CLASSICAL CRYPTOGRAPHY COURSE
BY LANAKI
November 13, 1995
Revision 1

LECTURE 3
SUBSTITUTION WITH VARIANTS PART II
MULTILITERAL SUBSTITUTION

SUMMARY

In Lecture 3, we continue our look into substitution ciphers, and move into the multiliteral substitution case, we field more tools for cryptanalysis, look at some fascinating historical variations, we review "the unbreakable cipher" and solve homework problems.

MULTILITERAL SUBSTITUTION WITH SINGLE-EQUIVALENT CIPHER ALPHABETS

Monoalphabetic substitution methods are classified as uniliteral and multiliteral systems. Uniliteral systems maintain a strict one-to-one correspondence between the length of the units of the plain and those of the cipher text. Each letter of plain text is replaced by a single character in the cipher text. In multiliteral monoalphabetic substitution systems, this correspondence is no longer one plain to one cipher but may be one plain to two cipher, where each letter of the plain text is replaced by two characters in the cipher text; or one plain to three cipher, where a three-character combination in the cipher text represents a single letter of the plain text. We refer to these systems as uniliteral, biliteral, and triliteral, respectively. Ciphers in which one plain text letter is represented by cipher characters of two or more elements are classed as multiliteral. [FR1], [FR2],[FR5]

BILITERAL CIPHERS

Friedman gives some interesting examples of biliteral monoalphabetic substitution. [FR1] Many cipher systems start with a geometric shape. Using the square in Figure 3-1,

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

Figure 3-1

We derive the following cipher alphabet:

```
Plain :  a  b  c  d  e  f  g  h  i  j  k  l  m
Cipher: WW WH WI WT WE HW HH HI HT HT HE IW IH

Plain :  n  o  p  q  r  s  t  u  v  w  x  y  z
Cipher: II IT IE TW TH TI TT TE EW EH EI ET EE
```

The alphabet derived from the cipher square or matrix is referenced by row and column coordinates, respectively.

The key to this system is that when a message is enciphered by this biliteral alphabet, the cryptogram is still monoalphabetic in character. A frequency distribution based upon pairs of letters will have all the characteristics of a simple uniliteral distribution for a monoalphabetic substitution cipher.

Numbers can be used as effectively as letters in the biliteral cipher. The simplest form is A=01, B=02, C=03,...Z=26. So, the plain text letters have as their equivalents two-digit numbers indicating their position in the normal alphabet.

Other dinome (two digit) cipher matrices are previewed:

	1	2	3	4	5	6	7	8	9	0
1	.	A	B	C	D	E	F	G	H	I	J
2	.	K	L	M	N	O	P	Q	R	S	T
3	.	U	V	W	X	Y	Z	.	,	:	;

Figure 3-2

Note that frequently-used punctuation marks can be enciphered in the above matrix.

Another four examples are:

Figure 3-3

	5	6	7	8	9	0
1	. A	B	C	D	E	F
2	. G	H	IJ	K	L	M
3	. N	O	P	Q	R	S
4	. T	UV	W	X	Y	Z

Figure 3-4

	1	2	3	4	5	6	7	8	9
1	. A	B	C	D	E	F	G	H	I
2	. J	K	L	M	N	O	P	Q	R
3	. S	T	U	V	W	X	Y	Z	*

Figure 3-5

	M	U	N	I	C	H
B	.A	7	E	5	R	M
E	.G	1	N	Y	B	2
R	.C	3	D	4	F	6
L	.H	8	I	9	J	O
I	.K	L	O	P	Q	S
N	.T	U	V	W	X	Z

Figure 3-6

	A	B	C	D	E	F	G	H	I
A	. A	D	G	J	M	P	S	V	Y
B	. B	E	H	K	N	Q	T	W	Z
C	. C	F	I	L	O	R	U	X	1
D	. 2	3	4	5	6	7	8	9	0

It is possible to generate false or pseudo-code or artificial code language by using an enciphering matrix with vowels as row indicators and consonants as column indicators.

Figure 3-7

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

Enciphering the word RAIDS would be OCABE FAFOD. [FR5]

Another subterfuge used to camouflage the biliteral cipher matrix is to append a third character to the row or column indicator. This third character may be produced through the use of cipher matrix shown in Figure 3-8 (wherein A=611, B=612, etc.) or the third character can be the "sum checking" digit which is the non-carrying sum (modulo 10) of the

preceding two digits such as trinomes 257, 831, and 662. It may also involve self summing groups such as 254, 830, 669 all which sum to the constant 1, or finally the third digit can be random, inserted solely for the pleasure of the cryptanalyst.

Figure 3-8

```
      1  2  3  4  5
    ..................
61  .  A  B  C  D  E
72  .  F  G  H IJ  K
83  .  L  M  N  O  P
94  .  Q  R  S  T  U
05  .  V  W  X  Y  Z

A=611 ,  B=612    X=053
```

All the above matrices are bipartite. They can be divided into two separate parts that can be clearly and cleanly defined by row and column indicators. This is the primary weakness of this type of cipher. [FR1]

Sinkov presents a good description of the modulo arithmetic required to solve biliteral cipher challenges. [SINK] A more involved look at the statistics involved can be found in [CULL].

BILITERAL BUT NOT BIPARTITE

Consider the following cipher matrix:

Figure 3-9

```
      1  2  3  4  5
    ..................
09  .  H  Y  D  R  A
15  .  U  L  IJ C  B
21  .  E  F  G  K  M
27  .  N  O  P  Q  S
33  .  T  V  W  X  Z
```

We can produce a biliteral cipher alphabet in which the equivalent for any letter in the matrix is the sum of the two coordinates which indicate its cell in the matrix:

```
Plain      A   B   C   D   E   F   G   H   I   J   K   L   M
Cipher    14  20  19  12  22  23  24  10  18  18  25  17  26

Plain      N   O   P   Q   R   S   T   U   V   W   X   Y   Z
Cipher    28  29  30  31  13  32  34  16  35  36  37  11  38

          A = 9+5 =14,  E = 21 + 1 =22
```

The cipher units are biliteral but they are not bipartite. Cipher text equivalent of plain text letter "A" is 14 and digits 1 and 4 have no meaning per se. Plain text letters whose cipher equivalents begin with 1 may be found in two different rows of the matrix and those of whose equivalents end in 4 appear in three different columns. [FR1]

Another possibility lends itself to certain multiliteral ciphers in the use of a word spacer or word separator. The word space might be represented by a value in the matrix; i.e., the separator is enciphered as a value (dinome 39 in Figure 3-4). The word space might be an unenciphered element.

Lets break from the theory and look at four interesting multiliteral historical ciphers before discussing the general cryptanalytic attack on the multiliteral cipher.

TRITHEMIAN

The abbot Trithemius, born Johann von Heydenberg (1462-1516) invented one of the first multiliteral ciphers. It was fashioned similar to the Baconian Cipher and was a means for disguising secret text. His work "Steganographia" published in 1499 describes several systems of 'covered writing.' [TRIT][WATS], [FR1] The science of steganography is named after him. Several Internet discussion groups currently discuss the use of steganography to hide messages in graphics files. (.GIFfiles)

His alphabet, modified to include 26 letters of present-day English, is shown in Figure 3-10, below; it consists of all the permutations of three things taken three at a time or 3 ** 3 = 27 in all.

Figure 3-10

A - 111	G - 131	M - 221	S - 311	Y - 331
B - 112	H - 132	N - 222	T - 312	Z - 332
C - 113	I - 133	O - 223	U - 313	* - 333
D - 121	J - 211	P - 231	V - 321	
E - 122	K - 212	Q - 232	W - 322	
F - 123	L - 213	R - 233	X - 323	

The cipher text does not have to be restricted to digits; any groupings of three things taken three at a time will do.

BACON

Sir Francis Bacon (1561-1626) invented a cipher in which the cipher equivalents are five-letter groups and the resulting cipher is monoalphabetic in character. Bacon uses a 24 letter cipher with I and J, U and W used interchangeably.

A =	aaaaa	I/J =	abaaa	R =	baaaa
B =	aaaab	K =	abaab	S =	baaab
C =	aaaba	L =	ababa	T =	baaba
D =	aaabb	M =	ababb	U/V =	baabb
E =	aabaa	N =	abbaa	W =	babaa
F =	aabab	O =	abbab	X =	babab
G =	aabba	P =	abbba	Y =	babba
H =	aabbb	Q =	abbbb	Z =	babbb

Bacon described the steganographic effect of message enfolding in an innocent external message. Suppose we let capitals be the "a" element and lower-case letters represent the "b" elements. The message "All is well with me today" can be made to convey the message "Help." Thus,

A	L	l	i	s		W	E	l	L		W		I	t	H		m	E		T	o	d	a	Y
a	a	b	b	b		a	a	b	a		a		a	b	a		b	a		a	b	b	b	a
		H						E							l							P		

Bacon describes many several variations on the theme. [FR1], [DEAU] Note the regularity of construction of Bacon's biliteral alphabet, a feature which permits its reconstruction from memory.

HAYES CIPHERS

Probably the most corrupt political election occurred on November 7, 1876 with the election of President Rutherford B. Hayes (Republican). He defeated Samuel Jones Tilden (Democrat). Tilden had won the popular vote by 700,000 votes but because of frauds surrounding the electoral college, he was deprived of the high office of President. Actual both

candidates were involved with bribery, election tampering, voter fraud, conspiracy and a host of other goodies. Tilden ran on a law and order ticket that credited him with convicting Boss Tweed and the Tweed Ring in New York City, which controlled the city through Tammany Hall. For two years into Hayes Presidency, the scandals persisted.

With the help of New York Tribune, Republicans finished the Tilden 'honesty' horse. They published the Tilden Ciphers and keys. There were about 400 of them representing substitution and transposition forms. We will revisit the transposition forms at a later juncture. They represented secret and illegal operations by Tilden's men in Florida, Louisiana, South Carolina and Oregon. The decipherments were done by investigators of the Tribune. Here are two examples and their solution. [TILD] , [FR1] , [TRIB]

GEO. F. RANEY, Tallahassee.

```
P P Y Y E M N S N Y Y Y P I M A S H N S Y Y S S I T E P A A E
N S H N S P E N N S S H N S M M P I Y Y S N P P Y E A A P I E
I S S Y E S H A I N S S S P E E I Y Y S H N Y N S S S Y E P I
A A N Y I T N S S H Y Y S P Y Y P I N S Y Y S S I T E M E I P
I M M E I S S E I Y Y E I S S I T E I E P Y Y P E E I A A S S
I M A A Y E S P N S Y Y I A N S S S E I S S M M P P N S P I N
S S N P I N S I M I M Y Y I T E M Y Y S S P E Y Y M M N S Y Y S
S I T S P Y Y P E E P P P M A A A Y Y P I I T
```

L' Engle goes up tomorrow. Daniel

Examination of the message discloses a bipartite alphabet cipher with only ten different letters used. Dividing the messages by twos, assigning arbitrary letters for pairs of letters and performing a triliteral frequency distribution will yield a solution.

```
    PP  YY  EM  NS  NY  YY  PI  MA  SH  NS  YY  SS  etc
    A   B   C   D   E   B   F   G   H   D   B   I   etc
```

Message reads:

Have Marble and Coyle telegraph for influential men from Delaware and Virginia. Indications of weakening here. Press advantage and watch board.

Here is another Tilden cipher using numerical substitutes:

S. PASCO AND E. M. L'ENGLE

84 55 84 25 93 34 82 31 31 75 93 82 77 33 55 42

93 20 93 66 77 66 33 84 66 31 31 93 20 82 33 66

52 48 44 55 42 82 48 89 42 93 31 82 66 75 31 93

DANIEL

There were several messages of this type. They disclosed that only 26 different numbers were used.

Message reads:

Cocke will be ignored, Eagan called in. Authority reliable.

The Tribute experts gave the following alphabets:

```
AA = O   EN = Y   IT = D   NS = E   PP = H   SS = N
AI = U   EP = C   MA = B   NY = M   SH = L   YE = F
EI = I   IA = K   MM = G   PE = T   SN = P   YI = X
EM = V   IM = S   NN = J   PI = R   SP = W   YY = A
-------------------------------------------------
20 = D   33 = N   44 = H   62 = X   77 = G   89 = Y
25 = K   34 = W   48 = T   66 = A   82 = I   93 = E
27 = S   39 = P   52 = U   68 = F   84 = C   96 = M
31 = L   42 = R   55 = O   75 = B   87 = V   99 = J
```

William F. Friedman correlated these alphabets with the results being amusing:

```
          H  I  S  P  A  Y  M  E  N  T
          1  2  3  4  5  6  7  8  9  0
        ------------------------------
   H 1 .                             .
   I 2 .              K     S        D .
   S 3 .  L     N  W               P    .
   P 4 .     R     H           T       .
   A 5 .     U        O                 .
   Y 6 .     X           A     F       .
   M 7 .              B     G           .
   E 8 .     I     C        V     Y    .
   N 9 .        E        M        J    .
   T 0 .                             .
        ------------------------------
```

The blank squares may have contained proper names and money designations. Key = HISPAYMENT for bribary seems to be appropriate. [HIS1], [TRIB], [TILD], [FR1]

BLUE AND GREY

One of the most fascinating stories of the American Civil War (1861-65) is about communications using flag telegraphy or also known as the wigwag signal system.

Wigwag is a system of positioning a flag (or flags) at various angles that indicate the corresponding twenty-six letters of the alphabet. It was created in the mid-1800s by three men working at separate locations: Navy Captain Phillip Colomb and, Army Captain Francis Bolton, in England, and Surgeon-inventor Albert J. Meyer in America. [WRIX] Meyer observed the railroad electromagnetic telegraph, developed by Alexander Bain, and invented a touch method of communication for the deaf and later the wigwag system. He developed companion methods with torches and disks. The name "wigwag" derived from the flag movements.

Three main color combinations were used in flags measuring two, four and six feet square. The white banners had red square centers while the black or red flags had white centers. Myers method required three motions (elements) to be used for each letter. The first position always initiated a message sequence. Motion one went from head to toe and back on right side. Motion 2 went from head to toe and back on left side. Motion three went from head to toe and back in front of the man. Each motion made quickly. Chart 3-1 indicates the multiliteral alphabet and directional orders required to convey a message.

Chart 3-1

A - 112	H - 312	O - 223	V - 222
B - 121	I - 213	P - 313	W - 311
C - 211	J - 232	Q - 131	X - 321
D - 212	K - 323	R - 331	Y - 111
E - 221	L - 231	S - 332	Z - 113
F - 122	M - 132	T - 133	
G - 123	N - 322	U - 233	

Myers Signal Directions

3 - End of a word
33 - End of a sentence
333 - End of message
22.22.22.3 - Signal of assent. Message understood
22.22.22.333 - Cease signaling
121.121.121.3 - Repeat
212121.3 - Error
211.211.211.3 - Move a little to the right
221.221.221.3 - Move a little to the left

As the Civil War wore on, Myer increased the wigwag motions to four. This enabled more specialized words and abbreviations to be used. In 1864, Myer invented a similar daytime system with disks.

For night signals, Myer applied his system with torches on the signal poles and lanterns. A foot torch was used as a reference point. Thus the direction of the flying wave could better be seen. Compare this to the semaphore system used by ships at sea when radio silence is a must.

Myer continuously improved his invention through 1859 and presented his findings gratis to the Union Army (which gave him a luke warm yawn for his trouble). Alexander Porter, his chief assistant joined the Confederate Army and used the wigwag system in actual combat. Porter was able to warn Colonel Nathan Evans at Manassas Junction - Stone Bridge that the Union Army had reached Sudley Ford and was about to surprise General Beauregard's best Division. Porter sent from his observation tower, the following message to Colonel Evans at the Stone Bridge defenses: "Look out for your left, you are turned."

Colonel Evans turned his cannons and musket fire toward the Federal troops before they could initiate their attack. Porter was credited later (and decorated) for his vigilance led to changes in the tactics of the entire struggle around Manassas Junction. The application of the new signal system had directly influenced the shocking Union defeat that eventful July day.

Myers signaling system was catapulted into use at the Battle of Gettysburg. General Lee had invaded northern soil in June 1863. His Potomac crossing was relayed by flag system to the War Department. General Joseph Hooker resigned under fire on June 28. General George Meade (of NSA grounds fame) took over command of the Army of the Potomac. His headquarters were at Taneytown, MD. Startling news came via signalmen on July 1. A skirmish on the Maryland border indicated that General Buford was facing a major force not in Maryland but in Pennsylvania. Lee was himself in command at Gettysburg. Signalmen of each army unit sent out calls for help. Reinforcements from dozens of units several miles away were committed to the fray. By July 1, 73,000 gray and 88,000 blue met in one of history's most decisive battles. Rarely, if at all, do textbooks even hint that the secret message system of flags affected these history changing events. Yet the crucial sightings by Union observers directly tipped the scales against Lee's best tactics. The most famous incident was when Captain Castle on Cemetery Ridge, refused to submit to Confederate artillery barrage as General George Pickett charged the "thin blue line", used a wooden pole and a bedsheet to make a makeshift flag to alert Union forces under General Meade who ordered counter-measures. Pickett's charge was stopped short of breaching the Union lines. General Lee's gamble failed. Previously disregarded flagmen enabled George Meade to enter the shrine of heros. [BLUE], [ANNA], [MYER], [NIBL], [TRAD], [WRIX], [KAHN]

FURTHER NOTES ON CRYPTANALYSIS OF MULTILITERAL CIPHERS

LIMITED CHARACTERS

Multiliteral ciphers are often recognized by the fact that the cryptographic text is usually composed of but a very limited number of different characters. They are handled in the same way as are uniliteral monoalphabetic substitution ciphers. So long as the same character or number is used to represent the same plain text letter, and so long as a given letter of plain text is always represented by the same character or combination of characters, then the substitution is strictly monoalphabetic and can be handled by methods in my Lectures 1and 2.

BILITERAL CIPHERS

In the case of biliteral ciphers where the row and column indicators are not identical, the direction of reading the cipher pairs is chosen at will for each succeeding cipher pair, and analysis of contacts of the letters comprising the cipher pairs will disclose that there are two distinct families of letters, and the cipher pair will never consist of two letters of the same family. We reduce by further substitution to uniliteral terms and solve by known methods.

WORD SEPARATORS

If a multiliteral cipher includes a provision for the encipherment of a word separator, the cipher equivalent of this word separator may be readily identified because it will have the highest frequency of any cipher unit.

Friedman presents data on word separators:

For English, the average word length is 5.2 letters. The word separator will be close to 16% frequency. [FR1] The letters of the alphabet take on new percentage frequencies as follows:

A - 6.2	J - 0.16	S - 5.1
B - 0.84	K - 0.25	T - 7.7
C - 2.6	L - 3.0	U - 2.2
D - 3.5	M - 2.1	V - 1.3
E - 11.0	N - 6.6	W - 1.3
F - 2.3	O - 6.3	X - 0.41
G - 1.3	P - 2.3	Y - 1.6
H - 2.9	Q - 0.25	Z - 0.08
I - 6.2	R - 6.4	

On the other hand, if the word separator is a single character, this character may be identified by its positional appearance spaced 'wordlength-wise' in the cipher text and by the fact that it never contacts itself.

It is advisable to reduce multiliteral cipher text to uniliteral equivalents, especially if a triliteral frequency distribution is made. If not more than 36 combinations are present in the cryptogram, the extra values over 26 may be represented by digits for the purpose of reduction. For more than 36 groups, cipher text can be attacked in multiliteral groupings.

ANAGRAMING

One of the first steps to solving a multiliteral cipher with a cipher matrix, is to anagram the letters comprising the row and column indicators in an attempt to disclose the key words used. When the anagraming process does disclose any key word(s), a skeleton reconstruction matrix which is the duplicate of the original enciphering matrix is made to show the order of the row and column indicators. Partial recovery of plain text may be possible at this point in the analysis. Looking at the frequency analysis (and location of the crests and troughs) may tell us something about the enciphering alphabet as normal or keyed.

NUMERICAL CIPHERS

Cipher alphabets whose cipher components consist of numbers are practicable for telegraph or radio transmission. They may take forms corresponding to those employing letters.

Standard numerical cipher alphabets are those in which the cipher component is a normal sequence of numbers.

```
Plain  -  A   B   C   D   E   F   G   H   I   J   K   L   M
Cipher - 11  12  13  14  15  16  17  18  19  20  21  22  23

Plain  -  N   O   P   Q   R   S   T   U   V   W   X   Y   Z
Cipher - 24  25  26  27  28  29  30  31  32  33  34  35  36
```

We could easily have started the cipher alphabet with A= 01, B=02,..., Z=26 with the same results.

Mixed numerical cipher alphabets are those that have been keyed by a key word turned into numerical cipher equivalents or have a random combination of two or more digits for each letter of plain text.

```
Plain  -  A   B   C   D   E   F   G   H   I - J   K   L   M
Cipher - 76  88  01  67  04  80  66  99  96  96  02  69  90

Plain  -  N   O   P   Q   R   S   T   U   V   W   X   Y   Z
Cipher - 77  05  87  60  39  79  03  78  68  98  86  70  97
```

The computer whizzes are now thinking that the example has all numbers less than 100. Therefore, a brute force attack on all combinations of two letter-equivalents of the above ciphertext numerical values taken two at a time in combination with the digram frequency data could be a good approach to the cipher matrix construction problem. The ASOLVER computer program at the CDB does this kind analysis and adds threshold limitations on the search.

Figure 3-3 and 3-4 could be arranged for simple numerical equivalents like this:

Figure 3-3a

```
     1  2  3  4  5
   ..............
1  . A  B  C  D  E
2  . F  G  H IJ  K
3  . L  M  N  O  P
4  . Q  R  S  T  U
5  . V  W  X  Y  Z
```

Figure 3-4a

```
     1  2  3  4  5  6  7  8  9
   ...........................
1 . A  B  C  D  E  F  G  H  I
2 . J  K  L  M  N  O  P  Q  R
3 . S  T  U  V  W  X  Y  Z  *
```

where: A = 11, R=42 Z=55

Numerical cipher values lend themselves to treatment by various mathematical processes to further complicate the cipher system in which they are used. These processes, mainly addition or subtraction, may be applied to each cipher equivalent individually, or to the complete numerical cipher message by considering it as one number. [OP20]

Reference [NIC4] on Russian Cryptography describes the VIC Cipher and the one-time pad. Both involve mathematical treatment to numerical based ciphers. The Hill cipher is another good example of the use of mathematical transformation processes on ciphers and is presented in David Kahn's book. [KAHN]

In modern cryptographic systems, the DES family of ciphers use simple S-Boxes [substitution boxes] that are reorganized by ordered non-linear mathematical rules applied several times over (know as rounds). [NIC4], [OP20], [RHEE], [HILL], [IBM1]

ONE-TIME PAD

The question of 'unbreakable' mathematical ciphers might be poised at this juncture. Lets look at the famous one-time pad and see what it offers. [NIC4]

The one-time pad is truly an unbreakable cipher system. There are many descriptions of this cipher. One of the better descriptions is by Bruce Schneier. [SCHN] It consists of a nonrepetitive truly random key of letters or characters that is

used just once. The key is written on special sheets of paper and glued together in a pad. The sender uses each key letter on the pad to encrypt exactly one plain text letter or character. The receiver has an identical pad and uses the key on the pad, in turn, to decrypt each letter of the ciphertext. [SHAN]

Each key is used exactly once and for only one message. The sender encrypts the message and destroys the pad's page. The receiver does the same thing after decrypting the message. New message - new page and new key letters/numbers - each time.

The one-time pad is unbreakable both in theory and in practice. Interception of ciphertext does not help the cryptographer break this cipher. No matter how much ciphertext the analyst has available, or how much time he had to work on it, he could never solve it. [KAHN]

The reason is that no pattern can be constructed for the key. The perfect randomness of the one time system nullifies any efforts to reconstruct the key or plain text via horizontal or lengthwise analysis, via cohesion, via re-assembly (such as Kasiski or Kerckhoff's columns) via repeats or via internal framework erection. [KAHN] [KAH1], [WRIX], [NIC4], [SCHN]

Brute force (trial and error) might bring out the true plaintext but it would also yield every other text of the same length, and there is no way to tell which is the right one. The worst of it is that the possible solutions increase as the message lengthens.

Supposing the key were stolen, would this help to predict future keys? No, because a random key has no underling system to exploit. If it did, it would not be random. [KAHN]

A random key sequence XOR 'ed with a nonrandom plain text message produces a completely random ciphertext message and no amount of computing will change that. [SCHN] The one-time pad can be extended to encryption of binary data. Instead of letters, we use bits. [SCHN]

FRESH KEY DRAWBACK

The one-time pad has a drawback - the quantities of fresh key required. For military messages in the field (a fluid situation) a practical limit is reached. It is impossible to produce and distribute sufficient fresh key to the units. During WWII, the US Army's European theater HQ's transmitted, even before the Normandy invasion, 2 million five (5) letter code groups a day! It would have therefore, consumed 10 million letters of key every 24 hours -the equivalent of a shelf of 20 average books. [KAH1] , [FRAA]

RANDOMNESS

The real issue for the one-time pad, is that the keys must be truly random. Attacks against the one-time pad must be against the method used to generate the key itself. [SCHN] Pseudo-random number generators don't count; often they have nonrandom properties. Reference [SCHN], Chapter 15, discusses in detail random sequence generators and stream cipher. I take exception to his remarks regarding keyboard latency measurement. People's typing patterns are anything but random (especially us two finger types). [SCHN] [MART]

ONE-TIME PAD SIMPLE EXAMPLE W/O SUPERENCIPHERMENT OR XOR

Begin with a cipher (A=1, B=2 ...)

```
PT:   T  A   X  A   T  I  O  N    I  S    T  H  E  F  T
CE:  20  1  24  1  20  9 15 14    9 19   20  8  5  6  20
```

>From a table of truly random numbers:

```
  10480 15011 01536 02011 81647 91646 69719 22368
  45673 25595 85393 30995 89198 27982 24130 48360
  22527 97265 76393 64809 15179 42167 ....
```

Add the cipher equivalent to the random key:

```
   T         A       X       A       T       I
   20        1       24      1       20      9
10480    15011   01536   02011   81647   91646
-----    -----   -----   -----   -----   -----  ...
10500    15012   01560   02012   81667   91655
```

Transmit new cipher text:

```
10500  15012  01560  02012  81667  91655  69734  .....
```

Receiver subtract key out of message and decodes equivalents.

Many variations exist. Note in the cipher text T1 .ne. T2 .ne. T(i) and A1 .ne. A2 .ne. A(i), etc. [MARO]

ONE-TIME PAD HISTORICAL CONSIDERATIONS

The one-time pad originated from the work of Gilbert Vernam in 1917. Vernam worked for ATT. He got his idea from the French telegrapher Emile Baudot. Baudot code replaced letters with electrical impulses, called units. Every character was given 5 units that either signified a pulse of electrical current ("marks") or its absence ("spaces") during a given time period. [32 combinations in all]. In 1917, paper tape was used and the marks and spaces were read by metallic fingers. Vernam essentially automated the process and devised a cipher on it.

In modern computer terms, key bits were added modulo 2 to plaintext bits on a bit by bit basis. If X = x1, x2, x3.. denotes the plain text, and K = k1, k2, k3 .. the keystream, Vernam's cipher produces a cipher text bit stream Y = Ek(X) = y1, y2, y3. [VERN]

CONCURRENT DEVELOPMENTS

Other countries conducted similar research. Between 1918-1920, other one-time pad methods were developed. The German Foreign Office employed the one-time pad in 1920. The Russians first stole and then improved the German system. It was fully deployed in 1925 for diplomatic use! OSS and SOE operatives in WWII had special grid one-time pad's. By 1944, OSS technicians had developed pages made of film that were read with a hand magnifying glass. By 1960, Russian pads were the size of a postage stamp or scrolls the size of a large eraser. The Russians were first to conceal the one-time pad in microfilm. One-time pads were made of cellulose nitrate for rapid destruction. [RHEE] ,[VERN], [TERR], [KAHN]

RUSSIAN IMPLEMENTATION OF THE ONE-TIME PAD

So why classify the one-time pad with Russian Ciphers? Because they have been serious about using it since 1925! Before 1917, Russian diplomatic and military systems could be expressed by the old axiom:

Cryptography + Loose Discipline = Chaos

After her loss of trade information to the British in 1920, and defeats of her Army in WWI because of poor cipher handling, she woke up. By 1916, Russia's intercept service at Nicolaieff was in full service against the Germans. From 1920 through today, Russia has targeted stealing other countries codes with "great vigor" as Kennedy once said. Code stealing was done through the COMINT efforts of the former KGB and GRU. The Spets-Odel (Special Department) was a primary agency involved with Ciphers and Cryptanalysis. Section 6 grew 400% over a 10 year period prior to WWII.

The Soviet Union has employed the one-time pad to protect ALL her diplomatic missions from 1930 on. Consequently her crucial Foreign Office messages were not read by foes, neutrals, nor allies. The GRU and the Soviet Spy rings - "LUCY", "RED ORCHESTRA, and "Sorge's Net" all used the one- time pad. They also used a straddling checkerboard variant (not unbreakable).

The one-time pad is used in the old fashioned form in the Soviet Mission - diplomatic , secret police, military, commercial, political (Communist Party) - all have their own keys. All cables coming into a legation look alike: simple groups of five digits. Letters that are photographed, codenames are applied and then enciphered in one-time pad system. [COVT], [BLK], [BARR]

Agents in the field use the one-time pad. Radio links to Moscow, are encrypted via one-time pads. The main Soviet spy cipher today still employs the one-time pads.

The most dramatic spy stories (Klaus Fuchs, Iger Gouzenko, Vladimir Petrov, Colonel Zabotin, Rudolf Abel, Gregory Liolios, Eleftherious Voutsas, the Krogers, Guiseppe Martelli, Ali Abbasi, Reino Hayhanen, Aldridge Ames ...) all have used the one-time pads.

Such is cryptology in the Soviet Union - complex, enigmatic, focused, state-of-the-art, applying the one-time pad principles to other ciphers. Do you remember when the diplomatic ciphers in use at the American embassy in Moscow were solved? Russia has a profound understanding of cryptography and cryptanalysis. [VOGE], [SUVO], [KAHN]

The U.S. history was different. Some would argue that the U.S. became serious and superplayers in 1953. Some would argue 1943. But not many will argue 1925 (we still had SIGTOT then). [SISI]

LECTURE 4

In Lecture 4, we will complete our look into English substitution ciphers, by describing multiliteral substitution with difficult variants. The Homophonic and GrandPre Ciphers will be covered. A synoptic diagram of the substitution ciphers presented in Lectures 1-4 will be presented.

LECTURE 5 - 6

We will cover recognition and solution of XENOCRYPTS (language substitution ciphers) in detail.

SOLUTION TO HOMEWORK PROBLEMS FROM LECTURE 2

BOZOL gets the kudo for best solution on the homework. Both problems were unkeyed.

Pd-1. Daniel

```
H Z K L X   A L H X P   N C I N Z   X F L I X   G N W Q X   P N Z K T   L N K X O

L X N I Z   X G I N X   P N E Z K   X W Q X P   Z X L H X   P N C I N   Z X S N Q

N T X W Q   X P N W V   S N I K L   K H B L X   N W Q L X   H F Z I L   N X A Z K

S B W E N   I.
```

Problem 1 breaks down as follows:

```
High frequency (top 7%), count = 8 : XNLZI
Medium frequency letters:          : KPWHQS
Lo frequency  (less than 3)        : ABCEFGTOV
Zero (0) frequency                 : DJMRUY
By "N" Gram Count
```

6 gram	Count	CT Frequency
HXPNCI	2	5 19 6 17 2 8
LHXPNC	2	10 5 19 6 17 2
NCINZX	2	17 2 8 17 9 19
PNCINZ	2	6 17 2 8 17 9
XPNCIN	2	19 6 17 2 8 17

5 grams	Count	CT Frequency
CINZX	2	2 8 17 9 19
HXPNC	2	5 19 6 17 2
LHXPN	2	10 5 19 6 17
NCINZ	2	17 2 8 17 9
PNCIN	2	6 17 2 8 17
WQXPN	2	6 5 19 6 17
XPNCI	2	19 6 17 2 8
XWQXP (THATS)?	2	19 6 5 19 6

4 grams	Count	CT Frequency
CINX	2	2 8 17 9
HXPN	2	5 19 6 17
INZX	2	8 17 9 19
LHXP	2	10 5 19 6
NCIN	2	17 2 8 17
PNCI	2	6 17 2 8
QXPN	2	5 19 6 17
WQXP	2	6 5 19 6
YPNC	2	19 6 17 2
XWQX (THAT)?	2	19 6 5 19

3 grams	Count	CT Frequency
CIN	2	2 8 17
HXP	2	5 19 6
INZ	2	8 17 9
LHX	2	10 5 19
LXN	2	10 19 17
NCI	2	17 2 8
NWQ	2	17 6 5
NZX	2	17 9 19
PNC	2	6 17 2
QXP	3	5 19 6
WQX	3	6 5 19
XPN	5	19 6 17
XWQ	2	19 6 5

2 grams	Count	CT Frequency
CI	2	2 8
HX	2	5 19
IN	3	8 17
KL	2	7 10
KX	2	7 19
LH	2	10 5
LN	2	10 17
LX	4	10 19
NC	2	17 2
NI	2	17 8
NW	3	17 6
NX	2	17 19
NZ	3	17 9
PN	5	6 17
QX	3	5 19
SN	2	3 17
WQ	4	6 5
XA	2	19 2
XG	2	19 2
XN	2	19 17
XP	6	19 6
XW	2	19 6
ZK	4	9 7
ZX	4	9 19

	Frequency	* Variety	=	Contacts
A	2	3	6	XLZ
B	2	4	8	HLSW
C	2	2	4	NI
D	0	0	0	
E	2	3	6	NZW
F	2	4	8	XLHZ
G	2	3	6	XNI
H	5	6	30	ZLXKBF
I	8	7	56	CNLXZGK
J	0	0	0	
K	7	8	56	ZLTNXIHS
L	10	11	110	KXAHFITNOBQ
M	0	0	0	
N	17	13	221	PCIZGWLKXESQT
O	1	2	2	XL
P	6	3	18	XNZ
Q	5	4	20	WXNL
R	0	0	0	
S	3	5	15	XNVKB
T	2	4	8	KLNX
U	0	0	0	
V	1	2	2	WS
W	6	6	36	NQXVBE
X	19	15	285	LAHPZFIGQKONWST
Y	0	0	0	
Z	9	9	81	HKNXIEPFA

>From above data we try X= t and N=e, P=h. Then E=y, L=l, W=o, S = D.

Message reads: Sanity is the great virtue of the ancient literature; the want of that is the great defect of the modern, in spite of its variety and power. Matthew Arnold

Pd-2. Join the army. Daniel

F L B B A O I A F Q E A O M Z U I L O N R Z O Q A O P I L O M O L S F

P F L I P F L B B A O E R I C A O Q E F O P Q B L O W A V H Z O W E A

P X Z Q Q G A P Z I V V A Z Q E G A Q E F H T E L G L S A P L R O W L

R I Q O U F I E F P E A Z O Q Z I V I L Q T F Q E E F P G F M P L I G

U B L G G L T H A.

Problem 2 breaks down as follows:

```
High frequency (top 7%), count = 10 : LOAFQEI
Medium frequency letters:           : PZGBRVHMTUW
Lo frequency  (less than 3)         : SCNX
```

Zero (0) frequency : DJKY

By "N" Gram Count

6 gram	Count	CT Frequency
FLBBAO	2	12 15 6 6 14 15
5 grams		
FLBBA	2	12 15 6 6 14
LBBAO	2	15 6 6 14 15
4 grams		
BBAO	2	6 6 14 15
FLBB	2	12 15 6 6
LBBA	2	12 6 6 14
3 grams		
BAO	2	6 14 15
BBA	2	6 6 14
EFP	2	11 12 10
FLB	2	12 15 6
FQE	2	12 12 11
ILO	2	11 15 15
LBB	2	15 6 6
PFL	2	10 12 15
QEF	2	12 11 12
ZIV	2	8 11 4
ZOQ	2	8 15 12
2 grams		
AO	5	14 15
AP	3	14 10
AZ	2	14 8
BA	2	6 14
BB	2	6 6
BL	2	6 15
EA	3	11 14
EF	4	11 12
FL	3	12 15
FP	3	12 10
FQ	2	12 12
GA	2	7 14
GL	2	7 15
IL	3	11 15
IV	2	11 4
LB	2	15 6
LG	2	15 7
LI	2	15 11
LO	3	15 15
LR	2	15 4
LS	2	15 2

OM	2	15	3
OP	2	15	10
OQ	3	15	12
OW	3	15	3
PF	2	10	12
PL	2	10	15
QE	5	12	11
RI	2	4	11
ZI	2	8	11
ZO	3	8	15
ZQ	2	8	12

	Frequency	* Variety	=	Contacts
A	14	14	196	BOIFEQCWVPGZSH
B	6	5	30	LBAQU
C	1	2	2	IA
D	0	0	0	
E	11	12	132	QAORFWGTLIPE
F	12	13	156	LAQSPEOHUITGM
G	7	9	63	QAELPFIUG
H	3	5	15	VZFTA
I	11	13	143	OAULPRCZVQFEG
J	0	0	0	
K	0	0	0	
L	15	12	180	FBIOSEGPRWQT
M	3	4	12	OZFP
N	1	2	2	OR
O	15	13	195	AIMLNZQPEFWRU
P	10	11	110	OIFQAXZLEGM
Q	12	12	144	FEOAPBZQGILT
R	4	6	24	NZEILO
S	2	3	6	LFA
T	3	5	15	HEQFL
U	3	6	18	ZIOFGB
V	4	4	16	AHIV
W	3	4	12	OAEL
X	1	2	2	PZ
Y	0	0	0	
Z	8	10	80	MUROHQXPIA

BOZOL tried the crib word World from "Join the Army ..see the world" The crib failed but did show him some possibilities. LANAKI's caveat - Forget the tip, it is usually a red hering.

Try the A=e, Q=t, e=h, O=r, and I=n. Look for words offer, battles, death, country.

Message reads: "I offer neither pay nor quarters nor provisions. I offer hunger, thirst, forced marches, battles and death. Let him who loves our country in his heart and not with his lips only, follow me." Made famous by Girabaldi.

HOMEWORK LECTURE 3

Solve the following cipher problems.

Mv-1. From Martin Gardner.

8 5 1 8 5 1 9 1 1 9 9 1 3
1 6 1 2 5 1 1 2 1 6 8 1 2 5
2 0 9 3 3 1 5 4 5 2 0 8 1
2 0 9 2 2 5 1 4 5 2 2 5
1 8 1 9 5 5 1 4 2 5 6 1 5
1 8 5 1 3 1 2 5 2 5 2 5 1 5
2 1 3 1 1 4 2 1 1 9 5 9 2 0
9 1 4 2 5 1 5 2 1 1 8 3 1 5
1 2 2 1 1 3 1 4

1 3 1 1 8 2 0 9 1 4 7 1 1 8 4 1 4 5 1 8
8 5 1 4 4 5 1 8 1 9 1 5 1 4 2 2 9 1 2 1 2 5
1 4 1 5 1 8 2 0 8 3 1 1 8 1 5 1 2 9 1 4 1

Solve and reconstruct the cryptographic systems used.

Mv-2.

0 6 0 2 1 0 0 5 0 1 0 1 0 5 1 5 2 2 0 2 0 6 0 8 2
3 2 5 1 0 0 8 0 4 0 2 2 1 0 9 0 8 0 4 0 8 2 2 1 1
0 8 0 4 1 7 1 5 1 3 1 4 2 2 2 1 0 2 2 4 0 2 0 1 2
2 0 2 0 2 0 1 0 8 1 9 0 6 1 5 1 7 0 8 0 1 1 1 2 2
1 4 0 2 0 1 1 9 0 6 0 5 1 0 0 2 0 2 1 1 2 2 1 4 0
6 2 3 1 9 0 5 1 5 0 1 2 2 1 3 0 2 0 5 0 6 1 3 0 2
0 5 0 1 1 0 0 5 2 3 0 6 2 1 0 2 2 2 1 4 0 6 0 2 0
2 2 2 1 4 0 6 0 2 0 2 2 6 0 2 0 6 0 5 2 1 1 9 0 2
0 2 1 1 2 2 0 3 0 2 1 7 2 4 0 2 1 9 0 2 0 6 1 5 0
5 1 1 0 6 0 2 1 9 0 5 0 6 2 2 0 1 0 5 0 5 0 1 1 9
0 5 2 1 1 5 2 2 1 5 0 5 0 1 2 2 0 5 1 8 0 5 0 6 0
6 0 5 0 3

Mv-3.

5 3 2 4 1	5 4 5 3 2	2 4 4 3 2	5 1 2 4 3	2 4 2 3 1
5 4 4 4 5	4 5 3 2 5	1 4 3 4 4	1 4 1 5 2	1 4 1 1 5
4 3 4 5 3	5 2 1 2 3	3 5 1 2 5	1 1 4 2 1	5 3 3 3 4
5 3 2 4 4	2 3 1 5 4	5 4 5 2 4	4 3 2 4 1	4 4 4 3 2
1 2 5 3 2	4 4 3 4 4	2 4 1 5 4	4 4 5 2 4	4 3 3 5 2
1 5 3 3 3	1 3 1 4 4	4 1 5 4 5	4 4 5 1 4	3 2 5 1 5
2 3 2 4 1	5 5 2 2 4	4 3 1 5 3	1 3 3 1 3	3 1 4 5 5
3 2 4 1 3	4 5 2 1 2	5 3 3 5 2	2 4 3 4 1	3 1 2 4 5
4 4 5 2 3	3 4 4 3 3	2 2 3 3 3	5 3 3 4 5	2 1 3 5 2
4 4 4 4 4	4 5 3 2 1	5 1 3 1 5	5 2 2 4 4	3 1 5 3 1
2 4 5 1 1	3 1 4 2 4	4 4 3 3 4	3 1 5 2 2	3 5 2 4 2
5 3 5 2 1	3 3 1 3 3	1 2 3 1 2	1 3 1 4 3	3 4 5 3 3
1 2 1 3 4	4 4 1 2 4	4 3 3 3 1	2 1 4 3 2	2 4 3 3 3
1 3 2 4 5	1 2 2 5 3	5 1 2 5 3	2 3 3 5 1	2 5 1 1 4
4 4 1 5 4	5 4 1 4 3	2 4 4 4 2	4 1 3 4 5	1 5 2 2 1
2 5 1 4 5	1 2 1 3 2	4 4 5 3 2	1 2 5 1 4	4 1 5 1 3
1 4 2 5 2	4 2 4 4 5			

REFERENCES / RESOURCES

[ACA] ACA and You, "Handbook For Members of the American Cryptogram Association," ACA publications, 1995.

[ACA1] Anonymous, "The ACA and You - Handbook For Secure Communications", American Cryptogram Association, 1994.

[ANNA] Anonomous., "The History of the International Code.", Proceedings of the United States Naval Institute, 1934.

[B201] Barker, Wayne G., "Cryptanalysis of The Simple Substitution Cipher with Word Divisions," Course #201, Aegean Park Press, Laguna Hills, CA. 1982.

[BALL] Ball, W. W. R., Mathematical Recreations and Essays, London, 1928.

[BAR1] Barker, Wayne G., "Course No 201, Cryptanalysis of The Simple Substitution Cipher with Word Divisions," Aegean Park Press, Laguna Hills, CA. 1975.

[BARK] Barker, Wayne G., "Cryptanalysis of The Simple Substitution Cipher with Word Divisions," Aegean Park Press, Laguna Hills, CA. 1973.

[BARR] Barron, John, "'KGB: The Secret Work Of Soviet Agents," Bantom Books, New York, 1981.

[BAUD] Baudouin, Captain Roger, "Elements de Cryptographie," Paris, 1939.

[BLK] Blackstock, Paul W. and Frank L Schaf, Jr., "Intelligence, Espionage, Counterespionage and CovertOperations," Gale Research Co., Detroit, MI., 1978.

[BLUE] Bearden, Bill, "The Bluejacket's Manual, 20th ed., Annapolis: U.S. Naval Institute, 1978.

[BOSW] Bosworth, Bruce, "Codes, Ciphers and Computers: An Introduction to Information Security," Hayden Books, Rochelle Park, NJ, 1990.

[BP82] Beker, H., and Piper, F., " Cipher Systems, The Protection of Communications", John Wiley and Sons, NY, 1982.

[BRIT] Anonymous, "British Army Manual of Cryptography", HMF, 1914.

[BRYA] Bryan, William G., "Practical Cryptanalysis - Periodic Ciphers -Miscellaneous", Vol 5, American Cryptogram Association, 1967.

[CAR1] Carlisle, Sheila. Pattern Words: Three to Eight Letters in Length, Aegean Park Press, Laguna Hills, CA 92654, 1986.

[CAR2] Carlisle, Sheila. Pattern Words: Nine Letters in Length, Aegean Park Press, Laguna Hills, CA 92654, 1986.

[CCF] Foster, C. C., "Cryptanalysis for Microcomputers", Hayden Books, Rochelle Park, NJ, 1990.

[COUR] Courville, Joseph B., "Manual For Cryptanalysis Of The Columnar Double Transposition Cipher, by Courville Assoc., South Gate, CA, 1986.

[COVT] Anonymous, "Covert Intelligence Techniques Of the Soviet Union, Aegean Park Press, Laguna Hills, Ca. 1980.

[CULL] Cullen, Charles G., "Matrices and Linear Transformations," 2nd Ed., Dover Advanced Mathematics Books, NY, 1972.

[DAGA] D'agapeyeff, Alexander, "Codes and Ciphers," Oxford University Press, London, 1974.

[DAN] Daniel, Robert E., "Elementary Cryptanalysis: Cryptography For Fun," Cryptiquotes, Seattle, WA., 1979.

[DAVI] Da Vinci, "Solving Russian Cryptograms", The Cryptogram, September-October, Vol XLII, No 5. 1976.

[DEAU] Bacon, Sir Francis, "De Augmentis Scientiarum," tr. by Gilbert Watts, (1640) or tr. by Ellis, Spedding, and Heath (1857,1870).

[DOW] Dow, Don. L., "Crypto-Mania, Version 3.0", Box 1111, Nashua, NH. 03061-1111, (603) 880-6472, Cost $15 for registered version and available as shareware under CRYPTM.zip on CIS or zipnet.

[ELCY] Gaines, Helen Fouche, Cryptanalysis, Dover, New York, 1956.

[ENIG] Tyner, Clarence E. Jr., and Randall K. Nichols, "ENIGMA95 - A Simulation of Enhanced Enigma Cipher Machine on A Standard Personal Computer," for publication, November, 1995.

[EPST] Epstein, Sam and Beryl, "The First Book of Codes and Ciphers," Ambassador Books, Toronto, Canada, 1956.

[FREB] Friedman, William F., "Cryptology," The Encyclopedia Britannica, all editions since 1929. A classic article by the greatest cryptanalyst.

[FR1] Friedman, William F. and Callimahos, Lambros D., Military Cryptanalytics Part I - Volume 1, Aegean Park Press, Laguna Hills, CA, 1985.

[FR2] Friedman, William F. and Callimahos, Lambros D., Military Cryptanalytics Part I - Volume 2, Aegean Park Press, Laguna Hills, CA, 1985.

[FR3] Friedman, William F. and Callimahos, Lambros D., Military Cryptanalytics Part III, Aegean Park Press, Laguna Hills, CA, 1995.

[FR4] Friedman, William F. and Callimahos, Lambros D., Military Cryptanalytics Part IV, Aegean Park Press, Laguna Hills, CA, 1995.

[FR5] Friedman, William F. Military Cryptanalysis - Part I, Aegean Park Press, Laguna Hills, CA, 1980.

[FR6] Friedman, William F. Military Cryptanalysis - Part II, Aegean Park Press, Laguna Hills, CA, 1980.

[FRE] Friedman, William F. , "Elements of Cryptanalysis," Aegean Park Press, Laguna Hills, CA, 1976.

[FREA] Friedman, William F. , "Advanced Military Cryptography," Aegean Park Press, Laguna Hills, CA, 1976.

[FRAA] Friedman, William F. , "American Army Field Codes in The American Expeditionary Forces During the First World War, USA 1939.

[FR22] Friedman, William F., The Index of Coincidence and Its Applications In Cryptography, Publication 22, The Riverbank Publications, Aegean Park Press, Laguna Hills, CA, 1979.

[FRS] Friedman, William F. and Elizabeth S., "The Shakespearean Ciphers Examined," Cambridge University Press, London, 1957.

[GIVI] Givierge, General Marcel, " Course In Cryptography," Aegean Park Press, Laguna Hills, CA, 1978. Also, M. Givierge, "Cours de Cryptographie," Berger-Levrault, Paris, 1925.

[GODD] Goddard, Eldridge and Thelma, "Cryptodyct," Marion, Iowa, 1976

[GORD] Gordon, Cyrus H., " Forgotten Scripts: Their Ongoing Discovery and Decipherment," Basic Books, New York, 1982.

[HA] Hahn, Karl, " Frequency of Letters", English Letter Usage Statistics using as a sample, "A Tale of Two Cities" by Charles Dickens, Usenet SCI.Crypt, 4 Aug 1994.

[HEMP] Hempfner, Philip and Tania, "Pattern Word List For Divided and Undivided Cryptograms," unpublished manuscript, 1984.

[HILL] Hill, Lester, S., "Cryptography in an Algebraic Alphabet", The American Mathematical Monthly, June-July 1929.

[HIS1] Barker, Wayne G., "History of Codes and Ciphers in the U.S. Prior to World War I," Aegean Park Press, Laguna Hills, CA, 1978.

[HITT] Hitt, Parker, Col. " Manual for the Solution of Military Ciphers," Aegean Park Press, Laguna Hills, CA, 1976.

[IBM1] IBM Research Reports, Vol 7., No 4, IBM Research, Yorktown Heights, N.Y., 1971.

[INDE] PHOENIX, Index to the Cryptogram: 1932-1993, ACA, 1994.

[KAHN] Kahn, David, "The Codebreakers", Macmillian Publishing Co. , 1967.

[KAH1] Kahn, David, "Kahn On Codes - Secrets of the New Cryptology," MacMillan Co., New York, 1983.

[KOBL] Koblitz, Neal, " A Course in Number Theory and Cryptography, 2nd Ed, Springer-Verlag, New York, 1994.

[KULL] Kullback, Solomon, Statistical Methods in Cryptanalysis, Agean Park Press, Laguna Hills, Ca. 1976

[LAFF] Laffin, John, "Codes and Ciphers: Secret Writing Through The Ages," Abelard-Schuman, London, 1973.

[LANG] Langie, Andre, "Cryptography," translated from French by J.C.H. Macbeth, Constable and Co., London, 1922.

[LEWY] Lewy, Guenter, "America In Vietnam", Oxford University Press, New York, 1978.

[LYNC] Lynch, Frederick D., "Pattern Word List, Vol 1.," Aegean Park Press, Laguna Hills, CA, 1977.

[LYSI] Lysing, Henry, aka John Leonard Nanovic, "Secret Writing," David Kemp Co., NY 1936.

[MANS] Mansfield, Louis C. S., "The Solution of Codes and Ciphers", Alexander Maclehose & Co., London, 1936.

[MARO] Marotta, Michael, E. "The Code Book - All About Unbreakable Codes and How To Use Them," Loompanics Unlimited, 1979. [This is terrible book. Badly written, without proper authority, unprofessional, and prejudicial too boot. And, it has one of the better illustrations of the Soviet one-time pad with example, with three errors in cipher text, that I have corrected for the author.]

[MART] Martin, James, "Security, Accuracy and Privacy in Computer Systems," Prentice Hall, Englewood Cliffs, N.J., 1973.

[MILL] Millikin, Donald, " Elementary Cryptography ", NYU Bookstore, NY, 1943.

[MYER] Myer, Albert, "Manual of Signals," Washington, D.C., USGPO, 1879.

[MM] Meyer, C. H., and Matyas, S. M., " CRYPTOGRAPHY - A New Dimension in Computer Data Security, " Wiley Interscience, New York, 1982.

[NIBL] Niblack, A. P., "Proposed Day, Night and Fog Signals for the Navy with Brief Description of the Ardois Hight System," In Proceedings of the United States Naval Institute, Annapolis: U. S. Naval Institute, 1891.

[NIC1] Nichols, Randall K., "Xeno Data on 10 Different Languages," ACA-L, August 18, 1995.

[NIC2] Nichols, Randall K., "Chinese Cryptography Parts 1-3," ACA-L, August 24, 1995.

[NIC3] Nichols, Randall K., "German Reduction Ciphers Parts 1-4," ACA-L, September 15, 1995.

[NIC4] Nichols, Randall K., "Russian Cryptography Parts 1-3," ACA-L, September 05, 1995.

[NIC5] Nichols, Randall K., "A Tribute to William F. Friedman", NCSA FORUM, August 20, 1995.

[NIC6] Nichols, Randall K., "Wallis and Rossignol," NCSA FORUM, September 25, 1995.

[NIC7] Nichols, Randall K., "Arabic Contributions to Cryptography,", in The Cryptogram, ND95, ACA, 1995.

[NIC8] Nichols, Randall K., "U.S. Coast Guard Shuts Down Morse Code System," The Cryptogram, SO95, ACA publications, 1995.

[NIC9] Nichols, Randall K., "PCP Cipher," NCSA FORUM, March 10, 1995.

[OP20] "Course in Cryptanalysis," OP-20-G', Navy Department, Office of Chief of Naval Operations, Washington, 1941.

[PIER] Pierce, Clayton C., "Cryptoprivacy", 325 Carol Drive, Ventura, Ca. 93003.

[RAJ1] "Pattern and Non Pattern Words of 2 to 6 Letters," G & C. Merriam Co., Norman, OK. 1977.

[RAJ2] "Pattern and Non Pattern Words of 7 to 8 Letters," G & C. Merriam Co., Norman, OK. 1980.

[RAJ3] "Pattern and Non Pattern Words of 9 to 10 Letters," G & C. Merriam Co., Norman, OK. 1981.

[RAJ4] "Non Pattern Words of 3 to 14 Letters," RAJA Books, Norman, OK. 1982.

[RAJ5] "Pattern and Non Pattern Words of 10 Letters," G & C. Merriam Co., Norman, OK. 1982.

[RHEE] Rhee, Man Young, "Cryptography and Secure Communications," McGraw Hill Co, 1994

[ROBO] NYPHO, The Cryptogram, Dec 1940, Feb, 1941.

[SACC] Sacco, Generale Luigi, " Manuale di Crittografia", 3rd ed., Rome, 1947.

[SCHN] Schneier, Bruce, "Applied Cryptography: Protocols, Algorithms, and Source Code C," John Wiley and Sons, 1994.

[SCHW] Schwab, Charles, "The Equalizer," Charles Schwab, San Francisco, 1994.

[SHAN] Shannon, C. E., "The Communication Theory of Secrecy Systems," Bell System Technical Journal, Vol 28 (October 1949).

[SIG1] "International Code Of Signals For Visual, Sound, and Radio Communications," Defense Mapping Agency, Hydrographic/Topohraphic Center, United States Ed. Revised 1981

[SIG2] "International Code Of Signals For Visual, Sound, and Radio Communications," U. S. Naval Oceanographic Office, United States Ed., Pub. 102, 1969.

[SINK] Sinkov, Abraham, "Elementary Cryptanalysis", The Mathematical Association of America, NYU, 1966.

[SISI] Pierce, C.C., "Cryptoprivacy," Author/Publisher, Ventura Ca., 1995. (XOR Logic and SIGTOT teleprinters)

[SMIT] Smith, Laurence D., "Cryptography, the Science of Secret Writing," Dover, NY, 1943.

[SOLZ] Solzhenitsyn, Aleksandr I. , "The Gulag Archipelago I-III, " Harper and Row, New York, N.Y., 1975.

[STIN] Stinson, D. R., "Cryptography, Theory and Practice," CRC Press, London, 1995.

[SUVO] Suvorov, Viktor "Inside Soviet Military Intelligence," Berkley Press, New York, 1985.

[TERR] Terrett, D., "The Signal Corps: The Emergency (to December 1941); G. R. Thompson, et. al, The Test(December 1941 - July 1943); D. Harris and G. Thompson, The Outcome;(Mid 1943 to 1945), Department of the Army, Office of the Chief of Military History, USGPO, Washington,1956 -1966.

[TILD] Glover, D. Beaird, Secret Ciphers of The 1876 Presidential Election, Aegean Park Press, Laguna Hills, Ca. 1991.

[TRAD] U. S. Army Military History Institute, "Traditions of The Signal Corps., Washington, D.C., USGPO, 1959.

[TRIB] Anonymous, New York Tribune, Extra No. 44, "The Cipher Dispatches, New York, 1879.

[TRIT] Trithemius:Paul Chacornac, "Grandeur et Adversite de Jean Tritheme ,Paris: Editions Traditionelles, 1963.

[TUCK] Harris, Frances A., "Solving Simple Substitution Ciphers," ACA, 1959.

[TUCM] Tuckerman, B., "A Study of The Vigenere-Vernam Single and Multiple Loop Enciphering Systems," IBM Report RC2879, Thomas J. Watson Research Center, Yorktown Heights, N.Y. 1970.

[VERN] Vernam, A. S., "Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications," J. of the IEEE, Vol 45, 109-115 (1926).

[VOGE] Vogel, Donald S., "Inside a KGB Cipher," Cryptologia, Vol XIV, Number 1, January 1990.

[WAL1] Wallace, Robert W. Pattern Words: Ten Letters and Eleven Letters in Length, Aegean Park Press, Laguna Hills, CA 92654, 1993.

[WAL2] Wallace, Robert W. Pattern Words: Twelve Letters and Greater in Length, Aegean Park Press, Laguna Hills, CA 92654, 1993.

[WATS] Watson, R. W. Seton-, ed, "The Abbot Trithemius," in Tudor Studies, Longmans and Green, London, 1924.

[WEL] Welsh, Dominic, "Codes and Cryptography," Oxford Science Publications, New York, 1993.

[WOLE] Wolfe, Ramond W., "Secret Writing," McGraw Hill Books, NY, 1970.

[WOLF] Wolfe, Jack M., " A First Course in Cryptanalysis," Brooklin College Press, NY, 1943.

[WRIX] Wrixon, Fred B. "Codes, Ciphers and Secret Languages," Crown Publishers, New York, 1990.

[YARD] Yardley, Herbert, O., "The American Black Chamber," Bobbs-Merrill, NY, 1931.

[ZIM] Zim, Herbert S., "Codes and Secret Writing." William Morrow Co., New York, 1948.