CLASSICAL CRYPTOGRAPHY COURSE
BY LANAKI

25 DECEMBER 1996
Revision 0

LECTURE 21

CRYPTANALYSIS OF THE NAVY CSP 1500 CIPHER MACHINE
[HAGELIN C-38 FAMILY]

SUMMARY

Lecture 21 looks, in some detail, at an early cipher machine, the Navy CSP 1500 cipher machine, which is the equivalent of the Hagelin cipher machine, type C-38, to illustrate some of the interesting cryptographic principles surrounding the era of cipher machines and the famous engineer Hagelin. We develop our subject via a select group of references. [FR8], [NICH], [BARK], [DOW], [KULL]

MACHINE CIPHER SYSTEMS

Cryptographic principles or methods which are too complicated for hand operation may nonetheless be readily mechanized and become highly practical. Electrical and electromechanical cipher machines have been developed which are capable of producing cryptograms of great complexity; these cipher machines are to be differentiated from cipher devices, which are relatively simple mechanical contrivances for encipherment and decipherment, usually hand-operated or manipulated by the fingers, such as sliding strips or rotating disks. [Who would have guessed that we would equip SEALS with hand sets to access satellites via encrypted channels and that the newest CRAY system will perform 3 Trillion calculations per second - a cryptographers dream computer.]

Back to history circa 1930. Machine cipher systems may be classed into two broad categories: (1) literal systems, in which the plaintext and ciphertext symbols produced or accepted are alphabetical characters and digits; and (2) nonliteral systems, designed for the transmission of data in which the symbols or signals produced or accepted are other than the normal alphabet and the digits (e.g. teleprinter, ciphony, cifax, civision, etc.) Furthermore, literal cipher machines may be divided into two general classes of key generators and alphabet generators, or a combination of the two; nonliteral machines are usually of the key generator class. [FR8]

TRANSPOSITION CIPHER MACHINES

Transposition machines are rarely encountered although they do exist. Rudolf Zschweigert was granted a patent on 12 November 1920 in Germany on the first transposition cipher machine. The problems of letter storage, and automatic transposing of letters within lines and the irregular displacements of the key are not were not easily accomplished.

SUBSTITUTION CIPHER MACHINES

Substitution methods lend themselves much more readily to automatic encipherment than do transposition methods. The substitution principle lends itself ideally to mechanization by cipher machines; these cipher machines range from the most primitive types which afford only monoalphabetic substitution to very complex types in which the number of alphabets and the length of the keying cycle run into the millions. If the encipherment is monoalphabetic for a succession of 20 or more letters before alphabet changes, the cryptosecurity is low, especially if the various alphabets are interrelated as a result of their derivation from a limited number of primary components. In some cipher machines the number of secondary alphabets is quite limited, or the manner in which the mechanism operates to bring cipher alphabets into play is so ingenious that the solution of cryptograms produced by means of the machine is exceedingly difficult. [FR8]

Other things being equal, the manner of shifting about or varying the cipher alphabets contributes more to the cryptosecurity than does the number of alphabets involved, or their type. It is possible to employ 26 direct standard alphabets in such an irregular sequence as to yield greater security than is afforded by use of a 1000 or more different random-mixed alphabets in a regular way or an easily ascertained method. inventors sometimes forget this principle. [FR8]

In the following paragraphs we will discuss the CSP 1500 which is the U.S. Navy version of the Hagelin C-38 cipher machine as a typical key generator.

HAGELIN C-38 CIPHER MACHINE FAMILY

Historically - in the United States the Hagelin Cryptograph is probably best known as the U.S. Army's M-209 or the U.S. Navy's CSP-1500. [Later versions were designated by Hagelin as C-48 but I will focus on the C-38 plain vanilla machine.] This machine is one of an array of ingenious machines invented and manufactured by a Swedish engineer by the name of Boris Caesar Wilhelm Hagelin. The C-38 (CSP 1500 or M-209A) is a small, compact, hand-operated, tape-printing, mechanical cipher machine, weighing 6 pounds, with overall dimensions 7.25 " x 5.50 " x 3.5 ".

The cryptographic principle embodies polyalphabetic substitution, employing a complex mechanical arrangement to generate a long running key which is used in conjuction with reversed standard alphabets for the primary components. In encipherment, the machine in effect subtracts (mod 26) each 0p from the key to yield the 0c, and subtracts each 0c from the key to yield the 0p. Actually, the machine adds the key to the complements of the plain or of the cipher. Remember that I used the designation of "theta", i.e. 0c, 0p, 0k for the cipher, plain and key, to represent characters or letters without indicating its identity. So rather than "any letter of the plain text," we use the symbol 0p and so forth. Because of the subtraction feature , the C-38 and machines of similar genre have been called "letter subtractor machines."

PICS

References with pictures of the Hagelin C-38 [C36/C48] include: Friedman's "Military Cryptanalytics Part II - Volume 2," page 463, published by Aegean Park Press, C- 45, 1985; Barker's "Cryptanalysis of the Hagelin Crypt ograph," C-17, by Aegean Park Press, 1978; [BARK -pages 1, 124,127,131] ; "Operating Instructions for Converter M-209," U.S. Army, Technical Manual 11-380, 17 March 1944; Oakley, "The Hagelin Cryptographer - Model C-38, Converter M-209: Reconstruction of Key Elements," 12 May 1950; Kahn's "The Codebreakers," Macmillan Co., page 429, 1967; Deavours, Cipher A. and Louis Kruh, "Machine Cryptography and Modern Cryptanalysis, Artech House, 1985. Several excellent Cryptologia articles have pictures of the Hagelin machines.

I recently sent a DOC file with a picture of the outside of CSP 1500 machine to our CDB. It is readable in WORD 6. Thanks to both PHOENIX and MEROKE for the CSP 1500 DOC picture file. A copy of page 463 from [FR8] has been sent to all my non-Internet students.

WHEELS OR ROTORS

The CSP 1500 has six wheels or rotors of identical diameters; these wheels have individual periods of 26, 25, 23, 21, 19, and 17. Equidistant around the peripheries of the wheels are engraved the following sequences of letters:

Rotor I or "26 wheel": ABCDEFGHIJKLMNOPQRSTUVWXYZ
Rotor II or "25 wheel": ABCDEFGHIJKLMNOPQRSTUVXYZ
Rotor III or "23 wheel": ABCDEFGHIJKLMNOPQRSTUVX
Rotor IV or "21 wheel": ABCDEFGHIJKLMNOPQRSTU
Rotor V or "19 wheel": ABCDEFGHIJKLMNOPQRS
Rotor VI or "17 wheel": ABCDEFGHIJKLMNOPQ

At each lettered position there is associated a small pin near the edge of the wheel, which pin may be pushed to the left (or "inactive position") or to the right (or "active position"). The six wheels of the CSP 1500 move one step with each encipherment or decipherment; If they are initially aligned at AAAAAA, the second alignment will be BBBBBB, the 18th will be RRRRRA, and the 27th will be ABDFHJ. The formal name of these wheels is "variable pin rotors," to distinguish them from "fixed pin rotors" used in some types of cipher machines, and from "wired rotors used in electrical cipher machines.

Since the number of wheels are relatively prime to each other, the cycle of the machine will be the product (26x25x23x21x19x17) or 101,405,850; in other words, the wheels will not return to their initial position until after this number of letters has been enciphered.

THE SQUIRREL-CAGE

Just behind the six wheels is a revolving drum something like a squirrel-cage, composed of two circular retaining plates holding 27 horizontal bars, on each of which are two lugs, one or both of which may be set at six effective positions (corresponding to the six wheels) on the bar, or to neutral positions. The retaining plates actually had 29 slots, and in some models were equipped with 29 bars. The pins, when in the active position on a specific wheel, serve to engage those lugs which have been set opposite that wheel causing the particular bars to be displaced slightly to the left; these displaced bars act as teeth of a gear wheel, displacing the reversed standard alphabets a corresponding number of positions. In reality, an 'active' pin, when it reaches the sensing or 'reading' position, pushes back a key- wheel lever situated behind its wheel, and it is this lever that engages the lugs in that wheel position and causes the bars to move to the left; a lever in the forward position does not come into contact with lugs. If Rotors I-VI are aligned at the apparent or 'window' setting of AAAAAA on the bench mark, the reading or effective positions of the six wheels will be at PONMLK.

The number of lugs in the path of a particular wheel is known as the kick of that wheel; the total kick or key is the sum of all the kicks contributed at a given position of the six key wheels, as governed by those key-wheel levers which are in a position to contact the lugs on the drum. When both lugs on a bar have been set to effective positions, the activity of either one or both of the wheels involved will still contribute only one kick for that bar, since the bar acts as one tooth of a gear. This situation is known as the double lug effect, and the amount of overlap (i.e, the number of displaced bars having two effective lugs) must be subtracted from the total number of lugs actuated at a given setting to ascertain the actual total key; for example, if wheels with kicks of 1, 4, and 7 are the only ones at a given position with effective kicks, and if among the bars displaced there is an overlap of 2, the total key is (1+4+7) -2 =10.

LETTER ENCIPHERMENT

The encipherment (or decipherment) of a letter is accomplished by obtaining the sum mod 26 of the key and the complement of the letter. For example, assuming the juxtaposition of the reversed standard alphabets to be fixed as:

```
   Plain :  ZYXWVUTSRQPONMLKJIHGFEDCBA
   Cipher:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

I R(plain) is enciphered at a setting of the machine where the total key is 5, the cipher equivalent is N (cipher), measured 5 intervals to the right of the complement, I: if the key were six, E (plain) would be enciphered as B (cipher); etc. In the operation of the CSP 1500, the kick imparted to the type wheel is in the order of the ascending alphabet, whereas the sequence on the indicating disk moves in the reverse direction. The relative juxtaposition of the reverse standard alphabets may be varied by what is known as a slide , which has the effect of adding a constant to all the elements of key being generated by the machine. The slide is brought about mechanically by adjusting the relative displacement of the type wheel and the indicating disk. In the example above, the slide was really A=Z (=0,mod 26). If instead of K - P = C we express the Hagelin formula as P(bar) + (K + S) = C, where P (bar) is the complement (The complement of a number a, mod m, is m-a). of the plain and S is the slide, and if we use the mod 26 scale:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21

V	W	X	Y	Z
22	23	24	25	0

It can be seen that if R (plain) is enciphered with a kick of 7 and a slide of 22, then:

```
  R(bar-plain) +(7 +22) = (26-18) +(7+22) = 37
                        = (11, mod 26) =  K (cipher)
```

Since the CSP 1500 employs reciprocal alphabets, the operations of encipherment and decipherment are complementary; therefore the decipherment formula is C (bar) + (K + S) = P, as is shown by the example

```
  K(bar-cipher) +(7 + 22) = (26-11) +(7+22) = 44
                          = (=18, mod 26) = R (plain)
```

AN EXAMPLE OF KEY GENERATION IN THE CSP 1500

As an illustration of the generation of key in the CSP 1500, let us assume that the six wheels have the following pattern of active (x) pins and inactive (.) pins:

```
Rotor I  : ABCDEFGHIJKLMNOPQRSTUVWXYZ
           ..xxx.x.x x...xx.xxxx..x.x

Rotor II : ABCDEFGHIJKLMNOPQRSTUVXYZ
           .x.x.x..x.x....xxxx.xxxx.

Rotor III: ABCDEFGHIJKLMNOPQRSTUVX
           .x.xx.x..x..xxxx.x.x.xx

Rotor IV : ABCDEFGHIJKLMNOPQRSTU
           xx.x.x.x.xxx....x...x

Rotor V  : ABCDEFGHIJKLMNOPQRS
           ..xxxx.x.x..x...xxx

Rotor VI : ABCDEFGHIJKLMNOPQ
           x..xxxx...x...x.x
```

Let us also assume that the lugs have been set up against their respective wheels as shown below (with the overlap distributed as is indicated by the brackets):

```
        I   II   III   IV   V   VI
       |--2--| |-----1------|
        8    9    4    1    6   2
```

The sum of the kicks of the individual wheels is 30; this number minus the three overlaps shows that 27 bars have been used. With this particular overlap pattern, when wheels I and II are effective, their combined kick is 15; when II and V are effective, their combined kick is 14: and when wheels I, II, and V are effective, their combined kick is 20. If the rotors are aligned so the effective setting is at HHGNKF (so the apparent setting in this case would be SSQBSM) and if the slide is o, (if the slide were any value than 0, the total key would be increased by a constant equal to the amount of the slide) the generation of the first 30 key elements is shown in the following diagram: [The brackets in the individual key streams mark the cycle of the respective key wheels in terms of the initial alignment.]

```
          1  2  3  4  5  6  7  8  9  10  11  12  13  14
          --------------------------------------------
--- I     .  8  .  8  .  .  .  8  8  .   8   8   8   8
2
--- II    .  9  .  9  .  .  .  .  9  9   9   9   .   9
---
    III   4  .  .  4  .  .  4  4  4  4   .   4   .   4

    IV    .  .  .  1  .  .  .  1  1  1   .   1   .   1
1
---  V    .  .  6  .  .  .  6  6  6  .   .   6   6   6

     VI   2  2  .  .  .  2  .  .  .  2   .   2   2   .

Total     6  17 6  20 0  2 10 19 25 16  15  27  16  25
Key

         15  16  17  18  19  20  21  22  23  24  25  26
         ---------------------------------------------
--- I     .   .   8   .   8   .   .   8   8   8   .   8]
2
--- II    9   9   9   .   .   9   .   9   .   9   .]  .
---
    III   .   4   4   .   4   .   4   4   .]  4   .   .

    IV    .   1   .   1   1   1   .]  .   .   .   1   .
1
---  V    6   .   6   .   6   .   .   6   .   .   .   6

     VI   .   2   2]  2   2   .   .   .   2   .   .   .

Total    14  16  26   3   21 10   4  24  10  19   1  14
Key

         27  28  29  30
         -------------
--- I     .   8   .   8
2
--- II   9    .   9   .
---
    III  4    .   .   4

    IV   .    .   1   1
1
---  V   6    6   .   .

     VI  2    .   2   2

Total    20  14  12  15
Key
```

If the first word of a message was ADVANCE, it would be enciphered as EMJSLYE with the keys 6 17 6 20 0 2 10. Note in the diagram above, that the key of 26 in column 17 is equivalent to 0, and the key of 27 in column 12 is equivalent to 1. Also note that there are several ways to obtain certain keys, such as a key of 10 in columns 7, 20, and 23. There are 64 possible combinations of six things, and since there are only 26 different displacements possible of the primary components, there is of necessity a considerable duplication of key elements. With this particular lug arrangement, there are 7 key values (2,3,4,5,23,24,25) that can occur in only one way, since 26 = 0 and 27 =1, 6 key values that can occur in four ways, and 1 key value 15 that can occur in five ways. With some lug arrangements, certain key values may be impossible to produce.

MESSAGE ENCIPHERMENT

The following are detailed steps performed in the encipherment of a message with the CSP 1500:

(1) First, the pins and lugs are set up according to the key for the particular date. A slide is selected and is set on the machine. An initial message rotor alignment is chosen and recorded for future use. The slide and the initial alignment will be incorporated as indicator groups which are usually included with the final cryptogram. These indicator groups are usually not sent in the clear. The letter counter is reset to a multiple of 5 and recorded; the knob is set to "C" for cipher position.

(2) The first letter of the message plain text is now set on the indicating disk against a bench mark and the drive knob is given a clockwise turn. This causes the drum to make a complete revolution, imparting a kick to the print-wheel assembly equal to the number of bars which have been displaced by the action of the pins against the key-wheel levers, and the enciphered letter is printed on the tape at the end of the operating cycle. The six key wheels have moved one step each during the process, and new pins have come into contact with the key-levers to set up the key for the encipherment of the next letter.

(3) The succeeding plaintext letters are treated in the same fashion; at the end of every word a fixed letter (usually Z or K) may be enciphered as a word separator. After the encipherment of every 5th letter the machine causes the tape to advance another space, so that the final cryptogram is in 5 letter groups ready for transmission.

(4) In decipherment, the pins and lugs of the machine are set up according to the key, and the slide and the message rotor alignment for the particular message are established from the indicators. The encipher-decipher knob is set to the "D" position, and the first letter of the cipher message is set on the indicating disk against the benchmark; when the drive knob is operated, the decipherment is printed on the tape. The "D" position also suppress the Z plain word separator.

The Hagelin C-38 was used during World War II by the United States armed forces as a low-echelon cipher machine, under the nomenclature of M-209 in the Army and CSP 1500 in the Navy; the U.S. machines, however, where not generally equipped with a settable slide: the reversed standard alphabets were set at A=Z. [FR8]

CRYPTANALYSIS OF THE CSP 1500

Colonel Barkers' cryptanalysis of the Hagelin Cryptograph represents a clear way to illustrate the process. [BARK] Message encipherment and decipherment on the CSP 1500 are performed mechanically. We must consider the equivalent "on paper" processes of the cryptographic machine.

The first basic rule is given any two elements of the following: ciphertext, plaintext, key; the third element may be found. Thus, during encipherment, plaintext enciphered with key results in ciphertext. The reverse process is true during decipherment. However, important from the viewpoint of the cryptanalyst, given ciphertext with the plaintext known, the key may be recovered.

The CSP 1500 is based on the Beaufort Tableau shown in Table 21-1. The Beaufort Tableau provides the relationship between the ciphertext, plaintext and key. Note that the numerical key is runs from 0-27; and that 1 and 27 are equivalent, as are the numbers 0 and 26.

Table 21-1
C-38 Hagelin Cipher Machine (CSP1500)
Beaufort Tableau

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0/26	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A
1/27	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B
2	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C
3	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D
4	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E
5	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F
6	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G
7	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H
8	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I
9	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J
10	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K
11	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L
12	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M
13	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N
14	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O
15	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P
16	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q
17	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R
18	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S
19	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T
20	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U
21	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V
22	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W
23	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X
24	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y
25	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z

Note the beautiful diagonal letter symmetries. (You can see what this course is doing to me. Instead of thinking about say Michelangelo' paintings or a desert sunset, I am defining beauty as a diagonal letter group.)

Barker's analysis is cumulative. He starts with the mythical 'one wheel effective' CSP 1500 and builds up to the six wheel CSP 1500.

WORD SPACING WITH THE LETTER Z

In order to obtain spacing between words - making the plaintext more easily readable - the CSP 1500 is designed so that the plaintext letter Z prints as a space. For example the following plaintext:

HELPZNEEDEDZONZHILLZSSIXZONEZZEROZZERO

is read from the tape:

HELP NEEDED ON HILL SIX ONE ERO ERO

The letter Z actually does occur in the message text, and appears as a space as designed, so it must read into the text. Some Hagelin machines used a K instead of the Z.

Because the Z is hardwired in the CSP 1500 to produce a space, the enciphered plaintext is particularly "unusual" or "rough" statistically. So non-normal in fact is Hagelin plaintext that the mathematical approach in the general solution can easily be described as extremely effective. The statistical tests used in matching distributions, such as the Chi test, are decidedly more accurate than if the text were simply normal English text without the letter "Z" between words.

Based on a distribution of 50,000 letters of English military text in some 9,619 words with the letter "Z" being used as a space between words, the average frequencies per 1000 letters are the following [BARK]:

A	62	J	1	S	51
B	8	K	2	T	77
C	26	L	31	U	22
D	35	M	21	V	13
E	109 **	N	67	W	13
F	24	O	63	X	4
G	14	P	22	Y	16
H	28	Q	3	Z	162 **
I	62	R	64		

By examining these expected frequencies of letters in Hagelin plaintext, it will be seen that the two letters E and Z comprise over 25% of the text! The six letters, E, N, O, R, T, and Z, comprise over 50% of the text. The normal text is obviously skewed. Thus with the abnormal high-frequency of the letter Z especially, one can understand that the statistical tests used in analyzing the CSP 1500 traffic, such as the Chi test, for example, are very successful in matching distributions even when the amount of available text was limited.

Let's give ourselves some quick Table 21-1 experience.

1) Given the keying sequence " 5 26 12 19 0 27 6 5 0 21 8 4 0 5 13" and ciphertext, we read the plain: "Return to base."

```
5 26 12 19 0  27 6 5 0 21   8 4 0 5 13
N V  S  Y  I   N G L L V    G D H A N
R E  T  U  R   N Z T O Z    B A S E Z
```

2) Given the key "0 6 6 0 0 0 6 0 6 0 0 6 6 0 6 0 6 6 0 6", we decipher the following ciphertext to read:
 "Furnish information."

```
0 6 6 0 0   0 6 0 6 0   0 6 6 0 6   0 6 6 0 6
U L O M R   H Y A X M   U R O N F   G X R M G
F U R N I   S H Z I N   F O R M A   T I O N Z
```

3) Given the plaintext "SEND MORE SUPPLIES," we recover the key used to encipher the following message:

```
  S E N D Z   M O R E Z   S U P P L   I E S Z Z
  H D M W I   N T I D I   H N K S O   Z D P A I
  0 8 0 0 8   0 8 0 8 8   0 8 0 8 0   8 8 8 0 8
```

ANALYSIS OF A SINGLE-WHEEL CSP 1500 CIPHER MACHINE

The cryptographic security basically inherent in the Hagelin family of machines is provided principally by the manner in which key is generated.

Recognize that the single wheel Hagelin is a "mythical" machine, as are the two, three and even four wheel varieties. In each case the remaining wheels would have to be in a non-effective position.

We know that each wheel has a given length with given number of pin positions. As letters are enciphered (or deciphered), the wheels simultaneously revolve step-by-step, one position to the next. A 17 position, or pins, wheel, after encipherment of 17 letters will have returned to its original position.

The two mechanical variables set prior to encipherment (or decipherment) by the cryptographic clerk in the CSP 1500 are lug-settings and pin-settings. Both of these affect key generation.

First, the number of lugs may be made effective for each wheel. The number of lugs on a wheel may be 1,2,3,..12,..etc. If no lugs are set to effective position, than the wheel is in non-effective condition. Again, the number of lugs in the path of a particular wheel is known as the kick of that wheel; the total kick or key is the sum of all the kicks contributed at a given position of the six key wheels, as governed by those key-wheel levers which are in a position to contact the lugs on the drum.

Second, each position of the wheel may be made effective or non-effective by pushing a pin to the right or the left. If a pin is pushed to the left, it is non-effective; if a pin is pushed to the right, the position is effective (contributes to the key).

Third, when a position on the wheel is effective, when its "pin" is to the right, the key generated by the wheel will be equal to its kick or equal to the number of "lugs" set on the wheel. When a position on the wheel is non-effective, the key will be 0. For example, the key generated from a wheel of 17 positions might look as follows:

0 8 8 8 0 0 8 0 8 0 8 0 0 8 8 0 8] 0 8 8 8 0 0 8 0 8 ...

It can be seen that in this generated keying sequence the number of lugs set on the wheel is eight; the first position is in non-effective (left) position; in the next three position's, the pins are effective (right). The bracket shows that after 17 numbers of the key, the keying sequence, repeats.

For a single wheel case, the generated keying sequence always consists of a combination of but two numbers, one being 0, representing a "pin" in a non-effective position.

Consider the following cryptogram enciphered with a single-wheel:

```
Y V X L M   G A L U V   C G X A N   P F V Q R

W A C V N   L H H P I   B A W B A   X G B K A

W Y Z C H   D R W G H   C T A P G   A M H J S

W A Q A A.
```

Rather than the trial-and-error approach, lets take advantage of the 'Z' word-spacer at the final group of the message. Assume that the letter 'Z' was used as a null to complete the last five-letter group of the message. Examining the last group:

```
        cipher:  W  A  Q  A  A
 assumed plain :  Z  Z  Z  Z  Z
 resulting key : 22  0  16 0  0
```

We can disregard the W, for it most likely is the last letter of the message; but the last four letters appear to represent Z's. The generated key probably consists of the numbers 0 and 16.

Testing our theory on the cryptogram for the first 20 letters the possibilities are:

```
ciphertext  : Y V X L M G A L U V C G X A N P F V Q R
if key = 0  : B E C O N T Z O F E X T C Z M K U E J I
if key = 16 : R U S E D W P E V U N K S P C A K U Z Y
```

We use the letter Z to show the probable spaces between words.

```
        B E C O N T Z O F E X T C Z M K U E J I
        R U S E D W P E V U N K S P C A K U Z Y
```

yields

```
B E C O N T   O F E X T C   M K U E   I
R U S E D W   E V U N K S   C A K U   Y
```

The plaintext is evident:

```
B E C O N T   O F E X T C   M K U E   I
R U S E D W   E V U N K S   C A K U   Y
```

or

```
RECENT EVENTS MAKE I(T)...
```

ANALYSIS OF A TWO-WHEEL CSP 1500 CIPHER MACHINE

The two-wheel CSP 1500 is highly unlikely, but can be duplicated by making all the remaining wheels non-effective by either (1) putting all the pins of the remaining wheels to the left or (2) by failing to put any lugs on the remaining wheels.

Lets consider two keying sequences produced by a 17 letter wheel and a 19 letter wheel respectively.

```
Key 1 '17'  = 2 0 2 0 2 2 0 2 0 2 0 2 2 0 2 2 0]2 0
Key 2 '19'  = 0 3 0 3 3 0 0 3 0 3 3 3 0 0 3 0 3 0 3
Resultant Key 2 3 2 3 5 2 0 5 0 5 3 5 2 0 5 2 3 2 3]

              2 0 2 0 2 2 0 2 0 2 0 2 2 0 2]2 0 2 0
              0 3 0 3 3 0 0 3 0 3 3 3 0 0 3 0 3 0 3]
              2 3 2 3 5 2 0 5 0 5 3 5 2 0 5 2 3 2 3
```

Note that the resultant key consists of four different numbers, 0,2,3,and 5, the latter is the sum of 2 and 3. The brackets show the length of one revolution of the wheels.

We say the generated key consists of four numbers, 0, x, y, and z, where x = y = z.

The resulting key sequence will not repeat until the lowest common multiple of the lengths of the two wheels is reached, in this case 323 letters. the lowest common multiple of 17 and 19.

Let us turn to the analysis of a cryptogram produced from keying sequence generated from two wheels in the above fashion.

Given:

Begins "TO"

```
Q P G D V   W V I J O   K H T B K   S G L X M
A N V F W   W Z C A E   L P O A T   B O U F W
K M H V A   R X L N R   W Z E A G
```

>From the first word we have the first three keying letters:

```
          plain :  T  O  Z
          cipher:  Q  P  G
   recovered key : 10  4  6
```

The recovered key , 10, 6, 4 follows the property 4+6=10. Indeed, with the known 0 in the keying sequence, we may know all the numbers which comprise the resultant, generated key: 0, 4, 6, and 10. We set up the four possible plaintext equivalents for each ciphertext letter in the following form:

```
     Q P G D V W V I J O K H T B K S G L X M A N V F
     -----------------------------------------------
0:   J K T W E D E R Q L P S G Y P H T O C N Z M E U
4:   N O X A I H I V U P T W K C T L X S G R D Q I Y
6:   P Q Z C K J K X W R V Y M E V N Z U I T F S K A
10:  T U D G O N O B A V Z C Q I Z R D Y M X J W O E

     W W Z C A E L P O A T B O U F W K M H V A R X L
     -----------------------------------------------
0:   D D A X Z V O K L Z G Y L F U D P N S E Z I C O
4:   H H E B D Z S O P D K C P J Y H T R W I D M G S
6:   J J G D F B U Q R F M E R L A J V T Y K F O I U
10:  N N K H J F Y U V J Q I V P E N Z X C O J S M Y

     N R W Z E A G
     -------------
0:   M I D A V Z T
4:   Q M H E Z D X
6:   S O J G B F Z
10:  W S N K F J D
```

We again use the spacer letter 'Z' between words to identify word lengths. We note that three Z's fall in the last three columns, strong confirmation that the four numbers of the keying sequence selected are correct.

The plaintext becomes evident:

TO GENERAL SMITH SIX WOUNDED FOUR KILLED TWO MISSING

The complete recovery process is diagramed: Ciphertext -> Plaintext -> Key -> Pin Settings -> Length of Wheels.

With the plaintext now known, the keying sequence can be recovered:

```
Cipher:  Q P G D  V  W V I  J O  K H T  B K S G L X  M
Plain:   T O Z G  E  N E R  A L  Z S M  I T H Z S I  X
Key:    10 4 6 10 0 10 0 0 10 0 10 0 6 10 4 0 6 4 6 10

Cipher:  A  N  V F  W W Z C A  E L  P O A T  B O U  F
Plain:   Z  W  O U  N D E D Z  F O  U R Z K  I L L  E
Key:     0 10 10 0 10 0 4 6 0 10 0 10 6 0 4 10 0 6 10

Cipher:  W  K  M H  V A R X L N R  W Z E A G
Plain:   D  Z  T W  O Z M I S S I  N G Z Z Z
Key:     0 10  6 4 10 0 4 6 4 6 0 10 6 4 0 6
```

With the keying sequence now recovered, the final step is to determine the "pin settings" of the two CSP 1500 wheels; and at the same time to determine the lengths of the two wheels involved.

With the four numbers 0,4,6, and 10, we know:

(1) that a 0 results when both wheels are in a non-effective position.

(2) that when a 4 results, the position of the wheel containing four lugs is active, and the other with six lugs is non-effective.

(3) that when a 6 results, the position of the wheel containing six lugs is active, and the other with four lugs is non-effective.

(4) that when a 10 results, the positions, or pins of both wheels are effective.

```
Key:     10 4 6 10 0 10 0 0 10 0 10 0 6 10 4 0 6 4 6 10
Wheel 1:  6 0 6  6 0  6 0 0  6 0  6 0 6  6 0 0 6 0 6  6
Wheel 2:  4 4 0  4 0  4 0 0  4 0  4 0 0  4 4 0 0 4 0  4

Key:      0 10 10 0 10 0 4 6 0 10 0 10 6 0 4 10 0 6 10
Wheel 1:  0  6  6 0  6 0 0 6 0  6 0  6 6 0 0  6 0 6  6
Wheel 2:  0  4  4 0  4 0 4 0 0  4 0  4 0 0 4  4 0 0  4

Key:      0 10 6 4 10 0 4 6 4 6 0 10 6 4 0 6
Wheel 1:  0  6 6 0  6 0 0 6 0 6 0  6 6 0 0 6
Wheel 2:  0  4 0 4  4 0 4 0 4 0 0  4 0 4 0 0
```

Examination of the pin settings determined for the two wheels reveals that Wheel #1 is repeating every 19 letters and Wheel #2 is repeating every 21 letters. Thus, the two wheels and their individual keying sequences are as follows:

```
Wheel 1: 6 0 6 6 0 6 0 0 6 0 6 0 6 6 0 0 6 0 6
Wheel 2: 4 4 0 4 0 4 0 0 4 0 4 0 0 4 4 0 0 4 0 4 0
```

OVERLAP

The CSP 1500 has an additional security element known as overlap. An overlap of lug setting exists between two wheels, when both wheels are effective, the effective sum of the lugs (kick) from each wheel is reduced by the amount of the overlap. For the above example, Wheel #1 with six lugs and Wheel #2 with four lugs , if there was an overlap of one lug, with both wheels effective the sum of the lugs between the two wheels is 9 not 10. So our equation becomes z <= x + y.

ANALYSIS OF A THREE-WHEEL CSP 1500 CIPHER MACHINE

Given the cryptogram below and the known beginning MESSAGE followed by a number, with known wheels of 17, 19, and 21:

```
  U B I M G   Z V M H Z   H O A H M   L A T H Z
  T V B I H   H A R Q A   I M R S Z   P M S C F
  L H H B Z   N N B Q B   G T S Q V   T B H G H
```

We start with the word MESSAGE, and Z's at end of cryptogram.

```
      plain  :  m e s s a g e Z      - z z z z
      cipher :  U B I M G Z V M      T B H G H
      key    :  7 6 1 5 7 6 0 12     - 1 7 6 7
```

We also know that the number of the message is 16, so:

```
plain  :  s i x t e  e n z
cipher :  H Z H O A  H M L
key    :  0 8 5 8 5 12 0 11
```

We have identified eight numbers comprising the keying sequence: 0 1 5 6 7 8 11 12. We can deduce that one wheel has numbers 0 1, another 0 5 and the third wheel 0 7. It appears that there is an overlap of one lug between the wheel with five lugs and the wheel with seven lugs; thus 5 + 7= 11 and 1 + 5 + 7 = 12 fitting perfectly the actual key. We show the overlap as:

```
    |-1-|
1   5   7
```

To complete the solution we must still:

(1) Determine to which wheel the known lug settings apply.

(2) Determine the pin-settings of the three wheels.

(3) Read the text.

We "lay out" the message showing the overlaps and wheels:

```
Plain   : m e s s a g e z  s i  x t e e  n z
Cipher  : U B I M G Z V M  H Z  H O A H  M L  A T
Key     : 7 6 1 5 7 6 0 12 0 8  5 8 5 12 0 11
          ---------------------------------------
Wheel 17:                                      ]
Wheel 19:
Wheel 21:
          ---------------------------------------
          1 2 3 4 5 6 7 8  9 10 . . . . 15 .  . 18


          H Z T V B I H H A R Q A I M R S Z P M S C F L

          --------------------------------------------
Wheel 17:                                ]
Wheel 19:  ]                                     ]
Wheel 21:      ]
          ---------------------------------------------
          . 20. . . . 25. . . . 30. . . . . 35. . . 40 .


                                          Z Z Z
          H H B Z N N B Q B G T S Q V T B H G H
                                          7 6 7
          ------------------------------------
Wheel 17:                    ]
Wheel 19:
Wheel 21:  ]                             ]
          ------------------------------------
          . . .45 . . . .50 . . . . 55 . . . . 60
```

The brackets show the repeats for the wheels. Now, we see that pins 1-3 and 58-60 have been enciphered with the same pins of wheel 19. Letters in positions 1,18,35, and 52 have been enciphered with the key generated with the same pin of wheel length 17.

Position 3, with the key of 1, position 60 with its key of 7 provide evidence that wheel length 19 must have five lugs because:

(1) Positions 3 and 60 of Wheel length 19 are enciphered with the same pin; there is a multiple of 19 positions between them.

(2) The pin of Wheel length 19 in both positions 3 and 60 must be non-effective, since an effective pin could not contribute to both a 1 and a 7 generated key; so keys of 1 and 7 can only arise from two different single effective wheels, in one case a single wheel with one lug and in the other case a different single wheel with seven lugs.

(3) Since wheel length 19 is non-effective in position 3, then either wheel length 17 or 21 but not in both, must be effective with one lug in order to give rise to a key of 1 in that position.

(4) Same thing is true at position 60, either wheel length 17 or wheel length 21 but not both must be effective with seven lugs to give rise to the key of seven in this position.

(5) Logically, with wheel lengths of one and seven divided between wheel 17 and 21, wheel length 19 must contain five lugs.

This type of reasoning works to find the number of lugs on wheels 17 and 21:

(1) Positions 7 and 58 are enciphered with the same pin of wheel length 17.

(2) That pin must be ineffective because the total generated key in position 7 is 0.

(3) Since the pin in 58 is ineffective, and wheel length 19 has 5 lugs, the key for 7 in position 58 can only come from wheel length 21 being effective with 7 lugs.

(4) Since wheel length 19 having five lugs and the wheel length 21 has seven lugs, wheel length 17 must contain one lug.

We now know the number of lugs on each wheel known, the effectiveness of the pins recovered generated key can be determined as follows:

```
Plain   : m e s s a g e z  s i  x t e e  n z
Cipher  : U B I M G Z V M  H Z  H O A H  M L  A T
Key     : 7 6 1 5 7 6 0 12 0 8  5 8 5 12 0 11
          ----------------------------------------
Wheel 17: 0 1 1 0 0 1 0 1  0 1  0 1 0 1  0 0   ]
Wheel 19: 0 5 0 5 0 5 0 5  0 0  5 0 5 5  0 5
Wheel 21: 7 0 0 0 7 0 0 7  0 7  0 7 0 7  0 7
          ----------------------------------------
          1 2 3 4 5 6 7 8  9 10 . . . . 15 .  . 18


          H Z T V B I H H A R Q A I M R S Z P M S C F L

          ---------------------------------------------
Wheel 17:                      ]
Wheel 19:  ]                                     ]
Wheel 21:      ]
          ---------------------------------------------
          . 20. . . . 25. . . . 30. . . . . 35. . . 40.
```

```
                                          Z Z Z
          H H B Z N N B Q B G T S Q V T B H G H
                                          7 6 7
          --------------------------------------
Wheel 17:                    ]            0 1 0
Wheel 19:                                ]0 5 0
Wheel 21:  ]                              7 0 7
          --------------------------------------
          . . .45 . . . .50 . . . . 55 . . . .60
```

The logic holds that generated keys can only arise if a certain wheel or wheels are effective and other wheels are non-effective. Remember there is an overlap effect between wheels lengths 19 and 21. If both wheels are effective, their joint effectiveness is 5 + 7 -1 =11. When all three wheels are effective, the resulting keys is 1 + 5 + 7 - 1 = 12.

With the effectiveness of the pins determined, we mark the message:

```
Plain   : m e s s a g e z  s i  x t e e  n z (a)(r)
Cipher  : U B I M G Z V M  H Z  H O A H  M L  A T
Key     : 7 6 1 5 7 6 0 12 0 8  5 8 5 12 0 11
          ----------------------------------------
Wheel 17: 0 1 1 0 0 1 0 1  0 1  0 1 0 1  0 0   ]0
Wheel 19: 0 5 0 5 0 5 0 5  0 0  5 0 5 5  0 5
Wheel 21: 7 0 0 0 7 0 0 7  0 7  0 7 0 7  0 7
          ----------------------------------------
          1 2 3 4 5 6 7 8  9 10 . . . . 15 .  . 18
```

```
       (t)(i)(L)L E R Y Z F I R E Z S T I L L Z ? E A S
          H Z T V B I H H A R Q A I M R S Z P M S C F L

          ---------------------------------------------
Wheel 17: 1 1 0 0 1 0 1 0 1 0 1 0 1 0 0 -]0 1 1 0 0 1 0
Wheel 19:  ]0 5 0 5 0 5 0 5 0 0 5 0 5 5 0 5 ? ? ?]0 5 0
Wheel 21:      ]7 0 0 0 7 0 0 7 0 7 0 7 0 7 0 7 ? 7 0 7
          ---------------------------------------------
          . 20. . . . 25. . . . 30. . . . . 35. . . 40.
```

```
          E Z E A S T Z O F Z R I V E R   Z Z Z
          H H B Z N N B Q B G T S Q V T B H G H
                                          7 6 7
          --------------------------------------
Wheel 17: 1 0 1 0 1 0 1 0 0 1]0 1 1 0 0 1 0 1 0
Wheel 19: 5 0 5 0 5 0 0 5 0 5 5 0 5 0 5 -]0 5 0
Wheel 21: -]7 0 0 0 7 0 0 7 0 7 0 7 0 7 0 7 0 7
          --------------------------------------
          . . .45 . . . .50 . . . . 55 . . . .60
```

At this point, identified pins fill most of the spaces in the subject message. The student needs to confirm the above and fill in the rest.

ANALYSIS OF A FOUR-WHEEL CSP 1500 CIPHER MACHINE

We now turn our attention to the use of frequency considerations rather that the probable word method or use of a stereotyped beginning. I will bypass the standard five letter groupings and write the sample cryptogram in a period of 17 columns. Each column represents those letters enciphered with the same pin setting of wheel length 17. We assume that the 770 letter cryptogram is 128 words long with word sizes about 6 letters long. The pin of wheel length 17 is either effective or non-effective. Thus the 17 columns in effect represent two classes of columns, those columns with effective pins on wheel length 17 and those columns with non-effective pins on wheel length 17 [Hereafter designated group a and group b.]

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17

N G A P Y Z A T P X  H  C  I  R  F  S  P
B K M F J R M H J O  F  C  N  J  E  V  V
O Q D M W E T Q P V  Q  T  B  Q  I  M  L
G O M J H D A U G V  I  A  X  V  N  H  K
W H O B E S V B I Q  I  E  N  I  X  A  T
C H H R D R L G V M  X  X  J  N  M  G  U
A B D V I H B R D M  B  N  D  R  M  F  A
W X V I Z V O C F I  M  L  X  S  Q  O  P
Q U X D K W V W I R  R  R  A  C  L  O  W
A R P X B A T Y B D  T  Z  J  F  A  T  R
X V D Z K I M O N N  X  Y  P  U  R  Z  W
G L R C S B R M L W  I  T  J  F  R  O  K
A X D K Q A S D H X  U  T  W  B  W  J  N
Q A Y A F B H Q P D  P  S  F  G  S  H  Q
H A O I D N J F G Z  D  T  Y  U  D  A  J
F A R L Z P W L H N  I  Q  I  H  I  O  Q
J N F C M G Q L D J  C  E  O  O  P  Y  Q
R U P R L V V Q K Y  D  H  J  N  S  E  Q
F Y X D L E V K J M  Q  O  E  B  C  O  J
G M I T Y I P H P N  O  F  C  P  N  V  I
A K U J R H X U M M  O  P  B  G  N  Y  Z
X A P M X V F W G I  C  G  N  J  I  V  X
A M E M Q W Y F B R  H  D  A  V  E  J  E
R V S Y V A L W X S  J  L  P  R  W  A  A
O L L L H P Y L V Y  I  L  U  K  O  B  Z
M K U Y D H H J I D  D  Z  T  A  Z  T  G
K Q H A R H L Q F Y  E  Y  V  T  M  H  P
I Y W O J Q U M D S  X  L  S  B  W  K  N
K I U L W K J Y H S  N  M  N  H  I  C  J
N L M F D F J U R D  Q  S  P  Z  Y  J  E
U N W L U G S M I D  X  Y  D  Y  J  L  I
P V X I T S K B V D  C  D  N  M  Y  B  C
P U N X R Z Q V Z B  K  Y  L  A  J  C  X
R A B X V X F V D M  J  U  Y  U  U  A  O
U E Q O U A G J R T  Q  D  S  D  E  D  A
M K N P V L B V D P  M  Y  H  T  A  Q  H
B Z V Y N B M V K B  Y  N  M  J  L  R  I
T W Y E M R C A Q A  I  R  O  J  T  M  B
P D I V J Q U A G L  S  V  V  L  U  O  J
M W R L M W J D U U  K  I  N  O  A  M  C
H P T N S E L L J E  O  L  F  K  I  O  B
I G K R T R B J U S  H  U  F  A  Y  B  B
A S D V J B V Y Q D  Q  E  C  J  C  A  F
E K T Z M A H E I D  D  S  H  P  C  X  B
G V H L M L D E G T  M  E  Z  L  I  B  N
V P D N D.
```

MONOALPHABETS

We see the pattern of monoalphabetic substitutions which combine as we increase the number of wheels:

Number of Wheels	Number of Monoalphabetic Substitutions which Combine
1	2
2	4
3	8
4	16
5	32
6	64

Of the 16 alphabets that are available with four wheels, we have two distinct types:

(1) Letters within columns where the pins of wheel length 17 are non effective are enciphered as the result of the other three wheels generating 8 Beaufort cipher alphabets. For these letters wheel length 17 doesn't exist.

(2) Letters within columns where the pins of wheel length 17 are effective are enciphered as the result of the other three wheels generating 8 Beaufort cipher alphabets plus a constant effectiveness of wheel length 17.

Remembering our statistics Lecture 15, by matching frequency distributions of each of the 17 columns we attempt to divide the columns into their two classes. Success depends on a sufficient number of letters within the column to provide the differentiation required between polyalphabeticity within one class of eight alphabets and a different eight alphabets of another. The frequency distributions of each column are straight forward and are left for my students, if required.

Our key test is the Chi test, or cross product sum test defined by Solomon Kullback. [KULL] As a refresher, I will use the first two distributions:

	A	B	C	D	E	F	G	H	I	J	K	L	M
Frequency Distribution #1	6	2	1		1	2	4	2	2	4	2		3
Frequency Distribution #1	5	1		1	1		2	2	1		5	3	2
	30	2			1		8	4	2		10		6

	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	2	2	3	2	3		1	2	1	2	2		
	2	1	2	2	1	1		3	4	3	2	1	1
	4	2	6	4	3			6	4	6	4		

```
Chi test (#1 and #2) = Sum of cross-products
                       ---------------------
                          N1 x N2

                     =  102 / 2116 = 0.048
```

```
where:
N1 x N2 = 46 x 46 = 2116
Sum of cross-products =
30+2+1+8+4+2+10+6+4+2+6+4+3+6+4+6+4 = 102
```

Likewise, we can make Chi tests on each pair of frequency distributions -- the partial results are as follows:

```
#1 + #2 = 0. 048    #1 + #3 = 0.037    #1 + #4 = 0.034
#1 + #5 = 0. 030    #1 + #6 = 0.048    #1 + #7 = 0.036
#1 + #8 = 0. 036    #1 + #9 = 0.042    #1 + #10= 0.030
#1 + #11= 0. 037    #1 + #12= 0.026    #1 + #13= 0.037
#1 + #14= 0. 043    #1 + #15= 0.039    #1 + #16= 0.045
#1 + #17= 0. 044
-------------------------------------------------------
#2 + #3 = 0. 039    #2 + #4 = 0.040    #2 + #5 = 0.037
#2 + #6 = 0. 048    #2 + #7 = 0.043    #2 + #8 = 0.044
#2 + #9 = 0. 039    #2 + #10= 0.034    #2 + #11= 0.031
#2 + #12= 0. 032    #2 + #13= 0.033    #2 + #14= 0.039
#2 + #15= 0. 035    #2 + #16= 0.039    #2 + #17= 0.040
```

and so forth for all the columns. [BARK]

The above 17(17-1) /2 = 136 Chi test results indicate the degree of likelihood that matched pairs of frequency distributions are from the same class of "eight-alphabet polyalphabeticity". The larger the value of the result, the more likely the pair of distributions come from the same class; the lower the result, the less likely it is that the pairs are of the same class.

[BARK] presents a tabulation of the results:

(1) the three lowest results are 0.026, 0.027, and 0.028.

(2) the three highest results are 0.054, 0.057, and 0.058.

(3) the average or median result is 0.039.

Based on these results, we can say that a result less than 0. 039 is more likely to be an incorrect match, and a result larger than 0.039 is likely to be a correct match. We will assume the validity of (1) and (2).

We start off with the following results:

```
  Correct Match          Incorrect Match
  -------------          ---------------
  #7 + #8 = 0.054        #1 + #12= 0.026
  #5 + #10= 0.057        #12+ #17= 0.027
  #3 + #10= 0.058        #10+ #17= 0.028
```

We conclude that:

(1) #7 and #8 are in the same class.
(2) #1 and #17 are in the same class.
(3) #3, #5, #10 and #12 are in the same class.
(4) #1 and #17 are not in the same class #3, #5, #10, and #12.

We label the first group as Class A and the second as Class B.

We compare frequency distributions across the board and find quickly the following separations:

Class A	Class B
1	3
2	4
6	5
7	10
8	11
14	12
16	15
17	

In some of the cases, it was necessary to compute an average Chi test for each class and compare the "closer" frequency distributions to it as well as the outlying statistics. We are able to divide 15 of 17 pins on wheel length 17 into two arbitrary classes A and B. One of the classes represents the effective pins and the other represents the non-effective pins. Using a lowercase 'a' and 'b' we return to the cryptogram and identify the individual letters. Here is the tabulation:

```
1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17

Na Ga Ab Pb Yb Za Aa Ta P  Xb Hb Cb I Ra Fb Sa Pa
Ba Ka Mb Fb Jb Ra Ma Ha J  Ob Fb Cb N Ja Eb Va Va
Oa Qa Db Mb Wb Ea Ta Qa P  Vb Qb Tb B Qa Ib Ma La
Ga Oa Mb Jb Hb Da Aa Ua G  Vb Ib Ab X Va Nb Ha Ka
Wa Ha Ob Bb Eb Sa Va Ba I  Qb Ib Eb N Ia Xb Aa Ta
Ca Ha Hb Rb Db Ra La Ga V  Mb Xb Xb J Na Mb Ga Ua
Aa Ba Db Vb Ib Ha Ba Ra D  Mb Bb Nb D Ra Mb Fa Aa
Wa Xa Vb Ib Zb Va Oa Ca F  Ib Mb Lb X Sa Qb Oa Pa
Qa Ua Xb Db Kb Wa Va Wa I  Rb Rb Rb A Ca Lb Oa Wa
Aa Ra Pb Xb Bb Aa Ta Ya B  Db Tb Zb J Fa Ab Ta Ra
Xa Va Db Zb Kb Ia Ma Oa N  Nb Xb Yb P Ua Rb Za Wa
Ga La Rb Cb Sb Ba Ra Ma L  Wb Ib Tb J Fa Rb Oa Ka
Aa Xa Db Kb Qb Aa Sa Da H  Xb Ub Tb W Ba Wb Ja Na
Qa Aa Yb Ab Fb Ba Ha Qa P  Db Pb Sb F Ga Sb Ha Qa
Ha Aa Ob Ib Db Na Ja Fa G  Zb Db Tb Y Ua Db Aa Ja
Fa Aa Rb Lb Zb Pa Wa La H  Nb Ib Qb I Ha Ib Oa Qa
Ja Na Fb Cb Mb Ga Qa La D  Jb Cb Eb O Oa Pb Ya Qa
Ra Ua Pb Rb Lb Va Va Qa K  Yb Db Hb J Na Sb Ea Qa
Fa Ya Xb Db Lb Ea Va Ka J  Mb Qb Ob E Ba Cb Oa Ja
Ga Ma Ib Tb Yb Ia Pa Ha P  Nb Ob Fb C Pa Nb Va Ia
Aa Ka Ub Jb Rb Ha Xa Ua M  Mb Ob Pb B Ga Nb Ya Za
Xa Aa Pb Mb Xb Va Fa Wa G  Ib Cb Gb N Ja Ib Va Xa
Aa Ma Eb Mb Qb Wa Ya Fa B  Rb Hb Db A Va Eb Ja Ea
Ra Va Sb Yb Vb Aa La Wa X  Sb Jb Lb P Ra Wb Aa Aa
Oa La Lb Lb Hb Pa Ya La V  Yb Ib Lb U Ka Ob Ba Za
Ma Ka Ub Yb Db Ha Ha Ja I  Db Db Zb T Aa Zb Ta Ga
Ka Qa Hb Ab Rb Ha La Qa F  Yb Eb Yb V Ta Mb Ha Pa
Ia Ya Wb Ob Jb Qa Ua Ma D  Sb Xb Lb S Ba Wb Ka Na
Ka Ia Ub Lb Wb Ka Ja Ya H  Sb Nb Mb N Ha Ib Ca Ja
Na La Mb Fb Db Fa Ja Ua R  Db Qb Sb P Za Yb Ja Ea
Ua Na Wb Lb Ub Ga Sa Ma I  Db Xb Yb D Ya Jb La Ia
Pa Va Xb Ib Tb Sa Ka Ba V  Db Cb Db N Ma Yb Ba Ca
Pa Ua Nb Xb Rb Za Qa Va Z  Bb Kb Yb L Aa Jb Ca Xa
Ra Aa Bb Xb Vb Xa Fa Va D  Mb Jb Ub Y Ua Ub Aa Oa
Ua Ea Qb Ob Ub Aa Ga Ja R  Tb Qb Db S Da Eb Da Aa
Ma Ka Nb Pb Vb La Ba Va D  Pb Mb Yb H Ta Ab Qa Ha
Ba Za Vb Yb Nb Ba Ma Va K  Bb Yb Nb M Ja Lb Ra Ia
Ta Wa Yb Eb Mb Ra Ca Aa Q  Ab Ib Rb O Ja Tb Ma Ba
Pa Da Ib Vb Jb Qa Ua Aa G  Lb Sb Vb V La Ub Oa Ja
Ma Wa Rb Lb Mb Wa Ja Da U  Ub Kb Ib N Oa Ab Ma Ca
Ha Pa Tb Nb Sb Ea La La J  Eb Ob Lb F Ka Ib Oa Ba
Ia Ga Kb Rb Tb Ra Ba Ja U  Sb Hb Ub F Aa Yb Ba Ba
Aa Sa Db Vb Jb Ba Va Ya Q  Db Qb Eb C Ja Cb Aa Fa
Ea Ka Tb Zb Mb Aa Ha Ea I  Db Db Sb H Pa Cb Xa Ba
Ga Va Hb Lb Mb La Da Ea G  Tb Mb Eb Z La Ib Ba Na
Va Pa Db Nb Db.
```

We now examine Wheel length 19. We keep the designations of class throughout our investigation and rewrite the cryptogram 'in depth' of wheel length 19.

```
1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19

Na Ga Ab Pb Yb Za Aa Ta P  Xb Hb Cb I  Ra Fb Sa Pa Ba Ka
Mb Fb Jb Ra Ma Ha J  Ob Fb Cb N  Ja Eb Va Va Oa Qa Db Mb
Wb Ea Ta Qa P  Vb Qb Tb B  Qa Ib Ma La Ga Oa Mb Jb Hb Da
Aa Ua G  Vb Ib Ab X  Va Nb Ha Ka Wa Ha Ob Bb Eb Sa Va Ba
I  Qb Ib Eb N  Ia Xb Aa Ta Ca Ha Hb Rb Db Ra La Ga V  Mb
Xb Xb J Na  Mb Ga Ua Aa Ba Db Vb Ib Ha Ba Ra D  Mb Bb Nb
D  Ra Mb Fa Aa Wa Xa Vb Ib Zb Va Oa Ca F  Ib Mb Lb X  Sa
Qb Oa Pa Qa Ua Xb Db Kb Wa Va Wa I  Rb Rb Rb A Ca Lb  Oa
Wa Aa Ra Pb Xb Bb Aa Ta Ya B  Db Tb Zb J  Fa Ab Ta Ra Xa
Va Db Zb Kb Ia Ma Oa N  Nb Xb Yb P  Ua Rb Za Wa Ga La Rb
Cb Sb Ba Ra Ma L  Wb Ib Tb J  Fa Rb Oa Ka Aa Xa Db Kb Qb
Aa Sa Da H  Xb Ub Tb W  Ba Wb Ja Na Qa Aa Yb Ab Fb Ba Ha
Qa P  Db Pb Sb F  Ga Sb Ha Qa Ha Aa Ob Ib Db Na Ja Fa G
Zb Db Tb Y  Ua Db Aa Ja Fa Aa Rb Lb Zb Pa Wa La H  Nb Ib
Qb I  Ha Ib Oa Qa Ja Na Fb Cb Mb Ga Qa La D  Jb Cb Eb O
Oa Pb Ya Qa Ra Ua Pb Rb Lb Va Va Qa K  Yb Db Hb J Na  Sb
Ea Qa Fa Ya Xb Db Lb Ea Va Ka J  Mb Qb Ob E  Ba Cb Oa Ja
Ga Ma Ib Tb Yb Ia Pa Ha P  Nb Ob Fb C Pa  Nb Va Ia Aa Ka
Ub Jb Rb Ha Xa Ua M  Mb Ob Pb B Ga Nb Ya  Za Xa Aa Pb Mb
Xb Va Fa Wa G  Ib Cb Gb N  Ja Ib Va Xa Aa Ma Eb Mb Qb Wa
Ya Fa B  Rb Hb Db A  Va Eb Ja Ea Ra Va Sb Yb Vb Aa La Wa
X  Sb Jb Lb P  Ra Wb Aa Aa Oa La Lb Lb Hb Pa Ya La V  Yb
Ib Lb U  Ka Ob Ba Za Ma Ka Ub Yb Db Ha Ha Ja I  Db Db Zb
T  Aa Zb Ta Ga Ka Qa Hb Ab Rb Ha La Qa F  Yb Eb Yb V  Ta
Mb Ha Pa Ia Ya Wb Ob Jb Qa Ua Ma D  Sb Xb Lb S Ba Wb  Ka
Na Ka Ia Ub Lb Wb Ka Ja Ya H  Sb Nb Mb N  Ha Ib Ca Ja Na
Na La Mb Fb Db Fa Ja Ua R  Db Qb Sb P  Za Yb Ja Ea Na Wb
Lb Ub Ga Sa Ma I  Db Xb Yb D  Ya Jb La Ia Pa Va Xb Ib Tb
Sa Ka Ba V  Db Cb Db N  Ma Yb Ba Ca Pa Ua Nb Xb Rb Za Qa
Va Z  Bb Kb Yb L  Aa Jb Ca Xa Ra Aa Bb Xb Vb Xa Fa Va D
Mb Jb Ub Y  Ua Ub Aa Oa Ua Ea Qb Ob Ub Aa Ga Ja R  Tb Qb
Db S  Da Eb Da Aa Ma Ka Nb Pb Vb La Ba Va D  Pb Mb Yb H
Ta Ab Qa Ha Ba Za Vb Yb Nb Ba Ma Va K  Bb Yb Nb M  Ja Lb
Ra Ia Ta Wa Yb Eb Mb Ra Ca Aa Q  Ab Ib Rb O  Ja Tb Ma Ba
Pa Da Ib Vb Jb Qa Ua Aa G  Lb Sb Vb V  La Ub Oa Ja Ma Wa
Rb Lb Mb Wa Ja Da U  Ub Kb Ib N  Oa Ab Ma Ca Ha Pa Tb Nb
Sb Ea La La J  Eb Ob Lb F  Ka Ib Oa Ba Ia Ga Kb Rb Tb Ra
Ba Ja U  Sb Hb Ub F  Aa Yb Ba Ba Aa Sa Db Vb Jb Ba Va Ya
Q  Db Qb Eb C  Ja Cb Aa Fa Ea Ka Tb Zb Mb Aa Ha Ea I  Db
Db Sb H  Pa Cb Xa Ba Ga Va Hb Lb Mb La Da Ea G  Tb Mb Eb
Z La Ib  Ba Na Va Pa Db Nb Db.
```

Each of the above 19 columns represent letters which are enciphered with the same pin-setting of Wheel length 19. 8 different alphabets are represented. We have identified two groups. In any column, all letters followed by an a have been enciphered with both the same pin setting of wheel length 19 causing these letters to result from only 4 alphabets. The same holds true of letters with the 'b' designation. Note that the polyalphabeticity comes from the remaining two wheels of lengths 21 and 23.

We repeat the process of making frequency distributions of the columns (in this case length 19), then using the Chi test we re-divide the 19 columns into two groups, a Class C and Class D. [BARK] describes a shortcut using the sum of the cross products and lesser tests. I do not agree with the procedure because it lacks the rigor of the full Chi test.

The results show that wheel 19 has at minimum 10 identified distributions:

Class C	Class D
1	3
2	4
5	9
6	
7	
8	
10	

LUGS

Consider the multiple alphabets generated by four wheels with respective lug-settings, for example, of 5, 4, 3, and 1:

Wheel	No of Lugs	Different keys Generated
1	5	0 5
2	4	0 5 + 4 9
3	3	0 5 4 9 + 3 8 7 12
4	1	0 5 4 9 3 8 7 12 + 1 6 5 10 4 8 13

The plus sign represents the additional keys generated by the additional wheel. Consider the Class A and B sets on the Wheel 17. One class of the two pairs of alphabets must have a 0 for the non-effectiveness pin. The second set of eight alphabets is the same as the first plus a number representing the number of lugs on the wheel.

We know that the ciphertext letters A and V represent Z and E and the class with the number 0 will have a higher frequency distribution. In our example, class A has a large number of A's and V's. We can superimpose the class B distribution over the A distribution to get the number of lugs because Class A + the number of lugs equals Class B. Our shift was three spaces to the right representing 3 lugs on wheel 17.

The same analysis and superimposition holds true for wheel 19. The four classes have the following keys:

```
A = 0 5 4 9 + 3 8 7 12
B = 1 6 5 10 + 4 9 8 13
C = 0 5 4 9 + 1 6 5 10
D = 3 8 7 12  + 4 9 8 13
```

An unknown ciphertext letter, if found to be in both Class A and Class C, its key will be one of the four, 0 5 4 9. Similarly, a ciphertext letter known to be in Class B and Class D will have keys of 4 9 8 13.

ANALYSIS OF A SIX-WHEEL CSP 1500 CIPHER MACHINE

Barkers analysis of the five-wheel CSP 1500 does not add to our knowledge but confirms that the computer is required for further resolution of the 32 alphabets presented. He also details the lug logic demonstrated in the previous case. [BARK]

We have at last arrived at the problem of solving a six-wheel Hagelin Cryptograph. Before we discuss the general solution, we will look at two common "assists" that occurred in the field in WWII. In Special Case 1, we will have the advantage of knowing the initial wheel-settings of the messages. In Special Case 2, we will take advantage of a 'stagger'. We first looked at the 'stagger' in Lecture 12.

Special Case 1 - Indicators are Unenciphered.

>From unenciphered indicators we shall derive exactly what portion of the keying sequence, running from 1 to 101405850, have been used to encipher given messages.

Given: 3 messages selected from a large traffic base, starting with the word Message, followed by a number and the word STOP.

We also know that the first two five-letter groups are the indicator groups where:

(1) The first six letters represent the unenciphered initial settings of the six Hagelin wheels used to encipher the message.

(2) The seventh through tenth letters indicate the number of letters in the message, where A=1, B=2, C=3, etc.; in message 1 the letters are J J I E, or 0 0 9 5, meaning the message 1 count is 95 letters.

```
No. 1

J Y B T M   H J J I E   A I W I Z   U Q I Y Q
E W A R N   S A U Y Q   D U L J M   V O H B L
H K R M I   L W G Z W   F C V F Q   F O T G K
F O Y G R   P M Z I Z   M J W Z T   W I B C L
F X X E S   M V S S A   H F X X P   B J D H R
A J B Q P.

No. 2

O E J I F   E J J G J   R M S U E   P T E G B
N R Q X Q   R P A Y U   G Y A F R   Y J E M M
M U A F M   X T I M Q   P W P H W   P K J X J
F L H F D   J R X P T   J E Z G S   R C G W K.

No. 3

W L O L G   D J J I E   E N R W T   K F S Q D
F W Q G X   D V Z L X   W X F N K   E H F V F
L U L C I   V Y P O M   X A F R J   Y R M V J
N F X E K   T K K O C   W B Y G N   J U H F E
H D B E W   M S O U W   W P C D G   S R D W L
A Z E A A.
```

The message indicators representing the initial wheel settings of the messages are:

No. 1 - J Y B T M H
No. 2 - O E J I F E
No. 3 - W L O L G D

The first letter of the indicator represents the wheel-setting of Wheel Length 26, the second letter represents the wheel-setting of wheel 25, etc.

The six wheel lengths of 26, 25, 23, 21, 19 and 17 represent 26 x 25 x 23 x 21 x 19 x 17 = 101,405,850 possible different starting points for the encipherment (decipherment) of messages. Each starting point is represented by different initial setting of the six wheels; and as the six wheels turn in progression, letters are enciphered (or deciphered) at progressive points along the generated key which is 101,405,850 positions in length.

First, we convert the above literal indicators into successive numerical indicators; that is, we want to convert the wheel-setting AAAAAA, for example into 1, the wheel setting BBBBBB into 2, CCCCCC into 3...ZZXUSQ into 101,405,850. We are looking for the successive numerical indicators along the total generated key for the messages enciphered.

The process (which is easily computerized) is:

(1) Replace the letters with there positional equivalents below -

Wheel Length					
26	25	23	21	19	17
--	--	--	--	--	--
A = 1	A = 1	A = 1	A = 1	A = 1	A = 1
B = 2	B = 2	B = 2	B = 2	B = 2	B = 2
C = 3	C = 3	C = 3	C = 3	C = 3	C = 3
D = 4	D = 4	D = 4	D = 4	D = 4	D = 4
E = 5	E = 5	E = 5	E = 5	E = 5	E = 5
F = 6	F = 6	F = 6	F = 6	F = 6	F = 6
G = 7	G = 7	G = 7	G = 7	G = 7	G = 7
H = 8	H = 8	H = 8	H = 8	H = 8	H = 8
I = 9	I = 9	I = 9	I = 9	I = 9	I = 9
J = 10	J = 10	J = 10	J = 10	J = 10	J = 10
K = 11	K = 11	K = 11	K = 11	K = 11	K = 11
L = 12	L = 12	L = 12	L = 12	L = 12	L = 12
M = 13	M = 13	M = 13	M = 13	M = 13	M = 13
N = 14	N = 14	N = 14	N = 14	N = 14	N = 14
O = 15	O = 15	O = 15	O = 15	O = 15	O = 15
P = 16	P = 16	P = 16	P = 16	P = 16	P = 16
Q = 17	Q = 17	Q = 17	Q = 17	Q = 17	Q = 17
R = 18	R = 18	R = 18	R = 18	R = 18	
S = 19	S = 19	S = 19	S = 19	S = 19	
T = 20	T = 20	T = 20	T = 20		
U = 21	U = 21	U = 21	U = 21		
V = 22	V = 22	V = 22			
W = 23	X = 23	X = 23			
X = 24	Y = 24				
Y = 25	Z = 25				
Z = 26					

The three indicators become:

```
No. 1  -  J Y B T M H  = 10 24 2 20 13 8
No. 2  -  O E J I F E  = 15 5 10 9 6 5
No. 3  -  W L O L G D  = 23 12 15 12 7 4
```

(2) We multiply each number obtained by a constant, for each position of the indicator and obtain the sum of the multiplications, as follows:

No. 1

```
10 x 89705175 =  897051750
24 x 56787276 = 1362894624
 2 x 92587950 =  185175900
20 x 82090450 = 1641809000
13 x 42697200 =  555063600
 8 x 41755350 =  334042800
                ----------
                4976037674
```

No. 2

```
15 x 89705175 = 1345577625
 5 x 56787276 =  283936380
10 x 92587950 =  925879500
 9 x 82090450 =  738814050
 6 x 42697200 =  256183200
 5 x 41755350 =  208776750
                ----------
                3759167505
```

No. 3

```
23 x 89705175 = 2063219025
12 x 56787276 =  681447312
15 x 92587950 = 1388819250
12 x 82090450 =  985085400
 7 x 42697200 =  298880400
 4 x 41755350 =  167021400
                ----------
                5584472787
```

The constants used for multiplication apply only to the Model Type CSP 1500. A machine with other wheels will have different constants. Determining these constants is an exercise in solving simultaneous congruences. Chapter V of "Recreations in the Theory of Numbers - The Queen of Mathematics Entertains" by Albert H. Beiler (Dover) 1977 presents a good elementary overview of the theory involved.

(3) The third step to obtain the desired successive numerical indicators is to divide the sums of the multiplications by 26 x25 x 23 x 21 x 19 x 17 = 101405850. The remainders of the divisions will be the successive numerical indicators.

```
No. 1

    4976037674
    ---------- = 49 +  7151024     No. 1 = 7151024
     101405850

No. 2

    3759167505
    ---------- = 37 +  7151055     No. 2 = 7151055
     101405850

No. 3

    5584472787
    ---------- = 55 +  7151037     No. 3 = 7151037
     101405850
```

Since the above successive indicators are so close together, we immediate suspect that we are fortunate enough to have what is termed as an overlap. An overlap exists when two messages have been enciphered with the same generated key. In this example we have three messages overlapping.

STRIPPING OFF THE GENERATED KEY

We prepare a worksheet with the messages "in depth", and knowing that the messages start with the word MESSAGE, we are able to "strip off" some of the generated key as follows:

```
Pos:  24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44
Key:  13 13 15 1* 0* 1* 21 8                 17 18 10 15 20 17 10 18
No.1: A  I  W  I  Z  U  Q  I  Y  Q  E  W  A  R  N  S  A  U  Y  Q  D
      m  e  s  s  a  g  e  z                 z  e  r  o  z  s  t  o


                                      No. 3: E  N  R  W  T  K  F  S
                                             m  e  s  s  a  g  e  z

-------------------------------------------------------------------
45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68
                              4  17 11 13 5  22 24 4
U  L  J  M  V  O  H  B  L  H  K  R  M  I  L  W  G  Z  W  F  C  V  F  Q
                              t  z  y  e  t  z  r  e

                     No. 2:   R  M  S  U  E  P  T  E  G  B  N  R  Q  X
                              m  e  s  s  a  g  e  z

Q  D  F  W  Q  G  X  D  V  Z  L  X  W  X  F  N  K  E  H  F  V  F  L  U
                              s  t  o  p  z  i  n  z
```

```
-----------------------------------------------------------------------
69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92

F  O  T  G  K  F  O  Y  G  R  P  M  Z  I  Z  M  J  W  Z  T  W  I  B  C


Q  R  P  A  Y  U  G  Y  A  F  R  Y  J  E  M  M  M  U  A  F  M  X  T  I


L  C  I  V  Y  P  O  M  X  A  F  R  J  Y  R  M  V  J  N  F  X  E  K  T
```

*In the generated key a 0 might also be a 26; and a 1 might be a 27.

```
----------------------------------------------------------------------
93 94 95 96 97 98 99 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16

L  F  X  X  E  S  M  V  S  S  A  H  F  X  X  P  B  J  D  H  R  A  J  B

M  Q  P  W  P  H  W  P  K  J  X  J  F  L  H  F  D  J  R  X  P  T  J  E

K  K  O  C  W  B  Y  G  N  J  U  H  F  E  H  D  B  E  W  M  S  O  U  W
-----------------------------------------------------------------------
17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

Q  P.


Z  G  S  R  C  G  W  K.


W  P  C  D  G  S  R  D  W  L  A  Z  E  A  A.
-----------------------------------------------------------------------
```

In is evident that the messages are correctly aligned "in depth" and portions of the generated key so far recovered or "stripped off" are correct. We can try probable words in one message and confirm the text in another message. Message No. 3 numbers will occur in positions 45 through 54; numbers also will follow the word Message in message No. 2.

PIN AND LUG SETTINGS

It is instructive to attempt a further solution by recovering the pin and lug settings as follows:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
13	13	15	1	0	1	21	8	-	-	-	-	0	17	18	10	15	20	17	10	18	10	11	23	1

26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
21	6	12	17	0	25	4	17	11	13	5	22	24	4	25	10	11	17	10	20	5	17	8	20	13

51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
10	6	12	15	5	22	12	14	17	11	12	13	14	20	6	15	8	19	7	17	10	15	15	9	22

76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
12	15	7	18	9	21	5	22	12	10	19	6	16	12	10	19	10	8	21	15	11	22	6	6	22

101	102	103	104	105	106	107	108
10	23	5	9	21	9	0	0

We look for the wheel with the most lugs. We start with wheel 17 and write it out in length 17.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
13	13	15	1	0	1	21	8	-	-	-	-	0	17	18	10	15
20	17	10	18	10	11	23	1	21	6	12	17	0	25	4	17	11
13	5	22	24	4	25	10	11	17	10	20	5	17	8	20	13	10
6	12	15	5	22	12	14	17	11	12	13	14	20	6	15	8	19
7	17	10	15	15	9	22	12	15	7	18	9	21	5	22	12	10
19	9	16	12	10	19	10	8	21	15	11	22	6	6	22	10	23
5	9	21	9	0	0											

Note column 14. If wheel 17 contains seven lugs, with a total of 25 in the column, the pin of wheel length 17 is effective, and there must be a total of 5 within the same column, so there cannot be more than 5 lugs on wheel 17. We can look at wheel 19.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
13	13	15	1	0	1	21	8	-	-	-	-	0	17	18	10	15	20	17
10	18	10	11	23	1	21	6	12	17	0	25	4	17	11	13	5	22	24
4	25	10	11	17	10	20	5	17	8	20	13	10	6	12	15	5	22	12
14	17	11	12	13	14	20	6	15	8	19	7	17	10	15	15	9	22	12
15	7	18	9	21	5	22	12	10	19	9	16	12	10	19	10	8	21	15
11	22	6	6	22	10	23	5	9	21	9	0	0						

Columns 2 and 3 suggest that wheel length 19 has 7 lugs + or - 2. Making this assumption, we can identify the effective (+) and non-effective pins (-) based on the assumption that < 7 is non-effective and > than 22 is certainly effective. The ambiguous columns are resolved. We have:

```
-  +  -  -  +  -  +  -           +  -  -        -  +  +
1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19
-------------------------------------------------------
13 13 15 1  26 1  21 8  -  -  -   -  0 17 18 10 15 20 17
10 18 10 11 23 1  21 6  12 17  0 25 4  17 11 13 5  22 24
4  25 10 11 17 10 20 5  17 8  20 13 10 6  12 15 5  22 12
14 17 11 12 13 14 20 6  15 8  19 7  17 10 15 15 9  22 12
15 7  18 9  21 5  22 12 10 19 9  16 12 10 19 10 8  21 15
11 22 6  6  22 10 23 5  9  21 9  26 0
```

In a similar fashion, we do the other 4 wheels. We find that wheel 17 contains no more than 5 lugs; wheel 19 contains 7 lugs - 14 of 19 pins are identified; wheel 21 contains 5 lugs; wheel 23 contains eight lugs with 17 pins identified; wheel 25 contains 1 lug; wheel 26 contain s up to 5 lugs.

The final efforts are derived from the same layout of the recovered key:

```
Key: 13 13 15 1  26 1  21 8 -  -  -  -  0  17 18 10 15 20 17
     -------------------------------------------------------
17:           0     0     0             0             ]
19:  0  7  0  0  7  0  7  0       0  7  0  0        0  7  7]
21:        0  0     0       0           0
23:  8  0     0  8  0  0  8 0   8 0     0  8  8  0  8     0
25:           1  0  1     0             0
26:           0     0                   0
    --------------------------------------------------------
     1  2  3  4  5  6  7  8 9 10 11 12  13 14 15 16 17 18 19
```

and so forth for the balance of the recovered key. Not the non-effective pins in position 8.

ENCIPHERED INDICATORS

Initial wheel settings are rarely encountered in the clear. We face several challenges when the initial wheel indicators are enciphered.

(1) Attempts to put the messages "in depth" or equate the messages by their indicators may be successful only if the enciphering method for the indicators is weak cryptographically.

(2) Recovery of a solved message does not mean that we can "read' all the additional traffic as easily as the correspondents.

(3) Table 21-2 shows the important relationship between the wheel settings as viewed on the face of the CSP 1500 and the "effective" pin positions internally within the machine that actually effect the operations of the machine:

Table 21 -2

Wheel 26

Letter Shown:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Internal Pin:	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O

Wheel 25

Letter Shown:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z
Internal Pin:	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	M	N

Wheel 23

Letter Shown:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X
Internal Pin:	N	O	P	Q	R	S	T	U	V	X	A	B	C	D	E	F	G	H	I	J	K	L	M

Wheel 21

Letter Shown:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
Internal Pin:	M	N	O	P	Q	R	S	T	U	A	B	C	D	E	F	G	H	I	J	K	L

Wheel 19

Letter Shown:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
Internal Pin:	L	M	N	O	P	Q	R	S	A	B	C	D	E	F	G	H	I	J	K

Wheel 17

Letter Shown:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
Internal Pin:	K	L	M	N	O	P	Q	A	B	C	D	E	F	G	H	I	J

Special Case 2 - Operator Error and Stagger

It is actually a blessing when an enemy cryptographer makes the mistake of enciphering the same message twice, makes a one or two letter mistake, or a second cryptographer uses the same settings to encrypt the message again. All of these situations may give rise to a great find known as the 'stagger.'

In Lecture 12, we found that the stagger procedure applies to a periodic cryptogram which contains a long passage repeated in its plain text, the second occurrence occurring at a point in the keying cycle different from the first occurrence. If the passage is long enough, the equivalencies from the two corresponding sequences may be chained together to yield an equivalent primary component. In effect, we by-pass the solution by frequency analysis or making assumptions in the plain text of a polygraphic cipher.

Given two CSP 1500 messages transmitted within one hour of each other:

No. 1

```
   B G K T D   W Z V N P   M R E V W   W W R M G
   T U K R G   K B U E C   J J I P R   P V T K P
   U T T I U   N F G N U   A F Z W U   J R G A W
   F O M B J   B X Q S F   I W V D W   B S C G V
   S E G R K   A J B Y M   E Q H G L   U H P Y B
   W E W X Q   V D W W H   V Q V G U   U W V V N
   L O A U A   D W N H Y   Q V V T V   J Y L S T
   X I N V K   F P K T K   T M L G Z   L D A B W.
```

No. 2

```
   B G K T D   W Z V N P   M R E G F   W T X K T
   L O H I F   J V O B F   V V Q V K   X D E E G
   R I R N G   W F H R L   V N Q T Z   V Y R U X
   T N U U P   G M A T B   S L G X X   P D L M W
   C Y J J H   O L B K Z   O U R H H   T B W X G
   V U S M F   W N Q R Z   C V M L T   H K U N E
   D V Z W J   W M K V Z   L U X Q N   S N M W U
   R T H U H   N C A H P   A Q L H I   X C U B W.
```

Note that the first two letters and the last two letters are the same. The lengths of the messages are the same. The conclusion: the internal plaintext of the messages is the same; and the generated key of the CSP 1500 could well be the same.

Lets find out. From the point where the two messages differ the next 20 letters may be put "in depth" as follows:

```
Pos.    14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33
Key:
No. 1:  V  W  W  W  R  M  G  T  U  K  R  G  K  B  U  E  C  J  J  I


No. 2:  G  F  W  T  X  K  T  L  O  H  I  F  J  V  O  B  F  V  V  Q
```

We expect that the key of both messages is the same; and that the messages are correctly "in depth." We also expect that the plaintext is the same, except that at position 14 (where the ciphertext differs) either a letter was added or deleted from one of the messages.

We assume that the key in position 14 to be 0. The resulting plaintext letters will be:

```
Pos.    14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33
Key:    0
No. 1:  V  W  W  W  R  M  G  T  U  K  R  G  K  B  U  E  C  J  J  I
        e

No. 2:  G  F  W  T  X  K  T  L  O  H  I  F  J  V  O  B  F  V  V  Q
        t
```

From this point on there are two possibilities:

(1) The plaintext of message No. 1 from position 14 on is the same as that as message No. 2 or

(2) The plaintext of message No. 2 from position 14 is the same as that of message No. 1 from position 15 on.

For possibility (1), the plaintext for both messages is:

```
Pos.    14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33
Key:    0  10 10 7  8  1  8  13 8  21 19 7  10 21 8  15 16 9  21 2
No. 1:  V  W  W  W  R  M  G  T  U  K  R  G  K  B  U  E  C  J  J  I
        e  n  n  k  q  o  b  t  n  k  b  a  z  t  n  k  n  z  l  t

No. 2:  G  F  W  T  X  K  T  L  O  H  I  F  J  V  O  B  F  V  V  Q
        t  e  n  n  k  q  o  b  t  n  k  b  a  z  t  n  k  n  z  l
```

If we consider possibility (2):

```
Pos.    14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33
Key:    0  16 7  7  5  20 16 16 25 21 5  3  8  0  25 15 16 20 8  21
No. 1:  V  W  W  W  R  M  G  T  U  K  R  G  K  B  U  E  C  J  J  I
        e  t  k  k  n  h  j  w  e  k  n  w  x  y  e  k  n  k  y  m

No. 2:  G  F  W  T  X  K  T  L  O  H  I  F  J  V  O  B  F  V  V  Q
        t  k  k  n  h  j  w  e  k  n  w  x  y  e  k  n  k  y  m  e
```

Neither possibility is right based on the initial key being 0. Actually, the key could be any number from 0 - 25. We return to the use of the "completing the plain component rundown" that we used in Lectures 12 -13. Our attempt with possibility (1) will fail. Possibility (20) has better results:

```
e t k k n h j w e k n w x y e k n k y m
f u l l o i k x f l o x y z f l o l z n
g v m m p j l y g m p y z a g m p m a o
h w n n q k m z h n q z a b h n q n b p
i x o o r l n a i o r a b c i o r o c q
j y p p s m o b j p s b c d j p s p d r
k z q q t n p c k q t c d e k q t q e s
l a r r u o q d l r u d e f l r u r f t
m b s s v p r e m s v e f g m s v s g u
n c t t w q s f n t w f g h n t w t h v
o d u u x r t g o u x g h i o u x u i w
p e v v y s u h p v y h i j p v y v j x
q f w w z t v i q w z i j k q w z w k y
r g x x a u w j r x a j k l r x a x l z
s h y y b v x k s y b k l m s y b y m a
t i z z c w y l t z c l m n t z c z n b
u j a a d x z m u a d m n o u a d a o c
v k b b e y a n v b e n o p v b e b p d
w l c c f z b o w c f o p q w c f c q e
x m d d g a c p x d g p q r x d g d r f
y n e e h b d q y e h q r s y e h e s g
z o f f i c e r z f i r s t z f i f t h   ***
a p g g j d f s a g j s t u a g j g u i
b q h h k e g t b h k t u v b h k h v j
c r i i l f h u c i l u v w c i l i w k
d s j j m g i v d j m v w x d j m j x l
```

The correct recovered key "in depth" is:

```
Pos.    14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33
Key:    21 11 2  2  0  15 11 11 20 16 0  24 3  21 20 10 11 15 3  16
No. 1:  V  W  W  W  R  M  G  T  U  K  R  G  K  B  U  E  C  J  J  I
        z  o  f  f  i  c  e  r  z  f  i  r  s  t  z  f  i  f  t  h

No. 2:  G  F  W  T  X  K  T  L  O  H  I  F  J  V  O  B  F  V  V  Q
        o  f  f  i  c  e  r  z  f  i  r  s  t  z  f  i  f  t  h  z
```

The difference between the two messages is a single word spacer 'Z' omitted at position 14.

The cryptanalyst must be alert to find the stagger and the find is well worth the effort. There is a mistaken belief that re-enciphering the same text twice with the same wheel settings is not a blunder - however, as you see, it is a big one.

GENERAL SOLUTION OF SIX-WHEEL CSP 1500 CIPHER MACHINE

The general solution of the CSP 1500 has been described in principle under the subtitle "Analysis of a Four-Wheel CSP 1500 Cipher Machine." Given a cryptogram of sufficient length (the more the better) the first step is to analyze the text of the cryptogram divided into the period of the shortest wheel length so that the maximum amount of text per wheel-pin is obtained. In the case of the CSP 1500 (or the C-38 or M209), the shortest is wheel-length 17. The 17 distributions are initially obtained from the cryptogram, each representing every 17th letter of ciphertext.

For any given number of wheels, there will result ciphertext which will be a combination of a given number of different monoalphabetic substitutions. The simplest case is that of one wheel which results in ciphertext which is a combination of two monoalphabetic substitutions, one being the text resulting when the pin of the wheel is in a non-effective position (key = 0) and the other being the text resulting when the pin is in the effective position (key = the number of lugs on the wheel). We know that resulting ciphertext for a six wheel CSP 1500 is a combination of 64 different monoalphabetic substitutions. In the case of the 17 distributions initially obtained from the cryptogram, the letters within a single distribution are the result of the other five wheels and represent a combination of 32 monoalphabetic substitutions. That is the text within a single distribution represents a combination of 32 different alphabetic substitutions. More specifically, Class A represents one set of 32 different monoalphabetic substitutions and Class B represents another set of 32 different monoalphabetic substitutions.

We must think of the concept of the "degree of randomness". A combination of 32 monoalphabetic substitutions is not purely random, though more random, than if only 16 monoalphabetic substitutions were combined. A single monoalphabetic distribution provides ciphertext that clearly not random, (demonstrated in many ways between Lectures 1-14). As we increase the number of monoalphabetic substitutions in the combination process, the ciphertext does become more random. But not perfectly random. In the case of the 17 distributions , we were able to delineate the distributions into two classes, where one class consists of text resulting from one set of 32 different monoalphabetic substitutions and the other class consists of text resulting from another set of 32 different monoalphabetic distribution.

When four wheels were engaged, we matched distributions that resulted from eight monoalphabetic substitutions. Since in the six wheel case we are dealing with 32 monoalphabetic distributions, it is obvious that we need more text to successfully differentiate between the two classes of text. Our mathematical computations are much larger and require computer augmentation to match the distributions.

After successfully dividing the 17 distributions into two classes, in effect we will have found the effective and non-effective pins of wheel length 17, though we still do not know which class represents the effective pins and which the non-effective pins,

We again use the computer to combine all the distributions of each class separately. We next shift one of the combined distributions through each of 26 positions, we attempt to find the number of lugs on wheel 17.

After initial success with wheel length 17, we turn to wheel length 19, and divide the pin settings again into two classes to find the pin settings on wheel length 19. We continue with the procedure for the wheel lengths of 21, 23, 25 and finally 26.

It is possible to combine several shorter cryptograms in order to obtain sufficient text for the general solution. However, this is not a simple add/subtract procedure. It is necessary to use the computer to match the 17 distributions of one cryptogram against the 17 distributions of another cryptogram by shifting the distributions of one of the cryptograms through the 17 possible shifts until the total 17 distributions of one message match the total 17 distributions of the other message. At this point wheel 17 of both cryptograms will be in the same effective position; and for the purpose of pin settings of wheel 17, separating the 17 distributions into two classes, the two cryptograms may be combined.

in summary, the general solution follows the procedures described under the four wheel analysis.

****

[NB: This lecture contains several different fonts to account for the table widths. As a ASCII file this may be a problem for some e-mail systems. I will also send a DOC file from WORD to the CDB for those who need it.]