CLASSICAL CRYPTOGRAPHY COURSE
BY LANAKI

May 05, 1996
Revision 0

LECTURE 11

POLYALPHABETIC SUBSTITUTION SYSTEMS II
CRYPTANALYSIS OF VIGGY'S FAMILY

SUMMARY

In Lectures 11-12, we continue our course schedule with a study of fascinating cipher systems known as the "Viggy" based on multiple alphabets - Polyalphabetic Substitution systems.

We will continue developing our subject via an overview based on the Op-20-GYT course notes (Office of Chief Of Naval Operations, Washington) [OP20]. We will revisit polyalphabetic cipher systems using Friedman's detailed analysis. We will cover the Viggy, Variant, PORTA systems and other family members. [FRE4], [FRE5], FRE6], [FRE7], [FRE8]. We will take material from ACA's Practical Cryptanalysis Volume V by William G. Bryan on "Periodic Ciphers - Miscellaneous: Volume II" [BRYA] and Sinkov's [SINK] text to discover Viggy's secrets. We will look at [ELCY's] treatment of these systems.

In Lecture 12, we will describe the difficult aperiodic polyalphabetic case and give a diagram of topics considered in Lectures 10 - 12. [FR3] We will complete the Viggy family. I will also cover decimation processes in detail.

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

ZEN CRYPTO

In Lectures 1- 10, I have purposely stayed away from the heavier mathematics of cryptography (subject to change). Everything I am presenting can and has been reduced to mathematical models and computerized for ease of work. For my readers who can not live without the math diet, there are plenty of guru' s like [SCHN] and [SCH2] to have breakfast with. There are plenty of computer aids at the Crypto Drop Box to help you do the setup work.

BUT those who embark on a course of 'only the computer' do this without knowing the real effort -the brain power - the shortcuts - the tradecraft - the historical implications, in my opinion, have lost the real heart of Cryptography. The 'ah ha's of inspiration are what make the difference. First, there is a fundamental problem in that computer models do not apply to all variant cases. Simple changes to the system can fool even the most adept computer program. For example, placing clever nulls will defeat many a statistical based model.

Second, we lose the sense of urgency that was required for wartime cryptography. If President Kennedy's Playfair message [that's right it was not English as in the movie PT-109] on the back of a coconut had been intercepted and deciphered by the Japanese [which they very capable of doing], we might not have had the graceful light of his Presidency or who knows the moon landings. As another case in point, the solution of ENIGMA during the mid - final Atlantic Campaigns of World War II, reduced the operational effectiveness of the U-Boat to one day and hence saved allied tonnage and warships suppling Europe. The American and British Crypee's 'thought' more like their German counterparts than their counterparts. Computer solutions were bulky, machine dependent [the solution "stops"] and not reliable until 1945. People made the difference.

SOLVING A PERIODIC POLYALPHABETIC CIPHER

There are three fundamental steps to solve a Periodic cipher.

1) Determine the period. This sets up the correct geometrical positioning of ciphertext alphabets.

2) Identify the Cipher System and reduce or consolidate the multiple alphabet distribution into a series of monoalphabetic frequency distributions.

3) Solve the monoalphabetic distributions by known principles. We have covered this in Lectures 1-3 and Lecture 10.

Friedman presents a more detailed and eloquent version of this procedure in [FR7].

THE LONG AND SHORT OF KASISKI

Step one is finding the period. Bryan reminds us that there are at least two ways to find the period. The short approach makes use of the distances between patent cipher text repetitions and factors the differentials. The long approach is used when there are no patent repetitions to factor. In this case we set up a possibilities matrix and factor every combination looking for the highest probable common factor. [BRYA]

As an example of the first case take:

```
          10            20            30            40
BGZEY  DKFWK  BZVRM  LUNYB  QNUKA  YCRYB  GWMKC  DDTSP

          50            60            70            80
OFIAK  OWWHM  RFBLJ  JQFRM  PNIQA  VQCUP  IFLAZ  HKATJ

          90           100           110           120
UVVQE  EKESZ  DUDWE  KKESL  IZQAT  SBYUZ  UUVAZ  IXYEZ

         130           140
JFTAJ  EMRAS  QKZSQ  FOPHM  W.
```

We tabulate the repetitions and the cipher text letter differences between repetitions.

Delta	Factors	
BG 29	-	
RM 45	3,5,9	
KA 53	-	
MR 77	7,11	
QA 39	3,13	
VQ 17	-	
AZ 40	4,5,8,10	
AT 26	13	
UV 31	-	
EK 9	3,9	
KES 10	5,10	.... this trigraph more important than QA or AT digraphs. Suggest that the period is
SQ 4	4	either 5 or 10. Practice dictates that the larger number is the proper.

But suppose there are no repeats or those that do exist do not establish a period. What then?

Given:

```
         10             20             30             40
RNQJH  AUKGV  WGIVO  BBSEJ  CRYUS  FMQLP  OFTLC  MRHKB

         50             60             70             80
BUTNA  WXZQS  NFWLM  OHYOF  VMKTV  HKVPK  KSWEI  TGSRB

         90            100            110            120
LNAGJ  BFLAM  EAEJW  WVGZG  SVLBK  IXHGT  JKYUC  HLKTU

MWWK.
```

We set up the following vertical tally. We note the actual position of every letter.

```
A  6 45 83 89 92 115
B  16 17 40 41 80 86 104
C  21 35
D  ---
E  19 74 91 93
F  26 32 52 60 87
G  9 12 77 84 98 100 109
H  5 38 57 66 108 116
I  13 75 106
J  4 20 85 94 111
K  8 39 63 67 70 71 105 112 118 124
L  29 34 54 81 88 103 117
M  27 36 55 62 90 121
N  2 44 51 82
O  15 31 56 59
P  30 69
Q  3 28 49
R  1 22 37 79
S  18 25 50 72 78 101
T  33 43 64 76 110 119
U  7 24 42 114 120
V  10 14 61 65 68 97 102
W  11 46 53 73 95 96 122 123
X  107
Y  23 47 58 113
Z  48 99
```

Now we take each difference and every difference in each case. For example, A45-6, 83-6,89-6,92-6,115-6; and 83-45,89-45,92-45,115-45; and 89-83,92-83,115-83; and 92-89,115-89, and 115-92. Then we factor these differences, setting up a matrix (Table 11-1) of potential periods from 3 -12 inclusive and total the tabulations for each factor in each of the letters of the alphabet. The highest column total represents the period. The number is correct more than 98 per cent of the time.

Table 11-1

	3	4	5	6	7	8	9	10	11	12	
A	3	1		1	1		1	1	2	1	
B	9	7	4	5	3	7	4	2	1	2	
C		1	1		1	1		1			
D											
E	1	1	1	1			1		1	1	
F	2	3	3	1	2	1	1	1	1		
G	5	5	4	1	4	3	2	1	3	1	
H	6	3	2	2	3	1	1	2	1		
I	1										
J	3	1	2	1	1	1	3	1			
K	13	10	4	9	8	5	3	1	2	3	
L	4	3	4	1	4	1	3	1	2		
M	4	2	3	2	6		3	1	1		
N	1	1	1	1	3	1		1			
O	1	3	1		1	1			1		
P	1										
Q	1		1		1						
R	5	1	1	3	2		1			1	
S	4	4	2	3	2	1	1	1	1		
T	4	3	1	1	2		1	1	2	2	
U	5	1	2	5	1	2	3	1	2	2	
V	5	6	2	2	1	2	3		1	1	
W	9	4	5	3	8	1	4	4	3	1	
X											
Y	2	2	3	2	1	2		1	3	1	
Z	1										
	87	61	47	43	57	30	35	21	25	16	Columns total
X	3	4	5	6	7	8	9	10	1	112	times period
	261	244	235	258	399	240	315	210	275	192	Total
					===						

The period is 7.

WHAT CIPHERS MAKE UP THE VIGGY FAMILY?

The Viggy (or more correctly the Vigenere) Family is group of ciphers. Included in this group are: Vigenere, Variant, Beaufort, Gronsfeld, Porta, Portax, and Quagmires I-IV. Other ciphers may be included in the group. They are Nihilist Substitution, Auto - Key, Running Key and Interrupted ciphers. Bryan includes the Tri-square, the periodic Fractionated Morse, the Seriated Playfair and the Homophonic in the same class of ciphers.

These ciphers were invented at different times by different authors, sometimes with confusion of authorship, and in different countries. They are similar in that they represent permutations of the same cryptographic concept and can be cracked with the same general methodology, albeit with slight variations in procedure. What is also interesting is that these ciphers can be viewed in tableaux form, in slide form or matrix form.

The theory of polyalphabetic substitution is simple. The encipherer has at his disposal several simple substitution alphabets, usually 26. He uses one such alphabet to encipher only one letter, another alphabet for the second letter, and so forth, until some preconcerted plan has been followed. The earliest known ciphers of this kind, the Porta (1563), the Vigenere (1586) used tableau's for encipherment, in which all the alphabets were written out in full below each other. The Gronsfield (1655) had a mental key, and the Beaufort (1857) which came two hundred years later, again used the tableaux. The process was reduced to strips or slides in 1880 at the French military academy of Saint-Cyr. The polyalphabetic deciphering slides now bear that name. [ELCY]

To know thoroughly any of these ciphers is to understand the fundamental principles of all. Lets look at the papa bear.

THE VIGENERE CIPHER

The father of the Viggy family is the Vigenere Cipher. Like most of the periodic ciphers, the 'Viggy' is actually a series of monoalphabetic substitutions such as Aristocrats, and since a keyword is used, under each letter of the keyword, there is a separate simple substitution cipher - each one different- , using all the letters, in such a manner, that the resulting cipher is a combination of several such substitutions.

Attributed to Blaise de Vigenere, the cipher named for him was invented by him in 1586. In his "Traicte des Chiffres" he did invent an autokey system which used both a priming key and did not recommence his plaintext key with each word, nut kept it running continuously. He described a second autokey system which was more open but still secure. Both systems were forgotten and were re-invented in the 19th century. Historians have credited Vigenere with the simpler polyalphabetic substitution system. Legend grew around this cipher that it was "impossible of translation" as late as 1917. [KAHN]

The original Viggy was composed of an enciphering and deciphering tableaux. Letters were enciphered and deciphered one letter at a time. The modern Vigenere tableaux is shown in Figure 11-1.

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

The normal alphabet at the top of the tableaux is for plaintext and the keyletters are shown at the extreme left under the 'A' of the top row. Where the two lines intersect in the body of Figure 11-1, the ciphertext is found.

For example using the keyword TENT, we encipher "COME AT ONCE"

```
we have:        TENT        TENT
                ----        ----
                COME        VSZX    (ciphertext)
                ATON        TXBG
                CE          VI--
```

The enciphering and deciphering problem are done as a group of letters to improve speed and accuracy of the process.

Another way to look at this is that the Viggy is really a two dimensional slide problem. We can construct (or purchase for about $2.00 from ACA) a set of two Saint-Cyr slides that operate the same way as the tableaux shown in Figure 11-1. What is useful is that each slide bears the standard normal alphabet from A-Z with high frequency letters colored or shaded. Each slide is a double-alphabet to allow flexibility.

Figure 11-2

```
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ
GHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEF
*                           *
```

Figure 2 shows the Saint- Cyr slide at a key of G. Check with Figure 11-1 to see that the results are the same for Nplain =Tcipher or Iplain = Ocipher.

The practical use of the Saint Cyr slide is that the whole column of plaintext is enciphered as a unit. So C A C would be enciphered as V A V, plaintext O T E becomes S X I, etc. This eliminates mistakes. The cipher is taken off in 5 letter groups by rows, so we would have VSZXT XBGVI for our previous example.

Friedman points out that the sliding components produce the same type of cipher with the circular disks like the old U. S. Army version. [FRE7]

Koblitz [KOBL] describes the Viggy as follows:

For some fixed k, regard blocks of k letters as vectors in (Z/NZ)**k. Where N is the N-letter alphabet and a digraph integer correspondence exists between modulo N**2 array and it is a vector mapping. Choose some fixed vector b which exists in the plane (Z/NZ)**k which can be remembered by a key word and encipher by means of the vector translation C = P +b where C is the ciphertext message unit and P is the plaintext message unit which is a k-tuple of the integers modulo N.

The object is to guess N and k, break up the ciphertext in blocks of k letters and performs a frequency analysis on the first letter of each block to determine the first component of b and then proceeds onto the second letter in the block, etc.

Konheim's description is worse than Koblitz's. [KONH]

Seberry and Pieprzyk describe the Viggy as made up of key sequence k= k1...kd where ki , (i=1,d) gives the amount of shift in the ith alphabet, fi(a) = a+ki(mod n) and the ciphertext is described as fi**(-1) = (ki -c) mod n so that

fi(a) = [(n-1)-a +(ki +1)] mod n [SEAB]

The latter four descriptions are boring - even to my engineering background. They also do not hold water for randomized alphabets or tableauxs with disruption areas in place. These represent discontinuities in the mathematical function. They are discontinuous and tractable. Or differentiable if the model is such. SCYER's program may have solved the discontinuity integer problem by area limits or module limits. When he publishes the procedure, maybe he will tell us.

WHICH WAY ?

Does it matter with the Viggy, that we encipher S by B (B alphabet or Key B) to find cipher T or encipher B by S (S alphabet or Key S) to find T? No. This is an interesting characteristic not shared by all in the Viggy family. It may be its downfall.

For instance, the message:

Send Supplies To Morley's Station

enciphered with the repeating key, BED under the original method of encipherment as might be described by Blaise de Vigenere would be:

```
Key    : BEDB  EDBEDBED  BE  DBEDBED  BEDBEDB
Plain  : SEND  SUPPLIES  TO  MORLEYS  STATION
Cipher: TIQE  WXQTOJIV  US  PPVOFCV  TXDUMRO
```

The modern Saint-Cyr slide encipherment of the above would be:

```
  Key        B E D     B E D     B E D
  Plain      S E N     D S U     P P L
  Cipher     T I Q     E W X     Q T O

             I E S     T O M     O R L
             J I V     U S P     P V O

             E Y S     S T A     T I O
             F C V     T X D     U M R

             N
             O
```

which gives:

```
        5         10          15          20          25
T I Q E W   X Q T O J   I V U S P   P V O F C   V T X D U

      30
M R O X X   (two ending nulls and a bad choice at that)
```

With the Saint Cyr slide, we would encipher S, I, E, N; then D, T, S, and finally P, O , T by setting the B key on the bottom slide under the A key of the top slide and reading off the equivalents. [SINK], [ELCY]

DECIPHERMENT BY PROBABLE WORD

Refer to Figure 11-3:

Figure 11-3

Deciphering with the Key:

```
Key    :  B E D B E D B E D B E D  ........
Cipher:  T I Q E W X Q T O J I V  ........
Plain :  S E N D S U P P L I E S  ........
```

Deciphering with the Message:

```
Plain :  S E N D S U P P L I E S  ........  (trial key)
Cipher:  T I Q E W X Q T O J I V  ........
Key   :  B E D B E D B E D B E D  ........  (true  key)
```

Figure 11-3 indicates a possible solution method. The message fragment works well as a trial key, and if applied in the same manner as the true key, the true original key will be revealed. The Vigenere Cipher works equally well in reverse. It is this peculiarity that portends the use of a probable word attack.

Suppose we have the cryptogram:

```
   U S Z H L    W D B P B    G G F S ...
```

which we suspect that the presence of the word SUPPLIES. We decipher the first 8 letters using this probable word as a trial key, and obtain the jumbled series: C Y K S A O Z J,

which is unsatisfactory. We next drop the first U, and obtain group : A F S W L V X X. We fail again on the third and fourth trials. The fifth decipherment obtains the series TCOMETCO. We see the TCO repeats and the key word COMET. [ELCY]

F. R. Carter of the ACA shows us a more organized approach in Figure 11-4:

Figure 11-4

```
Cryptogram Fragment: U S Z H L W D B P B G G F S ......

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

Look down at an angle between the stars to find the key word COMET. The first letter S was used to decipher every possible key letter which can produce S. The entire row of equivalents were produced at the same time. The resulting rows of decipherment indicate all the possible keyletters that could produce S, then U, then P, and so on. Carter actually shortened the procedure to three full rows and then partials thereafter. He assumes that the keyword is readable and discards non readable text.

DECIPHERMENT BY PROBABLE TRIGRAM SEQUENCE

For the case where we have no probable word or the sequence is very short, we may use Ohaver's Trigram Method. We start with a list of usual trigrams THE, AND, THA, ENT, ION, TIO. The key fragments deciphered by these will be short and numerous, some correct and some incorrect to bring out the repeating key sequence. A secondary worksheet is used to test the various fragments as keys. If any one of them is a fragment of the original key, it must bring out fragments of plaintext at regular intervals.

A scheme like Carters can be used with the trigrams THE, AND.. replacing the word SUPPLIES. Refer to Figure 11-5.

Given:

```
                  10                  20              26
  L N F V E  O L N V M  R N G Q F  H H R N H  I R V F E  B
```

The cipher text is only 26 letters long. Every letter except the final two might begin a cipher trigram. So we have 24 cipher trigrams. Write them out in full on two worksheets.

Figure 11-5

```
ION               Trial 1

    LNF NFV FVE VEO EOL OLN LNV NVM VMR MRN RNG NGQ
    AZS FRI XHR NQB WAY GXA DZI FHZ NYE EDA JZT FSD
                                        ---
    GQF QFH FHH HHR HRN RNH NHI HIR IRV RVF VFE FEB
    YCS IRU XTU ZTE ZDA ZJU FTV ZUE ADI JHS NRR XQO


EDA               Trial 2

    LNF NFV FVE VEO EOL OLN LNV NVM VMR MRN RNG NGQ
    HKF JCV BSE RBO ALL KIN HKV JSM RJR ION NKC JDQ
                                        ---
    GQF QFH FHH HHR HRN RNH NHI HIR IRV RVF VFE FEB
    CNF MCH BEH DER DON NKH JEI DFR EOV NSF RCE BBB
```

Trial 1 tests for THA, THE, AND fail but ION gives us FRI and WAY. But anyone of these 24 decipherments on the second row might be a fragment of the original key. Trial 2 fails to confirm FRI or WAY but test of key-fragment EDA yields ION. If this sequence is actually a portion of the original key, then the plaintext will be brought out at some constant distance apart. The point we found the trigram is the tenth cryptogram letter; that is every trigram presents only one new letter so to find a completely different trigram in either direction, we must count backwards or forwards a distance of three trigrams.

Beginning at the tenth trigram we examine every third trigram in both directions. The following is found: HKF, RBO, HKV,ION, CNF, DER,JEI, NSF. These are incoherent. This would be equivalent to a period of three - not likely. Try every fourth decipherment: JCV,KIN,ION,MCH,NKH,NSF. Not usable for a consecutive sequence, continuously written cryptogram. Trying the decipherments at a proposed period of 5, we get ALL, ION, BEH, DFR. This possibility is good. We try to decipher the T before ION and get the letter C. We now have four letters in our key C E D A. With a little anagraming we have the word D A * C E. A probable word FRIDAY comes to mind.

BRYAN'S SAINT-CYR 'HITS' METHOD

William G. Bryan shows us how to use the high frequency letters on the Saint-Cyr slide to good use.

Given the Viggy with a known period of 7 based on a similar effort used in Table 11-1:

```
PXIZH  GVGEU  UOXIX  MYEEJ  ZCOCM  OWZCL  FMTOR  ISIGH  LKWPS

MSIDX  WCFBR  KPYXO  PRJIL  HFMCR  IHUDU  LVRLJ  FVVVS  HTYFR

RGPHQ  WIIBL  XQXMM  TDVGU  EITFM  QEEJH  WUHFW.
```

We reset the problem in groups of 7:

```
1234567
PXIZHGV
GEUUOXI
XMYEEJZ
COCMOWZ
CLFMTOR
ISIGHLK
WPSMSID
XWCFBRK
PYXOPRJ
ILHFMCR
IHUDULV
RLJFVVV
SHTYFRR
GPHQWII
BLXQXMM
TDVGUEI
TFMQEEJ
HWUHFW
```

Now each column represents a separate simple substitution cipher. They will not produce consecutive plaintext, but merely show isolated letters in that particular substitution, to be coupled with those letters that fall on either side in other substitutions, to make a true plain text sequence. Here's where the underlined high-frequency letters on the slide come in:

We go down column 1 and tabulate all the letters which appear\more than once. P-2, G-2, X-2, C-2, I-3, T-2. We rearrange them in their normal sequence = C G I P T X. The lower slide is moved successively so that the first letter C is under the high frequency letters, in turn, A E H I N O R S T, and a reading is made of the number of 'hits' , the number of other cipher text letters G I P T X that fall below the high frequency letters. If they do then the letter under A of the top slide is the key letter for that column. If they don't further trials are necessary.

High frequency letters don't always show up. Some times medium frequency letters may be required. So with C under A: G-E, I-G,P-N, T-R, X-V; With C under E:G-I, I-K, P-R, T-V, X-Z; With C under the H: G-L, I-N, P-U, T-Y, X-C; with C under the I: G-M,I-O,P-V, T-Z, X-D; and with C under the N: G-R, I-t, P -A, T-E, X-I (six hits); and we have found the setting. So we set P under the A in the top slide, and decipher the entire column A R I N N T H I A T T C D R, and write it into a blank column as column 1.

Proceeding with Column 2, we have no results. Column shows 2 passable results at P and U, Column 4 seems to go with Y, column 5, setting B has 4 hits, Column 6 has 5 hits indicating an E, and Column 7, R gives six hits.

The keyword thus recovered is P P Y B E R. We choose to decipher the ending B E R as the ending of a keyword to produce:

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

These are almost all good fragments. The GHT must have an I or U before it. Since cipher letter G is involved, we place the G under the I which results in the Y we already had and putting G under the U gives us M under the A, we choose the latter.

Now we have MBER has a key fragment. Deciphering column 4 with M adds N I I S A A U A T C T R T M E E U E V to the evidence.

There are several possibilities NGCE preceded by an O, UGHT preceded by an O, TANT preceded by an OR; TLYA preceded by an N; UTAR preceded by an O or A; and EWIV preceded by R/H.

With the Viggy cipher, remember to read the setting for the keyword letter below the A of the Stationary slide; and the plain text appears on the same slide as this A, while the cipher text is in the lower slide.

VIGENERE COMPUTER SOLUTION IS QUICKER

At this juncture, I wondered how our Viggy solver at the CDB would do on this problem. I brought up my faithful computer program and entered the cipher text into Vigenere.exe without telling it the period and found the following:

The period was found within 1 second. The trial keyword was PLQMBER, which I assumed was PLUMBER. Using PLUMBER as my keyword, it typed out the answer: "AMONG CERTAIN TRIBES OF INDIANS IN ALASKA.. ends BUT ARE USED AS SLAVES." The process took less than 3 seconds of compute time on my 486/50.

I then rearranged the ciphertext with five nulls strategically added. The next pass gave me a period of nine and a gibberish trial keyword. So for well defined problems the computer is less fun but a clear winner. For the clever cryptographer, the computer can be defeated.

PRIMARY COMPONENTS

We have seen that equivalents obtainable from use of square tables may be duplicated by slides or revolving disks [FR2], [FR7] or computer models. Cryptographically, the results may be quite diverse from different methods of using such paraphenalia, since the specific equivalents obtained from one method may be altogether different from those obtained from another method. But from the cryptanalytic point of view the diversity referred to is of little significance.

There are, not two, but four letters involved in every case of finding equivalents by means of sliding components; furthermore, the determination of an equivalent for a given plaintext letter is represented by two equations involving four equally important elements, usually letters.

Consider this juxtaposition:

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

Question - what is the equivalent of Pplain when the Key letter is K? Answer - without further specification, the cipher equivalent can not be stated. Which letter do we set K against and in which alphabet? We have previously assumed that the K cipher would be put against A in the plain. But this is only a convention.

Figure 11-6

```
                          Index            Plain
                            *               *
 1. Plain:                    ABCDEFGHIJKLMNOPQRSTUVWXYZ
 2. Cipher:FBPYRCQZIGSEHTDJUMKVALWNOXFBPYRCQZIGSEHTDJUMKVALWNOX
                            *               *
                          Key               Cipher
```

With this setting Pplain = Zcipher.

The four elements are:

1. The Key letter, 0k
2. The index letter, 01
3. The plaintext letter, 0p
4. The cipher letter. 0c

The index letter is commonly the initial letter of the component, but by convention only. We will assume from now on that 01 is the initial letter of the component in which it is located. Refer to Figure 11-6 to confirm this assumption. The enciphering equations above are:

```
                (I) Kk = A1 ; Pp = Zc      k=key, p=plain,
                                           c=cipher, 1= initial
```

There is nothing sacred about the sliding components. Consider Figure 11-6b.

Figure 11-6b

```
                          Index            Cipher
                            *               *
1. Plain:                    ABCDEFGHIJKLMNOPQRSTUVWXYZ
2. Cipher:FBPYRCQZIGSEHTDJUMKVALWNOXFBPYRCQZIGSEHTDJUMKVALWNOX
                            *               *
                          Key               Plain
```

thus (II) Kk = A1; Pp = Kc

Since equations (I) and (II) yield different results even with the same index, key and plain text letters, it is obvious that a more precise formula is required. Adding locations to these equations does the trick.

(I) Kk in component (2) =A1 in component (1); Pp in component (1) = Zc in component (2).

(II) Kk in component (2) =A1 in component (1); Pp in component (2) = Zc in component (1).

In shorthand notation:

(1) Kk/2 = A1/1; Pp/1 + Zc/2
(2) Kk/2 = A1/1; Pp/2 + Zc/1

Employing two sliding components and four letters implies twelve different resulting systems for the same set of components and twelve enciphering conditions. These constitute the Viggy Family:

Table 11-2

(1) 0k/2=01/1; 0p/1=0c/2	(7) 0k/2=0p/1; 01/2=0c/1
(2) 0k/2=01/1; 0p/2=0c/1	(8) 0k/2=0c/1; 01/2=0p/1
(3) 0k/1=01/2; 0p/1=0c/2	(9) 0k/1=0p/2; 01/1=0c/2
(4) 0k/1=01/2; 0p/2=0c/1	(10) 0k/1=0c/2; 01/1=0p/2
(5) 0k/2=0p/1; 01/1=0c/2	(11) 0k/1=0p/2; 01/2=0c/1
(6) 0k/2=0c/1; 0p/1=0p/2	(12) 0k/1=0c/2; 01/2=0p/1

The first two equations (1) and (2) define the Vigenere type of encipherment and are widely used. Equations (5) and (6) define the Beauford type and Equations (9) and (10) define the Delastelle type of encipherment. [FR7]

FURTHER REMARKS ON REPETITIONS

I have said that the three steps in the cryptanalysis of repeating key systems are : 1) Find the length of the period, 2) Allocate or distribute the letters of the ciphertext into their respective alphabets, thereby reducing the polyalphabetic text to monoalphabetic terms, and 3) analysis of the individual monoalphabetic distributions to determine the plain text values of their cipher equivalents in each distribution or alphabet.

As a direct result of using a repeating key (no matter how long) certain phenomena are manifested externally to the cryptogram. Regardless of what system is used, identical plain text letters enciphered by the same cipher alphabet with single equivalents must yield identical cipher letters. This happens each time the same key letter is used to encipher identical plaintext letters.

Since the number of columns or positions with respect to the key are limited, and there is a normal redundancy in the language, it follows that there will be in a message of fair length many cases where identical plain text letters must fall into the same column. This will be enciphered by the same cipher alphabet, resulting in many repetitions. There are two types of repetitions: causal and accidental (random) repetitions. The former we can trace back to the key. The latter occurs when different plaintext letters fall in different columns and by chance produce identical cipher text letters.

Accidental repetitions will occur frequently with individual letters, less frequently with digraphs (because the accident must occur twice in succession, much less in the case of trigraphs and very much less in the case of a tetragraph. The probability of chance repetition decreases significantly as the repetition increases in length. Friedman has developed statistical tables based on the binomial and Poisson distributions to determine the individual and cumulative probabilities for expected number of repetitions in n letter text to occur x or more times in samples of random text.

The use of these tables is important. They tell us when we are dealing with cryptographically maneuvered text versus random noise designed to fool the listener. They indicate what may be a hoax (Beale or Bacon - Shakespeare controversies) versus valid enciphered text.

Tables 11-3 to 11-6 show the above theory.

Table 11-3

Number of Letters	Expected Number of Digraphs Occurring Exactly x Times E(2)	E(3)	E(4)	E(5)	E(6)	E(7)	E(8)	E(9)	E(10)
100	6.21	.298	.011						
200	21.8	2.12	.154	.009					
300	42.5	6.23	.683	.060	.004				
400	65.3	12.8	1.87	.220	.022	.002			
500	88.1	21.6	3.97	.582	.071	.008			
600	110.	32.3	7.11	1.25	.184	.023	.003		
700	129.	44.3	11.4	2.35	.403	.059	.008	.001	
800	145.	57.1	16.8	3.96	.777	.130	.019	.003	
900	158.	70.1	23.2	6.16	1.36	.257	.043	.006	.001
1000	169.	83.0	30.6	9.03	2.21	.466	.085	.014	.002

Table 11-4

Number of Letters	Expected Number of Trigraphs Occurring Exactly x Times E(2)	E(3)	E(4)
100	.269	.001	
200	1.10	.004	
300	2.48	.014	
400	4.40	.033	
500	6.85	.064	
600	9.81	.111	.001
700	13.3	.175	.002
800	17.3	.261	.003
900	21.8	.371	.005
1000	26.8	.505	.008

Table 11-5

Number of Letters	Expected Number of Tetragraphs Occurring Exactly x Times E(2)	E(3)
100	.010	
200	.043	
300	.096	
400	.171	
500	.270	
600	.389	
700	.530	
800	.693	
900	.877	
1000	1.08	0.001

Table 11-6

Number of Letters	Expected Number of Pentagraphs Occurring Exactly x Times E(2)
100	
200	.002
300	.004
400	.007
500	.011
600	.015
700	.021
800	.027
900	.034
1000	.042

By way of illustration, of the use of these tables, from Table 11-3, we obseve that in a sample of 300 letters of random text, we may expect 43 digraphs to occur twice, 6 digraphs to occur three times and 1 digraph to occur four times. If we sum the values under E(2) through E(6) we have the cumulative probability in the 300 letter sample. The sum is 49.477, which indicates that in a sample of 300 letters or so, 49 digraphs will occur two or more times.

STATISTICAL PROOF OF THE MONOALPHABETICITY OF THE DISTRIBUTIONS

The second step in the solution of periodic ciphers is to distribute the cipher text into the component monoalphabets. The period once established tells us the number of cipher alphabets. By rewriting the message in groups corresponding to the length of the key (period) in columnar fashion, we automatically have divided up the text so that letters belonging to the same cipher alphabet occupy similar positions in the groups or in the same columns.

If we make separate uniliteral frequency distributions for the isolated alphabets, each of these resulting distributions is therefore, a monoalphabetic frequency distribution. Were this not so, if they did not have the characteristic crest and trough appearance including the expected number of blanks, if the observed values of Phi are not sufficiently close to the expected value of Phi plain, or do not yield I.C.'s in the close vicinity of the expected value, then the entire analysis is fallacious.

The I.C. values of these individual distributions may be considered an index of correctness of the factoring process. Both theoretically and practically, the correct hypothesis with respect to these distributions will tend to conform more closely to the expected I.C. of a monoalphabetic frequency distribution.

Friedman demonstrates the above with an example: [FR7]

Plaintext Message:

The artillery battalion marching in the rear of the advance guard keeps its combat train with it insofar as practical.

Keyword BLUE using direct standard alphabets.

Cipher Alphabets

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

   B L U E B L U E B L U E B L U E B L U E B L U E ...
   T H E A R T I L L E R Y B A T T I L I O N M A R ...
```

Cipher Text

```
USYES  ECPMP  LCCLN  XBWCS  OXUVD  SCRHT
HXIPL  IBCIJ  USYEE  GURDP  AYBCX  OFPJW
JEMGP  XVEUE  LEJYQ  MUSCX  JYMSG  LLETA
LEDEC  GBMFI
```

Friedman gives a useful formula for monographic I.C. of a 26 character text:

I.C. = 26 sum f(f-1)/N(N-1) = Phi(o) / Phi (r)

and since Phi (p) for English is 0.0667N (N-1)

and Phi (r) = 0.0385 N (N-1) where N is the total number of elements in the distribution. I.C. for English plain = 1.73 and 1.0 for random text. We may apply the I.C. test to the distributions of periodic polyalphabetic ciphers to confirm the monoalphabeticity of their character. This also confirms the period length and correctness. if the correct period is assumed, then the Phi test applied to each of the alphabets should approximate closely and consistently the value of Phi(p) and conversely, if the incorrect period is assumed, then the Phi(o) should approximate the value of Phi(r). Deviation from this hypothesis must be statistically significant. [FR7]

So we break down the four alphabets:

```
  4 1 4 1 1 1 1 1 3     1   1 1     1 1 4      Phi =42
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  I.C.=1.68

1   2   4   1         2 1     4     4 1     1 2 2 Phi=44
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  I.C.=1.91

1   5     1   1 1 1   5 2 1     1       2 1   1 2 Phi=46
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  I.C.=1.99

    1   6   2   2 1     1   1 1   2 2     1 1 3 1 Phi=44
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  I.C.=1.91
```

It is seen that all these distributions are monoalphabetic since their observed Phi's are closer to the Phi (p) = 40. rather than Phi (r) = 23. Any other period assumed at four or a multiple of four, will not yield monoalphabetic distributions.

In light of the foregoing principles, we now look at two additional cryptanalytic techniques for the Viggy family. The first compares the distributions to the normal and the second is very important - completing the plain-component.

SOLUTION BY FITTING THE DISTRIBUTIONS TO THE NORMAL

Given message text A:

```
            5         10         15         20         25
A.  A U K H Y  J A M K I  Z Y M W M  J M I G X  N F M L X
B.  E T I M I  Z H B H R  A Y M Z M  I L V M E  J K U T G
C.  D P V X K  Q U K H Q  L H V R M  J A Z N G  G Z V X E
D.  N L U F M  P Z J N V  C H U A S  H K Q G K  I P L W P
E.  A J Z X I  G U M T V  D P T E J  E C M Y S  Q Y B A V
F.  A L A H Y  P O I X W  P V N Y E  E Y X E E  U D P X R
G.  B V Z V I  Z I I V O  S P T E G  K U B B R  Q L L X P
H.  W F Q G K  N L L L E  P T I K W  D J Z X I  G O I O I
J.  Z L A M V  K F M W F  N P L Z I  O V V F M  Z K T X G
K.  N L M D F  A A E X I  J L U F M  P Z J N V  C A I G I
L.  U A W P R  N V I W E  J K Z A S  Z L A F M  H S
```

The period is 5 and the I.C. confirms this hypothesis.

We make uniliteral frequency distributions for the 5 alphabets to determine if we have standard alphabets.

```
Alphabet 1     I.C. = 1.44
5 1 2 3 3   3 2 2 6 2 1   6 1 5 3   1   2   1     6
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

Alphabet 2     I.C. = 1.47
5   1 1   3   3 1 2 4 9 1   2 5     1 2 4 4     4 3
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

Alphabet 3     I.C. = 1.71
2 3     1       8 2 2 4 8 1   1 2     3 4 5 1 1   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

Alphabet 4     I.C. = 1.36
3 1   1 3 4 4 4     2 2 3 3 1 1   1   2   2 4 9 2 2
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Alphabet 5     I.C. = 1.91
        6 2 4   8 1 3   7   1 2 1 4 3     5 2 2 2
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
```

Except for possibly Alphabet 1, all are standard distributions. It is clear that the Aplain for alphabets 2,3,4,5 are H,I,T,E cipher. A little experimentation gets us Aplain in alphabet 1=Wcipher. The key word under Aplain is WHITE. The five complete cipher alphabets are shown in matrix form in Figure 11-7.

Figure 11-7

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

Applying these values to the first groups of our message:

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

Look at the I.C.'s for these alphabets. The expected is 1.73. The third alphabet is almost exact. Three alphabets seem low and one is high or are they? Actually these deviations are within one sigma of the samples of these sizes 55 tallies, so the deviations are not abnormal. The standard deviations may be calculated with:

For plain text:

Sigma (O) = Sqrt[(0.0048)N**3 + (.1101)N**2- (.1149) N]

Sigma(I.C.)= 26/(N-1)sqrt(N) * sqrt[(0.0048)N**2 + (.1101)N- (.1149)]

The more important deviation is from random rather than observed:

Sigma(Phi) = 0.2720 sqrt[N (N-1)]

Sigma(I.C.)= 7.0711/sqrt[N(N-1)]

where: sqrt is the square root function
The latter two equations apply to a 26 letter alphabet only.

Since simage is defined as a difference between the observed and the expected number, divided by the standard deviation, it may be shown that the I.C. of Alphabet 1 is 1.44-1.00/.13 = 3.38 sigma over random; for this type of distribution which follows the Chi squared distribution, this amounts to 1 chance in 300 of being random.

In the foregoing example, standard alphabets were used. We could easily of used reversed standard alphabets. The U.S. Army Cipher Disk produces just this type of cipher. It is known as the Beaufort Cipher. The direction of the crests and troughs is reversed when fitting the distributions to the normal.

SOLUTION BY COMPLETING THE PLAIN-COMPONENT SEQUENCE

When direct standard alphabets are used we can mechanically solve the cipher by completing the plain component. The plain text reappears on only one generatrix and this generatrix is the same for the whole message. It is the only generatrix that yields intelligible text. This same process can be modified to work with the alphabets of a Viggy. In this case the correct generatrix should be distinguishable from the others because it shows a more favorable assortment of high frequency letters, and thus can be selected by eye from the whole set of generatrixes.

Using the previous example, we let the first ten cipher letters in each alphabet be set down in a horizontal line and the assumption is made that the alphabets are direct standard with normal sequences. See Figure 11-8.

We use the following selection rules:

1. Circle all low frequency letters J, K, Q, X, Z and discard any row that has two or more of these letters in it.

2. We weight the eight highest frequency letters (ETANORISH) as 1 and the remaining letters as 0. The sum of the weights is recorded at the side of each row.

3. Select the highest score. This works 8 out of 10 times. The correct answer is 10 out of 10 if we examine the top three scores. Friedman presents the statistical proof for this method in FRE7].

This method works regardless of the key (which might be a number) as in the Gronsfeld Cipher.

Figure 11-8

Gen./		Alphabet 1		Alphabet 2		Alphabet 3		Alphabet 4
1		AJZJNEZAIJ	2	UAYMFTHYLK	2	KMMIMIBMVU		HKWGLMHZMT
2		BKAKOFABJK		VBZNGUIZML		LNNJNJCNWV	5	ILXHMNIANU
3		0 CLBLPGBCKL	4	WCAOHVJANM		MOOKOKDOXW		JMYINOJBOV
4		0 DMCMQHCDLM		XDBPIWKBON	2	NPPLPLEPYX		KNZJOPKCPW
5	*	7 ENDNRIDEMN		YECQJXLCPO		OQQMQMFQZY		LOAKPQLDQX
6		7 FOEOSJEFNO		ZFDRKYMDQP	7	PRRNRNGRAZ	3	MPBLQRMERY
7		2 GPFPTKFGOP		AGESLZNERQ	7	QSSOSOHSBA		NQCMRSNFSZ
8		HQGQULGHPQ	5	BHFTMAOFSR	6	RTTPTPITCB	*8	ORDNSTOGTA
9		5 IRHRVMHIQR	4	CIGUNBPGTS		SUUQUQJUDC	4	PSEOTUPHUB
10		JSISWNIJRS		DJHVOCQHUT	4	TVVRVRKVED		QTFPUVQIVC
11		KTJTXOJKST	4	EKIWPDRIVU	3	UWWSWSLWFE		RUGQVWRJWD
12		LUKUYPKLTU		FLJXQESJWV		VXXTXTMXGF		SVHRWXSKXE
13		MVLVZQLMUV		GMKYRFTKXW	1	WYYUYUNYHG	3	TWISXYTLYF
14		4 NWMWARMNVW		HNLZSGULYX		XZZVZVOZIH		UXJTYZUMZG
15		OXNXBSNOWX	4	IOMATHVMZY	5	YAAWAWPAJI		VYKUZAVNAH
16		3 PYOYCTOPXY		JPNBUIWNAZ		ZBBXBXQBKJ	3	WZLVABWOBI
17		QZPZDUPQYZ		KQOCVJXOBA	2	ACCYCYRCLK		XAMWBCXPCJ
18		RAQAEVQRZA	1	LRPDWKYPCB		BDDZDZSDML		YBNXCDYQDK
19		5 SBRBFWRSAB		MSQEXLZQDC	*8	CEEAEATENM		ZCOYDEZREL
20		4 TCSCGXSTBC	*6	NTRFYMARED	2	DFFBFBUFON	4	ADPZEFASFM
21		2 UDTDHYTUCD	5	OUSGZNBSFE	2	EGGCGCVGPO	4	BEQAFGBTGN
22		4 VEUEIZUVDE	4	PVTHAOCTGF	0	FHHDHDWHQP	2	CFRBGHCUHO
23		2 WFVFJAVWEF	1	QWUIBPDUHG		GIIEIEXIRQ	3	DGSCHIDVIP
24		XGWGKBWXFG		RXVJCQEVIH		HJJFJFYJSR		EHTDIJEWJQ
25		YHXHLCXYGH		SYWKDRFWJI		IKKGKGZKTS		FIUEJKFXKR
26		ZIYIMDYZHI		TZXLESGXKJ	2	JLLHLHALUT		GJVFKLGYLS

```
        Alphabet 5
1       YIMXXIRMEG
2       ZJNYYJSNFH
3       AKOZZKTOGI
4     2 BLPAALUPHJ
5       CMQBBMVQIK
6     4 DNRCCNWRJL
7       EOSDDOXSKM
8     5 FPTEEPYTLN
9       GQUFFQZUMO
10    4 HRVGGRAVNP
11    4 ISWHHSBWOQ
12      JTXIITCXPR
13      KUYJJUDYQS
14      LVZKKVEZRT
15    3 MWALLWFASU
16      NXBMMXGBTV
17    3 OYCNNYHCUW
18      PZDOOZIDVX
19      QAEPPAJEWY
20      RBFQQBKFXZ
21    4 SCGRRCLGYA
22    3 TDHSSDMHZB
23   *8 UEITTENIAC
24      VFJUUFOJBD
25      WGKVVGPKCE
26      XHLWWHQLDF
```

The high frequency generatrixes are selected and their letters are juxtaposed in columns, the consecutive letters of intelligible plain text present themselves. If reversed standard alphabets are used, we must convert the cipher letters of each isolated alphabet into their normal, plain component equivalents, and then proceed as in the case of direct standard alphabets.

```
For Alphabet 1, generatrix 5..  E N D N R I D E M N
For Alphabet 2, generatrix 20.. N T R F Y M A R E D
For Alphabet 3, generatrix 19.. C E E A E A T E N M
For Alphabet 4, generatrix 8..  O R D N S T O G T A
For Alphabet 5, generatrix 23.. U E I T T E N I A C
```

(Read down the columns for plain text.)

Friedman describes a graphical method for generatrix development in [FR7] and [FR8].

Time to move on to other family members. We shall identify the systems and peculiarities of each, but remember that the solution techniques presented for the papa bear apply equally well to the children and cousins.

VARIANT CIPHER

The Variant Cipher is just that, a variant of the Vigenere, except that if the Viggy procedure is followed through, a peculiar keyword appears, like JYUWFT. Going back to the slides, In the Variant, the plaintext appears in the opposite slide from the one containing the key letter: Vigenere below the 'A' and Variant above the 'A'. The application of the high frequency letters is the same. The keyword is obtained in a different fashion. For the simple encipherment of COME AT ONCE with the keyword TENT:

```
T E N T     T E N T
-------     -------
C O M E     J K Z L
A T O N     H P B U
C E - -     J A - -
```

The setting of the slides for say , the initial T of the keyword is:

```
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
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
```

The decipherment of a Variant is the same as a Vigenere.

VARIANT SOLUTION BY COMPUTER

>From our trusty CDB, I found Variant.exe and applied it to the following cryptogram:

```
UALOT SILKH RWEBN NRHNL THURD VPVCH DLSUC OABSM YMXFO QAUBR
NFHFR IBAOH YTMWT ENJVQ UPZHF AQWGZ MVHTB OENJD IGIMF SULUA
BPMLZ RNFNX SMJTG DJHAF EKKSZ QWDZQ CLVRN FZXBZ WISTJ LMRNH
RZ.
```

The solution was found in two steps with a period of 7, keyword "RABBVTS" which is RABBITS, and reads: Lamp black is extensively in the manufacture of printing inks, as a pigment for oil painting and also for waxing and lacquering of leather as well as in darkening a furniture polish. Total time 2 or 3 minutes.

BEAUFORT CIPHER

A third member of the Viggy family, the Beaufort, and while the same procedure is applied, the slides (or tables) are different. One is a normal alphabet, extending double length A-Z; the other is reversed, double length Z-A. So if I = T at one setting, then T=I at the same setting. It does not matter what the index for the key is, the results are the same.

So:

```
ABCDEFGHIJKLMNOBQRSTUVWXYZABCDEFGHIJKL
TSRQPONMLKJIHGFEDCBAZYWXVUTSRQPONMLKJI
*                          *
```

Again the simple example.

```
T E N T     T E N T
-------     -------
C O M E     R Q B P
A T O N     T L Z G
C E - -     R A --
```

BEAUFORT SOLUTION BY COMPUTER NEEDS WORK

I found BEAUFORT.exe at the CDB and applied it two the following message:

```
LDYUP AKUPT LVDTO BXUFW SERZP QMQPD NITHA NXUHE UGZTG HMGSM
SRCUF LBQPZ XRYOB FDMNZ TGCUP QQUFB PANAQ HBOON XOOQP DJCJK
TPFDV TBRKL TTSZG ODUFB TETEL POIEB HRTSM DBGGA YUT.
```

Not so successful this time. It croaked at period = 6. The best i could get was "light-" I then reran the program with a wider key range and found that the true period was 10. After some trial and error, the keyword is LIGHTHOUSE and the message starts:

A fine head land of granite pierced by a natural arch on.. Solution time 15 minutes with at least two wrong trails.

RELATIONSHIPS

LEDGE points out some interesting relationships between the Vigenere, Variant and Beaufort. Let A=0, B=1, C=2 .. Z=25, then:

- Vigenere: Cipher Letter = Plaintext letter + keyletter (modulo 26)
- Variant: Cipher letter = Plaintext letter - keyletter (modulo 26)
- Beaufort: Cipher letter = Keyletter - Plaintext letter (modulo 26)

Suppose plain text = B and Key = C. Since B=1 and C=2, Vigenere ciphertext = 1 + 2 = 3 or D; For Variant ciphertext 1-2=-1 +26 = 25 = Z.

For Vigenere and Variant if key letter = A, since A=0,the cipher text = plain text. If we reconstruct a cipher assuming it is a Vigenere, but it is actually a Variant, we will get the true plain text but strange keyword. By subtracting the Variant equation from the Vigenere equation and setting cipher text (Viggy) = ciphertext (Variant) and similarly plaintext (Viggy) = plaintext (Variant), we get the keyletter (Variant) = - keyletter(Vigenere) the same relationship as that between ciphertext and plaintext when the keyletter is A in the Beaufort (since A=0). Hence, we encipher our strange keyword with the A Beaufort alphabet to get the Variant key. The same holds true if we have a Variant and assume it a Viggy.

If we have a Vigenere and a fragment of the same message enciphered with the same key in Variant (or visa versa) then,

a. Plaintext = (Ciphertext(Variant)) + Ciphertext(Vigenere))/2(modulo 13)

b. Key = (Ciphertext(Vigenere) - Ciphertext(Variant))/2(modulo 13)

If we have a Vigenere and a fragment of a Beaufort for the same key and plaintext or visa versa then,

c. Plaintext = (Ciphertext(Vigenere)) - Ciphertext(Beaufort))/2(modulo 13)

d. Key = (Ciphertext(Vigenere) + Ciphertext(Beaufort))/2(modulo 13)

In equations a-d, two answers are produced because modulo 13 will give one number from 0-12 and another 13-25. Solution is by inspection.

PORTA (aka NAPOLEON'S TABLE)

Table 11-7 defines the PORTA Cipher. In this table the alphabets are all reciprocal, for example Gplain(Wkey) = Rcipher, Rplain(Wkey)=Gcipher. They are called complementary alphabets. Either of two letters may serve as a key letter indifferently: Gplain(Wkey) or Gplain(Xkey) = Rcipher.

Table 11-7

	A	B	C	D	E	F	G	H	I	J	K	L	M
AB	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	A	B	C	D	E	F	G	H	I	J	K	L	M
CD	O	P	Q	R	S	T	U	V	W	X	Y	Z	M
	A	B	C	D	E	F	G	H	I	J	K	L	M
EF	P	Q	R	S	T	U	V	W	X	Y	Z	N	O
	A	B	C	D	E	F	G	H	I	J	K	L	M
GH	Q	R	S	T	U	V	W	X	Y	Z	N	O	P
	A	B	C	D	E	F	G	H	I	J	K	L	M
IJ	R	S	T	U	V	W	X	Y	Z	N	O	P	Q
	A	B	C	D	E	F	G	H	I	J	K	L	M
KL	S	T	U	V	W	X	Y	Z	N	O	P	Q	R
	A	B	C	D	E	F	G	H	I	J	K	L	M
MN	T	U	V	W	X	Y	Z	N	O	P	Q	R	S
	A	B	C	D	E	F	G	H	I	J	K	L	M
OP	U	V	W	X	Y	Z	N	O	P	Q	R	S	T
	A	B	C	D	E	F	G	H	I	J	K	L	M
QR	V	W	X	Y	Z	N	O	P	Q	R	S	T	U
	A	B	C	D	E	F	G	H	I	J	K	L	M
ST	W	X	Y	Z	N	O	P	Q	R	S	T	U	V
	A	B	C	D	E	F	G	H	I	J	K	L	M
UV	X	Y	Z	N	O	P	Q	R	S	T	U	V	W
	A	B	C	D	E	F	G	H	I	J	K	L	M
WX	Y	Z	N	O	P	Q	R	S	T	U	V	W	X
	A	B	C	D	E	F	G	H	I	J	K	L	M
YZ	Z	N	O	P	Q	R	S	T	U	V	W	X	Y

The Porta Cipher permits 13 different ways to disguise a plain letter.

Again our simple encipherment:

```
T E N T    T E N T
C O M E    Y M S N
A T O N    W E I E
C E - -    Y T - -
```

A peculiarity of this system is that since half the alphabet is represented by the half of the alphabet, there never will be found the letters A-M of the plaintext appearing as A-M in the ciphertext; no N-Z plaintext appearing as the N-Z ciphertext. This helpful in placing a tip. THE shows up as a (A-M) (N-Z) (N-Z) combination. [BRYA]

Table 11-8 shows a different view of the PORTA Cipher

Table 11-8

Plain Text

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

Using the message text A from page 20 as an example with key word WHITE , the distribution of 5 alphabets is:

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

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

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

     1   1   4 4     2 2 3 3 1 9 2 2 3 1   1 3 3 2   2 4
4.   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

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

Now we can divide the M and N distributions, and each half may be used to fit a normal distribution. In alphabet 1, the sequence CDEFGHIJ cipher may easily be recognized as NOPQRSTU plain; this would fix the keyletters as WX, and therefor the A...Mplain sequence should begin with Ycipher. In alphabets 2,3, and 5 the RSTplain sequence may be spotted at BCDcipher, ABCcipher, and CDEcipher, respectively, whereas in alphabet 4, if Ncipher = Eplain, then Ecipher = Nplain; therefore the original assumptions for the first halves will be confirmed by the goodness of fit of the distributions for the second halves. The keys fore these 5 alphabets are derived as (W,X), (G,H) (I,J), (S,T), and (E,F); from these letters we get WHITE.

In completing the plain component sequence for the Porta encipherment, the cipher letters are first converted to their Porta plain-component equivalents and then these letters are used for the decipherment. EXCEPT, cipher letters A-M are completed in a downward direction and cipher letters N-Z are completed in an upward direction.

Reference [FR7] gives the example:

```
P K T F F  C D V I T  O B V Z X  C V R E E  G I V J E
T P R K T  O Q C F L  P B V P X  ....
```

The conversion process and plain component completion of the first three alphabets are shown below using the generatrix elimination and weighting scheme developed earlier:

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

The generatrixes with the highest scores are the correct ones.

MODIFIED PORTA

Just as the Vigenere table consisting of direct standard alphabets has its complementary table of reversed standard alphabets, a variant of the Porta table can be constructed where the lower halves of the sequences run in opposite direction to the upper half. For example,

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

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

PROBABLE WORD METHOD OF SOLUTION FOR PORTA

The probable word method is very easy way to attack a Porta cipher. Let 1 = any letter in the A-M sequence, and 2 equal any letter in the N-Z sequence.

```
P K T F F  C D V I T   O B V Z X  C V R E E  G I V J E
2 1 2 1 1  1 1 2 1 2   2 1 2 2 2  1 2 2 1 1  1 1 2 1 1

T P R K T  O Q C F L   P B V P X  ....
2 2 2 1 2  2 2 1 1 1   2 1 2 2 2
```

Use the probable word INFANTRY, which has the class notation of 12112222, but in encipherment is reversed to 21221111 pattern. At position 15, X C V R E E G I, we find:

```
plain       I N F A N T R Y
cipher      X C V R E E G I

key         E W G I S E W G
derived     F X H J T F X H
```

Read diagonally, we see WHITE repeated.

COMPUTER SOLUTION OF PORTA

At the trusty CDB is a program called PORTA.exe. Using it on the following cipher message found a period of 9 with a possible key of KL/IJ/CD/MN/AB/OP/OP/EF/QR. I came up with the keyword LIDNAOOER

```
EYWRR  MOTJJ  QOHFA  LTYQV  SQFPG  EPWTG  RVGUC  DVVBT  EMLMN
BYSOE  OHFKW  YARQL  PEBSB  ETVXM  WVBCV  XRTIT  JJAMX  EHADX
VCAXN  MMWZR  WALFY  BTJSP  RTLLP  LZDVD  FZHGE  PBKQR  RUKWQ
AEAOP  Y
```

and behold the message cracked to:

While the Romans used leeks in the culinary depart..

The process took less than two minutes but did not yield the actual keyword or require it.

GRONSFELD

The GRONSFELD Cipher uses a numerical key and restricts the Viggy table to just ten alphabets. We can construct a slide with one normal alphabet and numbered one like this:

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

One half the digits are used for encipherment and the other half for decipherment. For example the key is derived as follows:

```
C O N S T I T  U  T  I O N
1 6 4 8 9 2 10 12 11 3 7 5
```

The first duplicate letter carries the lower number.

So back to:

```
6 2 3 4     6 2 3 4
C O M E     I Q P I
A T O N     G V R R
C E - -     I G - -
```

Slide method: put the 0 over the C, take the letter to the right in juxtaposition of the 6 = I, same for A which is G and so on. We decipher by looking to the left.

A typical decipherment might look like this for the test word "YOUR":

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


T S V H Y Q B V Y I G L M G U X A S R M F K C I A A O V I Z
-----------------------------------------------------------
Y     9 0   3   0   8     8     2       7   4   2 2
O         2   7             6     4                 0
U           7   4             3                       1
R             4                 9
```

LECTURE 11 PROBLEMS

11.1 Viggy.

```
SYCVT  HFXEQ  DPTLN  KTGMP  FHMPA  SRVIT  LSEXH  DPITX
KELIQ  WDXEC  VNLIP  HPWXD  XXIXH  UTRIH.
```

11.2 Beaufort.

```
SXSXZ  IYLEQ  AWEQF  EZEPP  QZQRD  VANKH  HLZJX  OQSEU
YSOVS  SZKLE  DRMRU  THTUW  SCLOX  NEHLA  OPEEU  GAZIA
UUOQG  OJX.
```

11.3 Variant.

```
JQRSB  YBKNF  WWTGK  UXDTK  ZAOAA  MCVJU  KBCEX  GUYLB
UASWY  TIENQ  XLPYX  CWASU  VAKOM  XIGIK  XHWZT  SWGOP
WRTSJ  NAWG.
```

11.4 Gronsfeld.

```
ZRWQU  IKLMS  IXAWI  UQMWP  KFQEL  RBWJG  XHIXT  NLVKS  ZHVHS
ZRUEK  KWPIM  GSXIA  XVUEL  RHZPI  SLBWT  NHU.
```

11.5 Viggy or Beaufort; same message and key starts ONOIHT.

```
ORQGX  HPNKW  QQCHI  ABIFZ  NQCHR  VLVLU  HYUDT  MCYJN  WAUHP
HLVIN  BZCCB  GCGKZ  JNLMM  WTVLY  DYCCV  JPUVG  KLKQX  YTTKI
XOQYB  JJMHJ  BYHQY  LFQWF  NRYUC  XCECN  GPCBW  TPAXE  ABKGC
PVHKL  OIKQW  TPKOW  KNCMM  HFFAV  A.
```

ANSWERS TO LECTURE 10 PROBLEMS

Thanks to JOE O for a fine analysis of all three problems.

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

```
1234567  1234567  1234567  1234567  1234567  1234567  1234567
THEFIRS  TIMEaVI  SITOREX  CLAIMSA  HROMANT  ICVENIC  ESINKIN
KKQHPQR  KTYOiTA  TLGAWBM  XORKTAT  BSOOIYI  CGICEJV  UCYZRJP

ALNSFRZ  UCQDXIS  TDRBFYS  YTFDZBD  USQWKMT  CPPDOAI  CAAKEHK

UAYFHQA  TLNIFSI  SIGJHAS  V.
```

QQ-1 Quagmire I Solution.

VERDICT/nose. Period =7.
The first time visitor exclaims "Ah, romantic Venice sinking into the sea." The seasoned traveler exclaims,"Ah, stinking Venice rising out of the sea.

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

QQ-2 QUAGMIRE III Tedious. (CRYPTANALYTIC METHODS) DOPPELSCHACH
Period= 6

```
12345  61234  56123  45612  34561  23456  12345  61234  56123
THETI  MEREQ  UIRED  BYS.......
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.
```

HARDER/decorative. Period = 6. The time required by some cryptanalytic methods grows extremely rapidly as key length or message length increases. All possible keys for a columnar transposition instead of making an entry by building up a from a pair of columns is an example.

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

QQ-3 QUAGMIRE IV Economics Lesson. EDNASANDE

(BUSINESSACTIVITYDURINGAPERIOD)

THEEC ONOMY OFTHE NATIO .....
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.

EXCHANGE/stock/MARKET. The economy of the Nation is built on supply and demand, the result of inflation. Recession is a temporary falling off of business activity during a period when such activity has been generally increasing..

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

REFERENCES / RESOURCES [updated 5 May 1996]

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

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

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

[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.

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

[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.

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

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

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

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

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

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

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

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

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

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

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

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

[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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[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 Solution of the ENIGMA," Aegean Park Press, Laguna Hills, CA, 1988.

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

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

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

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

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

[DONI] Donitz, Karl, Memoirs: Ten Years and 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. [A text that every serious player should have!]

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

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

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

[EVES] 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.

[FRAN] Franks, Peter, "Calculator Ciphers," Information Associates, Champaign, Il. 1980.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[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.

[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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[ROOM] Hyde, H. Montgomery, "Room 3603, The Story of Britis 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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