CLASSICAL CRYPTOGRAPHY COURSE
BY
LANAKI

May 30, 1996
Revision 0

LECTURE 12

POLYALPHABETIC SUBSTITUTION SYSTEMS III
CRYPTANALYSIS OF VIGGY'S EXTENDED FAMILY
DECIMATION IN DETAIL

SUMMARY

In Lectures 12 - 13, we continue our study of the "Viggy" cipher family or Polyalphabetic Substitution systems. We will cover decimation processes in detail and investigate special solutions for periodic ciphers. The important principle of Superimposition will be introduced.

The Resources Section has been updated with more than 50 ACA published references on these and similar systems - focusing on the cryptanalytic attack and areas of historical interest. Thanks to PHOENIX for his help in compiling these sources. [INDE]

"INCOMING"

In Lecture 13, we will tackle the difficult aperiodic polyalphabetic case and introduce auto/running key systems. We will diagram the topics covered in Lectures 10 - 13.

Lecture 14 will be presented by LEDGE. He will cover further Cryptarithm topics.

Lectures 15-18 will discuss the various geometric, transposition and fractionation ciphers.

PORTAX CIPHER

We start with a difficult cousin of the PORTA described in Lecture 11. The PORTAX uses pairs of letters as a unit for encipherment and decipherment as apart from single letters.

A special slide is required for its operation, and a keyword is needed.

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

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

(The above slide-setting is for G-H (key) directly under the A-indicator of the stationary alphabet.)

To encipher the digraph RE, we take the R in the upper row of letters (stationary slide) and the E from the lower pair of letters (sliding), and use the opposite corners of the rectangle formed to obtain the ciphertext, or PI. However, if the digram ER is to be enciphered, we take the E from the stationary alphabet at the top, and the R from the sliding alphabet at the bottom to obtain FP.

Note that if the first letter of a digraph is in the range of A-M, the equivalent ciphertext is dependent on where the slide is used for the key-letter; but, if the first letter of the digraph is in the range of N-Z, then it slides along with the paired rows of lower letters, and therefore all such digraphs having the first letter in the N-Z are constant, without dependent of the key. There is an exception when both letters in the plaintext digraph are in the same column, in which case the key letter has to be known, for letters appearing above the needed letters are used for the ciphertext. [BRYA]

To encipher with keyword, the plaintext is written in two rows under it; continuing to the end of the message. When the final group is reached, if there are not enough letters to make it complete (an even number), add a single null.

For example, encipher the word INNOVATION using the key OFTEN :

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

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

O F T E N   (keyword)
---------
I N N O V
A T I O N
g w
e b
---------
S A R E F
O U N D x
u i
k e
```

Setting the O of the sliding pairs under the 'A' indicator of the stationary alphabet, we enciphering IA as GE (opposite corners); then SO, continuing down the column we encipher the whole column. We then slide the strip until E-F (key) is under the A indicator and encipher that column.

To find the period in the PORTAX is dependent on possible fragments of the plaintext which are known (through the N-Z combinations produced from the unchanged relationship of letters). Lets partially decipher the following PORTAX:

```
SNPOW  LBAMP  ISCWU  OOBXC  WKMAT  ZKTOW  JCBLN   CBJGB
TAAJD  IWUKW  HHVZN  MNUFM  APBJW  PCBSX  JCJQX   TMVUB
MDCBJ  CGUGR.   (90)
```

Assuming a period of 6:

```
S N P O W L
B A M P I S
n   t u r                   natural ?
l   e d s        good
-----------
C W U O O B
X C W K M A
  o y s
  s o c          ok
-----------
T Z K T O W
J C B L N C
r o   s t o
n y   n d s      better
-----------
B J G B T A
A J D I W U
        y
        m
-----------
K W H H V Z
N M N U F M
  t     p t
  s     r y
-----------
A P B J W P
C B S X J C
  n     r o
  f     t e
-----------
J Q X T M V
U B M D C B
  n   t o n
  h u n   r
-----------
J C R   - -
U G R
-----------
```

Note the NY-NDS which could be NYaNDS or NYeNDS. Look at the final group, we find -NTON -HUN-R (hundred?) We next test the keyword by putting T in the final position and testing the precursor letter; A C E F H I L N O P R S and U, At the E setting, OM = TC, making -OYST/-SOCCU with R in the next group confirming OCCUR. The E substitution also gives us the HUNDRED. The rest of the analysis is left for the student for credit.

THE NIHILIST SUBSTITUTION CIPHER

One of my favorite ciphers is the Nihilist Substitution Cipher. Classified as a periodic, it employs numbers to represent letters. Numbers are derived from a 5 x 5 Polybius Square.

We set up a block of 25 letters and combine I/J in one cell.

Figure 12-1a

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

So A = 11, L = 31, T = 44. (Row by Column)

The Polybius Square can be keyed. For example, using UNITED STATES OF AMERICA and eliminating the duplicate letters, we have:

Figure 12-1b

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

We can also mix it up further with a little transposition.

Use BLACKSMITH, transpose and remove the ciphertext by columns starting at 1:

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

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

The resulting square reads:

Figure 12-1c

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

Figure 12-1c shows the effect of the transposition applied first.

Now the message COME AT ONCE enciphered with a keyword of TENT (period = 4) is:

```
T-44  E-15  N-35  T-44
----------------------
C-13  O-34  M-32  E-16
A-11  T-44  O-34  N-33
C-13  E-15   -     -
```

We add the key and the plaintext equivalents together to produce the ciphertext: COME: 57 49 65 59; ATON: 55 59 67 77; CE: 57 30. Each column represents a monoalphabetic substitution in itself, and the reading or value of these letters is dependent on the letters on either side of them.

WEAKNESSES

The lowest number of any key-letter which may be added to the lowest plaintext letter is 11, with a total of 22; the highest combination is two 55's or 10 (110). The numbers 6,7,8, or 9, are not involved in either the tens or the one's additions - but they may result in a sum. Cipher 22 must equal 11 plus 11; and 10 can only mean the sum of two 55's. Zero in the one's column means that two 5's have been added. This is also true in the ten's column. If at any time we find that a 6-7-8-9 is involved we can discard the period assumed as wrong. What we are looking for is a number in the 1-2-3-4-5 range that may be added to produce first the ten's sum and then the one's sum.

FINDING THE PERIOD

There are two ways to find the period - the short and the long way.

SHORT METHOD

The short way of finding the period is to look for two or more 30's. We treat them like a repeated digraph and factor the interval between them looking for a common factor. We may also try the same procedure with the lowest number versus the highest number, for example the distance between two 94's or two 26's.

LONG METHOD

The long way is to assume a 3 period and test the 1'st and 4'th, 2'nd and 5'th, 3'rd and 6'th in the same manner as the short method. When conflicts arise, discard the choice. We continue with an assumption of periods 4, 5, 6, etc. and increase the differentials between ciphertext numbers. [BRYA]

CRYPTANALYSIS OF THE NIHILIST SUBSTITUTION

Gaines [ELCY] suggests that cracking this cipher parallels the Viggy. The period is found through repeated sequences, or in their absence, through repeated single letters, yielding individual frequency counts on the several alphabets of the period. If the arrangement of the ciphertext follows the normal Polybius (aka Checkerboard) Square, the frequency counts will follow the graph of the normal alphabet less one letter. Even with the keyword mixed ciphertext alphabet, no matter how badly mixed, the frequency counts are parallel, the several alphabets combined follow one graph, and can be "lined up."

Notice that the primary alphabet contains only the digits 1-2-3-4-5. The maximum difference is 4 and addition of any number to all of them does not change this fact. the maximum difference between any to sums is still 4. Now the number added during encipherment is also a number containing no digit other than 1-2-3-4-5; thus any number found in the cryptogram can be considered as carrying two separate additions, one for tens and one for ones. The two 5's added give us the revealing 0; the carried digit 1 can be mentally borrowed back, by decreasing the size of the digit preceding the zero. If we find a 40 , we look at it as 3 tens with ten units or finding 110, we may regard this as ten tens and ten units. If we find the numbers 29 and 87 in the cryptogram, we know they were not enciphered by the same key. This is because a difference greater than 4 in the respective tens units exists and no digit whatever added to any two digits of the original square can produce a difference greater than 4. Say we have 30 and 77, with no difference greater than 4, the presence of the zero needs to be accounted for. The number 30 has 2 tens and ten units; 7 - 2 >4, hence, we reject the same key hypothesis.

Four giveaways are 22, 30, 102, and 110. The presence of any one of these numbers gives away the key to the whole cipher alphabet.

[BRYA] presents a useful aid for the standard Polybius Square in Table 12-1. At the top is the key-number, at the left is the plaintext letter, and at ciphertext is found at the intersection. Any two of the three variables yields the unknown letter/number.

Table 12-1

	11 A	12 B	13 C	14 D	15 E	21 F	22 G	23 H	24 I/J	25 K	31 L	32 M
A 11	22	23	24	25	26	32	33	34	35	36	42	43
B 12	23	24	25	26	27	33	34	35	36	37	43	44
C 13	24	25	26	27	28	34	35	36	37	38	44	45
D 14	25	26	27	28	29	35	36	37	38	39	45	46
E 15	26	27	28	29	30	36	37	38	39	40	46	47
F 21	32	33	34	35	36	42	43	44	45	46	52	53
G 22	33	34	35	36	37	43	44	45	46	47	53	54
H 23	34	35	36	37	38	44	45	46	47	48	54	55
I 24	35	36	37	38	39	45	46	47	48	49	55	56
K 25	36	37	38	39	40	46	47	48	49	50	56	57
L 31	42	43	44	45	46	52	53	54	55	56	62	63
M 32	43	44	45	46	47	53	54	55	56	57	63	64
N 33	44	45	46	47	48	54	55	56	57	58	64	65
O 34	45	46	47	48	49	55	56	57	58	59	65	66
P 35	46	47	48	49	50	56	57	58	59	60	66	67
Q 41	52	53	54	55	56	62	63	64	65	66	72	73
R 42	53	54	55	56	57	63	64	65	66	67	73	74
S 43	54	55	56	57	58	64	65	66	67	68	74	75
T 44	55	56	57	58	59	65	66	67	68	69	75	76
U 45	56	57	58	59	60	66	67	68	69	70	76	77
V 51	62	63	64	65	66	72	73	74	75	76	82	83
W 52	63	64	65	66	67	73	74	75	76	77	83	84
X 53	64	65	66	67	68	74	75	76	77	78	84	85
Y 54	65	66	67	68	69	75	76	77	78	79	85	86
Z 55	66	67	68	69	70	76	77	78	79	80	86	87

Table 12-1
continued

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

Consider Edwin Linquist's challenge:

24 66 35 77 37 77 55 59 55 45 55 88 28 66 46

88 37 67 33 59 58 65 45 66 67 58 44 55 34 79

44 59 55 45 42 87 28 76 43 78 46 86 26 67 24

85 26 67 28 76 26 78 46 65 65 88 36 49 54 67

28 65 42 88 36 49 44 89 57 58 54 66 47 67 26

Try period = 2. Starting at the first number 24 constant we scan the line looking for differences greater than 4 using a constant difference of 2. We come to 33 and 38 and stop.

Try period = 3. The first comparison fails at 24 and 77.

Try period = 4. We are able to go through the entire cryptogram, comparing numbers at an interval of 4, without find any difference in either tens or units greater than 4. We now must look at the numbers collectively in columns to verify the period is 4. We recopy the cryptogram into a block.

Key = 4?

24	66	35	77
37	77	55	59
55	45	55	88
28	66	46	88
37	67	33	59
58	65	45	66
67	58	44	55
34	79	44	59
55	45	42	87
28	76	43	78
46	86	26	67
28	76	26	78
46	65	65	88
36	49	54	67
28	65	42	88
36	49	44	89
57	58	54	65
47	67	26	-

Alphabet 1: The tens-half of the first column contains the digit 2 and since this can only come from the addition of 1 plus 1, the only possible key digit is 1. The units-half has a range of 4-5-6-7-8, maximum range possible. The smallest digit to result in 8 is 3, the largest digit to result in 4 is also 3, that is the only digit which can result in all of the digits 4-5-6-7-8 is 3, so that the cipher key for this column is 13. It cannot be anything else.

Alphabet 2: The tens-half of the second column ranges over the full five digits 4-5-6-7-8 (key 3), and the units-half ranges over 5-6-7-8-9 (key 4). This suggests the key digit is 34.

Alphabet 3: The tens-half of the third column contains the 'giveaway' digit of 2 and the units-half also contains the digit 2. The key digit to produce this situation is 11.

Alphabet 4: The tens-half of the fourth column ranges only over the digits 5-6-7-8, with nothing to indicate whether the missing digit is 4 or 9. The key might be either 3 or 4. The units has the full range of digits 5-6-7-8-9, hence key = 4. So we have either 34 o 44 for our key digit. The normal square suggests COAO or COAT as the key word. We use Table 12-1 to good advantage and decipher this cryptogram.

We decipher the whole cryptogram a column at a time:

```
 'C'   'O'   'A'   'T'
  --    --    --    --
  A     M     I     N
  I     S     T     E
  R     A     T     T
  E     M     P     T
  I     N     G     E
  U     L     O     G
  Y     I     N     A
  F     U     N     E
  R     A     L     S
  E     R     M     O
  M     W     E     H
  A     V     E     H
  E     R     E     O
  N     L     Y     T
  H     E     S     H
  E     L     L     T
  H     E     N     U
  T     I     S     G
  O     N     E
```

Reads: A minister attempting eulogy in a funeral sermon: We have here only the shell, the nut has gone.

For the most difficult case presenting multiple key possibilities, we line up the alphabets graphically against their frequency counts to eliminate the extra key digits.

GROMARK

MASTERTON describes a cipher called the GROMARK. The Gromark is akin to the GRONSFELD in that the components never change their position relative to each other and every plain text values has 10 possible cipher representatives. The GROMARK uses a different keying method; encipherment is effected by means of a normal alphabet plain set against a mixed cipher text alphabet. However, instead of cycles or predictable slides of the cipher component, one finds the plain value on the top (normal) component and counts a specified number of positions to the right, then takes the letter in the cipher alphabet immediately below. The choice of how far to count along the sequence is determined by the digital key. One essentially is adding 0 to 9 to the plain value, as in the Gronsfeld, but it is on the mixed sequence, set underneath a plain sequence. The key is derived from a Fibonacci series. On some cycle (frequently 5 wide) the key is derived from a starting group, by adding the first position to the second and placing the result in the sixth position. Similarly, positions 2 and 3 are added to make position number 7, 3, and 4 to make 8, and so forth. All additions are non carrying -a very common cryptographic practice. [MAST]

Example:

Use the starter or "seed" of 48671, the key is:

48671 24383 67119 382021 ...

Solution follows the normal Viggy methods. The crib placement can be interesting.

Example:

```
7 7 2 6 6 4 9 8 2 0 3 7 0 2 3 0 7 2 5 3 7 9 7
J C N W Z Y C A C J N A Y N L Q P W W S T W P
```

without knowing the cipher sequence, we are given the crib SUBSTITUTES and runs somewhere from the J to the final P above.

Since the plain sequence is normal, a repeated cipher letter, with different key letters on it, must stand for plain values removed from each other exactly by the difference of the two numbers. Thus C A C with keys 9 8 2 above it implies that the first cipher C is M for example, the second C is seven positions to the right on the plain sequence, or T.

Or:

```
J K L M N O P Q R S T U V W X
                        C
                        *
```

We prepare a difference table. We are looking for a favorable case where the differences in the cipher repeats matches the plain differences, at the correct interval. To match these differences, we measure them in one direction for the plain and the reverse for the cipher. Table 12-1 shows subtraction of the left hand letter from the right, and we must look at the cipher in the other direction. Differences may be calculated modulo 26.

```
                          Table 12-1

adjacent         19 21  2 19 20  9 20 21 20  5 19
diff's            S  U  B  S  T  I  T  U  T  E  S
xx                2  7 17  1 15 11  1  25 11 14
x-x                9 24 18 16  0  12  0  10
x--x                  0  25  7 ...
```

There is a difference of 7 with the C-C hit, but it doesn't appear on the second row of the table. The keyword must first between A (between C's) and W.

```
7 7 2 6 6 4 9 8 2 0 3 7 0 2 3 0 7 2 5 3 7 9 7
J C N W Z Y C A C J N A Y N L Q P W W S T W P
              S U B S T I T U T E S
```

This is a good tip placement and confirmed by the N-N hit. The A---A in the cipher matches the S---T plain. We build the cipher component by writing the cipher component, and a normal alphabet, count along it from any given plain the number of steps given by the key, then write the cipher value. Find S on the top strip, count 8 to right, place an A. C is two spaces to the right of the position held by the U, and so on. Decipher other letters by counting backwards the number of steps given by the key. Cipher C ahead of thew crib translates to N.

```
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
A J             Y     P               Q W N C L
```

Without a tip the system will fall to statistics. The numbers associated with any given cipher letter represent a stretch of 10 consecutive values along a normal alphabet such as C to L or X to G, we could prepare a table with A to Z as the rows and 9 to 0 as the columns. Frequencies can be combined and a stretch such as PQRST area will show as the normal. The backwards normal sequence yields a bar graph of the segment of the normal alphabetic frequencies.

DECIMATION PROCESSES - FURTHER REMARKS

In Lecture 11, we presented QUAGMIRES I-IV and solved them by a variety of methods. Inherent in their solution was Friedman's principle of indirect symmetry. [FRE7] Prima facie to this symmetry principle is a process of alphabet dissociation called Decimation. This same process effects all Viggy class ciphers and is important from a theoretical point of view. Decimation is especially effective in solving mixed alphabet systems like the Quagmire III & IV. Decimation is a process of selection and derivation of a sequence of equivalent components according to some fixed interval. For example, the sequence A E I M is derived by decimation of extracting every fourth letter from a normal alphabet.

Consider the two mixed alphabets in a QUAGMIRE III:

```
                01
                 *       *
Plain:           QUESTIONABLYCDFGHJKMPRVWXZ
Cipher:  QUESTIONABLYCDFGHJKMPRVWXZQUESTIONABLYCDFGHJKMPRVWXZ
                 *       *
                0k
```

By setting the two sliding components against each other in the two positions shown: A in the first set and B in the second set we can derive two, we can derive two different sets of secondary alphabets based on the key letters.

```
                 01 *       *
Plain:            QUESTIONABLYCDFGHJKMPRVWXZ
Cipher:  QUESTIONABLYCDFGHJKMPRVWXZQUESTIONABLYCDFGHJKMPRVWXZ
                  *       *
                  0k
```

Secondary Alphabet (1)

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

Secondary Alphabet (2)

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

Sliding strips will yield the same results as a Viggy type table based on the Keyword QUESTIONABLY (see a partial table in Table 11-2.

```
      Table 12-2
  Partial Reconstruction

QUESTIONABLYCDFGHJKMPRVWXZ
UESTIONABLYCDFGHJKMPRVWXZQ
ESTIONABLYCDFGHJKMPRVWXZQU
STIONABLYCDFGHJKMPRVWXZQUE
TIONABLYCDFGHJKMPRVWXZQUES
IONABLYCDFGHJKMPRVWXZQUEST
ONABLYCDFGHJKMPRVWXZQUESTI
NABLYCDFGHJKMPRVWXZQUESTIO
ABLYCDFGHJKMPRVWXZQUESTION
BLYCDFGHJKMPRVWXZQUESTIONA
LYCDFGHJKMPRVWXZQUESTIONAB
YCDFGHJKMPRVWXZQUESTIONABL
CDFGHJKMPRVWXZQUESTIONABLY
.                        .
```

Superficially secondary alphabets (1) and (2) show no resemblance of symmetry despite the fact that they were both created from the same primary alphabet. We do find a Latent Symmetry Of Position (aka Indirect Symmetry of Position). This phenomenon has widespread use in the Viggy family. Consider alphabet (2):

Secondary Alphabet (2)

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

We construct a chain of alternating plaintext and ciphertext equivalents, beginning at any point and continuing until the chain is completed. We start Aplain = Jcipher, Jplain = Qcipher, Qplain = Bcipher...., dropping the common letters we have A J Q B. The complete sequence of letters is:

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

When slid against itself it will produce exactly the same secondary alphabets as do the primary components based upon the word QUESTIONABLY. For example, compare the secondary alphabets given by the two settings of the externally different components below:

```
                 *        *
Plain:           QUESTIONABLYCDFGHJKMPRVWXZ
Cipher:  QUESTIONABLYCDFGHJKMPRVWXZQUESTIONABLYCDFGHJKMPRVWXZ
                 *        *
```

Secondary Alphabet (1)

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

```
         *  *
Plain:   AJQBKULMEYPSCRTDVIFWOGXNHZ
Cipher: AJQBKULMEYPSCRTDVIFWOGXNHZAJQBKULMEYPSCRTDVIFWOGXNHZ
         *  *
```

Secondary Alphabet (2)

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

Since the sequence A J Q B K ... gives exactly the same equivalents in the secondary alphabets as does the sequence QUEST......XZ, the former is cryptographically equivalent to the latter sequence. For this reason the A J Q B K .. sequence is termed an equivalent primary component. If the real or original primary component is a keyword mixed sequence, it is hidden or latent within the equivalent primary sequence; it can also be made patent by the process of decimation of the equivalent primary component.

Friedman in [FRE7] describes the process as follows: find three letters in the equivalent primary component that are a likely unbroken sequence in the original primary component, and see if the interval between the first and second is the same as that of the second and third. Try X, Y, Z in the equivalent primary component above. Note the sequence ....W O G X N H Z...; the distance or interval between W X Z is three letters. Continuing the chain by adding letters three intervals removed, the latent original primary component is made patent.

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

24 25 26
 P  R  V
```

KEYWORD - MIXED SEQUENCE

We can combine the previous steps into one operation. Starting with any pair of letters in the cipher component of the secondary alphabets, likely to be sequent in the keyword-mixed sequence, such as JK, the following chains of digraphs may be produced. Thus JK plain stand over QU cipher respectively, QU in the plain stand over BL in the cipher, respectively, etc. Connecting the pairs:

```
JK>QU>BL>KM>UE>LY>MP>ES>YC>PR>ST>CD>RV>TI>DF>VW>IO>FG>WX>
ON>GH>XZ>NA>HJ>ZQ>AB>JK.....
```

We then unite by common letters:

```
JK>KM>MP>PR>RV>VW>WX>XZ>ZQ>QU>UE>ES>ST>TI>IO>ON>NA>
AB>BL>LY>YC>CD>DF>FG>GH>HJ>JK.....
```

or:

JKMPRVWXZ-QUESTIONABLY-CDFGH

HALF CHAINS

Only 12 /26 alphabets will yield a complete equivalent primary component, as shown above. Even number of intervals for sliding the alphabets will yield half chains or 13 letter chains. Friedman [FRE7] describes several methods to combine the half chains into fully equivalent primary components.

FRIEDMAN'S OBSERVATIONS

Friedman observed that in the case of a 26-element component sliding against itself (both components proceeding in the same direction), it is only the secondary alphabets resulting from odd-interval displacements of the primary components which permit reconstructing a single 26-letter chain of equivalents. This is true except for the 13th interval displacement, which acts like an even number displacement, in that no complete chain of equivalents can be established from the secondary alphabet. Friedman states the general rule as: any displacement interval which has a factor in common with the number of letters in the primary sequence will yield a secondary alphabet from which no complete chain of 26 equivalents can be derived for the construction of a complete equivalent primary component. Components sliding in opposite directions act as a 13 interval displacement because of their reciprocal nature.

Friedman concluded that whether or not a complete equivalent primary component is derivable by decimation from an original primary component (and if not, the lengths and numbers of chains of letters, or incomplete components, that can be constructed in attempts to derive such equivalent components) will depend upon the number of letters in the original primary component and the specific decimation interval selected. [FRE7] Friedman constructed a table relating the number of characters in the original primary component, decimation interval and total number of complete sequences that can be formed. See Table 12-3.

TABLE 12-3

Decimation Interval	Number of Characters in Original Primary Component: 32	30	28	27	26	25	24	22	21	20	18	16
2	16	15	14	27	13	25	12	11	21	10	9	8
3	32	10	28	9	26	25	8	22	7	20	6	16
4	8	15	7	27	13	25	6	11	21	5	9	4
5	32	6	28	27	26	5	24	22	21	4	18	16
6	16	5	14	9	13	25	4	11	7	10	3	8
7	32	30	4	27	26	25	24	22	3	20	18	16
8	4	15	7	27	13	25	3	11	21	5	9	2
9	32	10	28	3	26	25	8	22	7	20	2	16
10	16	3	14	27	13	5	12	11	21	2	9	8
11	32	30	28	27	26	25	24	2	21	20	18	16
12	8	5	7	9	13	25	2	11	7	5	3	4
13	32	30	28	27	2	25	24	22	21	20	18	16
14	16	15	2	27	13	25	12	11	3	10	9	8
15	32	2	28	9	26	5	8	22	7	4	6	
16	2	15	7	27	13	25	3	11	21	5	9	
17	32	30	28	27	26	25	24	22	21	20		
18	16	5	14	3	13	25	4	11	7	10		
19	32	30	28	27	26	25	24	22	21			
20	8	3	7	27	13	5	6	11				
21	32	10	4	9	26	25	8					
22	16	15	14	27	13	25	12					
23	32	30	28	27	26	25						
24	4	5	7	9	13							
25	32	6	28	27								
26	16	15	14									
27	32	10										
28	8	15										
29	32											
30	16											
Total Number Of Sequences	14	6	10	16	10	18	6	8	10	6	4	6

>From Table 12-3, we see that in a 26-letter original primary component, decimation interval 5 will yield a complete equivalent primary component of 26 letters, whereas decimation intervals of 4 or 8 will yield 2 chains of 13 each. In a 24-letter component, decimation interval 5 will also yield a complete equivalent primary component of 24 letters, but decimation interval 4 will yield 6 chains of 4 letters each, and decimation interval 8 will yield 3 chains of 8 letters each.

It follows that in the case of an original primary component in which the total number of characters is a prime number, all decimation intervals will yield complete equivalent primary components. Table 12-3 omits the prime number sequences from 16-32. [FRE7]

SPECIAL SOLUTIONS FOR PERIODIC CIPHERS

Special circumstances give rise atypical solutions of periodic ciphers. We shall look at four special cases:
1) isologs, 2) 'stagger', 3) long latent repetition and 4) superimposition.

ISOLOGS

Recall that an Isolog is defined as the exact same plain text message enciphered by two different keys in the same cryptosystem. Lets use two monoalphabetic substitution systems to illustrate the point. Assume two messages are intercepted going from station A to B. B had called for a retransmit because of some error in transmission. We suspect the messages are the same plaintext content and they both have the same length. We superimpose one message over the other:

```
1. NXGRV MPUOF ZQVCP VWERX QDZVX WXZQE TBDSP VVXJK RFZWH 2.
EMLHJ FGVUB PRJNG JKWHM RAPJM KMPRW ZTAXG JJMCD HBPKY
```

chaining from 1 to 2: NE>EW>WK>KD>DA ......

```
1. ZUWLU IYVZQ FXOAR
2. PVKIV QOJPR BMUSH
```

Next we initiate a chain of ciphertext equivalents (reducing the common letter) from message 1 to message 2, yielding:

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


24 25 26
 V  J  C
```

With some experimentation, we find the Key word QUESTIONABLY and the decimation interval of +5 Modulo 26. The complete 26 letter chain was available for reconstruction, but this is not a requirement.

Why is it possible to reconstruct the primary component and solve the above two messages without having any plain text at all? Since the plain text of both messages is the same, the relative displacement of the same primary components in the case of message 1 differs from the relative displacement of the same primary components in message 2 by a FIXED interval. Therefore, the distance between N and E (1st two cipher letters of the two messages) on the primary component, regardless of what plaintext letter these two cipher letters represent, is the same distance between E and W (18th letters), W and K (17th letters), and so forth. Thus this fixed interval permits the establishing of a complete chain of letters separated by constant intervals and this chain becomes an equivalent primary component.

To solve, we take the frequency distributions of message 1 and 2:

```
                                       E       S T I   O
     1 1 1 2 2 3 1 1 1 1 1 1 1 1 2 3 4 4 1 1 3 7 4 6 1 6
1:   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

                   E   S T   I     O
     2 3 1 1 1 1 3 4 1 7 4 1 6 1 1 7 1 4 1 1 2 3 2 1 1 1
2:   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
```

We set up two key word mixed alphabets and slide against each other. With some trial and error we find:

```
NABLYCDFGHJKMPRVWXZQUESTIO
QUESTIONABLYCDFGHJKMPRVWXZ
```

The plain text reads: Five squadrons must be in position by H plus six zero two at Jackson Ridge.

The same procedure is applied on two repeating key ciphers suspected of being Isologs:

Message 1

```
YHYEX  UBUKA  PVLLT  ABUVV  DYSAB  PCQTU
NGKFA  ZEFIZ  BDJEZ  ALVID  TROQS  UHAFK
```

Message 2

```
CGSLZ  QUBMN  CTYBV  HLQFT  FLRHL  MTAIQ
ZWMDQ  NSDWN  LCBLQ  NETOC  VSNZR  BJNOQ
```

The first step is to find the length of the period. The usual method fails for lack of long repetitions and the digraphs are not promising. We use the Principle of Superimposition to get a hold on the period for both cryptograms.

```
1 2 3 4 5 6 7 8 9101112131415161718192021222324252627282930
Y H Y E X U B U K A P V L L T A B U V V D Y S A B P C Q T U
C G S L Z Q U B M N C T Y B V H L Q F T F L R H L M T A I Q

313233343536373839404142434445464748495051525354555657585960
N G K F A Z E F I Z B D J E Z A L V I D T R O Q S U H A F K
Z W M D Q N S D W N L C B L Q N E T O C V S N Z R B J N O Q
```

We employ a subterfuge will be employed based upon the theory of factoring. We search for cases of identical superimposition. We have:

```
    4      44                              6  18    30
    E  and E   are separated by 40 letters, U, U and U  which
    L      L                               Q  Q     Q
```

are separated by 12 letters. We factor these intervals as if they were ordinary repetitions. The most frequent factor should correspond to the period. We are dealing with Isologs. The plain text is the same in both messages, so the principle of identity of superimposition can only be the result of identity of encipherments by identical cipher alphabets. The same relative position in the keying cycle has been reached in both cases of the identity. The distance between identical superimpositions must be equal to or a multiple of the length of the period. The following is the complete set of superimposed pairs:

Repetition	Interval	Factors
EL - EL	40	2,4,5,8,10,20
UQ - UQ -UQ	12	2,3,4,6
UB - UB	48	2,3,4,6,,8,12,24
KM - KM	24	2,3,4,6,12
AN -AN -AN	36/12	2,3,4,6;9,12,18
VT -VT -VT	8/28	2,4; 2,4,7,14
TV - TV	36	2,3,4,6,9,12,18
AH - AH	8	2,4
BL -BL -BL	8/16	2,4,;8
SR - SR	32	2,4,8,16
FD - FD	4	2
ZN - ZN	4	2
DC - DC	8	2, 4

Only the factors 2 and 4 are common. We discard 2 as improbable. We break up the message into groups of four.

```
     1234 1234 1234 1234 1234 1234 1234 1234
1.   YHYE XUBU KAPV LLTA BUVV DYSA BPCQ TUNG 2.   CGSL ZQUB
MNCT YBVH LQFT FLRH LMTA IQZW
     *    *    *    *
```

```
     1234 1234 1234 1234 1234 1234 1234
1.   KFAZ EFIZ BDJE ZALV IDTR OQSU HAFK
2.   MDQN SDWN LCBL QNET OCVS NZRB JNOQ
```

We develop a decipherment Tableaux:

O	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
1		L		F	S			J	O		M	Y			N					I				Z	C	Q
2	N			C		D		G				B				M	Z				Q				L	
3	Q	U	T			O			W	B		E		Z		C			R	V		F			S	
4	H				L		W				Q						A	S			B	T				N

Using the meyhods previously described, we build up the equivalent primary component and combine our digrams.

BL, DF, ES, HJ, IO, KM, LY, ON,TI, XZ, YC, ZQ.

BLYC .DF   TION   XZQ(U) [ES]TION(A)BLY CDF (G) H

JKM(P) (R) (V) XZ

It is not a long jump to a key word QUESTIONABLY and the equivalent primary component:

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

The fact that the original primary component was exposed was pure chance, it could have been an equivalent primary sequence alphabet.

>From here we apply the completion of the plain-component sequence using the high frequency letter assortments. For the first message:

```
Gen Alphabet 1    Alphabet 2    Alphabet 3    Alphabet 4

1    YXKLBDBTKE   1HUALUYPUFF   5YBPTVSCNAI    EUVAVAQGZZ
2   2CZMYLFLIMS   4JEBYECREGG   5CLRIWTDABO    SEWBWBUHQQ
3   2DQPCYGYOPT   3KSLCSDVSHH   3DYVOXIFBLN    TSXLXLEJUU
4   4FURDCHCNRI    MTYDTFWTJJ   3FCWNZOGLYA    ITZYZYSKEE
5   3GEVFDJDAVO    PICFIGXIKK    GDXAQNHYCB    OIQCQCTMSS
6   2HSWGFKFBWN   4RODGOHZOMM    HFZBUAJCDL   5NOUDUDIPTT
7    JTXHGMGLXA    VNFHNJQNPP    JGQLEBKDFY   8ANEFEFORII*
8    KIZJHPHYZB    WAGJAKUARR   1KHUYSLMFGC   6BASGSGNVOO
9    MOQKJRJCQL    XBHKBMEBVV   2MJECTYPGHD   5LBTHTHAWNN
10   PNUMKVKDUY    ZLJMLPSLWW    PKSDICRHJF    YLIJIJBXAA
11  4RAEPMWMFEC    QYKPYRTYXX    RMTFODVJKG    CYOKOKLZBB
12  3VBSRPXPGSD    UCMRCVICZZ   2VPIGNFWKMH   2DCNMNMYQLL
13  4WLTVRZRHTF    EDPVDWODQQ    WROHAGXMPJ   2FDAPAPCUYY
14   XYIWVQVJIG   3SFRWFXNFUU    XVNJBHZPRK   3GFBRBRDECC
15   ZCOXWUWKOH    TGVXGZAGEE    ZWAKLJQRVM   1HGLVLVFSDD
16   QDNZXEXMNJ    IHWZHQBHSS    QXBMYKUVWP   1JHYWYWGTFF
17   UFAQZSZPAK    OJXQJULJTT    UZLPCMEWXR    KJCXCXHIGG
18   EGBUQTQRBM    NKZUKEYKII    EQYRDPSXZV    MKDZDZJOHH
19  3SHLEUIUVLP   5AMQEMSCMOO    SUCVFRTZQW    PMFQFQKNJJ
20  6TJYSEOEWYR?  4BPUSPTDPNN    TEDWGVIQUX    RPGUGUMAKK
21   IKCTSNSXCV   8LRETRIFRAA*   ISFXHWOUEZ   3VRHEHEPBMM
22  5OMDITATZDW?  3YVSIVOGVBB    OTGZJXNESQ    WVJSJSRLPP
23   NPFOIBIQFX   3CWTOWNHWLL    NIHQKZASTU    XWKTKTVYRR
24  5ARGNOLOUGZ?   DXINXAJXYY    AOJUMQBTIE    ZXMIMIWCVV
25  4BVHANYNEHQ    FZOAZBKZCC   5BNKEPULIOS    QZPOPOXDWW
26   LWJBACASJU    GQNBQLMQDD   7LAMSREYONT*   UQRNRNZFXX
```

We choose generatrices 20/22/24; 21; 26; 7 because of the highest two category scores. it is not much of a jump to find Alphabet 1 generatrix as alphabet 24:

```
1 2 3 4
A L L A
R R A N
G E M E
N T S F
O R R E
L I E F
O F Y O
U R O R
G A N I
Z A T I
```

>From a Vigenere Square (Figure 12-1) based on the keyword QUESTIONABLY, we find the key words SOUP for message 1 and TIME for message 2.

```
S O U P  S O U P  S O U P  S O U P  S O U P  S O U P
----------------------------------------------------
Y H Y E  X U B U  K A P L  L L T A  B U V V  D Y S A
A L L A  R R A N  G E M E  N T S F  O R R E  L I E F

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

I D T R   O Q S U   H A F K
E N S U   S P E N   D E D X

T I M E  T I M E  T I M E  T I M E  T I M E  T I M E
____________________________________________________

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

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

O C V S   N Z R B  J N O Q
E N S U   S P E N   D E D X
```

Figure 12-1

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

SOLUTION OF ISOLOGS INVOLVING THE SAME SET OF PRIMARY COMPONENTS BUT WITH KEY WORDS OF DIFFERENT LENGTHS

The example previous had two keywords the same lengths. The Method of Superimposition works with Keywords of different lengths. Friedman works an interesting example:

Message 1

```
VMYZG  EAUNT  PKFAY  JIZMB  UMYKB  VFIVV
SEOAF  SKXKR  YWCAC  ZORDO  ZRDEF  BLKFE
SMKSF  AFEKV  QURCM  YZVOX  VABTA  YYUOA
YTDKF  ENWNT  DBQKU  LAJLZ  IOUMA  BOAFS
KXQPU  YMJPW  QTDBT  OSIYS  MIYKU  ROGMW
CTMZZ  VMVAJ
```

Message 2

```
ZGANW  IOMOA  CODHA  CLRLP  MOQOJ  EMOQU
DHXBY  UQMGA  UVGLQ  DBSPU  OABIR  PWXYM
OGGFT  MRHVF  GWKNI  VAUPF  ABRVI  LAQEM
ZDJXY  MEDDY  BOSVM  PNLGX  XDYDO  PXBYU
QMNKY  FLUYY  GVPVR  DNCZE  KJQOR  WJXRV
GDKDS  XCEEC.
```

Both messages permit factoring at periods of 4 and 6 letters, respectively. Superimposing the two messages and marking the position of each letter in the corresponding period, we have:

```
        12341  23412  34123  41234  12341  23412
No. 1   VMYZG  EAUNT  PKFAY  JIZMB  UMYKB  VFIVV
No. 2   ZGANW  IOMOA  CODHA  CLRLP  MOQOJ  EMOQU
        12345  61234  56123  45612  34561  23456

        34123  41234  12341  23412  34123  41234
No. 1   SEOAF  SKXKR  YWCAC  ZORDO  ZRDEF  BLKFE
No. 2   DHXBY  UQMGA  UVGLQ  DBSPU  OABIR  PWXYM
        12345  61234  56123  45612  34561  23456

        12341  23412  34123  41234  12341  23412
No. 1   SMKSF  AFEKV  QURCM  YZVOX  VABTA  YYUOA
No. 2   OGGFT  MRHVF  GWKNI  VAUPF  ABRVI  LAQEM
        12345  61234  56123  45612  34561  23456

        34123  41234  12341  23412  34123  41234
No. 1   YTDKF  ENWNT  DBQKU  LAJLZ  IOUMA  BOAFS
No. 2   ZDJXY  MEDDY  BOSVM  PNLGX  XDYDO  PXBYU
        12345  61234  56123  45612  34561  23456

        12341  23412  34123  41234  12341  23412
No. 1   KXQPU  YMJPW  QTDBT  OSIYS  MIYKU  ROGMW
No. 2   QMNKY  FLUYY  GVPVR  DNCZE  KJQOR  WJXRV
        12345  61234  56123  45612  34561  23456

        34123  41234
No. 1   CTMZZ  VMVAJ.
No. 2   GDKDS  XCEEC.
        12345  61234
```

What is neat about this superimposition is that we can establish secondary alphabets by distributing the letters from the 12 different superimposed pairs of numbers. The 1 - 1 superimposition is placed in the tableau at the 0 - 1 row, column in the tableaux.

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

We construct the complete equivalent primary component:

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

Ok. We have the cipher component. Is it normal? reversed? Mixed? Same questions for the plain component sequence. We assume that the primary plain component is normal direct sequence. We attempt to solve and fail. Normal reverse will also fail. We assume a K3 situation, i.e. the plain and cipher components are identical. Again the test fails. We assume that the plain is in reverse mode. Nope. So we have a K4 situation, both primary components are different mixed sequences.

Message 1 transcribed into periods of four letters.

Message 1

```
VMYZ GEAU NTPK FAYJ IZMB UMYK BVFI VVSE
OAFS KXKR YWCA CZOR DOZR DEFB LKFE SMKS
FAFE KVQU RCMY ZVOX VABT AYYU OAYT DKFE
NWNT DBQK ULAJ LZIO UMAB OAFS KXQP UYMJ
PWQT DBTO SIYS MIYK UROG MWCT MZZV MVAJ
```

The Uniliteral frequency distributions for the four secondary alphabets are shown in 1A -4A. We have the reconstructed cipher alphabet, 1B-4b shows the sequences rearranged.

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

We now shift 1B-4B for superimposition and combine the distributions. The latter distributions may be combined so as to yield a single monoalphabetic distribution for the entire message. In other words, the polyalphabetic message can be converted into monoalphabetic terms, and thereby simplifying the situation considerably.

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

        6 2 5 4 2 7  15 9 2    21 9 6 410 3 1 1 7 2 918 9 1
1B-4B   I T K N P Z H M W B Q E U L F C S J A X R G D V O Y
combinedH M       L   R S       O       A       I Y N E T
Plain
Equiv's
```

I have converted 2B-4B into terms of 1B. The 2 E's of 2B add to 1B I. The two K's of alphabet 3 becomes I's and the N becomes a T, and so forth. We solve the monoalphabetic cipher.

```
12341  23412  34123  41234  12341  23412

ENEMY  HASCA  PTURE  DHILL  ONETW  OONEO
VDVTG  ISWNZ  KOFMV  LIRZZ  UDVOB  UUDVU

URTRO  OPSHA  VEDUG  INAND  CANHO  LDFOR
FMOMU  UKWIS  YVLFC  RDSDL  NSDIU  ZLJUM

ANHOU  RORPO  SSIBL  YLONG  ERREQ  UESTR
SDIUF  MUMKU  WWRPZ  GZUDC  VMMVA  FVWOM

EINFO  RCEME  NTSTO  PADDI  TIONA  LTROO
VVDJU  MNVTV  DOWOU  KSLLR  ORDUS  ZOMUU

PSSHO  ULDBE  SENTV  IAGEO  RGETO  WNFRE
KWWIU  FZLPV  WVDOY  RSCVU  MCVOU  BDJMV

DERIC  KROAD.
LVMRN  XMUSL.
```

Having the plain text, the derivation of the plain or equivalent plain component is straightforward. We may base the reconstruction upon any of the secondary alphabets, since the plaintext - ciphertext relationship is known directly, and the primary cipher component is at hand. So:

```
1 2 3 4 5 6 7 8 9 1011121314151617181920212223242526
H M P C B L . R S  W . . O D U G A F Q K I Y N E T V
```

with Key words of STAR and OCEANS for messages 1 and 2.

NECESSARY AND SUFFICIENT CONDITIONS FOR SUPERIMPOSITION AND CONVERSION TO MONOALPHABETIC TERMS

This example shows the power of the method of superimposition and conversion of a polyalphabetic cipher to monoalphabetic terms. This conversion is possible because the sequence of letters forming the cipher component has been reconstructed and was known, and the uniliteral distributions for the respective secondary cipher alphabets could theoretically be shifted to correct superimpositions for monoalphabeticity. The data was sufficient to give proper indications for alignment of the alphabets and relative displacements. The chi test could also have been brought to bear to match columns. The above constitutes the necessary and sufficient conditions to convert theory to actuality.

SOLUTION OF ISOLOGS INVOLVING DIFFERENT PAIRS OF UNKNOWN PRIMARY COMPONENTS

The principle of superimposition continues to work for us even when the primary components are different, and the repeating keys are of different lengths.

There are two general attacks. The first is a slight modification of the procedures previously discussed. We first factor the messages, then superimpose the messages on a width of the least common multiple, then create a reconstruction matrix based on the cipher values. We must limit our observations to within the matrix, because the given messages are different and therefore the indirect symmetry does not extend to the 0 or assumed plain line. The wrinkle in the fabric is we must restrict our observations to a homogeneous set of lines, like 1-1,1-2,1-3,1-4 etc. From this data, we reduce the reconstruction matrix to a smaller set and solve for the equivalent primary component. It is possible to invert the matrix so that values for the second message will yield its equivalent primary component.

ARBITRARY REDUCTION METHOD

It is not necessary to recognize the plain text to solve a problem involving Isologs. The next cryptanalytic attack is applicable for many types of ciphers. The procedure exposes latent letter relationships and reduces the imposed chaos of the cryptogram. Given:

Message 1

```
BWXPS  OBYII  UYHLF  KFSOP  VGEYW  PBVXO
UGJPB  WDXUG  HSWDH  KHKHC  UAYKP  NFSPD
OBBYB  INKFL  WABOX  PJXUV  WKFXR  WXYWS
SDYZQ  ZHETA  JXXZW  XJROS  PDEEW  OJONK
GIRXR  WUYDK  NTJWR  EVBUR  DLISJ  BLCKK
FODEV  DYZQZ  SHCTW  DIEXZ
```

Factoring gives us periods of 4 and 5 for messages 1 and 2, respectively. We write out the messages on a width of the least common multiple of 20.

Message 2

```
JNLEJ  HWUAH  JHUIV  YNCHC  HLPKD  EWZJJ
JNAHB  HZBIM  TUBQE  FJAKM  JVBEF  XNCTL
FAAKV  KIABG  CVFNY  FWBIQ  GERSA  TZUSD
SXBUD  SHAWA  YXLJD  CQLED  HXGZL  ZWHNB
VTJSA  TSUUC  MIAKK  JEMIY  DSKGB  VTJYC
XYLZE  CXLSU  MVMND  ONFJY
```

```
12341  23412  34123  41234        20
BWXPS  OBYII  UYHLF  KFSOP
JNLEJ  HWUAH  JHUIV  YNCHC
12345  12345  12345  12345
A             A  A
12341  23412  34123  41234        40
VGEYW  PBVXO  UGJPB  WDXUG
HLPKD  EWZJJ  JNAHB  HZBIM
12345  12345  12345  12345
              A         A
12341  23412  34123  41234        60
HSWDH  KHKHC  UAYKP  NFSPD
TUBQE  FJAKM  JVBEF  XNCTL
12345  12345  12345  12345
              A
12341  23412  34123  41234        80
OBBYB  INKFL  WABOX  PJXUV
FAAKG  KIABG  CVFNY  FWBIQ
12345  12345  12345  12345
    A      A    A       A
12341  23412  34123  41234       100
WQFXR  WXYWS  SDYZQ  ZHETA
GERSA  TZUSD  SXBUD  SHAWA
12345  12345  12345  12345

12341  23412  34123  41234       120
JXXZW  XJROS  PDEEW  OJONK
YXLJD  CQLED  HXGZL  ZWHNB
12345  12345  12345  12345

12341  23412  34123  41234       140
GIRXR  WUYDK  NTJWR  EVBUR
VTJSA  TSUUC  MIAKK  JEMIY
12345  12345  12345  12345
        A            A  A
12341  23412  34123  41234       160
DLISJ  BLCKK  FODEV  DYZQZ
DSKGB  VTJYC  XYLZE  CXLSU
12345  12345  12345  12345
 A
12341  23412                     170
SHCTW  DIEXZ
MVMND  ONFJY
12345  12345
         A
```

We arbitrarily assign the value of A(plain) as the first letter of the plain text. Since in message 1, B(cipher)= A(plain), then every B(cipher) in alphabet 1 must equal A(plain); these values are entered in the table above. Also the 65th and 73rd letter of message 1 are A(plain), this establishes that in message 2, G(cipher) in alphabet 5 and F(cipher) in alphabet 3 are also A(plain); we enter these values. Similarly, every J(cipher) in alphabet 1 of message 2 equals A(plain). We continue the process and recover all the A(plains) of the pseudo-plain text with the resulting worksheet shown above.

We arbitrarily assign the value of B(plain) to the V(cipher) at the 21st position of message 1. The other V(cipher) of message number 1 establishes the E(cipher) of message 2 also as a B(plain). This procedure of arbitrary assignments is continued until all the cipher letters of alphabet 1 of message 1, are placed. we are able to reduce most of the text to monoalphabetic terms. The worksheet is as follows:

```
12341  23412  34123  41234        20
BWXPS  OBYII  UYHLF  KFSOP
JNLEJ  HWUAH  JHUIV  YNCHC
12345  12345  12345  12345
ACHDIIFCK     ACCA   FME D

12341  23412  34123  41234        40
VGEYW  PBVXO  UGJPB  WDXUG
HLPKD  EWZJJ  JNAHB  HZBIM
12345  12345  12345  12345
B  CE   F LI  AMF F  BHOAM

12341  23412  34123  41234        60
HSWDH  KHKHC  UAYKP  NFSPD
TUBQE  FJAKM  JVBEF  XNCTL
12345  12345  12345  12345
CEOOC  D FCM  AJODB   MEBO

12341  23412  34123  41234        80
OBBYB  INKFL  WABOX  PJXUV
FAAKG  KIABG  CVFNY  FWBIQ
12345  12345  12345  12345
DGFCA   IFMA  OJAIH  DFOA

12341  23412  34123  41234       100
WQFXR  WXYWS  SDYZQ  ZHETA
GERSA  TZUSD  SXBUD  SHAWA
12345  12345  12345  12345
EB EJ  CHCEE  LOOHE  LCF J

12341  23412  34123  41234       120
JXXZW  XJROS  PDEEW  OJONK
YXLJD  CQLED  HXGZL  ZWHNB
12345  12345  12345  12345
FOHLE  O HDE  BOPFO   FIIF

12341  23412  34123  41234       140
GIRXR  WUYDK  NTJWR  EVBUR
VTJSA  TSUUC  MIAKK  JEMIY
12345  12345  12345  12345
G  EJ  CACHD  IIFC   ABGAH

12341  23412  34123  41234       160
DLISJ  BLCKK  FODEV  DYZQZ
DSKGB  VTJYC  XYLZE  CXLSU
12345  12345  12345  12345
HAM F  G  ND    HFC  OOHEL
```

```
12341  23412                     170
SHCTW  DIEXZ
MVMND  ONFJY
12345  12345
IJGIE   MALH
```

The above table is about 85% reduced and note the idiomorphic repetition ACHDIIFC representing Artillery becomes patent in the reduction process. This is rather exciting. From no patent clues to reduction and latent clues exposed. Clever.

The solution is continued by setting up sequence reconstruction matrices for both messages. The 0 line represents the pseudo-plain text and the values inside the matrix being cipher text.

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

0	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
1	J	H	T	F	G	Y	V	D	M			S			C											
2	S	E	H		U	W	A	Z	I	V			N		X											
3	F		U		C	A	M	L	H				K		B	G										
4	I	T	K	E	S	Z		U	N		A	J	B	Y	Q											
5	G	F	E	C	D	B		Y	J	A		U	M		L											

>From the above we chain out the equivalent primary components used for each message. Having reconstructed the cipher component for each message, the alphabets are aligned, combined and reduced to monoalphabetic terms. After solution of these messages, we find message 1 is a case of direct symmetry with the cipher component based on the keyword HYDRAULIC, and message 2 is a case of indirect symmetry with both components being keyword-mixed sequences based on our favorite keyword QUESTIONABLY. Friedman points out that the keywords are prime to each other (9 vs 11). Primality is not a necessary condition for solution based on this procedure. [FRE7]

The method of Arbitrary Reduction is very powerful and works in other ares besides solving periodic polyalphabetic ciphers. It represents a workable approach where the cryptosystem involves nonrelated, random-mixed secondary alphabets among which no symmetry of any sort exists!

SOLUTION BASED ON INDIRECT SYMMETRY OF A "STAGGER'

Given two messages with group counts nearly identical and two isologous initial fragments which are identical except by one letter (called a 'stagger') we can solve the isologous portions of the messages and recover the primary cipher component by the process of indirect symmetry. Transmission garble usually creates stagger messages. Machine cipher systems sometimes produce these when a word separator is added. Staggers may be progressively larger as further word separators are omitted or added.

Given:

Message A

```
                    *                *
ZFWAY  ITBVX  XWZQV  PEBGS  GGFIZ  TUAMF
RFEQX  PEPPO  PCNBP  QPOTX  VNAIH  HVRXC
NHVGM  FRFSI  ESQMV
    *
```

Message B

```
                    *                 *
ZFWAY  ITBVX  XWZQV  PDRKF  USVAG  XLJKC
NDVPR  OWBRH  YFJMS  HRFVS  BAHWG  ZFAJO
JMFAV  CNDVD  ORZPH  A
       *
```

We note that both messages have the same 16 letter beginnings and that message B is 1 letter longer than message A. Note that the tetragraphs MFRF (29) and (65) are spaced 1 less letter than CNDV at (30) and (66). The D in position 17 of message 2 is the extra letter.

Starting from the E in position 17 of message 1, we superimpose message one over message 2 starting at the R in position 18. [We use a period of 6 because the tetragraph delta equals 36 which factors into 3,4,6 and 9; 6 is confirmed via the message.]

```
5612345612345612345612345612345612345612345612345612345612345612
EBGSGGFIZTUAMFRFEQXPEPPOPCNBPQPOTXVNAIHHVRXCNHVGMFRFSIESQMV
RKFUSVAGXLJKCNDVPROWBRHYFJMSHRFVSBAHWGZFAJOJMFAVCNDVDORZPHA
```

O	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
1-2					B		F	Z						M			P	D		S						X
2-3		S				V		F					H			R			U	L				B		
3-4					P		S									H			D		J	A				
4-5	K						V		O					H	Y		R	J								
5-6	W				R	A							C			F								O		
6-1		K	J			N			G						V	W			Z							

It is fairly easy to align properly the cipher components after the primary cipher component or its equivalent have been recovered, thereby expediting the reduction of the cipher into monoalphabetic terms. Note that B(cipher) of alphabet 2 is under E(cipher) of alphabet 1; V(cipher) of alphabet 3 is under F(cipher) alphabet 2;P(cipher) of alphabet 4 is under E(cipher) of alphabet 1. From this point on solution follows the normal path of reconstruction, keyword recovery and combination of alphabets, reduction to monoalphabetic terms and solution by frequency analysis.

LONG LATENT REPETITIONS

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

FINAL REMARKS REGARDING SOLUTION BY SUPERIMPOSITION

In solving an ordinary repeating-key cipher the first step, ascertaining the length of the period, is a relatively minor consideration. It paves the way for the second step, which consists of allocating the letters of the cryptogram into individual monoalphabetic distributions. The third step is to solve these distributions. The text is transcribed into its periods and written out in successive lines corresponding to the length of the period. The columns of letters as a series belong to the same monoalphabet.

We also can see the letters as transcribed into superimposed periods; in such a case the letters in each column have undergone the same kind of treatment by the same elements (plain and cipher components of the cipher alphabet.)

If we have a case of a very long repeating key and a short message (few cycles in the text) we have a difficult problem. But supposing there were several short cryptograms enciphered by the same key, each message beginning at identical starting points in the key. We can superimpose these messages "in flush depth" or "head on" and know that 1) the letters in the columns belong to the same individual alphabets, 2) and that if there are enough messages (about 25-30 in English), then the frequency distributions applicable to the successive columns of text can be solved - without knowing the length of the key. Any difficulties that may have arisen because we were not able to factor the problem correctly are circumvented. The second step of the normal solution to the problem is by-passed. The assumption of probable initial words of messages and stereotyped beginnings is a powerful method of attack in such situations. Since the superimposed texts in these cases comprise only the beginnings of messages, assumptions of probable words are more easily made than when words are sought in the interior of the messages. Some common introductory words are REQUEST, REFER, ENEMY, WHAT, WHEN, and SEND. High frequency initial digraphs will manifest themselves in the first two columns of the superimposed diagram. The high frequency RE diagram manifests itself in such words as REQUEST, REQUIRE, REFERENCE, REFERRING, REQUISITIONS, REPEAT, RECOMMEND, REPORT, RECONNAISSANCE, REINFORCEMENTS and perhaps REGIMENT. (I assume the military text here.)

This same superimposition principle applies even if the messages start at different initial points, providing the messages can be correctly superimposed, so that the letters which fall in one column really belong to one cipher alphabet. The superimposed messages are said to be "in depth." The chi test may be used to advantage in finding and combining columns of the superimposed diagram which were enciphered by identical keys, thus assisting in the analysis of frequencies of larger samples than were available before the amalgamation. [FRE7]

CONCLUSION

In summary, we have seen that the chaining process between cipher texts applies to the latent characteristics of the cipher components, regardless of the identity of the plain components and regardless whether direct or indirect symmetry is involved in the cryptosystems. The principle of super-imposition ranks as one of the most important principles of cryptanalysis. A pretty impressive tool.

LECTURE 11 SOLUTIONS

Thanks to BOZOL for the quick response and correct too!

11.1 Vigenere. Key= SLEEP. "Any reputable physician will agree..

11.2 Beaufort. Key = SILENCE. "Although every one may not subscribe to ..

11.3 Variant. Key = IMPSHGXW (HINSNOTI). Because of the many pressures... [the correct key is SOLITUDE]

11.4 GRONSFELD. 6-3-8-4-0. "Too much discussion, especially..

11.5 BEAUFORT. Key = OCCUPATION. "Almost every man has a job, many find..

BOZOL reports that the tip did not help him and that the first pass at the key was ORCUPATMON which he mystically came up with organization.

LECTURE 12 PROBLEMS

12.1 Nihilist Substitution

74 46 66 44 79 47 45 37 58 66 37 60 25 54 33 69 78 35 68 27
47 36 28 88 36 60 33 48 43 29 87 35 49 57 76 37 37 88 36 60
33 77 74 50 86 55 47 27 76 45 40 55 56 58 66 78 57 30 94 58
38 26 55 57 59 88 56 79 46 46 66 60 58 55 48 56. (DGGLWLRQ, ends WXEOIW)

12.2 Nihilist Substitution

38 76 54 76 64 76 76 54 74 55 35 76 77 76 47 58 76 85 74 44
65 88 63 74 47 36 95 74 63 44 37 58 57 96 65 36 66 85 74 63
55 79 53 67 57 56 58 64 67 67 56 67 57 74 55 55 57 86 03 43
46 67 73 96 67 39. (ETARVQITCO, ends HSMX)

12.3 PORTA

```
      QLAMU  CHQGO  FTESV  XKEWC  GMXPH
UCLUS WSGXT  EVURH  TMTSU  TKVSQ  GCQCW
LHMDX NUFUE  EFXRF  XPHUN  RGPKC  OXULB
BBCUS IBBHW.  (HAVE)
```

12.4 PORTA

```
      XFXYW  ZJICZ  IBUZN  HJXEA  ACWBE
JOOCZ UPXFQ  BXHFI  CGMAZ  KVQEG  BBCAF
KLLXF BVOUN  TSAYZ  KKXLR  CWAJC  LVVVI
XNBFQ JVWBW  BSWEY  VUNGX  ODFRZ  PTEWO
PJQNH WZPNA  YRCLV  YYWCQ  ULOJB  VK.  (GSRWXERX)
```

12.5 PORTAX

```
      UXCUD  ZMVBA  FWWPV  DIKDO  JISMA
WRBBA YLOYX  AKUXR  JGDCJ  MYAPV  RJWJA
DMUKL KLUAM  KAOEN  YBFCC  IQGFK  QZAA. (PQXKEG)
```

12.6 PORTAX

```
      WWQPE  JBDTM  TMNWH  CTJSW  WKIAC
BJKWL YHBYN  OAKRZ  PDYZM  DIVGB  QKNJP
RNSRU FXWMU  TKMJS  KDNLW  WFHKR  JSCVF
HTJIS JD.  (UHDOLCH)
```

12.7 GROMARK

```
      HPMZU  IBQHI  SDHHH  JKUNC  OYJSC
      24106
RBLOF REXTG  EXAZA  ILAXX  XHFNH  CDUYQ

YUOMQ NVOIN  XYMBR  WAHNT  FGPFB  DOOMA

CWHDH JXTTX  CJIUR  PVMZR  EILDZ  QJJTT

ILNNP TREVL  BQLL. ( tip: UCAUKYKUJK; ends tivpw.)
```

REFERENCES / RESOURCES [updated 30 May 1996]

[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.

[ACM] Association For Computing Machinery, "Codes, Keys and Conflicts: Issues in U.S. Crypto Policy," Report of a Special Panel of ACM U. S. Public Policy Committee (USACM), June 1994.

[ADFG] ASTROLABE, "ADFGVX Cipher - The German Field Cipher of 1918," AS53, The Cryptogram, American Cryptogram Association, 1953.

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

[ALAN] Turing, Alan, "The Enigma", by A. Hodges. Simon and Schuster, 1983.

[ALBA] Alberti, "Treatise De Cifris," Meister Papstlichen, Princeton University Press, Princeton, N.J., 1963.

[ALEX] Alexander, D. A., "Secret codes and Decoding," Padell Book Co., New York, 1945.

[ALGE] MINIMAX, "Introduction To Algebraic Cryptography," FM51, The Cryptogram, American Cryptogram Association, 1951.

[ALKA] al-Kadi, Ibrahim A., Origins of Cryptology: The Arab Contributions, Cryptologia, Vol XVI, No. 2, April 1992, pp. 97-127.

[ALP1] PICCOLA, "Lining Up the Alphabets," AM37, The Cryptogram, American Cryptogram Association, 1937.

[ALP2] PICCOLA, "Recovering a Primary Number Alphabet," JJ37, The Cryptogram, American Cryptogram Association, 1937.

[ALP3] CLEAR SKIES, "Method For Recovering Alphabets," AM46, The Cryptogram, American Cryptogram Association, 1946.

[ALP4] PICCOLA, "Lining Up the Alphabets," AM37, The Cryptogram, American Cryptogram Association, 1937.

[ALP5] MACHIAVELLI,"Recovery of Incomplete Cipher Alphabets," SO78, The Cryptogram, American Cryptogram Association, 1978.

[ALP6] BOZO,"Recovery of Primary Alphabets I," JJ35, The Cryptogram, American Cryptogram Association, 1935.

[ALP7] BOZO,"Recovery of Primary Alphabets II," AS35, The Cryptogram, American Cryptogram Association, 1935.

[ALP8] ZYZZ,"Sinkov - Frequency-Matching," JA93, The Cryptogram, American Cryptogram Association, 1993.

[AMS1] RED E RASER,"AMSCO," ON51, The Cryptogram, American Cryptogram Association, 1951.

[AMS2] PHOENIX,"Computer Column: Amsco Encipherment," SO84, The Cryptogram, American Cryptogram Association, 1984.

[AMS3] PHOENIX,"Computer Column: Amsco Decipherment," MA85, The Cryptogram, American Cryptogram Association, 1985.

[AMS4] PHOENIX,"Computer Column: Amsco Decipherment," MJ85, The Cryptogram, American Cryptogram Association, 1985.

[AMS5] PHOENIX,"Computer Column: Amsco Decipherment," JA85, The Cryptogram, American Cryptogram Association, 1985.

[AND1] Andree, Josephine, "Chips from the Math Log," Mu Alpha Theta, 1966.

[AND2] Andree, Josephine, "More Chips from the Math Log," Mu Alpha Theta, 1970.

[AND3] Andree, Josephine, "Lines from the O.U. Mathematics Letter," Vols. I,II,III, Mu Alpha Theta, 1971, 1971, 1971.

[AND4] Andree, Josephine and Richard V., "RAJA Books: a Puzzle Potpourri," RAJA, 1976.

[AND5] Andree, Josephine and Richard V., "Preliminary Instructors Manual for Solving Ciphers," Project CRYPTO, Univ of Oklahoma, Norman, OK, 1977.

[AND6] Andree, Josephine and Richard V., "Teachers Handbook For Problem Solving and Logical Thinking," Project CRYPTO, Univ of Oklahoma, Norman, OK, 1979.

[AND7] Andree, Josephine and Richard V., "Preliminary Instructors Manual for Cryptarithms," Project CRYPTO, Univ of Oklahoma, Norman, OK, 1976.

[AND8] Andree, Josephine and Richard V., "Sophisticated Ciphers: Problem Solving and Logical Thinking," Project CRYPTO, Univ of Oklahoma, Norman, OK, 1978.

[AND9] Andree, Josephine and Richard V., "Logic Unlocs Puzzles," Project CRYPTO, Univ of Oklahoma, Norman, OK, 1979.

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

[ANK1] Andreassen, Karl, "Cryptology and the Personal Computer, with Programming in Basic," Aegean Park Press, 1986.

[ANK2] Andreassen, Karl, "Computer Cryptology, Beyond Decoder Rings," Prentice-Hall 1988.

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

[ANN1] Anonymous., " Speech and Facsimile Scrambling and Decoding," Aegean Park Press, Laguna Hills, CA, 1981.

[ARI1] OZ,"The Construction of Medium - Difficulty Aristocrats," MA92, The Cryptogram, American Cryptogram Association, 1992.

[ARI2] HELCRYPT,"Use of Consonant Sequences for Aristocrats," ON51, The Cryptogram, American Cryptogram Association, 1951.

[ARI3] HELCRYPT,"Use of Tri-Vowel Sequences for Aristocrats," JJ52, The Cryptogram, American Cryptogram Association, 1952.

[ARI4] AB STRUSE, "Equifrequency Crypts," JF74, The Cryptogram, American Cryptogram Association, 1974.

[ARI5] HOMO SAPIENS,"End-letter Count for Aristocrats," FM45, The Cryptogram, American Cryptogram Association, 1945.

[ARI6] S-Tuck, "Aristocrat Affixes," ON45, The Cryptogram, American Cryptogram Association, 1945.

[ASA] "The Origin and Development of the Army Security Agency 1917 -1947," Aegean Park Press, 1978.

[ASHT] Ashton, Christina, "Codes and Ciphers: Hundreds of Unusual and Secret Ways to Send Messages," Betterway Books, 1988.

[ASIR] Anonymous, Enigma and Other Machines, Air Scientific Institute Report, 1976.

[AUG1] D. A. August, "Cryptography and Exploitation of Chinese Manual Cryptosystems - Part I:The Encoding Problem", Cryptologia, Vol XIII, No. 4, October 1989.

[AUG2] D. A. August, "Cryptography and Exploitation of Chinese Manual Cryptosystems - Part II:The Encrypting Problem", Cryptologia, Vol XIV, No. 1, August 1990.

[AUT1] PICCOLA,"Autokey Encipherment,"DJ36, The Cryptogram, American Cryptogram Association, 1936.

[AUT2] PICCOLA,"More about Autokeys,"FM37, The Cryptogram, American Cryptogram Association, 1937.

[AUT3] ISKANDER,"Converting an Autokey to a Periodic," "JJ50, The Cryptogram, American Cryptogram Association, 1950.

[BAC1] SHMOO,"Quicker Baconian Solutions," ND80, The Cryptogram, American Cryptogram Association, 1980.

[BAC2] XERXES,"Sir Francis Bacon Cipher," AS36, The Cryptogram, American Cryptogram Association, 1936.

[BAC3] AB STRUSE,"Solving a Baconian," JJ48, The Cryptogram, American Cryptogram Association, 1948.

[BAC4] B.NATURAL,"Tri-Bac Cipher," JA69, The Cryptogram, American Cryptogram Association, 1969.

[BAC5] annonomous,"Numerical Baconian," JF62, The Cryptogram, American Cryptogram Association, 1962.

[BAC6] FIDDLE,"Extended Baconian," SO69, The Cryptogram, American Cryptogram Association, 1969.

[BADE] Badeau, J. S. et. al., The Genius of Arab Civilization: Source of Renaissance. Second Edition. Cambridge: MIT Press. 1983.

[BAMF] Bamford, James, "The Puzzle Palace: A Report on America's Most Secret Agency," Boston, Houghton Mifflin, 1982.

[BARB] Barber, F. J. W., "Archaeological Decipherment: A Handbook," Princeton University Press, 1974.

[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.

[BAR3] Barker, Wayne G., "Cryptanalysis of the Hagelin Cryptograph, Aegean Park Press, 1977.

[BAR4] Barker, Wayne G., "Cryptanalysis of the Enciphered Code Problem - Where Additive Method of Encipherment Has Been Used," Aegean Park Press, 1979.

[BAR5] Barker, W., ed., History of Codes and Ciphers in the U.S. Prior To World War I," Aegean Park Press, 1978.

[BAR6] Barker, W., " Cryptanalysis of Shift-Register Generated Stream Cipher Systems," Aegean Park Press, 1984.

[BAR7] Barker, W., ed., History of Codes and Ciphers in the U.S. During the Period between World Wars, Part I, 1919-1929, Aegean Park Press, 1979.

[BAR8] Barker, W., ed., History of Codes and Ciphers in the U.S. During World War I, Aegean Park Press, 1979.

[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.

[BAZE] Bazeries, M. le Capitaine, " Cryptograph a 20 rondelles-alphabets," Compte rendu de la 20e session de l' Association Francaise pour l'Advancement des Scienses, Paris: Au secretariat de l' Association, 1892.

[BEA1] S-TUCK, "Beaufort Auto-key," JJ46, The Cryptogram, American Cryptogram Association, 1946.

[BEA2] PICCOLA, "Beaufort Ciphers," JJ36, The Cryptogram, American Cryptogram Association, 1936.

[BEA3] LEDGE, "Beaufort Fundamentals (Novice Notes)," ND71, The Cryptogram, American Cryptogram Association, 1971.

[BEA4] SI SI, "Comparative Analysis of the Vigenere, Beaufort and Variant Ciphers," JA80, The Cryptogram, American Cryptogram Association, 1980.

[BEA5] O'PSHAW, "Porta, A special Case of Beaufort," MA91, The Cryptogram, American Cryptogram Association, 1991.

[BECK] Becket, Henry, S. A., "The Dictionary of Espionage: Spookspeak into English," Stein and Day, 1986.

[BEES] Beesley, P., "Very Special Intelligence", Doubleday, New York, 1977.

[BENN] Bennett, William, R. Jr., "Introduction to Computer Applications for Non-Science Students," Prentice-Hall, 1976. (Interesting section on monkeys and historical cryptography)

[BIGR] PICCOLA, "Use of Bigram Tests" AS38, The Cryptogram, American Cryptogram Association, 1938.

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

[BLOC] Bloch, Gilbert and Ralph Erskine, "Exploit the Double Encipherment Flaw in Enigma", Cryptologia, vol 10, #3, July 1986, p134 ff. (29)

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

[BODY] Brown, Anthony - Cave, "Bodyguard of Lies", Harper and Row, New York, 1975.

[BOLI] Bolinger, D. and Sears, D., "Aspects of Language," 3rd ed., Harcourt Brace Jovanovich,Inc., New York, 1981.

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

[BOWE] Bowers, William Maxwell, "The Bifid Cipher, Practical Cryptanalysis, II, ACA, 1960.

[BOW1] Bowers, William Maxwell, "The Trifid Cipher," Practical Cryptanalysis, III, ACA, 1961.

[BOW2] Bowers, William Maxwell, "The Digraphic Substitution," Practical Cryptanalysis, I, ACA, 1960.

[BOW3] Bowers, William Maxwell, "Cryptographic ABC'S: Substitution and Transposition Ciphers," Practical Cryptanalysis, IV, ACA, 1967.

[BOWN] Bowen, Russell J., "Scholar's Guide to Intelligence Literature: Bibliography of the Russell J. Bowen Collection," National Intelligence Study Center, Frederick, MD, 1983.

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

[BRAS] Brasspounder, "Language Data - German," MA89, The Cryptogram, American Cryptogram Association, 1989.

[BREN] Brennecke, J., "Die Wennde im U-Boote-Krieg:Ursachen und Folgren 1939 - 1943," Herford, Koehler, 1984.

[BROO] Brook, Maxey, "150 Puzzles in Cryptarithmetic," Dover, 1963.

[BROW] Brownell, George, A. "The Origin and Development of the National Security Agency, Aegean Park Press, 1981.

[BRIG] Brigman,Clarence S., "Edgar Allan Poe's Contribution to Alexander's Weekly Messenger," Davis Press, 1943.

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

[BROG] Broglie, Duc de, Le Secret du roi: Correspondance secrete de Louis XV avec ses agents diplomatiques 1752-1774, 3rd ed. Paris, Calmann Levy, 1879.

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

[BUGS] Anonymous, "Bugs and Electronic Surveillance," Desert Publications, 1976.

[BUON] Buonafalce, Augusto, "Giovan Battista Bellaso E Le Sue Cifre Polialfabetiche," Milano, 1990

[BURL] Burling, R., "Man's Many Voices: Language in Its Cultural Context," Holt, Rinehart & Winston, New York, 1970.

[BWO] "Manual of Cryptography," British War Office, Aegean Park Press, Laguna Hills, Ca. 1989. reproduction 1914.

[CAND] Candela, Rosario, "Isomorphism and its Application in Cryptanalytics, Cardanus Press, NYC 1946.

[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.

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

[CHEC] CHECHEM,"On the Need for a Frequency Counter," AM48, The Cryptogram, American Cryptogram Association, 1948.

[CHOI] Interview with Grand Master Sin Il Choi.,9th DAN, June 25, 1995.

[CHOM] Chomsky, Norm, "Syntactic Structures," The Hague: Mouton, 1957.

[CHUN] Chungkuo Ti-erh Lishih Tangankuan, ed "K'ang-Jih chengmien chanch'ang," Chiangsu Kuchi Ch'upansheh, 1987., pp. 993-1026.

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

[CONS] S-TUCK and BAROKO, "Consonant-Line and Vowel-Line Methods," MA92, The Cryptogram, American Cryptogram Association, 1992.

[CONT] F.R.CARTER,"Chart Showing Normal Contact Percentages," AM53, The Cryptogram, American Cryptogram Association, 1953.

[CON1] S-TUCK."Table of Initial and Second-Letter Contacts," DJ43, The Cryptogram, American Cryptogram Association, 1943.

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

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

[COLF] Collins Gem Dictionary, "French," Collins Clear Type Press, 1979.

[COLG] Collins Gem Dictionary, "German," Collins Clear Type Press, 1984.

[COLI] Collins Gem Dictionary, "Italian," Collins Clear Type Press, 1954.

[COLL] Collins Gem Dictionary, "Latin," Collins Clear Type Press, 1980.

[COLP] Collins Gem Dictionary, "Portuguese," Collins Clear Type Press, 1981.

[COLR] Collins Gem Dictionary, "Russian," Collins Clear Type Press, 1958.

[COLS] Collins Gem Dictionary, "Spanish," Collins Clear Type Press, 1980.

[COPP] Coppersmith, Don.,"IBM Journal of Research and Development 38, 1994.

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

[CREM] Cremer, Peter E.," U-Boat Commander: A Periscope View of The Battle of The Atlantic," New York, Berkley, 1986.

[CRYP] "Selected Cryptograms From PennyPress," Penny Press, Inc., Norwalk, CO., 1985.

[CRY1] NYPHO'S ROBOT, "Cryptometry Simplified," DJ40, FM41, AM41, The Cryptogram, published by the American Cryptogram Association, 1940, 1941, 1941.

[CRY2] AB STRUSE, "Non-Ideomorphic Solutions," AM51, The Cryptogram, published by the American Cryptogram Association, 1951.

[CRY3] MINIMAX, "Problems in Cryptanalysis - A Transposition that cannot be Anagrammed," MA60, The Cryptogram, published by the American Cryptogram Association, 1960.

[CRY4] FAUSTUS, "Science of Cryptanalysis," AS32, The Cryptogram, published by the American Cryptogram Association, 1932.

[CRY5] FAUSTUS, "Science of Cryptanalysis,The " JA91, The Cryptogram, published by the American Cryptogram Association, 1991.

[CRY6] BEAU NED, "Semi-Systems in Crypt-Cracking," FM36, The Cryptogram, published by the American Cryptogram Association, 1936.

[CRY7] Y.NOTT, "Systems Of Systems," ON35, The Cryptogram, published by the American Cryptogram Association, 1935.

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

[CUNE] CHECHACO, "The Decipherment of Cuneiform," JJ33, The Cryptogram, published by the American Cryptogram Association, 1933.

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

[DALT] Dalton, Leroy, "Topics for Math Clubs," National Council of Teachers and Mu Alpha Theta, 1973.

[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.

[DEAC] Deacon, R., "The Chinese Secret Service," Taplinger, New York, 1974.

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

[DELA] Delastelle, F., Cryptographie nouvelle, Maire of Saint-Malo, P. Dubreuil, Paris, 1893.

[DENN] Denning, Dorothy E. R.," Cryptography and Data Security," Reading: Addison Wesley, 1983.

[DEVO] Deavours, Cipher A. and Louis Kruh, Machine Cryptography and Modern Cryptanalysis, Artech, New York, 1985.

[DEV1] Deavours, C. A., "Breakthrough '32: The Polish Solution of the ENIGMA," Aegean Park Press, Laguna Hills, CA, 1988.

[DEV2] Deavours, C. A. and Reeds, J.,"The ENIGMA," CRYPTOLOGIA, Vol I No 4, Oct. 1977.

[DEV3] Deavours, C. A.,"Analysis of the Herbern Cryptograph using Isomorphs," CRYPTOLOGIA, Vol I No 2, April, 1977.

[DEV4] Deavours, C. A., "Cryptographic Programs for the IBM PC," Aegean Park Press, Laguna Hills, CA, 1989.

[DIFF] Diffie, Whitfield," The First Ten Years of Public Key Cryptography," Proceedings of the IEEE 76 (1988): 560-76.

[DIFE] Diffie, Whitfield and M.E. Hellman,"New Directions in Cryptography, IEEE Transactions on Information Theory IT-22, 1976.

[DONI] Donitz, Karl, Memoirs: Ten Years and Twenty Days, London: Weidenfeld and Nicolson, 1959.

[DOUB] TIBEX, " A Short Study in doubles (Word beginning or ending in double letters)," FM43, The Cryptogram, published by the American Cryptogram Association, 1943.

[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.

[EIIC] Ei'ichi Hirose, ",Finland ni okeru tsushin joho," in Showa gunji hiwa: Dodai kurabu koenshu, Vol 1, Dodai kurabu koenshu henshu iinkai, ed., (Toyko: Dodai keizai konwakai, 1987), pp 59-60.

[ELCY] Gaines, Helen Fouche, Cryptanalysis, Dover, New York, 1956. [A text that every serious player should have!]

[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.

[ERSK] Erskine, Ralph, "Naval Enigma: The Breaking of Heimisch and Triton," Intelligence and National Security 3, Jan. 1988.

[EVES] , Howard, "An Introduction to the History of Mathematics, " New York, Holt Rinehart winston, 1964.

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

[FIBO] LOGONE BASETEN, "Use of Fibonacci Numbers in Cryptography," JF69, The Cryptogram, published by the American Cryptogram Association, 1969.

[FING] HELCRYPT, "Cryptography in Fingerprinting," FM51, The Cryptogram, published by the American Cryptogram Association, 1951.

[FL] Anonymous, The Friedman Legacy: A Tribute to William and Elizabeth Friedman, National Security Agency, Central Security Service, Center for Cryptological History,1995.

[FLI1] Flicke, W. F., "War Secrets in the Ether - Volume I," Aegean Park Press, Laguna Hills, CA, 1977.

[FLIC] Flicke, W. F., "War Secrets in the Ether - Volume II," Aegean Park Press, Laguna Hills, CA, 1977.

[FLIC] Flicke, W. F., "War Secrets in the Ether," Aegean Park Press, Laguna Hills, CA, 1994.

[FORE] DELAC, "Solving a Foreign Periodic by Lining Up the Alphabets," JJ46, The Cryptogram, published by the American Cryptogram Association, 1946.

[FOWL] Fowler, Mark and Radhi Parekh, " Codes and Ciphers, - Advanced Level," EDC Publishing, Tulsa OK, 1994. (clever and work)

[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.

[FRAN] Franks, Peter, "Calculator Ciphers," Information Associates, Champaign, Il. 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.

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

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

[FRSG] Friedman, William F., "Solving German Codes in World War I, " Aegean Park Press, Laguna Hills, CA, 1977.

[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.

[FR7] Friedman, William F. and Callimahos, Lambros D., Military Cryptanalytics Part II - Volume 1, Aegean Park Press, Laguna Hills, CA, 1985.

[FR8] Friedman, William F. and Callimahos, Lambros D., Military Cryptanalytics Part II - Volume 2, Aegean Park Press, Laguna Hills, CA, 1985.

[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.

[FRS6] Friedman, W. F., "Six Lectures On Cryptology," National Archives, SRH-004.

[FR8] Friedman, W. F., "Cryptography and Cryptanalysis Articles," Aegean Park Press, Laguna Hills, CA, 1976.

[FR9] Friedman, W. F., "History of the Use of Codes," Aegean Park Press, Laguna Hills, CA, 1977.

[FRZM] Friedman, William F.,and Charles J. Mendelsohn, "The Zimmerman Telegram of January 16, 1917 and its Cryptographic Background," Aegean Park Press, Laguna Hills, CA, 1976.

[FROM] Fromkin, V and Rodman, R., "Introduction to Language," 4th ed.,Holt Reinhart & Winston, New York, 1988.

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

[FUMI] Fumio Nakamura, Rikugun ni okeru COMINT no hoga to hatten," The Journal of National Defense, 16-1 (June 1988) pp85 - 87.

[GAJ] Gaj, Krzysztof, "Szyfr Enigmy: Metody zlamania," Warsaw Wydawnictwa Komunikacji i Lacznosci, 1989.

[GAR1] Gardner, Martin, "536 Puzzles and Curious Problems," Scribners, 1967.

[GAR2] Gardner, Martin, "Mathematics, Magic, and Mystery ," Dover, 1956.

[GAR3] Gardner, Martin, "New Mathematical Diversions from Scientific American," Simon and Schuster, 1966.

[GAR4] Gardner, Martin, "Sixth Book of Mathematical Games from Scientific American," Simon and Schuster, 1971.

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

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

[GAR2] Garlinski, Jozef, 'The Enigma War', New York, Scribner, 1979.

[GE] "Security," General Electric, Reference manual Rev. B., 3503.01, Mark III Service, 1977.

[GERH] Gerhard, William D., "Attack on the U.S., Liberty," SRH-256, Aegean Park Press, 1981.

[GERM] "German Dictionary," Hippocrene Books, Inc., New York, 1983.

[GILE] Giles, Herbert A., "Chinese Self-Taught," Padell Book Co., New York, 1936?

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

[GLEN] Gleason, Norma, "Fun With Codes and Ciphers Workbook," Dover, New York, 1988.

[GLE1] Gleason, Norma, "Cryptograms and Spygrams," Dover, New York, 1981.

[GLEA] Gleason, A. M., "Elementary Course in Probability for the Cryptanalyst," Aegean Park Press, Laguna Hills, CA, 1985.

[GLOV] Glover, D. Beaird, "Secret Ciphers of the 1876 Presidential Election," Aegean Park Press, Laguna Hills, CA, 1991.

[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.

[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

[GRAH] Graham, L. A., "Ingenious Mathematical Problems and Methods," Dover, 1959.

[GRAN] Grant, E. A., "Kids Book of Secret Codes, Signals and Ciphers, Running Press, 1989.

[GRAP] DR. CRYPTOGRAM,"The Graphic Position Chart (On Aristocrats)," JF59, The Cryptogram, American Cryptogram Association, 1959.

[GREU] Greulich, Helmut, "Spion in der Streichholzschachtel: Raffinierte Methoden der Abhortechnik, Gutersloh: Bertelsmann, 1969.

[GRI1] ASAP,"An Aid For Grille Ciphers," SO93, The Cryptogram, American Cryptogram Association, 1993.

[GRI2] DUN SCOTUS,"Binary Number Grille," JA60, The Cryptogram, American Cryptogram Association, 1960.

[GRI3] S-TUCK,"Grille Solved By the Tableaux Method," DJ42, The Cryptogram, American Cryptogram Association, 1942.

[GRI4] The SQUIRE,"More About Grilles," ON40,DJ40, The Cryptogram, American Cryptogram Association, 1940, 1940.

[GRI5] OMAR,"Rotating Grille Cipher," FM41, The Cryptogram, American Cryptogram Association, 1941.

[GRI6] S-TUCK,"Solving The Grille. A New Tableaux Method," FM44, The Cryptogram, American Cryptogram Association, 1944.

[GRI7] LABRONICUS,"Solving The Turning Grille," JF88, The Cryptogram, American Cryptogram Association, 1988.

[GRI8] BERYL,"The Turning Grille," ND92, The Cryptogram, American Cryptogram Association, 1992.

[GRI9] SHERLAC and S-TUCKP,"Triangular Grilles," ON45, The Cryptogram, American Cryptogram Association, 1945.

[GRIA] SHERLAC,"Turning Grille," ON49, The Cryptogram, American Cryptogram Association, 1949.

[GRIB] DUN SCOTUS,"Turning (by the numbers)," SO61, The Cryptogram, American Cryptogram Association, 1961.

[GRIC] LEDGE,"Turning Grille (Novice Notes)," JA77, The Cryptogram, American Cryptogram Association, 1977.

[GRO1] DENDAI, DICK," Analysis of Gromark Special,"ND74, The Cryptogram, American Cryptogram Association, 1974.

[GRO2] BERYL," BERYL'S Pearls: Gromark Primers by hand calculator," ND91, The Cryptogram, American Cryptogram Association, 1991.

[GRO3] MARSHEN," Checking the Numerical Key,"JF70, The Cryptogram, American Cryptogram Association, 1970.

[GRO4] PHOENIX," Computer Column: Gronsfeld -> Gromark," "MJ90, The Cryptogram, American Cryptogram Association, 1990.

[GRO5] PHOENIX," Computer Column: Perodic Gromark," MJ90 The Cryptogram, American Cryptogram Association, 1990.

[GRO6] ROGUE," Cycles for Gromark Running Key," JF75, The Cryptogram, American Cryptogram Association, 1975.

[GRO7] DUMBO," Gromark Cipher," MA69, JA69, The Cryptogram, American Cryptogram Association, 1969.

[GRO8] DAN SURR," Gromark Club Solution," MA75, The Cryptogram, American Cryptogram Association, 1975.

[GRO9] B.NATURAL," Keyword Recovery in Periodic Gromark," SO73, The Cryptogram, American Cryptogram Association, 1973.

[GROA] D.STRASSE," Method For Determining Term of Key," MA75, The Cryptogram, American Cryptogram Association, 1975.

[GROB] CRUX," More On Gromark Keys," ND87, The Cryptogram, American Cryptogram Association, 1987.

[GROC] DUMBO," Periodic Gromark ," MA73, The Cryptogram, American Cryptogram Association, 1973.

[GROD] ROGUE," Periodic Gromark ," SO73, The Cryptogram, American Cryptogram Association, 1973.

[GROE] ROGUE," Theoretical Frequencies in the Gromark," MA74, The Cryptogram, American Cryptogram Association, 1974.

[GRON] R.L.H., "Condensed Analysis of a Gronsfeld," AM38, ON38,The Cryptogram, American Cryptogram Association, 1938,1938.

[GRN1] CHARMER, "Gronsfeld," AS44, The Cryptogram, American Cryptogram Association, 1944.

[GRN2] PICCOLA, "Gronsfeld Cipher," ON35, The Cryptogram, American Cryptogram Association, 1935.

[GRN3] S-TUCK, "Gronsfeld Cipher," AS44, The Cryptogram, American Cryptogram Association, 1944.

[GROU] Groueff, Stephane, "Manhattan Project: The Untold Story of the Making of the Atom Bomb," Little, Brown and Company,1967.

[GUST] Gustave, B., "Enigma:ou, la plus grande 'enigme de la guerre 1939-1945." Paris:Plon, 1973.

[GYLD] Gylden, Yves, "The Contribution of the Cryptographic Bureaus in the World War," Aegean Park Press, 1978.

[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.

[HAFT] Haftner, Katie and John Markoff, "Cyberpunk," Touchstine, 1991.

[HAGA] Hagamen,W. D. et. al., "Encoding Verbal Information as Unique Numbers," IBM Systems Journal, Vol 11, No. 4, 1972.

[HAWA] Hitchcock, H. R., "Hawaiian," Charles E. Tuttle, Co., Toyko, 1968.

[HAWC] Hawcock, David and MacAllister, Patrick, "Puzzle Power! Multidimensional Codes, Illusions, Numbers, and Brainteasers," Little, Brown and Co., New York, 1994.

[HEBR] COMET, "First Hebrew Book (of Cryptology)," JF72, The Cryptogram, published by the American Cryptogram Association, 1972.

[HELD] , Gilbert, "Top Secret Data Encryption Techniques," Prentice Hall, 1993. (great title..limited use)

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

[HEPP] Hepp, Leo, "Die Chiffriermaschine 'ENIGMA'", F-Flagge, 1978.

[HIDE] Hideo Kubota, " Zai-shi dai-go kokugun tokushu joho senshi." unpublished manuscript, NIDS.

[HIER] ISHCABIBEL, "Hieroglyphics: Cryptology Started Here, MA71, The Cryptogram, American Cryptogram Association, 1971.

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

[HIL1] Hill, L. S. 1929. Cryptography in an Algebraic Alphabet. American Mathematical Monthly. 36:306-312.

[HIL2] Hill, L. S. 1931. Concerning the Linear Transformation Apparatus in Cryptography. American Mathematical Monthly. 38:135-154.

[HINS] Hinsley, F. H., "History of British Intelligence in the Second World War", Cambridge University Press, Cambridge, 1979-1988.

[HIN2] Hinsley, F. H. and Alan Strip in "Codebreakers -Story of Bletchley Park", Oxford University Press, 1994.

[HIN3] Hinsley, F. H., et. al., "British Intelligence in The Second World War: Its Influence on Strategy and Operations," London, HMSO vol I, 1979, vol II 1981, vol III, 1984 and 1988.

[HISA] Hisashi Takahashi, "Military Friction, Diplomatic Suasion in China, 1937 - 1938," The Journal of International Studies, Sophia Univ, Vol 19, July, 1987.

[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.

[HODG] Hodges, Andrew, "Alan Turing: The Enigma," New York, Simon and Schuster, 1983.

[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.)

[HOF1] Hoffman, Lance. J., et. al.," Cryptography Policy," Communications of the ACM 37, 1994, pp. 109-17.

[HOLM Holmes, W. J., "Double-Edged Secrets: U.S. Naval Intelligence Operations in the Pacific During WWII", Annapolis, MD: Naval Institute Press, 1979.

[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.

[HYDE] H. Montgomery Hyde, "Room 3603, The Story of British Intelligence Center in New York During World War II", New York, Farrar, Straus, 1963.

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

[IC1] GIZMO, "Bifid Period Determination Using a Digraphic Index of Coincidence, JF79, The Cryptogram, American Cryptogram Association, 1979.

[IC2] PHOENIX, "Computer Column: Applications of the Index of Coincidence, JA90, The Cryptogram, American Cryptogram Association, 1990.

[IC3] PHOENIX, "Computer Column: Digraphic Index of Coincidence, ND90, The Cryptogram, American Cryptogram Association, 1990.

[IC4] PHOENIX, "Computer Column: Index of Coincidence (IC), JA82, The Cryptogram, American Cryptogram Association, 1982.

[IC5] PHOENIX, "Computer Column: Index of Coincidence, (correction) MA83, The Cryptogram, American Cryptogram Association, 1983.

[IMPE] D'Imperio, M. E, " The Voynich Manuscript - An Elegant Enigma," Aegean Park Press, Laguna Hills, CA, 1976.

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

[ITAL] Italian - English Dictionary, compiled by Vittore E. Bocchetta, Fawcett Premier, New York, 1965.

[JAPA] Martin, S.E., "Basic Japanese Conversation Dictionary," Charles E. Tuttle Co., Toyko, 1981.

[JAPH] "Operational History of Japanese Naval Communications, December 1941- August 1945, Monograph by Japanese General Staff and War Ministry, Aegean Park Press, 1985.

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

[KADI] al-Kadi, Ibrahim A., Cryptography and Data Security: Cryptographic Properties of Arabic, Proceedings of the Third Saudi Engineering Conference. Riyadh, Saudi Arabia: Nov 24-27, Vol 2:910-921., 1991.

[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.

[KAH2] Kahn, David, "An Enigma Chronology", Cryptologia Vol XVII,Number 3, July 1993.

[KAH3] Kahn, David, "Seizing The Enigma: The Race to Break the German U-Boat Codes 1939-1943 ", Houghton Mifflin, New York, 1991.

[KARA] Karalekas, Anne, "History of the Central Intelligence Agency," Aegean Park Press, Laguna Hills, CA, 1977.

[KASI] Kasiski, Major F. W. , "Die Geheimschriften und die Dechiffrir-kunst," Schriften der Naturforschenden Gesellschaft in Danzig, 1872.

[KAS1] Bowers, M. W., {ZEMBIE} "Major F. W. Kasiski - Cryptologist," The Cryptogram, XXXI, JF, 1964.

[KAS2] ----, "Kasiski Method," JF64,MA64, The Cryptogram, American Cryptogram Association, 1964.

[KAS3] PICCOLA, "Kasiski Method for Periodics," JJ35,AS35, The Cryptogram, American Cryptogram Association, 1935, 1935.

[KAS4] AB STRUSE, "Who was Kasiski?" SO76, The Cryptogram, American Cryptogram Association, 1976.

[KATZ] Katzen, Harry, Jr., "Computer Data Security,"Van Nostrand Reinhold, 1973.

[KERC] Kerckhoffs, "la Cryptographie Militaire, " Journel des Sciences militaires, 9th series, IX, (January and February, 1883, Libraire Militaire de L. Baudoin &Co., Paris. English trans. by Warren T, McCready of the University of Toronto, 1964

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

[KONH] Konheim, Alan G., "Cryptography -A Primer" , John Wiley, 1981, pp 212 ff.

[KORD] Kordemsky, B., "The Moscow Puzzles," Schribners, 1972.

[KOTT] Kottack, Phillip Conrad, "Anthropology: The Exploration Of Human Diversity," 6th ed., McGraw-Hill, Inc., New York, N.Y. 1994.

[KOZA] Kozaczuk, Dr. Wladyslaw, "Enigma: How the German Machine Cipher was Broken and How it Was Read by the Allies in WWI", University Pub, 1984.

[KRAI] Kraitchek, "Mathematical Recreations," Norton, 1942, and Dover, 1963.

[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.

[LAI] Lai, Xuejia, "On the Design and Security of Block Ciphers," ETH Series in Information Processing 1, 1992. (Article defines the IDEA Cipher)

[LAIM] Lai, Xuejia, and James L. Massey, "A Proposal for a New Block Encryption Standard," Advances in Cryptology -Eurocrypt 90 Proceedings, 1992, pp. 55-70.

[LAKE] Lakoff, R., "Language and the Women's Place," Harper & Row, New York, 1975.

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

[LAN1] Langie, Andre, "Cryptography - A Study on Secret Writings", Aegean Park Press, Laguna Hills, CA. 1989.

[LAN2] Langie, Andre, and E. A. Soudart, "Treatise on Cryptography, " Aegean Park Press, Laguna Hills, CA. 1991.

[LATI] BRASSPOUNDER, "Latin Language Data, "The Cryptogram," July-August 1993.

[LAUE] Lauer, Rudolph F., "Computer Simulation of Classical Substitution Cryptographic Systems" Aegean Park Press, 1981, p72 ff.

[LEAR] Leary, Penn, " The Second Cryptographic Shakespeare," Omaha, NE [from author] 1994.

[LEA1] Leary, Penn, " Supplement to The Second Cryptographic Shakespeare," Omaha, NE [from author] 1994.

[LEAU] Leaute, H., "Sur les Mecanismes Cryptographiques de M. de Viaris," Le Genie Civil, XIII, Sept 1, 1888.

[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!]

[LENS] Lenstra, A.K. et. al. "The Number Field Sieve," Proceedings of the 22 ACM Symposium on the Theory of Computing," Baltimore, ACM Press, 1990, pp 564-72.

[LEN1] Lenstra, A.K. et. al. "The Factorization of the Ninth Fermat Number," Mathematics of Computation 61 1993, pp. 319-50.

[LEWF] Lewis, Frank, "Problem Solving with Particular Reference to the Cryptic (or British) Crossword and other 'American Puzzles', Part One," by Frank Lewis, Montserrat, January 1989.

[LEW1] Lewis, Frank, "The Nations Best Puzzles, Book Six," by Frank Lewis, Montserrat, January 1990.

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

[LEW1] Lewin, Ronald, 'The American Magic - Codes, ciphers and The Defeat of Japan', Farrar Straus Giroux, 1982.

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

[LEVI] Levine, J., U.S. Cryptographic Patents 1861-1981, Cryptologia, Terre Haute, In 1983.

[LEV1] Levine, J. 1961. Some Elementary Cryptanalysis of Algebraic Cryptography. American Mathematical Monthly. 68:411-418

[LEV2] Levine, J. 1961. Some Applications of High-Speed Computers to the Case n =2 of Algebraic Cryptography. Mathematics of Computation. 15:254-260

[LEV3] Levine, J. 1963. Analysis of the Case n =3 in Algebraic Cryptography With Involuntary Key Matrix With Known Alphabet. Journal fuer die Reine und Angewante Mathematik. 213:1-30.

[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.

[LYN1] Lynch, Frederick D., "An Approach To Cryptarithms," ACA, 1976.

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

[MACI] Macintyre, D., "The Battle of the Atlantic," New York, Macmillan, 1961.

[MADA] Madachy, J. S., "Mathematics on Vacation," Scribners, 1972.

[MAGN] Magne, Emile, Le plaisant Abbe de Boisrobert, Paris, Mecure de France, 1909.

[MANN] Mann, B.,"Cryptography with Matrices," The Pentagon, Vol 21, Fall 1961.

[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 a 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.

[MAST] Lewis, Frank W., "Solving Cipher Problems - Cryptanalysis, Probabilities and Diagnostics," Aegean Park Press, Laguna Hills, CA, 1992.

[MAU] Mau, Ernest E., "Word Puzzles With Your Microcomputer," Hayden Books, 1990.

[MAVE] Mavenel, Denis L., Lettres, Instructions Diplomatiques et Papiers d' Etat du Cardinal Richelieu, Historie Politique, Paris 1853-1877 Collection.

[MAYA] Coe, M. D., "Breaking The Maya Code," Thames and Hudson, New York, 1992.

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

[MELL] Mellen G. 1981. Graphic Solution of a Linear Transformation Cipher. Cryptologia. 5:1-19.

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

[MERK] Merkle, Ralph, "Secrecy, Authentication and Public Key Systems," Ann Arbor, UMI Research Press, 1982.

[MER1] Merkle, Ralph, "Secure Communications Over Insecure Channels," Communications of the ACM 21, 1978, pp. 294-99.

[MER2] Merkle, Ralph and Martin E. Hellman, "On the Security of Multiple Encryption ," Communications of the ACM 24, 1981, pp. 465-67.

[MER3] Merkle, Ralph and Martin E. Hellman, "Hiding Information and Signatures in Trap Door Knapsacks," IEEE Transactions on Information Theory 24, 1978, pp. 525-30.

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

[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.

[MRAY] Mrayati, Mohammad, Yahya Meer Alam and Hassan al-Tayyan., Ilm at-Ta'miyah wa Istikhraj al-Mu,amma Ind al-Arab. Vol 1. Damascus: The Arab Academy of Damascus., 1987.

[MULL] Mulligan, Timothy," The German Navy Examines its Cryptographic Security, Oct. 1941, Military affairs, vol 49, no 2, April 1985.

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

[NBS] National Bureau of Standards, "Data Encryption Standard," FIPS PUB 46-1, 1987.

[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.

[NICX] Nichols, R. K., Keynote Speech to A.C.A. Convention, "Breaking Ciphers in Other Languages.," New Orleans, La., 1993.

[NICK] Nickels, Hamilton, "Codemaster: Secrets of Making and Breaking Codes," Paladin Press, Boulder, CO., 1990.

[NIHL] PHOENIX," Computer Column: Nihilist Substitution," MA88, The Cryptogram, American Cryptogram Association, 1988.

[NIH1] PHOENIX," Computer Column: Nihilist Substitution," MJ88, The Cryptogram, American Cryptogram Association, 1988.

[NIH2] PHOENIX," Computer Column: Nihilist Substitution," JA88, The Cryptogram, American Cryptogram Association, 1988.

[NIH3] PHOENIX," Computer Column: Nihilist Substitution," JA89, The Cryptogram, American Cryptogram Association, 1989.

[NIH4] FIDDLE and CLEAR SKYS," FIDDLE'S slide for Nihilist Number Substitution," ON48, The Cryptogram, American Cryptogram Association, 1948.

[NIH5] RIG R. MORTIS," Mixed Square Nihilist," JA60, The Cryptogram, American Cryptogram Association, 1960.

[NIH6] PICCOLA," Nihilist Number Cipher," AS37, The Cryptogram, American Cryptogram Association, 1937.

[NIH7] PICCOLA," Nihilist Transposition," DJ38, The Cryptogram, American Cryptogram Association, 1938.

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

[NORW] Marm, Ingvald and Sommerfelt, Alf, "Norwegian," Teach Yourself Books, Hodder and Stoughton, London, 1967.

[NSA] NSA's Friedman Legacy - A Tribute to William and Elizabeth Friedman, NSA Center for Cryptological

[NSA1] NMasked Dispatches: Cryptograms and Cryptology in American History, 1775 -1900. Series 1, Pre World War I Volume I, National Security Agency, Central Security Service, NSA Center for Cryptological History, 1993.

[OHAV] OHAVER, M. E., "Solving Cipher Secrets," Aegean Park Press, 1989.

[OHA1] OHAVER, M. E., "Cryptogram Solving," Etcetera Press, 1973.

[OKLA] Andre, Josephine and Richard V. Andree, "Cryptarithms," Unit One, Problem Solving and Logical Thinking, University of Oklahoma, Norman, Ok. Copy No: 486, 1976.

[OKLI] Andre, Josephine and Richard V. Andree, " Instructors Manual For Cryptarithms," Unit One, Problem Solving and Logical Thinking, University of Oklahoma, Norman, Ok. Copy No: 486, 1976.

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

[OTA] "Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information," Office of Technology Assessment, 1988.

[OZK] OZ,"Variation in Letter Frequency with Cipher Length or Where Did All Those K's Come From? ," SO59, The Cryptogram, American Cryptogram Association, 1959.

[PEAR] "Pearl Harbor Revisited," U.S. Navy Communications Intelligence, 1924-1941, U.S. Cryptological History Series, Series IV, World War II, Volume 6, NSA CSS , CH-E32-94-01, 1994.

[PECK] Peck, Lyman C., "Secret Codes, Remainder Arithmetic, and Matrices," National Counsil of Teachers of Mathematics, Washington, D.C. 1971.

[PERR] Perrault, Charles, Tallement des Reaux, Les Historiettes, Bibliotheque del La Pleiade, Paris 1960, pp 256-258.

[PGP] Garfinkel, Simson, "PGP: Pretty Good Privacy," O'reilly and Associates, Inc. Sebastopol, CA. 1995.

[PHL] PHIL,"System Identification by General Frequencies," AM48, The Cryptogram, American Cryptogram Association, 1948.

[PHIL] Phillips, H., "My Best Puzzles in Logic and Reasoning," Dover, 1961.

[PIER] Pierce, Clayton C., "Cryptoprivacy", 325 Carol Drive, Ventura, Ca. 93003, 1994.

[PIE1] Pierce, Clayton C., "Privacy, Cryptography, and Secure Communication ", 325 Carol Drive, Ventura, Ca. 93003, 1977.

[POLY] Polya, G., "Mathematics and Plausible Reasoning," Princeton Press, 1954.

[POL1] Polya, G., "How To Solve It.," Princeton Press, 1948.

[POPE] Pope, Maurice, "The Story of Decipherment: From Egyptian Hieroglyphic to Linear B., Thames and Hudson Ltd., 1975.

[PORT] Barker, Wayne G. "Cryptograms in Portuguese," Aegean Park Press, Laguna Hills, CA., 1986.

[POR1] Aliandro, Hygino, "The Portuguese-English Dictionary," Pocket Books, New York, N.Y., 1960.

[POUN] Poundstone, William, "Biggest Secrets," Quill Publishing, New York, 1993. (Explodes the Beale Cipher Hoax.)

[PRIC] Price, A.,"Instruments of Darkness: the History of Electronic Warfare, London, Macdonalds and Janes, 1977.

[PROT] "Protecting Your Privacy - A Comprehensive Report On Eavesdropping Techniques and Devices and Their Corresponding Countermeasures," Telecommunications Publishing Inc., 1979.

[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.

[RAND] Randolph, Boris, "Cryptofun," Aegean Park Press, 1981.

[RB1] Friedman, William F., The Riverbank Publications, Volume 1," Aegean Park Press, 1979.

[RB2] Friedman, William F., The Riverbank Publications, Volume 2," Aegean Park Press, 1979.

[RB3] Friedman, William F., The Riverbank Publications, Volume 3," Aegean Park Press, 1979.

[REJE] Rejewski, Marian, "Mathematical Solution of the Enigma Cipher" published in vol 6, #1, Jan 1982 Cryptologia pp 1-37.

[RELY] Relyea, Harold C., "Evolution and Organization of Intelligence Activities in the United States," Aegean Park Press, 1976.

[RENA] Renauld, P. "La Machine a' chiffrer 'Enigma'", Bulletin Trimestriel de l'association des Amis de L'Ecole superieure de guerre no 78, 1978.

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

[RIVE] Rivest, Ron, "Ciphertext: The RSA Newsletter 1, 1993.

[RIV1] Rivest, Ron, Shamir, A and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Communications of the ACM 21, 1978.

[ROAC] Roach, T., "Hobbyist's Guide To COMINT Collection and Analysis," 1330 Copper Peak Lane, San Jose, Ca. 95120- 4271, 1994.

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

[ROHE] Jurgen Rohwer's Comparative Analysis of Allied and Axis Radio-Intelligence in the Battle of the Atlantic, Proceedings of the 13th Military History Symposium, USAF Academy, 1988, pp 77-109.

[ROHW] Rohwer Jurgen, "Critical Convoy Battles of March 1943," London, Ian Allan, 1977.

[ROH1] Rohwer Jurgen, "Nachwort: Die Schlacht im Atlantik in der Historischen Forschung, Munchen: Bernard and Graefe, 1980.

[ROH2] Rohwer Jurgen, et. al. , "Chronology of the War at Sea, Vol I, 1939-1942, London, Ian Allan, 1972.

[ROH3] Rohwer Jurgen, "U-Boote, Eine Chronik in Bildern, Oldenburs, Stalling, 1962. Skizzen der 8 Phasen.

[ROOM] Hyde, H. Montgomery, "Room 3603, The Story of British Intelligence Center in New York During World War II", New York, Farrar, Straus, 1963.

[ROSE] Budge, E. A. Wallis, "The Rosetta Stone," British Museum Press, London, 1927.

[RSA] RSA Data Security, Inc., "Mailsafe: Public Key Encryption Software Users Manual, Version 5.0, Redwood City, CA, 1994

[RUNY] Runyan, T. J. and Jan M. Copes "To Die Gallently", Westview Press 1994, p85-86 ff.

[RYP1] A B C, "Adventures in Cryptarithms (digital maze)," JA63, The Cryptogram, published by the American Cryptogram Association, 1963.

[RYP2] CROTALUS "Analysis of the Classic Cryptarithm,"MA73, The Cryptogram, published by the American Cryptogram Association, 1973.

[RYP3] CLEAR SKIES "Another Way To Solve Cryptarithms,"DJ44, The Cryptogram, published by the American Cryptogram Association, 1944.

[RYP4] CROTALUS "Arithemetic in Other Bases (Duodecimal table),"JF74, The Cryptogram, published by the American Cryptogram Association, 1974.

[RYP5] LEDGE, "Basic Patterns in Base Eleven and Twelve Arithmetic,"SO77, ND77, The Cryptogram, published by the American Cryptogram Association, 1977,1977.

[RYP6] COMPUTER USER, "Computer Solution of Cryptarithms," JF72, The Cryptogram, published by the American Cryptogram Association, 1972.

[RYP7] PIT, "Cryptarithm Crutch," JA80, The Cryptogram, published by the American Cryptogram Association, 1980.

[RYP8] DENDAI, DICK, "Cryptarithm Ccub root," ND76, The Cryptogram, published by the American Cryptogram Association, 1976.

[RYP9] S-TUCK, "Cryptarithm in Addition," AM44, The Cryptogram, published by the American Cryptogram Association, 1944.

[RYPA] APEX DX, "Cryptarithm Line of Attack," ND91, The Cryptogram, published by the American Cryptogram Association, 1991.

[RYPB] HUBBUBBER and CROTALUS, "Cryptarithm Observations," ND73, The Cryptogram, published by the American Cryptogram Association, 1973.

[RYPC] CROTALUS, "Cryptarithms and Notation," JF73, The Cryptogram, published by the American Cryptogram Association, 1973.

[RYPD] JUNKERL, "Cryptarithms: The digital root method," AS43, The Cryptogram, published by the American Cryptogram Association, 1943.

[RYPE] CROTALUS, "Divisibility by Eleven," ND89, The Cryptogram, published by the American Cryptogram Association, 1989.

[RYPF] S-TUCK, "Double Key Division," JJ43, The Cryptogram, published by the American Cryptogram Association, 1943.

[RYPG] NEOTERIC, "Duo-Decimal Cryptarithms," AM40, The Cryptogram, published by the American Cryptogram Association, 1940.

[RYPH] QUINTUPLEX, "Duo-Decimal Cryptarithms," JJ40, The Cryptogram, published by the American Cryptogram Association, 1940.

[RYPI] FIDDLE, "Exhausitive for Three," JF59, The Cryptogram, published by the American Cryptogram Association, 1959.

[RYPJ] ---, "Finding the Zero In Cryptarithms," DJ42, The Cryptogram, published by the American Cryptogram Association, 1942.

[RYPK] FILM-D, "Greater than Less than Diagram for Cryptarithms," DJ51, The Cryptogram, published by the American Cryptogram Association, 1951.

[RYPL] MI TI TI, "Introduction To Cryptarithms," SO63, The Cryptogram, published by the American Cryptogram Association, 1963.

[RYPM] FORMALHUT, "Leading Digit Analysis in Cryptarithms," JA91, The Cryptogram, published by the American Cryptogram Association, 1991.

[RYPN] CROTALUS, "Make Your Own Arithmetic Tables In Other Bases," MJ89, The Cryptogram, published by the American Cryptogram Association, 1989.

[RYPO] BACEDI, "Method for Solving Cryptarithms," JF78, The Cryptogram, published by the American Cryptogram Association, 1978.

[RYPP] SHERLAC, "More on Cryptarithms," DJ44, The Cryptogram, published by the American Cryptogram Association, 1944.

[RYPQ] FIRE-O, "Multiplicative Structures," MJ70, The Cryptogram, published by the American Cryptogram Association, 1970.

[RYPR] CROTALUS, "Solving A Division Cryptarithm," JA73, The Cryptogram, published by the American Cryptogram Association, 1973.

[RYPS] CROTALUS, "Solving A Multiplication Cryptarithm," MJ73, The Cryptogram, published by the American Cryptogram Association, 1973.

[RYPT] PHOENIX, "Some thoughts on Solving Cryptarithms," SO87, The Cryptogram, published by the American Cryptogram Association, 1987.

[RYPU] CROTALUS, "Square Root Cryptarithms," SO73, The Cryptogram, published by the American Cryptogram Association, 1973.

[RYPV] FIDDLE, "Theory of Duplicated Digital Figures," JJ53, The Cryptogram, published by the American Cryptogram Association, 1953.

[RYPW] FIDDLE, "Theory of Three Unlike Digital Figures," AS52, The Cryptogram, published by the American Cryptogram Association, 1952.

[RYPX] CROTALUS, "Unidecimal Tabless," MJ73, The Cryptogram, published by the American Cryptogram Association, 1973.

[RYSK] Norbert Ryska and Siegfried Herda, "Kryptographische Verfahren in der Datenverarbeitung," Gesellschaft fur Informatik, Berlin, Springer-Verlag1980.

[SADL] Sadler, A. L., "The Code of the Samurai," Rutland and Tokyo: Charles E. Tuttle Co., 1969.

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

[SALE] Salewski, Michael, "Die Deutscher Seekriegsleitung, 1938- 1945, Frankfurt/Main: Bernard and Graefe, 1970-1974. 3 volumes.

[SANB] Sanbohonbu, ed., "Sanbohonbu kotokan shokuinhyo." NIDS Archives.

[SAPR] Sapir, E., "Conceptual Categories in Primitive Language," Science: 74: 578-584., 1931.

[SASS] Sassoons, George, "Radio Hackers Code Book", Duckworth, London, 1986.

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

[SCH2] Schneier, Bruce, "Applied Cryptography: Protocols, Algorithms, and Source Code C," 2nd ed., John Wiley and Sons, 1995.

[SCHU] Schuh, fred, "Master Book of Mathematical Recreation," Dover, 1968.

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

[SEBE] Seberry, Jennifer and Joseph Pieprzyk, "Cryptography: An Introduction to Computer Security," Prentice Hall, 1989. [CAREFUL! Lots of Errors - Basic research efforts may be flawed - see Appendix A pg 307 for example.]

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

[SHIN] Shinsaku Tamura, "Myohin kosaku," San'ei Shuppansha, Toyko, 1953.

[SHUL] Shulman, David, "An Annotated Bibliography of Cryptography," Garland Publishing, New York, 1976.

[SIC1] S.I. Course in Cryptanalysis, Volume I, June 1942, Aegean Park Press, Laguna Hills , CA. 1989.

[SIC2] S.I. Course in Cryptanalysis, Volume II, June 1942, Aegean Park Press, Laguna Hills , CA. 1989.

[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.

[SIMM] Simmons, G. J., "How To Insure that Data Acquired to Verify Treaty Compliance are Trustworthy, " in "Authentication without secrecy: A secure communications problem uniquely solvable by asymmetric encryption techniques.", IEEE EASCON 79, Washington, 1979, pp. 661-62.

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

[SMIH] Smith, David E., "John Wallis as Cryptographer", Bulletin of American Mathematical Society, XXIV, 1917.

[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.

[SPAN] Barker, Wayne G. "Cryptograms in Spanish," Aegean Park Press, Laguna Hills, CA., 1986.

[STAL] Stallings, William, "Protect Your Privacy: A Guide for PGP Users," Prentice Hall PTR, 1995.

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

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

[STIX] Stix, F., Zur Geschicte und Organisation der Wiener Geheimen Ziffernkanzlei, Mitteilungen des Osterreichischen Instituts fir Geschichtsforschung, LI 1937.

[STUR] Sturtevant, E. H. and Bechtel, G., "A Hittite Chrestomathy," Linguistic Society of American and University of Pennsylvania, Philadelphia, 1935.

[SURV] Austin, Richard B.,Chairman, "Standards Relating To Electronic Surveillance," American Bar Association Project On Minimum Standards For Criminal Justice, Tentative Draft, June, 1968.

[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.

[THEO] Theodore White and Annalee Jacoby, "Thunder Out Of China," William Sloane Assoc., New York, 1946.

[THOM] Thompson, Ken, "Reflections on Trusting Trust," Communications of the ACM 27, 1984.

[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.

[TORR] Torrieri, Don J., "Principles of Military Communication Systems," Artech, 1981.

[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.

[TUKK] 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.

[TURN] Turn, Rein, "Advances in Computer Security," Artec House, New York, 1982. [Original papers on Public Key Cryptography, RSA, DES]

[UBAL] Ubaldino Mori Ubaldini, "I Sommergibili begli Oceani: La Marina Italian nella Seconda Guerra Mondiale," vol XII, Roma, Ufficio Storico della Marina Militare, 1963.

[USAA] U. S. Army, Office of Chief Signal Officer, "Instructions for Using the Cipher Device Type M-94, February, 1922," USGPO, Washington, 1922.

[USAH] Gilbert, James L. and John P. Finnegan, Eds. "U. S. Army Signals Intelligence in World War II: A Documentary History," Center of Military History, United States Army, Washington, D.C. 1993

[USSF] "U.S. Special Forces Operational Techniques," FM 31- 20, Headquarters Department Of The Army, December 1965.

[USOT] "U.S. Special Forces Recon Manual," Elite Unit Tactical Series, Lancer, Militaria, Sims, ARK. 71969, 1982.

[VAIL] Vaille, Euggene, Le Cabinet Noir, Paris Presses Universitaires de Frances, 1950.

[VALE] Valerio, "De La Cryptographie," Journal des Scienses militares, 9th series, Dec 1892 - May 1895, Paris.

[VAND] Van de Rhoer, E., "Deadly Magic: A personal Account of Communications Intilligence in WWII in the Pacific, New York, Scriber, 1978.

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

[VIAR] de Viaris in Genie Civil: "Cryptographie", Publications du Journal Le Genie Civil, 1888.

[VIA1] de Viaris, "L'art de chiffre et dechiffre les depeches secretes," Gauthier-Villars, Paris, 1893.

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

[VN] "Essential Matters - History of the Cryptographic Branch of the Peoples Army of Viet-Nam, 1945 - 1975," U.S. Cryptological History Series, Series V, NSA CSS, CH-E32-94-02, 1994.

[WALL] Wallis, John, "A Collection of Letters and other Papers in Cipher" , Oxford University, Bodleian Library, 1653.

[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.

[WAY] Way, Peter, "Codes and Ciphers," Crecent Books, 1976.

[WEBE] Weber, Ralph Edward, "United States Diplomatic Codes and Ciphers, 1175-1938, Chicago, Precedent Publishing, 1979.

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

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

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

[WHOR] Whorf, B. L., "A Linguistic Consideration of Thinking In Primitive Communities," In Language, Thought, and Reality: Selected Writings of Benjamin Lee Whorf, ed. J. B. Carroll, Cambridge, MA: MIT Press, pp. 65-86., 1956.

[WILL] Williams, Eugenia, "An Invitation to Cryptograms," Simon and Schuster, 1959.

[WILD] Wildman, Ted, "The Expendables," Clearwater Pub., 1983

[WINJ] Winton, J., " Ultra at Sea: How Breaking the Nazi Code Affected Allied Naval Strategy During WWII," New Uork, William Morror, 1988.

[WINK] Winkle, Rip Van, "Hungarian: The Cryptogram,", March - April 1956.

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

[WINR] Winter, Jack, "Solving Cryptarithms," ACA, 1984.

[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.

[XEN1] PHOENIX, "Xenocrypt Handbook," American Cryptogram Association, 1 Pidgeon Dr., Wilbraham, MA., 01095-2603, for publication March, 1996.

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

[YAR1] Yardley, H. O., "The Chinese Black Chamber," Houghton Mifflin, Boston, 1983.

[YAR2] Yardley, H. O., "Yardleygrams", Bobbs Merrill, 1932.

[YAR3] Yardley, H. O., "The Education of a Poker Player, Simon and Schuster, 1957.

[YOKO] Yukio Yokoyama, "Tokushu joho kaisoka," unpublished handwritten manuscript.

[YOUS] Youshkevitch, A. P., Geschichte der Mathematik im Mittelatter, Liepzig, Germany: Teubner, 1964.

[YUKI] Yukio Nishihara, "Kantogan tai-So Sakusenshi," Vol 17., unpublished manuscript, National Institute for Defense Studies Military Archives, Tokyo.,(hereafter NIDS Archives)

[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)

[ZYZZ] ZYZZ,"Sinkov's Frequency Matching," JA93, The Cryptogram, American Cryptogram Association, 1993.