and "b" by "n" and so on.

Slide 12

I show in the next slide the form in which Porta set forth his alphabets in his own book. Those of you who care to see the original edition of Porta's great work, and indeed he was a great cryptographer in those days, may see the book.

I have it with me.

Slide 13

This slide is turned the wrong way but it also represents a case in which the key letters can be used to produce multiple representation, or multiple-alphabet encipherment. That is a very old device used by Queen Elizabeth.

SLIDE No. 2

Slide 14

In this case you will notice that the key words are optimus dominus, and in order to represent a letter of the plain text you take the co-ordinates which indicate the position occupied in the diagram by the letter that you are enciphering. "A", for example, would be represented by "OD", and so on.

Slide 15

Many of you have heard about the Viginere Square. This was supposed to have been invented by a great French crypyographer and described by him in a book about 1587. The square consists of 26 normal alphabets, simply arranged in cyclic order, with the plain text letters at the top and the key letters at the side. The book itself shows the square in a little different form.

Slide 16

Here you will notice that the key letters and the plain text letters at the top and side are displaced a bit and, in

fact, Viginere does not say that the key letters and the letters at the top have to be in normal order. He says you can mix those up if you wish to, and that is a point which has been overlooked by pretty nearly all commentators on Viginere's work.

Slide 16

Francis Bacon was very much interested in cryptography. In one of his earliest books, De Augmentes Scientarium, he published a description of a cipher system which he says he invented when he was a youth in Paris, and that was over forty years before. I found it interesting enough to show you what it is about. Bacon says, draw up a biliteral alphabet - you will see that at the upper part of the left hand corner of the slide - in which you have five "a's" representing the letter "a" and [redacted] 4 "a's" and a "b" representing the letter "b" and so on. In other words, what you have here are permutations of two things through five places giving you a possible alphabet of 32 characters. But we only need 24 of those. In those days "i and j", and "u and v", were considered the same letters. So there are the 24 permutations which Bacon says we can use for a biliteral alphabet. Then he goes on and says if you want to represent a plain text word by means of such an alphabet, just replace the letters of the word by the permutations given in your alphabet. So you have in the lower part of the left hand slide an example, "fuge,"

in which the letter "f" is represented by "A,A,B,A,B," the "u" by "B, A,A,B,B," and so on.

Slide 17

Now here is an example of the way in which you would use such an alphabet in a very simple, rather amusing form. This was done for me by a doctor friend of mine who got interested in the subject, and the bricks are of two kinds, you will notice in this castle. Some of them are plain and some of them are shaded. And if you cinsider a brick which is plain as an "a" form and one which has shading, a "b" form, and start reading those bricks from left to right and from the top downward this is what the message says:

"My business is to write prescriptions and then to see my doses taken; but now I find I spend my time endeavoring to out-Bacon Bacon."

Slide 18

Here is a further example of that same sort of alphabet. Here is a picture. It might pass any sort of scrutiny by a censor, but if you examine it very carefully you will see that some of those officers are looking straight forward and some are looking to the left side or the right side. If you will assign the letter "a" to any of the officers who are looking straight forward, and the letter "b" to those who are looking to one side or the other, and take them in groups of 5, beginning at the rear row, the left hand part of the picture, you will get the following message: Knowledge is power". That

incidentally is a picture of the first class in cryptography in the United States operated in the last war. I had the good fortune to be director of that school. It was out in Chicago.

Slide 19

Now, Bacon goes on to say that that is a very simple scheme, but we are going to make it a little bit better. We are going to show you how to enfold a message in an external text so that it will not be evident that you are conveying a cipher message, or a secret message. So he draws up what he calls a bi-formed alphabet in which you have two kinds of capital "A's" and two kinds of small "a's" and 2 kinds of capital "B's" and two kinds of small "b's", etc. Then if you will take those capital letters of the two different kinds and the small letters of the two different kinds, and manipulate them in accordance with the requirements of the secret message which you want to enfold, you can put across, externally, an innocent-looking message, but it will contain an internal secret message. As for example, in this case: Here is a message which reads "Berta terrais" etc. "All is lost; Maoris is killed; the soldiers want food; we can neither get hence nor stay longer here." It's a difficult situation to be in. But here is how he enfolds the message. On the right hand side, you will see the external message in which that secret message has been enfolded by a proper use

of the two different kinds of type.

Slide 20

Now I have often had people say to me, "Well, that sort of thing is pretty far-fetched. I don't think that anybody could get away with a secret message enfolded in that manner today." But I think that it is possible. For example, here is a paragraph which I put in one of the texts which I wrote a number of years ago, and it contains a secret message, and I doubt very much whether anybody would suspect that it does contain a secret message. In fact, if I hadn't put the footnote 2, there which reads" "the sub-paragraph which the student has just read contains a hidden cryptographic message. "With the hints given in paragraph 35e, let the student see if he can find it." In fact I believe if I had not done this, nobody would ever suspect that it contains a secret message; and even with that hint there have been very few people who have solved and found the secret message. I won't give that message to you right now.

Slide 21

Thomas Jefferson used a simple code. In fact it is what we call a syllabary, today. Here is a section of that syllabary. You will see that the plain text words are represented by combinations of digits. This is the deciphering section of that syllabary. You will see that the numbers run in numerical order and are accompanied by their meanings, and those are in

random order. There was, of course an encoding version in which the words and the phrases, a few of them, arranged in alphabetical order accompanied by their equivalent code groups in random order.

Slide 22

Here is a picture taken from a frontespiece of an old book of cryptography, dated 1794. The lady at the desk, I presume, is the version of the WACs that they had in those days. The gentleman who is dictating to her is giving her a plain language message to encipher. She has before her something which is labeled, "Table a Chiffrier"! I guess she is enciphering the message, and in the cabinets and drawers alongside the wall you see the various keys or key lists that were used in those days. At the top you have bottles or containers that no doubt contain secret ink materials.

Slide 23

This slide shows a photograph of a message which is known today as the Benedict Arnold "indecipherable cow" letter. Nobody has suceeded in finding the meaning of this message. Obviously, there isn't enough of it here to do anything with. The secret meanings of certain of the words were agreed upon between Arnold and his correspondent. The message begins, "I have bought a cow and calf from General John Joseph Bullus," and so forth. I don't think that anybody will succeed in deciphering this message. I show it merely as a matter of interest.

~~TOP SECRET~~

Slide 24

The use of cryptography had considerable stimulus during our Civil War. Here is an instrument which was used by the Confederate Army, captured at the Battle of Vicksburg. Cryptographically it is nothing but the Viginere cipher in which the Viginere table has been wrapped around the cylinder and the pointers that you see on the bar at the top can be slid into position, one to represent your plain text letters, and the other to represent the key letter; and then you could rotate the cylinder forward or backward as you had to find the letters involved.

Slide 25

This message was supposed to have sent by President Lincoln in 1862. It is addressed as you see to General Burnside, Falmouth, Va. And if you read it from left to right, it doesn't make very much sense, but if you will read backwards you will see that it does contain a pretty good message. "If I should be in a boat off Aquia Creek at dark tomorrow, Wednesday evening, could you without inconvenience meet -see the WORD flesh represents meat - and pass an hour or two with me. A. Lincoln." I don't know how authentic this is. I came across it in a secret British text on cryptography.

Mr. 7. The source is Bates' Lincoln in the Telegraph Office. I think it authentic Glover

Slide 26

The Federal Army used a cipher known as the route cipher. In this form they would have a design of certain dimensions --

~~TOP SECRET~~

certain number of columns and rows and the message would be inscribed in that design and taken out by following a certain route as you will notice in this case of this example. The top diagram begins with the number one in the lower right hand corner. After you had written your message in that design you would take the words out by taking the last work in the last row and then going up the column and then diagonally to the left and so on. In addition, to that simple form of transposition they had arbitary groups which represented the names of important people. For example, the president of the United States was represented by "Adam or Asia;" the secretary of state by "Abel or Austria," etc.

Slide 27

Here is an actual message which was sent in a system of that sort and addressed to General Grant. "For U. S. Grant, no expedition to Texas will be undertaken," and so forth.

SIDE 3

Slide 28

The period of the World War we come to next, the first world war. I want to show you some examples of the cryptography used by the various belligerents.

Here is the type of cipher used by the Russians. The plain text alphabet is seen at the top and then underneath are several rows of cipher equivalents composed of two-digit

combinations. The key is shown in the first column - 31456782, apparently taken from about 10 different lines of numbers and rearranged according to the key for the day. The table below is the deciphering version of that same system. You will notice that in the enciphering version the equivalents for the letters are in random order so that you had to have a deciphering version of the same system. You will notice that in the enciphering version the equivalents for the letters are in random order so that you had to have a deciphering table.

Slide 29

Here is the type of cipher which was used by the French Army at one time in World War I period. They had a transposition rectangle made up of a certain number of columns with the day numbers at the top and instead of taking the letters out of the columns in simple key number order, they drew diagonals through certain places in that diagram and took the letters out of the diagonals first; and then they took the remaining letters out of the columns in key number I won't undertake to go through this example, but you will see that it is a bit more complicated than simply taking the letters out of the columns in key number order.

Slide 30

The Italians used a modified form of Vigenère square. Here it is. Instead of having letters to represent the letters of the plain text they had numbers, but the basic principle of the scheme is exactly the same as the Vigenere

square which I showed you a few minutes ago. The numbers internally in that square, you see, run in strict serial order.

Slide 31

The Germans used a form of Cipher which we call the "adfgvx" cipher because the text of the messages consisted solely of the letters "adfgvx". The method of encipherment is as follows: Suppose you had a message, plain text: "request reenforcements immediately." There would be a square with the key internally disposed in the lines and columns as you will see at the upper right hand corner. In that particular square the letters read to QU, I can't make out the next one, 5ST, etc. disarranged internally. The co-ordinates are in normal fashion, adfgvx, both at the side and at the top. Now you encipher your message first by replacing the letters of your plain text by the two letter combinations given by this cipher square. As you will see the line marked biliteral substitution, "r" is represented by "xd", "e", by "af", "q" by "aa" and, so on. The next step is to have a key word from which you derive a sequence of numbers in disarranged order. You will find alongside the expression "key word": "the quick brown fox jumped." And the key numbers 14, 16, 6, 2, etc. derived by numbering the letters of that key sequence in accordance with the position the letters occupy in the normal alphabet. Next thing is to take the two letter equivalents for this plain text message and write them underneath the columns and

the diagram formed by putting down those key numbers. As you will see the letter "r" in the upper part of the diagram is represented by "xd", so you have "xd" in the first two positions of the first line of the final diagram. Next comes "af", "aa", "ad", etc. When you have finished writing out those two letter equivalents in that fashion then you take the letters out of the columns in key number order. In this case, the message begins "adaf". You see where the column is headed by the digit 1, so that you will see what the transposed text is like. That is a pretty complicated cipher and I might say that in those days this cipher was used by the high command for only its most important messages. We didn't know in those days how to solve this type of traffic unless there were some special cases to work with; for example, messages which began alike or messages which ended in a similar fashion. But nevertheless, and despite the fact that we could only handle the traffic when we had those favorable cases, we did succeed in reading approximately 75% of all the traffic that was transmitted in that system.

Slide 32

Now we come to a bit about code. Roughly code is a type of cryptography in which entire words and phrases, sometimes entire sentences, are replaced by groups of letters. Here you see an example of a type of code which you can obtain by going to a telegraph or cable office. This is one

put out a number of years ago by the Commercial Cable Company. The code groups you see in the heavy black letters are all five-letter groups. They differ from one another by at least two letters. If you will take any one of them you will find that there are two letters which distinguish that group from any other group in that code. The method of use of course if very simple. You replace the words and phrases that you wish to transmit by the equivalent code groups as you find them in the book.

Slide 33

Now there are all sorts of codes suited to different businesses, specializing in rubber, textiles, automobiles, etc. Here I show you a slide of a code used in China called the "Official Chinese Telegraph Code". In this example the characters are disposed in regular rows and columns 100 of them to a page and each character is represented by a number. A very simple method of use.

Slide 34

Here is an interesting example of a highly specialized code. There are as you know lots of people who believe in the treatment of disease, not by means of medicines, by by the use of proper words; and here is a code gotten out by a meta physician who believed in the treatment of disease by the word method; and he fixed it up so that even if he

was away, or if the patient was away, he could treat the patient by means of the proper message. In this he was apparently well versed in some of the phases of practical cryptography. His code groups show not only a two-letter difference but a three-letter difference. He realized that it might be pretty serious matter to have a mistake made in transmission and so he wanted to insure that the mistakes would be corrected. It would be a rather serious thing if you were to think that you were suffering from delerium tremens and got treated for coma.

Slide #35

A French Army Code of the World War 1 period. Here you see the plain text codes are in alphabetic order accompanied by code groups in random order. The groups in this case being 4-digit groups and therefore thissort of a code required two parts, an encoding version and a decoding version. This is a picture of the encoding version.

Slide #36

The code used by the German Army. I think I should mention that in the World War 1 period the use of code books did not begin until about 1917. It was thought at that time that the code books could not be produced in the field and nobody tried it until the Germans first came out with one the latter part of 1916. This is a picture of a couple of pages from the codebook captured in early 1918. The plain

text words you will notice are in the left hand side of the columns and the code groups at the right. In this code, the groups begin with the letters "K-R-U-S-A", so we call it the "Krusa" code. You will see that some of the words have more than one equivalent, and at the bottom of the page you see what are called "Blinde Signalen", which means "dummy groups."

Slide #37

When the American Army first got to France, they were in a rather bad way for codes. Here is an authentic example of a code made up under the circumstances and it is rather interesting to me. You will see that was used by the 52nd Infantry Brigade dated 17th of April 1918. If you wanted to indicate "casualties", the word "killed" was reported by "strike out"; "seriously wounded" - "base on balls", "slightly wounded" - "hit by pitched ball". In the lower part I notice some very interesting names probably of no significance to most of my audience. I wonder if anyone of you remembers who Johnson, was or Leonard or Wagner, etc.

Slide #38

Here is a picture of a page from a British field code. They had the code sectionalized. Here for example, is a section on "gas and gas attack" relating to our forces and long phrases in complete sentences representedby 3-digit groups in numerical order. This, of course, required encipherment so that it was a two-step process for them.

Slide #39

Now when the Americans came, we didn't have any codes, as I told you, but we first began using what was called the "playfair cipher", copied from the British, as a matter of fact. Here is an example of how the "playfair cipher" operates. You have a keyword which is inscribed in a square with the rest of the unused letters of the alphabet in a normal sequence. This square happens to have only 25 positions, so that the letter I and the letter J are treated as the same letter. Now, if you have a message "The enemy moves at dawn" and you want to encipher that, you have to follow certain rules for drawing up your equivalents. The letters "TH", for example, are represented by "HW"; a diagraphic cipher in other words. I will not undertake to tell you in detail how this cipher operates.

Slide#40

Well, as I told you, we first started out with the "playfair cipher" and then we began making up codes and here is an example of one of the field codes printed at GHQ in the AEF. These codes were replaced every ten days and it was a great source of astonishment to our British and French allies that we could do that. They were unable to produce their codes nearly as rapidly as the Americans could. Here you see the words are listed in alphabetical order, accompanied by their code groups in random order; and there are many variants.

Slide #41

Now we are going to take a few examples of types of ciphers which were encountered in the last war by censorship. For example, here is a card which was mailed in New York on August 8, 1916 addressed to a Mr. Charles Mcalvin, in London.

Slide #42

Now on the back of that card there appeared some writing in German, but if you read it as it runs, why, it doesn't make any sense.

Slide #43

However, if you apply to the text a grill, which is a device containing apertures in certain positions, then

(Slide #44)

you see that the words of the messages come out in their intended order. In this case, it reads "Lieber Charles Zei Mit, etc." "Dear Charles, Be very careful with the following secret message."

Slide #45

And you could apply that grill in one or all four positions that are possible. Now here is a form of cipher writing using music. Many people think that we have something brand new and suggest that it would be possible to convey a secret message by means of an apparently innocent sheet of music. This actually comes from a very old book of cryptography. Nevertheless, every once in a while we do

run across instances of the use of music for conveying secret messages by people who are unskilled in the art of cryptography.

Slide #46

Here is a map which was found on the person of a spy in the last war. It is a map of a city in Denmark and nothing particularly noticeable about it except that if you examine it very carefully, you will see dots and dashes along one of the tramways. Now when those dots and dashes were written down,

Slide #47

they still didn't make sense, but as you will see, the elements of a simple substitution cipher have been applied to this thing. The top line of dots and dashes are in the Morse equivalent for the letters BTADC and so on. Then if you apply the particular type of cipher alphabet involved in that, the BTA comes out "OEL" the word "oil", "Oil has been received and everything is ready."

Slide #48

Many people have an idea that they can enfold a secret message in an apparently innocent text by putting the secret words in certain positions, every 4th on every 5th etc. and here is an example of a case where a person intended to have every 4th word make the sense of the secret message; but the clue is given in the second and third lines of the first paragraph. You see how the word fourth stands out in the

middle of the second line and the word "word" at the beginning of the third line, so that the clue is the "4th word". Now if you will take the (Slide #42) message in the next paragraph and read every 4th word, you will see that it reads "Great gain in arms although still very far etc.)