CLASSICAL CRYPTOGRAPHY COURSE
BY LANAKI

July 01, 1996

LECTURE 15

STATISTICAL ATTACKS

SUMMARY

Lecture 15 considers the role and influence that statistics and probability theory exert on the cryptanalysis of unknown ciphers. We develop our subject by the following references: [FRE3], [SINK], [MAST], [ELCY], [GLEA], [KULL].

DISCUSSION

As you may know, William F. Friedman and Dr. Solomon Kullback were the first Americans to apply Probability Theory and Applied Statistics to the Science of Cryptanalysis. Their achievements were so dynamic that American Crypee's were able to read the secret messages of many of the Foreign Governments that it dealt with. [YARD]

SCOPE

We shall look at three tests: Kappa test for coincidences, Chi test or cross product test for superimposition, and Phi test for monoalphabeticity. We will briefly touch on Gleason's logarithmic weighting scheme for determination of number of letters to differentiate a transposition. The References and Resource section is substantially broadened with nearly 150 more choice plums.

BASIC THEORY OF COINCIDENCES

We have already looked at a table of Phi Values For Monoalphabetic and Digraphic Text By Kullback in Lecture 1. We have also studied various Phi values for Xenocrypts in Lecture 5. We found that the probability is related to coincidences and that it is of significance when we investigate repetitions of letters in a cipher.

We know that the probability of monographic coincidence (1) of random text employing a 26 letter alphabet is 0.0385 , (2) in English telegraphic plain text is 0.0667. We have defined these values as Kr and Kp respectively.

One of the most important techniques in cryptanalysis is that of applying the Kappa Test or Test of Coincidences. The most important purpose for this test is to ascertain whether two or more sequences are correctly superimposed. Correct means the sequences are so arranged to facilitate or make possible a solution. The Kappa test has the following theoretical basis the following circumstances:

(1) If any two rather lengthy sequences of characters are superimposed, it will be found that as successive pairs of letters are brought into vertical juxtaposition, thatin a certain number of cases the two superimposed letters will coincide,

(2) If we are dealing with random text (26 alphabet) there will be 38 or 39 cases of coincidence per 1000 pairs of letters examined because Kr = 0.0385.

(3) If we are dealing with plain text (English) there will be 66 or 67 cases of coincidence per 1000 pairs of letters examined because Kp = 0.0667.

(4) If the superimposed sequences are wholly monoalphabetic encipherments of plain text by the same cipher alphabet, there will be 66 or 67 cases of coincidence per 1000 pairs of letters examined because in monoalphabetic substitution there is a fixed or unvarying relation between plain text and cipher text, so that for statistical purposes the cipher text behaves just as if it were normal plain text.

(5) Even if the two superimposed sequences are polyalphabetic in character, there still will be 66 or 67 cases of coincidence or identity per 1000 pairs of letters examined provided the two sequences really belong to the same cryptographic system and are superimposed at the proper point with respect to the keying sequence.

(6) This last point may be seen in the two polyalphabetic messages below: They have been enciphered poly-alphabetically by the same two primary components sliding against each other. The two messages begin at the same point in the keying sequence. Consequently, they are identically enciphered, letter for letter, the only differences between them is due to differences in plain text.

No. 1

```
Alpha   16 21 13 5 6 4 17 19 21 21 2 6 3 6 13 13 1 7 12 6
Plain   W  H  E  N I N T  H  E  C  O U R S E  L  O N G M
Cipher  E  Q  N  B T F Y  R  C  X  X L Q J N  Z  O Y A W
```

No. 2

```
Alpha   16 21 13 5 6 4 17 19 21 21 2 6 3 6 13 13 1 7 12 6
Plain   T  H  E  G E N E  R  A  L  A B S O L  U  T E L Y
Cipher  P  Q  N  T U F B  W  D  J  L Q H Y Z  P  T M Q I
```

Note, that (a) in every case in which two superimposed cipher letters are the same, the plain text letters are identical and (b) in every case in which two superimposed cipher letters are the different, the plain text letters are different. In such a system, even though the cipher alphabet changes from letter to letter, the number cases of identity or coincidence in the two members of a pair of superimposed cipher letters will still be about 66 or 67 per thousand cases examined, because the two members of each pair of superimposed letters are in the same alphabet and it has been seen in (4) that in monoalphabetic cipher text K is the same as for plain text, viz, 0.667. The fact that in this case each monoalphabet contains just two letters does not affect the theoretical value of K (Kappa) and whether the actual number of coincidences agrees closely with the expected number based upon Kp = 0.0667 depends upon the lengths of the two superimposed sequences. Messages No's 1 and 2 are said to be superimposed correctly , that is brought into proper juxtaposition with respect to the keying sequences.

(7) Now change the situation by changing the juxtaposition to an incorrect superimposition with respect to the keying sequence.

No. 1

```
Alpha   16 21 13 5 6 4 17 19 21 21 2 6 3 6 13 13 1 7 12 6
Plain   W  H  E  N I N T  H  E  C  O U R S E  L  O N G M
Cipher  E  Q  N  B T F Y  R  C  X  X L Q J N  Z  O Y A W
```

No. 2

```
Alpha     16 21 13 5 6 4 17 19 21 21 2 6 3 6  13 13 1 7
Plain      T  H  E G E N E  R  A  L  A B S O   L  U  T E
Cipher     P  Q  N T U F B  W  D  J  L Q H Y   Z  P  T M
```

It is evident that the two members of every pair are not in the same cipher alphabets and any identical letters after superimposition is strictly accidental. Actually the number of repetitions will approximate Kr = 0.0385.

Note again, that in every case in which two superimposed cipher letters are the same, the plain text letters are not identical and in every case in which two superimposed cipher letters are the different, the plain text letters are no always different. Look at the superimposed T(cipher)'s representing two different plain text letters and that the S in "COURSE" gives the value J (cipher) and in the word ABSOLUTELY gives H (cipher). It should be clear that an incorrect superimposition by two different plain-text letters enciphered by two different alphabets may "by chance" produce identical cipher letters, which on superimposition yield coincidence but have no external indications as to dissimilarity in plain text equivalents. This incorrect superimposition will coincide by a value of Kr = 0.0385.

(8) Note the two Z's and they represent the plain text L. This occurred because the same cipher alphabet came into play by chance twice to encipher the same plain text letter both times. This may distort the Kr value for some systems.

(9) In general, in the case of correct superimposition the probability of identity or coincidence is Kp = 0.0667; in the case of incorrect superimposition, the probability is greater than or equal to Kr = 0.0385. The Kappa test, aka coincidence test is defined by these values.

APPLYING THE KAPPA TEST

When we say Kp = 0.0667, this means that in a 1000 cases where two letters are drawn at random from a large volume of plain text, we should expect 66 or 67 cases of two letters to coincide or be identical. Nothing is specified what these letters shall be; they can be two Z's or two E's. Another way is to consider that at random 6.67% of the comparisons made will yield coincidences. So for 2000 examinations, we expect 2000 x 6.67% = 133.4 coincidences [use integers and round down to 133]. Or 20,000 comparisons means 1,334 coincidences.

A more practical approach is to find the ratio of observed number of coincidences to the total number of cases in question that may occur, i.e. the total number of comparisons of superimposed letters. When the ratio is closer to 0.0667 than 0.0385 the correct superimposition has been found. This is true because both members of each pair of superimposed letters belong to the same monoalphabet and therefore the probability of their coinciding is 0.067; whereas, in the case of incorrect superimposition, each pair belongs to different monoalphabets and the probability of their coinciding approaches 0.0385 rather than 0.0667.

To use the Kappa test requires calculating the total number of comparisons in a given case and the actual number of coincidences in the case under consideration. When two messages are superimposed, the total number of comparisons made equals the number of superimposed letters. When more than two messages are superimposed in a superimposition diagram (Lecture 13) it is necessary to calculate the number of comparisons based on the number of letters in the column.

$$n \text{ letters} = n(n-1)/2 \text{ pairs or comparisons, in column}$$

For a column of 3 letters , there are 3(2)/2 = 3 comparisons. We compare the 1st with the 2nd, 2nd with 3rd and 1st with 3rd columns. The more general probability formula is

$$nCr = n!/r!(n-r)!$$

where we determine the number of combinations of n different things taken r at a time. For two letters, r is always 2, so n!/r!(n-r)! is the same as

$$n(n-1)(n-2)!/2(n-2)!$$

$$\text{becomes} \quad n(n-1)/2$$

with the cancellation of terms using (n-2)!.

RULE

The number of comparisons per column times the number of columns in the superimposition diagram of letters gives the total number of comparisons. The extension to this reasoning is where the superimposition diagram involves columns of various lengths, then we add together the number of comparisons for columns of different lengths to obtain a grand total. Table 15-1 shows the number of letters in a column versus the number of comparisons calculated. [FRE3]

Table 15 -1

Number of letters in column	Number of comparisons	Number of letters in column	Number of comparisons
2	1	16	120
3	3	17	136
4	6	18	153
5	10	19	171
6	15	20	190
7	21	21	210
8	28	22	231
9	36	23	253
10	45	24	276
11	55	25	300
12	66	26	325
13	78	27	351
14	91	28	378
15	105	29	406
		30	435

In ascertaining the number of coincidences in the case of a column containing several letters, we still use the n(–1)/2 formula, only in this case, n is the number of identical letters in the column. The reasoning is essentially the same as above. The total number of coincidences is the sum of the number of coincidences for each case of identity.

Given the column:

C
K
B
K
Z
K
C
B
B
K

There are 10 letters with 3B's, 2C's 4K's and 1 Z. The 3B's yield 3 coincidences, the 2 C's yield 1 coincidence, the 4 K's yield 6 coincidences. The sum is 3 + 1 + 6 = 10 coincidences in 45 comparisons = 0.2222

ENCIPHERMENT WITH SAME KEY BUT DIFFERENT INITIATION POINTS

In Lecture 13, I ended with the note that several messages enciphered by the same keying sequence but each beginning at a different point presented a challenge. The best attack is that by superimposition and the Kappa test is used to correctly line up the messages with respect to each other.

It is understood that the messages may be shifted relative to each other at many points of superimposition but there is only one point of superimposition for each message which corresponds to monoalphabetic columnar superimposition of the cipher text.

The method:

(1) Number the message according to their lengths.

(2) Fix message 1, message 2 is placed under it so that the first pair of letters coincide.

(3) Examine, calculate total number of cases in which superimposed letters are identical, thus the observed number of coincidences. The total number of superimposed pairs is calculated and multiplied by 0.0667 to find the expected number of coincidences.

(4) If the observed number is considerably below the expected number, or if the ratio of the observed number of coincidences to the total is closer to 0.0385 than 0.0667, then the superimposition is wrong and we shift message 2 one letter to the left.

(5) Repeat steps (3) - (4) until the correct superimposition is found.

(6) Test message 3 against message 1 and then against message 2.

(7) Continue the process until all the messages are lined up correctly.

Computers are a big help in this process.

EXAMINE OF KAPPA TEST

Given 4 messages of 30 intercepted using a long enciphered keying sequence:

Message 1

```
PGLPN  HUFRK  SAUQQ  AQYUO  ZAKGA  EOQCN
PRKOV  HYEIU  YNBON  NFDMW  ZLUKQ  AQAHZ
MGCDS  LEAGC  JPIVJ  WVAUD  BAHMI  HKORM
LTFYZ  LGSOG  K.                   [101]
```

Message 2

```
CWHPK  KXFLU  MKURY  XCOPH  WNJUW  KWIHL
OKZTL  AWRDF  GDDEZ  DLBOT  FUZNA  SRHHJ
NGUZK  PRCDK  YOOBV  DDXCD  OGRGI  RMICN
HSGGO  PYAOY  X.                   [101]
```

Message 3

```
WFWTD  NHTGM  RAAZG  PJDSQ  AUPFR  OXJRO
HRZWC  ZSRTE  EEVPX  OATDQ  LDOQZ  HAWNX
THDXL  HYIGK  VYZWX  BKOQO  AZQND  TNALT
CNYEH  TSCT.                       [99]
```

Message 4

```
TULDH  NQEZZ  UTYGD  UEDUP  SDLIO  LNNBO
NYLQQ  VQGCD  UTUBQ  XSOSK  NOXUV  KCYJX
CNJKS  ANGUI  FTOWO  MSNBQ  DBAIV  IKNWG
VSHIE  P                           [96]
```

Superimpose messages 1 and 2.

```
              *     *      *
No. 1      PGLPN  HUFRK  SAUQQ  AQYUO  ZAKGA  EOQCN
No. 2      CWHPK  KXFLU  MKURY  XCOPH  WNJUW  KWIHL

                                                 *
No. 1      PRKOV  HYEIU  YNBON  NFDMW  ZLUKQ  AQAHZ
No. 2      OKZTL  AWRDF  GDDEZ  DLBOT  FUZNA  SRHHJ

            *                        *      *
No. 1      MGCDS  LEAGC  JPIVJ  WVAUD  BAHMI  HKORM
No. 2      NGUZK  PRCDK  YOOBV  DDXCD  OGRGI  RMICN

                     *
No. 1      LTFYZ  LGSOG  K.                   [101]
No. 2      HSGGO  PYAOY  X.                   [101]
```

The number of comparisons is 101 x 0.0667 = 7 coincidences which is less than the observed 8. Nice start but suspicious. Shifting one letter to right the number of coincidences is 4. One more shift = 3. Then:

```
                 *      *    *
No. 1      PGLPNHUFRKSAUQQAQYUOZAKGAEOQCN
No. 2         CWHPKKXFLUMKURYXCOPHWNJUWKW

               *                        *
No. 1      PRKOVHYEIUYNBONNFDMWZLUKQAQAHZ
No. 2      IHLOKZTLAWRDFGDDEZDLBOTFUZNASR

                              *        **
No. 1      MGCDSLEAGCJPIVJWVAUDBAHMIHKORM
No. 2      HHJNGUZKPRCDKYOOBVDDXCDOGRGIRM

                 *
No. 1      LTFYZLGSOGK.
No. 2      ICNHSGGOPYAOYX.          [98]
```

Now 98 x 0.0667 = 6.5366 versus 9 coincidences or 30% more than the first comparison. The first test was accidental. The jump is normal from incorrect to correct. The correct superimposition is either 100% correct or incorrect.

Friedman suggests that tests be made first to the right and then to the left, one letter at a time for best efficiency. [FRE3]

It is possible to systematize our investigation by testing three or four messages at a time.

We make a diagram where the number of coincidences are tallied with all three messages:

```
          1     2     3
        ----------------
      1|  x     9     3
       |
      2|  x     x     3
       |
      3|  x     x     x
```

The number of tallies in cell 1-2 is 9 as examined. A column which shows identical letters in messages 1 and 3 yields a tally in 1-3, between 2 and 3 goes to 2-3 and so forth. Only when a superimposition yields three identical letters in a column is a tally to be recorded in 1-3 or 1-2 (3 coincidences.

So adding message 3 to the investigation:

```
                    *
No. 1      PGLPNHUFRKSAUQQAQYUOZAKGAEOQCN
No. 2         CWHPKKXFLUMKURYXCOPHWNJUWKW
No. 3      WFWTDNHTGMRAAZGPJDSQAUPFROXJRO

            *   *            *
No. 1      PRKOVHYEIUYNBONNFDMWZLUKQAQAHZ
No. 2      IHLOKZTLAWRDFGDDEZDLBOTFUZNASR
No. 3      HRZWCZSRTEEEVPXOATDQLDOQZHAWNX

            *      *
No. 1      MGCDSLEAGCJPIVJWVAUDBAHMIHKORM
No. 2      HHJNGUZKPRCDKYOOBVDDXCDOGRGIRM
No. 3      THDXLHYIGKVYZWXBKOQOAZQNDTNALT


No. 1      LTFYZLGSOGK.
No. 2      ICNHSGGOPYAOYX.
No. 3      CNYEHTSCT.
```

so:

```
          1     2     3
       -----------------
     1|   x     9     3
      |
     2|   x     x     3
      |
     3|   x     x     x
```

Successive number of columns are examined and coincidences (of messages 1 and 3 and 2 and 3) are tabulated. We find:

Combination	Total Number of Comparisons	Number of Coincidences Expected	Observed	Delta %
1 - 3	99	~ 7	3	-57
2 - 3	96	~ 6	3	-50
1- 2- 3	293	~ 20	15	-21

A correct superimposition for one of the three combinations may yield such good results as to mask the bad results for the other two combinations.

We shift message 3 one space to the right with the following results:

```
                                 *
No. 1       PGLPNHUFRKSAUQQAQYUOZAKGAEOQCN
No. 2          CWHPKKXFLUMKURYXCOPHWNJUWKW
No. 3        WFWTDNHTGMRAAZGPJDSQAUPFROXJR

             *   *               *   *
No. 1       PRKOVHYEIUYNBONNFDMWZLUKQAQAHZ
No. 2       IHLOKZTLAWRDFGDDEZDLBOTFUZNASR
No. 3       OHRZWCZSRTEEEVPXOATDQLDOQZHAWN

                           *    *
No. 1       MGCDSLEAGCJPIVJWVAUDBAHMIHKORM
No. 2       HHJNGUZKPRCDKYOOBVDDXCDOGRGIRM
No. 3       XTHDXLHYIGKVYZWXBKOQOAZQNDTNAL

              *    *
No. 1       LTFYZLGSOGK.
No. 2       ICNHSGGOPYAOYX.
No. 3       TCNYEHTSCT.
```

	1	2	3
1	x	9	10
2	x	x	7
3	x	x	x

Combination	Total Number of Comparisons	Number of Coincidences Expected	Observed	Delta %
1 - 3	99	~ 7	10	+43
2 - 3	97	~ 6	6	0
1- 2- 3	294	~ 20	25	+25

The results are very good. We add the fourth message.

```
No. 1       PGLPNHUFRKSAUQQAQYUOZAKGAEOQCN
No. 2          CWHPKKXFLUMKURYXCOPHWNJUWKW
No. 3        WFWTDNHTGMRAAZGPJDSQAUPFROXJR
No. 4         TULDHNQEZZUTYGDUEDUPSDLIOLNN

No. 1       PRKOVHYEIUYNBONNFDMWZLUKQAQAHZ
No. 2       IHLOKZTLAWRDFGDDEZDLBOTFUZNASR
No. 3       OHRZWCZSRTEEEVPXOATDQLDOQZHAWN
No. 4       BONYLQQVQGCDUTUBQXSOSKNOXUVKCY
```

```
No. 1      MGCDSLEAGCJPIVJWVAUDBAHMIHKORM

No. 2      HHJNGUZKPRCDKYOOBVDDXCDOGRGIRM
No. 3      XTHDXLHYIGKVYZWXBKOQOAZQNDTNAL
No. 4      JXCNJKSANGUIFTOWOMSNBQDBAIVIKN

No. 1      LTFYZLGSOGK.
No. 2      ICNHSGGOPYAOYX.
No. 3      TCNYEHTSCT.
No. 4      WGVSHIEP.
```

	1	2	3	4
1	x	9	10	7
2	x	x	7	7
3	x	x	x	5
4	x	x	x	x

Combination	Total Number of Comparisons	Number of Coincidences Expected	Observed	Delta %
1 - 3	96	~ 6	7	+16
2 - 3	95	~ 6	7	+16
3 - 4	96	~ 6	5	-16
1,2,3,4	581	~39	44	+10

This is actually the correct group of superimpositions. Testing another message 4 movement to right shows us the picture.

```
No. 1      PGLPNHUFRKSAUQQAQYUOZAKGAEOQCN
No. 2         CWHPKKXFLUMKURYXCOPHWNJUWKW
No. 3       WFWTDNHTGMRAAZGPJDSQAUPFROXJR
No. 4         TULDHNQEZZUTYGDUEDUPSDLIOLN

No. 1      PRKOVHYEIUYNBONNFDMWZLUKQAQAHZ
No. 2      IHLOKZTLAWRDFGDDEZDLBOTFUZNASR
No. 3      OHRZWCZSRTEEEVPXOATDQLDOQZHAWN
No. 4      NBONYLQQVQGCDUTUBQXSOSKNOXUVKC

No. 1      MGCDSLEAGCJPIVJWVAUDBAHMIHKORM
No. 2      HHJNGUZKPRCDKYOOBVDDXCDOGRGIRM
No. 3      XTHDXLHYIGKVYZWXBKOQOAZQNDTNAL
No. 4      YJXCNJKSANGUIFTOWOMSNBQDBAIVIK

No. 1      LTFYZLGSOGK.
No. 2      ICNHSGGOPYAOYX.
No. 3      TCNYEHTSCT.
No. 4      NWGVSHIEP.
```

```
          1     2     3     4
        ----------------------
      1|   x     9     10    3
       |
      2|   x     x     7     3
       |
      3|   x     x     x     2
       |
      4|   x     x     x     x
```

Combination	Total Number of Comparisons	Number of Coincidences Expected	Observed	Delta %
1 - 3	96	~ 6	3	-50
2 - 3	96	~ 6	3	-50
3 - 4	96	~ 6	2	-83
1,2,3,4	582	~39	33	-18

SUBSEQUENT SOLUTION STEPS

These four messages were enciphered by a long keying sequence. We now have found the correct superimposition of the four messages. Therefore, the text has been reduced to monoalphabetic columnar form and can be solved. What was not given on this example was that the enciphering device was a U. S. Army Cipher Disk and that the key was intelligent as well as the alphabets are reversed standard.

It doesn't matter to the Kappa test what kind of cipher alphabets were used or whether or not the key is random or intelligent. We try our favorite technique - the probable word on message 1 of DIVISION.

```
Ciphertext      P G L P N H U F R K S A U Q Q
Assumed Plain   D I V I S I O N
Resultant Key   S O G X F
```

nope, shift one letter right.

```
Ciphertext      P G L P N H U F R K S A U Q Q
Assumed Plain   . D I V I S I O N
Resultant Key   . J T K
```

nope, shift one more, and one and finally to the end with no resultant intelligent key.

```
Ciphertext      P G L P N H U F R K S A U Q Q
Assumed Plain           R E G I M E N T N O
Resultant Key           E L A N D O F T H E
```

which suggests LAND of T(HE) which yields REGIMENT NO. More assumptions yield an E before LAND and the cipher text yielding IS for the plain. The process continues one letter at a time and checking the cipher versus the plain for reconstructive clues.

We can use all four messages to gives us clues by multiple superimposition.

```
     Key                    E L A N D O F T
No 1 Ciphertext      P G L P N H U F R K S A U Q Q
     Plain                  R E G I M E N T

No 2 Ciphertext           C W H P K K X F L U M K
     Plain                  I E L D T R A I

No 3 Ciphertext        W F W T D N H T G M R A A Z
     Plain                  L I N G K I T C

No 4 Ciphertext          T U L D H N Q E Z Z U T Y
     Plain                  T I T A N K G U
```

We see No. 2 gives us FIELD TRAIN, No 3 has ROLLING KITCHEN, and No 4 with ANTITANK GUN. These words yield additional letters. If the key is unintelligent text we use the messages against each rather than against the key.

UNKNOWN SEQUENCES

The previous example assumed a known cipher alphabet. When it is not known, Data for solution by indirect symmetry by detection of isomorphs cannot be expected, for isomorphs may not be produced by the system. Solution can be reached only if there is sufficient text to permit analysis of columns for superimposition diagram. Large amount of text yields repetitions and the basis for probable word assumption. After establishment of a few values for cipher text letters does indirect symmetry come into play. Each column requires 15 -20 letters minimum. These can be studied statistically and if two columns have similar characteristics, they may be combined using the cross product test.

RUNNING KEY PRINCIPLE

The running - key principle may be interesting in principle but difficult in practice. Mistakes in encipherment or transmission, essentially decrease the likely hood of the correct decipherment. The running Key does improve cryptographic security but the mechanical details involved in the production, reproduction, and distribution of such keys represents a formidable challenge - enough to destroy the effectiveness of the system for practical purposes (voluminous communication).

Suppose a basic unintelligible, random sequence of keying characters which is not derived from the interaction of two or more shorter keys and which NEVER repeats is employed only ONCE as a key for encipherment. Can such a cryptogram be solved. No. No method of attack will solve this because the system is not uniquely solvable.

Two things are required for solution: the logical answer must be offered and it must be unique. The Bacon-Shakespeare "cryptographers tend to overlook the latter issue. To attempt to solve a cryptogram enciphered as previously described is like solving an equation in two unknowns with absolutely no data available for solution but the solution itself. The key is one unknown and the plain text is the other. Any one quantity may be chosen and yield a viable result without the required uniqueness constraint being observed. There are an infinite number of solutions possible.

The problem is better defined when the running key constitutes intelligent test, or if it is used to encipher more than one message, or if it is the secondary result of the interaction of two or more short primary keys which go thru cycles themselves. The additional information in these cases are enough to meet the uniqueness constraint.

CROSS-PRODUCT TEST OR CHI [X]

The KAPPA test is used to prepare data for analysis. It circumvents the polyalphabetic obstacle. It moves the solution from polyalphabetic to monoalphabetic terms. The solution can be reached if their is some cryptographic relationship between the columns, or the letters can be combined into a single frequency distribution.

The amount of data has to be sufficient for comparison purposes and this depends on the type of cipher alphabets involved. Although the superimposition diagram may be composed of many columns, often only a relatively small number of different cipher alphabets are put into play. The number of times that a secondary alphabet is employed is directly related to the key text or number of keying elements in the sequence.

In the running-key cipher using a long phrase or book as a key, the key is intelligible text and it follows that the secondary alphabets will be employed with frequencies directly related to the respective frequencies of occurrence of letters of plain text. The key letter 'E' alphabet should be most frequent, 'T' next and so forth. J, K, Q, X, Z are improbable, so the cryptanalyst usually handles no more than 19-20 secondary alphabets.

It is possible to study the various distributions for the columns of the superimposition diagram with the view of assembling those distributions which belong to the same cipher alphabet, say 'E', thus making the determination of values easier in a combined distribution.

If the key is random text, and assuming sufficient text within the columns, the columnar frequency distributions may afford the opportunity to amalgamate a large number of small distributions into a smaller number of larger distributions. This is known as matching and we use the Cross-Product or Chi Test, aka X test.

The Chi test is used to identify distributions which belong to the same cipher alphabet. It is used when the amount of data is not very large.

DERIVATION OF CHI TEST [KULL]

The theory of monographic coincidence in plain text was originally developed by Friedman and applied in his technical paper written in 1925 dealing with his solution of messages enciphered by a cryptographic machine known as the "Herbern Electric Super-Code." The paper is among the Riverbank Publications in 1934.

The probability of coincidence of two A's in plain text is the square of the probability of occurrence of the single letter A in such text. Samething with B's through Z's. The sum of these squares for all letters of the alphabet as shown in Table 15-2, is found to be 0.0667. This is almost double the combined probability of random text for hitting two random text letters coincidentally or:

26 letters x 1/26 x 1/26 = 1/26 = 0.0385 = Kr

Table 15-2

Letter	Frequency in 1000 Letters	Probability of Occurrence Separately	Square of Probability of Separate Occurrence
A	73.66	0.0737	0.0054
B	9.74	.0097	.0001
C	30.68	.0307	.0009
D	42.44	.0424	.0018
E	129.96	.1300	.0169
F	28.32	.0283	.0008
G	16.38	.0164	.0003
H	33.88	.0339	.0012
I	73.52	.0735	.0054
J	1.64	.0016	.0000
K	2.96	.0030	.0000
L	36.42	.0364	.0013
M	24.74	.0247	.0006
N	79.50	.0795	.0063
O	75.28	.0753	.0057
P	26.70	.0267	.0007
Q	3.50	.0035	.0000
R	75.76	.0758	.0057
S	61.16	.0612	.0037
T	91.90	.0919	.0084
U	26.00	.0260	.0007
V	15.32	.0153	.0002
W	15.60	.0156	.0002
X	4.62	.0046	.0000
Y	19.34	.0193	.0004
Z	.98	.0010	.0000
Total	1,000.00	1.0000	0.0667

We have seen this value before as Kp. It is the probability that any two letters selected at random in a large volume of normal English plain text will coincide.

Given a 50 letter plain-text distribution:

```
3   1 1 7 1   2 3     1 2 5 6     2 5 6 2   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
```

The number of pairings that can be made are n (n-1)/2 = (50 x 49)/2 = 1,225 comparisons. According to the theory of coincidences, there should be 1,225 x 0.0667 = 81.7065 or approximately 82 coincidences of single letters. We look at the distribution and finds there are 83 for a very close agreement. [N(N-1)/2]

```
3   1 1 7 1   2 3     1 2 5  6     2 5  6  2   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
3+0+0+1+21+0+0+1+3+0+0+0+1+10+15+0+0+1+10+15+1+0+1+0+0+0=83
```

If N is the total number of letters in the distribution, then the number of comparisons is N(N-1)/2 and the expected number of coincidences may be written:

.0067N(N-1)/2

or (.0067N**2 - 0.0667N)/2 eq. I

If we let Fa = number of occurrences of A in the foregoing distribution, the number of coincidences for letter A is Fa(Fa-1)/2. Similarly for B, we have Fb(Fb-1)/2. The total number of coincidences for the distribution is:

Fa(Fa-1)/2 +Fb(Fb-1)/2+...+Fz(Fz-1)/2.

Let Fa = any letter A..Z and d = the sum of all terms that follow it. The distribution d(Fa**2-Fa)/2 represents the actual coincidences.

Although derived from different sources we equate the terms.

d(Fa**2-Fa)/2 = (.0067N**2 - 0.0667N)/2

and dFa = N

d(Fa**2-Fa) = (.0067N**2 - 0.0667N)

dFa**2 - N = (.0067N**2 - 0.0667N)

dFa**2 = .0067N**2 + 0.9333N eg. II

Equation II tells us the sum of the squares of the absolute frequencies of a distribution is equal to 0.0667 times the square of the total number of letters in the distribution, plus 0.933 times the total number of letters in the distribution. We let S2 replace dFa**2.

Suppose two monoalphabetic distributions pertain to the same cipher alphabet. If they are to be correctly combined into a single distribution, the latter must still be monoalphabetic. We use subscripts 1 and 2 to indicate the distributions in question. So:

d(Fa1+Fa2)**2 = .0067(N1+N2)**2 + 0.9333(N1+N2)

expanding terms:

dFa1**2 +2dFa1Fa2 +dFa2**2 =0.0667(N1**2 +2N1N2 + N2**2) +.9333N1 +.9333N2 eq. III

dFa1**2 = .0067N1**2 + 0.9333N1

dFa2**2 = .0067N2**2 + 0.9333N2

and rearranging:

.0667N1**2 +.9333N1 +2dFa1Fa2 + .0667 N2**2 + .9333N2 =

.0667(N1**2 +2N1N2 +N2**2) + .9333N1 +.9333N2

further reducing:

2dFa1Fa2 = 0.667 (2N1N2)

finally:

$$dFa1Fa2 = \frac{0.667}{N1N2} \qquad \text{eq. IV}$$

This equation permits the establishment of an expectant value for the sum of products of the corresponding frequencies of the two distributions being considered for amalgamation. The Chi test or Cross-product test is based on Equation IV.

Given two distributions to be matched:

```
     1 4   3   1     1     1     1     3 2 2 1   1 3   2
F1 - 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

       2       3     1   1     1 1     3 1 1         1 2
F2 - 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 juxtapose the frequencies for convenience.

```
                                                N1 = 26
Fa1    1 4   3   1     1     1     1     3 2 2 1   1 3   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
Fa2      2       3     1   1     1 1     3 1 1         1 2
                                                N2 = 17
Fa1Fa2 0 8 0 0 0 3 0 0 1 0 0 0 0 0 1 0 0 9 2 2 0 0 0 0 0 4
             d=30
```

N1N2 = 26 x 17 = 442

$$\frac{dFa1Fa2}{N1N2} = \frac{30}{442} = 0.0711$$

or 442 x 0.0667 = 28.15 expected value versus 30. The two distributions very probably belong together.

To point out the effectiveness of the correct Chi test placement, we look at the example but juxtaposed one interval to the left.

```
                                                  N1=26
     1 4   3   1     1     1     1     3 2 2 1   1 3   2
F1 - 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
F2 - 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
     2       3     1   1     1 1     3 1 1         1 2
                                                  N2=17
Fa1Fa2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 3 2 0 0 0 0 3 0 0
          dFa1Fa2=2+3+2+3= 10
```

```
dFa1Fa2      10
--------  = ---- =  0.226
 N1N2        442
```

Thus, if the two distribution pertain to the same primary components then they are not properly superimposed. The Chi test may be applied also to cases where two or more frequency distributions must be shifted relatively in order to find the correct superimposition. The problem determines whether we use direct superimposition or shifted superimposition of the second distribution in question.

APPLYING THE CHI TEST TO PROGRESSIVE-ALPHABET SYSTEM

We assume for this example that the secondary alphabets were derived from the interaction of two identical mixed primary components. The cipher alphabet is based on HYDRAYLIC...Z sequence shifted one letter to the right for each encipherment. Based on Figure 15-1, the horizontal sequences are all identical and shifted relatively. The letters inside the square are plain-text letters.

Instead of letters in the cells of the square we tally the normal frequencies of the letters occupying the respective cells. For the first 3 rows we have:

```
  1 . . . 5 . . . . 10 . . . . 15 . . . . 20 . . . . . 26

A 7 3 4 8 3 1 12 3 2     3 8 7  3   6 9 1 1      3 2 4  8
B 112 3 2     3 8 7  3   6 9 1 1      3 2 4  8 7 3 8 3  1
C 3 112 3 2     3 8 7  3   6 9  1 1     3 2 4  8 7 3 4  8
```

The shift required in this case is 5 to the right to match up A and B. Note that amount of displacement, or number of intervals, the B sequence must be shifted to make it match A sequence corresponds exactly to the distance between the letters A and B in the primary cipher component.

```
                  ..... A U L I C B ......
                        0 1 2 3 4 5
```

The fact that the primary plain component is identical with the primary cipher component is coincidental. The displacement interval is being measured on the cipher component.

The Given Cipher message is written into a 26 column (26 alphabets) square rather than the standard 5 letter groups.

FIGURE 15-1

ALPHABET NO

```
        1   5    10   15   20    26
   A | AULICBEFGJKMNOPQSTVWXZHYDR
   B | BEFGJKMNOPQSTVWXZHYDRAULIC
   C | CBEFGJKMNOPQSTVWXZHYDRAULI
   D | DRAULICBEFGJKMNOPQSTVWXZHY
   E | EFGJKMNOPQSTVWXZHYDRAULICB
   F | FGJKMNOPQSTVWXZHYDRAULICBE
C  H | HYDRAULICBEFGJKMNOPQSTVWXZ
I  I | ICBEFGJKMNOPQSTVWXZHYDRAUL
P  J | JKMNOPQSTVWXZHYDRAULICBEFG
H  K | KMNOPQSTVWXZHYDRAULICBEFGJ
E  L | LICBEFGJKMNOPQSTVWXZHYDRAU
R  M | MNOPQSTVWXZHYDRAULICBEFGJK
   N | NOPQSTVWXZHYDRAULICBEFGJKM
   O | OPQSTVWXZHYDRAULICBEFGJKMN
L  P | PQSTVWXZHYDRAULICBEFGJKMNO
E  Q | QSTVWXZHYDRAULICBEFGJKMNOP
T  R | RAULICBEFGJKMNOPQSTVWXZHYD
T  S | STVWXZHYDRAULICBEFGJKMNOPQ
E  T | TVWXZHYDRAULICBEFGJKMNOPQS
R  U | ULICBEFGJKMNOPQSTVWXZHYDRA
   V | VWXZHYDRAULICBEFGJKMNOPQST
   W | WXZHYDRAULICBEFGJKMNOPQSTV
   X | XZHYDRAULICBEFGJKMNOPQSTVW
   Y | YDRAULICBEFGJKMNOPQSTVWXZH
   Z | ZHYDRAULICBEFGJKMNOPQSTVWX
```

```
   1 . . . 5 . . . .10 . . . .15 . . . .20 . . . . . 26
1  W G J J M M M J X E D G C O C F T R P B M I I I K Z
2  R Y N N B U F R W W W W Y O I H F J K O K H T T A Z
3  C L J E P P F R W C K O O F F F G E P Q R Y Y I W X
4  M X U D I P F E X M L L W F K G Y P B B X C H B F Y
5  I E T X H F B I V D I P N X I V R P W T M G I M P T
6  E C J B O K V B U Q G V G F F F K L Y Y C K B I W X
7  M X U D I P F F U Y N V S S I H R M H Y Z H A U Q W
8  G K T I U X Y J J A O W Z O C F T R P P O Q U S G Y
9  C X V C X U C J L M L L Y E K F F Z V Q J Q S I Y S
10 P D S B B J U A H Y N W L O C X S D Q V C Y V S I L
11 I W N J O O M A Q S L W Y J G T V P Q K P K T L H S
12 R O O N I C F E V M N V W N B N E H A M R C R O V S
13 T X E N H P V B T W K U Q I O C A V W B R Q N F J V
14 N R V D O P U Q R L K Q N F F F Z P H U R V W L X G
15 S H Q W H P J B C N N J Q S O Q O R C B M R R A O N
16 R K W U H Y Y C I W D G S J C T G P G R M I Q M P S
17 G C T N M F G J X E D G C O P T G P W Q Q V Q I W X
18 T T T C O J V A A A B W M X I H O W H D E Q U A I N
19 F K F W H P J A H Z I T W Z K F E X S R U Y Q I O V
20 R E R D J V D K H I R Q W E D G E B Y B M L A B J V
21 T G F F G X Y I V G R J Y E K F B E P B J O U A H C
22 U G Z L X I A J K W D V T Y B F R U C C C U Z Z I N
23 N D F R J F M B H Q L X H M H Q Y Y Y M W Q V C L I
24 P T W T J Y Q B Y R L I T U O U S R C D C V W D G I
25 G G U B H J V V P W A B U J K N F P F Y W V Q Z Q F
26 L H T W J P D R X Z O W U S S G A M H N C W H S W W
27 L Y R Q Q U S Z V D N X A N V N K H F U C V V S S S
28 P L Q U P C V V V W D G S J O G T C H D E V Q S I J
29 P H Q J A W F R I Z D W X X H C X Y C T M G U S E S
30 N D S B B K R L V W R V Z E E P P P A T O I A N E E
31 E E J N R C Z B T B L X P J J K A P P M J E G I K R
32 T G F F H P V V V Y K J E F H Q S X J Q D Y V Z G R
33 R H Z Q L Y X K X A Z O W R R X Y K Y G M G Z B Y N
34 V H Q B R V F E F Q L L W Z E Y L J E R O Q S O Q K
35 O M W I O G M B K F F L X D X T L W I L P Q S E D Y
36 I O E M O I B J M L N N S Y K X J Z J M L C Z B M S
37 D J W Q X T J V L F I R N R X H Y B D B J U F I R J
38 I C T U U U S K K W D V M F W T T J K C K C G C V S
39 A G Q B C J M E B Y N V S S J K S D C B D Y F P P V
40 F D W Z M T B P V T T C G B V T Z K H Q D D R M E Z
41 O O
```

A frequency distribution square is compiled, each column of the text forming a separate distribution in columnar form in the square. See Figure 15-2. Note the size of each distribution on the right side of the square under N.

The Chi test is applied to the horizontal rows in the square. Since the test is statistical, it is more reliable as the size of the distribution increases. We choose the V and W distributions because they have the greatest total number of tallies at 53 and 52 occurrences, respectively.

Figure 15-2

```
   1 . . . 5 . . . .10 . . . .15 . . . .20 . . . . . 26 N
A  1       1   1 4 1 3 1   1       3   2       3 3 1    25
B        6 3   3 7 1 1   1   1 2   1 2 1 8     1 4      43
C  2 3   2 1 3 1 1 1 1   1 2   4 2   1 5 2 6 4   2   1  45
D  1 4   4     2     2 7       1 1  2   1 3 3 1   1 1    34
E  2 3 2 1       4   2     1 4 2   3 2 1   2 1   1 3 1  35
F  2   4 2   3 7 1 1 2 1     6 3 9 3   2       2 1 1 1  51
G  3 6     1 1 1     1 1 4 2   1 4 3   1 1   3 2   3 2  39
H    5     7       4       1   3 4   2 6     2 2   2 1  38
I  4     2 3 2   2 2 1 3 1   1 4       1     3 2 8 4 2  45
J    1 4 3 4 4 3 6 1     3   4 2   1 3 2   4       2 2  50
K    3       2   3 3   4       6 2 2 2 2 1 2 2     2 1  37
L  2 2   1 1     1 2 2 7 4 1       2 1   1 1 1   3 1 1  33
M  2 1   1 3 1 5   1 3     2 1       2   4 7     3 1    37
N  3   2 5           1 7 1 3 2   3       1     1 1   4  34
O  2 3 1   6 1         2 2 1 5 4   2     1 3 1   2 2    38
P  4       2 9   1 1     1 1   1 1 1 9 5 1 2     1 3    43
Q      5 3 1   1 1 1 3   2 2     3     2 5 1 7 5   3    45
R  5 2 1 1 2   1 4 1 1 3 1   2 1   3 4   3 4 1 3   1 2  46
S  1   2       2     1     5 4 1   4   1       3 6 1 8  39
T  3 2 6 1   2     2 1 1 1 2     6 4     3     2 1   1  39
U  1   3 3 2 4 2   2     1 2 1   1   1   2 1 2 4 1      33
V  1   2     2 6 4 8     7     2 1 1 1 1 1   6 4    2 4 53
W  1 1 5 3   1     2 8 1 7 6   1     2 3   2 1 2    4 2 52
X    4   1 3 2 1   5     3 2 3 2 3 1 2     1       1 3 37
Y    1 1     3 3   1 4     4 2   1 4 2 4 3   5 1    2 3 44
Z      2 1     1 1   3 1   2 2     2 2     1   3 3    3 27
   1 . . . 5 . . . .10 . . . .15 . . . .20 . . . . . 26
```

The results of three relative displacements are given.

Test 1

```
  FV  1   2     2 6 4 8     7     2 1 1 1 1 1   6 4   2 4
      1 . . . 5 . . . .10 . . . .15 . . . .20 . . . . . 26
  FW    4 2 1 1 5 3   1     2 8 1 7 6   1     2 3   2 1 2
      24. . 1 . . . 5 . . . .10 . . . .15 . . . .20 . . .
FVFW      4     1018  8    14    14 6   1      18     2 8

                NV = 53, NW =52
                dFVFW = 103

                dFVFW = 103
                -----   ---  = 0.037      nok.
                NVNW    2756
```

```
                          Test 2

  FV  1   2     2 6 4 8     7     2 1 1 1 1 1   6 4   2 4
      1 . . . 5 . . . .10 . . . .15 . . . .20 . . . . . 26
  FW  2 3   2 1 2   4 2 1 1 5 3   1     2 8 1 7 6   1
      . .20 . . . 24. . 1 . . . 5 . . . .10 . . . .15 . .
FVFW  2         4  16 16   35     2     2 8 1  36

               NV = 53, NW =52
               dFVFW = 122

               dFVFW = 122
               -----   ---  = 0.044      nok.
               NVNW    2756

                          Test 3

  FV  1   2     2 6 4 8     7     2 1 1 1 1 1   6 4   2 4
      1 . . . 5 . . . .10 . . . .15 . . . .20 . . . . . 26
  FW  3   1     2 8 1 7 6   1     2 3   2 1 2   4 2 1 1 5
      . 5 . . . .10 . . . .15 . . . .20 . . . . .26 1 . .
FVFW  3   2     4 48 4 56   7     4 3   2 1 2   24 8 2 20

               NV = 53, NW =52
               dFVFW = 190

               dFVFW = 190
               -----   ---  = 0.069      OK!
               NVNW    2756
```

More tests would indicate that we have found the best correlation for these two cipher alphabets. Therefore, the primary cipher component has the letters V and W in these positions. The 4th cell of the W distribution must be placed under the 1 st cell of the V distribution per Test 3.

```
                   1 2 3 4
               . . . V . . W . . .
```

The next best row is F with 51 occurrences. We must test this row against V, W, and V+W. Test 4,5 and 6 show the correct superimpositions for the F row. Note that the computer can be a big time help in this evaluation.

```
                          Test 4

  FV  1   2     2 6 4 8     7     2 1 1 1 1 1   6 4   2 4
      1 . . . 5 . . . .10 . . . .15 . . . .20 . . . . . 26
  FF  1 1 2 1     6 3 9 3   2       2 1 1 1 2   4 2   3 7
      . .10 . . . .15 . . . .20 . . . . .26 1 . . . 5 . .
FVFF  1   4      36 12 72   14      2 1 1 1 2  24 8   6 28

               NV = 53, NF =51
               dFVFF = 212

               dFVFW = 212
               -----   ---  = 0.078
               NVNF    2703

                          Test 5

  FW  1 1 5 3   1     2 8 1 7 6   1     2 3   2 1 2   4 2
      1 . . . 5 . . . .10 . . . .15 . . . .20 . . . . . 26
  FF    3 7 1 1 2 1     6 3 9 3   2       2 1 1 1 2   4 2
      5 . . . .10 . . . .15 . . . .20 . . . . .26 1 . . .
FVFF    3 35    2      48 3 63 18 2       6   2 1 4  16 4

               NW = 52, NF =51
               dFWFF = 210

               dFWFF = 210
               -----   ---  = 0.078
               NWNF    2703

                          Test 6

FV+W  4   3     414 515 6   8    4  4 1 3 2  3 10 6 1 3  9
      1 . . . 5 . . . .10 . . . .15 . . . .20 . . . . . 26
  FF  1 1 2 1     6 3 9 3   2       2 1 1 1  2  4 2   3  7
      . .10 . . . .15 . . . .20 . . . . . 26 1 . . . 5 . .
FV+W  4   6      84 15 35 18 16     8 1 3 21 6  40 12 9 63
*FF
               N(V+W) = 105, NF = 51
               dF(W+V)FF = 422

               dF(W+V)FF = 422
               --------    ---  = 0.079
               N(W+V)NF    5355
```

This test yield the sequence:

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

     V . . W . . . F .
```

As the work progresses, we use smaller and smaller distributions. This decrease in information is counterbalanced by the number of superimpositions being reduced as the primary cipher alphabet comes to the surface.

The completely reconstructed primary cipher component (both plain and cipher were specified as identical) is:

```
1 . . . 5 . . . .10 . . . .15 . . . .20 . . . . . 26
V A L W N O X F B P Y R C Q Z I G S E H T D J U M K
```

In practice, the matching process would be interrupted after a few letters of the primary component were retrieved and the skeleton of a few words became apparent.

We ascertain the initial position for the primary cipher component and decipher the cryptogram.

```
   1 . . . 5 . . . .10 . . . .15 . . . .20 . . . . . 26
1  W G J J M M M J X E D G C O C F T R P B M I I I K Z
   W I T H T H E I M P R O V E M E N T S I N T H E A I

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

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

..... and so forth.

The interesting point is that all the tallies in the frequency square were made of cipher letters occuring in the cryptogram, and the tallies represented their actual occurences. We compared cipher alphabet to cipher alphabet. The plain text letters were held as unknown through out the process.

CRACKING THE PROGRESSIVE CIPHER USING INDIRECT SYMMETRY

What happens when we do not have enough data to foster the statistical attack? We can use indirect symmetry because of certain phenomena arising from the mechanics of the progressive cipher encipherment method itself.

Take:

```
Plain    HYDRAULICBEFGJKMNOPQSTVWXZ
Cipher   FBPYRCQZIGSEHTDJUMKVALWNOX
```

Encipher FIRST BATTALION by the progressive method sliding the cipher component to the left one interval after each encipherment.:

```
         1 2 3 4 5 6 7 8 91011121314
Plain    F I R S T B A T T A L I O N
Cipher   E I C N X D S P Y T U K Y Y
Index    F E B C I L U A R D Y H Z X
shift(-)   1 2 3 4 5 6 7 8 910111213
```

Repeated letters in the text are two I's, three T's and two A's. Lets look at them:

```
         F I R S T B A T T A L I O N
         1 2 3 4 5 6 7 8 91011121314
Plain    . I . . . . . . . . . I . .
Cipher   . I . . . . . . . . . K . .
Plain    . . . . T . . T T . . . . .
Cipher   . . . . X . . P Y . . . . .
Plain    . . . . . . A . . A . . . .
Cipher   . . . . . . S . . T . . . .
```

The two I's are 10 letters apart in both the plain and cipher components. Since the cipher component is displaced one step after each encipherment, two identical letters n intervals apart in the plain text must yield cipher equivalents which are n intervals apart in the cipher component. This leads to the probable word and indirect symmetry attack on the progressive cipher.

A second flaw concerns the repeated cipher letters. Look at the three Y's.

```
         1 2 3 4 5 6 7 8 91011121314
Plain    . . . . . . . . T . . . O N
Cipher   . . . . . . . . Y . . . Y Y
```

Reference to the plain component shows that the N O . . . T is reversed in order with respect to the plain text. The intervals are correct. Since the cipher component is shifted one to the left each encipherment, two identical letters n intervals apart in the cipher text must yield plain text equivalents which are n intervals apart in the cipher component. If the cipher is displaced to the left than the order of the plain is logically reversed.

Given the following message, which is assumed to start with the military greeting COMMANDING GENERAL FIRST ARMY (probable words) the data yielded by this assumption is:

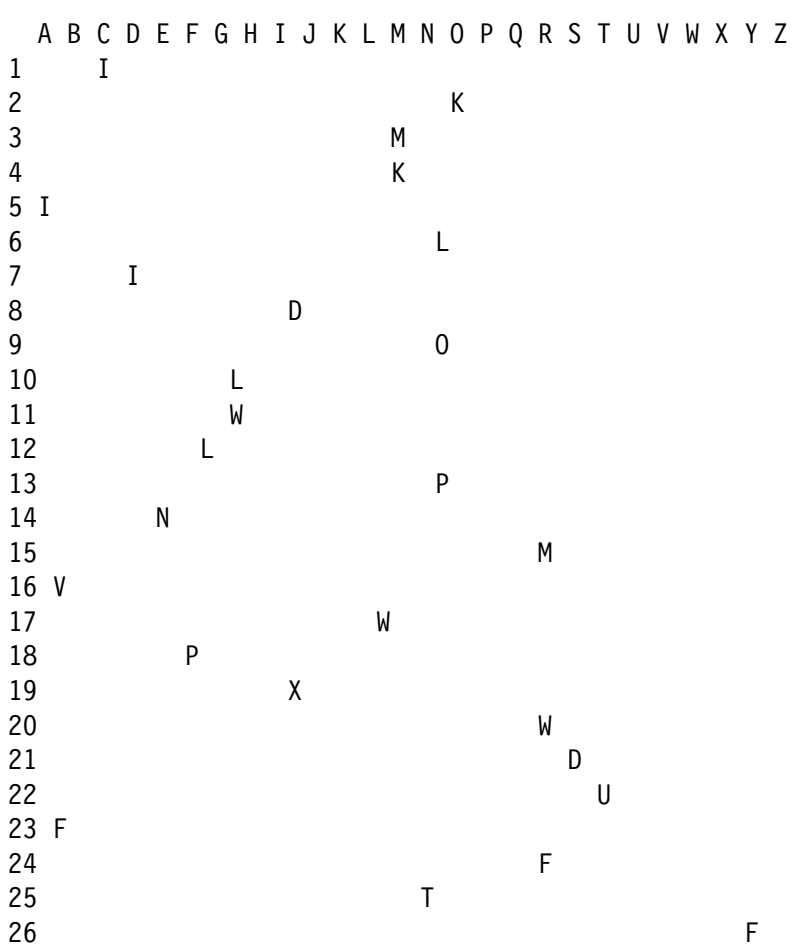
```
IKMKI  LIDOL  WLPNM  VWPXW  DUFFT
FNIIG  XGAMX  CADUV  AZVIS  YNUNL ...

               1.....................26

Plain (assumed) COMMANDINGGENERALFIRSTARMY
Cipher          IKMKILIDOLWLPNMVWPXWDUFFTF
```

Set up the decryption square in Figure 15-3.

Figure 15-3



Applying indirect symmetry to the above square gives:

```
       1 . . . 5 . . . .10 . . . .15 . . . .20 . . . . . 26
Plain  A     L I C   E F G   M N O     S             Y D R
Cipher     M K V . L W N O . F . P . . . . . I . . . . T
       D . . . . . . . . . . M
```

Setting C (plain) = I (cipher) for the first encipherment, the 8th value, I (plain) = D (cipher) which yields D and eventually X. We use the partial sequences to unlock other letters. Using the word ARMY we open the gaps some more.

```
           1 2 3 4 5 6 7 8 9 10 11 12
Plain      N I I G X G A M X  C  A  D
Cipher     . I L . . . . E O  .  .  R
```

The next word after ARMY might be WILL. We then insert the W in the plain and G in the Cipher.

The presence of MMM, WWW, FFF in the cipher might be a short word used several time.. hmm how about THE?? replacing any one of the triplets with THE, applying indirect symmetry, we may have a wedge.

MACHINE CRYPTOGRAPHY

The principles discussed in the previous paragraph may be used with progressive systems in which the interval is > 1 and with modifications to those intervals which are irregular but follow a pattern such as 1-2-3, 1-2-3, ... or 2-5-7-3-1, 2-5-7-3-1- and so on. The latter type of progression is encountered in certain mechanical cryptographs. [FRE3]

THE PHI TEST h FOR MONOALPHABETICITY

The Chi test is based on the general theory of coincidences and the probability constants Kp and Kr. Now two monoalphabetic distributions when correctly combined will yield a single distribution which still will be monoalphabetic in character. The Phi (h) test is used to confirm that a distribution is in fact alphabetic.

DERIVATION Of PHI h TEST

Start with a uniliteral frequency distribution, the total number of pairs of letters for comparison purposes is:

N(N-1)/2 for N letters

from the discussion on the Chi (a) test we found that the expected value of Fa(Fa-1)/2 +..+Fz(Fz-1) for A...Z is equal to the theoretical number of coincidences of two letters to be expected in N(N-1)/2 for N letters, which for normal English plaintext is Kp x N(N-1)/2 and for random text is Kr x N(N-1)/2.

d Fi (Fi-1) = E(hp) = Kp x N(N-1)

for i= A to Z for plain text

d Fi (Fi-1) = E(hr) = Kr x N(N-1)

for i= A to Z for random text

E(a) means the average or expected value of the expression in parenthesis, Kp = 0.0667 for normal English plain text, Kr = 0.0385 for random English text (26 letters).

Example 1:

Is the following enciphered monoalphabetically:

```
1     1 2 3 4 2     1       4 2   1           1   3  N=25
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(ao) = 1x0+1x0+2x1+3x2+4x3+2x1+1x0+4x3+2x1+1x0+1x0+3x2= 2+6+12+2+12+2+6 = 42 o = observed

E(ap) = Kp x N(N-1) = 0.0667 x 25 x 24 = 40 plain

E(ar) = Kr x N(N-1) = 0.0385 x 25 x 24 = 23.1 random

Since the E(ao) =42 is closer to E(ap) = 40, the distribution is most likely monoalphabetic.

Example 2:

```
Y O U I J   Z M M Z Z  M R N Q C   X I Y T W   R G K L H
```

The distribution is

```
    1       1 1 2 1 1 1 3 1 0 2 1 2   1 1   1 1 2 3 N=25
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
```

d Fi(Fi-1) = 18

Since E(ar) is closer to E(ao) the enciphement is probabably polyalphabetic to suppress the frequency distribution. The message was enciphered actually by 25 alphabets used in sequence.

LOGARITHMIC WEIGHT: CHI SQUARED TEST

Gleason discusses an important application of the theory of testing hypothesis. Given a number of messages, some of which are transposed English text and some are flat text. We want to develop a test for picking out the transpositions, and to accomplish this is possible to frame a statistical hypothesis concerning each message. Gleason discusses a 5 step procedure to 1) obtain probability information, 2) calculate its critical region, 3) differentiate by weighted logs 4) calculate the values of alpha and beta statistical inference 5) examine the normal distribution for given values of alpha and beta. The answer tells us how many letters to examine at some level of certainty to determine if we are dealing with a transposition. Chapter 13 Problem 1 gives a reasonable look at the process. [GLEA] Problems 2 and 3 look at the concept of Bayesian probability applied to transposition problems and should be of interest.

WITZEND'S TABLES TO AID CRYPTARITHM SOLUTION

WITZEND has graciously produced several cryptarithmic tables to aid in solution for problems involving bases from ten to sixteen. They are given as Tables 15 - 3 through 15 - 9 and should ease the pain.

Table 15 - 3
DECIMAL - BASE 10

ADDITION

	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	10
2	2	3	4	5	6	7	8	9	10	11
3	3	4	5	6	7	8	9	10	11	12
4	4	5	6	7	8	9	10	11	12	13
5	5	6	7	8	9	10	11	12	13	14
6	6	7	8	9	10	11	12	13	14	15
7	7	8	9	10	11	12	13	14	15	16
8	8	9	10	11	12	13	14	15	16	17
9	9	10	11	12	13	14	15	16	17	18

MULTIPLICATION

	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	10	12	14	16	18
3	0	3	6	9	12	15	18	21	24	27
4	0	4	8	12	16	20	24	28	32	36
5	0	5	10	15	20	25	30	35	40	45
6	0	6	12	18	24	30	36	42	48	54
7	0	7	14	21	28	35	42	49	56	63
8	0	8	16	24	32	40	48	56	64	72
9	0	9	18	27	36	45	54	63	72	81

N	1	2	3	4	5	6	7	8	9
N Square	1	4	9	16	25	36	49	64	81
N Cube	1	8	27	64	125	216	343	512	729
N Fourth	1	16	81	256	625	1296	2401	4096	6561
N Fifth	1	32	243	1024	3125	7776	16807	32768	59049
N Sixth	1	64	729	4096	15625	46656	117649	262144	531441
N Sevnth	1	128	2187	16384	78125	279936	823543	2097152	4782969

X	2	4	5	5	5	5	6	8
Y	6	6	3	5	7	9	6	6
X * Y	12	24	15	25	35	45	36	48

Table 15 - 4
UNDECIMAL - BASE 11

ADDITION

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

MULTIPLICATION

	1	2	3	4	5	6	7	8	9	A
1	1	2	3	4	5	6	7	8	9	A
2	2	4	6	8	A	11	13	15	17	19
3	3	6	9	11	14	17	1A	22	25	28
4	4	8	11	15	19	22	26	2A	33	37
5	5	A	14	19	23	28	32	37	41	46
6	6	11	17	22	28	33	39	44	4A	55
7	7	13	1A	26	32	39	45	51	58	64
8	8	15	22	2A	37	44	51	59	66	73
9	9	17	25	33	41	4A	58	66	74	82
A	A	19	28	37	46	55	64	73	82	91

N	1	2	3	4	5	6	7	8	9	A
N Square	1	4	9	15	23	33	45	59	74	91
N Cube	1	8	25	59	104	187	292	427	603	82A

Table 15 - 5
DUODECIMAL - BASE 12

ADDITION

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

MULTIPLICATION

	1	2	3	4	5	6	7	8	9	A	B
1	1	2	3	4	5	6	7	8	9	A	B
2	2	4	6	8	A	10	12	14	16	18	1A
3	3	6	9	10	13	16	19	20	23	26	29
4	4	8	10	14	18	20	24	28	30	34	38
5	5	A	13	18	21	26	2B	34	39	42	47
6	6	10	16	20	26	30	36	40	46	50	56
7	7	12	19	21	2B	36	41	48	53	5A	65
8	8	14	20	28	34	40	48	54	60	68	74
9	9	16	23	30	39	46	53	60	69	76	83
A	A	18	26	34	42	50	5A	68	76	84	92
B	B	1A	29	38	47	56	65	74	83	92	A1

N	1	2	3	4	5	6	7	8	9	A	B
N Square	1	4	9	14	21	30	41	54	69	84	A1
N Cube	1	8	23	54	A5	160	247	368	569	874	92B

X	2	3	3	4	4	6	6	6
Y	6	4	8	3	6	2	4	6
X * Y	10	10	20	10	20	10	20	30
X	6	6	8	8	8	9	9	2
Y	8	A	3	6	9	4	8	1
X * Y	40	50	20	40	60	30	60	2
X	2	3	3	3	4	4	4	4
Y	7	1	5	9	1	4	7	A
X * Y	12	3	13	23	4	14	24	34

Table 15 - 6
TERDECIMAL - BASE 13

ADDITION

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

MULTIPLICATION

	1	2	3	4	5	6	7	8	9	A	B	C
1	1	2	3	4	5	6	7	8	9	A	B	C
2	2	4	6	8	A	C	11	13	15	17	19	1B
3	3	6	9	C	12	15	18	1B	21	24	27	2A
4	4	8	C	13	17	1B	22	26	2A	31	35	39
5	5	A	12	17	1C	24	29	31	36	3B	43	48
6	6	B	15	1B	24	2A	33	39	42	48	51	57
7	7	11	18	22	29	33	3A	44	4B	55	5C	66
8	8	13	1B	26	31	39	44	4C	57	62	6A	75
9	9	15	21	2A	36	42	4B	57	63	6C	78	84
A	A	17	24	31	3B	48	55	62	6C	79	86	93
B	B	19	27	35	43	51	5C	84	78	86	94	A2
C	C	1B	2A	39	48	57	66	75	84	93	A2	B1

N	1	2	3	4	5	6	7	8	9	A	B	C
N Square	1	4	9	13	1C	2A	3A	4C	63	79	94	B1
N Cube	1	8	21	4C	98	138	205	365	441	5BC	785	A2C

Table 15 - 7
QUADECIMAL - BASE 14

ADDITION

	1	2	3	4	5	6	7	8	9	A	B	C	D
1	2	3	4	5	6	7	8	9	A	B	C	D	10
2	3	4	5	6	7	8	9	A	B	C	D	10	11
3	4	5	6	7	8	9	A	B	C	D	10	11	12
4	5	6	7	8	9	A	B	C	D	10	11	12	13
5	6	7	8	9	A	B	C	D	10	11	12	13	14
6	7	8	9	A	B	C	D	10	11	12	13	14	15
7	8	9	A	B	C	D	10	11	12	13	14	15	16
8	9	A	B	C	D	10	11	12	13	14	15	16	17
9	A	B	C	D	10	11	12	13	14	15	16	17	18
A	B	C	D	10	11	12	13	14	15	16	17	18	19
B	C	D	10	11	12	13	14	15	16	17	18	19	1A
C	D	10	11	12	13	14	15	16	17	18	19	1A	1B
D	10	11	12	13	14	15	16	17	18	19	1A	1B	1C

MULTIPLICATION

	1	2	3	4	5	6	7	8	9	A	B	C	D
1	1	2	3	4	5	6	7	8	9	A	B	C	D
2	2	4	6	8	A	C	10	12	14	16	18	1A	1C
3	3	6	9	C	11	14	17	1A	1D	22	25	28	2B
4	4	8	C	12	16	1A	20	24	28	2C	32	36	3A
5	5	A	11	16	1B	22	27	2C	33	38	3D	44	49
6	6	C	14	1A	22	28	30	36	3C	44	4A	52	58
7	7	10	17	20	27	30	37	40	47	50	57	60	67
8	8	12	1A	24	2C	36	40	48	52	5A	64	6C	76
9	9	14	1D	28	33	3D	47	52	5B	66	71	7A	85
A	A	16	22	2C	38	44	50	5A	66	72	7C	88	94
B	B	18	25	32	3D	4D	57	64	71	7C	89	96	A3
C	C	1A	28	36	44	52	60	6C	7A	88	96	A4	B2
D	D	1C	2B	3A	49	58	67	76	85	94	A3	B2	C1

N	1	2	3	4	5	6	7	8	9	A	B	C	D
N **2	1	4	9	12	1B	28	37	48	5B	72	89	A4	C1
N **3	1	8	1D	48	8D	116	1A7	288	3A1	516	6B1	8B6	B2D

X	2	4	6	7	7	7	7	7
Y	7	7	7	2	4	6	8	A
X * Y	10	20	30	10	20	30	40	50

X	7	8	A	C	2	4	6	7
Y	C	7	7	7	8	8	8	3
X * Y	60	40	50	60	12	24	36	17

X	7	7	7	7	7	8	A	C
Y	5	7	9	B	D	8	8	8
X * Y	27	37	47	57	67	48	5A	6C

Table 15 - 8
QUINDECIMAL - BASE 15

ADDITION

	1	2	3	4	5	6	7	8	9	A	B	C	D	E
1	2	3	4	5	6	7	8	9	A	B	C	D	E	10
2	3	4	5	6	7	8	9	A	B	C	D	E	10	11
3	4	5	6	7	8	9	A	B	C	D	E	10	11	12
4	5	6	7	8	9	A	B	C	D	E	10	11	12	13
5	6	7	8	9	A	B	C	D	E	10	11	12	13	14
6	7	8	9	A	B	C	D	E	10	11	12	13	14	15
7	8	9	A	B	C	D	E	10	11	12	13	14	15	16
8	9	A	B	C	D	E	10	11	12	13	14	15	16	17
9	A	B	C	D	E	10	11	12	13	14	15	16	17	18
A	B	C	D	E	10	11	12	13	14	15	16	17	18	19
B	C	D	E	10	11	12	13	14	15	16	17	18	19	1A
C	D	E	10	11	12	13	14	15	16	17	18	19	1A	1B
D	E	10	11	12	13	14	15	16	17	18	19	1A	1B	1C
E	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D

MULTIPLICATION

	1	2	3	4	5	6	7	8	9	A	B	C	D	E
1	1	2	3	4	5	6	7	8	9	A	B	C	D	E
2	2	4	6	8	A	C	E	11	13	15	17	19	1B	1D
3	3	6	9	C	10	13	16	19	1C	2A	2E	33	37	3B
4	4	8	C	11	15	19	1D	22	26	2A	2E	40	45	4A
5	5	A	10	15	1A	20	25	2A	30	35	3A	40	45	4A
6	6	C	13	19	20	26	2C	33	39	40	46	4C	53	59
7	7	E	16	1D	25	2C	34	3B	43	4A	52	5E	61	68
8	8	11	19	22	2A	33	3B	44	4C	55	5D	66	6E	77
9	9	13	1C	26	30	39	43	4C	56	60	69	73	7C	86
A	A	15	20	2A	35	40	4A	55	60	6A	75	80	8A	95
B	B	17	23	2E	3A	46	52	5D	69	75	81	8C	98	A4
C	C	19	26	33	40	4C	5E	66	73	80	8C	99	A7	B3
D	D	1B	29	37	45	53	61	6E	7C	8A	98	A7	B4	C2
E	E	1D	2C	3B	4A	59	68	77	86	95	A4	B3	C2	D1

N	1	2	3	4	5	6	7	8	9	A	B	C	D	E
N **2	1	4	9	11	1A	26	34	44	56	6A	81	99	B4	D1
N **3	1	8	1C	44	85	E6	17D	242	339	46A	5DB	7A3	9B7	C2E

X	3	3	5	5	5	5	6	6
Y	5	A	3	6	9	C	5	A
X * Y	10	20	10	20	30	40	20	40

X	9	9	A	A	A	A	C	C
Y	5	A	3	6	9	C	5	A
X * Y	30	60	20	40	60	80	80	40

X	3	3	5	5	5	5	6	9
Y	6	B	4	7	A	D	B	6
X * Y	40	80	13	23	10	25	35	45

Table 15 - 9
SEXDECIMAL - BASE 16

ADDITION

	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10
2	3	4	5	6	7	8	9	A	B	C	D	E	F	10	11
3	4	5	6	7	8	9	A	B	C	D	E	F	10	11	12
4	5	6	7	8	9	A	B	C	D	E	F	10	11	12	13
5	6	7	8	9	A	B	C	D	E	F	10	11	12	13	14
6	7	8	9	A	B	C	D	E	F	10	11	12	13	14	15
7	8	9	A	B	C	D	E	F	10	11	12	13	14	15	16
8	9	A	B	C	D	E	F	10	11	12	13	14	15	16	17
9	A	B	C	D	E	F	10	11	12	13	14	15	16	17	18
A	B	C	D	E	F	10	11	12	13	14	15	16	17	18	19
B	C	D	E	F	10	11	12	13	14	15	16	17	18	19	1A
C	D	E	F	10	11	12	13	14	15	16	17	18	19	1A	1B
D	E	F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C
E	F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D
F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E

MULTIPLICATION

	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	2	4	6	8	A	C	E	10	12	14	16	18	1A	1C	1E
3	3	6	9	C	F	12	15	18	1B	1E	21	24	27	2A	2D
4	4	8	C	10	14	18	1C	20	24	28	2C	30	34	38	3C
5	5	A	F	14	19	1E	23	28	2D	32	37	3C	41	46	4B
6	6	C	12	18	1E	24	2A	30	36	3C	42	48	4E	54	5A
7	7	E	15	1C	23	2A	31	38	3F	46	4D	54	5B	62	69
8	8	10	18	20	28	30	38	40	48	50	58	60	68	70	78
9	9	12	1B	24	2D	36	3F	48	51	5A	63	6C	75	7E	87
A	A	14	1E	28	32	3C	46	50	5A	64	6E	78	82	8C	96
B	B	16	21	2C	37	42	4D	58	63	6E	79	84	8F	9A	A5
C	C	18	24	30	3C	48	54	60	6C	78	84	90	9C	A8	B4
D	D	1A	27	34	41	4E	5B	68	75	82	8F	9C	A9	B6	C3
E	E	1C	2A	38	46	54	62	70	7E	8C	9A	A8	B6	C4	D2
F	F	1E	2D	3C	4B	5A	69	78	87	96	A5	B4	C3	D2	E1

N	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
N **2	1	4	9	10	19	24	31	40	51	64	79	90	A9	C4	E1
N **3	1	8	1B	40	7D	D8	157	200	2D9	3E8	533	6C0	895	AB8	D2F

LECTURE 14 SOLUTIONS

14-1. Multiplication (Two words, 0-1) original by EDNASANDE

WOMEN X MEN = UTNNLM + TIWENO + NWTWNN = NLSMTUWM

0123456789
SLOWMINUET

14-2. Division (Two words, 0 -9) MORDASHKA

ATOM / ASK = N; - GNC = IS

0123456789
TASKCOMING

14-3. Multiplication. (No word, 0-1) FOMALHAUT

ASAP X MAB = RITMT + TMPRY + PDBYD =PAYDIRT

0123456789
DBARTMPIYS

14-4. Unidecimal multiplication. (Two words 0-X) WALRUS

TOUGH X DIG = IDIGDN + NYYDNG + UIHDOU = DDCUUILN

0123456789X
CLOUDYNIGHT

LECTURE 15 PROBLEMS - Taken from OP- 20 -G course:

15-1. Naval Text. Recover Keys.

J Z S S W B P D Z Z L F O M E K Q P D J H C K U M C

A B C O O X M Y S I I G B S G G Y V D S W A J O Q E

K U P W K N J K C C H W O Z Q Q B P Y N V J J O Q E

K U C D S L R W C F Q I A V M S R S I X Y T P O P G

D H U V N K V K C Y Y A L R Q O O Q D N Z C G L R E

K F H Q R N J B.

15-2. Naval Text.

A U V Z I S Z F B F Y E I R B I O W A O Y J L B L D

D G K U I T T Z B D B E Q I O C J R F W X D Y H G M

S P P I S W Y P F V S Y G G S H Q K L A L Z A Q F N

U T C Q H D G Y L B Z P D V C S J N W G N T P T M S

H J T W C K O C M X Z P Z R R U Y I W H H M E Z F L

O C F I S W L P D N W T Z H H T I R L Y I P N Q F N

U T C Q H D G Y L B Z P D V C S J N W G N T P T M E

O S V B W J B L V X Z P Z R R U Y I W H H P L P F T

R B P G X B U L V N W J P R H I H F Q X L N B L P S

H J T W I J T T Q W E E Q F O I I Z P M B J Q P Y M

D U Q W A T Z O W D C L Z Q M P U K.

REFERENCES / CRYPTOGRAPHIC RESOURCES [updated 01 July 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.

[ANDE] D. Andelman, J. Reeds, On the cryptanalysis of rotor and substitution-permutation networks. IEEE Trans. on Inform. Theory, 28(4), 578--584, 1982.

[ANGL] D. Angluin, D. Lichtenstein, Provable Security in Crypto-systems: a survey. Yale University, Department of Computer Science, #288, 1983.

[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.

[AUT4] UBET,"Auto-Transposition Cipher," SO62, The Cryptogram, American Cryptogram Association, 1962.

[AUT5] BARGE,"Decrypting the Auto-Transposition Cipher," ND63, The Cryptogram, American Cryptogram Association, 1963.

[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] Anonymous, "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.

[BAZ1] OZ,"Bazeries Cipher," MA59, The Cryptogram, American Cryptogram Association, 1959.

[BAZ2] ALII KIONA,"Bazeries Cipher," F35, The Cryptogram, American Cryptogram Association, 1935.

[BAZ3] ZANAC,"A Poker Player's Method to Solve Bazeries Ciphers," JF82, The Cryptogram, American Cryptogram Association, 1982.

[BAZ4] HI-FI,"Bazeries Ciphers Revisited," SO64, The Cryptogram, American Cryptogram Association, 1964.

[BAZ5] MACHIAVELLI,"Bazeries Cipher - Dutch," ND71, The Cryptogram, American Cryptogram Association, 1971.

[BAZ6] MACHIAVELLI,"Bazeries Cipher - English," JF71, The Cryptogram, American Cryptogram Association, 1971.

[BAZ7] MACHIAVELLI,"Bazeries Cipher - French," JF71, The Cryptogram, American Cryptogram Association, 1971.

[BAZ8] MACHIAVELLI,"Bazeries Cipher - German," MA71, The Cryptogram, American Cryptogram Association, 1971.

[BAZ9] MACHIAVELLI,"Bazeries Cipher - Italian," JA71, The Cryptogram, American Cryptogram Association, 1971.

[BAZA] MACHIAVELLI,"Bazeries Cipher - Portuguese," SO71, The Cryptogram, American Cryptogram Association, 1971.

[BAZB] MACHIAVELLI,"Bazeries Cipher - Spanish," MJ71, The Cryptogram, American Cryptogram Association, 1971.

[BAZC] MACHIAVELLI,"Bazeries Cipher - Unknown Language," MJ72, The Cryptogram, American Cryptogram Association, 1972.

[BAZD] HANO,"Bazeries Cipher - Swedish," JA81, The Cryptogram, American Cryptogram Association, 1981.

[BAZE] D. STRASSE,"Bazeries Cipher - Esperanto," SO74, The Cryptogram, American Cryptogram Association, 1974.

[BAZ5] MACHIAVELLI, "Equivalents of 'e' in the Bazeries Cipher" SO72, The Cryptogram, American Cryptogram Association, 1972.

[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.

[BEKE] H. Beker, F. Piper, Cipher Systems. Wiley, 1982.

[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)

[BEN1] John Bennett, Analysis of the Encryption Algorithm Used in the WordPerfect Word Processing Program. Cryptologia 11(4), 206--210, 1987.

[BERG] H. A. Bergen and W. J. Caelli, File Security in WordPerfect 5.0. Cryptologia 15(1), 57--66, January 1991.

[BETH] T. Beth, Algorithm engineering for public key algorithms. IEEE Selected Areas of Communication, 1(4), 458--466, 1990.

[BIF1] ESP, "4-Square Method for C. M. Bifid," SO92, The Cryptogram, American Cryptogram Association, 1992.

[BIF2] GALUPOLY, "6X6 Bifid," JA62, The Cryptogram, American Cryptogram Association, 1962.

[BIF3] DR. CRYPTOGRAM, "Bifid and Trifid Cryptography," MJ59, The Cryptogram, American Cryptogram Association, 1959.

[BIF4] TONTO, "Bifid Cipher," JJ45, The Cryptogram, American Cryptogram Association, 1945.

[BIF5] GOTKY, "Bifid Cipher with Literal Indices Only," FM47, AM47, The Cryptogram, American Cryptogram Association, 1947.

[BIF6] SAI CHESS, "Bifid-ian Timesaver," ON48, The Cryptogram, American Cryptogram Association, 1948.

[BIF7] LABRONICUS, "Bifid Period by Pattern," ND89, The Cryptogram, American Cryptogram Association, 1989.

[BIF8] TONTO, "Bifid recoveries," ON50, The Cryptogram, American Cryptogram Association, 1950.

[BIF9] GIZMO, "Bifid Period Determination Using a Digraphic Index of Coincidence," JF79, The Cryptogram, American Cryptogram Association, 1979.

[BIFA] GALUPOLY, "Bifid with Conjugated Matrices," JF60, The Cryptogram, American Cryptogram Association, 1960.

[BIFB] XAMAN EK, "Bifid Workshop, Part 1 - Encoding a Bifid," MA93, The Cryptogram, American Cryptogram Association, 1993.

[BIFC] XAMAN EK, "Bifid Workshop, Part 2 - Problem Setup," MJ93, The Cryptogram, American Cryptogram Association, 1993.

[BIFD] XAMAN EK, "Bifid Workshop, Part 3 - Tip Placement," JA93, The Cryptogram, American Cryptogram Association, 1993.

[BIFE] XAMAN EK, "Bifid Workshop, Part 4 - Solving a Bifid," SO93, The Cryptogram, American Cryptogram Association, 1993.

[BIFF] DUBIOUS and GALUPOLY, " Chi-Square Test for Bifids," JA60, The Cryptogram, American Cryptogram Association, 1960.

[BIFG] FIDDLE, "C. M. Bifid, Simplified Solution," MJ73, The Cryptogram, American Cryptogram Association, 1973.

[BIFH] ZYZZ, "Conjugated Matrix Bifid, Modified Solving Technique," SO92, The Cryptogram, American Cryptogram Association, 1992.

[BIFI] X.GOTKY, "Delastelle Bifid Cipher," AS45, The Cryptogram, American Cryptogram Association, 1945.

[BIFJ] D.MORGAN, "Finding the Period in a Bifid," JJ46, The Cryptogram, American Cryptogram Association, 1946.

[BIFK] S-TUCK, "Finding the Period in a Bifid," AM46, The Cryptogram, American Cryptogram Association, 1946.

[BIFL] S-TUCK, "Finding the Period in Bifids," ON44, The Cryptogram, American Cryptogram Association, 1944.

[BIFM] ROGUE, "General Probabilities of Part Naturals in Bifid, Trifid" JA70, The Cryptogram, American Cryptogram Association, 1970.

[BIFN] B.NATURAL, "In Line Bifid Method," MA62, The Cryptogram, American Cryptogram Association, 1962.

[BIFO] ABC, "Short Cut in a Bifid," SO61, The Cryptogram, American Cryptogram Association, 1961.

[BIFP] ROGUE, "Specific Probabilities of Part Naturals in Bifid, Trifid" SO70, The Cryptogram, American Cryptogram Association, 1970.

[BIFQ] ROGUE, "Split Half Method For Finding A Period of Bifid," MA71, The Cryptogram, American Cryptogram Association, 1971.

[BIFR] ABC, "Twin Bifids - A Probable Word Method," JA62, The Cryptogram, American Cryptogram Association, 1962.

[BIFS] GALUPOLY, "Twin Bifids," MJ60, JA60, The Cryptogram, American Cryptogram Association, 1960.

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

[BIHS] E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, vol. 4, #1, 3--72, 1991.

[BISH] E. Biham, A. Shamir, Differential cryptanalysis of Snefru, Khafre, REDOC-II, LOKI and LUCIFER. In Proceedings of CRYPTO '91, ed. by J. Feigenbaum, 156--171, 1992.

[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.

[BOYA] J. Boyar, Inferring Sequences Produced by Pseudo-Random Number Generators. Journal of the ACM, 1989.

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

[BRAG] G. Brassard, Modern Cryptology: a tutorial. Spinger-Verlag, 1988.

[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.

[BRIK] E. Brickell, J. Moore, M. Purtill, Structure in the S-boxes of DES. In Proceedings of CRYPTO '86, A. M. Odlyzko ed., 3--8, 1987.

[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.

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

[BROP] L. Brown, J. P ieprzyk, J. Seberry, LOKI - a cryptographic primitive for authentication and secrecy applications. In Proceedings of AUSTCRYPT 90, 229-236, 1990.

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

[BRO1] L. Brown, A proposed design for an extended DES, Computer Security in the Computer Age. Elsevier Science Publishers B.V. (North Holland), IFIP, W. J. Caelli ed., 9--22, 1989.

[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.

[CAD1] NIP N. BUD,"Cadenus - A Lesson in Practical Cryptography," SO55, The Cryptogram, American Cryptogram Association, 1955.

[CAD2] BERYL,"Cadenus Xenocrypt Note," SO91, The Cryptogram, American Cryptogram Association, 1991.

[CAD3] PHOENIX,"Computer Column :Cadenus," SO89, The Cryptogram, American Cryptogram Association, 1989.

[CAEL] H. Gustafson, E. Dawson, W. Caelli, Comparison of block ciphers. In Proceedings of AUSCRYPT '90, J. Seberry and J. Piepryzk eds., 208--220, 1990.

[CAMP] K. W. Campbell, M. J. Wiener, Proof the DES is Not a Group. In Proceedings of CRYPTO '92, 1993.

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

[CARJ] John Carrol and Steve Martin, The Automated Cryptanalysis of Substitution Ciphers. Cryptologia 10(4), 193--209, 1986.

[CARL] John Carrol and Lynda Robbins, Automated Cryptanalysis of Polyalphabetic Ciphers. Cryptologia 11(4), 193--205, 1987.

[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.

[CHE1] ABAKUSAN, " A tip for Checkerboard Solution," AS40, The Cryptogram, American Cryptogram Association, 1940.

[CHE2] X.GOTSKY, " On the Checkerboard, AS44,The Cryptogram, American Cryptogram Association, 1944.

[CHE3] QUARTERNION, "Straddling Checkerboard, " MA76, The Cryptogram, American Cryptogram Association, 1976.

[CHE4] PICCOLA, "The Checkerboard Alphabet, " DJ34, The Cryptogram, American Cryptogram Association, 1934.

[CHE5] SI SI, "The Hocheck Cipher Examined, " JA90, The Cryptogram, American Cryptogram Association, 1990.

[CHE5] SI SI, "The Checkerway Cipher Examined, " MJ90, The Cryptogram, American Cryptogram Association, 1990.

[CHE6] GEMINATOR, "The Homophonic Checkerboard, " MA90, The Cryptogram, American Cryptogram Association, 1990.

[CHE6] GEMINATOR, "The Checkerway Cipher, " JF90, The Cryptogram, American Cryptogram Association, 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.

[CROT] Winter, Jack, "Solving Cryptarithms," American Cryptogram Association, 1984.

[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.

[DAVJ] M. Davio, J. Goethals, Elements of cryptology. in Secure Digital Communications, G. Longo ed., 1--57, 1983.

[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.

[DEVR] HOMO SAPIENS, "De Vries Cipher," SO60, The Cryptogram, The American Cryptogram Association, 1960.

[DIG1] DENDAI, "Digrafid, A Footnote to Tip Placement," SO84, The Cryptogram, The American Cryptogram Association, 1984.

[DIG2] B. NATURAL, "Digrafid, Cipher solution," MJ61, The Cryptogram, The American Cryptogram Association, 1961.

[DIG3] KNUTE, "Digrafid Cipher," SO60, The Cryptogram, The American Cryptogram Association, 1960.

[DIG4] THE RAT, "The Buzzsaw, an Enhanced Digrafid," JA83, The Cryptogram, The American Cryptogram Association, 1983.

[DIG5] BERYL, "Digrafid, Cipher," SO93, The Cryptogram, The American Cryptogram Association, 1993.

[DIFF] W. Diffie, M. Hellman, Privacy and Authentication: An introduction to cryptography. IEEE proceedings, 67(3), 397--427, 1979.

[DIF2] W. Diffie, The first ten years of public key cryptography. IEEE proceedings, 76(5), 560--577, 1988.

[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.

[EDUC] OZ, "Educational Cryptography," MA89, The Cryptogram, The American Cryptogram Association, 1989.

[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!]

[ELLI] Carl M. Ellison, A Solution of the Hebern Messages. Cryptologia, vol. XII, #3, 144-158, Jul 1988.

[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.

[EQUI] THE OAK, "An Equi-Frequency Cipher System," JA55, The Cryptogram, The American Cryptogram Association, 1955.

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

[EVEN] S. Even, O. Goldreich, DES-like functions can generate the alternating group. IEEE Trans. on Inform. Theory, vol. 29, #6, 863--865, 19 83.

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

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

[FEI1] H. Feistel, Cryptography and Computer Privacy. Scientific American, 228(5), 15--23, 1973.

[FEI2] H. Feistel, H, W. Notz, J. Lynn Smith. Some cryptographic techniques for machine-to-machine data communications, IEEE proceedings, 63(11), 1545--1554, 1975.

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

[FIDD] FIDDLE, (Frederick D. Lynch, Col.) "An Approach to Cryptarithms," ACA Publications, 1964.

[FID1] FIDDLE, " The International Chess Cable Code," MJ55, The Cryptogram, American Cryptogram Association, 1955.

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

[FIRE] FIRE-O, "A Tool for Mathematicians: Multiplicative Structures," The Cryptogram, Vol. XXXVI, No 5, 1977.

[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.

[FOR1] VULPUS, "Four-Square Cipher," JA63, The Cryptogram, The American Cryptogram Association, 1963.

[FOR2] FIDDLE, "Further Comments on Solution of Four-Square Ciphers by Probable Word Method," FM50, The Cryptogram, The American Cryptogram Association, 1950.

[FOR3] GALUPOLY, "Numerical Four-Square Cipher," MA62, MJ62, The Cryptogram, The American Cryptogram Association, 1962.

[FOR4] SAI CHESS, "Sharpshooting the Four-Square Cipher," AM49,JJ49, The Cryptogram, The American Cryptogram Association, 1949.

[FOR5] B. NATURAL, "Solution of Type II-X Four-Square Cipher," MJ62, The Cryptogram, The American Cryptogram Association, 1962.

[FOR6] FIDDLE, "Solutionof Four-Square Ciphers by Probable Word Method," DJ49, The Cryptogram, The American Cryptogram Association, 1949.

[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.

[FRA1] SI SI, "Analysis and Optimization of the Fractionated Morse Cipher," ND81, The Cryptogram, The American Cryptogram Association, 1981.

[FRA2] B. NATURAL, "Elementary Study of the Fractionated Morse Cipher," AS51, The Cryptogram, The American Cryptogram Association, 1951.

[FRA3] X.GOTKY, "Fractionated Morse Cipher," AM50, The Cryptogram, The American Cryptogram Association, 1950.

[FRA4] CROTALUS, "Fractionated Morse Frequencies Reissued," MA93, The Cryptogram, The American Cryptogram Association, 1993.

[FRA5] RIG R. MORTIS, "Fractionated Morse Keyword Recovery," MA60, The Cryptogram, The American Cryptogram Association, 1960.

[FRA6] LAMONT CRANSTON, "Fractionated Morse Made Easy," JA92, The Cryptogram, The American Cryptogram Association, 1992.

[FRA7] MOOJUB, "General Break For Fractionated Morse," AS51, The Cryptogram, The American Cryptogram Association, 1951.

[FRA8] FIDDLE, "Periodic Fractionated Morse," AS54, The Cryptogram, The American Cryptogram Association, 1954.

[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.

[GARO] G. Garon, R. Outerbridge, DES watch: an examination of the sufficiency of the Data Encryption Standard for financial institutions in the 1990's. Cryptologia, vol. XV, #3, 177--193, 1991.

[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

[GOOD] I. J. Good, Good Thinking: the foundations of probability and its applications. University of Minnesota Press, 1983.

[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)

[HELL] M. Hellman, The mathematics of public key cryptography. Scientific American, 130--139, 1979.

[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.

[HUNT] D. G. N. Hunter and A. R. McKenzie, Experiments with Relaxation Algorithms for Breaking Simple Substitution Ciphers. Computer Journal 26(1), 1983.

[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.

[KAMD] J. Kam, G. Davida, A structured design of substitution-permutation encryption networks. IEEE Trans. Information Theory, 28(10), 747--753, 1978.

[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

[KINN] P. Kinnucan, Data encryption gurus: Tuchman and Meyer. Cryptologia, vol. II #4, 371--XXX, 1978.

[KING] King and Bahler, Probabilistic Relaxation in the Cryptanalysis of Simple Substitution Ciphers. Cryptologia 16(3), 215--225, 1992.

[KINB] King and Bahler, An Algorithmic Solution of Sequential Homophonic Ciphers. Cryptologia 17(2), in press.

[KNUT] D. E. Knuth, The Art of Computer Programming, volume 2: Seminumerical Algorithms. Addison-Wesley, 1981.

[KOCH] Martin Kochanski, A Survey of Data Insecurity Packages. Cryptologia 11(1), 1--15, 1987.

[KOCM] Martin Kochanski, Another Data Insecurity Package. Cryptologia 12(3), 165--177, 1988.

[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.

[KOZC] W. Kozaczuk, Enigma. University Publications of America, 1984 ov, Elementary Cryptanalysis. Math. Assoc. Am. 1966.

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

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

[KUL1] Soloman Kullback, Information Theory and Statistics. Dover, 1968.

[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.

[LAKS] S. Lakshmivarahan, Algorithms for public key cryptosystems. In Advances in Computers, M. Yovtis ed., 22, Academic Press, 45--108, 1983.

[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!]

[LED1] LEDGE, "Basic Patterns in Base Eleven and Twelve Arithmetic (Part 1) ," The Cryptogram, American Cryptogram Association, Vol XLIII, No. 5, 1977.

[LED2] LEDGE, "Basic Patterns in Base Eleven and Twelve Arithmetic (Part 2) ," The Cryptogram, American Cryptogram Association, Vol XLIII, No. 6, 1977.

[LEMP] A. Lempel, Cryptology in transition, Computing Surveys, 11(4), 285--304, 1979.

[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.

[LEWN] 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.'

[LUBY] C. Rackoff, M. Luby, How to construct psuedorandom permutations from psuedorandom functions. SIAM Journal of Computing, vol. 17, #2, 373--386, 1988.

[LUCK] Michael Lucks, A Constraint Satisfaction Algorithm for the Automated Decryption of Simple Substitution Ciphers. In CRYPTO '88. 598--605, 1979.

[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.

[MASS] J. Massey, An introduction to contemporary cryptology, IEEE proceedings, 76(5), 533--549, 1988.

[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.

[MER4] R. Merkle, Fast software encryption functions. In Proceedings of CRYPTO '90, Menezes and Vanstone ed., 476--501, 1991.

[MEYE] C. Meyer and S. Matyas, Cryptography: A new dimension in computer security. Wiley, 1982.

[MEYR] C. Meyer, Ciphertext/plaintext and ciphertext/key dependence vs. number of rounds for the Data Encryption Standard. AFIPS Conference proceedings, 47, 1119--1126, 1978.

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

[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.

[ORAN] The ``Orange Book" is DOD 520 0.28-STD, published December 1985 as part of the ``rainbow book" series. Write to Department of Defense, National Security Agency, ATTN: S332, 9800 Savage Road, Fort Meade, MD 20755-6000, and ask for the Trusted Computer System Evaluation Criteria. Or call 301-766-8729. The ``Orange Book" will eventually be replaced by the U.S. Federal Criteria for Information Technology Security (FC) online at the NIST site [FTPNS], which also contains information on other various proposed and active federal standards.

[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.

[PATT] Wayne Patterson, Mathematical Cryptology for Computer Scientists and Mathematicians. Rowman & Littlefield, 1987.

[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.

[PELE] S. Peleg and A. Rosenfeld, Breaking Substitution Ciphers Using a Relaxation Algorithm. CACM 22(11),

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

[PFLE] C. Pfleeger, Security in Computing. Prentice-Hall, 1989.

[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.

[PRI1] W. Price, D. Davies, Security for computer networks. Wiley, 1984.

[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.

[REED] J. Reeds, `Cracking' a Random Number Generator Cryptologia 1(1), 20--26, 1977.

[REE1] J. A. Reeds and P. J. Weinberger, File Security and the UNIX Crypt Command. AT&T Bell Laboratories Technical Journal, Vol. 63 #8, part 2, 1673--1684, October, 1984.

[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

[RUEP] R. Rueppel, Design and Analysis of Stream Ciphers. Springer-Verlag, 1986.

[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 Tables," 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.]

[SALO] A. Saloma, Public-key cryptography. Springer-Verlag, 1990.

[SHAF] Shafi Goldwasser, Silvio Micali, Probabilistic Encryption and How To Play Mental Poker Keeping Secret All Partial Information. Proceedings of the Fourteenth Annual ACM Symposium on Theory of Computing, 1982.

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

[SHAN] C. Shannon, Communication Theory of Secrecy Systems Bell System Technical Journal 28(4), 656--715, 1949.

[SHEM] B. Kaliski, R. Rivest, A. Sherman, Is the Data Encryption Standard a Group. Journal of Cryptology, vol. 1, #1, 1--36, 1988.

[SHIM] A. Shimizu, S. Miyaguchi, Fast data encipherment algorithm FEAL. EUROCRYPT '87, 267--278, 1988.

[SHIR] K. Shirriff, C. Welch, A. Kinsman, Decoding a VCR Controller Code. Cryptologia 16(3), 227--234, 1992.

[SIMM] G. Simmons (ed.), Contemporary Cryptology: the Science of Information Integrity. IEEE press, 1991.10.4. Reference articles

[SORK] A. Sorkin, LUCIFER: a cryptographic algorithm. Cryptologia, 8(1), 22--35, 1984.

[SPIL] R. Spillman et al., Use of Genetic Algorithms in Cryptanalysis of Simple Substitution Ciphers. Cryptologia 17(1), 31--44, 1993.

[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.

[WELH] D. Welsh, Codes and Cryptography. Claredon Press, 1988.

[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.

[YAOA] A. Yao, Computational Information Theory. In Complexity in Information Theory, ed. by Abu-Mostafa, 1988.

[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.