CLASSICAL CRYPTOGRAPHY COURSE
BY LANAKI

April 6, 1996
Revision 0

LECTURE 10

POLYALPHABETIC SUBSTITUTION SYSTEMS I
VIGGY'S FAMILY AND QUAGMIRES I - IV
APPLICATIONS OF THE PRINCIPALS OF SYMMETRY

SUMMARY

In Lecture 10, we return to our course schedule with a study of fascinating cipher systems based on multiple alphabets -Polyalphabetic Substitution systems. What is amazing about these systems is how long they remained secure. The Viggy systems (my name for Vigenere) was considered unbreakable for over 200 years. Along comes Major Kasiski, and poof, we have recreational cryptography.

I think the best way to introduce the subject is via an overview based on the Op-20-GYT course notes (Office of Chief Of Naval Operations, Washington) [OP20]. From there, I will bring in MASTERTON's dissolution of QUAGMIRES I-IV. [MAST]

In Lecture 11, we will revisit polyalphabetic cipher systems and the polygraphic cases using Friedman's detailed analysis. We will cover the PORTA system and other family members. I will cover decimation processes in detail. [FRE4], [FRE5], FRE6], [FRE7], [FRE8]

In Lecture 12, we will describe the aperiodic polyalphabetic case and give a diagram of topics considered in Lectures 10 -12. [FR3]

I have updated our Resources Section with many references on these systems - focusing on the cryptanalytic attack and those of historical interest. Kahn has some interesting stories about the Viggy family. [KAHN]

POLYALPHABETIC SUBSTITUTION

A cipher system which employs two or more cipher alphabets and includes a method for designating which cipher alphabet is to be used for the encipherment of each plain-text letter, is called a polyalphabetic substitution system. Cipher systems employing variant values may appear to use more than one alphabet, but they have characteristics of mono-alphabetic substitution and are properly classified as such.

Polyalphabetic substitution systems consists of two general types; periodic and non-periodic.

(a) In the periodic type the text of a message is divided into definite, regular groups or cycles of letters which are enciphered with identical portions of the key. Periodic systems are further subdivided as follows:

(1) Multiple Alphabet Ciphers in which any number of cipher alphabets are used in order designated by a prearranged key.

(2) Progressive Alphabet Ciphers in which a primary cipher alphabet and its 25 secondary alphabets are used either in regular succession, sliding the components one letter at a time, or in irregular order according to a prearranged shift.

(b) In the non-periodic type there are no cyclic repetitions of the key.

The cipher alphabets employed in multiple alphabet substitution systems may be constructed by any number of methods. As an example, the QUAGMIRE IV uses both vertical and horizontal keywords.

Example:

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

Here the plain component is a normal sequence, and the cipher component are identical keyword sequences. The same keyword sequences may be used in both the plain cipher components, or different sequences may be used. The key which determines the setting of the cipher alphabets against the plain component (RED) may be any prearranged word or phrase. Also, each cipher alphabet may be assigned a number and the alphabets used in accordance with a prearranged numerical key.

The process of enciphering a message with the multiple alphabet system above would appear as follows:

Cipher Alphabet No.

```
          1-2-3-1-2-3-1-2-3-1-2-3-1-2-3-1-2-3-1-2-3-1-2-3

Plain  -  M Y C O U R S E Z E R O T H R E E Z E R O A T T
Cipher -  I Z G S V P F L B W R X G B P W L B W R X R U N

          1-2-3-1-2-3-1-2-3-1-2-3-1-2-3-1-2-3-1-2-3

Plain  -  H I R T E E N T H I R T Y T H R E E
Cipher -  Z D P G L J L U O P R N O U O D L J
```

In order to reduce the chances of encipherment by the wrong alphabet, the plain text is often written so that the letters designated by the key for encipherment by each alphabet are placed in the same vertical column.

Note the repetitions in the plain text which begin at the same point in the key produce repetitions in the cipher text, while others [may not] do not. Friedman discusses accidental repetitions in [FR7].

PRINCIPLES OF FACTORING

Major Friedrich W. Kasiski (1805-1881) was a career officer in East Prussia's 33 Infantry Regiment. He is credited with a revolutionary insight regarding polyalphabetic repeating key systems - that the conjuction of a repeated portion of the key with the repetition in the plaintext produces a repetition in the ciphertext. Like causes produce like effects. The interval between plaintext or ciphertext repetitions is noted throughout the cryptogram, factored and the commonality of the factor is a good indication of the key and number of alphabets used to encipher the original methods. The fall of the Vigenere family is attributed to Kasiski's examination. [KASI] [KAS1], [KAHN]

If there are several long repetitions in the cipher text of an unknown system, the intervals between the initial letters of these repetition have a common factor, this factor represents the number of alphabets used to encipher the message and the exact number of repetitions of the key.

A simple example:

Given the cryptogram:

IZGSV PFLBW RXGBP WLBWR XRUNZ

DPGLJ LUOPR NOUOD LJ

Factoring:

Repetition	Interval	Factors	Common Factor(s)
LBWRX	9	3,3	3
LJ	12	2,2,3	3
UO	6	2,3	3

The "period" or common factor is three and this is the number of alphabets employed.

Digraph and trigraph repetitions may be the result of chance instead of plain text repetitions. [FR7] discusses in detail.

When factoring results in more than one common factor we shall use the highest common factor and check with frequencies of the expected alphabets to see how close to normal they are. Only short messages fail to lead to the correct determination of the number of cipher alphabets employed in the system. When factoring fails on a longer message, an aperiodic cipher may have been employed.

SOLUTION OF A MULTIPLE ALPHABET CIPHER

Phamplet Number 7, Office of Operations Cryptanalysis, Office of the Chief of Naval Operations, Washington, 1930 [OP20] prepared this problem for discussion.

From: A B (Black Force Commander)
To: CD, EF, GH, IJ (Black Ships)
Time Groups: 0013-2300 April 1930
Remarks: Cruiser transmitter.

Cryptogram written out in worksheet format:

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

Collateral Information:

The Black and Blue Fleets are engaged in war maneuvers in the Caribbean Sea. The Fleets are not in contact. The location of the enemy (the Black Fleet) is unknown. The message in question was intercepted by the Blue Flagship at 0015 on 14 April 1930. The operator had reason to believe that a cruiser sent the message.

The composition of the Black Fleet is as follows:

Battleships	Cruisers
West Virginia (flag)	Trenton (flag)
Maryland	Marblehead
Tennessee	Richmond
New Mexico	Memphis
Mississippi	
California	
Destroyers	**Air Force**
Litchfield (flag)	Saratoga (flag)
Preble	Langley
Pruitt	Gannet
Noa	
Decatur	**Submarine Force**
Sicard	
Hulbert	Argonne (flag and tender)
William B. Preston	V-1, V-2, V-3

Factoring:

Repetition	Interval	Factors
ZMJKAQJBF	210	2,3,5,7,10
ZMJKAQJBF	270	2,3,3,5,10
ZMJKAQJBF	60	2,2,3,5,10
MHZMVHA	120	2,2,2,3,5,10
ZMV	40	2,2,2,5,10
ZMV	160	2,2,2,2,2,5,10
KPK	50	2,5,5,10

The highest common factor is 10; the period and number of alphabets used is 10, so the sequence repeats itself after each 10 letters.

"Lining-up" is one of the basic operations of solution. We group the message in lines of ten letters. The letters in each column are enciphered by the same alphabet. Checking the frequency tables, each alphabet resembles a single alphabet.

Frequency Tables

#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
A 1	A 1	A 1	A 9	A 4	A 1	A 4	A	A 2	A 2
B	B 3	B 1	B 4	B 2	B 1	B 6	B	B	B
C	C	C 3	C 2	C	C 5	C 1	C 2	C 1	C
D 1	D 2	D	D 3	D	D 1	D 2	D 1	D	D
E 2	E 1	E	E	E 2	E	E	E	E 1	E
F	F 5	F	F	F	F	F	F 4	F	F
G 1	G 2	G	G 1	G 1	G	G 4	G 1	G 2	G
H	H	H 3	H	H	H 1	H	H 3	H 6	H 6
I 2	I	I	I 1	I	I	I 1	I	I	I
J 1	J 4	J 1	J	J 4	J 3	J	J 1	J 1	J 1
K 4	K	K 5	K 1	K	K 2	K 2	K 1	K 1	K
L 2	L	L 1	L 1	L	L 6	L 1	L 2	L	L
M 7	M	M 4	M	M	M	M	M 8	M 1	M 1
N	N	N 1	N	N	N 2	N 3	N	N	N
O 3	O	O 2	O	O	O 1	O 1	O 1	O 5	O
P	P 4	P	P 1	P 1	P 2	P 1	P 1	P	P 1
Q	Q	Q 1	Q 1	Q 4	Q	Q	Q	Q 1	Q 2
R	R	R	R 1	R	R	R 1	R	R	R 1
S 1	S	S 1	S	S 4	S 1	S	S	S 3	S 2
T	T	T 2	T	T 1	T	T 1	T	T 3	T 2
U	U	U	U	U 3	U 1	U	U	U	U
V	V 6	V	V	V	V 3	V	V 1	V	V
W	W	W 3	W	W 3	W	W	W 3	W	W 2
X 1	X 1	X 1	X 3	X	X	X	X 1	X	X
Y 1	Y 1	Y	Y	Y	Y	Y	Y	Y	Y
Z 3	Z	Z	Z 1	Z 1	Z	Z 2	Z	Z 2	Z 9
30	30	30	30	30	30	30	30	29	29

SOLUTION BY KNOWN-WORD METHOD

When ample collateral information is available, the known-word attack is the easiest and potentially the quickest method of solution. From the given data, the message is presumably from the Commander of a cruiser division to his four cruisers, giving orders for scouting operations of the cruiser division.

The words most likely to appear are:

Scouting	Scouting line	Trenton	Latitude
Course	Scouting course	Marblehead	Longitude
Speed	Scouting speed	Richmond	Hundred
Distance	Scouting distance	Memphis	Numbers
Position	Commence scouting	Enemy	Times/Dates

Our concern is not with guessing words but standardizing the solution.

The Known-Word" method applied in two ways:

(1) Start at a particular point in the cryptogram indicated by the repetitions, symmetrical sequences, and try to fit the known-word at this point. This is called the "Obvious Location Method."

(2) Start with a "Known-word" and find a place where it will fit. This may be called the "Obvious Word Method."

The best method to use depends on the circumstances. In this problem both methods apply.

OBVIOUS LOCATION

The long repetitions are words or phrases, important to the subject of the message, and may be known-words. They are excellent points of attack. The beginning of the message or the end of the message are usually good points of attack.

The second longest repetition is the right length for Trenton, Memphis, or Hundred; furthermore it links in the letters of the longest repetition.

Original Assumptions -

```
MHZ MVHA     lines 15-27  TRENTON is best assumption.
TRE NTON
MEM PHIS
HUN DRED
```

Check

```
MOZ MJKAQJBF  lines 24, 30     MOZ MJKAQJBF  could be
T E N  N      Excellent        TEE NHUNDRED  excellent
M M P  S      Poor             THE E--N ---  poor
H N D  D      Poor
```

Check

```
MCZ MVX       lines 1-12
TWE NTY       excellent
M M PH        poor
H V DP        poor
```

Check the values of TEEN HUNDRED and TRENTON

```
Line 2-3       12345678910     12345678910
               IAMCBBNMSZ      MJKAQJBFZA
                      T E      NHUNDRED
 suggests            ATTE      NHUNDRED

Line 23-24     GVWBZCAMOZ      MJKAQJBFDI
                T     TEE      NHUNDRED
 suggests         THIR
                  FOUR
                   FIF
                   SIX
               ATSEVEN
                  EIGH

Lines 29-30    OPLAULBMOZ      MJKAQJBF--
                  N  ETEE      NHUNDRED
suggests          NINETEE      NHUNDRED
```

It is possible that all the above assumptions are incorrect but they are too good to ignore. We enter the above values into the cryptogram to see if skeletons of words appear.

Possibilities are indicated below:

```
Lines 19-20     12345678910     12345678910
                EFWKGCBFTH      SVCBBUAHSS
                      ED         T      T
                   SPEEDFI      FTEENKNOTS
                        SI      X
```

Line 19 ED could be Speed.. building on that we have other possibilities.

```
Lines 21-22     KPKDECGOHZ      LVODSCOCHA
                  U     RE       T      R
                COURSETHRE      ETHREEZERO

Lines 11-12     ZEWIJKGMCZ      MVXXUNBWZT
                       T E      NT    E
                       TWE      NTYMILES
                      T             THREE
                                   FIVE
```

TRENTON is the most obvious break. Check letter-combinations of frequencies to see which of the three chosen words fitted best.

```
HZ =1       ZMV=1    ZM =4   HA=1
RE          ENT      EN      ON      Trenton is only assumption
EM          MPH      MP      IS
UN          NDR      ND      ED

Frequency     869  7639
Cipher        MHZ  MVHA

Frequency     XXX  XXXX      X = high frequency
Plain         TRE  NTON
                             - = intermediate frequency
Frequency     -X-  --XX
Plain         MEM  PHIS      O + low frequency

Frequency     --X  -XX-
Plain         HUN  DRED
```

OBVIOUS WORD METHOD - LOCATION BY FREQUENCIES

One method of fixing the location of an obvious word is by frequencies, provided the obvious word has one or more letters of very low frequency. The word should be 10 or more letters to be practical.

The possibilities are RENDEZVOUS and MARBLEHEAD.

First, frequencies are written over each letter of the cryptogram. The Known-word is put on a card and slid over the cryptogram until it fits with the very low frequency letters and neighbors. This method is rather tedious and painful, but good in a pinch.

OBVIOUS WORD METHOD - LOCATION BY SYMMETRY OR REPETITIONS

Location of words by symmetry is commonly employed when dealing with single key ciphers. With double key ciphers its application depends much on chance. If the alphabets are repeated in the key or the key is short, we employ a limited form of symmetry.

With a non repeating key or very long key, this method fails. With a fairly short key we employ this method provided:

(1) We assume a word or phrase longer than the key, and
(2) This word or phrase happens to contain a letter repeated at an interval equal to the length of the key.

For our sample problem, one of our choices might be

10 letter key - SCOUTINGDISTANCE

Therefore, any place in the cryptogram where two successive lines have common letters in the same column is a possible location of our word. Failure to find this location, eliminates the possibility of this word.

Table one partially shows the ciphertext where repeated letters are ten spaces apart. Of the twelve possibilities for the word "SCOUTINGDISTANCE" some are eliminated by frequencies of the letters C,G,C, others by letter combinations and the balance by test. All fail.

Our Navy students would try the scouting line of cruisers as:

```
  4             3                   1          2
MEMPHIS       RICHMOND           TRENTON    MARBLEHEAD
  2             1          OR       3          4
MARBLEHEAD    TRENTON            RICHMOND   MEMPHIS
               (flag)
```

These names might appear as follows:

```
       MEMPHISRIC                  MARBLEHEAD
       HMONDTRENT      OR          TRENTONRIC
       ONMARBLEHE                  HMONDMEMPH
       AD                          IS
```

These can be checked against Table I and cross checked by frequency or digram analysis.

We have a little luck at Line 14 - 15 - 16

```
Line 14             LGTBWPLVTT
                    --MEMPHISR

Line 15             OBOXJLRMHZ
                    ICHMONDTRE

Line 16             MVHAWADGGZ
                    NTONMARBLE
```

check

```
Line 29             OPLAULDMOZ          Line 11        MOZ
                    I  N N T E                         I E
                       NINETEE                         TWE

Line 30             MJKAQJBF            Line 12        MVX
                    NHUNDRED                           NT
                                                       NTY
```

OBVIOUS LOCATION METHOD

Table I gives a list of obvious locations. We suspect the word COURSE followed by a ZERO and ONE TWO or THREE.

Some possibilities are:

```
COURSEZERO              COURSETHRE
FOUR                    EZERO

COURSEONET              COURSETHRE
WO                      EONE


COURSEZERO              (promising but no check)
FOUR

COURSETHRE
ETHREE                  (checks with #9 in Table I)
```

Assumption

```
Line 21         KPKDECGOHZ        Line 26   S KPKGULT
                                              COU
                                            S COUTING

Line 22         LVODSCOCHA
                ETHREEZERO
```

Both assumptions are entered into the cryptogram.

TABLE I

Lines		Reference
6-7	ZFSAASZDEPZXCDJD	1
8-9	KAHPLGHAJMKTVAMK	2
8-9	HAJMKTVAMKHMBCAA	3
10-11	ZZDWIJKGMCZMVXXU	4
15-16	ZMVHAWADGGZYFARQ	5
17-18	FARQVKMMQKFMPSLG	6
18-19	FPMSLGXAHEFWKGCB	7
18-19	HEFWKGCBFTHSVCBB	8
21-22	DECGOHZLVODSCOCH	9
21-22	CGOHZLVODSCOCHAG	10
21-22	HZLVODSCOCHAGVWB	11
22-23	VCDSCOCHAGVWBZCA	12
22-23	COCHAGVWBZCAMOZM	13
24-25	AQJBFJHXBHAAVAKO	14
25-26	OSKPKGULTJOQDFQQ	15
28-29	AEPZWQROPLAULBMO	16
29-30	AVLBMOZMJKAQJBF	17

TABLE II

12345678910	12345678910	12345678910		12345678910	
COURSEZERO	COURSETHRE	COURSEONE		COURSETWO	
ZERO	EZERO	ERO	Z	ERO	Z
ONE	ONE	NE	O	NE	O
TWO	TWO	WO	T	WO	T
THREE	THREE	HREE	T	HREE	T
FOUR	FOUR	OUR	F	OUR	F
FIVE	FIVE	IVE	F	IVE	F
SIX	SIX	IX	S	IX	S
SEVEN	SEVEN	EVEN	S	EVEN	S
EIGHT	EIGHT	IGHT	E	IGHT	E
NINE	NINE	INE	N	INE	N

COURSEZERO	COURSETHRE	COURSEONET	COURSETWOT
FOUR	EZER	WO	WO
	EONE		
	ETHREE		

DISCOVERY OF THE SYSTEM

We study the values assumed previously:

Value	Alphabets	Value	AlphabetS
C=E	3,6,8	H=O, O=H	3,6,8
O=H	3,8	N=L,L=N	3,6,8
H=O	3,8	K=U, U=K	3,6,8
B=E	4,7	N=A,A=N	4,7
A=N	4,7	S=E,E=S	5

The common values indicate that alphabets 3,6, and 8 are identical and similarly so are 4 and 7. Five reciprocal values are noted without inconsistencies. Seven different alphabets are used. The alphabets are probably reciprocal.

If the seven alphabets are Secondary (derived from the same cipher component set against the same plaintext but in different alignments) a short cut solution is possible. We can next combine the alphabets into one system.

We have enough clear text to solve the cryptogram - I leave the balance to the student.

Alpha. -	1	2	3	4	5	6	7	8	9	10
1	K	P	T	X	S	L	I	C	T	M
	C	O		M	E	N		E		
2	I	A	M	C	B	B	N	M	S	Z
			T		N		A	T	T	E
3	M	J	K	A	Q	J	B	F	Z	A
	N	H	U	N	D	R	E	D		O
4	J	G	M	B	S	L	N	P	H	H
			T	E	E	N	A		R	I
5	E	E	J	Z	W	N	C	L	O	W
			R			L		N	E	
6	Z	F	S	A	A	S	Z	D	E	P
				N						
7	Z	X	C	D	J	D	D	H	A	J
			E	R			R	O		
8	O	D	B	K	A	H	P	L	G	H
				S		O		N		I
9	A	J	M	K	T	V	A	M	K	H
		H	T	S			N	T		I
10	M	B	C	A	A	C	N	W	S	Z
	N		E	N		E	A	S	T	E
11	Z	D	W	I	J	K	G	M	C	X
			S			U	T	T	W	E
12	M	V	X	X	U	N	B	W	Z	T
	N	T	Y	M	I	L	E	S		
13	I	Y	N	C	P	O	G	H	H	W
			I			H	T	O	R	
14	L	G	T	B	W	P	L	V	T	T
	E			E						
15	O	B	O	X	J	L	R	M	H	Z
			H	M		N		T	R	E

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

TABLE III
DECIPHERING TABLE

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

TABLE IV
ENCIPHERING TABLE

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

Op-20-G gives us the quick and dirty of the problem. We need to understand what equivalent cipher alphabets are and how the multiple alphabet system lends itself to reconstruction.

EQUIVALENT CIPHER ALPHABETS

Any sequence containing 26 letters may be rearranged so that all the letters which are originally separated by equal intervals will also be spaced at equal intervals in the new related sequences. Including the original sequence, a total of of six related sequences may be constructed. [Friedman expands on this principle in FR7.]

Example:

	1	3	5	7	9	11																				
1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	A	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W	Z	C	F	I	L	O	R	U	X
3	A	F	K	P	U	Z	E	J	O	T	Y	D	I	N	S	X	C	H	M	R	W	B	G	L	Q	V
4	A	H	O	V	C	J	Q	X	E	L	S	Z	G	N	U	B	I	P	W	D	K	R	Y	F	M	T
5	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R
6	A	L	W	H	S	D	O	Z	K	V	G	R	C	N	Y	J	U	F	Q	B	M	X	I	T	E	P

In this example, a normal alphabet sequence has been re-spaced to form five related sequences. In constructing them, the original sequence is regarded as a circle and the letters are counted off in equal intervals, then written in adjacent positions to form a related sequence.

Only the odd intervals from 3 - 11 can be used in re-spacing a 26 letter sequence to form different related sequences. {primes} Even intervals will produce only 13 letter sequences, and the interval 13 can not be used. Odd intervals from 15-25 will produce identical sequences with those from 1-11 but in reversed direction. (like the Porta)

Cipher alphabets may be re-spaced to form equivalent cipher alphabets by the same process as that applied to construct related sequences.

Example:

Original Cipher Alphabet

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

Equivalent Cipher Alphabet

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

An equivalent cipher alphabet can not be distinguished from the original cipher alphabet unless a systematic construction or some outside information is available to identify the original one. The secondary alphabets generated by shifting the points of coincidence of the plain and cipher components are the same alphabets regardless of which equivalent cipher alphabet has been shifted.

Example:

Original Cipher Alphabet

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

Equivalent Cipher Alphabet

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

The secondary alphabet of this example has been derived by shifting the cipher component of the original alphabet of the previous paragraph, and the equivalent secondary cipher alphabet by shifting the cipher component of the equivalent alphabet of the previous paragraph.

The number of spaces each cipher component has been shifted is not the same in each case, yet the plain and cipher values correspond exactly. This illustrates the most important principle of symmetry in the secondary alphabets.

RECONSTRUCTION OF MULTIPLE ALPHABET SYSTEMS

When the same sequence has been used for each of the cipher components of a multiple alphabet system, there are definite relationships between the individual cipher values which may be used in recovering other cipher values after a few have been identified through analysis.

(a) When the plain component is originally a normal sequence the cipher sequences will be recovered in their original order and new values may be placed in the various cipher components as soon as their relative positions have been established.

(b) When the plain and cipher components are originally the same mixed sequence, the plain component enters into the reconstruction in the same manner as the other cipher component.

(c) The reconstruction of a multiple alphabet system in which the plain component is a different mixed sequence from that used in the cipher components, requires a relatively large number of values for analysis.

The principles are explained by another example in which the plain and cipher components are different mixed sequences:

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

The interval between letters of two cipher components, letters which occur in the same vertical column, is equal to the amount of displacement of one component from the other.

O (1) To N(2) is an interval of one, the amount of shift between the cipher components (1) and (2).

E (3) to O (1) is the same interval as O (3) to U (1), and is the same interval as U (3) to F (1), etc.

Thus a chain of letters, EOUF with current relative spacings could be made from the vertical relationship alone, when the order of plain component sequence is unknown. A set of equivalent alphabets might be the result of construction by this means, but the original in this case would be recognized when the proper spacing is found.

If the vertical relationship is used between components which are displaced an even number of letters, such as ciphers (2) and (3), a chain of 13 letters will result, and if the components were originally displaced 13 letters, they would show only reciprocal relationships.

APPLICATION OF SYMMETRY PRINCIPLES

Suppose the Enciphering table obtained during the solution of a cryptogram appeared as follows:

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

Since the interval between R and P in the cipher sequence is the same as that between P and F, we may arbitrarily assume this interval to be one and build up a cipher sequence accordingly.

The vertical columns remain unchanged. We write:

```
0    E I       R in the third cipher           S E I
1    R P F     component appears under         G R P F U O
2    U O       S plain, so we continue   G R P F U O
3  R P F                                   G R P F U O
```

The progress of adding values to the plain and cipher sequences progresses through the various stages:

```
0              T     S E I R B     Y
1              I S   G R P F U O E H      T
2        I S    G R P F U O E H     T
3             I S   G R P F U O E H      T

0          O     L T     S E I R B     Y   N C
1          W J   V I S   G R P F U O E H   C T   B Z
2    W J   V I S   G R P F U O E H   C T   B Z
3       W J   V I S   G R P F U O E H   C T   B Z
```

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

The intervals between E, F, G and between V, W, X in the cipher sequence obtained above, indicate the equivalent alphabets have been recovered which should be re-spaced by counting off every third letter in the reverse direction.

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

CONTINUATION OF BLACK FORCE CRYPTOGRAM

A few more values are necessary in Table IV in order to completely reconstruct the system used.

```
Line 1                          Line 18

Alpha    1 2 3 4 5 6 7 8 9 10   Alpha    1 2 3 4 5 6 7 8 9 10
Cipher   K P T X S L I C        Cipher   K F M P S L G X A H
Plain    C O   M E N   E        Plain    C   T   E N T Y   I
New          M       C          New            W

Line 3 to 5

Alpha    1 2 3 4 5 6 7 8 9 10   1 2 3 4 5 6 7 8 9 10    1
Cipher   M J K A Q J B F Z A    J G M B S L N P H H     E
Plain    N H U N D R E D   O        T E E N A   R I
New                      F      U R           P         L
```

Adding these new values to Table IV gives the following table for use in reconstruction of the system:

TABLE IV
Revised
ENCIPHERING TABLE

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

The reciprocal relationship will be ignored.

On account of L and B being found in two vertical columns, a good starting point is to assume that L and B are adjacent in the cipher component. Then we would have the following in the cipher component: GN, KI, MA, FQ, CS, PQ, AND WE.

Using the PGN sequence in the first three cipher components, partial reconstruction can be made:

```
PLAIN-          W T A           O R         P   L
1                 P G N                       W E
2                 V             P G N
3-6-8             M A           H J         P G N
4-7             P G N             D
5                                         P G N
9               C S               H J
10                            M A
```

Since HJ appears with the same interval as LB, then OC and SM are also adjacent in the cipher sequence being constructed.

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

We combine the three partials:

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

I think you can see that most of the cipher sequence could be obtained without considering the fact that the plain component is the same sequence reversed. The important point is that the complete system may be reconstructed from relatively few values obtained through analysis of the cryptogram.

The sequence used in this problem is randomly mixed, therefore the original one can not be distinguished from a related one which may be reconstructed. The ten cipher components are set with the key GUANTANAMO under the A plain.

FURTHER REMARKS

The same method used in determining which cipher values probably represent vowels or consonants may be applied to poly-alphabetic substitution ciphers as described in Lectures 1 and 2. However, the values in each alphabet must be considered with their respective prefixes and suffixes in adjacent alphabets, in studying the frequencies of their combinations.

After the original sequences of a poly-alphabetic substitution system are recovered, subsequent messages using these sequences may be solved by a modified method. The "generatrix frequency" method was developed by W. F. Friedman and is described in FR7.

SOLVING CIPHER SECRETS

MASTERTON (Frank W. Lewis) was a personal 'pick' of William F. Friedman. His experience and book [MAST] is as insightful as it is brilliant. He takes us through the QUAGMIRE family. The American Cryptogram Association calls the class of periodic polyalphabetic substitution QUAGMIRES I, II, II, IV after the terminology used for keying Aristocrats. QUAGMIRES have a mixed alphabet in at least one of the components. QUAGMIRE I uses a keyword-mixed plain component with a determined number of normal cipher alphabets at different settings; QUAGMIRE II uses a normal plain and various settings of the same mixed cipher component; QUAGMIRE III employs the same mixed alphabet for plain and cipher (juxtaposition repeated on a cycle); and QUAGMIRE IV which has one mixed alphabet for plain and a series of slides of another mixed alphabet for the cipher components. [MAST] The use of normal alphabets on a cycle, either direct or reverse, is a weakness because the components are known and are more vulnerable to solution.

QUAGMIRE I

We will take the QUAGMIRES in turn, making sure we understand the method of encipherment and tricks of unraveling the text.

Lets build an alphabet on the Keyword ENCIPHERMENT:

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

Let us take a NORMAL alphabet, with C under the first letter of plain sequence. This is cipher setting No 1. Slide the normal alphabet to I, under E, P, H, E, R to get:

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

I have numbered the alphabets for ease of use. The initial column keyword is standard practice.

To encipher the word regarding: The first R is found in the plain sequence, and the letter under it in alphabet 1 is I, we use the cipher alphabets sequentially and return to alphabet 1 after using the sixth alphabet.

QUAGMIRE I ATTACK

Given:

```
WBFWX  LWVPY  WICQJ  HJYDL  LNABF  JCQFB  BHMPA  XGKIU  CRHVK

YNEJO  VMDEJ  SPQPT  GLFFB  YOEYD  MIHYY  JJCPY  YDVIE  TOFXX

LWPSC  YTBKJ  ORCYZ  DBYDH  YHR.
```

The Cryptogram usually provides a tip: "ILEANDTHENREPLIED. " This will appear in the text someplace.

The repeat method of factoring doesn't work to well on this example. So assume 6, 7 or 8. Write the crib based on those cycles.

```
    awh            awh            awh
ILEAND         ILEANDT        ILEANDTH
THENRE         HENREPL        ENREPLIE
PLIED          IED            D
```

We have added a possible text of awh to the crib. The middle crib has the I over an I 13 letters apart and the E's interval of 6. The stretch of cipher we want will have a repeat as:

```
                  ----X------Y-----XY---.
```

The stretch "glffbYoeydmihYyjjcpYYdvie" fits the bill. We rewrite the cryptogram into a cycle of seven letters either in columns or rows. We fill in the tip and number the alphabets:

```
1234567  1234567  1234567  1234567  1234567  1234567  1234567
WBFWXLW  VPYWICQ  JHJYDLL  NABFJCQ  FBBHMPA  XGKIUCR  HVKYNEJ


1234567  1234567  1234567  1234567  1234567  1234567  1234567
OVMDEJS  PQPTGLF  FBYOEYD  MIHYYJJ  CPYYDVI  ETOFXXL  WPSCYTB
               a  whILEAN  DTHENRE  PLIED

1234567  1234567  1
KJORCYZ  DBYDHYH  R.
```

We prepare a deciphering tableux, putting the plain values above the normal cipher strip and using the plain E to start.

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

Since the fourth alphabet also has a plain L, we enter it on the top line, and similarly place a plain N from the fifth alphabet. The N is confirmed by its appearance in the 7th alphabet, so we know we are on the right track.

Since we have the plain L, the second alphabet comes in too and hence the plain H and T. This gives us the third alphabet and the plain I. There is more help. Looking down the various columns we find the Keyword COUNTRY which must have been placed under the first letter of the plain sequence. Snowballs.

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

The clues add up. The Keywords are PLOWING and COUNTRY.

The RST sequence is obvious. The message reads: The city slicker asked the farmer what's your mules name? The farmer thought awhile and replied I don't rightly know but I call him JACK.

QUAGMIRE II

This polyalphabetic substitution uses a Normal plain and a keyword mixed cipher alphabet. Lets tackle a problem with the tip of 20 letters TAPHORICORTABOONATUR and also the tip "usage." Sometimes we have hunches. Assume the period is 10, and write out the tip on this basis. Nice pattern with a digraphic hit TT, OO, RR

```
TAPHORICOR
TABOONATURe   I have added the e
```
possibility.

and the cipher is:

```
12345678910 12345678910 12345678910 12345678910 12345678910
GJGQHJLELW  SZGGETGMQS  YVAHUOLFYN  NIRJHVKJDS  XMZVUEPETG

12345678910 12345678910 1
HIAHWZOTFN  HIHVWQUQDN  UENAEQMFQA  YXIOVUIVYG  NYLUJMOCVL
TAPHORICOR  TABOONATUR  e

RXSOTVSSMT  CIIFHVEFYA  VJLEUVDQFX  OZJHNNUHQY  EOGQDYGHEG


RXVVVOBVYY  SR
```

Now we develop the deciphering tableaux.

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

QUAGMIRE II ATTACK

We know that the plain sequence is normal. it is in the right order and we can base our interval analysis on the plain. We introduce Mr. Friedman's principle of symmetry to discover the relationships in the cipher alphabets.

We know that the cipher text reads from left to right just as we see it. The skeleton sequence is:

```
   H------V------A, Q---Z----T, U-------O, and  F-----D,
```

We can fill in a few letters. The Q---Z is either QVW-Z or Q-VWZ. In No 1 Q cipher is either Y or Z and Z cipher is either C or D. [MASTERTON jumps in with a NIO combination and VW but I didn't see this until after the solution.] Alpha 4 puts V +6 from H, transposing that to alpha 1, puts a V under the A plain, and suggests Q V W X Z sequence with Y in the Keyword. X is pretty unpopular in keywords so we will go with this assumption.

INTERMEDIATE DECIPHERING TABLEUX

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

So we build up alpha's 1, 3, 5, 6, 8. We can place the H's back in them from the Q by -6. in alpha 8 and 5. We see that U +8 = O in alpha 7. The sequence ---A starts the keyword from alpha three. Look at the T behind the Q by -17 offset in alpha 8. Remember my assumed 'e' = U in alpha 1. We place this hunch and let it play through.

We have U - - AT .....Y. I see the prefix UN and digram SA. The word "unsatisfactory" comes to mind but I haven't got enough hard evidence yet. We have a U +8 to O in the 7th alpha. Fill in the alphas.

FINAL DECIPHERING TABLEUX

```
Plain  O A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
       ---------------------------------------------------
Cipher 1 V W X Z U n s A T i f c O r Y b d e g H j k l m p Q
       2 I
       3   H           Q V W X Z U ? ? A T       O
       4               H           Q V W X Z U     A T
       5             H           Q V W X Z U     A T       O
       6 O             H           Q V W X Z U     A T
       7 U       T       O             H           Q V W X Z
       8   A T       O             H           Q V W X Z U
       9                           F           D
      10                                 N
```

I know that Y is in the keyword and could be the last letter of it. Look at the F-----D sequence. F is in the keyword and the O-------H is the only area than can fit the F and the Y.

Plug in my UNSATifcOrY guess. The lower letters require checking. Alphabet 1 fits the key as UNSATISFACTORY adjusted for duplicate letters.

The message reads in part: Slang is language or phrases of a vigorous colorful metaphoric or taboo nature invented to ...

QUAGMIRE III

The QUAGMIRE III is a very important class of ciphers because they introduce the one of the most important tools invented by Mr. Friedman, as explained in his Riverbank papers, called "Direct and Indirect Symmetry."

The title of this problem is "Inertia in the British Labor Market" and has the tip
"ANDTHREECALLINGFORAMANTOSTANDON."

```
IBWVU  PLTPJ  TKPPM  YCTDV  XYGNY  QYNTW  NFSUI  XNACX  CFTGV

AIKPS  RTCOJ  JWPRR  VOLAA  ZRURJ  NUIXM  XPQBV  UIBWO  GPCDP

LNNRD  FPSLI  BUGOC  DOTWK  CPIRQ  RVQGY  GCXLV  MNOBE  QFVOL

GBWGP  ATNJL  YWRMW  EKLAA  VICVE  AQBKU  VFJUR  DVIOZ  MPTZO

VSLIH  QBQXF  LLLWH  PUSGV  XP.
```

QUAGMIRE III ATTACK

Note the repeat of the first three letters IBW at interval 81. If the message starts with THE and the period turns out to be 9 we have found a wedge. Next place the tip in columnar line for a cycle of nine.

```
A N D T H R E E C            A I K P S R T C O
A L L I N G F O R            J J W P R R V O L
A M A N T O S T A            A A A R U R J N U
N D O N t w o f e e t  ?     I X M X P Q B V U
       t h e -------  ?      I B W O G P C D P
```

(also first three IBW)

The three A's in the first column followed by the two N's prove the period of 9. This is not accidental. My guesses of additional plain text are partially right - 'the' as you will see later. Note the triple R's, two U's and Two I's in the ciphertext lined up by columns in a period of 9.

Break the ciphertext into groups of nine.

```
123456789  123456789  123456789  123456789  123456789
IBWVUPLTP  JTKPPMYCT  DVXYGNYQY  NTWNFSUIX  NACXCFTGV


AIKPSRTCO  JJWPRRVOL  AAARURJNU  IXMXPQBVU  IBWOGPCDP
     ANDT  HREECALLI  NGFORAMAN  TOSTANDON  THE

LNNRDFPSL  IBUGOCDOT  WKCPIRQRV  QGYGCXLVM  NOBEQFVOL


GBWGPATNJ  LYWRMWEKL  AAVICVEAQ  BKUVFJURD  VIOZMPTZO


VSLIHQBQX  FLLLWHPUS  GVXP.
```

Place the extended tip. In a QUAGMIRE III, or in any case where the cipher component is the same as the plain component, if one cipher -plain matches E for E, all pairs must match, for the sequence is set A to A, B to B, etc. When this happens, we get a column of our write-out as "free plain text," which is of considerable help.

I can not overemphasize the next step. Because of the K3 nature of the keying, the Plain component and the Cipher 1 alphabet represents pairs that are the same distance removed -H to J, N to A, T to I, in this case. Similarly G to A, H to B, O to X, and R to J are equally separated - though not at the same interval as the first pairs obtained from line 1.

(Obviously, if H to J is "x" distance, H to B cannot be the same distance.) Check this observation of Symmetry on the decipher tableaux.

INITIAL DECIPHERING TABLEUX

```
Plain O A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
      --------------------------------------------------
Cipher1               J           A           I
      2             A B             X     J
      3         W A                         M
      4         P                   R         X
      5 P   R                             U
      6 R                         Q
      7       B               V J T
      8 N     C               O     V
      9                 L         U           O
```

Let us write down all the pairs we get by going from plain to cipher in each of the alphabets in turn. We can also write down the from the sidewise relationships. For instance, A to C on the plain sequence is the same distance P to R on Row 5. In addition, Row 7 to Row 8 tells us that BC is the same distance apart as VO.

This is a most powerful tool in solution of a sequence against itself. You can imagine a little "square" and go up, or down, or across, to find relationships within and between both plain and cipher components.

```
Plain sequence to Row 1  HJ NA TI
                      2  GA HB OX RJ
                      3  EW FA SM
                      4  EP OR TX
                      5  AP CRU      (CR-RU)
                      6  AR NQ
                      7  DB LV MJ NT
                      8  AN DC LOV    (LO-OV)
                      9  IL NU TO
>From Plain A to C        AC PR
>From Row 7 to 8          BC VO
```

There are a lot of relationships. I have not listed the sidewise ones like Plain to Row 1 - H to N and J to A.

MASTERTON points out that Row 1 is the reverse of Row 8. [MAST] I didn't see this "little" jump.

But I did make sense of the three letter chains; if L-O is the same as O-V we have a three letter segment. Do you see that the pairs in the listing above are separated by one letter in a sequence obtained from the next set, as evidenced by LV in 7 and LOV in 8? We can add the two together:

DCB LOV M-J AN-T

Look at the fragments, and realize that we have found some good information about the sequence. First of all the sequences are reversed alphabets. The sequence has BCD, VOL, JKM since we have used L and T-NA in it? [We can also look at a process called decimination to bring the sequence to bear. We will do that in the Friedman section.] Remember the very important part of the tool of symmetry - that because the plain and all the cipher alphabets are the same, we can associated pairs in the straight, sideways, down etc as we find them, using the plain or all nine cipher alphabets. In a QUAGMIRE IV, we cannot use the plain sequence in this way because of a different key.

We continue our recovery with A to N plain as the same distance as R to Q in alpha 6. We add QR to our line.

```
            VOL   TINA      BCD     HJKM   QR
```

Notice the H to B and G to A in the plain to alphabet 2 relationship. This tells us to put G ahead of H, then A goes behind B as we expect. Since O is in VOL and N is in TINA

```
             VOL/TINABCD/GHIJM/QR
```

the only missing element is P which we place as follows:

```
          ku  VOL/?/TINABCD (f)GHJMPQR swxyz
```

missing elements at this stage are e, k, u, w , x , y , z which likely the E and U are in the Keyword.

INTERMEDIATE DECIPHERING TABLEUX - PARTIALS

```
Plain 0   V O L         T I N A B C D F G H J M P Q R S
      ---------------------------------------------------
Cipher1 V O L         T I N A B C D F G H J M P Q R S w
      2     X                     T I N A B C D F G H J M P Q
      3                             T I N A B C D F G H J M P
      4   Q R S W? X
      5
      6
      7
      8     V O L            T I N A B C F G H J M P Q R S
      9
```

The line ups are not correct. We can find where alphabets 1, 2 and three start by putting the low frequency X in the right spot. I leave this part of the work to the you all. [Hint: compress the V O L -----T I N A space and what keyword will fit into - V O L u? T I (O)N. and place the E in the beginning.]

The answer is with Keywords EVOLUTION and BLUEPRINT:

FINAL DECIPHERING TABLEUX

```
Plain 0 E V O L U T I N A B C D F G H J K M P Q R S W X Y Z
      -----------------------------------------------------
Cipher1 V O L U T I N A B C D F G H J K M P Q R S W X Y Z E
      2 S W X Y Z E V O L U T I N A B C D F G H J K M P Q R
      3 W X Y Z E V O L U T I N A B C D F G H J K M P Q R S
      4 P Q R S W X Y Z E V O L U T I N A B C D F G H J K M
      5 C D F G H J K M P Q R S W X Y Z E V O L U T I N A B
      6 F G H J K M P Q R S W X Y Z E V O L U T I N A B C D
      7 Y Z E V O L U T I N A B C D F G H J K M P Q R S W X
      8 Z E V O L U T I N A B C D F G H J K M P Q R S W X Y
      9 X Y Z E V O L U T I N A B C D F G H J K M P Q R S W
```

The message reads: The British created a civil service job in eighteen hundred and three calling for a man to stand on the cliffs of Dover with a spyglass.....

QUAGMIRE IV

The QUAGMIRE IV is probably the most difficult of the QUAGMIRES because we need to recovery two keyworded alphabets and direct symmetry will not work with the plain.

We are given:

```
MWQYD  KMCAO  KHSEE  YULIH  WYTEW  YRLHG  LMEJC  ZHAKE  NYWUP
thegr  reat


QSQSO  ESYEP  BIZEW  QYPKZ  FHAAM  GWPTR  XNYWR  LKSQE  XHGRA



QCWAV  JNCPM  HDHZT  BCBHR  AMXUE  OLTWR  RIKNQ  AKKDZ  VJOYW
                                                        bet?


WHQJR  FGYVP  GILWV  WGPTF  MLYKX  TAKOZ  ATFGL  AUT.
weenl  atese  ptemb  erand  decem  berof  thaty  ear
```

QUAGMIRE IV ATTACK

The Title is "Lost Horsepower", the tips are starts with THE GREAT and has WEENLATESEPTEMBERANDDECEMBEROFTHATYEAR in the text. The letters bet?WEEN might be inferred.

Finding the cycle is our first challenge.

The WQY is +58, a discouraging number for factors. The cribs are pretty generous, so looking at them we might find something. Obviously, a plain hit at the correct interval of the cycle would result in a cipher coincidence at the same interval. Two occurrences of a plain letter at some interval other than the period or multiple of the cycle, the ciphers cannot be the same. MASTERTON describes a graphical technique for knocking out intervals. [MAST]

```
  OYWWHQJRFGYVPGILWVWGPTFMLYKXTAKOZATFGLAUT
  betweenlateseptemberanddecemberofthatyear
   * --9--  *
```

Thus the Y over E and H and Q over E "knock out" the intervals 3, 4 which are too short anyway, and also 11 because of the Y over P. Note the +9 hit for Y over E. So we write out the cipher in a period of nine:

```
123456789  123456789  123456789  123456789  123456789
MWQYDKMCA  OKHSEEYUL  IHWYTEWYR  LHGLMEJCZ  HAKENYWUP
thegreatE              E GH EE                   E A

QSQSOESYE  PBIZEWQYP  KZFHAAMGW  PTRXNYWRL  KSQEXHGRA
  E  ?HE   E T    EA  R      RT  ER    E    R E     E

QCWAVJNCP  MHDHZTBCB  HRAMXUEOL  TWRRIKNQA  KKDZVJOYW
   T    A  TE                   NH  E   E  R     bet

WHQJRFGYV  PGILWVWGP  TFMLYKXTA  KOZATFGLA  UT.
weenlates  eptembera  nddecembe  rofthatye  ar
```

Even with all the help and correct hits, the message is not a give a way.

INITIAL DECIPHERING TABLEUX

```
Plain O A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
      ---------------------------------------------------
Cipher1 U       P                 T       K   M     W
      2       F H     W             O G   T
      3       M Q Z                           I
      4         L   Y             J           A
      5     Y         T       R W           D
      6 F V     K
      7 M O     W               X             G
      8   T     Y                           G   C
      9 P       A   C                         V W
```

Since the alphabets are different we can not chain from the plain to cipher. However, WITHIN the cipher, the same rules apply as before - except their isn't nearly as much information. In Cipher 1 row we see that U to P is the same distance as F to K , M to W and P to A. Ok. Remember that we are dealing with unknown decimations, so the relationships between UPA, PK and PT is unknown.

By decimation I mean the process of selection of elements from a sequence according to some fixed interval. For example, the sequence A E I M is derived, by decimation , from a normal alphabet by selecting every fourth letter. It is the key to Symmetry solutions because the latent relationships in a cipher alphabet can be made patent by decimation. Lecture 11 will give two methods of decimation in detail. Table of Relationships in foregoing example:

```
UPA FK  MW          Plain A to E and Rows 1 to 9
PT  LJ               "    E to N
PK  HT  YG           "    E to R and Rows 1 to 6  adding UF
PM  QI  LAWG  YC     "    E to T and Rows 9 to 7 and 4 to 9
UMG  PW              "    A to T and Rows 1 to 7
TM  JA               "    N TO T
FH  MQ               "    D to E
WTD                  "    H to R and Rows 2 to 5
FV  MO               "    A to B
VK  OW  TY           "    B to E
OG  TC               "    B to T
PH  KT              Rows  1 to 2
PQ  MI              Rows  1 to 3
PL  TJ  MA          Rows  1 to 4
PY  KG  MC          Rows  1 to 8
FM  HQ  KW  VO      Rows  2 to O
HY  TG              Rows  2 to 9
QL  IA              Rows  3 to 4
QW  IG              Rows  3 to 7
QY  IC              Rows  3 to 8
QA  IW              Rows  3 to 9
LW  AG              Rows  4 to 7
LY  AC              Rows  4 to 8   and Plain A to G adding
                                   Cipher C under Plain G on Row
FP  KA              Rows  6 to 9   9
OT  WY  GC          Rows  7 to 8
YA  CW              Rows  8 to 9
```

Row 2 to 3 and 6 to 7 are combined. S and T in plain are most likely adjacent from VW in Cipher 9. Partials FH and MQ look good without an intervening letter.

LAWG is our best bet for the wedge. It ties together E and T in the same decimation. So:

```
Plain      E T
Cipher     P M
           H
           Q I
           L A W G

              K
           L A W G
              Y C
            L A W G
```

If FH and MQ are the right order, P is in the keyword, since the reverse bits of above (MP, IQ, GWAL) would not be consistent with MPQ. Unfortunately, we have run out of gas and must guess more plain. The plain E-gh-EE most likely is Eighteen and since they are talking about years, why not Seventy, since so many E's are fitting? The plain T of seventy is confirmed. The plain V may not produce much but the cipher G might be a bonanza. These new values add KE and JR to the chain.

```
123456789  123456789  123456789  123456789  123456789
MWQYDKMCA  OKHSEEYUL  IHWYTEWYR  LHGLMEJCZ  HAKENYWUP
thegreatE       T      EIGHTEEN  SEVENTY          E A

QSQSOESYE  PBIZEWQYP  KZFHAAMGW  PTRXNYWRL  KSQEXHGRA
  E  THE   E T    EA  R      RT  ER    E    R E     E

QCWAVJNCP  MHDHZTBCB  HRAMXUEOL  TWRRIKNQA  KKDZVJOYW
   T    A  TE                   NH  E   E  R     bet

WHQJRFGYV  PGILWVWGP  TFMLYKXTA  KOZATFGLA  UT.
weenlates  eptembera  nddecembe  rofthatye  ar
```

FINAL DECIPHERING TABLEUX

```
Plain O A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
      ---------------------------------------------------
Cipher1 U       P                 T       K L M     W
      2       F H     W             O G   T
      3       M Q Z     W                     I   G
      4         L   Y               J         A
      5     Y         T       R W M       D
      6 F V     K                         J   E
      7 M O     W               X             G
      8   T     Y                         G   C
      9 P       A   C                       V W
```

We look at VW and LM and KLM under the plain RST. We must conclude that G-C is correct. Rows 7 and 8 have a G and C under plain T, and WY under E and OT under B. This suggests that WXY and O-T are part of the final chain. So push the following chains:

KLM, G-C, VWXY, EA, O-T

The cipher sequence appears to go:

```
      JKLMQVWXYZ

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

The cipher keyword has this form O U T - P R - A I N G with S, E, D candidates. The keyword is SPREADING. The plain keyword can be derived as PANDEMIC and the cipher setting key is HORSETAIL. The groundwork is left to the student. Notice how resistant the QUAGMIRE IV was even with loads of help.

LECTURE 10 HOMEWORK PROBLEMS

QQ-1 QUAGMIRE I Travelogue. (Ends:SINGOUTOFTHESEA) RHIZOME

KKQHPQR KTYOHTA TLGAWBM XORKTAT BSOOIYI CGICEJV UCYZRJP

ALNSFRZ UCQDXIS TDRBFYS YTFDZBD USQWKMT CPPDOAI CAAKEHK

UAYFHQA TLNIFSI SIGJHAS V.

QQ-2 QUAGMIRE III Tedious. (CRYPTANALYTIC METHODS) DOPPELSCHACH

PNATV SJBAQ WGMTR BZYLU ACACR GBNTQ FGGCN APNID ULMVD

SCEPB AMCQF BBPVR EOBSL AFSAN HFYVV MCYTF LEMAO MFHVU

KBAAU ATTEA NGOHU GTQEX ISUGU SAKCC TLIRT TLSZM PBMGV

APYRV YIIGL WGNUF JFROG SNQGN HBOTU TACUO JUVQH HUGWW

WBIMT WNHVO GTLSZ MPYQZ BNCEN UWLC.

QQ-3 QUAGMIRE IV Economics Lesson. EDNASANDE
(BUSINESSACTIVITYDURINGAPERIOD)

TDNSE PMBSV FURMQ UFYSJ PAGGY FVIKT GYVLV FBTPH IIIAD

HVIUY QSAFA VQVFU HPIHE BIXNN HBSTN IRMQH IIIAD OVIXT

CTNOW EOJOZ BOWBU ONLFN GOBJS HBOQS VZMOU JSFQH SAHPS

JBBJT AAMIE XILRA TOTVL TUAML FLNEJ PPMNT XHVQV FCYSB

JODNF XJSFT UIUTM ONKDO UMMSB NWUL.

REFERENCES / RESOURCES [updated 6 April 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.

[AFM] 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.

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

[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.

[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.

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

[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.

[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.

[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)

[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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[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., pp993-1026.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[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.

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

[FREB] 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.

[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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[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.

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

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

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

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

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

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

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

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

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

[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 mthe 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.

[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.

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

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

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

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

[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.

[HUNG] Rip Van Winkel, "Hungarian," The Cryptogram, March - April, American Cryptogram Association, 1956.

[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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[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 History, 1992, pp 201 ff.

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

[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.

[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.

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

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

[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 The Beale Cipher Hoax.)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[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.

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

[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.

[SPEE] "Speech and Facsimile Scrambling and Decoding - A Basic Text on Speech Scrambling," Aegean Park Press, 1981.

[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.

[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.

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

[TRAI] Lange, Andre and Soudart, E. A., "Treatise On Cryptography," Aegean Park Press, Laguna Hills, Ca. 1981.

[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.

[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.

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

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

[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.

[WINT] 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.

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

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

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

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

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

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

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

[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)