CLASSICAL CRYPTOGRAPHY COURSE
BY LANAKI
December 05, 1995
Revision 0

LECTURE 4
SUBSTITUTION WITH VARIANTS PART III
MULTILITERAL SUBSTITUTION

SUMMARY

Welcome back from the Thanksgiving holiday break. The good news is that this lecture will come to you about Christmas, therefore, no homework. The not so good news is that this concluding Lecture 4 on Substitution with Variants covers some difficult material of wide practically in the field.

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

MULTILITERAL SUBSTITUTION WITH MULTIPLE-EQUIVALENT CIPHER ALPHABETS - aka "MONOALPHABETIC SUBSTITUTION WITH VARIANTS"

Each English letter in plain text has a characteristic frequency which affords definite clues in the solution of simple monoalphabetic ciphers. Associations which individual letters form in combining to make up words, and the peculiarities which certain of them manifest in plain text, afford further direct clues by means of which ordinary monoalphabetic substitution encipherments of such plain text may be readily solved. [FR1]

Cryptographers have devised methods for disguising, suppressing, or eliminating the foregoing characteristics in the cryptograms produced by methods described in Lectures 1-3. One category of methods call "variants or variant values" is that in which the letters of the plain component of a cipher alphabet are assigned two or more cipher equivalents.

Systems involving variants are generally multiliteral. In such systems, there are a large number of equivalents made available by combinations and permutations of a limited number of elements, each letter of the plain text may be represented by several multiliteral cipher equivalents which may be selected at random. For example, if 3-letter combinations are employed as multiliteral equivalents, there are 26**3 or 17,576 available equivalents for the 26 letters of the plain text.

They may be assigned in equal numbers of different equivalents for the 26 letters, in which case each letter would be representable by 676 different 3 letter equivalents or they be assigned on some other basis, for example proportionately to the relative frequencies of the plain text letters. [FR1]

The primary object of substitution with variants is again to provide several values which may be employed at random in a simple substitution of cipher equivalents for the plain text letters.

As a slight diversion, the reader may ask about uniliteral substitution with variants. It is but not very practical. Note the following cipher alphabet constructed in French by Captain Roger Baudouin in reference [BAUD]:

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

(Note that the Captain was not an ACA member. The H=H combination is not allowed.)

Baudouin proposed that the J and Y plain be replaced by I plain and K plain by C plain or Q plain and W plain by VV plain. Four cipher letters would be available as variants for the high-frequency plain text letters in French.

Mixed alphabets formed by including all repeated letters of the key word or key phrase in the cipher component were common in Edgar Allen Poe's day but are impractical because they are ambiguous, making decipherment difficult; for example:

Enciphering Alphabet:

```
Plain : 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
Cipher: N O W I S T H E T I M E F O R A L L G O O D M E N T
```

Inverse form for deciphering

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

The average cipher clerk would have difficulty in decrypting a cipher group such as TOOET, each letter having 3 or more equivalents, from which plain text fragments (n)inth, ft thi(s), it thi, etc. can be formed on decipherment. [FR1]

THEORETICAL DISTINCTIONS

In simple or single-equivalent monoalphabetic substitution with variants, two points are evident:

1) the same letter of the plain text is invariable represented by but one and always the same character or cipher unit of the cryptogram.

2) The same character or cipher unit of the cryptogram invariably represents one and always the same letter of the plain text.

In multiliteral - equivalent monoalphabetic substitution with variants, two points are also evident:

1) the same letter of the plain text may be represented by one or more different characters or cipher units of the cryptogram. But,

2) The same character or cipher unit of the cryptogram nevertheless invariably represents one and always the same letter of the plain text.

SIMPLE TYPES OF CIPHER ALPHABETS WITH VARIANTS

Figure 4-1

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

Figure 4-2

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

Figure 4-3

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

Figure 4-4

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

Figure 4-5

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

Figure 4-6

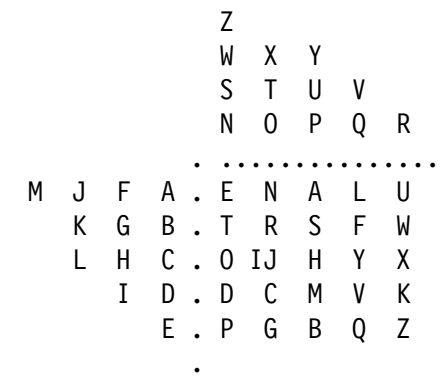


Figure 4-7

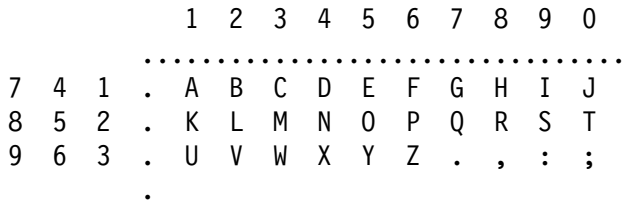


Figure 4-8

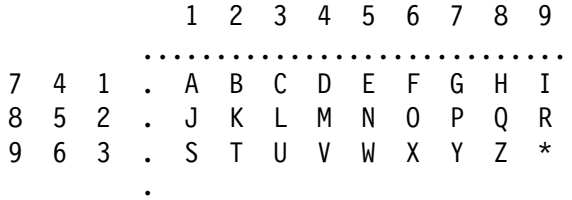


Figure 4-9

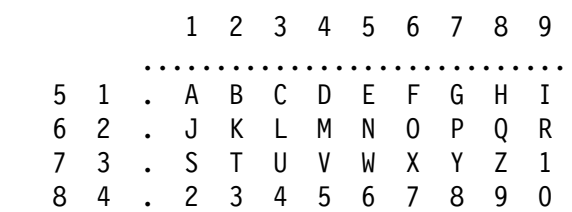
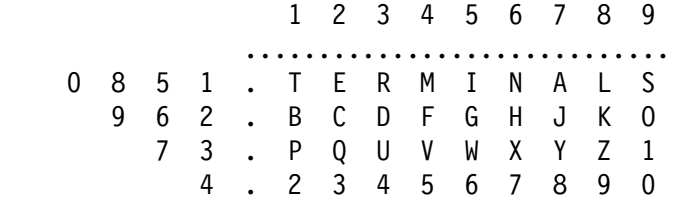


Figure 4-10



The matrices in Figures 4 -1 to 4-10 represent some of the simpler means for accomplishing monoalphabetic substitution with variants. The matrices are extensions of the basic ideas of multiliteral substitution presented in Lecture 3.

The variant equivalents for any plain text letter may be chosen at will; thus, in Figure 4-1, e= 10, 15, 60, or 65; in Figure 4-2, e= AU, AZ, FU, FZ, LU or LZ.

Encipherment by means of matrices shown in Figures 4-2, 4-3, 4-6 is commutative. The coordinates may be read row by column or visa versa. There is no cryptographic ambiguity. The remaining matrices are noncommutative. The general convention is to read row by column.

In Figures 4-5 and 4-6, the letters in the square have been inscribed in such a manner that, coupled with the particular arrangement of the row and column coordinates, the number of variants available for each plain text letter is roughly proportional to the frequencies of the letters in the plain text. Figure 35 incorporates a keyword on top of this idea. [FR1]

HOMOPHONIC

The Homophonic Cipher is a simple variant system. It is a 4-level (alphabets) dinome cipher. Consider Figure 4-11.

Figure 4-11

A	B	C	D	E	F	G	H	IJ	K	L	M	N
08	09	10	11	12	13	14	15	16	17	18	19	20
35	36	37	38	39	40	41	42	43	44	45	46	47
68	69	70	71	72	73	74	75	51	52	53	54	55
87	88	89	90	91	92	93	94	95	96	97	98	99

O	P	Q	R	S	T	U	V	W	X	Y	Z
21	22	23	24	25	01	02	03	04	05	06	07
48	49	50	26	27	28	29	30	31	32	33	34
56	57	58	59	60	61	62	63	64	65	66	67
00	76	77	78	79	80	81	82	83	84	85	86

The keyword TRIP is found by inspecting dinomes 01, 26, 51, and 76. (The lowest number in each of the four sequences.) [FR1] [FR5]

The Russians added an interesting gimmick called the Disruption Area. Consider Figure 4-12 and note the slashes under U - X for the fourth level of dinomes. The famous VIC cipher used this feature very effectively. [NIC4]

Figure 4-12

A	B	C	D	E	F	G	H	I	J	K	L	M	N
14	15	16	17	18	19	20	21	22	23	24	25	26	01
27	28	29	30	31	32	33	34	35	36	37	38	39	40
58	59	60	61	62	63	64	65	66	67	68	69	70	71
81	82	83	84	85	86	87	88	89	90	91	92	93	94

O	P	Q	R	S	T	U	V	W	X	Y	Z
02	03	04	05	06	07	08	09	10	11	12	13
41	42	43	44	45	46	47	48	49	50	51	52
72	73	74	75	76	77	78	53	54	55	56	57
95	96	97	98	99	00	//////////////				79	80

The keyword NAVY is represented by dinomes 01, 27, 53, and 79.

Security for Homophonic systems is greatly improved if the dinomes and the four sequences are assigned randomly. However, the easy mnemonic feature of the keyworded four sequences is lost.

The Mexican Cipher device is a Homophonic consisting of five concentric disks, the outer disk bearing 26 letters and the other four bearing sequences 01-26, 27-52, 53-78, 79-00. The cipher disk enhances frequent key changes. Figure 4-12 shows the matrix without the disruption area. [FR5] [NIC4]

HOMOPHONIC CRYPTANALYSIS

Lets solve the following cryptogram.

```
68321  09022  48057  65111  88648  42036  45235  09144
05764  22684  00225  57003  97357  14074  82524  40768
51058  93074  92188  47264  09328  04255  06186  79882
85144  45886  32574  55136  56019  45722  76844  68350
45219  71649  90528  65106  11886  44044  89669  70553
18491  06985  48579  33684  50957  70612  09795  29148
56109  08546  62062  65509  32800  32568  97216  44282
34031  84989  68564  53789  12530  77401  68494  38544
11368  87616  56905  20710  58864  67472  22490  09136
62851  24551  35180  14230  50886  44084  06231  12876
05579  58980  29503  99713  32720  36433  82689  04516
52263  21175  06445  72255  68951  86957  76095  67215
53049  08567  9730
```

Assuming we did not know that the above cryptogram was a HOMOPHONIC, we might may a preliminary analysis to see if we are dealing with a cipher or a code. We will cover code systems later in the course, but a few introductory remarks might be in order. The five letter groups could indicate either a cipher or a code.

If the cryptogram contains an even number of digits, as for example 494 in the previous message, this leaves open the possibility that the message is a cipher containing 247 pairs of digits; were the number of digits an exact odd multiple of five, such as 125, 135, etc., the possibility that the cryptogram is in code of the 5-figure group type must be considered.

We next study the message repetitions and what their characteristics are. If the cipher text is of 5-figure code type, then such repetitions as appear should generally be in whole groups of five digits, and they should be visible in the text just as the message stands, unless the code message has been superenciphered. If the cryptogram is a cipher, then repetitions should extend beyond the 5-digit groupings; if they conform to any definite at all they should for the most part contain even numbers of digits since each letter is probably represented by a pair (dinome) of digits.

We start with 4-part frequency distribution. We next assume a 25 character alphabet from 01-00. This is the common scheme of drawing up the alphabets. Breaking the text into dinomes (2-digit) pairs yields:

01 ///	26 ///	51 /////	76 //////
02	27	52 /////	77 /
03 ////	28 /	53 ///	78
04 /	29 /	54	79 /
05 /////	30 ///	55 ////	80 ///
06 //////	31	56 /////	81
07 ///	32 //////	57 //////	82 ////
08	33 /	58 //	83 /
09 ////	34 /	59	84 //////
10 ////	35 //	60	85 //////
11 /////	36 /////	61	86 ///
12 ///	37 /	62 //	87
13 /	38	63	88 ////
14 /	39 /	64 //////	89 /////
15 /	40 ///	65	90 //////
16 ///	41	66 /	91 ///
17	42 ////	67 //	92 /
18 //////	43 /	68 ///////	93 /
19	44 //////	69 //	94 /
20 /	45 //////	70 /	95 ///
21 //	46 ///	71 /	96
22 /////	47	72 ////	97 //////
23 //	48 ///	73	98 /
24	49 /////	74 ////	99
25 /	50 /////	75 /	00 //

What we have before us are four simple, monoalphabetic frequency distributions similar to those involved in a monoalphabetic substitution cipher using standard cipher alphabets. The next step is to fit the distribution to the normal. Since I=J for the 25 letter alphabet, we find that the Keyword is JUNE and the following alphabets result:

01	I-J	26	U	51	N	76	E
02	K	27	V	52	O	77	F
03	L	28	W	53	P	78	G
04	M	29	X	54	Q	79	H
05	N	30	Y	55	R	80	IJ
06	O	31	Z	56	S	81	K
07	P	32	A	57	T	82	L
08	Q	33	B	58	U	83	M
09	R	34	C	59	V	84	N
10	S	35	D	60	W	85	O
11	T	36	E	61	X	86	P
12	U	37	F	62	Y	87	Q
13	V	38	G	63	Z	88	R
14	W	39	H	64	A	89	S
15	X	40	IJ	65	B	90	T
16	Y	41	K	66	C	91	U
17	Z	42	L	67	D	92	V
18	A	43	M	68	E	93	W
19	B	44	N	69	F	94	X
20	C	45	O	70	G	95	Y
21	D	46	P	71	H	96	Z
22	E	47	Q	72	IJ	97	A
23	F	48	R	73	K	98	B
24	G	49	S	74	L	99	C
25	H	50	T	75	M	00	D

The first groups of the cryptogram decipher as follows:

```
68 32 10 90 22 48 05 76 51 11 88 64 84 20 36 45 23
e  a  s  t  e  r  n  e  n  t  r  a  n  c  e  o  f
```

If a 26-element alphabet were used only the distribution analysis would have been changed to be on a basis of 26, the process of fitting the distribution to the normal would be the same.

PLAIN COMPONENT COMPLETION METHOD

Suppose we know that two correspondents have been using the same variant system as in the previous Homophonic. The message intercepted is:

48226 88423 52099 93604 76059 05651 36683 52267 97114 54466 76

A variation of the plain-component completion method can be used to crack the new message. We copy the message into dinomes and separate by levels.

```
48 22 68 84 23 52 09 99 36 04 76 05 90 56 51 36 68 35 22 67 97  11 45 44 66 76
-------------------------------------------------------------------------------
2   1  3  4  1  3  1  4  2  1  4  1  4  3  3  2  3  2  1  3  4   1  2  2  3  4
```

Levels

(1) 22 23 09 04 05 22 11
(2) 48 36 36 35 45 44
(3) 68 52 56 51 68 67 66
(4) 84 99 76 90 97 76

These dinomes are converted into terms of plain component by setting each of the cipher sequences against the plain component at an arbitrary point of coincidence, such as the following:

```
A   B   C   D   E   F   G   H   IJ  K   L   M   N
01  02  03  04  05  06  07  08  09  10  11  12  13
26  27  28  29  30  31  32  33  34  35  36  37  38
51  52  53  54  55  56  57  58  59  60  61  62  63
76  77  78  79  80  81  82  83  84  85  86  87  88

O   P   Q   R   S   T   U   V   W   X   Y   Z
14  15  16  17  18  19  20  21  22  23  24  25
39  40  41  42  43  44  45  46  47  48  49  50
64  65  66  67  68  69  70  71  72  73  74  75
89  90  91  92  93  94  95  96  97  98  99  00
```

So: Levels

(1) 22=W; 23=X; 09=I; 04=D; 05=E; 22=W; 11=L
(2) 48=X; 36=L; 36=L; 35=K; 45=U; 44=T
(3) 68=S; 52=B; 56=F; 51=A; 68=S; 67=R; 66=Q
(4) 84=I; 99=Y; 76=A; 90=P; 97=W; 76=A

This method works because both the plain component (A,B..) and the cipher component (01, 02..) are known sequences.

The plain-component sequence is completed on the letters of the four levels by Caesar Rundown, as follows:

Level 1	Level 2	Level 3	Level 4
WXIDEWL	XLLKUT	SBFASRQ	IYAPWA
XYKEFXM	YMMLVU	TCGBTSR	KZBQXB
YZLFGYN	ZNNMWV	UDHCUTS	LACRYC
ZAMGHZO	AOONXW	VEIDVUT	MBDSZD
ABNHIAP	BPPOYX	WFKEWVU	NCETAE
BCOIKBQ	CQQPZY	XGLFXWV	ODFUBF
CDPKLCR	DRRQAZ	YHMGYXW	PEGVCG
DEQLMDS	ESSRBA	ZINHZYZ	QFHWDH
EFRMNET	FTTSCB	AKOIAZY	RGIXEI
FGSNOFU	GUUTDC	BLPKBAZ	SHKYFK
GHTOPGV	HVVUED	CMQLCBA	TILZGL
HIUPQHW	IWWVFE	DNRMDCB	UKMAHM
IKVQRIX	KXXWGF	EOSNEDC	VLNBIN
KLWRSKY	LYYXHG	FPTOFED	WMOCKO
LMXSTLZ	MZZYIH	GQUPGFE	XNPDLP
MNYTUMA	NAAZKI	HRVQHGF	YOQEMQ
NOZUVNB	OBBALK	ISWRIHG	ZPRFNR
OPAVWOC	PCCBML	KTXSKIH	AQSGOS
PQBWXPD	QDDCNM	LUYTLKI	BRTHPT
QRCXYQE	REEDON	MVZUMLK	CSUIQU
RSDYZRF	SFFEPO	NWAVNML	DTVKRV
STEZASG	TGGFQP	OXBWONM	EUWLSW
TUFABTH	UHHGRQ	PYCXPON	FVXMTX
UVGBCUI	VIIHSR	QZDYQPO	GWYNUY
VWHCDVK	WKKITS	RAEZRQP	HXZOVZ

The generatrices with the best assortment of high frequency letters for the four levels are:

Level 1	Level 2	Level 3	Level 4
EFRMNET	REEDON	EOSNEDC	NCETAE

Arranging the letters of these generatrices in order of appearance of their dinome equivalents, according to levels we have:

```
48 22 68 84 23 52 09 99 36 04 76 05 90 56 51 36 68 35 22 67 97
   E        F     R        M     N                    E
 R                     E                   E      D
      E        O                      S  N      E       D
         N            C        E     T                      A
```

The plain text reads "Reinforcements needed a[t once]". Looking at the equivalents 01,26, 51, 76 we reveal the keyword JUNE.

In evaluating generatrices, the sum of the arithmetic frequencies of the letters in each row may be used as an indication of the relative "goodness". A statistically better procedure uses the logarithm of the probabilities of the plain text letters forming the generatrices. See [FR2]

The Homophonic is a popular cipher and has been discussed in several issues of The Cryptogram as well as LEDGES' NOVICE NOTES. See references [HOM1 -HOM6] and [LEDG].

For our computer bugs, TATTERS Homophonic solver is very easy to use and available on the Crypto Drop Box.

MORE COMPLICATED TYPES OF CIPHER ALPHABETS WITH VARIANTS

GRANDPRE

Consider the cipher matrices shown in figures 4-11 to 4-13. These are called frequential matrices, since the number of cipher values available for any given plain text letter closely approximates its relative plain text frequency.

Figure 4-11

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

(676 - cell matrix)

In figure 4-11, the number of occurrences of a particular letter within the matrix is proportional to the frequency in plain text; the letters are inscribe in random manner, in order to enhance the security of the system.

Figure 4-12

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

In figure 4-12, the same idea as 4-11 is presented in reduced form from 26 x 26 to 10 x 10. The letters have been inscribed by a simple diagonal route, from left to right, within the square, and the coordinates scrambled by means of a key word or key number.

Figure 4-13
"Grandpre"

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

Figure 4-13 illustrates the famous Grandpre Cipher; in this square ten words are inscribed containing all the letters of the alphabet and linked by a column keyword ("equivalent") as a mnemonic for inscription of the row words. ACA literature also covers this cipher. See references [LEDG] and [GRA1 - 3] for solution hints for the Grandpre cipher.

SACCO

General Luigi Sacco proposed a frequential-type system that uses both enciphering and deciphering matrices. The inscribed dinomes were completely disarranged by applying a double transposition to suppress the relationships between letters. References [SACC] and [FR1] both give a good description of the process. The number of variant values in this system are reflective of the Italian language.

BACONIAN

The Baconian ciphers found in the Cryptogram are a variant system. The "a" elements may be represented by any one of 20 consonants as variants, while the "b" elements may be represented by any one of 6 vowels; or the letters A-M may be used to represent the "a" elements and the letters N-Z for the "b" elements; digits may be used for either the "a" or "b" elements, either on the basis of first five or last five digits, or odd versus even digits, or the first 10 consonants (B-M) and the last 10 consonants (N-Z)

SUMMING-TRINOME

Friedman describes a complex variant known as the summing-trinome system. Each plain text letter is assigned a value from 1-26; this value is expressed as a trinome, the digits of which sum to the designated value of the letter. The letter assigned the value of 4 may be represented by any of 15 permutations and combinations. Friedman discusses further ways of complication including disarrangement, addition of punctuation and nulls. See [FR1] pages 109-110. Note the inverted normal distribution representation of this cipher.

ANALYSIS OF A SIMPLE VARIANT EXAMPLE

The following cryptogram is available for study:

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

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

Note the total absence of A, E, I, O, U, and Y. Remarkable and definitely nonrandom event. Since a uniliteral substitution alphabet with 6 letters missing is highly unlikely, the next guess is we are dealing with a multiliteral substitution. Closer inspection shows that ten consonants are initials (B D G J L N Q S V X) and the remaining ten consonants are used as terminals (C F H K M P R T W Z). This implies both bipartite and biliteral character.

We construct a digraphic distribution:

```
     C  F  H  K  M  P  R  T  W  Z
   ..............................
B . 3  1  1  1  1  2  2  1  2  1 .
D . 4  1  3  3  1  1  1  3  4  2 .
G . 2  2  2     3        1     1 .
J . 1  1  1  1  1  1  2  1  1  1 .
L . 1  4     4  3  4  5  3  3  4 .
N . 4  1  4  3  1  1  1  2  3  3 .
Q .    2     2  1  1  1     1    .
S . 1  2  2     2  1              1 .
V . 1  4  1  3  4  4  4  3  4  3 .
X .    1     1  2  1  1     2    .
   ..............................
```

We assume the use of a small enciphering matrix with variants for rows and columns. We assume that the various possible cipher variants are of approximately equal frequency; the column indicators pair equally often with the row indicators of the enciphering matrix. We look for similar row profiles and column profiles. We match first the rows and then the columns.

Row L and V distributions have pronounced similarities. They are "heavy" in their frequency distributions in the same places. So are rows D and N. They have homologous attributes in appearance.

```
       C  F  H  K  M  P  R  T  W  Z
L    . 1  4     4  3  4  5  3  3  4 .
V    . 1  4  1  3  4  4  4  3  4  3 .

D    . 4  1  3  3  1  1  1  3  4  2 .
N    . 4  1  4  3  1  1  1  2  3  3 .
```

Finding the next rows are not obvious. We use a "goodness of match" procedure to equate interchangeable variants. We calculate the cross-product sums for each trial. The next heavy row is G. We test G against the remaining rows.

```
G    . 2  2  2     3        1     1 .
B    . 3  1  1  1  1  2  2  1  2  1 .
G*B +  6  2  2     3        1     1   = 15
```

We compare the balance of rows

```
G*B +      6  2  2     3        1     1   = 15
G*J +      2  2  2     3        1     1   = 11
G*Q +         4        3                  =  7
G*S +      2  4  4     6              1   = 17 !
G*X +         2        6                  =  8
```

The results are most probably match G and S.

The next heaviest row is B. Testing against the remaining three rows we have:

```
B*J +      3  1  1  1  1  2  4  1  2  1   = 17
B*Q +         2     2  1  2  2     2  1   = 12
B*X +         1     1  2  2  2     4      = 12
```

The correct pairings are B with J and Q with X. Since we have not found more than two rows for any one set of interchangeable values the original matrix has only five rows.

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

Values represent the sums of the combined rows. We apply the same process to matching columns. C and H are a matched pair. F with M and P with R. We use the cross product sums for the balance of the columns.

```
K*T+:  4  35  - 42  - =  81
K*W+:  4  49  - 49  9 = 113
K*Z+:  4  35  - 49  - =  88
T*W+:  6  35  - 42  - =  83
T*Z+:  4  25  2 42  - =  73
W*Z+:  6  35  - 49  - =  90

     Combinations:

KT, WZ:   81 +  90 = 171
KW, TZ:   113 + 73 = 186
KZ, TW:   88  + 83 = 171
```

We would expect that the proper pairings are K with W and T with Z.

```
          C  F  K  P  T
          H  M  W  R  Z
        ...................
B  J .  6  4  5  7  4  .   PHI(p) = 1962
D  N . 16  4 14  4 10  .   PHI(r) = 1132
G  S .  7  9  -  1  3  .   PHI(o) = 1670
L  V .  3 15 14 17  13 .
Q  X .  -  6  6  -  4  .
        ...................
```

We convert the multiliteral text to uniliteral equivalents using an arbitrary square for reduction to plain text.

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

The converted cryptogram is solved via the principals in Lectures 2 and 3. The beginning of the message reads Weather forecast. The original keying matrix is recovered with a keyword of ATMOSPHERIC.

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

The method of matching rows and columns applies equally well for all the matrices shown previously. It is key to start with the best rows and columns from not only heaviness standpoint but the distinctive crests and troughs. A second key is the low frequency letters. No variant system can adequately disguise low frequency letters and they will have the same frequency in the cipher text. Friedman describes a more general solution to variant analysis. [FRE1, p119 ff]

Chapter 10 of reference [FRE1] covers the disruption process associated with monome-dinome alphabets of Irregular-Length cipher text units. Figures 4-14 and Figure 4-15 show enciphering matrices where the encipherment is disrupted and commutative. The normal row conventions are used to encipher except when the row indicator was the same for the immediately preceding letter. In Figure 4-14, EIGHT could be encrypted 10 29 7 8 49 and then rearranged into standard groups of 5 letters (numbers). In Figure 4-15, E = 24 or 42, T = 621 or 162. Figure 4-16 is an example of the Russian disruption process added for security.

ISOLOGS

Cryptograms produced using identical plain text but subjected to different cryptographic treatment, and yielding different cipher texts are called isologs. (isos = equal and logos = word in Greek). Isologs are usually equal or nearly equal in length. Isologs, no matter how the cryptographic treatment varies, are among the most powerful tools available to the cryptanalyst to solve difficult cryptosystems.

Take two messages A and B suspected of being isologs and write them out under each other. We then examine the similarities and differences. Assume the messages both start Reference your message... I will arrange the messages in a special table to facilitate the study.

```
                        Group No.

                  5              10              15
       ..........................................
A      82 26 56 31 03 74 83 96 98 42 32 52 97 01 15
A'     30 15 08 74 97 14 51 19 73 60 49 67 65 01 06

B      80 27 78 91 06 94 00 01 38 28 54 08 24 00 65
B'     45 64 79 91 81 69 67 25 38 89 41 56 32 52 03

C      63 62 93 39 18 43 15 88 10 48 26 45 84 50 39
C'     90 62 87 75 36 20 35 11 05 70 89 27 77 50 11

D      81 71 35 25 38 73 30 92 07 49 61 75 21 64 76
D'     35 19 99 01 38 99 97 45 02 32 04 11 58 92 16

E      38 72 89 11 47 99 92 64 14 68 13 36 53 38 81
E'     38 46 31 75 47 14 64 80 06 46 85 86 45 38 98

F      89 69 79 38 16 51 75 05 70 74 11 80 44 32 55
F'     26 12 18 38 78 94 88 93 37 28 11 27 22 05 04

G      28 12 02 77 30 31 19 97 99 62 27 86 56 06 53
G'     06 48 43 21 03 98 71 54 26 62 80 76 08 98 80

H      90 87 04 08 67 46 59 41 98 55 10 82 22 29 87
H'     44 10 55 29 00 59 72 82 28 55 87 30 07 08 93

J      46 72 93 62 45
J'     59 68 24 62 53
```

The dinome distributions for these two messages are as follows:

```
     1 2 3 4 5 6 7 8 9 0          1 2 3 4 5 6 7 8 9 0
     ...................          ...................
 1 . 2 1 1 1 2 1 - 1 1 2      1 . 4 1 - 2 1 1 - 1 2 1
 2 . 1 1 - 1 1 2 2 2 1 -      2 . 1 1 - 1 1 2 2 2 1 1
 3 . 2 2 - - 1 1 - 5 2 2      3 . 1 2 - - 2 1 1 5 - 2
 4 . 1 1 1 1 2 2 1 1 1 -      4 . 1 - 1 1 3 2 1 1 1 -
 5 . 1 1 2 1 2 2 - - 1 1      5 . 1 1 1 1 2 1 - 1 2 1
 6 . 1 3 1 2 1 - 1 1 1 -      6 . - 3 - 2 1 - 2 1 1 1
 7 . 1 2 1 2 2 1 1 1 1 1      7 . 1 1 1 1 2 1 1 1 1 1
 8 . 2 2 1 1 - 1 2 1 2 2      8 . 1 1 - - 1 1 2 1 2 3
 9 . 1 2 2 1 - 1 2 2 2 1      9 . 1 1 2 1 - - 2 3 2 1
 0 . 2 1 1 1 1 2 1 2 - 2      0 . 2 1 2 2 2 3 1 3 - 1

      Message A                    Message B
```

Both distributions are too flat - no crests or troughs. We assume a variant system of a monoalphabetic cryptosystem. [FRE3] shows us how to use a Poisson exponential distribution to evaluate random text. The gist of the statistics is that the expected number of blanks is too low. The chi test indicates extreme non randomness for both messages. The chi test applied to both distributions implies that they both have been enciphered by the same cryptosystem because there exists a close correlation between the patterns of the two distributions. [FR1, p123} discusses the potentialities of the cryptomathematics as a supporting science to cryptography.

There are several identical values between the messages. This implies that not only has the same cryptosystem been used but also the same enciphering matrix. The values 38 and 62 must represent very low frequency letters because no variants are even provided for this letter.

We now form isolog chains between the messages.

(06 14 15 26 28 31 35 73 74 81 89 98 99)
(02 07 20 22 43 44 63 90)
(12 37 48 51 69 70 83 94)
(03 30 41 54 65 82 97)
(05 10 24 32 49 87 93)
(16 18 36 76 78 79 86)
(27 45 53 64 80 92)
(11 39 75 88)
(21 58 77 84)
(46 59 68 72)
(00 52 67)
(04 55 61)
(08 29 56)
(19 71 96)
(01 25)
(13 85)
(42 60)

Single Dinomes:
(38) (47) (50) (62) (91)

These chains of cipher values represent identical plain text pairs. Beginning with the first value in the message 82 and 30 a partial chain of equivalent variants is formed; now locating the other occurrences of either value we note the value that coincides with it in the other message. We therefore extend the chain.

We now assign a different letter arbitrarily to each chain and each single dinome value. We convert the messages to uniliteral terms and note the pattern of opening stereotype "Reference your message" and then quickly recover text. (This is how we attacked the German ciphers in WWII.) [NIC4]

The plain text values are arbitrarily fit into 10 x 10 square:

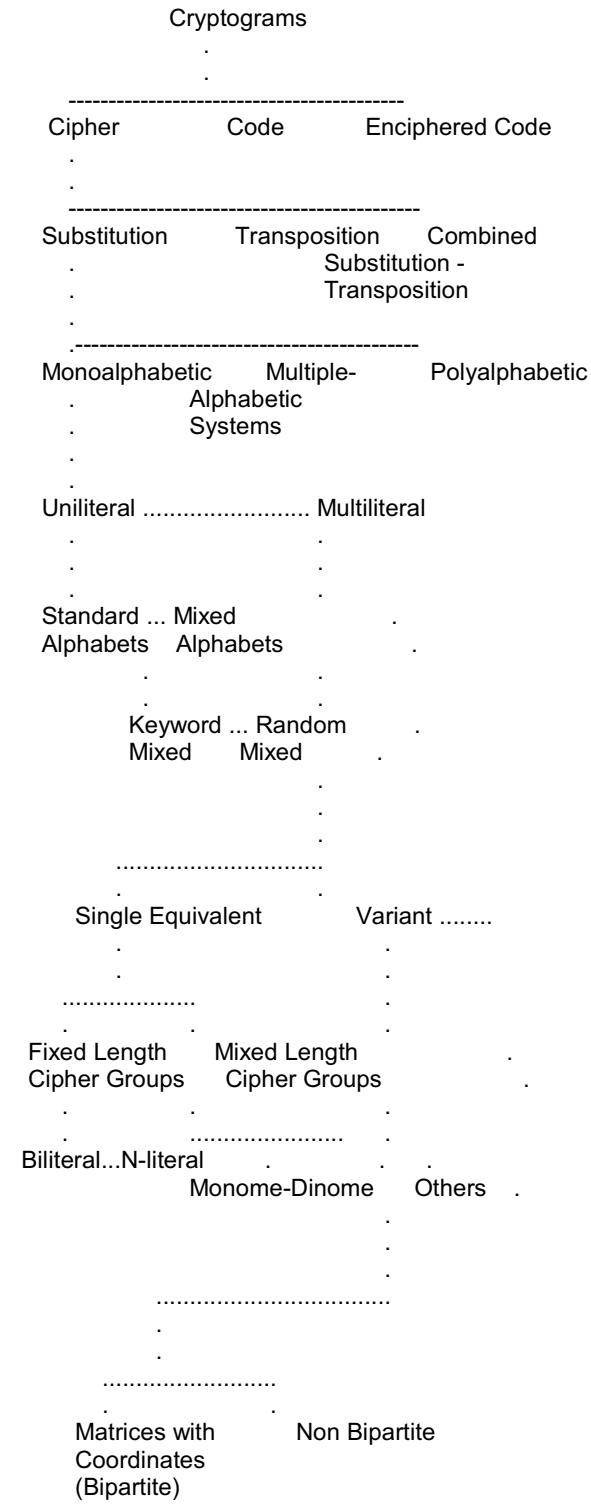
```
    1 2 3 4 5 6 7 8 9 0
    ....................
1 . D N H E E A - A C O
2 . I T - O M E S E F T
3 . E O - - E A N B D R
4 . R Y T T S L V N O -
5 . N U S R P F - I L X
6 . P W T S R - U L N Y
7 . C L E E D A I A A N
8 . E R N I H A O D E S
9 . G S O N - C R E E T
0 . M T R P O E T F - U
```

Manipulating the rows and columns with a view to uncovering the keys or symmetry, we find a latent diagonal pattern without keyword. We set up the following enciphering matrix:

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

I can not over emphasize the value of isologs. The value goes far beyond simple variant systems. Isologs produced by two different code books or two different enciphered code versions of the same plain text; or two encryptions of identical plain text at different settings of a cipher machine, may all prove of inestimable value in the attack on a difficult system.

SYNOPTIC CHART OF CRYPTOGRAPHY PRESENTED IN LECTURES 1 - 5



Here is the tentative plan for the balance of the course. Just a plan - subject to revision.

LECTURES 5 - 7

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

LECTURES 8 - 12

We will investigate and crack Polyalphabetic Substitution systems.

LECTURES 13 - 18

We will investigate and crack Cipher Exchange and Transpositions problems.

LECTURE 19

We will devote this lecture to International Law.

LECTURES 20 - 23

We will walk through the mathematical fields to solve Cryptarithms.

LECTURES 24 - 25

We will introduce modern cryptographic systems and field special topics. We will do a primer on PGP.

SOLUTIONS TO HOMEWORK PROBLEMS FROM LECTURE 3

Thanks to JOE-O for his concise sols.

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
```

I presented Mv-1 in a strange format. It fooled some but not all. The Key is 01=1=a, 02=2=b,...26=z. the alphabet is standard. Message reads: "Here's a simple alphabetic code that I've never seen before. Maybe you can use it in you column. Martin Gardner, Hendersonville, North Carolina.

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

Divide the original cipher into pairs, noting that each pair started with 0,1, or 2 and ended with 0 - 9. Construct a matrix similar to Figure 3-2. (3 x 10) Fill in the matrix with A=01, ending with Z=26. Used 00 =blank. Reduce by converting dinomes to letters. Apply the Phi test and found mon-alphabetic. Used frequency, VOC count, and consonant line to identify B, H, E as vowels and N,D,X,C,I,Y,R,J, as possible consonants. Marking the message with these assumptions, found last eight characters to be a pattern word in Cryptodict as TOMORROW. Working between cipher text and key alphabet matrix, rest fell.

Message reads:Reconnoiter Auys Cayes Bay at daylight seventeen April and then proceed through point George on course three three zero speed twelve period report noon position tomorrow.

Key = NEW YORK, 3 X 10 matrix, Rows 0,1,2, columns 0-9 and 00 blank.

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

Noted all entries were numbered 1-5. Assumed a 5 x 5 matrix filled with a straight alphabet, substituted letters for the dinomes. Used frequency count, contact count and phi test to confirm mono-alphabeticity. Identified 8 consonants and 2 vowels. Made the E, T assumption based on frequency. First word dropped as weather. Rest of message fell apart with addition of W, A, R to the matrix.

Message reads: Weather forecast Thursday partly cloudy ... at present about one thousand feet.

Key = Beginning column 1 = MONDAY, in 5 x 5 matrix.

My last two problems were taken from reference [OP20] course.

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.

[ANDR] Andrew, Christopher, 'Secret Service', Heinemann, London 1985.

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

[AFM] AFM - 100-80, Traffic Analysis, Department of the Air Force, 1946.

[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.

[BAR2] Barker, W., ed., History of Codes and Ciphers in the U.S. During the Period between World Wars, Part II, 1930 -1939., Aegean Park Press, 1990.

[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 Covert Operations," 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.

[CASE] Casey, William, 'The Secret War Against Hitler', Simon & Schuster, London 1989.

[CAVE] Cave Brown, Anthony, 'Bodyguard of Lies', Harper & Row, New York 1975.

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

[CI] FM 34-60, Counterintelligence, Department of the Army, February 1990.

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

[CLAR] Clark, Ronald W., 'The Man who broke Purple', Weidenfeld and Nicolson, London 1977.

[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.

[EYRA] Eyraud, Charles, "Precis de Cryptographie Moderne'" Paris, 1953.

[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.

[FRAB] Friedman, W. F., Field Codes used by the German Army During World War. 1919.

[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.

[GARL] Garlinski, Jozef, 'The Swiss Corridor', Dent, London 1981.

[GAR1] Garlinski, Jozef, 'Hitler's Last Weapons', Methuen, London 1978.

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

[GRA1] Grandpre: "Grandpre, A. de--Cryptologist. Part 1'Cryptographie Pratique - The Origin of the Grandpre', ISHCABIBEL, The Cryptogram, SO60, American Cryptogram Association, 1960.

[GRA2] Grandpre: "Grandpre Ciphers", ROGUE, The Cryptogram, SO63, American Cryptogram Association, 1963.

[GRA3] Grandpre: "Grandpre", Novice Notes, LEDGE, The Cryptogram, MJ75, American Cryptogram Association,1975

[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.

[HOFF] Hoffman, Lance J., editor, "Building In Big Brother: The Cryptographic Policy Debate," Springer-Verlag, N.Y.C., 1995. (A useful and well balanced book of cryptographic resource materials.)

[HOM1] Homophonic: A Multiple Substitution Number Cipher", S-TUCK, The Cryptogram, DJ45, American Cryptogram Association, 1945.

[HOM2] Homophonic: Bilinear Substitution Cipher, Straddling," ISHCABIBEL, The Cryptogram, AS48, American Cryptogram Association, 1948.

[HOM3] Homophonic: Computer Column:"Homophonic Solving," PHOENIX, The Cryptogram, MA84, American Cryptogram Association, 1984.

[HOM4] Homophonic: Hocheck Cipher,", SI SI, The Cryptogram, JA90, American Cryptogram Association, 1990.

[HOM5] Homophonic: "Homophonic Checkerboard," GEMINATOR, The Cryptogram, MA90, American Cryptogram Association, 1990.

[HOM6] Homophonic: "Homophonic Number Cipher," (Novice Notes) LEDGE, The Cryptogram, SO71, American Cryptogram Association, 1971.

[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.

[JOHN] Johnson, Brian, 'The Secret War', Arrow Books, London 1979.

[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, Aegean 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.

[LEDG] LEDGE, "NOVICE NOTES," American Cryptogram Association, 1994. [One of the best introductory texts on ciphers written by an expert in the field. Not only well written, clear to understand but as authoritative as they come!]

[LEWI] Lewin, Ronald, 'Ultra goes to War', Hutchinson, London 1978.

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

[LISI] Lisicki, Tadeusz, 'Dzialania Enigmy', Orzet Biaty, London July-August, 1975; 'Enigma i Lacida', Przeglad lacznosci, London 1974- 4; 'Pogromcy Enigmy we Francji', Orzet Biaty, London, Sept. 1975.'

[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 to 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.]

[MARS] Marshall, Alan, "Intelligence and Espionage in the Reign of Charles II," 1660-1665, Cambridge University, New York, N.Y., 1994.

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

[MAZU] Mazur, Barry, "Questions On Decidability and Undecidability in Number Theory," Journal of Symbolic Logic, Volume 54, Number 9, June, 1994.

[MEND] Mendelsohn, Capt. C. J., Studies in German Diplomatic Codes Employed During World War, GPO, 1937.

[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.

[MODE] Modelski, Tadeusz, 'The Polish Contribution to the Ultimate Allied Victory in the Second World War', Worthing (Sussex) 1986.

[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.

[NORM] Norman, Bruce, 'Secret Warfare', David & Charles, Newton Abbot (Devon) 1973.

[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/Topographic 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.

[STEV] Stevenson, William, 'A Man Called INTREPID', Macmillan, London 1976.

[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.

[TM32] TM 32-250, Fundamentals of Traffic Analysis (Radio Telegraph) Department of the Army, 1948.

[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 lEEE, 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.

[WELC] Welchman, Gordon, 'The Hut Six Story', McGraw-Hill, New York 1982.

[WINT] Winterbotham, F.W., 'The Ultra Secret', Weidenfeld and Nicolson, London 1974.

[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.

[ZEND] Callimahos, L. D., Traffic Analysis and the Zendian Problem, Agean Park Press, 1984. (also available through NSA Center for Cryptologic History)