CAUTION: THESE RECORDS WILL BE USED FOR OFFICIAL PURPOSES ONLY, DO NOT REMOVE PAPERS NOR REVEAL CONTENTS TO UNAUTHORIZED PERSON(S)

RECORDS CHARGE-OUT

REF ID:A64554

10208

DATE OF REQUEST	SUSPENSE DATE
25 Jan 61	10 Feb 61

FILE OR SERIAL NUMBER AND SUBJECT	From File of Special Consultant (Friedman) Military Cryptanalysis, Part II, Interim Edition (Second Section) Confidential
TO	NAME AND EXTENSION OF PERSON REQUESTING FILE: Mr. William Friedman LI6-8520 ORGANIZATION, BUILDING, AND ROOM NUMBER: 310 2nd,Str,SE,Wash,D.C.
RETURN TO	Mrs.Christian,AG-2$_4$,NSA,Ft.Geo.G.Meade,Md.
	DATE RET'ND.
	INITIAL HERE
INSTRUCTIONS	WHEN TRANSFERRING FILE TO ANOTHER PERSON, COMPLETE SELF-ADDRESSED TRANSFER COUPON BELOW, DETACH, STITCH TO BLANK LETTER-SIZE PAPER AND PLACE IN OUT-GOING MAIL SERVICE.

10208

2ND TRANSFER COUPON

TO

FILE (serial number and subject)

TRANSFERRED TO: (name and extension)

ORGANIZATION, BUILDING, AND ROOM NUMBER

DATE	(sig)	(ext.)

~~CONFIDENTIAL~~
Modified Handling Authorized

NATIONAL SECURITY AGENCY

MILITARY CRYPTANALYTICS
Part II

INTERIM EDITION
(Second Section)

By
LAMBROS D. CALLIMAHOS
and
WILLIAM F. FRIEDMAN

Office of Training Services
National Security Agency
Fort George G. Meade, Maryland

February 1958

~~CONFIDENTIAL~~
Modified Handling Authorized

~~CONFIDENTIAL~~
Modified Handling Authorized

NATIONAL SECURITY AGENCY

MILITARY CRYPTANALYTICS
Part II

INTERIM EDITION
(Second Section)

By
LAMBROS D. CALLIMAHOS
and
WILLIAM F. FRIEDMAN

S—70,022

Office of Training Services
National Security Agency
Fort George G. Meade, Maryland

February 1958

~~CONFIDENTIAL~~
Modified Handling Authorized

(BLANK)

TABLE OF CONTENTS

MILITARY CRYPTANALYTICS, PART II

Periodic Polyalphabetic Substitution Systems

* Chapters I-IX are contained in the First Section of the Interim Edition of Military Cryptanalytics, Part II.

* Appendices 4-9 are contained in the Third Section of the Interim Edition of Military Cryptanalytics, Part II.

CHAPTER X

REPEATING-KEY SYSTEMS WITH UNRELATED ALPHABETS

74. General remarks.--a. In the first nine chapters of this text we have treated only those periodic polyalphabetic systems which involve a relationship among the secondary alphabets. This relationship is brought about by the Vigenère properties of the basic cipher square, or the identical properties possessed by the interaction of sliding primary components. In the case of Porta systems, Vigenère-type properties also exist, but in a modified form. Since the Vigenère square incorporates cyclic permutations of a basic cipher component, the symmetry among the secondary alphabets when related to the original primary plain component is visible or direct; if some other component is considered as the plain component, the relationships among the secondary alphabets will be latent or indirect.

b. If instead of a cipher square of interrelated alphabets there was used a matrix of N different unrelated alphabets, of course no symmetry of any kind would be manifested. Therefore the initial solution of a cryptogram in such a system would progress along the usual lines of first principles (i.e., factoring, assumptions of letters based on frequencies or vowel-consonant analysis, attack by the probable word method, etc.) until the entire cryptogram is solved by the progressive synthesis of the plaintext message. The powerful tool of the reconstruction of the secondary alphabets by principles of direct or indirect symmetry is here inapplicable; therefore the plain text must be coaxed out "the hard way" in its entirety, and any unrecovered values must remain unrecovered until further traffic establishes these latter values.

c. If the N cipher alphabets of a system involving unrelated alphabets are systematically-mixed sequences (e.g., if these sequences are keyword-mixed sequences or transposition-mixed sequences based on different key words), then a partial recovery of the secondary alphabets might reveal what the situation is, and thus make possible the reconstruction of the complete secondary alphabets. If, however, the cipher alphabets are composed of random-mixed sequences, no complete reconstruction would be possible until enough cipher text has been accumulated to permit of establishing all the values in all the alphabets.

d. Once the N basic sequences of a cryptosystem with unrelated alphabets are reconstructed, the solution of subsequent messages using the same sequences is a simple matter, even if the sequences are used in a different order, as will presently be demonstrated.

75. Solution of a typical system involving unrelated alphabets.--a. The cryptography of a typical cryptosystem involving unrelated alphabets is quite simple. There are available N different alphabets, which may be used in one of the following ways: (1) all of the alphabets are used in the same sequence, starting at the same point in the sequence; (2) all the alphabets are used in the same sequence, but with different starting points; (3) all the alphabets are used, but in a different order, or (4) only a selection of a certain number of alphabets is made, the number and order of which are determined or controlled by a specific key. In Fig. 80, below, we have a total of 25 different cipher sequences[1] of 26 letters

Plain text

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

Figure 80.

[1] The sequences used in this illustration are actually the sequences used in the obsolete U. S. Army Cipher Device, Type M-94. See in this connection Appendix 6, "Cryptographic Supplement."

each in the form of 26-letter strips; these strips fit horizontally into a frame with space for up to 25 strips, and at the top of the frame there is affixed a normal sequence in which the plaintext letters are to be found. If it were standard practice to select a certain fixed number of strips for the cipher components, these cipher strips would be placed into the device in a predetermined order under the plaintext strip and the process of encryption and decryption would proceed as in any repeating-key cipher using a matrix.[2]

b. In Fig. 81 there is illustrated the inverse matrix derived from the previous figure, showing the plaintext equivalents for the 26 cipher letters.

Cipher text

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

Figure 81.

[2] If 10 different sequences were used for the cipher components, then the number of different permutations of 25 things taken 10 at a time is given by the formula $P_{10}^{25} = \frac{25!}{(25-10)!} = \frac{25!}{15!} = 11,861,676,288,000$, or, expressed in standard mathematical notation, approximately 1.19×10^{13}. If only 5 different sequences were used for the cipher components, the number of different permutations is 6.38×10^{6}, if 15 sequences were used, the number would be 4.27×10^{18}, if 20 were used, the number is 1.29×10^{23}, and if all 25 sequences were used, the number of permutations is 25! or 1.55×10^{25}. However, the fearless cryptanalyst goes ahead and solves his problem anyway, in spite of and with utter disregard for the fearful magnitude of these awe-inspiring numbers.

From the two foregoing matrices, there may be derived diagrams of limitations of the basic matrix. In Fig. 82a we have a diagram of the impossible ciphertext equivalents of plaintext letters, and in Fig. 82b we have a

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

Figure 82a.

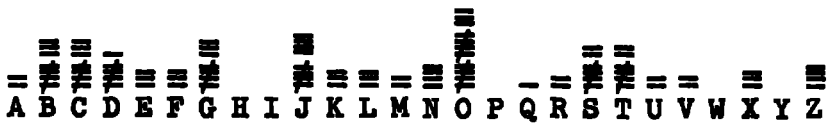
Cipher

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

Figure 82b.

diagram of the impossible plaintext equivalents of ciphertext letters. These two diagrams will be very useful in the analysis of cryptograms enciphered by means of these alphabets, once the basic sequences have been recovered from previous analysis or by compromise.

c. If strip No. 1 were used in a periodic polyalphabetic cryptogram involving n of the N available sequences, the theoretical expectations of the ciphertext frequencies of the No. 1 strip of Fig. 81 would have the following relative distributional appearance:



Thus, after having factored a periodic cipher in this system to the proper number of alphabets, it is clear that if strip No. 1 were involved in any of the alphabets of the cryptogram, this fact could be recognized by the goodness of fit of one of the distributions with the distribution of the theoretical ciphertext frequencies for strip No. 1. In this fashion, the entire array of the sequences of Fig. 81 could be represented by the theoretical ciphertext frequencies, as shown in Fig. 83, below (to a base of 100):

Theoretical ciphertext frequencies

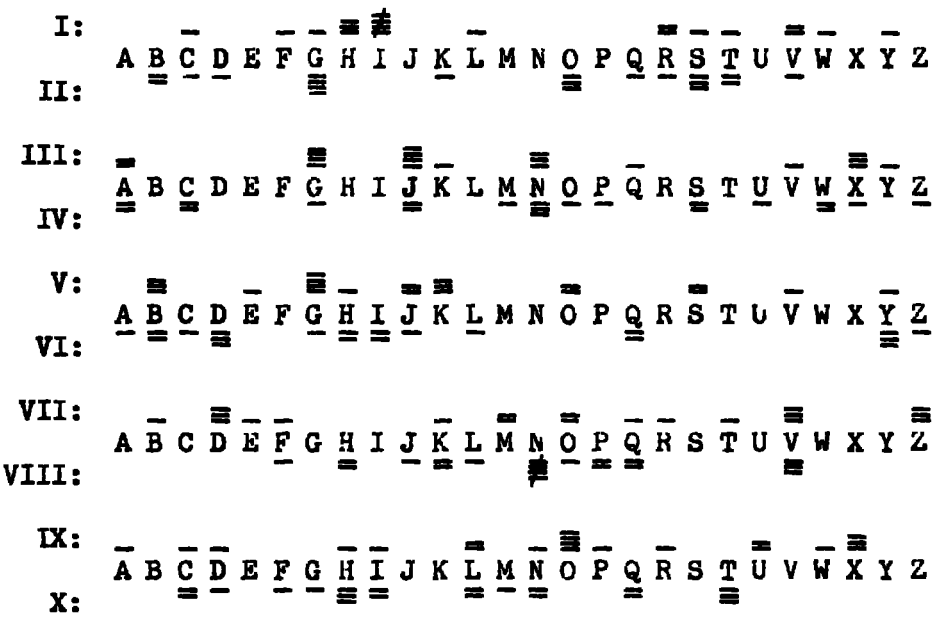
Strip nos.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	8	8	6	3	3	8	0	0	9	3	3	2	4	13	0	1	2	7	7	2	2	0	3	0	4
2	3	1	4	13	3	3	6	2	7	0	0	2	8	3	8	2	2	2	7	4	3	0	0	0	8	9
3	3	8	3	7	0	0	3	6	2	2	0	2	4	0	0	8	1	3	9	4	8	13	3	2	7	2
4	3	2	3	13	4	7	0	4	3	0	8	2	8	2	8	3	6	3	1	2	0	9	0	0	2	7
5	0	2	2	3	4	0	7	0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

Figure 83.

d. Let us use as an example the following message intercepted on an air force link:

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

Since the cryptogram factors to 10 alphabets, distributions are made accordingly, as follows:



e. Matching the distribution for the 1st alphabet against the successive rows of Fig. 83, we obtain the following:

	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 :			1			1	1	3	5			1						2	1	1		2	1		1		
χ(I,1):			8			3	8					3						4	7	7		4					= 44
χ(I,2):			4			3	6	6	3	5		2						4	7	4					8		= 79
χ(I,3):			3				3	1	8	1	0	2						6	9	4		2	6	3	7		= 91
χ(I,4):			3			7		1	2	1	5	2						6	1	2		1	8		2		= 68
χ(I,5):			2				7			3	0	1						4	7	9		4	3				= 67
χ(I,6):			4			9	7	2	4	6	5	2						14	8	2		4	8		4		= 151

* * * * *

On the 6th trial, the χ value of 151 is excellent when compared with χ_m = .0667(100x20) = 133.4 and χ_r = .0385(100x20) = 76.9; the ξ I.C. is here $\frac{151}{76.9}$ = 1.96. Having identified the strip (No. 6) associated with Alphabet I of the cryptogram, the letters of Alphabet I may be deciphered. Alphabet II of the cryptogram when matched with strip No. 1 gives a χ value of 144, which is the highest of the 25 possible matchings; this is equivalent to a ξ I.C. of 1.87, which likewise is very satisfactory; and Alphabet III when matched with strip No. 14 gives a χ of 153, which is a ξ I.C. of 1.99, very good indeed. At this point the cipher letters of the first three alphabets of the cryptogram are decipnered, as follows:

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

These decipherments certainly look like good plain text.

f. We now continue the matching one more step. In testing the distribution for Alphabet IV, we get a χ of 112 (= ξ I.C. of 1.46) against strip No. 10, a χ of 106 (= ξ I.C. of 1.38) against strip No. 15, and a χ of 100 (= ξ I.C. of 1.30) against strip No. 17. Decipherments of the letters of Alphabet IV on the hypothesis of either strip No. 10 or No. 15 do not produce good plaintext tetragraphs, but when strip No. 17 is tried, good plaintext continuations of the trigraphs are manifested. Note the pentagraphic repetition IBJSS; with the decipherment of the first three letters as $\overline{\text{ENE}}_p$, the word ENEMY may be assumed and thus by-pass further χ-test matching. All that is required, after the first three alphabets have been deciphered, is to find what strip will yield an M_p for an S_c, and, if there is more than one such strip, to find the one where $S_c = M_p$ and also where J_c represents a vowel or an R or L (in the sequence $\overline{\text{HRVJ}_c}$ at position 181 of the message); that is, we test for a strip that yields "good" decipherments for Alphabet IV. In other words, after matching 3 or 4 distributions, the plaintext fragments decrypted form a basis for word assumptions, with trials based on the plain-cipher limitations of

Figs. 82a and b. The complete solution now follows easily, and the order of the strips is found to be 6-1-14-17-11-20-4-9-22-24; the message begins with the words AIR RECONNAISSANCE.

g. If a cryptogram is not long enough to be solved by the procedure just described, it may still succumb to attack by the probable word method. For example, let us assume the following short cryptogram is at hand:

O C X Y D D L A N L W B B Y H S F O A I B N D Z E C K S O F

O C X C D L D N X I R C X B M

The message has been intercepted on circuits known to be passing administrative traffic, so a number of probable beginning words will be tried, among which are the following:

ACKNOWLEDGE	CONFIRM	FROM	RECEIPT	REQUIRE
ADVISE	DEPARTURE	INFORM	RECEIVE	REQUISITION
ARRIVAL	DISCONTINUE	IN REPLY	RECOMMEND	RERAD
ATTENTION	EFFECTIVE	ORDERS	REFERENCE	REURAD
CANCEL	EQUIPMENT	OUR	REFERRING	SEND
CITE	EXPEDITE	PARAPHRASE	REPEAT	STATUS
COMMANDING	FOLLOWING	PREPARE	REPORT	SUPPLY
COMMUNICATION	FOR	PROCEED	REQUEST	VERIFY

h. Referring to the diagram of Fig. 82b, we note that the first letter of the cryptogram, O_c, cannot represent S_p or V_p; this rules out the beginning words SEND, STATUS, SUPPLY, and VERIFY. The second letter of the cryptogram, C_c, cannot represent A, C, E, I, R, T, or X, so that 25 more from the list of 40 words are eliminated. The third cipher letter, X_c, cannot represent L, M, O, R, or U; therefore 7 more words are eliminated, leaving only CONFIRM, EFFECTIVE, EQUIPMENT, and INFORM remaining under consideration. Since the fourth cipher letter, Y_c, cannot represent either I_p or O_p, this reduces the possibilities to either CONFIRM or EFFECTIVE; neither one of these words can be eliminated by a continuation of the foregoing process.

i. The possibilities of strip numbers for these two probable words are as follows:

Plain:	C	O	N	F	I	R	M
Cipher:	O	C	X	Y	D	D	L
Strips:	6	1	14	17	3	20	2
	12		25		11		4
					21		

Plain:	E	F	F	E	C	T	I	V	E
Cipher:	O	C	X	Y	D	D	L	A	N
Strips:	1	4	6	20	8	18	24	23	10
	11				9	25		24	15
	22				23				

Since the cryptogram factors to 10 alphabets we will write out the cipher text on this width, and test the assumptions of strip numbers on other rows of the cipher text. Testing the word CONFIRM, with 6-1-14-17 as the first four strip numbers we get the following:

6 1 14 17
O C X Y D D L A N L
C O N F

W B B Y H S F O A I
O N O F

B N D Z E D K S O F
P L A N

O C X C D L D N X I
C O N S

R C X B M
I O N X

This certainly looks promising. If B_c at the next to last position is a null X_p, then M_c might be another X_p null; $M_c = X_p$ on strips 7 and 11, but only on strip 11 does D_c (the fifth letter of the cryptogram) equal I_p, so the correct strip for the fifth position is No. 11. In short order we recover the entire sequence of strips, which is the same as that given in subpar. f, above.

i. If a probable word is to be tested somewhere in the message, the position being unknown, then the diagram in Fig. 82a is useful. For instance, if the crib FLIGHT PLAN is to be tested in the cryptogram given in subpar. g, it will be found that the only place where this crib will fit without a contradiction (i.e., an impossible plain-cipher equivalency) is at the 15th position, beginning with the letters HSF... Where the period is known, the possible strip arrangements may be tested against other cycles of the cryptogram to reduce the key to a unique set of strips, as in the example in subpar. i. When the period of a short cryptogram cannot be determined, the placement of a crib will still yield a key, which, even if not unique, can be tested against the rest of the cipher text in the manner described in subpar. 22f(2).

76. Solution of a second case.--a. The cryptosystem which will now be treated involves a cipher device marketed in France in the 1930's under the misnomer of "transpositeur à permutations secrètes"; Baudouin[3] describes this device and shows one method of attack, albeit a weak one. This device, illustrated in Fig. 84, comprises a frame in which 10 compound strips, joined in the middle, are slid vertically. The upper halves of the strips (Fig. 85a) may be permuted among themselves, and so may the lower strips (Fig. 85b). Thus there are (10!)x(10!) or 13,168,189,440,000 possible permutations--a staggering number which apparently contributed so little to the inventor's Gallic exuberance. The secrecy imparted to messages is, we learn, "guaranteed absolute both mathematically and in practice"; as for the device, "if lost it will not enable the finders to decipher messages that might be intercepted." Still glowing with pride, the inventor goes on to say that since there are 13 trillion possibilities which must be tried

[3] Captain Roger Baudouin, Eléments de Cryptographie, pp. 188-196. Paris, 1939.

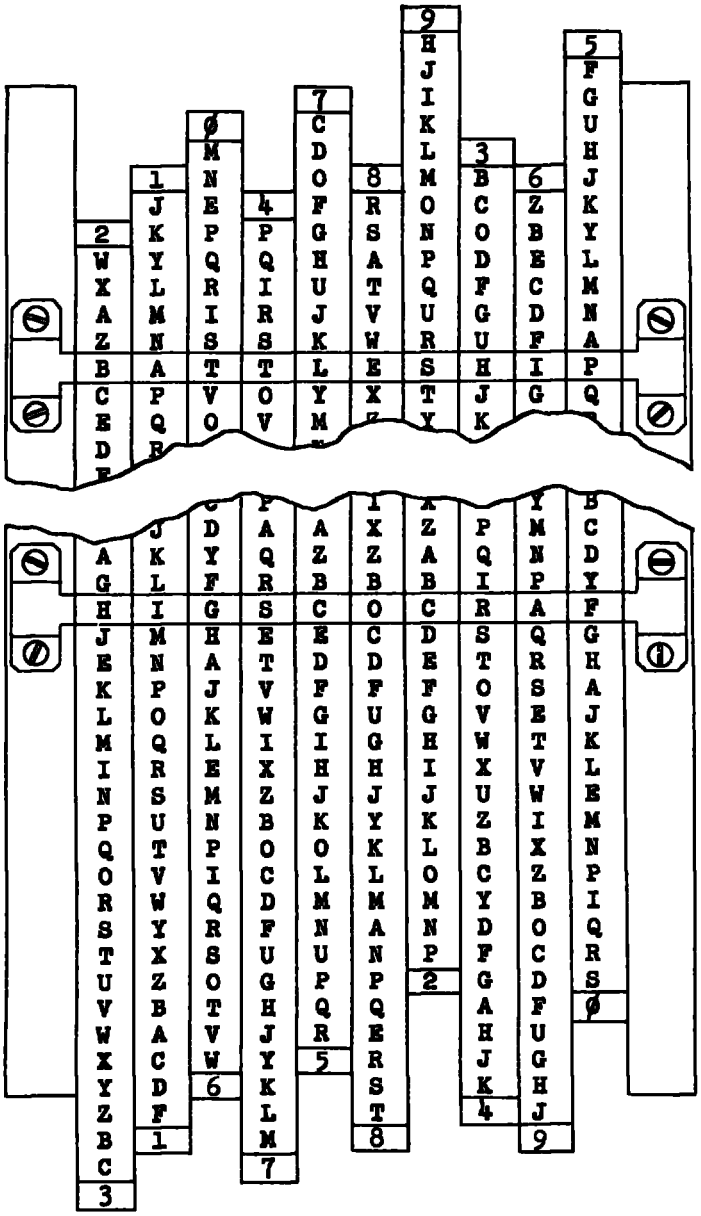


Figure 84.

in order to read an intercepted message, a trial-and-error procedure is rendered absolument impossible, thus "baffling all approaches in cryptanalytics used up to the present time." Stifling a slight yawn, we return to the device.

b. There are two fixed reading positions on the device; the upper one is used for the plain text, while the lower one (26 letters below the first one) is used for the cipher. In encryption, the 20 strips are first arranged according to a specific key; then the first 10 letters of the plain are aligned in the upper reading position, and their cipher equivalents are found in the lower reading position. The same treatment is then applied to the second set of 10 letters of the message, and so on. In decryption, after first arranging the strips according to the key for the message, the inverse procedure is followed, setting up the cipher text on the lower reading position and finding the plain text in the upper.

Upper strips

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

Figure 85a.

Lower strips

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

Figure 85b.

c. Now for some cryptanalytic observations.

(1) First of all, this system yields a periodic polyalphabetic encipherment of only 10 alphabets; any message enciphered by means of this device will always have a period of 10.

(2) In order to take advantage of certain reduced telegraph rates, this system has been constructed so that vowels are enciphered by vowels, and consonants by consonants, so that the resulting cipher text is pronounceable. This is penny wise and cipher foolish-what a wonderful asset in crib-placing! And--further to compound the cryptographic felony--no consonant will ever be enciphered by itself. This system seems to have been designed for cryptanalysis!

(3) It is true that all 20 of the strips are different from each other, so that we have what at first glance might seem to be "unrelated" alphabets. But on closer examination, it will be seen that all of them are but slight modifications of direct standard sequences. Taking upper strip No. 1 as an example,

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

this may be decomposed as follows:

J K	L M N	P Q R	S T V	W X Z	B C D	F G H
y	a	e	i	o	u	

All of the remaining 19 strips are, to our delight, constructed along similar lines. Thus, if we compare upper strip No. 1 and lower strip No. 1,

J K y L M N a P Q R e S T V i W X Z o B C D u F G H
G H e J K L i M N P o Q R S u T V W y X Z B a C D F

we note that we actually have <u>direct</u> symmetry among the consonants (arranged <u>in their normal alphabetical order</u>) and likewise among the vowels. This property is one more cryptanalytic boon bestowed upon us by the inventor.

<u>d</u>. As an example of solution of a cryptogram produced by the <u>transpositeur</u>, let us assume that the following message is at hand:

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

Since the consonants on the strips are arranged in their normal alphabetical order, we should be able to use the method of completing the plain-component sequence for the 20 possible <u>consonant</u> generatrices.[4] This we do forthwith. The completion diagrams for the first five out of the 10 alphabets are as follows:

[4] This easy general solution was overlooked by Baudouin, who employed a much less generally applicable method in his example which depended on a message beginning with a digraph composed of two consonants.

Gen.	Alphabet 1	Alphabet 2	Alphabet 3	Alphabet 4	Alphabet 5
1	~~ZJXBZBT~~	2 KPRFRLM	1 DSZG	~~KMCNQG~~	~~CFWKJKCQ~~
2	~~BKZCBCV~~	3 LQSGSMN	2 FTBH	2 LNDPRH	~~DGXLKLDR~~
3	ø CLBDCDW	4 MRTHTNP	ø GVCJ	~~MPFQSJ~~	1 FHZMLMFS
4	ø DMCFDFX	~~NSVJVPQ~~	ø BWDK	~~NQGRTK~~	3 GJBNMNGT
5	1 FNDGFGZ	~~PTWKWQR~~	~~JXFL~~	2 PRHSVL	1 HKCPNPHV
6	ø GPFHCHB	~~QVXLXRS~~	~~KZGM~~	~~QSJTWM~~	~~JLDQPQJW~~
7	~~HQGJHJG~~	~~RWZMZST~~	1 LBHN	~~RTKVXN~~	~~KMFRQRKX~~
8	~~JRHKJKD~~	3 SXBNBTV	ø MCJP	1 SVLWZP	4 LNGSRSLZ
9	~~KSJLKLF~~	1 TZCPCVW	~~NDKQ~~	~~TWMXBQ~~	3 MPHTSTMB
10	1 LTKMLMG	~~VBDQBWX~~	1 PFLR	~~VXNZCR~~	~~NQJVTVNC~~
11	2 MVLNMNH	~~WCFRFKZ~~	1 QGMS	1 WZPBDS	1 PRKWVWPD
12	2 NWMPNPJ	~~XDGSGZB~~	3 RHNT	~~XBQCFT~~	~~QSLXWXQF~~
13	~~FKNQPQK~~	1 ZFHTHBC	1 SJPV	1 ZCRDGV	~~RTMZXZRG~~
14	~~QZPRQRL~~	~~BGJVJGD~~	~~TKQW~~	1 BDSFHW	3 SVNBZBSH
15	4 RBQSRSM	~~CHKWKDF~~	1 VLRX	~~CFTGJX~~	2 TWPCBCTJ
16	5 SCRTSTN	~~DJLXLFG~~	1 WMSZ	~~DGVHKZ~~	~~VXQDGDVX~~
17	3 TDSVTVP	~~FKMZMGH~~	2 XNTB	ø FHWJLB	1 WZRFDFWL
18	2 VFTWVWQ	2 GLNBNHJ	ø ZPVC	~~GJXKMG~~	~~XBSGFGXM~~
19	~~WGVXWXR~~	~~HMPGPJK~~	ø BQWD	1 HKZLND	~~ZCTHGHZN~~
20	~~XHWZKZS~~	~~JNQDQKL~~	1 CRXF	ø JLBMPF	~~BDVJHJBP~~

The scores to the left of the columns are the sums of the two-category weights described in subpar. 21g; even though we are treating only the consonants, this scoring method suffices and there is no need to devise specially any new weights. (For greater sensitivity, we could of course use the $\log_{133}$ weights treated in par. 34.)

e. The generatrices with the highest scores are assumed to be the correct ones,[5] and the following decipherments result:

[5] In Alphabet 4 there are two generatrices with equal high scores, however, Generatrix No. 2 produces good consonant digraphs with Alphabet 3, whereas the digraphs produced by Generatrix No. 5 are not nearly as good. This is shown by the centiban scores of $\log_{224}$ (cf. Table 15, Appendix 2, Military Cryptanalytics, Part I) of

LL	NG	DS	PR	RS	
73	+ 73	+ 59	+ 66	+ 75	= 346,

whereas

PL	RG	HS	SR	VS	
59	+ 48	+ 38	+ 42	+ 0	= 187, thus confirming the choice

of Generatrix No. 2 of Alphabet 4 as the correct one.

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

For the vowels, the plain-component completion method is possible but too precarious; it is usually too difficult to distinguish the right answers from the wrong.[6] The simplest thing, having established the consonants for some of the alphabets, is to insert vowels in the word structures on the basis of contextual likelihood; one vowel correctly identified in a particular column will of course identify all the vowels in that column. Thus, in the diagram above, $\overline{\text{SMOLL}}_p$ = SMALL and $\overline{\text{CTONG}}_p$ = CTING, etc. Aided as we are both by the plaintext fragments thus far decrypted, and by the consonant-vowel configuration of the rest of the text, the entire cryptogram may now easily be solved, as follows:

[6] It is interesting to point out that in Alphabet 3 where there are 6 vowels, completion of the vowel-sequences together with the deciban scores based on $\log_{133}$ weights yields the following, in which the highest generatrix is the correct one:

Gen.		
1	O U Y O A Y	42
2	U Y A U E A	43
3	Y A E Y I E	46
4	A E I A O I	49
5	E I O E U O	48
6	I O U I Y U	42

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

f. All that remains now is the matter of the key, i.e., the specific arrangement of the upper and lower strips; given the plain text to the cipher, this is a very easy matter. We note, in Figs. 85a and b, that if S_p is found in upper strip No. 1, the only possible cipher equivalents (found in Fig. 85b on the same line with S_p in Fig. 85a) are as follows:

	(lower strip nos.)									
	1	2	3	4	5	6	7	8	9	0
S_p =	Q	B	N	V	D	J	X	G	T	F

Patently, $S_p = Z_c$ is impossible with any combination involving upper strip No. 1. In fact, it is compatible only with the following 7 out of the 100 possible combinations of the strips for the first alphabet:

(upper strip nos.):	2	4	5	6	8	9	0
(lower strip nos.):	3	8	4	1	6	7	5

But, in Alphabet 1, $I_p = I_c$ which should serve to cut down the 7 possibilities above; $I_p = I_c$ in only three of the 7 combinations given above, viz., $\frac{2}{3}$, $\frac{4}{8}$, and $\frac{6}{1}$. Thus, we may limit the possible strip arrangements for the ten alphabets to the following:

~~CONFIDENTIAL~~

Alphabet 1 ($S_p = Z_c$, $I_p = I_c$): $\frac{2}{3}$, $\frac{4}{8}$, $\frac{6}{1}$

Alphabet 2 ($M_p = K_c$, $O_p = Y_c$): $\frac{1}{1}$

Alphabet 3 ($R_p = D_c$, $A_p = O_c$): $\frac{7}{7}$, $\frac{9}{5}$, $\frac{0}{6}$

Alphabet 4 ($L_p = K_c$, $I_p = A_c$): $\frac{4}{7}$, $\frac{8}{2}$

Alphabet 5 ($L_p = C_c$, $E_p = O_c$): $\frac{7}{5}$, $\frac{5}{6}$

Alphabet 6 ($T_p = X_c$, $A_p = I_c$): $\frac{8}{8}$

Alphabet 7 ($R_p = B_c$, $E_p = O_c$): $\frac{3}{9}$, $\frac{4}{6}$, $\frac{5}{7}$, $\frac{9}{2}$

Alphabet 8 ($M_p = W_c$, $O_p = E_c$): $\frac{3}{4}$, $\frac{6}{9}$

Alphabet 9 ($S_p = D_c$, $E_p = Y_c$): $\frac{3}{4}$, $\frac{6}{9}$

Alphabet 10 ($F_p = T_c$, $I_p = E_c$): $\frac{1}{6}$, $\frac{5}{0}$

g. Since there is only one possibility of a strip pair in Alphabets 2 and 6, the positions of upper strips Nos. 1 and 8 and lower strips Nos. 1 and 8 are now fixed. This means that in Alphabet 4 only the pair $\frac{4}{7}$ will remain, as the upper strip No. 8 in the pair $\frac{8}{2}$ has already been used in Alphabet 6; similarly, in Alphabet 10, only the pair $\frac{5}{0}$ will remain. In Alphabet 1, only $\frac{2}{3}$ will remain; and since for Alphabets 8 and 9 we must have either $\frac{3}{4}$ and $\frac{6}{9}$, or vice versa, the only strip pair that remains for Alphabet 7 is $\frac{9}{2}$. This means that for Alphabet 3 the only strip pair must be $\frac{0}{6}$, and that the only strip pair for Alphabet 5 is $\frac{7}{5}$. The strips that have been fixed are as follows:

	Alphabet									
	1	2	3	4	5	6	7	8	9	10
upper strips:	2	1	0	4	7	8	9	·	·	5
lower strips:	3	1	6	7	5	8	2			0

The identity of the strip pairs for Alphabets 8 and 9 cannot be determined uniquely in this particular example; Alphabet 8 is either $\frac{3}{4}$ or $\frac{6}{9}$, and Alphabet 9 is either $\frac{6}{9}$ or $\frac{3}{4}$; either combination will decipher all cryptograms sent in the same key as the one just solved.

h. The foregoing solution is predicated on a knowledge of the device and its strips. If we had not known anything about the device, a single cryptogram of fair length would have sufficed for solution without much difficulty, and the completely filled-out reconstruction matrix (for the device as set up in Fig. 84, for example) might look like this:

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

Figure 86a.

Indirect symmetry extending to the plaintext line would have been manifested, and the following chains (from lines 4 and 10, as an example) would have been recovered:

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

The consonant chain, if decimated at an interval of -3, would yield the consonants in normal alphabetical order. The matrix might thereupon be rearranged as follows:

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

Figure 86b.

The cryptanalyst would make mental note of the direct symmetry manifested in Fig. 86b; he would see that he could solve further cryptograms by a modification of the plain-component sequence method as demonstrated in subpar. d; and he might perhaps be forever blissfully unaware of the existence of the 10 permutable upper strips and the 10 permutable lower strips. In other words, even though he might never know the exact mechanical details of the system, he could still cryptanalyze the traffic with ease. Situations of this sort are not at all uncommon in operational cryptanalytic practice.

77. Solution of a further example.--a. The system to be treated here is one of the machine ciphers used by AGGRESSOR, the maneuver enemy in U.S. joint maneuvers and training exercises. This system is included here because in its cryptanalysis certain interesting and pedagogically valuable techniques come into play, and furthermore some interesting applications of symmetry present themselves, even though the alphabets of the machine are random, nonrelated alphabets.

b. This electromechanical cipher machine is called the ZEN-40 in Aggressor nomenclature. The cryptographic principle embodies a polyalphabetic substitution matrix of 25 reciprocal nonrelated alphabets which are wired electrically in a bank of uniselector switches[7] in the machine's interior. These alphabets are of the Porta type, in which there are two distinct "families" of 13 letters each; a letter in one family has as its equivalents only the 13 letters in the other family. The exact composition of the letters composing the two families is determined by the plugging of a small plugboard located on the front panel of the ZEN-40. The plugboard serves a threefold purpose: (1) it determines the composition of the two families; (2) it changes the identity of the letters in the internally-wired matrix into isomorphic equivalents of the rows of the matrix; and (3) it permutes the order of the rows of the basic matrix. These three aspects will be explained in detail subsequently.

c. There are several procedures in using the ZEN-40, giving rise to a number of different types of cryptosystems. The particular cryptosystem with which we will be concerned in this discussion produces cryptograms enciphered by polyalphabetic substitution of a period of 25, with 25 reciprocal, nonrelated, Porta-type alphabets. The two variables in this cryptosystem are (1) the plugging which remains in force for a particular cryptoperiod (usually one day), and (2) the starting point (determined by a specific key) of the succession of the 25 alphabets. The specific key may be varied at will by the cipher clerk for each message; these keys are designated by indicators consisting of a consonant-vowel digraph repeated, followed by a fixed letter (usually X), such as in the indicator groups BABAX, VEVEX, etc.

d. In the solution of this cryptosystem, the initial cryptanalysis would be accomplished with a small volume of traffic as a polyalphabetic substitution cipher with 25 nonrelated alphabets, and during the course of solution the phenomena of reciprocity and the Porta-like families would have been observed and used to advantage. The sequence reconstruction matrix might look as in Fig. 87, below, using any one of the alphabets arbitrarily as the starting point for "Alphabet 1" of the matrix; in this case, the sequence of alphabets of a message with the indicator "BABAX" has been used as a base. (All reciprocal values of recoveries have been filled in.)

[7] Uniselector switches are multipole-multilevel switches such as those used in automatic dialing telephone systems.

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

Figure 87.

It is noted that the 12 different equivalents for A_p in the order in which they occur in the matrix are as follows: P L I R Y T U M F X W D; the equivalents for B_p are X I P Y M W L Q U. These equivalents for B_p are among the equivalents for A_p, with the addition of Q, which is the last letter comprising one family of 13 letters. It will also be noted that each row of the matrix contains letters exclusively from the one or the other of the two families of 13;[8] thus with but only a few entries in the reconstruction matrix, it is possible to segregate the two families with ease. In this case it is therefore easy to identify the families as (A B C E G H J K N O S V Z) and (D F I L M P Q R T U W X Y). This matrix may be vizualized as a Porta-like matrix of 25 nonrelated alphabets, as illustrated in the fragmentary matrix below:

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

[8] Each row of the matrix will contain from 9 to 13 different letters belonging to one family, because of the manner in which the internally-wired matrix is constructed.

e. The rows of matrices for subsequent periods will be related to those of Fig. 87, in that there will be a simple substitution of the letters in a row (i.e., preserving the idiomorphic pattern and thus isomorphic to the original row), and a transposition or permutation of the rows of the basic matrix. For example, row "G" of Fig. 87, which begins with the letters M M F R F F... might be shifted to the "X" row of a new matrix, with the identity of the letters changed to L L D C D D... . The partially recovered plugging, i.e., the simple substitution alphabet (which applies to both the isomorphic substitution and to the permutation of the rows of the matrix) is then for this case as follows:

"α":	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
"β":				D		X						L						C								

The M M F R F F of "α" will go to L L D C D D of "β" at the same position (i.e., starting in the same alphabet), if the two matrices actually start with the same alphabet; if the indicator system has not changed, a pair of messages with identical indicators in two cryptoperiods means that the relative starting points for the sequence of alphabets are identical. If the relative starting points of two reconstruction matrices are not the same, then the M M F R F F of row "G" of "α" will still go to L L D C D D of row "X" of "β", but at a displacement equivalent to the relative displacement between the starting points of the two matrices.

f. In order to illustrate the mechanics of this system, let us assume that we have solved some traffic in a cryptoperiod subsequent to that identified by the matrix in Fig. 87. A portion of the reconstruction matrix for this "β" period (denoting the matrix in Fig. 87 as belonging to the "α" period) is shown below; the beginning point of the sequence of alphabets here too is that for a "BABAX" message.

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

It is apparent from the foregoing that the "A" and "C" rows are in the same family, and that the two families for the "β" period are (A C F H I K S T U V W Y Z) and (B D E G J L M N O P Q R X). Now we note the idiomorphic sequence of row "A", beginning with Q Q R - - - R; this is identified as the isomorphic equivalent of row "M" of "α", as follows:

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
(β)	A:	Q	Q	R			E	R	X	Q				G	J	O		O	Q	N		P		J		M
(α)	M:	G	G	N			J	N	B	G	N	Z		V	A	Z	O	Z	G	S	N	H		A	S	O

From this we recover the following plugging (substitution alphabet):

"β":	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
"α":					J		V			A				O	S	Z	H	G	N					B		

And since the "A" row of "β" goes to the "M" row of "α", we may add this equivalent pair to the recovered plugging.

g. Now we may take row "C", for example, of the "β" matrix and transform it into its exact equivalents in terms of matrix "α", as follows:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
(β) C:	R	L	R			O	D	O	B		J	E	N	R	L		N	B	E				E	E	
(α) ?:	N		N			Z		Z			A		S	N			S		J				J	J	

Row "C" of "β" may be identified as row "T" of Matrix "α", which results in the following additional values in both rows:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
(β) C:	R	L	R			O	D	O	B		J	E	N	R	L		N	B	E				E	E	O
(α) T:	N	K	N			Z	E	Z	C		A	J	S	N	K		S	C	J				J	J	Z

Transferring the equivalent pairs from the foregoing to our recovered plugging, including the pairs A(β) = M(α) and C(β) = T(α) derived from the permutation of the rows, we now have the following plugging reconstruction:

"β":	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
"α":	M	C	T	E	J		V			A		K	O	S	Z	H	G	N						B		

h. Enough of the basic theory has been demonstrated how the foregoing procedures could be continued with other rows of a partially recovered new matrix, permitting the easy reconstruction of the relative plugging between key periods. However, a partially recovered matrix of a new cryptoperiod is not a prerequisite for the reconstruction of the new plugging; a simple technique based upon a crib attack will now be demonstrated. This technique, involving an interesting application of symmetry in cross-equating between values of two different key periods, will be treated in the subparagraphs below.[9]

i. Let us assume we have available, in a new key period, the following message suspected of beginning with the opening stereotype "REFERENCE YOUR MESSAGE":

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

The indicator, BABAX, shows that the beginning of the sequence of alphabets starts at the same point in the cycle as the BABAX matrix in Fig. 87 for the earlier cryptoperiod. The recoverable letter-families are observed to be (A D E G O Q R U Y) and (C I J M P V Z), and also (F S) and (H N) which are as yet indeterminate as to which of the larger chains they belong. From this it is obvious that the next word of the crib is not "NUMBER", since the 22d letter, D_c, cannot represent U_p because D and U are in the same family.

[9] This method was first pointed out to me by Mr. William E. May.

j. The matched plain-cipher of the crib is set down:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
R	E	F	E	R	E	N	C	E	Y	O	U	R	M	E	S	S	A	G	E
P	C	N	J	J	Z	S	Q	I	Z	I	J	V	D	M	H	H	Z	J	I

In the 16th and 17th positions, $S_p = H_c$. A search is made in the matrix of Fig. 87 for a repeated letter in these positions in one of the rows, but none is found. (The matrix has been only partially reconstructed, so this correspondence is still hidden.) Since there is also the vertical pair E_p/I_c in positions 9 and 20 of the crib, a search is made in Fig. 87 for corresponding repetitions in the 9th and 20th positions in one of the rows; such a correspondence is found in the "D" and "Z" rows. This means that, in the plugging for the new matrix (β), what is now E_p in β used to be D_p (or Z_p) in α, and what is now I_c in β used to be Z_c (or D_c) in α. Since the plugging effects a simultaneous transformation of both the plain and cipher elements of the basic matrix, whatever correspondence exists in the plain between two matrices will also exist in the cipher of the two matrices. Thus we may make the following diagram, assuming one of the possibilities[10] above that $Z_p(\alpha) = E_p(\beta)$ and $D_c(\alpha) = I_c(\beta)$:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Plain (α):		Z		Z		Z			Z						Z					Z
Plain (β):	R	E	F	E	R	E	N	C	E	Y	O	U	R	M	E	S	S	A	G	E
Cipher (α):									D		D									D
Cipher (β):	P	C	N	J	J	Z	S	Q	I	Z	I	J	V	D	M	H	H	Z	J	I

Figure 88a.

Note that we have placed a Z over every E (either plain or cipher) and likewise a D over every I (either plain or cipher) of the diagram.

k. Now in position 2, Z_p (of the α period) is found to equal U_c in α, by referring to the matrix of Fig. 87; likewise, Z_p (α) in positions 4, 6, and 15 in Fig. 88a may be found, by referring to the corresponding columns in Fig. 87, to equal X_c, T_c, and M_c in α. These equivalencies are set down in Fig. 88b, below:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Plain (α):		Z		Z		Z			Z						Z					Z
Plain (β):	R	E	F	E	R	E	N	C	E	Y	O	U	R	M	E	S	S	A	G	E
Cipher (α):		U		X		T			D		D				M					D
Cipher (β):	P	C	N	J	J	Z	S	Q	I	Z	I	J	V	D	M	H	H	Z	J	I

Figure 88b.

[10] The selection of the possibility to be tried is arbitrary at this stage. If a wrong equivalence is chosen, conflicts will develop during the course of the analysis. (See subpar. 77n.)

By transferring values just derived (e.g., a U above C in the cipher may be transferred to other occurrences of U in either the cipher or the plain), we obtain the following diagram:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Plain (α):		Z		Z		Z		U	Z					M	Z					Z
Plain (β):	R	E	F	E	R	E	N	C	E	Y	O	U	R	M	E	S	S	A	G	E
Cipher (α):		U		X	X	T			D	T	D				M			T	X	D
Cipher (β):	P	C	N	J	J	Z	S	Q	I	Z	I	J	V	D	M	H	H	Z	J	I

Figure 88c.

We now look up the equivalents in Fig. 87 for X (in position 5), U (pos. 8), T(10), D(11), M(14), T(18), and X(19), and we record these new values in the diagram, yielding the following:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Plain (α):		Z		Z	E	Z		U	Z		S	O		M	Z					Z
Plain (β):	R	E	F	E	R	E	N	C	E	Y	O	U	R	M	E	S	S	A	G	E
Cipher (α):		U		X	X	T		N	D	T	D	X		A	M			T	X	D
Cipher (β):	P	C	N	J	J	Z	S	Q	I	Z	I	J	V	D	M	H	H	Z	J	I

Figure 88d.

Since we have $E_p(\alpha) = R_p(\beta)$ in position 5, an E may be inscribed over the R in columns 1 and 13, yielding new cipher values of Q and X in the corresponding positions in the "cipher α" row. The diagram is now as complete as we can make it for the moment with the crib alone; the following is the result obtained:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Plain (α):	E	Z		Z	E	Z		U	Z		S	O	E	M	Z					Z
Plain (β):	R	E	F	E	R	E	N	C	E	Y	O	U	R	M	E	S	S	A	G	E
Cipher (α):	Q	U		X	X	T		N	D	T	D	X	L	A	M			T	X	D
Cipher (β):	P	C	N	J	J	Z	S	Q	I	Z	I	J	V	D	M	H	H	Z	J	I

Figure 88e.

1. From the foregoing, it is evident that the plugging for the β period (taking α as the base) thus far recovered is the following substitution:

	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
α:				D					I	R			V	M	Q	U		P		O	Z	C			J	
β:	D				I	R						V	M	Q	U		P		O	Z	C			J		E

Three more values could have been picked up (in columns 10, 18, and 19) if the matrix in Fig. 87 had been complete; any further values must now come from the exploitation of the rest of the message.

m. The entire cipher text is written out on a width of 25, in the manner of the diagrams of Figs. 88a-e, and substituted values from the recovered plugging and from the basic matrix are made throughout the message where possible. Thus:

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

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

Figure 88f.

If now an S_p is assumed as the last letter of the message plain text, the diagram above may be expanded to the following, which will result in the recovery of four more equivalent pairs (F-F, G-N, K-H, W-S), in the plugging:

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

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

Figure 88g.

The solution would continue in this manner, with the exploitation of further plaintext assumptions or additional cipher text. Any further plaintext assumptions of letters or probable words in the context would of course be based on the 13 possible plaintext equivalents for any given cipher letter in this key period.

n. In subpar. j, we started the diagram of Fig. 88a with the assumption that $Z_p(\alpha) = E_p(\beta)$ and $D_c(\alpha) = I_c(\beta)$; this subsequently proved to be correct, there being no conflicts in the equivalent pairs developed. If, however, we had started with the other possibility, $D_p(\alpha) = E_p(\beta)$ and $Z_c(\alpha) = I_c(\beta)$, inconsistencies would have developed. For example, in the early stages of analysis of this possibility, the following diagram would have been obtained:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Plain (α):	W	D		D	W	D		E	D			D	W	C	D				M	D
Plain (β):	R	E	F	E	R	E	N	C	E	Y	O	U	R	M	E	S	S	A	G	E
Cipher (α):		E		S	S			X	Z		Z	S	O	I	C				S	Z
Cipher (β):	P	C	N	J	J	Z	S	Q	I	Z	I	J	V	D	M	H	H	Z	J	I

Note that the tentative plugging D-U in column 12 is inconsistent with the plugging D-E in other columns of the diagram.

o. The examples of theoretical solution thus far demonstrated have involved matrices with identical starting points in the cycle of 25 alphabets. If in the β period we had no message with the indicator BABAX (i.e., starting at the same relative point in the new matrix as the start of the matrix in Fig. 87), and we had a crib in a message having an unknown starting point, we would have to search for isomorphism across all the columns consecutively, instead of searching the rows of specific columns as we did in subpar. j. Consider the following:

R E F E R E N C E Y O U R M E S S A G E
J J N Z Z Z M L M W Z X C U M E A X P X

We note the isomorphism in positions 4 and 6, and also 9 and 15, and we search in the matrix in Fig. 87 for a row with identical letters spaced at a distance of 2, and also 6, as in the matched plain-cipher, above. The only one we find[11] which fits both intervals is in the Z row, in positions 6 and 8, and 11 and 17. Our diagram thus begins as follows:

	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Plain (α):				Z		Z			Z						Z					
Plain (β):	R	E	F	E	R	E	N	C	E	Y	O	U	R	M	E	S	S	A	G	E
Cipher (α):				T		T			M						M					
Cipher (β):	J	J	N	Z	Z	Z	M	L	M	W	Z	X	C	U	M	E	A	X	P	X

From here on the solution would proceed as previously demonstrated. Note that the two pairs of identical letters enable us to arrive at once at the correct initial assumption, instead of having two or more possibilities from which to make an arbitrary choice as was the case in subpar. j.

78. Solution involving isologs.--a. The possibilities for a successful attack on complex cryptosystems by the exploitation of isologs is predicated upon the mechanics of the cryptosystems, and, usually, also upon the presence of special circumstances connected with the isologs. Each case is usually a very special case, dependent upon the amount of cryptanalytic technical information that can be derived from a particular isolog situation.

[11] It is quite possible that if the matrix in Fig. 87 were completely reconstructed, we might have found one or two other rows (in other columns) with the properties we are seeking, in any case, the selections would be greatly restricted if we had two pairs of identical letters as in the case at hand.

b. It has been indicated in subpar. 62i how the procedures of an attack on isologs may be adapted to a case of isologs involving two different sets of unrelated, random alphabets. For example, even if the two messages in subpar. 62b were enciphered with 4 and 5 distinct unrelated alphabets respectively, the procedures given in subpars. 62e to g could be used for solution. Thus a partial recovery of some of the alphabets of a system such as that described in subpar. 75a would be made possible by this special solution.

c. In the case of the strip system described in par. 76, isologs are generally not of much help in solution; but since the general solution described in subpars. 76d and e is adequate for solving a single message, an isolog attack is only of academic importance. Nevertheless, a pair of very short isologs might still be solvable in this system, if either the plain or the cipher strips are in a fixed order, and this order is known.

d. Isologs in a system such as the ZEN-40 described in par. 77 are again of not much assistance in arriving at a solution, unless further special circumstances also exist. For instance, if we had in this system a pair of cross-period isologs (i.e., in two different pluggings) in which there were two sets of families, and if these families were known, an adaptation of the generatrix method is possible.[12] Let us suppose that in the following pair of isologs, the families of Message "A" are known to be (A B D E G H L U V W X Y Z) and (C F I J K M N O P Q R S T), and

Message "A"

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

Message "B"

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

the families of Message "B" are known to be (A C E G H I J K L M N O P) and (B D F Q R S T U V W X Y Z). Then by superimposing Message "A" and "B" and writing the common letters which can represent decipherments of the vertical pairs, we have the following diagram for the first 30 letters of the messages:

[12] This situation may of course also arise in modified Porta systems.

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

Figure 89.

It is easily seen that, by reading various levels of the generatrices, the cryptanalyst can decipher the first two words of the message as ENEMY PATROLS. The rest of the plain text can be obtained by following this procedure; the completion of the solution is left to the student as an exercise. Having the matched plain and cipher, recovery of the plugging follows along the lines indicated in subpars. 77i to o.

79. Additional remarks.--a. The attack on a system such as that illustrated in Fig. 80 is fairly simple because the plain component in this case is the normal sequence; if the plain component had been any other fixed sequence that were known, the tables of plain-cipher limitations in Figs. 82a and b and the table of theoretical ciphertext frequencies in Fig. 83 would have to be modified accordingly. Instead of the normal sequence, any one of the 25 numbered strips in Fig. 80 could have been used as the plain component; this would complicate the solution to the extent that the table of theoretical ciphertext frequencies would have to be compiled for 25 x 24 or 600 different distributions, against which the uniliteral frequency distributions for a new cryptogram in this system must be tested. If the plain component were an entirely unknown sequence, different from any of the 25 numbered strips, solution would be greatly complicated and would have to follow along the general lines indicated in subpar. 74b, since neither tables of plain-cipher limitations nor a table of theoretical ciphertext frequencies could be constructed. This demonstrates that, even in a cryptosystem employing random cipher alphabets, maximum security is attained when the plain component is also a random sequence.

b. If in a system such as that of Fig. 80, each of the cipher strips were slidable against the plain component so as to make possible the juxtaposition of any letter of the cipher component against A_p, then purely manual methods of attack would be too laborious for a practical solution; machine techniques could here be used to good advantage. However, there is still the possibility of getting too many acceptable "good answers", from which the cryptanalyst would have to determine the correct answer.

c. We have seen how easily the strip device treated in par. 76 succumbs to cryptanalytic attack because of the major weaknesses of this system. The same firm that marketed the transpositeur later produced a modified cipher device called the "Sphinx"; this latter device also had 10 compound strips, but the 20 half-strips were not limited to an upper or lower position as was the case of the transpositeur, thus the number of possible arrangements is 20! or 2.4×10^{18} instead of the 1.3×10^{13} in the case of the transpositeur. In the Sphinx device there is no consonant-to-consonant and vowel-to-vowel limitation as there is in the transpositeur, so it looks as if the Sphinx is a decided improvement over its predecessor; however, in order to make the system easy to use by a cipher clerk, some of the strips are direct standard, others are reversed standard sequences. Therefore for each of the 10 columns we will have Vigenère encipherment with either direct or reversed standard alphabets, depending upon the identity of the strips used in the particular positions --what an "improvement"!

d. The security of the transpositeur could have been enhanced considerably by the incorporation of 20 random half-strips, not limited to upper or lower position, and by not having fixed plaintext and ciphertext reading positions. This variable-generatrix idea is incorporated in the Jefferson principle exemplified by the now obsolete U.S. Army cipher device M-94,[13] and in strip systems related to this device. The solution of these latter systems will be treated in Military Cryptanalytics, Part III.

e. In the solution of the transpositeur, as well as in the ZEN-40, we have seen further instances of the general applicability of the generatrix method. It is quite surprising how many times solutions to cryptanalytic problems depend upon or are aided by the generatrix method, with or without minor modifications; the student would do well to keep this always in mind, and try to adapt this method wherever the opportunity presents itself.

f. The reason for emphasizing the large numbers in pars. 75 and 76 is to demonstrate forcibly that numbers of combinations, permutations, or keys by themselves often have no bearing upon the cryptanalytic complexity of solution of a system. If some would-be inventors of cryptographic systems would only stop and consider that the number of possible 26-letter simple substitution alphabets is 26! or 4.03×10^{26}, and that nevertheless simple substitution ciphers are solved quite readily, they should be more circumspect in bandying about their astronomical numbers too glibly.

g. In passing, it is worth mentioning that, no matter how complex a system is as regards the generation or use of a large number of alphabets, if we have a sufficient number of messages in depth (say 25-30, for English), we will be able to solve the plain texts of the messages, even if the cryptographic features of the system remain an enigma.

---

[13] See subpar. 6c, Appendix 6.

CHAPTER XI

POLYALPHABETIC BIPARTITE SYSTEMS

80. General.--a. All the systems thus far treated have been characterized by polyalphabetic encipherment of single plaintext letters. Instead of single plaintext letters, the "plain text" to be subjected to polyalphabetic encipherment might be multiliteral elements of a first substitution, such as the left- and right-hand components of a bipartite substitution. This "plain text" may be considered either as a secondary or intermediate plain text, or as a primary encipherment; hereinafter we will use the expression "intermediate plain text" to describe this situation.

b. Periodic bipartite systems may take one of the following three principal forms:

(1) In the simplest form, a succession of N unrelated bipartite matrices is used cyclically to encipher the successive letters of a plaintext message.

(2) A single bipartite matrix with a fixed internal composition is used, the coordinates of which are slid in a manner giving rise to polyalphabetic substitution. For instance, if the row coordinates of a 5x5 matrix consisted of the digits 1-5 and the column coordinates consisted of the digits 6-0, the successive letters of the plain text might be enciphered with a cyclical shift of either the row or the column coordinates, or both.

(3) A single bipartite matrix with fixed internal composition and fixed coordinates is used, with an additive superimposed on the primary encipherment to yield a polyalphabetic substitution. The addition of the key might involve either carrying addition, or noncarrying (i.e., mod 10) addition.

c. The following remarks are generalizations of the cryptanalytic attack on the foregoing systems:

(1) In the case under subpar. b(1), it is obvious that solution must be predicated on the recovery of the N different matrices involved.

If there is no latent relationship among the various matrices, exploitation of such a system cannot be aided by any method of equating or correlating cipher values belonging to different matrices.

(2) In the case under subpar. b(2), an entering wedge might be forced into the system under the supposition that the matrices were unrelated; but if the frequency distributions for the row and column coordinates are closely examined, the phenomena associated with the use of sliding coordinates would soon manifest themselves and give an indication as to the true nature of the system under study, and thus could simplify the problem greatly.

(3) The third case, that under subpar. b(3), is the more general case of polyalphabetic bipartite systems. The techniques of solution are sufficiently detailed and specialized to warrant thorough treatment; this will be done in the paragraphs that follow.

81. Analysis of a simple case: the "Nihilist" cipher.--a. The first system we shall treat is that known in cryptologic literature as the "Nihilist" cipher,[1] so named because it was first used by anti-Tsarist factions in Russia in the latter part of the 19th century; the basic idea is so simple that it has been "invented" many times since. This system embraces a dinome substitution followed by a cyclic numerical key as an additive. The dinome substitution is accomplished by means of a 5x5 bipartite square in which a normal alphabet (I=J) is inscribed, the coordinates of which are the digits 1 to 5 in normal order; the plain text undergoes a primary encipherment, and to this encipherment is added (by carrying addition) a cyclic numerical key obtained by the encipherment of a key word with the basic matrix. Thus we have a polyalphabetic dinome encipherment with a period equal to the length of the key word.

b. An example of encipherment is given to illustrate this system. The basic matrix is that shown in Fig. 90; let the key word be WHITE, from which is derived the numerical key 52 23 24 44 15, and let the message be as follows: RESISTANCE ENCOUNTERED NORTH OF VILLAGE.

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

Figure 90.

[1] This is one of the several types of cipher systems known by the same name, this appellation has also been given to a kind of false double transposition, as well as to simple bipartite encipherment with the matrix in Fig. 90, without further complexities. This last system is still encountered occasionally in prisons for "grapevine" communications of the inmates.

The plain text is written on a width of five (i.e., equal to the length of the key word), and the primary bipartite encipherment accomplished as shown in Fig. 91a. The dinomes of the key are added to the dinomes of the primary encipherment, as shown in Fig. 91b. Note the four values in the fifth column in Fig. 91b in which the carrying addition gives a different result from that of the customary cryptographic noncarrying (or mod 10) addition.

Key word:	W	H	I	T	E
P:	R	E	S	I	S
C_1:	42	15	43	24	43
	T	A	N	C	E
	44	11	33	13	15
	E	N	C	O	U
	15	33	13	34	45
	N	T	E	R	E
	33	44	15	42	15
	D	N	O	R	T
	14	33	34	42	44
	H	O	F	V	I
	23	34	21	51	24
	L	L	A	G	E
	31	31	11	22	15

Figure 91a.

	W	H	I	T	E
Additive:	52	23	24	44	15
	R	E	S	I	S
	42	15	43	24	43
C_2:	94	38	67	68	58
	T	A	N	C	E
	44	11	33	13	15
	96	34	57	57	30
	E	N	C	O	U
	15	33	13	34	45
	67	56	37	78	60
	N	T	E	R	E
	33	44	15	42	15
	85	67	39	86	30
	D	N	O	R	T
	14	33	34	42	44
	66	56	58	86	59
	H	O	F	V	I
	23	34	21	51	24
	75	57	45	95	39
	L	L	A	G	E
	31	31	11	22	15
	83	54	35	66	30

Figure 91b.

The final cipher text, if transmitted in dinome groupings, would be as follows:

94 38 67 68 58 96 34 57 57 30 67 56 37 78 60 85 67 39 86 30
66 56 58 86 59 75 57 45 95 39 83 54 35 66 30

Since the enciphering equation is P + K = C, the deciphering equation is P = C - K; thus in decipherment the key dinome must be subtracted (with borrowing subtraction) from the cipher text to yield the plaintext dinome.

c. It will be observed that the lowest possible cipher value is 22 (arising from $A_p + A_k$), and that the highest cipher value is 110 (arising from $Z_p + Z_k$). But in Nihilist encipherment the trinomes from 100 to 110 (excluding the impossible 101) are customarily treated as dinomes by dropping the first digit; no ambiguity is present because the lowest bona fide dinome is 22, thus an initial "0" or "1" at once indicates the special situation involved. The student should note that in the Nihilist system there are certain cipher dinomes which arise from a unique combination of plain + key; these are:

(1) $22 = A_p + A_k$ (= 11 + 11) only,

(2) $30 = E_p + E_k$ (= 15 + 15) only,

(3) $02 = V_p + V_k$ (= 51 + 51) only, and

(4) $10 = Z_p + Z_k$ (= 55 + 55) only.

The first two dinomes, 22 and 30, can occur quite frequently, but the other two have a much smaller probability of occurrence.[2] A further observation in the Nihilist system is that if the units digit of a cipher dinome is ϕ, it could have arisen only from a plaintext 5 enciphered by a key of 5; and if either the units or the tens digit of a cipher dinome is 2, it could have arisen only from a plaintext 1 enciphered by a key of 1. These points are very helpful in analysis, as will subsequently be seen.

d. The classic Nihilist system may be recognized by the virtual absence of the digit "1"; this digit cannot occur at all in the units position of dinomes, and in the tens position it can occur only in the very rare case where Z_p is enciphered by Z_k, resulting in the dinome 10. The usual principles of factoring apply of course to a Nihilist cipher; the period will be a factor of the interval between two occurrences of a long repetition, and the ϕ test may be used to confirm a tentative period. But in the Nihilist cipher, advantage may be taken of its cryptographic idiosyncracies to permit factoring a cryptogram much more quickly than would be possible with the usual procedures, and to enable factoring a much shorter message than would otherwise be possible with the usual procedures for the determination of the period. The specific location in a cryptogram of cipher dinomes 22, 30, 02, and 10 may furnish clues not only as to possible periods, but also as to impossible periods. For instance, if a pair of 22's is found 24 dinomes apart, the period may be taken to be one of the factors of 24 (unless of course there is more than one E in the key word); conversely, if a 22 is found at a distance of 45 dinomes from a 30, the period cannot possibly be 5 or 9, since a 22 is predicated upon a key of 11 and a 30 is contingent upon a key of 15, and thus there would be a clash of key values if the cipher were written out on a width of either 5 or 9.

e. Once a Nihilist cipher is recognized as such, the easiest line of attack is by capitalizing on the cryptographic weaknesses of the system. These points are enumerated below:

(1) The distance between two identical dinomes of the (22, 30, 02, 10) class will be a multiple of the period, unless there are repeated letters in the key word.

[2] Since the key in the Nihilist system is derived from plain text, the probability of a 30 occurring is the square of the probability of Ep in English, i.e., $(.1300)^2$ or 0169, the probability of a 22 is .0054, the probability of an 02 is .0002, and the probability of a 10 is only .000001.

(2) The interval between two different dinomes of the (22, 30, 02, 10) class cannot be a multiple of the period, since the keys involved must be different.

(3) The maximum difference between the units digits of dinomes enciphered by the same key is 4. Since the maximum plaintext difference is 4 (i.e., 5-1), the addition of a key digit from 1 to 5 will not alter this characteristic in the cipher text. For instance, in the key of C(13), $E_p(15)$ becomes 28, and $F_p(21)$ becomes 34; the difference between the cipher dinomes (treating the units and the tens positions separately) is 14, which is the same as the difference between plaintext 15 and 21.

(4) The maximum difference between the tens digits of dinomes enciphered by the same key is also 4, if allowance is made for situations wherein the units digit is a ∅, in which case, for example, a cipher dinome 40 must be treated as (3,10) for the tens and units positions, respectively. For instance, in the key of E(15), $E_p(15)$ becomes 30, and $F_p(21)$ becomes 36; cipher 30 must however be treated as (2,10) in the tens and units positions, so that the difference between (2,10) and 36 is 14, which is the same as the difference between plaintext 15 and 21.

(5) From items (3) and (4), it therefore follows that if the difference between two cipher dinomes is 5 or more in either the units or the tens position, the dinomes cannot possibly belong to the same cipher alphabet. It also follows that if a difference of 5 or more is found in either the units or the tens position, this rules out a Nihilist cipher with a single dinome as key, i.e., a monoalphabetically enciphered dinome system.

(6) In Fig. 92. below, is given a table of possible key digits derivable from the range of low-high cipher digits in the Nihilist system. As an illustration of its use, let us say that in a particular column of a factored Nihilist message the lowest tens (or units) digit is a 5, the highest a 9; from the table, it is seen that the only key digit possible is 4. If on the other hand the lowest tens (or units) digit were a 4, the highest a 7, it is seen that the key is not unique, but must be either a 2 or a 3.

Highest cipher digit

Lowest cipher digit	2	3	4	5	6	7	8	9	ø
2	1	1	1	1	1				
3		1,2	1,2	1,2	1,2	2			
4			1,2,3	1,2,3	1,2,3	2,3	3		
5				1,2 3,4	1,2 3,4	2,3,4	3,4	4	
6					1,2,3 4,5	2,3 4,5	3,4,5	4,5	5
7						2,3 4,5	3,4,5	4,5	5
8							3,4,5	4,5	5
9								4,5	5
ø									5

Figure 92.

(7) Once several key digits have been established, either uniquely or with variants, it is possible to recover the entire literal key by anagramming among the choices of key possibilities. Even if the numerical key is not derived from a Nihilist encipherment of a plaintext word, the unique key values established can be used to decipher the particular columns pertaining to this key, and a selection from among the other multiple keys can be made on the basis of weights of trial plaintext decipherments; the weights used may be either monographic or digraphic weights.

f. It is time to try out theory in practice. Let us assume the enemy has been using the Nihilist system with periods up to 20, and that we have at hand the following cryptogram:

57 59 55 49 66 66 84 26 74 48 98 59 25 48 26 30 48 77 55 45
76 57 99 30 56 30 27 48 67 86 86 34 65 45 78 39 45 46 28 39
55 67 86 32 55 75 70 59 66 49 27 26 76 67 54 22 56 39 97

The cipher text is scanned, and it is noted that a 30 is found as the 16th, 24th, and 26th dinomes, and that there is a 22 in the 56th dinome. From the first 30 to the 22 is an interval of 40; from the second 30 to the 22 is an interval of 32; and from the third 30 to the 22 is an interval of 30. From this we determine that the period of the cryptogram

cannot be any of the factors of 40, 32, or 30, so this rules out 2, 3, 4, 5, 8, 10, 15, 16, and 20 as possible periods. The intervals between the three 30's are 2, 8, and 10--but since these possible periods have been eliminated no encouragement is obtained from these intervals, fraught as they are with naught.

(1) Rather than write out the cipher text in various widths, we will try to reject trial periods on the basis of differences of 5 or more in the tens or units digits, using a shortcut procedure. Assuming first a period of 6, we examine the first and seventh dinomes, the 2d and 8th dinomes, etc., until we come to the 7th and 13th positions where the dinomes 84 and 25 have a difference of 6 in the tens digits, causing us to reject the hypothesis of a period of 6. A period of 7 is assumed, and this too is quickly rejected from the 2d and 9th positions where the dinomes 59 and 74 have a difference of 5 in the units digits. 9 is rejected as a period from the 7th and 16th positions, where the dinomes 84 and 30 have a difference of 5 in the tens digits, and a period of 11 is rejected from the 5th and 16th positions, where the dinome 66 could not have been homogeneous with 30, since we know 30 must come from a key of 15 (see subpar. c, above). When we try a period of 12, no inconsistencies develop, so we assume that this is the correct period.

(2) The cryptogram is written out on a width of 12, and the four columns containing the unique dinomes 30 and 22 are deciphered at once, as is shown in Fig. 93, below:

Key:	15		15				11				15	
57	59	55	49	66	66	84	26	74	48	98	59	
	44		34				15				44	
	T		O				E				T	
25	48	26	30	48	77	55	45	76	57	99	30	
	33		15				34				15	
	N		E				O				E	
56	30	27	48	67	86	86	34	65	45	78	39	
	15		33				23				24	
	E		N				H				I	
45	46	28	39	55	67	86	32	55	75	70	59	
	31		24				21				44	
	L		I				F				T	
66	49	27	26	76	67	54	22	56	39	97		
	34		11				11					
	O		A				A					

Figure 93.

The key for the tenth column can be determined uniquely, since the range of the low-high digits (3-7) in the tens position indicates a key of 2, and the range (5-9) in the units position indicates a key of 4. Furthermore, the presence of the digit 2 in the tens positions of the first and third columns fixes the key as 1 in these positions, and the presence of

the digit ϕ in the units position of the 11th column fixes the key in this position as 5. The keys for the rest of the positions are not unique; by referring to the table of Fig. 92, the keys (with multiple values included) are found to be as follows:

				2							
2				33	1		21				
3		3		23	44	32		32		4	
14	15	14	15	34	55	43	11	43	24	55	15

(3) Since there are only three key possibilities (12, 13, or 14) for the first column, we will make trial decipherments and score these decipherments with the deciban weights with which the student is now familiar (cf. subpars. 34c and f). This information is shown in the diagram below:

	Trial key of 12		Trial key of 13		Trial key of 14	
		Wgt.		Wgt.		Wgt.
	45		44		43	
	U	6	T	9	S	8
	13		12		11	
	C	7	B	4	A	8
	44		43		42	
	T	9	S	8	R	8
	33		32		31	
	N	8	M	6	L	7
	54		53		52	
	Y	6	X	3	W	5
Scores:		36		30		36

With such scanty data of only five letters available per column, the deciban scores are not immediately conclusive; apparently the keys of 12 and 14 are equally good, with the key of 13 a third choice. However, since the second column of Fig. 93 has been deciphered, a much more sensitive discrimination among the three key possibilities for the first column may be obtained by the use of digraphic weights. The three sets of digraphs formed by the three possible decipherments of column 1 taken with the decipherment of column 2 are shown in the diagram below, together with the centiban weights of the digraphs (cf. Table 15 on p. 285 of Military Cryptanalytics, Part I).

	Case I		Case II		Case III	
	UT	58	TT	67	ST	88
	CN	13	BN	00	AN	89
	TE	91	SE	84	RE	96
	NL	42	ML	00	LL	73
	YO	55	XO	13	WO	67
Scores:		259		164		413

It is clear from the high score of 413 that Case III has the best statistical probability[3] of being the correct case; thus the key for the first column is 14. This process could be continued with other columns where necessary, until sufficiently long plaintext polygraphs are deciphered to permit finishing the solution by contextual analysis. The message is found to begin with the words STRONG RESISTANCE, and the key is now derived uniquely.

(4) The foregoing approach is a general approach, independent of the constitution of the additive key. Where the latter has been derived from the bipartite encipherment with the Nihilist square of a plaintext word, another approach is via the anagramming of the key word from the multiple possibilities; this is especially easy when the data are sufficient to reduce the number of multiple values. In the case just studied the key recovered in subpar. 81f(2) is given below, together with the multiple key-letter values involved:

					2						
2					33	1		21			
3		3		23	44	32		32		4	
14	15	14	15	34	55	43	11	43	24	55	15
B	E	C	E	H	M	L	A	F	I	U	E
C		D		I	N	M		G		Z	
D				N	O	N		H			
				O	P	Q		L			
					R	R		M			
					S	S		N			
					T			Q			
					U			R			
					W			S			
					X						
					Y						
					Z						

A few moments' inspection of the beginning and ending portions establishes that the key word is DECENTRALIZE.

g. We have seen how simple it is to solve a Nihilist cipher if the square is known. If the square had the row and column coordinates in an unknown permutation of the digits 1-5, or if the internal composition of the square consisted of an unknown mixed sequence, solution is hardly more difficult, as will now be demonstrated.

[3] Case III is better than Case I by a factor of $224^{1\ 54} = 4163$, that is, the difference between 413 and 259, treated as an exponent of the base (224) of the logarithmic weights.

(1) Let us consider the following Nihilist cryptogram enciphered with a modified square:

87 53 74 67 49 48 66 55 66 87 42 65 57 58 76 45 66 75 75 74
67 75 58 48 44 62 86 75 35 65 64 36 46 56 56 66 87 36 96 68
58 48 46 85 59 97 55 85 68 78 87 36 62 87 97 54 96 84 47 48
44 56 66 87 52 06 65 38 49 66 55 67 98 55 96 68 66 55 46 84
67 07 45 96 85 68 67 44 84 65 86 54 07 86 56 87 24 62 67 99
53 95 87 50 77 56 74 59 68 73 96 68

There are no occurrences of the unique dinomes 22, 30, 02, or 55, nor are there any readily discernible long polygraphic repetitions; nevertheless factoring is very easy by the process of inspection outlined in subpar. f(1), above. All periods between 1 and 20 are eliminated except 9 and 18, so it is assumed that 9 is the correct period and the cryptogram is written out as is shown below:

1	2	3	4	5	6	7	8	9
87	53	74	67	49	48	66	55	66
87	42	65	57	58	76	45	66	75
75	74	67	75	58	48	44	62	86
75	35	65	64	36	46	56	56	66
87	36	96	68	58	48	46	85	59
97	55	85	68	78	87	36	62	87
97	54	96	84	47	48	44	56	66
87	52	06	65	38	49	66	55	67
98	55	96	68	66	55	46	84	67
07	45	96	85	68	67	44	84	65
86	54	07	86	56	87	24	62	67
99	53	95	87	50	77	56	74	59
68	73	96	68					

(2) Referring to the table of Fig. 92, it may be seen that the keys for the columns must be as follows:

cols.:	1	2	3	4	5	6	7	8	9
keys:	54	21	52	33	25	34	11	31	34
			53	43			12	41	44
							13		

Since the keys for cols. 1, 2, 5, and 6 are unique, these keys are subtracted from the corresponding cipher dinomes to yield a conversion to monoalphabetic terms. This conversion is shown below:

cols.:	1	2	3	4	5	6	7	8	9
keys:	54	21			25	34			
	33	32			24	14			
	33	21			33	42			
	21	53			33	14			
	21	14			11	12			
	33	15			33	14			
	43	34			53	53			
	43	33			22	14			
	33	31			13	15			
	44	34			41	21			
	53	24			43	33			
	32	33			31	53			
	45	32			25	43			
	14	52							

The distributions for these columns are given below:

col. 1:

11 12 13 $\overline{14}$ 15 $\overline{\overline{21}}$ 22 23 24 25 31 $\overline{32}$ $\overline{\overline{33}}$ 34 35 41 42 $\overline{43}$ $\overline{44}$ $\overline{45}$ 51 52 $\overline{53}$ 54 55

col. 2:

col. 5:

$\overline{11}$ 12 $\overline{13}$ $\overline{\overline{14}}$ 15 21 $\overline{22}$ 23 $\overline{24}$ $\overline{25}$ $\overline{31}$ 32 $\overline{\overline{33}}$ 34 35 $\overline{41}$ 42 $\overline{43}$ 44 45 51 52 $\overline{\overline{53}}$ 54 55

col. 6:

The ϕ counts for col. 1 (16) and col. 6 (14) are excellent, but those for col. 2 (6) and col. 5 (6) are very poor. Nevertheless, the χ test performed between the distributions for cols. 1 and 2, and between cols. 1 and 5, give excellent results, thereby indicating that they belong together. The combined distribution of cols. 1, 2, 5, and 6 is as follows:

N = 50

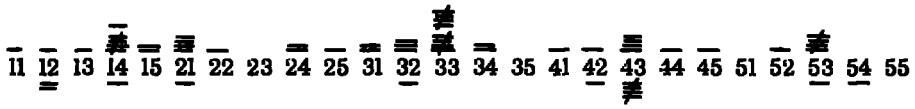
$\overline{11}$ $\overline{12}$ $\overline{13}$ $\overline{\overline{14}}$ $\overline{15}$ $\overline{\overline{21}}$ $\overline{22}$ 23 $\overline{24}$ $\overline{25}$ $\overline{31}$ $\overline{32}$ $\overline{\overline{33}}$ $\overline{34}$ 35 $\overline{41}$ $\overline{42}$ $\overline{\overline{43}}$ $\overline{44}$ $\overline{45}$ 51 $\overline{52}$ $\overline{\overline{53}}$ 54 55

The I.C. of this distribution[4] is $\frac{25\Sigma f(f-1)}{50 \times 49} = 1.82$, which is excellent.

(3) The key for col. 3 is either 52 or 53; what we will do now is make trial decipherments of col. 3 with both of these keys, and we will compare these decipherments with the combined distribution of cols. 1, 2, 5, and 6 to find the best match. This is shown below:

[4] In this case, we must remember that a 25-element alphabet is involved and modify the formula for the I.C. accordingly.

col 3:
(k=52)



col. 3:
(k=53)

The key of 52 gives a χ value of 24, and the key of 53 gives a χ value of 41; this shows that the key for col. 3 should be 53.

(4) The entire tabulation of trial keys for the five nonunique columns are given below, together with the χ values as compared with the combined distribution of cols. 1, 2, 5, and 6.

Col.	Key	11	12	13	14	15	21	22	23	24	25	31	32	33	34	35	41	42	43	44	45	51	52	53	54	55	χ
		1	1	1	6	2	4	1		2	1	2	3	10	2		1	1	4	1	1		1	5			
3	52			2		1		1						1					1	5					1	1	24
	53	2			1		1						1					1	5					1	1		41
4	33									1		1			1	5		1				1	1	1	1		13
	43				1		1			1	5		1				1	1	1	1							27
7	11			1							1			3	1	2					2					2	36
	12		1							1			3	1	2					2				2		28
	13	1							1			3	1	2					2					2			48
8	31									2	2	3				1			1					2	1		26
	41				2	2	3				1			1					2	1							48
9	34										2	1	3	3		1							1	1			50
	44					2	1	3	3			1						1	1								18

From the foregoing, it is evident that the keys for the nine columns are as follows:

1	2	3	4	5	6	7	8	9
54	21	53	43	25	34	13	41	34

(5) All nine columns of the cryptogram may now be converted into monoalphabetic terms, as follows:

33 32 21 24 24 14 53 14 32
33 21 12 14 33 42 32 25 41
21 53 14 32 33 14 31 21 52
21 14 12 21 11 12 43 15 32
33 15 43 25 33 14 33 44 25
43 34 32 25 53 53 23 21 53
43 33 43 41 22 14 31 15 32
33 31 53 25 13 15 53 14 33
44 34 43 25 41 21 33 43 33
53 24 43 42 43 33 31 43 31
32 33 54 43 31 53 11 21 33
45 32 42 44 25 43 43 33 25
14 52 43 25

The simple dinome substitution is readily solvable, and the plain text is found to begin with the words NO ADDITIONAL. The square as recovered is shown in Fig. 94a; upon observing the phenomena characteristic of a

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

Figure 94a.

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

Figure 94b.

keyword-mixed sequence inside the square, the rows and columns of the reconstruction square are permuted to yield the original enciphering square as shown in Fig. 94b. The additive key, when deciphered through the reconstructed square, is found to be based on WATER PUMP.

82. Analysis of a more complicated example.--a. In the next case to be considered, it will be assumed that the enemy is known to be using various types of dinome matrices in conjunction with an additive superencipherment, the arithmetic being performed mod 10. The following message has been intercepted:

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

The polygraphic repetition present at an interval of 125 dinomes suggests that the basic period is five dinomes (i.e., a 10-digit additive sequence). Since the message above is already written on a width of 20 dinomes, it will be convenient to make a distribution of the 10 columns, as follows:

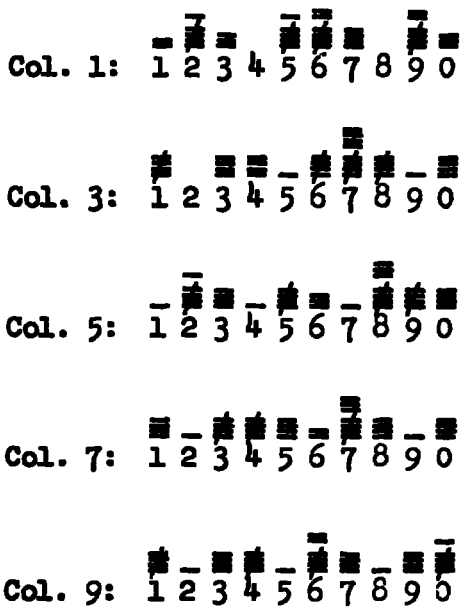


Figure 95a. Figure 95b.

b. It will be observed that the foregoing distributions may be classed into two families, one comprising the odd columns and the other comprising the even columns;[5] the reason for this is that the frequencies of the row coordinates of the underlying matrix have a distinct pattern of peaks and troughs, and likewise the frequencies of the column coordinates have a distinct pattern, different from that of the row coordinates. The addition, mod 10, of a key digit merely displaces the entire pattern of peaks and troughs, just as in a standard alphabet cipher a change of key letter displaces the distribution by the value of the key letter (mod 26).[6] Therefore

[5] Note that this is further proof that the underlying text is in dinomes. If the intermediate plain text had consisted of trinomes, or monomes and dinomes, the columnar distributions would not have fallen into two families, instead there would have been only one family discernible, and solution would progress by matching all the distributions together, without regard to their parity. See in this connection subpar 86g.

[6] Mod 10 addition is really a digital version of a Vigenère table with standard alphabets, as will be seen from the following diagram:

Plaintext digit

Key digit	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Cipher

the distributions within each of the families may be slid to find the best match, and we have the following:

Figure 96a. Figure 96b.

c. The relative displacements of the odd columns, in terms of col. 1, are 0, 1, 3, 8, and 4; the relative displacements of the even columns, in terms of col. 2, are 0, 4, 5, 7, and 3. Therefore if we arbitrarily treat the additive for the first dinome as 00, the second dinome has a relative key of 14, the third dinome a relative key of 35, the fourth a key of 87, and the fifth a key of 43.[7] The key digits are subtracted from the cipher, to yield a reduction in terms of the first of the five dinome columns. This is illustrated in the work sheet below:

[7] This relative additive differs from the true additive by a dinome constant.

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

Figure 97.

d. A dinome distribution is now taken on the pseudo-plain text; this is as follows:

	1	2	3	4	5	6	7	8	9	ø	
1		1	1	2	3						7
2	4		3	4	2	3	6	3	1		26
3	3		6	1	2	4		1		1	18
4		1	1	1						1	4
5	7	4	6		1	4	2	2		2	28
6	3		6	6	2	5	6	2	2		32
7	4	1	9	2	2	2		2			22
8		3	1	1							5
9	7	1	1	1	5	4	2	4	2	2	29
ø	2	1	11		1	3		1			19
	30	12	45	18	18	25	16	15	5	6	

Figure 98.

Matching propensities are detected among the rows of the matrix, but not among the columns; this points to the possibility of a variant matrix of 10 columns and perhaps three rows. This assumption is strengthened by the local variation among the distributions for the even columns in Fig. 95b (these variations being a direct function of the plain text being enciphered), and by the pronounced similarity of the distributions for the odd digits in Fig. 95a (the similarity of these distributions being caused by a "check-off" procedure in the variant usage).

e. We note in Fig. 98 that rows 1, 4, and 8 are homogeneous and that therefore they belong to one family. Row 6, with 32 tallies, is the row with the heaviest distribution; therefore we shall begin by taking the cross-products sum of row 6 with the remaining six rows that come into consideration (excluding the 1-4-8 family)[8]. This is shown in the diagram below:

	1	2	3	4	5	6	7	8	9	ø	
$\chi(6,2)$:	12	-	18	24	4	15	36	6	2	-	= 117
$\chi(6,3)$:	9	-	36	6	4	20	-	2	-	-	= 77
$\chi(6,5)$:	21	-	36	-	2	20	12	4	-	-	= 95
$\chi(6,7)$:	12	-	54	12	4	10	-	4	-	-	= 96
$\chi(6,9)$:	21	-	6	6	10	20	12	8	4	-	= 87
$\chi(6,0)$:	6	-	66	-	2	15	-	2	-	-	= 91

It is clear that there is an outstandingly good match between row 6 and row 2, so these rows belong to the same family. The other χ values are less clear, except for the outstandingly low value of the match 6-3, which indicates that 3 is in a different family.

f. We now compare row 3 with the remaining four rows, and we get the following:

	1	2	3	4	5	6	7	8	9	ø	
$\chi(3,5)$:	21	-	36	-	2	16	-	2	-	2	= 79
$\chi(3,7)$:	12	-	54	2	4	8	-	2	-	-	= 82
$\chi(3,9)$:	21	-	6	1	10	16	-	4	-	2	= 60
$\chi(3,0)$:	6	-	66	-	2	12	-	1	-	-	= 87

From this we see that row 3 and row ø undoubtedly belong together, and that in all probability row 9 (the lowest χ value) does not belong with 3 and ø; this would imply that row 9 belongs with rows 2 and 6, since the family of 1-4-8 is distinctive enough to permit no other additions, However, we shall leave this decision to one more test.

g. The only rows left to place are the 5, 7, and 9 rows. In order to facilitate the matching of these rows with the rows of the 2-6 and the 3-0 families, we will first amalgamate the members of the families as we

[8] See also pp. 112-113 of Military Cryptanalytics, Part I, in connection with the use of the cross-products sum in the analysis of a variant system.

have them so far so that we may have more typical distributions for these families; this amalgamation is as follows:

	1	2	3	4	5	6	7	8	9	ø
α = (1+4+8):	-	5	3	4	3	-	-	-	-	1
β = (2+6):	7	-	9	10	4	8	12	5	3	-
γ = (3+0):	5	1	17	1	3	7	-	2	-	1

We will now take the cross-products sum between the β row and rows 5, 7, and 9; and likewise between the γ row and rows 5, 7, and 9. This yields the following:

	1	2	3	4	5	6	7	8	9	ø	
$\chi(\beta,5)$:	49	-	54	-	4	32	24	10	-	-	= 173
$\chi(\beta,7)$:	28	-	81	20	8	16	-	10	-	-	= 163
$\chi(\beta,9)$:	49	-	9	10	20	32	24	20	6	-	= 170
$\chi(\gamma,5)$:	35	4	102	-	3	28	-	4	-	2	= 178
$\chi(\gamma,7)$:	20	1	153	2	6	14	-	4	-	-	= 200
$\chi(\gamma,9)$:	35	1	17	1	15	28	-	8	-	2	= 107

It is apparent that row 7 belongs to the γ family, since $\chi(\gamma,7)$ has the high value of 200 whereas the $\chi(\beta,7)$ has the much lower score of 163. Furthermore, the lowest score of 107 for $\chi(\gamma,9)$ when compared with the value of 170 for $\chi(\beta,9)$ confirms that row 9 belongs with the β family rather than with the γ family. The family relationship of row 5 is still indeterminate statistically, because the methods we are using do not have sufficient discriminatory power for us to be able to place row 5 with any confidence. Our consolidated frequency distribution (less the tallies of row 5) now looks as follows:

	1	2	3	4	5	6	7	8	9	ø
148	-	5	3	4	3	-	-	-	-	1
269	14	1	10	11	9	12	14	9	5	2
370	9	2	26	3	5	9	-	4	-	1

h. We will now convert the intermediate text of Fig. 97 to true monoalphabetic terms using the consolidated frequency matrix just obtained, calling the three rows "1", "2", and "3". The dinomes beginning with the digit 5 we will leave unchanged, since we do not know the relationship of this row. This conversion is shown in Fig. 99, below.

91 53 67 03 31 71 91 35 03 93 99 73 55 33 06 64 25 67 96 21
21 27 33 31 31 21 35 33 23 29 33 33 36 24 25 27 26 21

53 74 91 69 28 67 03 27 50 58 57 03 53 73 52 15 61 96 25 28
34 21 29 28 27 33 27 33 33 15 21 26 25 28

76 21 14 71 15 72 82 51 71 04 21 63 75 12 36 50 51 96 95 73
36 21 14 31 15 32 12 31 34 21 23 35 12 36 26 25 33

56 33 95 84 73 26 56 24 42 67 90 43 73 66 27 24 38 75 95 33
33 25 14 33 26 24 12 27 20 13 33 26 27 24 38 35 25 33

73 23 40 91 01 31 03 66 27 64 06 66 82 36 76 31 51 03 56 98
33 23 10 21 31 31 33 26 27 24 36 26 12 36 36 31 33 28

63 74 65 33 51 63 78 94 95 29 03 52 03 63 67 56 61 52 06 33
23 34 25 33 23 38 24 25 29 33 33 23 27 21 36 33

95 98 27 61 44 03 91 78 83 73 28 65 33 27 64 92 68 51 53 67
25 28 27 21 14 33 21 38 13 33 28 25 33 27 24 22 28 27

98 21 23 36 24 26 91 27 91 24 63 66 13 90 73 23 03 53 73 52
28 21 23 36 24 26 21 27 21 24 23 26 13 20 33 23 33 33

15 68 97 57 98 99 30 02 03 05 51 63 66 26 97 64 36 34 64 82
15 28 27 28 29 30 32 33 35 23 26 26 27 24 36 34 24 12

35 71 58 96 69 64 01 51 53 08
35 31 26 29 24 31 38

Figure 99.

The dinome of outstanding frequency, 31, may be assumed to be E_p; this, coupled with the idiomorphic pattern of the message beginning, establishes that the first word is INTELLIGENCE and places the "5" row in the 2-6-8 family. The text is easily solved, and a reconstruction matrix obtained as shown in Fig. 100a, which may be permuted into the matrix shown in Fig. 100b.

	1	2	3	4	5	6	7	8	9	Ø
148		U	W	V	Y					
2569	I	M	N	O	R	S	T	A	C	H
370	L	B	E	D	G	P		F		K

Figure 100a.

	2	4	3	8	5	9	0	1	6	7
2569	M	O	N	A	R	C	H	I	S	T
370	B	D	E	F	G	J	K	L	P	Q
148	U	V	W	X	Y	Z				

Figure 100b.

i. A closer examination of the sequence of digits comprising the column coordinates reveals that, if we subtract 7 (mod 10) from each of these digits, we will have a numerical key based upon the key word MONARCHIST--in other words, we are able to reduce the even digits of the dinome additives to their primary instead of relative equivalents. It will also be discovered that if 5 is subtracted from the digits comprising the row coordinates, we will get an assembly of digits that can be put into a logical numerical order which undoubtedly is the original set of row coordinates; or, if the lateral differences (called in cryptologic language the "deltas") between the dinomes of the relative additive key 00 14 35 87 43 are examined, the delta sequence 14 21 52 66 is the same as the dinome delta sequence of the numerical key based on MONARCHIST. This now proves the original primary enciphering matrix, as well as the original primary additive key. The true additive key is 57 61 82 34 90, and the original matrix is that shown in Fig. 100c, below.

	5	7	6	1	8	2	3	4	9	0
0741	M	O	N	A	R	C	H	I	S	T
852	B	D	E	F	G	J	K	L	P	Q
963	U	V	W	X	Y	Z				

Figure 100c.

j. We have shown (in subpars. b and c) with this problem only one method of equating columns of additive-enciphered dinome text. In the next paragraph there will be shown several other methods applicable for reducing polyalphabetically enciphered dinome text to simple (i.e., monoalphabetic) terms, without regard to the mechanics used to produce the dinome intermediate text.

83. Analysis of syllabary square systems with superencipherment.--a. A logical extension of the idea of bipartite systems with encipherment is a system wherein the original plain text is first enciphered with a syllabary square or a code chart, followed by a superimposed additive upon the primary encipherment. In the problem next to be considered, we will assume that the enemy is using the syllabary square illustrated in Fig. 101, below, in conjunction with a cyclic additive. For this first situa-

	1	2	3	4	5	6	7	8	9	ø
1	A	1	AL	AN	AND	AR	ARE	AS	AT	ATE
2	ATI	B	2	BE	C	3	CA	CE	CO	COM
3	D	4	DA	DE	E	5	EA	ED	EN	ENT
4	ER	ERE	ERS	ES	EST	F	6	G	7	H
5	8	HAS	HE	I	9	IN	ING	ION	IS	IT
6	IVE	J	ø	K	L	LA	LE	M	ME	N
7	ND	NE	NT	O	OF	ON	OR	OU	P	Q
8	R	RA	RE	RED	RES	RI	RO	S	SE	SH
9	ST	STO	T	TE	TED	TER	TH	THE	THI	THR
ø	TI	TO	U	V	VE	W	WE	X	Y	Z

Figure 101.

tion we will assume that the coordinates are known sequences, and that they are the digits 1-ø in normal order.

b. The following cryptogram is available for study:

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

The longer polygraphic repetitions present have a common factor of 8; but there are several shorter repetitions which factor to 4, so it will be assumed that the additive is 4 dinomes. (If we wished to play it safe, we could have made distributions on the basis of 8 columns; this would have disclosed good matching between the distributions for the 1st and 5th columns, etc., revealing that the period is actually four dinomes.)

c. Dinome distributions are made for the four dinome columns, as follows:

I

	1	2	3	4	5	6	7	8	9	ø	
1		1			1			2			4
2	1	2		1				3			7
3	2		1						1		4
4	3		2			2	5		3	1	16
5	2	1						5		1	9
6	2	6				3	4	1		1	17
7	5	3		6	1	4				1	20
8					2	2		1		1	6
9	1				1	4	1	2	1		10
ø		1		3					1		5
	16	14	3	10	5	15	10	14	6	5	

Figure 102a.

II

	1	2	3	4	5	6	7	8	9	ø	
1		5		1	1			1		1	9
2		3		1		2		4		1	11
3	1	3	2	2		1		1	6		16
4	1		6				1	2	1	2	13
5		3			4		2				9
6	2		1		1	3	3				10
7			2		2	1	2	2		2	11
8	1	1	1		2						5
9						1			3		4
ø	1		1		3			1	3	1	10
	6	15	13	4	13	8	8	11	13	7	

Figure 102b.

III

	1	2	3	4	5	6	7	8	9	ø	
1		6		5		1					12
2		1	5		2	2		2			12
3	3	3		1		1	7				15
4	4					2	2		3		11
5	2				1	1		1	1	1	7
6	3	2		4							9
7		1		2		1	3				7
8		2				1	1			2	6
9		1	5		2		1				9
ø				4		1		2	2	1	10
	12	16	10	16	5	10	14	5	6	4	

Figure 102c.

IV

	1	2	3	4	5	6	7	8	9	ø	
1	1		1	1	2				1		6
2	2			2	1	1	1	1	1		9
3	3		3					3			9
4	1			1		1	3				6
5	1		4		1	1	2				9
6		2						2		5	9
7		1		1		3		2		1	8
8	2	4					4		2	1	13
9	2		1	1		4	2	1	2	3	16
ø	1		4	1	1			1		5	13
	13	7	13	7	5	10	12	10	6	15	

Figure 102d.

We will now attempt to equate the first digits (1 and 3) of the dinome columns I and II, and also the second digits (2 and 4) of cols. I and II. This is shown in Figs. 103a and b, below:

$\chi(1,3)$

4	7	4	16	9	17	20	6	10	5	
9	11	16	13	9	10	11	5	4	10	= 976
11	16	13	9	10	11	5	4	10	9	= 898
16	13	9	10	11	5	4	10	9	11	= 820
13	9	10	11	5	4	10	9	11	16	= 888
9	10	11	5	4	10	9	11	16	13	= 907
10	11	5	4	10	9	11	16	13	9	= 935
11	5	4	10	9	11	16	13	9	10	= 1061
5	4	10	9	11	16	13	9	10	11	= 1072
4	10	9	11	16	13	9	10	11	5	= 1038
10	9	11	16	13	9	10	11	5	4	= 1009

Figure 103a.

$\chi(2,4)$

16	14	3	10	5	15	10	14	6	5	
6	15	13	4	13	8	8	11	13	7	= 917
15	13	4	13	8	8	11	13	7	6	= 1088
13	4	13	8	8	11	13	7	6	15	= 927
4	13	8	8	11	13	7	6	15	13	= 909
13	8	8	11	13	7	6	15	13	4	= 932
8	8	11	13	7	6	15	13	4	13	= 949
8	11	13	7	6	15	13	4	13	8	= 950
11	13	7	6	15	13	4	13	8	8	= 1019
13	7	6	15	13	4	13	8	8	11	= 944
7	6	15	13	4	13	8	8	11	13	= 909

Figure 103b.

In Fig. 103a, the matching of the row digits gives three outstanding χ values, but these values are too close together to permit an easy choice among them. On the other hand, the matching of the column digits produces one outstanding very high χ value, 1088, which indicates that the column digits of II have a relative displacement of +1 in relation to the column digits of I. In order to be able to discriminate among the three likely choices for the matching of the row coordinates of I and II, we will perform the χ test on dinome distributions; this test with dinomes is much more powerful than matching on the basis of single-digit distributions, not only because the latent primary encipherment has strong dinome characteristics, but also because of the cohesion of plain language, i.e., given a particular plaintext letter, the occurrence of the next letter is not based upon a random choice from a /biased/ population of plaintext frequencies but is governed by the cohesion or affinity of letters forming plaintext digraphs.

d. Since the relationship of the column coordinates of II in reference to I has been determined, and since the three highest χ values for the row coordinates of II indicate slides of 7, 6, and 8 with respect to I, we will rewrite the dinome distribution for II in three ways to permit an easier (and less subject to error!) matching of the dinome distributions of I and II. The three transformations of the distribution for II are shown below:

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

Figure 104a.

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

Figure 104b.

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

Figure 104c.

The cross-products sum of the dinome distributions is taken by multiplying the entries in each cell of I with the corresponding cell of II, and then adding up all the cross-products thus derived. (For example, cell 1-1 of I is compared with cell 8-2 of II; cell 1-2 of I is compared with cell 8-3 of II; etc.) The χ test of the dinome distribution of I against the dinome distributions of Figs. 104a, b, and c yields χ values of 123, 91, and 236, respectively; thus it is indicated that row 9 of II is equated to row 1 of I, or a slide of +7. This now means that if col. I is arbitrarily considered to have the additive 00, this fixes the relative additive for col. II as 81. The merged distribution for dinome columns I and II properly equated is now as follows:

	1	2	3	4	5	6	7	8	9	ø	
1		1			2			5			8
2	1	3		4			1	6	1	1	17
3	7		2	1			1		2		13
4	6		3		2	2	9		4	1	27
5	5	3	2		1		1	11		2	25
6	2	12				4	6	2	2	2	30
7	8	3		10	1	6				1	29
8		1		1	5	5		1		3	16
9	1	2		2	2	6	3	2	3		21
ø	1	2		5					1	1	10
	31	27	7	23	13	23	21	27	13	11	

Figure 105.

e. The process of equating dinome columns III and IV with the merged distribution for I and II continues as before, relying on the single-digit distributions for obtaining the best two or three choices or so, and then determining the correct choice by the χ-test analysis of the dinome distributions as was performed in subpar. d, above. By this process the relative additive for the four dinome columns is derived as 00 81 75 39. These key digits are now subtracted from the cipher text of the cryptogram given in subpar. b, reducing the complex text to monoalphabetic terms; the first line of the conversion is therefore as follows:

Additive:	00	81	75	39	00	81	75	39	00	81	75	39	00	81	75	39	00	81	75	39
Cipher text:	72	99	32	93	76	12	12	81	66	34	32	28	49	43	32	00	43	22	28	99
"Plain text":	72	18	67	64	76	31	47	52	66	53	67	99	49	62	67	71	43	41	53	60

The conversion of the entire text to monoalphabetic terms is given in Fig. 106, below:

72	18	67	64	76	31	47	52	66	53	67	99	49	62	67	71	43	41	53	60
80	20	84	68	31	76	22	97	47	58	50	85	62	82	74	24	76	31	47	52
66	49	62	67	71	43	41	71	61	80	20	84	68	31	76	22	97	57	58	50
85	62	39	61	74	80	76	31	47	52	66	04	24	97	07	18	40	95	76	49
39	60	11	82	74	24	76	31	47	52	66	49	62	76	62	09	02	41	39	60
67	62	34	02	41	84	20	51	70	58	50	74	85	62	02	86	04	18	57	69
22	28	51	92	62	67	71	43	41	71	49	31	76	22	97	47	58	50	72	18
95	74	99	47	58	58	17	31	49	99	47	80	46	04	97	92	09	94	58	50
74	92	15	09	75	31	28	95	31	28	81	74	99	47	80	04	47	74	15	67
51	15	09	24	52	66	85	62	62	45	28	15	04	57	34	31	67	37	49	95
28	39	39	28	18	86	02	33	67	99	33	61	74	62	58	96	71	86	99	67
72	51	47	12	58	69	62	45	28	18	33	09	58	47	28	02	33	67	99	33
61	74	62	58	96	71	83	28	28	85	62	04	51	51	96	53	43	41	86	75
49	71	99	47	58	58	09	79	98	01	71	18	46	24	96	58	21	02	31	76
22	97	47	58	50	55	96	53	18	94	69	24	96	74	49	65	91	86	86	90
66	92	39	61	74	33	61	74	71	85	62	39	96	58	58	27	86	04	47	58
71	68	01	71	04	96	58	86	62	45	28	68	67	62	34	02	41	00	12	98
76	24	49	67	62	34	02	41	60	27	74	53	96	51	17	74	72	28	53	26
88	69	28	72	98	53	72	62	86	28	51	17	74	85	62	71	47	31	65	24
15	96	74	53	71	47	27	71	12	58	49	39								

Figure 106.

All we need now is a single dinome as a corrective to convert the entire cipher text from our arbitrary base to the true base which would enable the reading of the message directly with the syllabary square shown in Fig. 101. As an easy solution, if the cryptogram in Fig. 106 ends with a signature, it is possible that the last element is an F_p (from INF); or the sequence 58 58 in the 4-dinome repetition of the 8th line of Fig. 106 may be tried as a doubled S_p, P_p, or L_p. The corrective for the additive is thus found to be 93, making the true additive sequence 93 74 68 22 which will decipher the beginning of the message as SECOND REGIMENT... .

f. Note that there are three sets of 5-dinome repetitions present in the cryptogram given in subpar. b. It is quite possible that two of these sets might represent identical plain text; if this is so, it will make possible a very easy method of equating the columns without recourse to analysis of distributions. For instance, let us suppose that the repeated sequences (76 12 12 81 66) and (41 60 47 33 31) actually are identical in their underlying plain text, and that the cryptogram has been factored to a period of 4. The sequences are aligned under their respective dinome columns thus:

I	II	III	IV
(76	12	12	81
66)	(41	60	
47	33	31)	

Then if the additive for col. I is taken as 00, it is clear that, if 41_c(III) is to represent 76, the additive for col. III must be 75; this shows the method how a relative additive can quickly be recovered by exploiting isologous ciphertext sequences. (The validity of the additive is confirmed if latent repetitions are now uncovered in other parts of the cipher text.) The student should keep this method in mind for possible use in the analysis of other types of systems which might lend themselves to this attack.

g. It should be clear to the student that the column-equating methods treated in the foregoing subparagraphs do not depend upon any known factors concerning the composition of the matrix or of the coordinates. One more generally applicable method of equating will now be demonstrated; and, in order to illustrate a different case, we will assume that the matrix is still that of Fig. 101, except that the coordinates are unknown mixed sequences. The following message, factoring[9] to a period of 6, will be studied:

[9] See in this connection subpar. 84d.

41 30 07 04 63 53 61 21 53 79 39 04 74 34 51 93 60 29 60 25 89 68 74 34
83 51 94 19 17 84 66 04 04 53 24 20 42 92 20 23 92 55 11 26 36 92 13 69
13 05 99 56 98 09 42 10 40 99 48 82 95 20 72 75 24 12 42 92 20 23 92 90
04 66 60 80 16 71 42 48 72 78 03 17 44 13 35 45 17 87 12 48 04 04 91 95
71 42 72 78 97 37 84 80 26 56 86 89 44 26 51 28 24 11 11 80 85 36 08 83
19 10 91 25 31 37 17 52 23 95 23 55 83 51 94 19 17 84 66 50 11 17 24 11
11 34 45 06 40 69 37 16 36 83 48 55 89

Figure 107.

This message is too short to permit analysis of the frequency distributions with confidence; and there are no sets of equal-length repetitions to allow us to equate columns by the method indicated in subpar. f, above. Nevertheless, the dinome columns may be equated if we can discover some latent repetitions in the cipher text which could then be exploited in a manner similar to that shown in subpar. f. These latent repetitions may be made patent by means of a differencing technique now to be described.

h. Let us examine the following isologous encipherments produced with the square of Fig. 101 and the additive 74 31 89 60 25 12:

74	31	89	60	25	12
D	I	V	IS	ION	HE
31	54	04	59	58	53
05	85	83	19	73	65
A	D	Q	U	AR	TER
11	31	70	03	16	96
85	62	59	63	31	08
S					
88					
52					

Figure 108a.

74	31	89	60	25	12
		D	I	V	IS
		31	54	04	59
		10	14	29	61
ION	HE	A	D	Q	U
58	53	11	31	70	03
22	84	90	91	95	15
AR	TER	S			
16	96	88			
80	27	67			

Figure 108b.

Referring to Fig. 108a, if we subtract (mod 10) each cipher dinome from the cipher dinome just below it (i.e., in the corresponding position of the next cycle of the period), we will derive the "delta" or difference stream 80 87 76 54 68 43 77; if we difference the plaintext dinomes the same way, we will get the identical delta stream. The reason for this is that the difference between two plaintext elements, $\alpha - \beta$, is unchanged if the same constant "k" is added to each of the elements; or, expressed algebraically, $(\alpha + k) - (\beta + k) = (\alpha - \beta)$. In other words, the difference between the cipher elements

at an interval corresponding to the period represents the difference between the underlying plaintext elements, thus removing the effect of the additive. Once therefore having established the period in a numerical system with additive superencipherment, if we derive a delta stream at an interval corresponding to the period, any latent polygraphic repetitions will be uncovered in this process. The delta streams obtained from Figs. 108a and b are shown below:

I	II	III	IV	V	VI
80	87	76	54	68	43
77					

Figure 108c.

I	II	III	IV	V	VI
		80	87	76	54
68	43	77			

Figure 108d.

The repetitions in the delta stream are of such length that they must be interpreted as having arisen causally, just as long ciphertext repetitions in a relatively small sample of text have to be attributed to the effect of identical keys applied to identical plain text, producing identical cipher text. The method of exploitation of the delta repetitions from this point on will be discussed in subpar. j, below.

i. The isologous passages in Figs. 108a and b were enciphered by two full cycles of the period. Note the examples below, in which the isologous plain text is less than two cycles in length:

74	31	89	60	25	12
0	B	SE	R	V	AT
74	22	89	81	04	19
48	53	68	41	29	21
ION	P	0	ST		
58	79	74	91		
22	00	53	51		

Figure 109a.

74	31	89	60	25	12
	0	B	SE	R	V
	74	22	89	81	04
	05	01	49	06	16
AT	ION	P	0	ST	
19	58	79	74	91	
83	89	58	34	16	

Figure 109b.

I	II	III	IV	V	VI
84	57	95	10		

Figure 109c

I	II	III	IV	V	VI
	84	57	95	10	

Figure 109d.

The delta repetition is four dinomes in length, which is one cycle less than the length of the isologous plain text; i.e., 10 - 6 = 4. Note, however, the following examples:

74	31	89	60	25	12
P	O	IN	T	F	IVE
79	74	56	93	46	61
43	05	35	53	61	73
SE	VE	N	F	OU	R
89	05	60	46	78	81
53	36	49	06	93	93

Figure 110a.

74	31	89	60	25	12
			P	O	IN →
			79	74	56
			39	99	68
← T	ON	E	SE	VE	N →
93	76	35	89	05	60
67	07	14	49	20	72
← F	I	VE			
46	54	05			
10	85	84			

Figure 110b.

I	II	III	IV	V	VI
10	31	14	53	32	20

Figure 110c.

I	II	III	IV	V	VI
			10	31	14 →
← 53	88	70			

Figure 110d.

Here the delta repetition is four dinomes also; this repetition, however, arises not from a long plaintext repetition, but from identical sets of a 4-dinome repetition in the plain text over another 4-dinome repetition in the plain text. This means that, if a delta repetition does not extend to a full cycle or more of the period, we must not jump to conclusions that a short delta repetition is the result of a single long plaintext repetition; in Figs. 110c and d, the 4-dinome repetition, as may be seen, is not the result of a 10-dinome plaintext repetition.

1. Now to get back to the cryptogram of Fig. 107. Since the cipher text factors to 6 dinomes, we will subtract each dinome from the one six places to the right of it to obtain the delta stream; this is shown in Fig. 111, below:

41 30 07 04 63 53 61 21 53 79 39 04 74 34 51 93 60 29 60 25 89 68 74 34
20 91 56 75 76 51 13 13 08 24 31 25 96 91 38 75 14 15

83 51 94 19 17 84 66 04 04 53 24 20 42 92 20 23 92 55 11 26 36 92 13 69
23 36 15 51 43 50 83 53 10 44 17 46 86 98 26 70 78 35 79 34 16 79 21 14

13 05 99 56 98 09 42 10 40 99 48 82 95 20 72 75 24 12 42 92 20 23 92 90
02 89 63 64 85 40 39 15 51 43 50 83 53 10 32 86 86 30 57 72 58 58 78 88

04 66 60 80 16 71 42 48 72 78 03 17 44 13 35 45 17 87 12 48 04 04 91 95
62 74 40 67 24 81 48 82 12 98 97 46 02 75 63 77 14 70 78 35 79 69 84 18

71 42 72 78 97 37 84 80 26 56 86 89 44 26 51 28 24 11 11 80 85 36 08 83
69 04 78 74 06 42 13 48 54 88 99 52 60 46 35 72 48 32 77 64 34 18 84 72

19 10 91 25 31 37 17 52 23 95 23 55 83 51 94 19 17 84 66 50 11 17 24 11
08 30 16 99 33 54 08 42 32 70 92 28 76 09 71 24 94 39 83 09 27 08 17 37

11 34 45 06 40 69 37 16 36 83 48 55 89
55 84 34 99 26 58 26 82 91 87 08 96 52

Figure 111.

Two sets of repetitions are revealed in the delta stream, one of 7 dinomes and one of 4 dinomes. The longer one must perforce represent a repeated plaintext passage beginning 6 dinomes to the left of the delta repetition, but there is no assurance that the 4-dinome delta repetition represents a longer plaintext repetition; in any case, we shall use only the information derived from the lengths of the delta repetitions as disclosed.

(1) Let us record the original ciphertext sequences which stand above the 7-dinome delta repetitions of Fig. 111; allocated into their proper positions in the key cycle, these are as follows:

I	II	III	IV	V	VI
		(94	19	17	84
66	04	04)			
	(10	40	99	48	82
95	20)				

Figure 112.

We will now arbitrarily assume that the initial 10_c in the second sequence represents 10_p; this of course gives us an additive of 00 for col. II. The 94_c in the initial position of the first sequence must also represent 10_p, so therefore the additive for col. III has to be 84. This additive, when applied to the second dinome of the second sequence, 40_c, deciphers it as 66_p. This zigzagging process is continued, quickly deriving the relative additive as follows:

	91	00	84	53	71	17
C:			(94	19	17	84
P:			10	66	46	77
C:	66	04	04)			
P:	75	04	20			
C:		(10	40	99	48	82
P:		10	66	46	77	75
C:	95	20)				
P:	04	20				

Figure 113.

(2) With a relative additive at hand, we now reduce the text of the cryptogram to monoalphabetic terms, as follows:

91 00 84 53 71 17 91 00 84 53 71 17 91 00 84 53 71 17 91 00 84 53 71 17
41 30 07 04 63 53 61 21 53 79 39 04 74 34 51 93 60 29 60 25 89 68 74 34
50 30 23 51 92 46 70 21 79 26 68 97 83 34 77 40 99 12 79 25 05 15 03 27

83 51 94 19 17 84 66 04 04 53 24 20 42 92 20 23 92 55 11 26 36 92 13 69
92 51 10 66 46 77 75 04 20 00 53 13 51 92 46 70 21 48 20 26 52 49 42 52

13 05 99 56 98 09 42 10 40 99 48 82 95 20 72 75 24 12 42 92 20 23 92 90
22 05 15 03 27 92 51 10 66 46 77 75 04 20 98 22 53 05 51 92 46 70 21 83

04 66 60 80 16 71 42 48 72 78 03 17 44 13 35 45 17 87 12 48 04 04 91 95
13 66 86 37 45 64 51 48 98 25 32 00 53 13 51 92 46 70 21 48 20 51 20 88

71 42 72 78 97 37 84 80 26 56 86 89 44 26 51 28 24 11 11 80 85 36 08 83
80 42 98 25 26 20 93 80 42 03 15 72 53 26 77 75 53 04 20 80 01 83 37 76

19 10 91 25 31 37 17 52 23 95 23 55 83 51 94 19 17 84 66 50 11 17 24 11
28 10 17 72 60 20 26 52 49 42 52 48 92 51 10 66 46 77 75 50 37 64 53 04

11 34 45 06 40 69 37 16 36 83 48 55 89
20 34 61 53 79 52 46 16 52 30 77 48 98

Figure 114.

All of the polygraphic repetitions originally present in the plain text are now disclosed. Since the matrix involved is the same as that in Fig. 101 except that the coordinates have been scrambled, we must make some plaintext assumptions. The best assumption for the repetition 20 26 52 49 42 52 is P O S IT ION S, based not only on the idiomorph present, but also on the fact that the first two dinomes begin with the same digit (P and O are in the same row of the matrix); moreover, by the time we have recorded the coordinates for the values P, O, S, and IT, the dinome 42 automatically gives the value ION, thus furnishing confirmation of the validity of the plaintext assumption. The derived coordinates are placed in the proper positions outside the basic matrix, so it now looks like this:

	6						2	ϕ	9
	A	1	AL	AN	AND	AR	ARE	AS	AT	ATE
	ATI	B	2	BE	C	3	CA	CE	CO	COM
	D	4	DA	DE	E	5	EA	ED	EN	ENT
	ER	ERE	ERS	ES	EST	F	6	G	7	H
4	8	HAS	HE	I	9	IN	ING	ION	IS	IT
	IVE	J	ϕ	K	L	LA	LE	M	ME	N
2	ND	NE	NT	O	OF	ON	OR	OU	P	Q
5	R	RA	RE	RED	RES	RI	RO	S	SE	SH
	ST	STO	T	TE	TED	TER	TH	THE	THI	THR
	TI	TO	U	V	VE	W	WE	X	Y	Z

From here on the rest of the solution follows easily, the deciphered values furnishing clues around which to make a few further assumptions until all ten row and column coordinates are recovered. For example, the repetition 51 92 46 70 21 (the middle dinome of which deciphers to I_p) must begin with one of the R or S groups of row 5; if 51 represents RE, then 21 automatically deciphers as NT, suggesting that the repetition represents RE G I ME NT, especially since the column coordinates for G and ME have already been placed by the first assumption.

(3) Since the additive recovered is on a relative base, so are the reconstructed coordinates on a relative base. The actual additive was 14 23 07 76 94 30, which can be derived from our recovered relative additive by adding a corrective of 23 to all the dinomes of the key; the matrix coordinates would then be changed by adding 8 to all the row coordinates, and 7 to all the column coordinates. But there is no way of deriving or of proving the correct base; besides, this point is only of academic importance.

k. The initial entry in the example in Fig. 114 was made by means of a repetition which was identified as representing POSITIONS; this pat solution may appear to the student as a very fortunate piece of hindsight indeed, in view of the fact that the author made up the problem. For the skeptical reader with a jaundiced eye, there will now be presented a mathematical method of arriving at several row and column coordinates (thereby identifying a number of plaintext values in the cipher), without recourse to any plaintext assumptions whatsoever.

(1) If the matrix in Fig. 101 were a known matrix, recovered from previous solution, a tabulation could be made of the frequencies of occurrence of the various plaintext elements within the matrix. Such a tabulation is shown in Fig. 115, below, wherein are listed the frequencies of over 1400

	1	2	3	4	5	6	7	8	9	ø	
1	30	6	3	2	3	13	3	1	14	3	78
2	1	10	3	8	20	1	3	8	6	3	63
3	26	1	5	5	30	5	4	5	9	1	91
4	10	1	1	2	1	18	1	22	1	15	72
5	1	3	4	36	1	19	8	14	7	8	101
6	1	2	7	7	28	3	9	23	8	28	116
7	1	6	10	28	11	17	13	12	50	4	152
8	31	8	22	1	1	4	13	54	10	1	145
9	13	15	22	3	2	2	10	6	2	3	78
ø	6	13	26	10	9	15	6	3	15	1	104
	120	65	103	102	106	97	70	148	122	67	1000

Figure 115.

plaintext values from representative messages, reduced to a base of 1000.

Note that the highest-frequency element, 88 (representing S_p), has a relative frequency of 54 in 1000 (i.e., 5.4%); the next highest, 79 (representing P_p), a relative frequency of 50; etc. Note also that the sums of the entries in the rows have greatly varying frequencies, and likewise the columnar sums.

(2) Referring back to Fig. 114, we will now take a dinome distribution of the monoalphabetically-converted text; this is shown below:

	1	2	3	4	5	6	7	8	9	ø	
1		1	3		3	1	1			4	13
2	4	2	1		3	5	2	1		9	27
3		1		2			3			2	8
4		4			1	8		5	2	1	21
5	9	6	7							2	24
6	1			2		4		1		1	9
7		2			4	1	6		3	4	20
8			3			1		1		3	8
9		7	1				1	4	1		14
ø	1		3	4	3					2	13
	15	23	18	8	14	20	13	12	6	28	

Figure 116.

Row 2 of this distribution, with 27 tallies, and row 5, with 24 tallies, should correspond either to true row 7 (weight of 152) and true row 8 (weight of 145) of Fig. 115, or vice versa; let us assume that true row 7 (with the higher score) is the correct equivalent for row 2. Col. ø, with 28 tallies, should be one of the three highest columns of Fig. 115: true col. 8 (weight of 148), true col. 9 (weight of 122), or true col. 1 (weight of 120). But cell 2-ø (with a high count of 9 tallies) should correspond to one of the following true row-column combinations: 7-8 (weight of 12), 7-9 (weight of 50), or 7-1 (weight of 1). The correct choice for cell 2-ø is obviously true 7-9. This means then that row 5 (with 27 tallies) should be true row 8 (weight of 145).

(3) Since col. ø (which has been identified as true col. 9) is not true col. 8 (which has a high weight of 148), true col. 8 should be col. 2 (with 23 tallies, the second ranking column); this is substantiated by cell 5-2 (with a frequency of 6), which shows a correspondence with true 8-8 (weight of 54). Now cells 5-1 (9 tallies) and 5-3 (7 tallies) should represent true 8-1 (weight of 31) or true 8-3 (weight of 22); in light of the higher number of tallies (18) of col. 3, this column should correspond to true col. 1 (weight of 120), making col. 1 (15 tallies) equal to true col. 3 (weight of 103). Cell 9-2 (7 tallies) should correspond to true 6-8 (weight of 23) or to true 4-8 (weight of 22); but comparing row 9 (14 tallies) with true row 6 (weight of 116) and with true row 4 (weight of 72), the agreement of row 9 is best with true row 4.

(4) Placing the recovered coordinates for three of the rows and four of the columns in position on the matrix, we have the following:

	3	1				2	ø		
	A	1	AL	AN	AND	AR	ARE	AS	AT	ATE
	ATI	B	2	BE	C	3	CA	CE	CO	COM
	D	4	DA	DE	E	5	EA	ED	EN	ENT
9	ER	ERE	ERS	ES	EST	F	6	G	7	H
	8	HAS	HE	I	9	IN	ING	ION	IS	IT
	IVE	J	ø	K	L	LA	LE	M	ME	N
2	ND	NE	NT	O	OF	ON	OR	OU	P	Q
5	R	RA	RE	RED	RES	RI	RO	S	SE	SH
	ST	STO	T	TE	TED	TER	TH	THE	THI	THR
	TI	TO	U	V	VE	W	WE	X	Y	Z

The plaintext values for the dinomes whose coordinates have been recovered are now placed in the cryptogram, yielding the following:

```
50 30 23 51 92 46  70 21 79 26 68 97  83 34 77 40 99 12  79 25 05 15 03 27
89  9 71 83 48     9 73    7     4     1        9  4  8     7              1 7
SE    ND RE  G       NT

92 51 10 66 46 77  75 04 20 00 53 13  51 92 46 70 21 48  20 26 52 49 42 52
48 83  9                 79  9 81  1  83 48     9 73     79  7 88     8 88
 G RE                     P     R     RE  G        NT      P    S       S

22 05 15 03 27 92  51 10 66 46 77 75  04 20 98 22 53 05  51 92 46 70 21 83
78        1  7 48  83  9                 79  4 78 81     83 48     9 73  1
OU             G   RE                    P    OU R      RE  G        NT

13 66 86 37 45 64  51 48 98 25 32 00  53 13 51 92 46 70  21 48 20 51 20 88
 1                 83    4  7  8  9   81  1 83 48     9   73    79 83 79
                   RE                R     RE  G        NT     P  RE  P

80 42 98 25 26 20  93 80 42 03 15 72  53 26 77 75 53 04  20 80 01 83 37 76
 9  8  4  7  7 79  41  9  8  1     8  81  7           81     79  9  3  1
                P   ER                R              R      P

28 10 17 72 60 20  26 52 49 42 52 48  92 51 10 66 46 77  75 50 37 64 53 04
 7  9     8  9 79   7 88     8 88     48 83  9                 89       81
               P      S       S       G RE                    SE       R

20 34 61 53 79 52  46 16 52 30 77 48  98
79     3 81    88        88  9
 P       R     S         S
```

Not only do the skeletal plaintext values constitute a nucleus for further assumptions, but derived single coordinates for the rows or columns (such as in the second dinome where 30 = -9) serve as a guide for the choice of additional values. The solution from here on is very straightforward.

(5) If the sample of text were large enough, it might be possible to recover most or even all of the row and column coordinates mathematically. But if we are to use statistical tools intelligently, and not merely for their own sake,[10] we should use just what is needed for the quickest solution possible.

1. In the foregoing subparagraphs there have been treated enciphered syllabary square systems wherein the composition of the matrix is known. If nothing were known about the basic matrix, solution would proceed by factoring and determining the period, and then reducing the cipher text to monoalphabetic terms by one of the methods already outlined. The last step, that of breaking into the reduced cipher text, is accomplished by attacks based on probable words, repetitions and similar sequences, idiomorphs, isologs, and other phenomena or special situations which can and will occur, sooner or later, when the system is used for regular traffic; the analysis of syllabary squares and code charts has been given adequate treatment in par. 80 of Chapter XI in Military Cryptanalytics, Part I, and in the associated problems (Appendix 9 of that text, pp. 423-427).

84. Additional remarks.--a. The discussion in this chapter has been limited to superenciphered numerical bipartite systems, i.e., where the matrix coordinates consist of digits. If the coordinates consisted of letters, and if these letters were enciphered with, say, direct standard alphabets, the techniques presented in this chapter can be adapted to this situation because the arithmetic is being performed on a known modulus (in this case, mod 26; e.g., B + E = G, Y + C = A, etc.). If the superencipherment involves unknown mixed cipher alphabets, the ordinary modular relationships do not obtain; therefore solutions must be based on a volume of traffic, plus whatever fortunate special situations may be present in the system as used by the enemy. However, the majority of cases of superenciphered bipartite systems encountered have involved matrices with numerical coordinates and mod 10 addition.

b. The cryptographic arithmetic treated in this chapter is the additive method, where P + K = C, and C - K = P. There are two other arithmetical methods of encipherment: the subtractive method, where P - K = C, and C + K = P; and the minuend method, where K - P = C, and K - C = P. Additive, subtractive, and minuend methods are complementary: an additive system may be solved as a subtractive system or a minuend system; any one of these may be solved as either of the other two. If an additive system is assumed and the cipher is actually a subtractive system, all that will happen is that a complementary key will be derived (e.g., in subpar. 82i the recovered key would have been 53 49 28 76 10 instead of the 57 61 82 34 90 as derived).

[10] See in this connection some remarks made by C. H. O'D. Alexander quoted on p. 223 of Military Cryptanalytics, Part I.

If a minuend system is solved as an additive or subtractive system, the intermediate plaintext digits will be the complements of the true intermediate plain (with or without the addition of a constant). In any case, the derived key can always be converted into the true key either (a) by the addition of a constant, or (b) by the addition of a constant to the complements of the derived key. Situations where it makes any difference if the correct method has not been assumed are rare; these cases usually involve certain aspects of key analysis, or situations wherein the true coordinates of a matrix are known. This matter will be dealt with at greater length in the next volume.

c. It should be clear to the student that if there are any limitations in either the left- or right-hand components of the dinome intermediate text, such limitations will simplify the problem of reduction to monoalphabetic terms.

d. The cryptogram in Fig. 107 was factorable by means of the polygraphic repetitions patent in the cipher text. The student should note that if these repetitions had not been in evidence, we still could have factored the cryptogram by generating delta streams at various intervals and examining these streams for evidences of long polygraphic repetitions; when the interval of 6 dinomes was considered, we would have the diagram as illustrated in Fig. 111, revealing from the latent repetitions now disclosed that the length of the period is 12 digits.

e. One further tool for factoring might occur to the student: the use of an I.C. to determine when the correct write-out has been reached, in the manner of that described in subpar. 18e. This very valuable method, especially rewarding in difficult cases, warrants detailed treatment; the application of this procedure will be taken up in the next chapter in subpars. 86b-d.

f. Attacks based on cribs, isologs, and other special situations may be devised to fit the specific situation at hand; the alert cryptanalyst should always be on the lookout for the possibility of exploitation by means of these methods in a particular case under study.

(BLANK)

CHAPTER XII

MONOME-DINOME SYSTEMS WITH CYCLIC ADDITIVES

85. General remarks.--a. In the preceding chapter we have seen demonstrated the various methods of attack on dinome systems superenciphered by cyclic additives. The determination of the length of the additive was made by the general method of factoring the interval between long (i.e., causal) repetitions; in the case of the Nihilist system the determination of the period was made by taking advantage of the cryptographic idiosyncracies of that system (as regards the "unique dinomes" 01, 10, 22, and 30).

b. The matrices in the foregoing chapter were dinome matrices, their particular dimensions being irrelevant. The reduction of the columns of the additive-enciphered text was accomplished (1) by equating the monomic distributions (cf. subpars. 82b and c), or (2) by equating the dinomic columns (as in subpar. 83d), or (3) by comparing sets of identical-length ciphertext repetitions assumed to contain identical underlying plain text (subpar. 83f), or (4) by analysis of the delta stream at an interval corresponding to the period (subpar. 83j).

c. If a cyclic additive encipherment is applied to intermediate plain text produced by a monome-dinome system, the problem gets more complicated, especially as regards column equating. The determination of the period may be made by the usual process of factoring; but if no long repetitions are in evidence, we must rely on deriving a columnar I.C. statistic for each width that comes into consideration,[1] hoping that the correct width will have a predominant I.C. and that there will be no other "good" answers for the incorrect widths. We might even apply the delta-stream method and with luck uncover possible latent sets of long plaintext repetitions which would then indicate that the interval of the delta stream tried is equivalent to the true period or a multiple of the period; but this method is hardly to be recommended except in cases where the additive is very short in comparison with the length of the message.

d. In additive-enciphered monome-dinome systems, once the period has been determined, the equating of columns is accomplished by sliding the monomic distributions to a correct match when there are a sufficient number of tallies per column. What constitutes "a sufficient number of tallies per column" is dependent on the over-all I.C. of the cipher text produced by the underlying monome-dinome matrix; if the matrix had the highest frequency letters in the monome row, much larger distributions would be necessary for column equating than if some medium or low frequency letters were

[1] Cf. the method shown in subpar. 18e.

represented by monomes. The problem of column equating is all the more complicated because each columnar distribution contains a mixture of monome elements and only one of the elements of a dinome--thus there is a "watering down" of the information that might have been available if the distributions pertained only to left-hand or right-hand members of dinomes as in the systems illustrated in the preceding chapter.

e. If there are several messages in the same system which have been enciphered at various points along the keying cycle, their correct superimpositions may be determined by locating long repetitions between messages and aligning them so that the repetitions are exactly superimposed. Otherwise, once the period has been determined, even without the presence of long repetitions we may still align the messages correctly by a variation of the χ-test method demonstrated in par. 72.

86. Analysis of a general case of an additive-enciphered monome-dinome system.--a. In this first case we will treat the cryptanalysis of a system involving an unknown monome-dinome matrix with an additive of unknown length; for purposes of illustration, it will be assumed that the enemy is known to be using additives from 20 to 40 digits in length. The following two messages are available for study:

Message "A"

90723	78168	94849	15771	16844	17454	66220	88312	87103	45436
51844	80725	95351	25207	71062	43897	67340	60921	05986	85348
28147	15733	58293	45515	05206	88337	34666	19895	67818	09150
66954	13321	61791	75797	51414	31979	86210	85627	71095	58825
20894	16966	09087	59634	80149	82880	81862	77470	01320	13674
11794	57837	24849	06800	00520	19613	90147	16045	20150	35129
06260	72364	91991	17821	62194	36516	06329	85610	90458	05395
55013	35800	92354	04365	92886	96225	20858	05926	00264	38137
81653	45991	26864	97686	06029	44327	74662	65027		

Message "B"

60542	47550	69060	75362	54662	15457	59157	87473	49316	85347
71001	54092	60653	01924	46954	28733	91803	65347	43818	08626
06354	13674	11794	57837	25513	51562	06723	19962	51163	49777
57217	35540	01953	28138	90813	05530	07142	06526	06554	84334
34903	31904	26742	97424	04573	22367	17863	25890	59816	42517
30323	83618	80859	15433	25890	58254	60200	14378	99263	49028
67137	40325	53354	15374	24063	75498				

There are many short repetitions present, but since the causal cases cannot be distinguished from the random, there is no information in the repetitions to indicate the length of the period. Furthermore, we really do not know whether or not the two messages are even in the same system; and if they are, whether the messages are in flush depth or at an offset in the key cycle.

b. Since the additive sequences used by the enemy in the past have been from 20 to 40 digits long, we will transcribe Message "A", the longer of the two, into the various widths successively, deriving the sum of the I.C.'s of the columns for each particular width.[2] The columnar frequencies for Message "A" when written out on a width of 20 are shown in the diagram below:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
ø	4	6	1	2	4	5	1	1	2	3	5	3	4		3		1	1	1	3	ø
1	1	3	5	2	2	5		2	1	2	1	7	1	2	1	5	1	2	4	3	1
2	4	2	3	3		1	2	1	4		2	1	3	3	3			1	7	1	2
3			4		3	1	1	5	3	1	1		1		2	4	2	3	3	1	3
4		1	1	6	4	3	2	2	1	3		3	1	2	6	2		1	1	1	4
5		2		5			8	1	2	3	4	2	1	2	1	3	7	1		5	5
6	4	4	1	1	1	1	4	2	4	4	2	4	2	6	3	1	1	4		1	6
7		3	2		2	3	1	2	1	5	3		1		1	1	4	2	3	4	7
8	4	1	5		3	3	2	2	1	1	1	1	5	3		4	3	6	1	1	8
9	5			3	3		1	4	3		3	1	3	4	2	2	3	1	2	2	9
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	

ϕ = 68 58 60 66 46 58 74 42 40 52 48 68 46 60 52 54 68 52 68 46 $\quad \Sigma\phi = 1126$

The sum of all the columnar ϕ values is 1126. Since in writing out the message (440 digits) on a width of 20, we get 20 columns of 22 tallies each, the ϕ_r is $\frac{20(22 \cdot 21)}{10} = 924$; thus the I.C. for this width is $\frac{1126}{924} = 1.22$, which seems surprisingly good for a random case, if it is random. Since the cryptanalyst should have learned by now that it is well to regard with suspicion any very good result on the very first trial, he proceeds to test other widths. The data for the first 10 tests are tabulated below:

Width	I.C.	Width	I.C.
20	1.22	25	0.97
21	0.93	26	0.92
22	0.91	27	0.91
23	1.01	28	1.06
24	1.11	29	1.11

[2] The process of transcribing text into a multitude of widths and making all the necessary computations is a laborious task when performed by hand, where machine methods are available, this presents no problem.

c. The next width to be considered is 30, so the message is written out accordingly, as follows:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
9	0	7	2	3	7	8	1	6	8	9	4	8	4	9	1	5	7	7	1	1	6	8	4	4	1	7	4	5	4
6	6	2	2	0	8	8	3	1	2	8	7	1	0	3	4	5	4	3	6	5	1	8	4	4	8	0	7	2	5
9	5	3	5	1	2	5	2	0	7	7	1	0	6	2	4	3	8	9	7	6	7	3	4	0	6	0	9	2	1
0	5	9	8	6	8	5	3	4	8	2	8	1	4	7	1	5	7	3	3	5	8	2	9	3	4	5	5	1	5
0	5	2	0	6	8	8	3	3	7	3	4	6	6	6	1	9	8	9	5	6	7	8	1	8	0	9	1	5	0
6	6	9	5	4	1	3	3	2	1	6	1	7	9	1	7	5	7	9	7	5	1	4	1	4	3	1	9	7	9
8	6	2	1	0	8	5	6	2	7	7	1	0	9	5	5	8	8	2	5	2	0	8	9	4	1	6	9	6	6
0	9	0	8	7	5	9	6	3	4	8	0	1	4	9	8	2	8	8	0	8	1	8	6	2	7	7	4	7	0
0	1	3	2	0	1	3	6	7	4	1	1	7	9	4	5	7	8	3	7	2	4	8	4	9	0	6	8	0	0
0	0	5	2	0	1	9	6	1	3	9	0	1	4	7	1	6	0	4	5	2	0	1	5	0	3	5	1	2	9
0	6	2	6	0	7	2	3	6	4	9	1	9	9	1	1	7	8	2	1	6	2	1	9	4	3	6	5	1	6
0	6	3	2	9	8	5	6	1	0	9	0	4	5	8	0	5	3	9	5	5	5	0	1	3	3	5	8	0	0
9	2	3	5	4	0	4	3	6	5	9	2	8	8	6	9	6	2	2	5	2	0	8	5	8	0	5	9	2	6
0	0	2	6	4	3	8	1	3	7	8	1	6	5	3	4	5	9	9	1	2	6	8	6	4	9	7	6	8	6
0	6	0	2	9	4	4	3	2	7	7	4	6	6	2	6	5	0	2	7										

The diagram for the columnar frequencies at this width is given below:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
ø	9	3	2	1	5	1			1	1		3	2	1		1		2		1		3	1		2	3	2		2	4	ø
1		1		1	1	3		2	3	1	1	6	4		2	5				3	1	3	2	3		2	1	2	2	1	1
2		1	5	6		1	1	1	3	1	1	2			2		1	1	4		5	1	1		1			4		2
3			4		1	1	2	7	3	1	1				2		1	1	3	1			1		2	4				3
4					3	1	2		1	3		2	1	4	1	3		1	1			1	1	4	6	1		2		1	4
5		3	1	3		1	4			1				2	1	2	7			5	4	1		2			4	2	2	2	5
6	2	6		2	2			5	3		1		3	3	2	1	2			1	3	2		2		1	3	1	1	4	6
7			1		1	2			1	5	3	1	2		2	1	2	1	1	4		2				1	3	1	2		7
8	1			2		5	4			2	3	1	2	1	1	1	1	6	1		1	1	8		2	1		2	1		8
9	3	1	2		2		2			5		1	4	2	1	1	3	5						3	1	1	1	4		2	9

ϕ = 80 42 36 40 30 28 30 64 24 28 32 40 24 32 12 28 46 38 38 38 38 16 58 28 36 20 26 20 20 28 $\Sigma\phi = 1020$

The sum of all the columnar ϕ values here is 1020. Since we have 20 columns of 15 tallies and 10 columns of 14 tallies, $\phi_r = \frac{20(15 \cdot 14) + 10(14 \cdot 13)}{10} = 602$, and the I.C. is therefore $\frac{1020}{602} = 1.69$. With such a high I.C., there is no question that the correct period is 30.

d. We now transcribe Message "B" on a width of 30 as shown below, together with its accompanying frequency diagram:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
6	0	5	4	2	4	7	5	5	0	6	9	0	6	0	7	5	3	6	2	5	4	6	6	2	1	5	4	5	7
5	9	1	5	7	8	7	4	7	3	4	9	3	1	6	8	5	3	4	7	7	1	0	0	1	5	4	0	9	2
6	0	6	5	3	0	1	9	2	4	4	6	9	5	4	2	8	7	3	3	9	1	8	0	3	6	5	3	4	7
4	3	8	1	8	0	8	6	2	6	0	6	3	5	4	1	3	6	7	4	1	1	7	9	4	5	7	8	3	7
2	5	5	1	3	5	1	5	6	2	0	6	7	2	3	1	9	9	6	2	5	1	1	6	3	4	9	7	7	7
5	7	2	1	7	3	5	5	4	0	0	1	9	5	3	2	8	1	3	8	9	0	8	1	3	0	5	5	3	0
0	7	1	4	2	0	6	5	2	6	0	6	5	5	4	8	4	3	3	4	3	4	9	0	3	3	1	9	0	4
2	6	7	4	2	9	7	4	2	4	0	4	5	7	3	2	2	3	6	7	1	7	8	6	3	2	5	8	9	0
5	9	8	1	6	4	2	5	1	7	3	0	3	2	3	8	3	6	1	8	8	0	8	5	9	1	5	4	3	3
2	5	8	9	0	5	8	2	5	4	6	0	2	0	0	1	4	3	7	8	9	9	2	6	3	4	9	0	2	8
6	7	1	3	7	4	0	3	2	5	5	3	3	5	4	1	5	3	7	4	2	4	0	6	3	7	5	4	9	8

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
ϕ	1	2			1	3	1			2	5	2	1	1	2							2	2	3		1		2	1	2	ϕ
1			3	4			2		1			1		1		4		1	1		2	4	1	1	1	2	1				1
2	3		1		3		1	1	5	1			1	2		3	1			2	1		1		1	1			1	1	2
3		1		1	2	1		1		1	1	1	4		4		2	6	3	1	1			7	1		1	3	1	3
4	1			3		3		2	1	3	2	1			4		2		1	3		3			1	2	1	3	1	1	4
5	3	2	2	2		2	1	5	2	1	1		2	5			3				2			1		2	6	1	1		5
6	3	1	1		1		1	1	1	2	2	4		1	1			2	3				1	5		1					6
7		3	1		3		3		1	1			1	1		1		1	3	2	1	1	1			1	1	1	1	4	7
8			3		1	1	2									3	2			3	1		4				2		2	8
9		2		1		1		1				2	2				1	1			3	1	1	1	1		2	1	3		9

ϕ = 18 12 14 20 14 14 10 22 22 10 24 16 16 22 26 24 12 32 18 16 10 20 14 26 42 6 32 10 12 16 $\quad \Sigma\phi = 550$

The ϕ_o is 550; the $\phi_r = \frac{30(11 \cdot 10)}{10} = 330$. The I.C. is $\frac{550}{330} = 1.67$, which proves that 30 is the correct period for this message also.

e. Now comes the problem of determining the relative juxtaposition of the two messages (if they are indeed homogeneous). Following the general procedure illustrated in par. 72 in connection with progressive alphabet systems, we will match the columnar frequency diagram of Message "B" at all possible offsets with the columnar frequency diagram of Message "A", deriving the columnar χ values for the columns at each juxtaposition.[3] The first test is shown below:

[3] A cut-out mask, exposing corresponding cells in the two frequency diagrams, will be found useful in avoiding errors in deriving the cross products.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
ϕ	9	3	2	1	5	1			1	1		3	2	1		1		2		1		3	1		2	3	2		2	4	ϕ
1		1		1	1	3		2	3	1	1	6	4		2	5				3	1	3	2	3		2	1	2	2	1	1
2		1	5	6		1	1	1	3	1	1	2			2		1	1	4		5	1	1		1				4		2
3			4		1	1	2	7	3	1	1				2		1	1	3	1			1		2	4					3
4					3	1	2		1	3		2	1	4	1	3		1	1			1	1	4	6	1		2		1	4
5		3	1	3		1	4			1				2	1	2	7			5	4	1		2			4	2	2	2	5
6	2	6		2	2			5	3		1		3	3	2	1	2			1	3	2		2		1	3	1	1	4	6
7			1		1	2			1	5	3	1	2		2	1	2	1	1	4		2				1	3	1	2		7
8	1			2		5	4			2	3	1	2	1	1	1	1	6	1		1	1	8		2	1		2	1		8
9	3	1	2		2		2				5		1	4	2	1	1	3	5					3	1	1	1	4		2	9

	1	2	29	30	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
ϕ	1	2			1	2	1	2		1	3	1			2	5	2	1	1	2							2	2	3		1		2	1	2	ϕ
1								3	4			2		1		1		1		4		1	1		2	4	1	1	1	2	1				1
2	3				1	1	3		1		3		1	1	5	1			1	2		3	1			2	1		1		1	1			1	1	2
3		1			3	1		1		2	1		1		1	1	1	4		4		2	6	3	1	1			7	1		1	3	1	3
4	1				1	1	1			3		3		2	1	3	2	1		4		2		1	3		3			1	2	1	3	1	1	4
5	3	2			1		3	2	2	2		2	1	5	2	1	1		2	5			3			2			1		2	6	1	1		5
6	3	1				3	1	1		1		1	1	1	2	2	4		1	1			2	3				1	5		1					6
7		3			1	4		3	1		3		3		1	1		1	1			1	3	2	1	1	1			1	1	1	1	4	7
8						2		3		1	1	2							3	2		3	1		4				2		2	8
9		2			3		2		1		1				2	2				1	1		3	1	1	1	1		2	1	3			9
	χ =				15	20	8	10	12	14	13	13	23	19	3	14	6	14	14	24	27	10	13	9	16	23	37	18	22	15	30	17	10	9		

The sum of the columnar χ values at this juxtaposition is 478. The expected sum of the cross products in a random case, χ_r, is $\frac{20(15\cdot11) + 10(14\cdot11)}{10} = 484$, so the §I.C. at this particular alignment of the two messages is $\frac{478}{484} = 0.99$.

f. We now slide the frequency diagram for Message "B" one position to the right with respect to the diagram for Message "A", and we derive the §I.C. for this setting. This §I.C., 1.04, is likewise void of cryptanalytic pith. After 20 unsuccessful trials,[4] on the 21st we finally reach the setting illustrated below:

[4] The student might wish to see the results of the first 20 trials. These are tabulated in the diagram below, wherein the entries under "slide" indicate the displacement of the frequency diagram for Message "B" to the right with respect to the frequency diagram for Message "A".

Slide	§I.C.	Slide	§I.C.	Slide	§I.C.	Slide	§I.C.
ϕ	0.99	5	0.83	10	0.93	15	0.92
1	1.04	6	1.06	11	0.82	16	0.99
2	0.90	7	1.01	12	0.94	17	0.86
3	1.16	8	1.14	13	1.13	18	1.01
4	0.86	9	0.89	14	0.94	19	1.04

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
ø	9	3	2	1	5	1			1	1		3	2	1		1		2		1		3	1		2	3	2		2	4	ø
1		1		1	1	3		2	3	1	1	6	4		2	5				3	1	3	2	3		2	1	2	2	1	1
2		1	5	6		1	1	1	3	1	1	2			2		1	1	4		5	1	1		1				4		2
3			4		1	1	2	7	3	1	1				2		1	1	3	1			1		2	4					3
4					3	1	2		1	3		2	1	4	1	3		1	1			1	1	4	6	1		2		1	4
5		3	1	3		1	4			1				2	1	2	7			5	4	1		2			4	2	2	2	5
6	2	6		2	2			5	3		1		3	3	2	1	2			1	3	2		2		1	3	1	1	4	6
7			1		1	2			1	5	3	1	2		2	1	2	1	1	4		2				1	3	1	2		7
8	1			2		5	4			2	3	1	2	1	1	1	1	6	1		1	1	8		2	1		2	1		8
9	3	1	2		2		2				5		1	4	2	1	1	3	5					3	1	1	1	4		2	9

	1	2		11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	1	2	3	4	5	6	7	8	9	10		29	30	
ø	1	2		5	2	1	1	2							2	2	3		1		2	1	2	1	2			1	3	1			2			1	2	ø
1					1		1		4		1	1		2	4	1	1	1	2	1						3	4			2		1					1
2	3					1	2		3	1			2	1		1		1	1			1	1	3		1		3		1	1	5	1		1	1	2
3		1		1	1	4		4		2	6	3	1	1			7	1		1	3	1		1		1	2	1		1		1			3	1	3
4	1			2	1			4		2		1	3		3		1	2	1	3	1	1	1			3		3		2	1	3			1	1	4
5	3	2		1		2	5			3				2		1		2	6	1	1		3	2	2	2		2	1	5	2	1		1			5
6	3	1		2	4		1	1			2	3			1	5		1					3	1	1		1		1	1	1	2					6
7		3				1	1		1		1	3	2	1	1	1			1	1	1	1	4		3	1		3		3		1	1		1	4	7
8									3	2			3	1		4					2		2		3		1	1	2						2	8
9		2			2	2				1	1			3	1	1	1	1		2	1	3			2		1		1		1			3		9
	χ =			49	33	30	31	28	32	31	54	25	28	25	37	22	24	21	23	46	24	30	19	36	16	31	31	11	18	20	19	29	21				

Here the sum of the columnar cross products is 844, so the § I.C. is $\frac{844}{484} = 1.74$, proving that the two messages <u>are</u> homogeneous after all, and that they may be correctly juxtaposed as indicated.

g. We may now ccnsolidate the corresponding columnar distributions of Message "A" and Message "B", in order to obtain more data and thus facilitate the equating of the monomic distributions by sliding them to the best fit. In Fig. 117<u>a</u>, below, we show the consolidated data for the first 6 columns of the combined distributions; and in Fig. 117<u>b</u> we have equated these distributions in terms of col. 1. This process is continued with the remaining columns; and, since we happen to have plenty of data to work with, the entire additive is obtained quite easily, yielding the following 20-digit sequence:

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

This is probably a <u>relative</u> additive; there is no way of proving at this point which one of the ten equivalent additive sequences is the original.

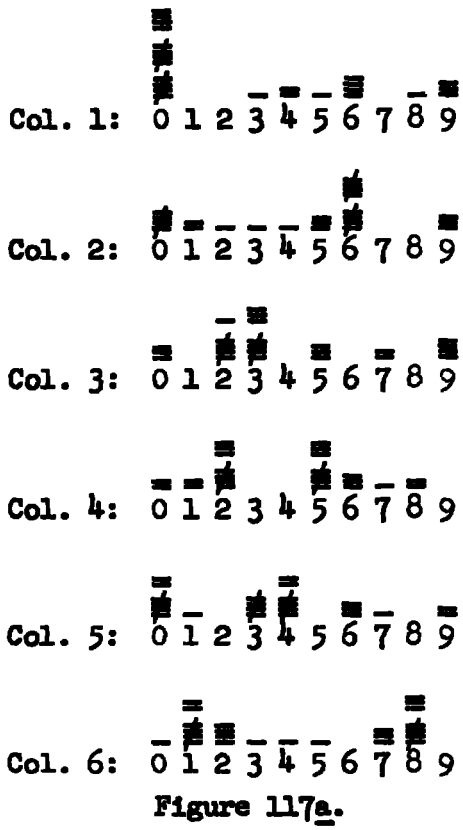


Figure 117a.

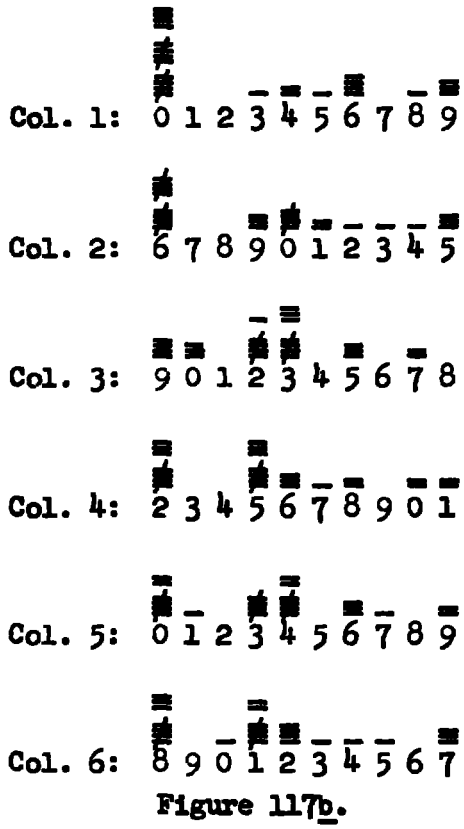


Figure 117b.

h. Having recovered the additive, we proceed to apply it to Message "A" to reduce the cipher to monoalphabetic terms. The first 60 digits of the message and their conversion are shown in the illustration below:

	0	6	9	2	0	8	5	3	3	4	9	1	8	6	3	1	5	4	9	7	2	7	8	1	4	0	7	5	2	6
C:	9	0	7	2	3	7	8	1	6	8	9	4	8	4	9	1	5	7	7	1	1	6	8	4	4	1	7	4	5	4
P:	9	4	8	0	3	9	3	8	3	4	0	3	0	8	6	0	0	3	8	4	9	9	0	3	0	1	0	9	3	8

C:	6	6	2	2	0	8	8	3	1	2	8	7	1	0	3	4	5	4	3	6	5	1	8	4	4	8	0	7	2	5.....
P:	6	0	3	0	0	0	3	0	8	8	9	6	3	4	0	3	0	0	4	9	3	4	0	3	0	8	3	2	0	9

Once the entire cryptogram has been reduced to monoalphabetic terms, the solution is quite straightforward, following the lines already discussed at length in the previous text.[5] The digits ∅ and 3 are identified as row coordinates, and when the converted text is divided accordingly the plain text is recovered, with Message "A" beginning with the words "REPORTS OF INTERROGATION..." The monome-dinome matrix is reconstructed as follows:

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

Since the additive sequence has probably been recovered on a relative base, the matrix coordinates are also relative.

[5] Cf Chapter X, Military Cryptanalytics, Part I.

i. In order to illustrate the general theory and techniques of solution of an additive-enciphered monome-dinome system, we have used in the foregoing example a matrix with a very favorable I.C. This facilitated the step of matching monomic distributions in subpar. g. If the monome-dinome matrix had cryptanalytically unfavorable characteristics, we would probably have required considerably more depth than the 26 lines of text we dealt with in subpar. g. The reason for the qualifying phrase is that, even with an unfavorable I.C. (which makes equating of monomic columns difficult and precarious), the presence of numerous repetitions in the underlying plain text at various positions in the keying cycle would facilitate the equating process, once some of these repetitions began to be uncovered in the process of solution.

j. In subpars. e and f we have shown a sensitive method employing the χ test for determining the correct juxtaposition of the frequency diagrams for the two messages; this method was demonstrated for pedagogical reasons, since it is the method which would have to be employed in a difficult case. It might be pointed out, however, that as a short cut we could have taken into account only one pair of corresponding rows (instead of the 10 pairs as in the example presented) of the two frequency diagrams to determine their relative placement. For example, if we consider only the "ø" rows in the illustration in subpar. e, we should expect that the entry "9" in position 1 of Message "A" will be aligned with one of the highest entries in the "ø" row of Message "B". In this case, our first trial of "9" in Message "A" against the "5" in Message "B" gives an excellent fit of the two sequences of digits as regards their corresponding peaks and troughs. The χ value at this juxtaposition of the two rows is 111; since the "ø" row of Message "A" contains 50 tallies and the "ø" row of Message "B" contains 34 tallies, the value of χ_r is $\frac{50 \cdot 34}{30} = 56.6$, and the ξ I.C. is $\frac{111}{56.6} = 1.96$. If we have to choose between two or more high scores obtained by this method, this preliminary test could be checked by performing the χ test on several entire columns of the diagram.

87. Analysis of a second case.--a. If an additive-enciphered monome-dinome system were used operationally, it is quite possible that the basic rectangle and coordinates might remain in force for a considerable period of time, so that cryptographic clerks might more easily memorize the equivalents for most or all of the letters and thus speed up operations. In such a case then, the only major variable element in the cryptosystem would be the length and composition of the additive sequence used to encipher the intermediate text.[6] If the basic matrix becomes known through previous solution, we may have recourse to a statistical method for reading traffic enciphered with the same matrix but with an unknown additive.

b. Let us assume that the enemy is still using the same monome-dinome matrix which was recovered in the previous paragraph, viz.:

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

[6] Another variable might be the specific starting point in the additive cycle

Since the ten cipher digits have greatly varying probabilities, we can calculate a set of weights which will be most useful in solving further systems incorporating the same matrix. First we shall replace the plaintext entries of the matrix with their theoretical frequencies in 1000 letters,[7] thus:

	9	4	8	1	2	7	6	5	ø	3
-	76	130	27	26	10	36	74	31		
ø	74	42	28	16	34	2	3	25	79	75
3	3	61	92	15	16	5	19	1		

The theoretical frequency of the digit ø will be the sum of all the entries in the "ø" row, plus the entries in the "ø" column; this is found to be 457. The theoretical frequency of the digit 3 will likewise be the sum of all the entries in the "3" row plus the entries in the "3" column; this is 287. The expected frequencies of the remaining digits will be the sum of the entries in each of the columns corresponding to the particular digit. Thus the theoretical distribution of the 10 digits obtained in the encipherment of 1000 letters of English plain text will be as follows:

ø	1	2	3	4	5	6	7	8	9
457	57	60	287	233	57	96	43	147	153

These frequencies will be used in the derivation of logarithmic weights, following the general procedure outlined in subpars. 34d and e on pp. 83-85.

c. In the table below, column (a) represents the frequencies of the ten digits comprising a plaintext "alphabet" of 10 categories; col. (b)

	(a)	(b)	(c)	(d)	(e)
ø	457	2.6599	1.0264	.99	9
1	57	1.7559	0.1224	.12	1
2	60	1.7782	0.1447	.14	1
3	287	2.4579	0.8244	.80	8
4	233	2.3674	0.7339	.71	7
5	57	1.7559	0.1224	.12	1
6	96	1.9823	0.3488	.34	3
7	43	1.6335	0.0000	.00	0
8	147	2.1673	0.5338	.51	5
9	153	2.1847	0.5512	.53	5

represents the logarithms (to the base 10) of these frequencies; col. (c) contains adjusted logarithms, obtained by subtracting the logarithm of the lowest frequency (43) from all the entries in col. (b), which is equivalent to dividing all the entries in col. (a) by 43;[8] col. (d) contains two-digit

[7] Cf. p. 28, Military Cryptanalytics, Part I.

[8] The purpose of this step is to reduce the lowest frequency, 43, to 1 on an arithmetical scale.

logarithms to a new base (10.88); and col. (e) represents deciban weights of col. (d), obtained by multiplying the entries in col. (d) by 10 and dropping the decimal point. The new base, C, is derived as follows:

$$\text{Let } \frac{457}{43} = C^{0.99}$$

$$\text{Then } (\text{Log}_{10}457 - \text{Log}_{10}43) = \text{Log}_{10}C^{0.99}$$

$$= (0.99)(\text{Log}_{10}C)$$

$$C = \text{Antilog } \frac{(\text{Log}_{10}457 - \text{Log}_{10}43)}{0.99} = \text{Antilog } \frac{1.0264}{0.99} = \text{Antilog } 1.0368$$

$$C = 10.88$$

Logarithms to a new base may be computed by the formula

$$\text{Log}_C Y = \frac{\text{Log}_{10}Y}{\text{Log}_{10}C}$$

Therefore if the entries in col. (c) are divided by 1.0368, we obtain the figures in col. (d) which are logarithms to the base 10.88.

d. For a demonstration problem, we will use Message "B" given in subpar. 86a; we will assume that the additive is unknown, but that the monome-dinome rectangle has been recovered from other messages. Since the message factors to a period of 30, it is written out on this width:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
6	0	5	4	2	4	7	5	5	0	6	9	0	6	0	7	5	3	6	2	5	4	6	6	2	1	5	4	5	7
5	9	1	5	7	8	7	4	7	3	4	9	3	1	6	8	5	3	4	7	7	1	0	0	1	5	4	0	9	2
6	0	6	5	3	0	1	9	2	4	4	6	9	5	4	2	8	7	3	3	9	1	8	0	3	6	5	3	4	7
4	3	8	1	8	0	8	6	2	6	0	6	3	5	4	1	3	6	7	4	1	1	7	9	4	5	7	8	3	7
2	5	5	1	3	5	1	5	6	2	0	6	7	2	3	1	9	9	6	2	5	1	1	6	3	4	9	7	7	7
5	7	2	1	7	3	5	5	4	0	0	1	9	5	3	2	8	1	3	8	9	0	8	1	3	0	5	5	3	0
0	7	1	4	2	0	6	5	2	6	0	6	5	5	4	8	4	3	3	4	3	4	9	0	3	3	1	9	0	4
2	6	7	4	2	9	7	4	2	4	0	4	5	7	3	2	2	3	6	7	1	7	8	6	3	2	5	8	9	0
5	9	8	1	6	4	2	5	1	7	3	0	3	2	3	8	3	6	1	8	8	0	8	5	9	1	5	4	3	3
2	5	8	9	0	5	8	2	5	4	6	0	2	0	0	1	4	3	7	8	9	9	2	6	3	4	9	0	2	8
6	7	1	3	7	4	0	3	2	5	5	3	3	5	4	1	5	3	7	4	2	4	0	6	3	7	5	4	9	8

e. Consider the digits comprising col. 1: one of the ten possible additive digits, when applied to the cipher digits of col. 1, will yield a set of plaintext digits belonging to the theoretical distribution (given at the end of subpar. b) of our known matrix. This gives us our cue for a modus operandi, and we once again bring to bear the versatile and valuable tool of the generatrix method. The top row of Fig. 118a, below, consists

of the digits of col. 1. In the succeeding nine rows we have completed the normal numerical sequence; this is equivalent to trying all ten digits as additives for the column. In Fig. 118b, we have replaced the digits of Fig. 118a by their deciban equivalents derived in subpar. c.[9] The sums of the log weights given at the right of Fig. 118b provide a means for evalu-

	Generatrices		Decibans		Σ
	6 5 6 4 2 5 0 2 5 2 6		3 1 3 7 1 1 9 1 1 1 3		31
	7 6 7 5 3 6 1 3 6 3 7		0 3 0 1 8 3 1 8 3 8 0		35
	8 7 8 6 4 7 2 4 7 4 8		5 0 5 3 7 0 1 7 0 7 5		40
	9 8 9 7 5 8 3 5 8 5 9		5 5 5 0 1 5 8 1 5 1 5		41
	0 9 0 8 6 9 4 6 9 6 0		9 5 9 5 3 5 7 3 5 3 9		63
1.	1 0 1 9 7 0 5 7 0 7 1		1 9 1 5 0 9 1 0 9 0 1		36
	2 1 2 0 8 1 6 8 1 8 2		1 1 1 9 5 1 3 5 1 5 1		33
	3 2 3 1 9 2 7 9 2 9 3		8 1 8 1 5 1 0 5 1 5 8		43
	4 3 4 2 0 3 8 0 3 0 4		7 8 7 1 9 8 5 9 8 9 7		78
	5 4 5 3 1 4 9 1 4 1 5		1 7 1 8 1 7 5 1 7 1 1		40

Figure 118a. Figure 118b.

ating the relative merits of each decipherment (i.e., each row) in Fig. 118a on the same row as the corresponding log weights in Fig. 118b. The predominantly high score of 78 indicates that the first cipher digit, 6_c, should be a 4_p; therefore the correct additive for col. 1 is 2.

f. The completion diagrams and the log weighting for the next nine columns of the cryptogram in subpar. d are shown below:

	0 9 0 3 5 7 7 6 9 5 7	9 5 9 8 1 0 0 3 5 1 0	41
	1	1 9 1 7 3 5 5 0 9 3 5	48
	2	1 1 1 1 0 5 5 5 1 0 5	25
	3	8 1 8 3 5 9 9 5 1 5 9	63
	4	7 8 7 0 5 1 1 9 8 5 1	52
2.	5	1 7 1 5 9 1 1 1 7 9 1	43
	6	3 1 3 5 1 8 8 1 1 1 8	40
	7	0 3 0 9 1 7 7 8 3 1 7	46
	8	5 0 5 1 8 1 1 7 0 8 1	37
	9	5 5 5 1 7 3 3 1 5 7 3	45

[9] The easiest procedure here is to complete the log sequences vertically, starting at the proper initial point determined by the appropriate digit in the top row of Fig. 118a. If desired, strips may be prepared as an aid in this process.

3.

	5 1 6 8 5 2 1 7 8 8 1										
6	3	1	0	5	3	8	1	5	5	5	1	37
7	0	8	5	9	0	7	8	5	9	9	8	68
8	5	7	5	1	5	1	7	9	1	1	7	49
9	5	1	9	1	5	3	1	1	1	1	1	29
0	9	3	1	8	9	0	3	1	8	8	3	53
1	1	0	1	7	1	5	0	8	7	7	0	37
2	1	5	8	1	1	5	5	7	1	1	5	40
3	8	5	7	3	8	9	5	1	3	3	5	57
4	7	9	1	0	7	1	9	3	0	0	9	46

4.

	4 5 5 1 1 1 4 4 1 9 3										
5	1	3	3	1	1	1	1	1	9	7	29
6	3	0	0	8	8	8	3	3	8	1	1	43
7	0	5	5	7	7	7	0	0	7	1	3	42
8	5	5	5	1	1	1	5	5	1	8	0	37
9	5	9	9	3	3	3	5	5	3	7	5	57
0	9	1	1	0	0	0	9	9	0	1	5	35
1	1	1	1	5	5	5	1	1	5	3	9	37
2	1	8	8	5	5	5	1	1	5	0	1	40
3	8	7	7	9	9	9	8	8	9	5	1	80

5.

	2 7 3 8 3 7 2 2 6 0 7										
3	8	5	7	5	7	5	8	8	0	1	5	59
4	7	5	1	9	1	5	7	7	5	1	5	53
5	1	9	3	1	3	9	1	1	5	8	9	50
6	3	1	0	1	0	1	3	3	9	7	1	29
7	0	1	5	8	5	1	0	0	1	1	1	23
8	5	8	5	7	5	8	5	5	1	3	8	60
9	5	7	9	1	9	7	5	5	8	0	7	63
0	9	1	1	3	1	1	9	9	7	5	1	47
1	1	3	1	0	1	3	1	1	1	5	3	20

6.

	4 8 0 0 5 3 0 9 4 5 4										
5	1	5	1	1	3	7	1	9	1	3	1	33
6	3	9	1	1	0	1	1	1	3	0	3	23
7	0	1	8	8	5	3	8	1	0	5	0	39
8	5	1	7	7	5	0	7	8	5	5	5	55
9	5	8	1	1	9	5	1	7	5	9	5	56
0	9	7	3	3	1	5	3	1	9	1	9	51
1	1	1	0	0	1	9	0	3	1	1	1	18
2	1	3	5	5	8	1	5	0	1	8	1	38
3	8	0	5	5	7	1	5	5	8	7	8	59

	7	7	1	8	1	5	6	7	2	8	0		
	8											5	5	1	5	1	3	0	5	8	5	1	39
	9											5	5	8	9	8	0	5	5	7	9	1	62
	0											9	9	7	1	7	5	5	9	1	1	8	62
	1											1	1	1	1	1	5	9	1	3	1	7	31
7.	2											1	1	3	8	3	9	1	1	0	8	1	36
	3											8	8	0	7	0	1	1	8	5	7	3	48
	4											7	7	5	1	5	1	8	7	5	1	0	47
	5											1	1	5	3	5	8	7	1	9	3	5	48
	6											3	3	9	0	9	7	1	3	1	0	5	41

	5	4	9	6	5	5	5	4	5	2	3		
	6											1	7	5	3	1	1	1	7	1	1	8	36
	7											3	1	9	0	3	3	3	1	3	8	7	41
	8											0	3	1	5	0	0	0	3	0	7	1	20
	9											5	0	1	5	5	5	5	0	5	1	3	35
8.	0											5	5	8	9	5	5	5	5	5	3	0	55
	1											9	5	7	1	9	9	9	5	9	0	5	68
	2											1	9	1	1	1	1	1	9	1	5	5	35
	3											1	1	3	8	1	1	1	1	1	5	9	32
	4											8	1	0	7	8	8	8	1	8	9	1	59
												7	8	5	1	7	7	7	8	7	1	1	59

	5	7	2	2	6	4	2	2	1	5	2		
	6											1	0	1	1	3	7	1	1	1	1	1	18
	7											3	5	8	8	0	1	8	8	1	3	8	53
	8											0	5	7	7	5	3	7	7	8	0	7	56
	9											5	9	1	1	5	0	1	1	7	5	1	36
9.	0											5	1	3	3	9	5	3	3	1	5	3	41
	1											9	1	0	0	1	5	0	0	3	9	0	28
	2											1	8	5	5	1	9	5	5	0	1	5	45
	3											1	7	5	5	8	1	5	5	5	1	5	48
	4											8	1	9	9	7	1	9	9	5	8	9	75
												7	3	1	1	1	8	1	1	9	7	1	40

	0	3	4	6	2	0	6	4	7	4	5		
	1											9	8	7	3	1	9	3	7	0	7	1	55
	2											1	7	1	0	8	1	0	1	5	1	3	28
	3											1	1	3	5	7	1	5	3	5	3	0	34
	4											8	3	0	5	1	8	5	0	9	0	5	44
10.	5											7	0	5	9	3	7	9	5	1	5	5	56
	6											1	5	5	1	0	1	1	5	1	5	9	34
	7											3	5	9	1	5	3	1	9	8	9	1	54
	8											0	9	1	8	5	0	8	1	7	1	1	41
	9											5	1	1	7	9	5	7	1	1	1	8	46
												5	1	8	1	1	5	1	8	3	8	7	48

g. In the generatrices for some of the columns there is only one outstandingly high score which leaves but little doubt as to the validity of the selection of the proper generatrix, such as the high score of 78 for col. 1, 80 for col. 4, and 75 for col. 9.[10] In other columns, such as col. 5 (with three close scores of 63, 60, and 59) and col. 10 (with the close scores of 56, 55, and 54), there are two or more possible choices for the correct generatrix. What we will do is to set down the possible plaintext digits for the first 10 digits of the cryptogram, and try to get started with a good plaintext fragment. From the foregoing generatrix diagrams, the following are the possible plaintext digits for the first 10 ciphers:

	1	2	3	4	5	6	7	8	9	10
C:	6	0	5	4	2	4	7	5	5	0
P:	4	3	7	3	9	4	9	0	3	4
					8		0			0
					3					6

We proceed to take the various possibilities into consideration, and we make trial decipherments as follows:

1. 4/3 7/3 9/4/9/0 3/4/
   E X Q E R O E

2. 4/3 7/3 8/4/9/0 3/4/
   E X T E R O E

3. 4/3 7/3 3/4/9/0 3/4/
   E X ? E R O E

4. 4/3 7/3 9/4/0 0/3 4/
   E X Q E N S

5. 4/3 7/3 8/4/0 0/3 4/
   E X T E N S

On the fifth trial, the beginning of the word EXTENSIVE manifests itself, and we are off to a flying start. We derive the additive, and decipher down the columns, yielding the following decipherments:

[10] In order to appreciate the significance of the scores, we should know the expected score for a correct generatrix, as well as the expected score for an incorrect one. For a correct case, the expected score is calculated by multiplying the probability of each digit by its log weight, summing the products thus obtained; this sum is then multiplied by the number of digits in the generatrix. In a random case, the expected score is the sum of the log weights in the scale (40) divided by 10, multiplied by the number of digits in the generatrix. Thus, the expected score in a correct case is 6.3N, and the random score is 4N, where N is the number of digits in the generatrix. (See also footnote 2 on p. 85.)

2 7 8 1 4 0 7 5 2 6
6 0 5 4 2 4 7 5 5 0.....
4/3 7/3 8/4/0 0/3 4/
E X T E N S

5 9 1 5 7 8 7 4 7 3
3 2/3 4/3 8/0 9/5/7/
S T A C L

6 0 6 5 3 0 1 9 2 4
4/3 8/4/9/0 4/4/0 8/
T E R D E F

4 3 8 1 8 0 8 6 2 6
2/6/0 0/4/0 1/1/0 0/
I N E G U N

2 5 5 1 3 5 1 5 6 2
0 8/7/0 9/5/4/0 4/6/
L A C E D I

5 7 2 1 7 3 5 5 4 0
3 0 4/0 3/3 8/0 2/4/
O T H E

0 7 1 4 2 0 6 5 2 6
8/0 3/3 8/0 9/0 0/0
O T A N

2 6 7 4 2 9 7 4 2 4
0 9/9/3 8/9/0 9/0 8/
R T R A F

5 9 8 1 6 4 2 5 1 7
3 2/0 0/2/4/5/0 9/1/
N B E C A U

2 5 8 9 0 5 8 2 5 4
0 8/0 8/6/5/1/7/3 8/
F I C U L T

6 7 1 3 7 4 0 3 2 5
4/0 3/2/3 4/3 8/0 9/
O B S T A

The rest of the solution follows easily by extending the plain text already recovered.

h. The foregoing figure has given us a clue as to the method to be followed when we have a placed crib, either at the very beginning or the very end of the message. If we had had the probable word EXTENSIVE as a stereotyped beginning, we would have obtained the same results. If, however,

a crib had to be dragged throughout a message, the procedure is quite laborious. In the absence of words, we could drag short plaintext fragments through the cipher, and examine the decipherments at cyclic recurrences of the key.[11] For example, suppose we were to drag TION, represented by the digits 3860300, through the message under examination. If we start TION at the fourth cipher digit (as being the earliest position TION could reasonably be expected to occur), we would get the decipherments shown in Fig. 119a. We then slide the crib over one position, and we get the decipherments shown in Fig. 119b.

```
        1 4 8 7 2 5 0
6 0 5 4 2 4 7 5 5 0 6 9.....
      3 8/6/0 3/0 0
        T I O N
5 9 1 5 7 8 7 4 7 3 4 9
      4/3 0/0 2/2/3
          . H B
6 0 6 5 3 0 1 9 2 4 4 6
      4/9/2/4/7/7/4/
        R B E L L E
4 3 8 1 8 0 8 6 2 6 0 6
      0 4/2/1/4/7/6/
          B U E L I
2 5 5 1 3 5 1 5 6 2 0 6
      0 9/7/4/3 1/2/
          L E V B
5 7 2 1 7 3 5 5 4 0 0 1
      0 3 5/8/3 9/0
            P Q
0 7 1 4 2 0 6 5 2 6 0 6
      3 8/2/9/3 7/6/
          B R X I
2 6 7 4 2 9 7 4 2 4 0 4
      3 8/1/0 2/7/4/
          U H L E
5 9 8 1 6 4 2 5 1 7 3 0
      0 2/6/5/3 6/7/
          I C Y L
2 5 8 9 0 5 8 2 5 4 6 0
      8/6/7/1/0 0/4/
        I L U N E
6 7 1 3 7 4 0 3 2 5 5 3
      2/3 6/3 1/7/5/
          Y V L C
```

Figure 119a.

```
        9 6 1 5 2 0 6
6 0 5 4 2 4 7 5 5 0 6 9.....
      3 8/6/0 3/0 0
        T I O N
5 9 1 5 7 8 7 4 7 3 4 9
      8/2/6/9/5/3 8/
          B I R C T
6 0 6 5 3 0 1 9 2 4 4 6
      4/4/0 4/0 4/8/
          E D D P
4 3 8 1 8 0 8 6 2 6 0 6
      9/4/7/1/0 6/4/
          E L U K E
2 5 5 1 3 5 1 5 6 2 0 6
      4/9/0 0/4/2/4/
          R N E B E
5 7 2 1 7 3 5 5 4 0 0 1
      8/7/4/0 2/0 4/
          L E H D
0 7 1 4 2 0 6 5 2 6 0 6
      3 4/5/0 0/6/4/
            C N I E
2 6 7 4 2 9 7 4 2 4 0 4
      3 3 6/9/0 4/4/
            R D E
5 9 8 1 6 4 2 5 1 7 3 0
      7/8/1/0 9/7/7/
          P U A R R
2 5 8 9 0 5 8 2 5 4 6 0
      1/9/7/7/3 4/0
          R L L S
6 7 1 3 7 4 0 3 2 5 5 3
      8/8/9/8/0 5/9/
          P R P M R
```

Figure 119b.

[11] The procedure here would be to derive a trial additive and write this additive on a slip of paper, then slide the additive down the column, noting what decipherments result. These decipherments are then partitioned into monomes and dinomes as far as possible, and the equivalent plaintext letters are judged as to their relative merits.

The patient cryptanalyst will, on the 136th trial, reap his just reward when he finally uncovers the following stretches of good English plain text:

```
                                                3 4 9 1 8 6 3
6 0 5 4 2 4 7 5 5 0 6 9 0 6 0 7 5 3 6 2 5 4 6 6 2 1 5 4 5 7
                                                3 8/6/3 8/0 9/
                                                  I T   A

5 9 1 5 7 8 7 4 7 3 4 9 3 1 6 8 5 3 4 7 7 1 0 0 1 5 4 0 9 2
                                                1/3 8/0 2/4/8/
                                                  T   H E P

6 0 6 5 3 0 1 9 2 4 4 6 9 5 4 2 8 7 3 3 9 1 8 0 3 6 5 3 4 7
                                                0 9/0 0/0 4/0
                                                    N   D

4 3 8 1 8 0 8 6 2 6 0 6 3 5 4 1 3 6 7 4 1 1 7 9 4 5 7 8 3 7
                                                4/0 2/0 9/3 1/
                                                  H   A   V

2 5 5 1 3 5 1 5 6 2 0 6 7 2 3 1 9 9 6 2 5 1 1 6 3 4 9 7 7 7
                                    /3 8/6/0 3/0 0/
                                      T I O   N

5 7 2 1 7 3 5 5 4 0 0 1 9 5 3 2 8 1 3 8 9 0 8 1 3 0 5 5 3 0
                                                0 4/0 9/0 5/0
                                                    A   M

0 7 1 4 2 0 6 5 2 6 0 6 5 5 4 8 4 3 3 4 3 4 9 0 3 3 1 9 0 4
                                                0 0 4/3 1/4/0
                                                      V E

2 6 7 4 2 9 7 4 2 4 0 4 5 7 3 2 2 3 6 7 1 7 8 6 3 2 5 8 9 0
                                                3 3 2/6/0 0/0
                                                    I N

5 9 8 1 6 4 2 5 1 7 3 0 3 2 3 8 3 6 1 8 8 0 8 5 9 1 5 4 3 3
                                                8/4/9/9/0 9/6/
                                                  E R R A I

2 5 8 9 0 5 8 2 5 4 6 0 2 0 0 1 4 3 7 8 9 9 2 6 3 4 9 0 2 8
                                                4/4/0 8/4/0 0/
                                                  E F E N

6 7 1 3 7 4 0 3 2 5 5 3 3 5 4 1 5 3 7 4 2 4 0 6 3 7 5 4 9 8
                                                4/0 3/3 2/0 0/
                                                  O W   N
```

Figure 119c.

If we were unlucky with TION, we would try other polygraphic cribs. As a last resort, we might even have to be content with dragging the digit equivalents of plaintext digraphs, such as TH, IN, ON, etc. (Digraphs such as RE and ER would be unsatisfactory, because the component letters are represented in the rectangle by monomes, so our decipherments would be next to useless--in fact, useless.)

i. As an illustration of the effectiveness of testing even a short crib through a cipher text, let us consider dragging the digraph TH (which has the tetranome equivalent 3802) through the message we have been using as an example. In Fig. 120a, below, we assume that TH begins the message;

	Scores
3 2 5 2	
6 0 5 4 2 4 7 5 5 0.....	
3 8/0 2/	
T H	
5 9 1 5 7 8 7 4 7 3	
2/7/6/3	
L I	7,8
6 0 6 5 3 0 1 9 2 4	
3 8/1/3	
U	6
4 3 8 1 8 0 8 6 2 6	
1/1/3 9/	
U Q	6,2
2 5 5 1 3 5 1 5 6 2	
9/3 0/9/	
. R	8
5 7 2 1 7 3 5 5 4 0	
2/5/7/9/	
C L R	7,7,8
0 7 1 4 2 0 6 5 2 6	
7/5/6/2/	
C I B	7,8,4
2 6 7 4 2 9 7 4 2 4	
9/4/2/2/	
E B B	9,4,4
5 9 8 1 6 4 2 5 1 7	
2/7/3 9/	
L Q	7,2
2 5 8 9 0 5 8 2 5 4	
9/3 3/7/	
? L	ø,7
6 7 1 3 7 4 0 3 2 5	
3 5/6/1/	
I U	7,6
	125

Figure 120a.

	Scores
4 9 1 8	
.....7 5 3 6 2 5 4 6 6 2.....	
8/6/3 8/	
I T	8,9
8 5 3 4 7 7 1 0 0 1	
3 8/0 2/	
T H	
2 8 7 3 3 9 1 8 0 3	
9/0 0/0	
N	8
1 3 6 7 4 1 1 7 9 4	
0 2/0 9/	
A	8
1 9 9 6 2 5 1 1 6 3	
8/6/0 3/	
I O	8,8
2 8 1 3 8 9 0 8 1 3	
4/0 9/0	
A	8
8 4 3 3 4 3 4 9 0 3	
0 4/3 1/	
V	5
2 2 3 6 7 1 7 8 6 3	
3 2/6/0	
I	8
8 3 6 1 8 8 0 8 5 9	
4/9/9/0	
R R	8,8
1 4 3 7 8 9 9 2 6 3	
4/0 8/4/	
F E	6,9
1 5 3 7 4 2 4 0 6 3	
0 3/3 2/	
W	5
	106

Figure 120b.

we derive the additive and decipher down the columns, and we partition the intermediate plain text as far as we can with assurance--then we decrypt the partitioned plain as shown. In Fig. 120b, where the TH happens to be placed correctly (starting at the 50th digit), we get the decipherments shown in that figure. With so much depth, it is no problem to pick out the correct case by eye from among a set of trials. If, however, the cryptanalyst were

testing a much shallower depth (i.e., fewer repetitions of the keying cycle), a statistical weighting of the decipherments would be necessary to enable recognition of the best case or cases from among the many trials. The scoring of the decipherments in Figs. 120a and b is accomplished by assigning to the deciphered plaintext letters (less the original TH) the deciban weights given in subpar. 34c (excluding the period for which no weight has been calculated), summing these weights, and dividing by the number of monomes and dinomes exposed in the partitioning process--this yields an average for the column. Thus, in Fig. 120a, the sum of the weights of the decrypted plaintext letters (including a weight of ϕ for the nonexistent dinome 33), is 125; the number of intermediate plaintext groupings (excluding the dinome 30 representing a period) is 21; therefore the average score is $\frac{125}{21} = 6.0$. In the case of Fig. 120b, the sum of the weights of the decrypted letters is 106, which when divided by 14 (the number of intermediate plaintext groupings in this case) gives an average of 7.6. Since the expected average score for an incorrect case is 5.8, and the expected average score for a correct case is 7.6,[12] it is clear that Fig. 120a is no better than random, while Fig. 120b is in all probability valid and can be used to extend further plain text.

88. Analysis involving isologs.--a. In enciphered monome-dinome systems, attacks based on the exploitation of isologs are particularly valuable, especially in those cases wherein the monome-dinome matrix has a low I.C., or where coordinates or additive keys are changed so frequently that not enough homogeneous traffic is available for study. Several typical examples of isolog attacks will be presented in the succeeding subparagraphs.

b. Let the following two message be examined:

Message "A"

80404	31105	22961	61428	00434	28663	47839	25767	04100	20012
07149	90313	87161	34078	16767	04100	20681	06449	73411	56005
13305	20885	09483	46222	99725	01138	00999	03729	43177	53265
12159	65970	19302	33919	12775	00560	33436	82551		

Message "B"

04378	88147	20798	22772	39352	81140	51367	49631	51142	28849
68493	29231	40648	48506	30631	51142	28418	67793	02339	19582
27833	44759	56425	44059	50079	30056	63476	17257	67041	00207
10986	26224	48220	96496	26203	24434	80478	80388		

Both messages are of the same length, and both messages have a long internal repetition beginning with the 38th and 73d digits; furthermore, there is a long repetition between the two messages, beginning with the 162d digit of Message "A" and the 89th digit of Message "B". These phenomena, among others, confirm the period as 35, show that the messages are isologs, and indicate that Message "B" is +3 on the keying cycle with respect to Message "A".

[12] Derivation of these constants has been shown in footnote 2 on p. 85.

c. The messages are now written out as follows:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
8	0	4	0	4	3	1	1	0	5	2	2	9	6	1	6	1	4	2	8	0	0	4	3	4	2	8	6	6	3	4	7	8	3	,
2	5	7	6	7	0	4	1	0	0	2	0	0	1	2	0	7	1	4	9	9	0	3	1	3	8	7	1	6	1	3	4	0	7	8
1	6	7	6	7	0	4	1	0	0	2	0	6	8	1	0	6	4	4	9	7	3	4	1	1	5	6	0	0	5	1	3	3	0	5
2	0	8	8	5	0	9	4	8	3	4	6	2	2	2	9	9	7	2	5	0	1	1	3	8	0	0	9	9	9	0	3	7	2	9
4	3	1	7	7	5	3	2	6	5	1	2	1	5	9	6	5	9	7	0	1	9	3	0	2	3	3	9	1	9	1	2	7	7	5
0	0	5	6	0	3	3	4	3	6	8	2	5	5	1																				

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
			0	4	3	7	8	8	8	1	4	7	2	0	7	9	8	2	2	7	7	2	3	9	3	5	2	8	1	1	4	0	5	1
3	6	7	4	9	6	3	1	5	1	1	4	2	2	8	8	4	9	6	8	4	9	3	2	9	2	3	1	4	0	6	4	8	4	8
5	0	6	3	0	6	3	1	5	1	1	4	2	2	8	4	1	8	6	7	7	9	3	0	2	3	3	9	1	9	5	8	2	2	7
8	3	3	4	4	7	5	9	5	6	4	2	5	4	4	0	5	9	5	0	0	7	9	3	0	0	5	6	6	3	4	7	6	1	7
2	5	7	6	7	0	4	1	0	0	2	0	7	1	0	9	8	6	2	6	2	2	4	4	8	2	2	0	9	6	4	9	6	2	6
2	0	3	2	4	4	3	4	8	0	4	7	8	8	0	3	8	8																	

We will assume arbitrarily that the additive for col. 1 is $\emptyset$; this makes the first digit of Message "A" an 8_p. The first digit of Message "B" must also be an 8_p, so the additive for col. 4 is 2, which makes the 4th digit of Message "A" a $\emptyset$. This criss-cross process is continued, until the entire additive is recovered. The recovery of the entire additive is possible here because the displacement interval of the two messages, 3, is not a factor of or has no multiple in common with the period, 35. If the displacement interval had been, say, 14, the common factor (7) would have resulted in a closed chain of additives for cols. 1, 8, 15, 22, and 29; thus there would be 7 distinct chains in all.

d. After the additive has been recovered in the foregoing problem, Message "A" is reduced to monoalphabetic terms; this is shown below, together with the recovered additive:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
0	3	4	2	7	3	9	1	8	6	1	2	8	1	0	6	4	7	2	5	0	7	9	3	6	8	5	4	4	8	9	2	5	0	6
8	7	0	8	7	0	2	0	2	9	1	0	1	5	1	0	7	7	0	3	0	3	5	0	8	4	3	2	2	5	5	5	3	3	3
2	2	3	4	0	7	5	0	2	4	1	8	2	0	2	4	3	4	2	4	9	3	4	8	7	0	2	7	2	3	4	2	5	7	2
1	3	3	4	0	7	5	0	2	4	1	8	8	7	1	4	2	7	2	4	7	6	5	8	5	7	1	6	6	7	2	1	8	0	9
2	7	4	6	8	7	0	3	0	7	3	4	4	1	2	3	5	0	0	0	0	4	2	0	2	2	5	5	5	1	1	1	2	2	3
4	0	7	5	0	2	4	1	8	9	0	0	3	4	9	0	1	2	5	5	1	2	4	7	6	5	8	5	7	1	2	0	2	7	9
0	7	1	4	3	0	4	3	5	0	7	0	7	4	1																				

The presence of the dinome 22 before and after the tripled digits[13] in two portions of the message makes the assumption of 2 as a row coordinate reasonable, and the four consecutive occurences of the digit $\emptyset$ makes this also a likely row coordinate. When the intermediate plain text is partitioned according to this hypothesis, the message plain text can be recovered easily,

[13] See footnote 3 on p. 191 of Military Cryptanalytics, Part I.

beginning with the words TO COMMANDING OFFICER... The matrix is reconstructed as follows:

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

e. The period of the isologs in subpar. b, above, was determined from the occurrence of a long internal polygraphic repetition within each message. If this repetition had not been present, we still could have factored the isologs by superimposing them and subtracting the cipher of Message "A" from that of Message "B". Since the plain text of the two messages is identical, these differences will represent the difference between the key digits at an interval corresponding to the relative displacement of the isologs; therefore these differences will repeat at an interval corresponding to the length of the period. The beginnings of the messages and their differences are shown in the following diagram:

"B":	04378	88147	20798	22772	39352	81140	51367	49631	51142	28849...
"A":	80404	31105	22961	61428	00434	28663	47839	25767	04100	20012...
	24974	57042	08837	61354	39928	63587	14538	24974	57042	08837

The differences repeat at an interval of 35 digits, revealing the length of the period. Note that the sequence of these differences is identical to the delta (or lateral differences) of the additive at an interval of 3 (i.e., the displacement interval of the two messages). If we take the delta at an interval of 3 of the key shown in subpar. d, we will obtain the stream 24974..., which is the same as the differences just derived above. If we had subtracted Message "B" from Message "A", we would of course have obtained the complements of these differences.

f. Isologs involving identical matrices and coordinates, but having additive keys of different lengths and composition, are readily susceptible to attack providing the additive lengths are relatively prime. As a demonstration of this, let us suppose that we have a pair of isologs, factoring to 15 and 16, respectively. The first 80 digits of the message are shown in Figs. 121a and b, below:

Message "A"

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

Figure 121a.

Message "B"

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

Figure 121b.

If we assume an arbitrary additive of ∅ for the first column of Message "A", we get the decipherments shown in Fig. 122a. These decipherments are now cribbed into Message "B", as shown in Fig. 122b together with the derived additive; this latter is used to decipher more digits in Message "B", and these decipherments in turn are cribbed into Message "A", and so on until

Message "A"

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
∅														
8	1	7	3	8	6	3	3	5	1	0	5	0	3	8
8														
0	1	4	5	4	6	4	8	3	0	3	8	1	0	2
0														
5	9	0	8	4	8	3	6	7	2	6	0	9	0	1
5														
1	2	9	5	3	0	4	7	5	6	8	8	3	6	4
1														
0	6	4	7	4	0	3	8	0	4	0	8	2	2	7
0														
7	9	7	7	5	.....									
7														

Figure 122a.

Message "B"

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

Figure 122b.

all the intermediate plain text has been recovered.[14]

g. The foregoing situation is easily exploitable no matter what the lengths of the periods are, so long as they are prime to each other. If the lengths of the periods are not relatively prime, the general approach in the previous subparagraph may still be used, if not to reduce the text to monoalphabetic terms, at least to reduce the text to several sets of families which might then be amalgamated by other means. In passing, it might be pointed out that a difference of 1 in the lengths of additives of a pair of isologs might arise from an error in copying out the additive, resulting in an added or a dropped digit.

g. In the next situation, we will assume that we have a pair of messages factoring to 15, having identical beginnings 20 digits long. The first 80 digits of these messages are given below:

Message "A"

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

Figure 123a.

Message "B"

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

Figure 123b.

[14] The plain text and basic matrix in this example are the same as those given in the preceding subparagraph.

Let us take the difference stream (designated as "Δ") for the two messages at an interval corresponding to the period. If each row is subtracted from the row immediately beneath, we have the following:

Δ, Message "A"

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

Figure 124a.

Δ, Message "B"

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

Figure 124b.

The difference streams for the two messages, beginning with the 19th digit of the Δ for Message "A" and the 21st digit of the Δ for Message "B", are identical. This is clear proof that the two messages are isologs;[15] the messages start out with the same plain text enciphered with identical keys, and then evidently a 2-digit stagger takes place. If we assume an arbitrary additive of ∅ for column 1, we derive plaintext values which can be cribbed from one message to the other, and both messages can be reduced to monoalphabetic terms, as in subpar. f, above. The cause of the error, after the intermediate plain text is solved, is discovered to be that, in Message "A", an F_p (=∅3) was left out of the word OFFICER, thus producing a stagger situation at an offset of 2 digits.

i. In the foregoing situation, the possibility that the two messages are isologs might have been indicated by their near-correspondence in length, Message "A" being two digits shorter than Message "B". But even if the texts of the two messages diverged completely after the 80 digits shown in Figs. 123a and b, the length of the exact correspondence of plain text would be revealed by the delta streams as shown in Figs. 124a and b, and solution would still go on as before. This is one more demonstration of the value of stagger situations, once they are recognized and exploited.

j. For the last example of an isolog situation, we will treat the case where a cipher clerk incorrectly enciphered a message using the equation P - K = C (i.e., corresponding to the deciphering equation) instead of the correct P + K = C, and subsequently he sent the corrected version.

(1) Let us examine the following pair of messages. (For the sake of illustration, we will assume the matrix to be known, and that it is the REPUBLIC matrix of subpar. 86h.)

[15] If these messages had been very short, both their periods and the fact that they are isologs could have been discovered by taking their individual difference streams at various intervals corresponding to trial periods; when a period of 15 was tried, we would have gotten the results as shown above.

Message "A"

77421	29282	51449	98657	94622	91878	57896	14694	85074	34064
24606	42952	61890	94115	05362	50380	91241	69655	52623	97711

Message "B"

11685	81828	31247	92253	14086	75038	99034	98098	23472	96842
48022	88116	29870	74575	67308	98706	95465	47095	96463	73999

All the differences of the corresponding digits between the two messages are even, pointing to the type of error involved. The length of the key is not known, nor can it be determined from the two messages at hand; nevertheless, solution of the plain text will proceed without knowing this length, and the additive will be recovered as the very last step in the process.

(2) The first thing we will do is add the two cipher texts, as shown below; this has the effect of giving us 2P, or twice the value of the plain-

C_1:	77421	29282	51449	98657	94622	91878	57896	14694	85074	34064
C_2:	11685	81828	31247	92253	14086	75038	99034	98098	23472	96842
2P:	88006	00000	82686	80000	08608	66806	46820	02682	08446	20806
P:	44003	00000	41343	40000	04304	33403	23410	01341	04223	10403
	99558	55555	96898	95555	59859	88958	78565	56896	59778	65958

C_1:	24606	42952	61890	94115	05362	50380	91241	69655	52623	97711
C_2:	48022	88116	29870	74575	67308	98706	95465	47095	96463	73999
2P:	62628	20068	80660	68680	62660	48086	86606	06640	48086	60600
P:	31314	10034	40330	34340	31330	24043	43303	03320	24043	30300
	86869	65589	95885	89895	86885	79598	98858	58875	79598	85855

text digit for each position, vitiating the effect of the key. Next, this value of 2P is decomposed into the two possible plaintext digits it can represent (for instance, a 2P of 8 could arise from a 4 + 4, or a 9 + 9). Then, knowing the matrix, it is a simple matter to recover the original plain text from the double stream of intermediate plaintext digits. The message text is recovered, beginning with the words RECONNAISSANCE PATROLS. Finally, the actual intermediate plain text is set against the cipher text of Message "B", and it is found that the additive is a 51-digit repeating sequence.[16]

(3) If the matrix were not known, it still might be possible to analyze the double plaintext stream if a favorable crib began the message. In the previous example, the probable word RECONNAISSANCE will permit the identification of the two row coordinates (in variant form, of course) and the equivalents for the 8 letters; but unless there are enough different letters in the

[16] This sequence is the value of e, the base of natural or Napierian logarithms, 2.71828...., taken to 50 decimals. There have been cases in cryptographic practice when key digits have been obtained from mathematical tables (such as tables of logarithms, trigonometric functions, etc.), or have been derived from a fraction yielding a long repeating decimal, or have been generated by some mathematical formula. In other cases, key has been derived from literal text by enciphering the latter with the monome-dinome rectangle, similar to the Nihilist method treated in the preceding chapter.

crib, it will be very difficult to recover the remainder of the plain text from the several variant decipherments for the rest of the cipher text.[17] In any case, the row- and column coordinates cannot be determined uniquely, but may be recovered on a relative base because of the variant aspects inherent in the solution.

89. Additional remarks.--a. In the examples in the preceding paragraphs, only one type of monome dinome matrix has been used; viz., matrices with two row coordinates. Of course, any type of monome-dinome matrix (such as one of those given in par. 75, Military Cryptanalytics, Part I) might have been used for producing the intermediate text, but this is immaterial insofar as the general methods for reducing to monoalphabetic terms are concerned. What does matter, as has already been remarked in subpar. 85d, is the theoretical I.C. of the intermediate text produced by a specific matrix. Several cases will be cited in the subparagraphs following.

b. The REPUBLIC matrix illustrated in pars. 86 and 87 has an I.C. of 1.62, calculated from the expected frequencies of the digits given in subpar 87b. The sum (N) of these frequencies is 1590; the ϕ_o, which is $\Sigma f(f-1)$, is 410,098. Since the formula for the δ I.C. is $\frac{c \Sigma f(f-1)}{N(N-1)}$, where c is the number of categories (in this case, 10), the δ I.C. is $\frac{10(410,098)}{1590 \cdot 1589} = 1.62$.

c. The I.C. of a particular matrix depends not only on what letters constitute the monome row, but also on the composition and arrangement of the letters in the dinome rows with respect to the letters in the monome row. Thus, in the following two matrices, Fig. 125a has an I.C. of 1.14,

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

Figure 125a.

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

Figure 125b.

while Fig. 125b has an I.C. of 1.16. The theoretical lower and upper limits of I.C.'s for matrices with two row coordinates are 1.02 and 2.10; these are the I.C.'s of the matrices in Figs. 125c and d, respectively, given below:

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

Figure 125c.

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

Figure 125d.

[17] This is similar to the process of solution of the Edgar Allen Poe cipher with variant plaintext values (cf. footnote 2, subpar. 2d), except that in this case the process is considerably more complicated in its application to monome-dinome ciphers.

Where the monome row consists of a key word, it has been found that the I.C.'s of such matrices are usually in the vicinity of 1.30 to 1.50, for what this generalization of the range might be worth.

d. Matrices with more than two row coordinates should be expected to have higher I.C.'s than matrices with only two row coordinates; however, in the matrix below, which has been manipulated to yield the lowest possible theoretical I.C., we get an I.C. of 1.00.[18]

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

Figure 125e.

e. In subpar. 86b we noted that the I.C. of the 440 digits of the cipher text, when written out on a width of 20, yielded an I.C. of 1.22, remarking that this I.C. "seems surprisingly good for a random case, if it is random." We subsequently found out that the correct width for this cryptogram was 30, so the reason for the "surprisingly good" I.C.[19] is now clear: on a width of 20 each column is actually composed not of an assortment of digits belonging to all possible families (and therefore possessing random characteristics), but of digits belonging to only three of these families.[20] If we had written out the cipher on a width of 15, we would

---

[18] If the expected value of the δ I.C. for this matrix were calculated using the theoretical frequencies (reduced to 1000 letters) given in subpar. 87b, it would be found to be 0.995, which is a mathematical absurdity since, by definition, the random I.C. is 1.00 and no sampling (with replacement) from a population could possibly have an expected I.C. of less than 1.00. The error present here is caused by discrepancies in rounding off to a base of 1000 the actual frequencies of an observed sample of 50,000 letters. A true picture of the estimated I.C. can be obtained by using a statistic known as the "gamma I.C.", derived by the formula γ I.C. $= \frac{c \sum f^2}{N^2}$, which turns out to be 1.002 for this case. The difference between the δ I.C. and the γ I.C. approaches $\emptyset$ as N grows large--if the actual frequencies of the 50,000 letters had been used, the δ I.C. would have been identical to the γ I.C. The δ I.C. suffices for most purposes, and is in fact preferable in treating small samples, since it gives an unbiased estimate of the roughness, independent of sample size.

[19] The reader with a background in statistics will realize that the phrase "surprisingly good" is certainly an understatement, to say the least. It can be shown that the sigmage of this I.C. is $\frac{440(1.22-1.00)}{\sqrt{2(20-9)}} = 5.1\sigma$, which may be translated as odds of 1 chance in 200,000. (We use here the χ^2 distribution for an evaluation of the sigmage, not the Normal [Gaussian] distribution, since it has been established that the χ^2 estimate is closer to the true value than is the Normal estimate.) This certainly shows that causal factors are responsible for this I.C.; but in view of the explanation given, it also shows the student that he must use cryptomathematics intelligently--not blindly jump to conclusions when he gets a high score in a particular test. The I.C. of 1.22 is doubtlessly causal, but it is not the right answer.

[20] Since our distributions consist of the merger of three separate families or distributions, the expected I.C. (when the families are equiprobable) is 1.00 plus one-third of the "bulge" between the I.C. of random and the I.C. of the matrix. In this case, the REPUBLIC matrix has a theoretical I.C. of 1.62, therefore on a width of 20 the expected I.C. is $1.00 + \frac{.62}{3} = 1.21$.

have obtained an I.C. of 1.27, understandable since each column is now composed of digits from only two families instead of digits from the total population of equiprobable families.[21]

f. The application to enciphered monome-dinome systems of the delta-stream method[22] is quite possible, but it is usually less likely to produce clear-cut exploitable results than in the case of enciphered dinome systems.

g. Dinome and split dinome counts might theoretically be useful in equating columns in enciphered monome-dinome systems; however, in actual practice if there is enough material to use these methods with confidence, there is also usually enough material to equate columns by means of monomic distributions. Nevertheless, in difficult cases the cryptanalyst might have no choice but to use these methods.

h. The higher the I.C. of the underlying monome-dinome matrix, the less material is generally necessary for the successful equating of columns. Thus, in subpar. 86c, it is possible to equate the columns of Message "A" without Message "B", but not without considerable trouble.

i. In systems employing matrices of very low I.C.'s (such as an I.C. of 1.02 for the matrix in Fig. 125c), the monomic roughness is not significantly above random to permit the use of the monomic δ I.C. in establishing the period or in equating columns. Nevertheless, the pronounced dinomic roughness inherent in all monome-dinome systems is enough to enable the factoring and subsequent equating of columns, given sufficient material.

j. It might not be amiss to observe that additive-enciphered dinome systems employing a single-digit word separator will give rise to manifestations of an additive-enciphered monome-dinome system. The processes of factoring and equating of columns here will be pursued as in monome-dinome systems, until the evidence of such a word-separator usage is uncovered and exploited.

k. Note that, in the two messages given in subpar. 86a et seq., Message "B" begins at the very next position in the keying cycle where Message "A" stopped. This phenomenon, known as tailing, can be used to "set" messages along the keying cycle without resort to exhaustive trials to prove the correct superimposition, if it has been observed that traffic emanating from a particular originator exhibits a high incidence of this situation.

l. This chapter has concerned itself entirely with additive-enciphered monome-dinome systems as illustrations of the methods of attack on periodic encipherments of mixed-length intermediate plaintext elements. It is clear, however, that the general approaches treated apply equally well in those cases where the intermediate plain text is composed of dinomes and trinomes, or other similar variations of mixed-length systems.

---

[21] The expected I.C. in this case is $1.00 + \frac{.62}{2} = 1.3$, as explained in footnote 20, above.

[22] Cf. subpar. 83l.

m. The observations made in subpar. 84b with respect to additive, subtractive, and minuend encipherments in the systems of the preceding chapter of course also apply to monome-dinome systems.

n. As a final remark, it might be noted that situations wherein the composition of the matrix is known, but the coordinates are unknown, is not of much help in attacking a cryptogram in the initial stages, unless a crib is also available.[23] As an example, let us consider the following cryptogram, factoring to 35:

```
 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35
 8 0 4 0 4 3 1 1 0 5 2 2 9 6 1 6 1 4 2 8 0 0 4 3 4 2 8 6 6 3 4 7 8 3 9
 2 5 7 6 7 0 4 1 0 0 2 0 0 1 2 0 7 1 4 9 9 0 3 1 3 8 7 1 6 1 3 4 0 7 8
 1 6 7 6 7 0 4 1 0 0 2 0 6 8 1 0 6 4 4 9 7 3 4 1 1 5 6 0 0 5 1 3 3 0 5
 2 0 8 8 5 0 9 4 8 3 4 6 2 2 2 9 9 7 2 5 0 1 1 3 8 0 0 9 9 9 0 3 7 2 9
 4 3 1 7 7 5 3 2 6 5 1 2 1 5 9 6 5 9 7 0 1 9 3 0 2 3 3 9 1 9 1 2 7 7 5
 0 0 5 6 0 3 3 4 3 6 8 2 5 5 1
```

It will be assumed that the enemy has been using a matrix with internal

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

Figure 126.

composition as shown in Fig. 126, above, but that we are faced with unknown coordinates. It is further believed that the cryptogram begins with the opening stereotype "TO COMMANDING OFFICER."

(1) It will be noted that the plaintext letters of the crib C, M, D, G, and F must all come from the same row of the matrix; therefore the first digits of all these dinome equivalents must be identical. If we arbitrarily assume this digit to be plaintext ϕ, we derive the relative additive for the appropriate columns which we use to decipher down the columns. Thus:

[23] Even in simple monoalphabetic substitution, a known plain component is of no assistance in the early stages; and in later stages is helpful only if the cipher component has been derived in some systematic fashion.

~~CONFIDENTIAL~~

```
1 2  3  4 5  6  7  8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35
     4     3  1        2        6     2  0     3
8 0 4 0 4 3 1 1 0 5 2 2 9 6 1 6 1 4 2 8 0 0 4 3 4 2 8 6 6 3 4 7 8 3 9
  / /0  / /0  /0  / / /0  / / /0  / /0  /0  / /0  / / /
T O  C  O M  M  A N  D  I N  G  O F  F  I  C  E R
2 5 7 6 7 0 4 1 0 0 2 0 0 1 2 0 7 1 4 9 9 0 3 1 3 8 7 1 6 1 3 4 0 7 8
    3  7  0        8        4     2  9     8

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

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

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

0 0 5 6 0 3 3 4 3 6 8 2 5 5 1
    1  0  3        0
```

We will call this family of columns the "α" family, for convenience. The distribution for the decipherments of the α family, excluding the digits from the original crib, is as follows:

$$\phi\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9$$

(2) Since T_p and C_p come from the same column of the matrix, it is obvious that cols. 1, 4, and 25 belong to one family; likewise, since O_p and G_p come from the same column of the matrix, it is clear that cols. 2, 5, 17, and 18 belong to one family, different from the two other families just established. By examining the plaintext letters composing the original crib, we will arrive at the following designation of families:

T	O	C	O	M	M	A	N	D	I	N	G	O	F	F	I	C	E	R
β	γ	$\alpha\beta$	γ	$\alpha\delta$	$\alpha\delta$	ε	ζ	$\alpha\zeta$	η	ζ	$\alpha\gamma$	γ	$\alpha\theta$	$\alpha\theta$	η	$\alpha\beta$	ι	θ

A total of 12 families is possible, which may be collapsed eventually into 10 families representing the equivalents for the 10 digits.

(3) Since the γ family is the heaviest family, next to α, we will take a distribution of the γ family equated in terms of an arbitrary additive ϕ for col. 2, again excluding the elements derived from the assumed crib. This is as follows:

$$\phi\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9$$

We will now perform a cross-products sum test between the distribution for α and all possible slides for γ; this is shown below:

	9 3 3 5 4 1 - 6 4 1	
1:	1 - 5 1 3 3 1 1 - 3	53
2:	- 5 1 3 3 1 1 - 3 1	59
3:	5 1 3 3 1 1 - 3 1 -	99
4:	1 3 3 1 1 - 3 1 - 5	47
5:	3 3 1 1 - 3 1 - 5 1	68
6:	3 1 1 - 3 1 - 5 1 3	83
7:	1 1 - 3 1 - 5 1 3 3	52
8:	1 - 3 1 - 5 1 3 3 1	59
9:	- 3 1 - 5 1 3 3 1 1	56

It is apparent that γ is at a slide of 3 with respect to α; the combined distribution for $(\alpha + \gamma)$ is therefore as follows:

∅	1	2	3	4	5	6	7	8	9
▪	▪	▪	▪	▪	▪		▪	▪	▪
▪		▪	▪				▪		
▪									

(4) The work sheet for the cryptogram will now look like this:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
β	γ	α	β	γ	α	δ	α	δ	ε	ζ	α	ζ	~	ζ	α	γ	γ	α	θ	α	θ	η	α	β	ι	θ								
	3	4		7	3		1				2				6	4	7	2		0			3											
8	0	4	0	4	3	1	1	0	5	2	2	9	6	1	6	1	4	2	8	0	0	4	3	4	2	8	6	6	3	4	7	8	3	9
	/7	/0		/7	/0		/0		/	/	/0		/	/	/0	7	/7	/0		/0		/	/0		/	/								
T	O		C	O	M		M	A	N		D		I	N	G		O		F		F	I		C	E	R								
2	5	7	6	7	0	4	1	0	0	2	0	0	1	2	0	7	1	4	9	9	0	3	1	3	8	7	1	6	1	3	4	0	7	8
	2	3		0	7		0				8				4	3	4	2		9			8											
1	6	7	6	7	0	4	1	0	0	2	0	6	8	1	0	6	4	4	9	7	3	4	1	1	5	6	0	0	5	1	3	3	0	5
	3	3		0	7		0				8				4	2	7	2		7			8											
2	0	8	8	5	0	9	4	8	3	4	6	2	2	2	9	9	7	2	5	0	1	1	3	8	0	0	9	9	9	0	3	7	2	9
	7	4		8	7		3				4				3	5	0	0		0			0											
4	3	1	7	7	5	3	2	6	5	1	2	1	5	9	6	5	9	7	0	1	9	3	0	2	3	3	9	1	9	1	2	7	7	5
	0	7		0	2		1				0				0	1	2	5		1			7											
0	0	5	6	0	3	3	4	3	6	8	2	5	5	1																				
	7	1		3	0		3				0																							

At this point the 10-digit repetition in the second and third lines is examined. If the 07 is a proper dinome, it represents G_p; and the repetition is just the right length for the assumption of REGIMENT. (Furthermore there is a hit with the cipher dinome 10 which is an M_p from COMMANDING.) This gives us $R_p = 3$, and $T_p = 8$; therefore $C_p = 08$ (cols. 4 and 25), which yields, in col. 4, $E_p = 4$. Substituting $E_p = 4$ in cols. 10 and 26, $T_p = 8$ in col. 1, and $R_p = 3$ in col. 27, we now get the following:

~~CONFIDENTIAL~~

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35
β γ α β γ α δ α δ ε ζ α ζ η ζ α γ γ α θ α θ η α β ι θ
0 3 4 2 7 3   1   6   2       6 4 7 2   0     3 6 8 5
8 0 4 0 4 3 1 1 0 5 2 2 9 6 1 6 1 4 2 8 0 0 4 3 4 2 8 6 6 3 4 7 8 3 9
8/7/0 8/7/0  /0  /9/ /0  / / /0 7/7/0  /0  / /0 8/4/3/
T O C O M   M A N D I N G O F   F I C E R
2 5 7 6 7 0 4 1 0 0 2 0 0 1 2 0 7 1 4 9 9 0 3 1 3 8 7 1 6 1 3 4 0 7 8
2 2/3/4/0 7/ /0  /4/ /8/     4 3 4 2   9     8 7 0 2
  R E G I M E N T
1 6 7 6 7 0 4 1 0 0 2 0 6 8 1 0 6 4 4 9 7 3 4 1 1 5 6 0 0 5 1 3 3 0 5
1 3/3/4/0 7/ /0  /4/ /8/     4 2 7 2   7     8 5 7 1
  R E G I M E N T
2 0 8 8 5 0 9 4 8 3 4 6 2 2 2 9 9 7 2 5 0 1 1 3 8 0 0 9 9 9 0 3 7 2 9
2 7 4 6 8 7   3   7   4       3 5 0 0   0     0 2 2 5

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

0 0 5 6 0 3 3 4 3 6 8 2 5 5 1
0 7 1 4 3 0   3   0   0
```

(5) The coordinates thus far reconstructed are the following:

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

We note that in col. 7, the additive must be such as to derive values where 1_c and 4_c do not yield any of the plain digits already recovered, viz., 0, 3, 4, 7, 8, or 9; the only possible additive for the column that meets this requirement is 9, which makes $1_c = 2_p$ and $4_c = 5_p$. The last two coordinate digits, 1 and 6, are now quickly determined from the context of the decipherments obtained thus far, so that the completed matrix is as follows:

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

The last 8 digits of the additive sequence and the remainder of the message plain text are easily recovered by extending the already derived plain text.

CHAPTER XIII

PERIODIC DIGRAPHIC SYSTEMS

90. General. In the usual literal periodic polyalphabetic systems, the plaintext units treated are single letters. It might occur to a cryptographer that, since ordinary [monoalphabetic] digraphic substitution is in principle exponentially more difficult[1] of solution than the usual monoalphabetic substitution, it follows that a polyalphabetic system where the unit of substitution is a digraph will give considerably more security than a polyalphabetic monographic substitution. This premise can be easily demonstrated in practice; a much larger volume of text and a larger number of favorable circumstances usually are prerequisites to the successful cryptanalysis of polyalphabetic digraphic ciphers. Fortunately, such systems are rarely encountered; the cryptography of systems suitable for practical use has inherent weaknesses which cannot be avoided except at the expense of inordinate complications in the work of the cipher clerks performing the encryption. In the next paragraph we will treat the cryptography of typical polyalphabetic digraphic systems where the "alphabets"[2] are used cyclically.

91. Cryptography of typical periodic digraphic systems.--a. The most elementary idea of a periodic digraphic system is perhaps a scheme incorporating N unrelated digraphic systems used in a cyclical fashion. For instance, four independent 26x26 digraphic tables might be drawn up; Table I would be used to encipher the 1st, 5th, 9th... plaintext digraphs, Table II would be used for the 2d, 6th, 10th... plaintext digraphs, etc. Since, however, such a scheme is rather clumsy in operation, it might occur to a cryptographer to use only one basic table and modify it so as to yield a polyalphabetic digraphic substitution. This might be accomplished through the use of a table such as the one illustrated in Fig. 127, below. This table, yielding pseudo-digraphic[3] encipherments, produces periodic encipherments of a period of 4 digraphs. The first letters of plaintext digraphs are enciphered monographically by means of the four alphabets at the side of the table; the second letters of digraphs are digraphically enciphered by the equivalents within the table proper, the particular encipherment being

[1] See subpar. 64e, Military Cryptanalytics, Part I.

[2] Each "alphabet" contains 26^2 elements bearing a one-to-one correspondence between plaintext and ciphertext units. Hence we can appreciate the notions of "monoalphabeticity" and "polyalphabeticity" as applied to digraphic systems.

[3] Cf. subpar. 68a, Military Cryptanalytics, Part I.

~~CONFIDENTIAL~~

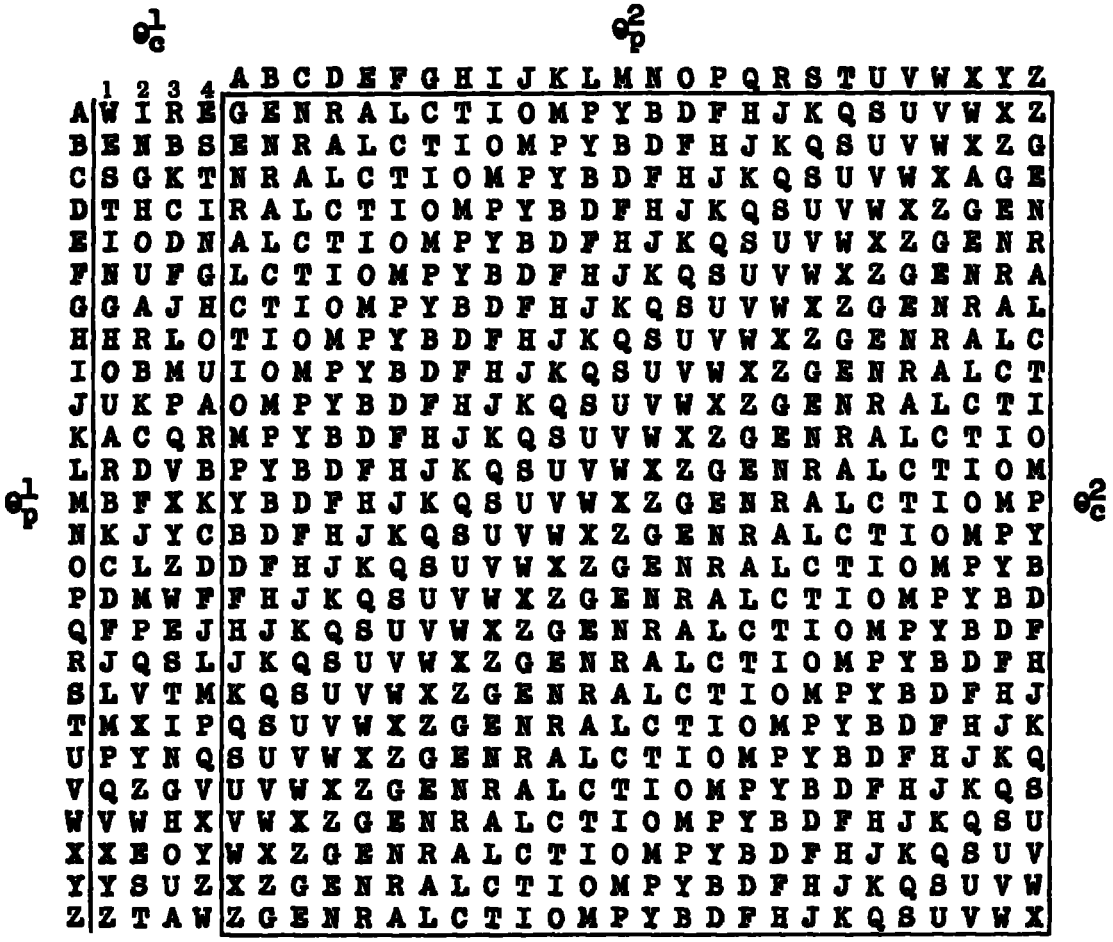


Figure 127.

governed by the identity of the first letter of the plaintext digraph. This scheme could be extended to include more alphabets for the encipherments of the first letters of digraphs; these alphabets might be slides of a basic sequence (as in the example above), or they might be N different, unrelated alphabets.

b. Another system for polyalphabetic digraphic encipherment might incorporate a 26x26 table such as that shown in Fig. 128; the coordinates in this case are written on strips which may be slid to any point of juxtaposition against a predetermined reference point (for example, the cell in the upper left-hand corner). The same key word or two different key words might be employed to set the two coordinate strips for a periodic digraphic system with a limited period; or the two strips might be moved one position at a time, to yield what for all intents and purposes is a progressive alphabet digraphic system with a period of 26 digraphs.

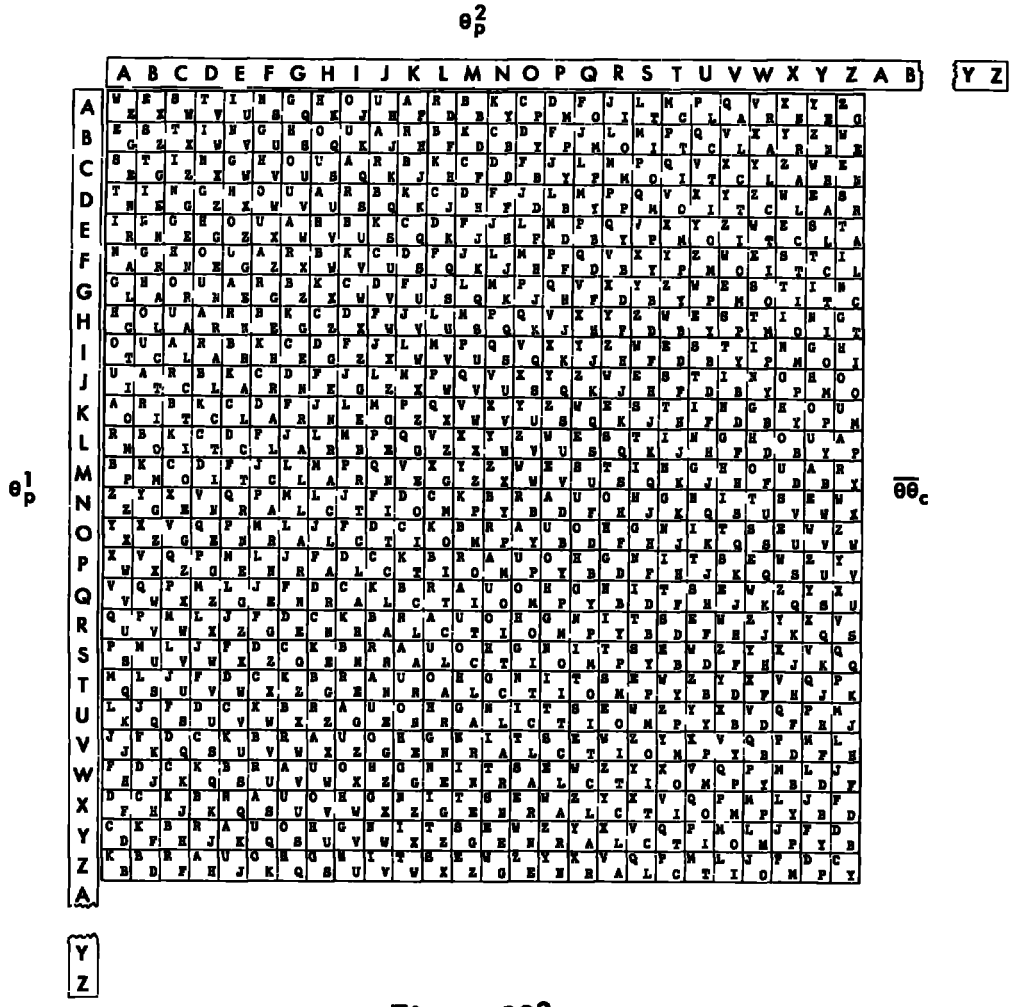


Figure 128.

c. Instead of 26x26 tables, small matrices such as four-squares, two-squares, or Playfairs might be used as a basis for cryptographic treatment in periodic digraphic systems. Since these matrices do not involve coordinates (as do the large tables), periodicity of encipherment would have to be obtained either (1) by the use of N different, unrelated small matrices for the succession of N digraphs in the period, or (2) by some scheme for permuting or deriving additional matrices from a basic matrix. In the two following subparagraphs there will be illustrated some typical means for deriving a multiplicity of matrices from a basic matrix, using a 5x5 Playfair square for the examples.

d. Let us assume that our basic Playfair matrix is that shown in Fig. 129a, below. We take the first four letters of the top row, HYDR, and we inscribe them on a diagonal to the right of the Playfair square, as shown in Fig. 129b. In Fig. 129c, we complete these four skeletal columns by permuting vertically the first four columns of the Playfair

square, using the diagonally inscribed letters as reference points; this now yields a total of 5 Playfair squares, starting in each of the first 5

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

Figure 129a.

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

Figure 129b.

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

Figure 129c.

columns as shown in the figure. The next four letters in the top row of our new diagram are ATOG; we inscribe these letters diagonally to the right of the diagram, and permute the columns as before. After performing this process five times, we have the diagram shown in Fig. 129d, below, which would then start to repeat itself. The reference numbers 1-20 are inscribed

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

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

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

Figure 129d.

over the diagram, as well as the key letters A-Z (which could be used for indicator purposes). This Playfair system actually consists, then, of a "band" composed of 20 interrelated Playfair squares, which are denoted either by the number or a letter over the upper left-hand corner of each square. In using the Playfair band, a 5x5 cut-out mask (provided with an aperture to expose the particular square indicator) is slid along the band according to a prearranged periodic key; or each square could be used successively to encipher the digraphs of the plain text, yielding a progressive alphabet digraphic system of a period of 20.

e. In the next scheme for deriving a plurality of Playfair squares, we will generate a band of 25 squares by a method of permuting two columns

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

Figure 130a.

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

Figure 130b.

at a time. We start with our basic Playfair square in Fig. 130a, taking the first two letters of each row (HY, UL, EF, NO, and TV) of the square, inscribing them vertically to the right of the square; this produces the second Playfair square. We now take the square just derived and, as shown in Fig. 130b, we go through the same process as before, the first two letters of each row in the second square being recorded in two columns to the right of the second square, yielding the third square. This procedure is continued for a total of 25 squares, as shown in Fig. 130c,

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

13	14	15	16	17	18	19	20	21	22	23	24	25	(check)				
W	S	Z	T	V	W	X	Z	E	V	G	X	M	E	O	G	Q	M	L	O	C	Q	Y	L	R	C	H	Y	D	R	A
G	N	M	P	O	S	Q	T	L	W	C	Z	Y	V	R	X	H	E	D	G	A	M	F	O	K	Q	U	L	I	C	B
F	X	K	E	U	G	I	M	B	O	N	Q	P	L	S	C	T	Y	W	R	Z	H	V	D	X	A	E	F	G	K	M
Q	I	L	B	C	N	Y	P	R	S	H	T	D	W	A	Z	F	V	K	X	U	E	I	G	B	M	N	O	P	Q	S
Y	D	R	A	H	F	D	K	A	U	F	I	K	B	U	N	I	P	B	S	N	T	P	W	S	Z	T	V	W	X	Z

Figure 130c.

after which point the band will repeat itself. (In Fig. 130c we have split the band into two sections for convenience, repeating the 13th square at the beginning of the second section to avoid errors.)

f. Many other methods for permuting a series of squares from a basic square are of course possible; the particular system of generation will determine just how many derived squares will be produced, and how many different encipherments of a given plaintext digraph will be available.[4]

g. In the foregoing system of 25 squares, there are numerous possibilities that lend themselves to keying procedures. In one system, the 25 squares might be used in cyclic order, beginning with any desired square;[5]

[4] In the system described in subpar. d, a particular plaintext digraph will have either 1, 6, or 8 different cipher equivalents, owing to the weak nature of the permutation used for deriving additional squares. However, in the system illustrated in subpar. e, there will be from 12 to 18 different equivalents for a digraph, with a mode of 13 occurring in slightly more than one-third of the cases. In other words, this latter system is a periodic digraphic system of a period of 25, involving an equivalent of 12 to 18 different Playfair squares.

[5] The indicator procedure might consist of the numerical designation of the selected square used to start the encipherment; or, since it will be noticed that each of the 25 letters occupies the upper left-hand corner of one particular square and one square only, a square may be designated by the letter occupying this position. Thus, square number 6 may also be designated as the "U" square. In an indicator such as AABUU, the first three letters might designate a particular numerical key (such as the one derived from HYDRAULIC ANALOGIES in this subparagraph) from among a set of keys, the last two letters showing the starting point in the sequence.

this amounts to a progressive alphabet digraphic system of a period of 25. In another system, there might be used a 25-element numerical key derived from a literal key, such as the numerical sequence given below,

				5					10					15					20					25
H	Y	D	R	A	U	L	I	C	A	N	A	L	O	G	I	E	S	H	Y	D	R	A	U	L
10	24	6	19	1	22	14	12	5	2	17	3	15	18	9	13	8	21	11	25	7	20	4	23	16

as a means of disarranging the normal 1, 2, 3,... progression of the Playfair squares in order to remove the cryptographic weakness of three columns in common between the squares used to encrypt adjacent plaintext digraphs. For instance, if the first plaintext digraph were enciphered in square number 6 as a starting point, the succeeding digraphs would be enciphered in square numbers 19 1 22 14 12 ..... 23 16 10 24 6, at which point the cycle repeats. Many other variations in the keying of this and other systems are possible. For example, in the system described in subpar. e, a selection of a small number of the squares might be made on the basis of a repeating key, such as the "G", "R", "A", "N", and "D" squares to yield a period of 5; or a 25-letter mixed sequence might be used. Other modifications involve aperiodic keying methods, which will be taken up in Military Cryptanalytics, Part III.

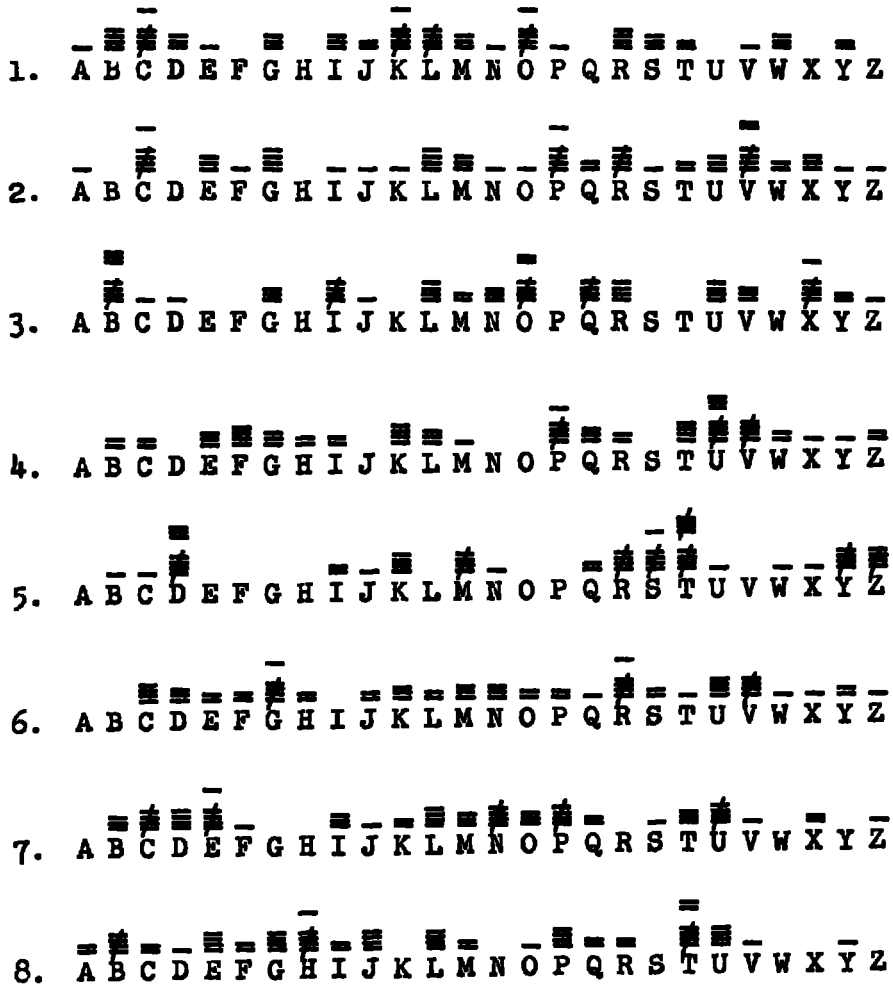
92. Analysis of a first case.--a. We will now consider a problem from the diagnostic stage to its ultimate solution. The following message is to be examined:

DVLTZ	ZLJDV	BMSUT	HKGII	TMEBS	CLQDJ	NHYLO	FCKDC	OEBVY	LCEJM
RPRKP	TNPQU	DJVRR	VOUDZ	NARRO	EIWCL	OROCZ	EMPJP	GUMVC	OCLCK
YNLLG	WOVTM	PTDIR	FTSDE	LPQPK	UUVKO	LLQYD	GBYXW	YCEQO	ROFUC
ITKCB	BMYIR	LMLGD	VDLMT	UPNNI	TTFBG	TGBFR	PYTKO	UUGXB	EDVTH
BXIVR	KSLGG	JBBFQ	BMGQU	DGNIA	NICZC	UUSCX	GDFUU	IVNLK	NKHLP
IEMQU	TITBU	IGEQL	VGUZL	EBTVR	PTGPB	WQBVY	CLJKL	UQSRN	TOUXT
RVEJC	QMRTG	PECEV	PZRXG	VADVK	HCCOU	YXSUT	HKGII	TMEBS	CUHMD
OGLCZ	ZSUCJ	BMMRT	GPECE	VKYHZ	YPPRP	RRJMW	JXWSO	XARVN	LQDFI
OUUQS	RNTWK	XTRPB	DIZOF	ZRKHK	CVKTP	OPYXQ	ZTVMP	CRGHX	EBFMW
QUWRL	MELBU	JXQUB	SXYDT	MPCRN	KMDOG				

The presence of several long repetitions at intervals factorable by 8 leads us to believe that we have here a periodic system of 8 alphabets. The message is transcribed accordingly and uniliteral distributions are taken on the columns, as shown below:

~~CONFIDENTIAL~~

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



b. The I.C.'s of the distributions (comprising 60 tallies each) and the observed number of blanks (Λ) for each are tabulated in the diagram below:

Alph.	Λ	I.C.	Alph.	Λ	I.C.
1	6	1.29	5	9	2.07
2	3	1.29	6	3	1.07
3	9	1.66	7	6	1.25
4	6	1.32	8	6	1.31

Except for alphabets 3 and 5, the I.C.'s are far from satisfactory; the period is unquestionably 8, but it does not appear that we have 8 monoalphabetic distributions. The average of the I.C.'s is $\frac{11.26}{8} = 1.41$, a figure considerably above random but nevertheless not nearly close enough to the expected I.C. of plain text for a sample of text this size. We note, however, that the average I.C. of the odd columns is $\frac{6.27}{4} = 1.57$, while the average I.C. of the even columns is $\frac{4.99}{4} = 1.25$; this strikes us as being expecially significant.[6] Furthermore, the average Λ for the odd columns is $\frac{30}{4} = 7.5$, while that of the even columns is $\frac{18}{4} = 4.5$; these figures are compared with the expected Λ_p of 8 and the Λ_r of 2.5 for distributions of this size.[7] Perhaps the odd columns do represent monoalphabetic encipherment of plain text after all, while the even columns have undergone different cryptographic treatment. We will pursue this matter further.

c. One of the possibilities that comes to mind to explain the foregoing phenomena is a pseudo-digraphic encipherment in which the initial letters of plaintext pairs are monographically enciphered. If this were the case the digraphic I.C.'s of columns 1-2, 3-4, 5-6, and 7-8 should be close to the expected 4.66 for English plain text;[8] these digraphic I.C.'s are 5.38, 7.31, 7.31, and 8.09, respectively, giving statistical credence to the hypothesis that the four pairs of adjacent columns represent digraphically enciphered plain text.[9]

[6] It can be shown that the I.C. of the odd columns, 1.57, represents a sigmage of $\frac{240(1.57 - 1.08)}{\sqrt{2(25 \cdot 4)}} = \frac{117.6}{14.14} =$ 8.3 σ, whereas the I.C. of the even columns, 1.25, represents a deviation of $\frac{240(1.25 - 1.08)}{\sqrt{2(25 \cdot 4)}} = \frac{40.8}{14.14} =$ 2.9 σ above random. (We used 1.08 in the formula instead of 1.00, because the former figure is the I.C. of the over-all cipher text.)

[7] Cf Chart 6 on p. 39 of Military Cryptanalytics, Part I.

[8] Cf. subpar. 67c, Military Cryptanalytics, Part I.

[9] See also subpar. 95a for further lines of attack on this problem if the digraphic I.C.'s of the pairs of adjacent columns had not been satisfactory.

d. The 14-letter repetition in the message is now examined. The uniliteral frequencies of the first letters of the cipher digraphs lend support to the assumption that this repetition represents the encipherment of RECONNAISSANCE, giving us the equivalents of C_p and N_p in column 1, A_p in col. 3, R_p and S_p in col. 5, and A_p and C_p in col. 7, in addition to the 7 values within the large square of the reconstruction matrix. The third letter of the repetition MR TG PE CE thus turns out to be S_p; frequency considerations of the first letters of these cipher digraphs make it quite likely that this repetition represents POSITION, which gives us additional values in our reconstruction matrix. Finally, the six digraphs at the beginning of the message just before RECONNAISSANCE are studied, and, from the standpoint of the length of the ciphertext passage, plus the AB -- -- -- AB idiomorph exhibited, plus a consideration of the uniliteral frequencies of the initial letters of the digraphs, the opening word is assumed to be PHOTOGRAPHIC. The values from these three plaintext assumptions are set forth in the reconstruction matrix in Fig. 131a, below:

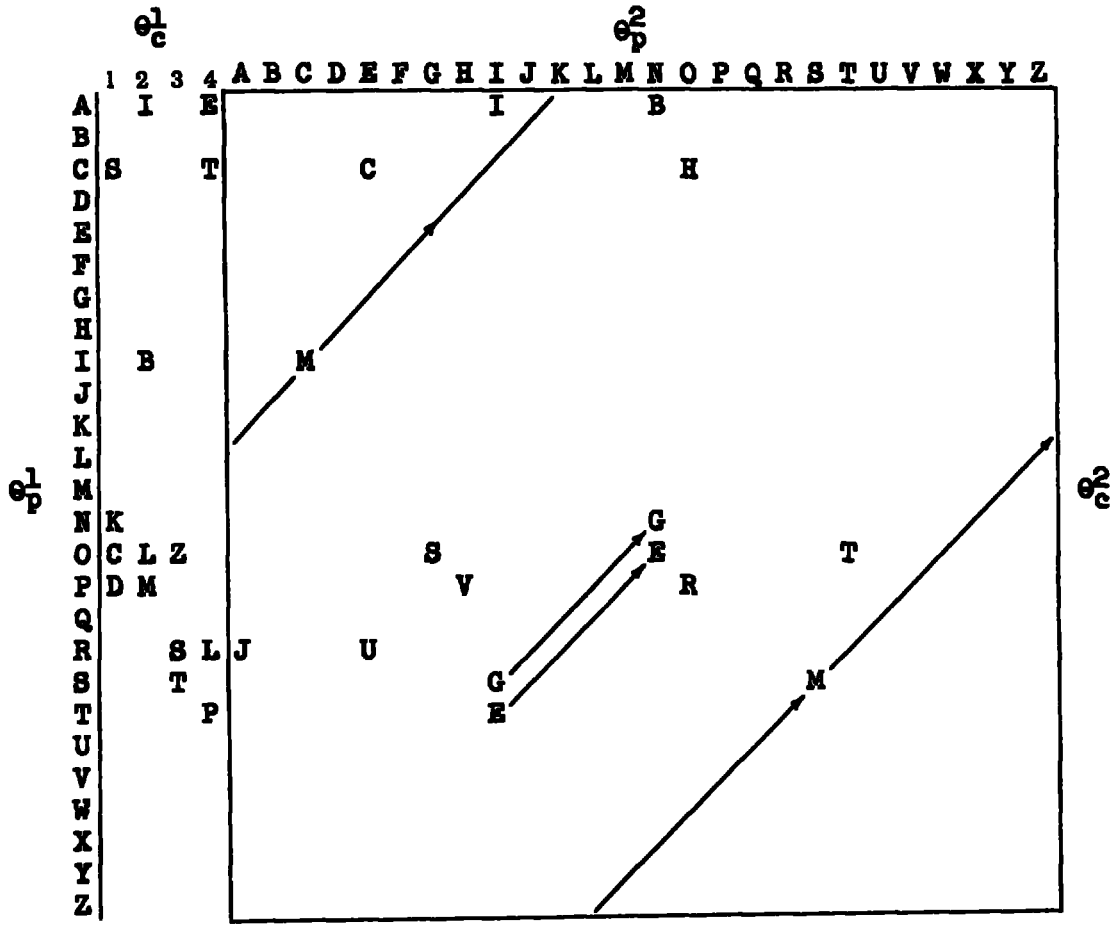


Figure 131a.

e. Evidence of vertical direct symmetry, as well as of diagonals of repeated letters characteristic of Vigenere-type squares, are manifested within the matrix, as shown by the lines in the foregoing figure; from these characteristics it appears that both the θ_p^1 and θ_p^2 sequences of this digraphic matrix consist of the normal A-Z sequence. If this is so, then direct symmetry should also be manifested among the four cipher sequences used to encipher the first letters of digraphs. Taking advantage of the principles of direct symmetry of position, the matrix in Fig. 131a is amplified into that shown in Fig. 131b, below:

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

θ_p^1 θ_c^2

Figure 131b.

The frequencies of the additional values placed by direct symmetry in the four monographic columns are checked, and they are found to correspond generally with the expected frequencies of their plaintext equivalents; this, then, is confirmation of the type of matrix assumed.

f. From the partially reconstructed matrix in Fig. 131b, above, the derived values may be entered on the work sheet, as follows:

DV	LT	ZS	LJ	DV	BM	SU	TH	KG	II	TM	EB	SC	LQ	DJ	NH
PH	OT	OG	RA	PH	IC	RE	CO	NN	AI	SS	AN	CE	O	EN	
YL	OF	CK	DC	OE	BV	YL	CE	JM	RP	RK	PT	NP	QU	DJ	VR
		D	OS		IO		NO				TO			EN	
RV	OU	DZ	NA	RR	OE	IW	CL	OR	OC	ZE	MP	JP	GU	MV	CO
		E				T	N			ON	S			IO	N
CL	CK	YN	LL	GW	OV	TM	PT	DI	RF	TS	DE	LP	QP	KU	UV
O	K		R			SS	TO	PT		SC	O			CT	
KO	LL	QY	DG	BY	XW	YC	EQ	OR	OF	UC	IT	KC	BB	MY	IR
N	O		OM	M			A				DE	NT	IF	I	DA
LM	LG	DV	DL	MT	UP	NN	IT	TF	BG	TG	BF	RP	YT	KO	UU
SS	OM	ES	O	TO			DE	D	IS	SI	L			C	
GX	BE	DV	TH	BX	IV	RK	SL	GG	JB	BF	QB	MG	QU	DG	NI
	IT	ES	CO	M	AW					B				EW	
AN	IC	ZC	UU	SC	XG	DF	UU	IV	NL	KN	KH	LP	IE	MQ	UT
	AG	OS				E		ES		C	ME	S	AB	I	
IT	BU	IG	EQ	LV	GU	ZL	EB	TV	RP	TG	PB	WQ	BV	YC	LJ
ED	IN	TH	A	SE		O	AN	DT		SI	TU		IO		RA
KL	UQ	SR	NT	OU	XT	RV	EJ	CQ	MR	TG	PE	CE	VP	ZR	XG
N		RM					AR	O	PO	SI	TI	ON		OP	
VA	DV	KH	CC	OU	YX	SU	TH	KG	II	TM	EB	SC	UH	MD	OG
	LL	CO	NT			RE	CO	NN	AI	SS	AN	CE		I	
LC	ZZ	SU	CJ	BM	MR	TG	PE	CE	VK	YH	ZY	PP	RP	RR	JM
SO		RE	NE	MY	PO	SI	TI	ON			Y	U			
WJ	XW	SO	XA	RV	NL	QD	FI	OU	UQ	SR	NT	WK	XT	RP	BD
		R								RM					L
IZ	OF	ZR	KH	KC	VK	TP	OP	YX	QZ	TV	MP	CR	GH	XE	BF
E		OP	ME	NT		S				SE	S	OP			L
MW	QU	WR	LM	EL	BU	JX	QU	BS	XY	DT	MP	CR	NK	MD	OG
T			RT	B	IN			MI		ED	S	OP		I	

From here on the addition of further values will snowball, and in very short order the plain text is solved in its entirety, and the enciphering matrix completed; the latter is found to be identical with the matrix illustrated in Fig. 127.

g. The steps in the solution of the foregoing problem were simple. The diagnosis of the system was straightforward, and the reconstruction of the plain text and of the matrix was begun by three word assumptions. In actual practice, the solution of a single message may not be so fortunate, but, as usual, we have shown the theoretical steps involving a single message which has been manipulated to make possible a solution on this limited traffic; in operational practice, several messages would probably have been required in order to find the two or three cribs necessary for solution. If the θ_p^1 and θ_p^2 sequences had been unknown mixed components, then the phenomena of indirect symmetry would have prevailed, and additional plaintext assumptions in the message would probably have been necessary in order to exploit the symmetrical phenomena in such a case.

h. A few remarks on the I.C.'s given in subpar. b might be added at this time. Alphabets 1 and 7 were a trifle low, and the average I.C. of 1.57 for the odd columns was also lower than we would have liked to have seen for monoalphabetic text. The vagaries of the plain text as it was allocated into the columns were responsible for this, since the over-all I.C. of the plaintext message may be found to be 1.74. On the other hand, the average I.C. of the even columns should have been lower than the observed 1.25,[10] but again this is "one of those things." The prudent cryptanalyst is prudent in his reverence for probabilities, small or large.

93. Analysis of a second case.--a. For our next example we will assume that the enemy is known to be using a system involving a multiplicity of Playfair squares to accomplish a polyalphabetic digraphic substitution. The following are the beginnings of 40 messages available for study:

	1	2	3	4	5	6	7	8	9	10
1.	IG	WN	CM	TO	SM	WT	LK	ET	RA	LN...
2.	HK	HV	YG	RT	MZ	EF	YO	DR	IM	OV...
3.	HK	CI	NT	IG	OE	OL	FC	NX	PI	FP...
4.	BS	UO	RO	CO	FR	DF	EN	ZO	AB	UV...
5.	LQ	IB	VY	CN	IH	FG	ZN	ZD	ZO	FL...
6.	OV	KH	LF	RC	GT	TU	NZ	RG	MT	YV...
7.	HZ	SF	WD	CQ	QE	YU	VO	PI	CA	AI...
8.	HK	HV	PG	IC	CO	DG	RM	NS	EA	XD...
9.	HA	PN	WE	ZU	VZ	NG	IR	OZ	HT	OE...
10.	NM	IF	HK	RC	CT	FR	FQ	EO	PI	MG...

[10] The expected I.C. for the second letters of digraphs of English text enciphered in a pseudo-digraphic system is $26(.0667)^2 = 1.16$, as compared with the usual I.C. of $26(.0637) = 1.73$. This I.C. of 1.16 is characteristic of plaintext autokey systems (cf. Appendix 6, "Cryptographic Supplement") which will be taken up in Military Cryptanalytics, Part III.

~~CONFIDENTIAL~~

11. HK LK ZL YF VD UC OD TS AB CI...
12. NT ZU NB FY OF ZL RG IR PI XV...
13. UN FZ BH NC UC ZU CS IX DZ CZ...
14. QP PB CO TO DE UO ZO BX TE NE...
15. IG WN CM TO NG BX QW UE NQ NP...
16. HK LK CI MU VD UC OD TS BX SV...
17. HU CD AR FY HI CU NZ UT EL UE...
18. OV KH LF SG IT EO IZ KB SD SL...
19. UN FZ BU DY TA LO LI UZ NT AT...
20. HR ZF RT VZ FR MS RQ TU AK KT...
21. HR IG CO TO UB ZO KI ZL TO XO...
22. TD VY MC RC GT TU NZ QC LD OD...
23. LQ OY LV HD PG AW PI EO BV SX...
24. HK NK PV HF UT DW IR GN CA CK...
25. FS WV NU DS ZO IT OX IR RC TI...
26. QD BP TO GS TL PH FI EO TS SR...
27. LV KH YG DC EO CD TB MD CM HX...
28. FS WV UZ OV FD OL XO SB IP PN...
29. UP NT BI FY FG RO HZ QT PI OP...
30. HZ SF WD NQ DP NQ ZO LF IR XR...
31. HU HX XY BU LO WZ PD CR RL ZB...
32. HK PG UZ OV UB ZQ FH LP ET EA...
33. NT ZU BH NC UC ZU CS KU EO TC...
34. AH IG IT BV EA VF PT AK NZ ZU...
35. NM WV OV SP OX BG OZ YK SC RC...

36. BR IB HE AM BU DA OX YD IM OV...

37. HK TG NC VS OE XB GE XO OZ PN...

38. GL WV YG DC EO CD RL ZD ZO FL...

39. GL AQ SN FY HI CU NZ LC KP PK...

40. LQ KZ UO RO BI CT NZ KB HW TX...

From the repetitive phenomena observed, it is concluded that the messages are in flush depth; i.e., each column represents a digraphic "monoalphabet".

b. Abridged digraphic distributions are now made for the first few digraphic columns; these are shown below:

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
H	S				S	L	K	G			Q		M	V		P			D	N					
	R				S	L	K	G			Q		T	V		D				N					
							Z				V		T							P					
							K				Q		M												
							A																		
							K																		
							K																		
							U																		
							R																		
							R																		
							K																		
							Z																		
							U																		
							K																		
							K																		

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
Q	P	I			Z		V	B		H	K		K	Y	N			F	G	O	Y	N			U
		D			Z		V	F		H	K		T		B			F				N			F
							X	G		H					G							V			U
								G		Z												V			
								B														V			
																						V			

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
R	H	M					K	T			F	C	T	V	G		O	N	O	Z	Y	D	Y	G	L
	U	O					E				F		B		V		T			Z		E		G	
	I	M									V		U							O		D		G	
	H	I											C												
		O																							

~~CONFIDENTIAL~~

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
M	U	O	Y		Y	S	D	G				U	C	V			T	G	O		Z				F	U
	V	N	S		Y		F	C					Q	V			C	P	O		S					
		Q	C		Y								C				C		O							
			C		Y												C		O							
																	O									

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
	U	O	E	O	R	T	I	H				O	Z	G	E	G	E		M	A	C	Z				O
	I	T	P	A	R	T	I	T							F					L	B	D				
				O	D										X						T	D				
					G										E						B					
																					C					

Note is taken of the high frequency digraphs in the columns, and also of the reversible digraphs. What follows now is a brief synopsis of the initial entries into the problem. In col. 1, HK_c, with 8 occurrences, is in all probability RE_p. Next, we study the tetragraphic repetition CO TO in Msg #14 and 21, and the repetition IG WN CM TO in #1 and 15; it is assumed that these represent TI ON and DI VI SI ON, respectively. Msg #32 is now assumed to begin with the word RE GI ME NT, which would make MO VE ME NT in #28. In #38, we have GL WV = FI VE; in #27 we have LV KH = YO UR and in #6 we have OV KH LF = FO UR TH. The 8-letter repetition between #6 and #22 is assumed to be DI VI SI ON; Msg #2 now appears to begin with the word RE FE RE NC E, which makes #8 RE FE RX RI NG TO. The initial word in #22 is assumed to be WH EN, and in #3, RE IN FO RC EM EN TS.

c. At this point the work sheet with the assumptions entered will now look as follows:

	1	2	3	4	5	6	7	8	9	10
1.	IG	WN	CM	TO	SM	WT	LK	ET	RA	LN...
	DI	VI	SI	ON						
2.	HK	HV	YG	RT	MZ	EF	YO	DR	IM	OV...
	RE	FE	RE	NC	E					
3.	HK	CI	NT	IG	OE	OL	FC	NX	PI	FP...
	RE	IN	FO	RC	EM	EN	TS			
4.	BS	UO	RO	CO	FR	DF	EN	ZO	AB	UV...
5.	LQ	IB	VY	CN	IH	FG	ZN	ZD	ZO	FL...
							NO			
6.	OV	KH	LF	RC	GT	TU	NZ	RG	MT	YV...
	FO	UR	TH	DI	VI	SI	ON			
7.	HZ	SF	WD	CQ	QE	YU	VO	PI	CA	AI...
8.	HK	HV	PG	IC	CO	DG	RM	NS	EA	XD...
	RE	FE	RX	RI	NG	TO				
9.	HA	PN	WE	ZU	VZ	NG	IR	OZ	HT	OE...
10.	NM	IF	HK	RC	CT	FR	FQ	EO	PI	MG...
				DI						

~~CONFIDENTIAL~~

11.	HK	LK	ZL	YF	VD	UC	OD	TS	AB	CI...
	RE									
12.	NT	ZU	NB	FY	OF	ZL	RG	IR	PI	XV...
13.	UN	FZ	BH	NC	UC	ZU	CS	IX	DZ	CZ...
14.	QP	PB	CO	TO	DE	UO	ZO	BX	TE	NE...
			TI	ON						
15.	IG	WN	CM	TO	NG	BM	QW	UE	NQ	NP...
	DI	VI	SI	ON						
16.	HK	LK	CI	MU	VD	UC	OD	TS	BX	SV...
	RE									
17.	HU	CD	AR	FY	HI	CU	NZ	UT	EL	UE...
							ON			
18.	OV	KH	LF	SG	IT	EO	IZ	KB	SD	SL...
	FO	UR	TH	RE	GI	ME	NT			
19.	UN	FZ	BU	DY	TA	LO	LI	UZ	NT	AT...
						NE				
20.	HR	ZF	RT	VZ	FR	MS	RQ	TU	AK	KT...
21.	HR	IG	CO	TO	UB	ZO	KI	ZL	TO	XO...
			TI	ON						
22.	TD	VY	MC	RC	GT	TU	NZ	QC	LD	OD...
	WH	EN	IS	DI	VI	SI	ON			
23.	LQ	OY	LV	HD	PG	AW	PI	EO	BV	SX...
24.	HK	NK	PV	HF	UT	DW	IR	GN	CA	CK...
	RE									
25.	FS	WV	NU	DS	ZO	IT	OX	IR	RC	TI...
	MO	VE								
26.	QD	BP	TO	GS	TL	PH	FI	EO	TS	SR...
				ER						
27.	LV	KH	YG	DC	EO	CD	TB	MD	CM	HK...
	YO	UR	RE	GI	ME	NT				
28.	FS	WV	UZ	OV	FD	OL	XO	SB	IP	PN...
	MO	VE	ME	NT		EN				
29.	UP	NT	BI	FY	FG	RO	HZ	QT	PI	OP...
30.	HZ	SF	WD	NQ	DP	NQ	ZO	LF	IR	XR...
31.	HU	HX	XY	BU	LO	WZ	PD	CR	RL	ZB...
32.	HK	PG	UZ	OV	UB	ZQ	FH	LP	ET	EA...
	RE	GI	ME	NT						
33.	NT	ZU	BH	NC	UC	ZU	CS	KU	EO	TC...
34.	AH	IG	IT	BV	EA	VF	PT	AK	NZ	ZU...
35.	NM	WV	OV	SP	OX	BG	OZ	YK	SC	RC...
		VE								

~~CONFIDENTIAL~~

36.	BR	IB	HE	AM	BU	DA	OX	YD	IM	OV...
37.	HK	TG	NC	VS	OE	XB	GE	XO	OZ	PN...
	RE				EM					
38.	GL	WV	YG	DC	EO	CD	RL	ZD	ZO	FL...
	FI	VE	RE	GI	ME	NT	S			
39.	GL	AQ	SN	FY	HI	CU	NZ	LC	KP	PK...
	FI						ON			
40.	LQ	KZ	UO	RO	BI	CT	NZ	KB	HW	TX...
							ON			

In the course of experimenting with the partial reconstruction of the Playfair squares for each column, we are able to determine that, in col. 4, $CO_c = TI_p$, $CN_c = TR_p$, $NC_c = RT_p$, $DS_c = -R_p$, $VS_c = EN_p$, and $RO_c = NI_p$. These recoveries facilitate further assumptions, and in reasonably short order we would have our work sheet looking like this:

	1	2	3	4	5	6	7	8	9	10
1.	IG	WN	CM	TO	SM	WT	LK	ET	RA	LN...
	DI	VI	SI	ON						
2.	HK	HV	YG	RT	MZ	EF	YO	DR	IM	OV...
	RE	FE	RE	NC	E					
3.	HK	CI	NT	IG	OE	OL	FC	NX	PI	FP...
	RE	IN	FO	RC	EM	EN	TS			
4.	BS	UO	RO	CO	FR	DF	EN	ZO	AB	UV...
				TI						
5.	LQ	IB	VY	CN	IH	FG	ZN	ZD	ZO	FL...
				TR			NO			
6.	OV	KH	LF	RC	GT	TU	NZ	RG	MT	YV...
	FO	UR	TH	DI	VI	SI	ON			
7.	HZ	SF	WD	CQ	QE	YU	VO	PI	CA	AI...
8.	HK	HV	PG	IC	CO	DG	RM	NS	EA	XD...
	RE	FE	RX	RI	NG	TO				
9.	HA	PN	WE	ZU	VZ	NG	IR	OZ	HT	OE...
10.	NM	IF	HK	RC	CT	FR	FQ	EO	PI	MG...
	SE	ND	AD	DI	TI	ON	AL			
11.	HK	LK	ZL	YF	VD	UC	OD	TS	AB	CI...
	RE	QU	ES	TA	RT	IL	LE	RY		
12.	NT	ZU	NB	FY	OF	ZL	RG	IR	PI	XV...
	EN	EM	YP	AT	RO	L				
13.	UN	FZ	BH	NC	UC	ZU	CS	IX	DZ	CZ...
	HE	AV	YA	RT	IL	LE	RY			
14.	QP	PB	CO	TO	DE	UO	ZO	BX	TE	NE...
	PO	SI	TI	ON						
15.	IG	WN	CM	TO	NG	BM	QW	UE	NQ	NP...
	DI	VI	SI	ON						

16.	HK	LK	CI	MU	VD	UC	OD	TS	BK	SV...
	RE	QU	IR	EA	RT	IL	LE	RY		
17.	HU	CD	AR	FY	HI	CU	NZ	UT	EL	UE...
	TH	IR	DB	AT	TA	LI	ON			
18.	OV	KH	LF	SG	IT	EO	IZ	KB	SD	SL...
	FO	UR	TH	RE	GI	ME	NT			
19.	UN	FZ	BU	DY	TA	LO	LI	UZ	NT	AT...
	HE	AV	Y			NE				
20.	HR	ZF	RT	VZ	FR	MS	RQ	TU	AK	KT...
	AD	VA	NC	E						
21.	HR	IG	CO	TO	UB	ZO	KI	ZL	TO	XO...
	AD	DI	TI	ON	AL					
22.	TD	VY	MC	RC	GT	TU	NZ	QC	LD	OD...
	WH	EN	IS	DI	VI	SI	ON			
23.	LQ	OY	LV	HD	PG	AW	PI	EO	BV	SX...
24.	HK	NK	PV	HF	UT	DW	IR	GN	CA	CK...
	RE	CO	NX	NA	IS	SA	NC	E		
25.	FS	WV	NU	DS	ZO	IT	OX	IR	RC	TI...
	MO	VE	YO	UR						
26.	QD	BP	TO	GS	TL	PH	FI	EO	TS	SR...
	PR	IS	ON	ER						
27.	LV	KH	YG	DC	EO	CD	TB	MD	CM	HX...
	YO	UR	RE	GI	ME	NT				
28.	FS	WV	UZ	OV	FD	OL	XO	SB	IP	PN...
	MO	VE	ME	NT	OF	EN	EM	Y		
29.	UP	NT	BI	FY	FG	RO	HZ	QT	PI	OP...
	IN	FO	RM	AT	IO	N				
30.	HZ	SF	WD	NQ	DP	NQ	ZO	LF	IR	XR...
31.	HU	HX	XY	BU	LO	WZ	PD	CR	RL	ZB...
32.	HK	PG	UZ	OV	UB	ZQ	FH	LP	ET	EA...
	RE	GI	ME	NT	AL					
33.	NT	ZU	BH	NC	UC	ZU	CS	KU	EO	TC...
	EN	EM	YA	RT	IL	LE	RY			
34.	AH	IG	IT	BV	EA	VF	PT	AK	NZ	ZU...
	RA	DI	O							
35.	NM	WV	OV	SP	OX	BG	OZ	YK	SC	RC...
	SE	VE	N							
36.	BR	IB	HE	AM	BU	DA	OX	YD	IM	OV...
37.	HK	TG	NC	VS	OE	XB	GE	XO	OZ	PN...
	RE	PO	RT	EN	EM	Y				
38.	GL	WV	YG	DC	EO	CD	RL	ZD	ZO	FL...
	FI	VE	RE	GI	ME	NT	S			
39.	GL	AQ	SN	FY	HI	CU	NZ	LC	KP	PK...
	FI	RS	TB	AT	TA	LI	ON			
40.	LQ	KZ	UO	RO	BI	CT	NZ	KB	HW	TX...
				NI			ON			

d. With so many plain-cipher equivalencies per column, reconstruction of the squares will be a very easy matter. The squares as recovered for the first three columns are the following:

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

Square No. 1

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

Square No. 2

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

Square No. 3

Square No. 1 is recognized as containing a keyword-mixed sequence, so this square is rewritten in its original form, with the missing letters filled in. It is noticed that three of the columns of square No. 1 are common to square No. 2, and that three of the columns of this latter square are common to square No. 3; these three squares are therefore rewritten as follows:

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

Square No. 1

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

Square No. 2

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

Square No. 3

A few moments' inspection will now reveal the relationships among the three squares; each succeeding square is derived from its predecessor by permuting two columns at a time, as demonstrated in subpar. 91e. Since we now know the method of square generation, we may read any message in its entirety without further ado after we have generated the pertinent band of Playfair squares.

e. The foregoing system was fairly easy to solve because of its progressive 1, 2, 3... selection of the Playfair squares from the band. If the order of square selection had been different, say in a scrambled order of 25 squares as treated in subpar. 91g, it would probably have been necessary to make entries in quite a few columns in order to reconstruct enough partial squares before we would have been able to see any relationships among the squares.

f. Once the Playfair band has been recovered, a message starting at any arbitrary point in the band may of course be read, since one of the 25 possible trials will yield plain text. If the same band continues to be used, but there is employed an unknown mixed sequence to govern the progression of enciphering squares, then a modification of the generatrix method is here applicable. For example, let us consider the following cryptogram, known to have been enciphered with the Playfair band just recovered, but with an unknown 25-element progression:

RQ CP CI IT TP CL ZL GP TD GH SC XW RQ XV EI
EW ZC RW ZN HS PY BT WM KY QD TF NI UX XY FG
DI PV MT VG VY

The procedure here is to complete the "plain component (digraphic) sequence" from the cipher digraphs by deciphering each digraph successively through all 25 squares. For example, the first digraph $\overline{RQ}_c$ represents $\overline{XK}_p$ in squares No. 1 and 2, $\overline{PI}_p$ in squares No. 3 and 4, $\overline{WN}_p$ in square No. 5, etc. The complete generatrix diagram for the first ten digraphs is the following:

	RQ	CP	CI	IT	TP	CL	ZL	GP	TD	GH...
1.	XK	IQ	IL	UW	WN	IU	VB	IG	WH	ED
2.	XK	IQ	IN	NP	LT	YQ	ES	IG	PF	UD
3.	PI	WR	IR	OC	WN	TS	ES	XR	CF	ED
4.	PI	WR	IR	OC	WN	ZI	LS	XR	CF	MR
5.	WN	QT	TG	GI	DT	NB	LS	XT	DS	MT
6.	HO	NC	TG	GI	AC	NY	LS	QC	DS	QV
7.	PO	RC	TG	GI	AC	SG	FO	QC	FV	QV
8.	HO	QI	AC	CK	HI	OM	FO	HQ	SA	HV
9.	HO	QI	AC	CK	HI	OY	XO	HQ	RW	HV
10.	LC	QT	RE	EN	NT	RY	DR	HQ	SA	HV
11.	YK	HT	RE	EN	NT	RY	DR	BW	SA	BY
12.	YL	HT	DO	OS	ZT	RO	RK	BW	SC	BY
13.	YL	BO	BQ	BS	AT	BI	RK	OM	SA	OY
14.	DM	BO	YU	EX	AT	BY	RK	ES	XA	UF
15.	YL	RY	YU	MQ	ZM	RO	ET	MN	QK	UF
16.	YL	TH	QN	MQ	ZM	WT	ET	ZH	QK	FN
17.	TB	YN	ZF	TQ	DQ	WY	CY	MN	HT	FN
18.	ZS	YN	ZF	TQ	DQ	VN	VQ	MN	HT	FN
19.	HO	ST	TN	FH	CT	SP	WC	MC	PF	QX
20.	HO	YN	TN	FH	YI	WG	KG	MN	WH	QX
21.	TO	MN	QN	FH	YI	OM	WC	ES	WH	DA
22.	HO	YN	YU	EP	NT	OY	WC	FS	BM	MR
23.	LC	YN	YU	EP	NT	RY	DC	IW	WH	ED
24.	CK	YZ	YM	NP	ZT	RY	WC	IW	WE	NL
25.	CK	DM	DQ	UW	WN	YQ	VQ	IG	WH	ED

By reading various levels of the generatrix diagram, it may be seen that the message begins "HOSTILE PATROL SIGHTED..."

g. It will be noted that the equivalency $\overline{CP}_c = \overline{ST}_p$ is unique to square No. 19, and that $\overline{CI}_c = \overline{IL}_p$ is unique to square No. 1; therefore these squares may be ruled out as key squares for any other positions along the cycle of 25. The multiple keys for the first 10 digraphs are as follows:

C:	RQ	CP	CI	IT	TP	CL	ZL	GP	TD	GH...
P:	HO	ST	IL	EP	AT	RO	LS	IG	HT	ED
	6	19	1	22	13	12	4	2	17	3
	8			23	14	15	5	25	18	23
	9						6			25
	20									
	22									

The first 10 keys might be made unique by considering the decipherments of the cipher digraphs in the next cycle. Since we have limited the possible keys in the foregoing diagram, only those keys come into question in the corresponding positions of the next cycle. The decipherments, therefore, of the digraphs in the next cycle are as follows:

	TF	NI	UX	XY	FG	DI	PV	MT	VG	VY
1.			·····CT							
2.								OS		
3.										EN
4.							NX			
5.							TW			
6.	DI						CH			
7.										
8.	SK									
9.	WA									
10.										
11.										
12.						IX				
13.					GW					
14.					NS					
15.						YQ				
16.										
17.									EV	
18.									EC	
19.			····UN							
20.	FI									
21.										
22.	PM				IO					
23.					VR					FP
24.										
25.								NZ		OV

The plain text revealed, "...DJ UN CT IO NS IX TW OS EV EN", is in this case found in unique squares, so the unambiguous key for the first 10 positions is found to be 6 19 1 22 14 12 5 2 17 3. When the rest of the plain text is solved, it will be found that of the remaining 15 columns, all but 4 will yield unique keys; if we had available another message or two, the ambiguity could probably be removed from the 4 ambiguous columns.

94. Analysis of other types of periodic digraphic systems.--a. Since there is a plethora of possible basic digraphic systems which may be used in conjunction with a polyalphabetic scheme, each case will present different aspects in its solution, depending on what may be known initially about the system, and what phenomena are uncovered and recognized during the process of solution. A sufficient volume of traffic, plus the inevitable cryptanalytic breaks which may be expected to occur in the course of the use and misuse of the system, are the deciding factors for successful solution.

b. In a system such as that illustrated in Fig. 128, once the period has been determined by factoring (with perhaps the digraphic ϕ test being used to prove the period), plaintext assumptions in the messages would be recorded initially in several skeleton 26x26 matrices, one for each column of the period, until enough data have accumulated to permit the revelation of the relationships latent among the matrices and among the sets of coordinates. If the composition of the interior of the matrix were known, even a single crib of moderate length might suffice to establish enough values in the sliding coordinates which would result in further automatic decryptions and rapid completion of the solution.

c. In those digraphic systems which yield trinomes for the ciphertext equivalents for plaintext digraphs, the primary cipher text might be subjected to encipherment by a cyclic additive as a means of increasing the security of the system. For example, the basic system might incorporate a matrix such as that illustrated in Fig. 132, below:[11]

0_p^2

	J	U	P	I	T	E	R	A	B	C	D	F	G	H	K	L	M	N	O	Q	S	V	W	X	Y	Z
V	001	002	003	004	005	006	007	008	009	010	011	012	013	014	015	016	017	018	019	020	021	022	023	024	025	026
E	027	028	029	030	031	032	033	034	035	036	037	038	039	040	041	042	043	044	045	046	047	048	049	050	051	052
N	053	054	055	056	057	058	059	060	061	062	063	064	065	066	067	068	069	070	071	072	073	074	075	076	077	078
U	079	080	081	082	083	084	085	086	087	088	089	090	091	092	093	094	095	096	097	098	099	100	101	102	103	104
S	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128	129	130
A	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156
B	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182
C	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208
D	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234
F	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260
G	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286
H	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312
I	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338
J	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364
K	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390
L	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416
M	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442
O	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467	468
P	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493	494
Q	495	496	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519	520
R	521	522	523	524	525	526	527	528	529	530	531	532	533	534	535	536	537	538	539	540	541	542	543	544	545	546
T	547	548	549	550	551	552	553	554	555	556	557	558	559	560	561	562	563	564	565	566	567	568	569	570	571	572
W	573	574	575	576	577	578	579	580	581	582	583	584	585	586	587	588	589	590	591	592	593	594	595	596	597	598
X	599	600	601	602	603	604	605	606	607	608	609	610	611	612	613	614	615	616	617	618	619	620	621	622	623	624
Y	625	626	627	628	629	630	631	632	633	634	635	636	637	638	639	640	641	642	643	644	645	646	647	648	649	650
Z	651	652	653	654	655	656	657	658	659	660	661	662	663	664	665	666	667	668	669	670	671	672	673	674	675	676

0_c^1 $\overline{00}_c$

Figure 132.

[11] For another type of trinome-digraphic system, see subpar. 66f, in Military Cryptanalytics, Part I.

Such an additive-enciphered digraphic system could pose considerable obstacles in the way of cryptanalysis; nevertheless, given enough traffic, and given enough special circumstances which, as the student has come to appreciate, are inevitable when any system is used among a group of correspondents over a period of time, solution of such a system by a staff of expert and trained cryptanalysts is only a matter of time and labor. If the matrix and its coordinates become known, either through compromise or by analytical reconstruction, then a crib attack is an easy entry into what would otherwise be a very difficult system.

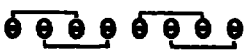
95. Additional remarks.--a. The question of diagnosis and recognition of periodic digraphic systems has been touched on rather lightly in our discussion thus far. It will be helpful to illustrate some general concepts which might facilitate the identification of this family of systems.

(1) Let us suppose a hypothetical system, in which four 4-square matrices are used in succession in a message. That is, the 1st, 5th, 9th... digraphs are enciphered with Matrix No. 1; the 2d, 6th, 10th... digraphs are enciphered with Matrix No. 2; etc. This may be diagrammed as follows, where the ligatures designate the letters enciphered digraphically:

$\widehat{ee}\ \widehat{ee}\ \widehat{ee}\ \widehat{ee}$

The characteristics of such a system would be: (a) the absence of one letter, usually J, in the traffic; (b) the presence of cyclical phenomena in the polygraphic repetitions present that would indicate a period of 8; (c) the general inadequacy of the monographic ϕ tests for the 8 distributions, including an insufficiency for the most part in the expected number of blanks; (d) the prevalence of repetitions of an even number of letters, which repetitions would begin for the most part in alphabets 1, 3, 5, and 7, and would have the tendency to end in alphabets 2, 4, 6, and 8; (e) good results in digraphic distributions, when the digraphic ϕ test is applied to the pairs 1-2, 3-4, 5-6, and 7-8, and poor results when the test is applied to the pairs 2-3, 4-5, 6-7, and 8-1; and (f) negative results when the digraphic χ test is applied, showing that the four digraphic encipherments are cryptographically nonhomogeneous.

(2) Now let us consider what would happen if, instead of the digraphic encipherment of successive pairs of letters, some other type of pairing is used, such as one of the following examples:

Case a: 

Case b: 

Case c: 

When counts are made on the digraphs composed of enciphered adjacent letters of plain text, as in the example in the preceding subparagraph, the digraphic κ_p is .0069; it is this constant which will be used in the digraphic ϕ and χ tests as a measure of the relative "digraphicity" of the cipher text.[12] If, however, the plaintext elements which are digraphically enciphered are not adjacent letters in running plain text but are widely separated, then the digraphs thus formed do not follow the frequency of English plaintext digraphs, but instead depend upon the product of the individual probabilities of English plaintext letters, so that our κ_p in this instance will be the square of the monographic κ_p, $(.0667)^2 = .0044$. This same constant, .0044, would be true in any digraphic encipherment of a more or less random assortment of letters taken from a population having the probabilities of English plaintext letters; thus it applies to a digraphic encipherment of a transposition cipher, or the encipherment of the vertical pairs in a periodic "seriation" such as in the following example:[13]

```
(R E F E R   (O U R M E   (N U M B E
(( ( ( (     ( ( ( ( (     (
E N C E Y    S S A G E    R...
```

The highest frequency digraph of the units thus formed would be $\overline{EE}_p$; next would be the digraphs $\overline{ET}_p$ and $\overline{TE}_p$; and so on, in descending order of the products of the probabilities of the individual letters composing the digraphs.[14]

(3) In case a, above, the digraphic κ_p would be less than .0069, but higher than .0044, since the frequencies of repeated trigraphs in English plain text govern an affinity of combination for certain letters with others; e.g., the frequent trigraphs $\overline{ENT}_p$, $\overline{ION}_p$, $\overline{AND}_p$, $\overline{ING}_p$,... will influence the higher probability of the separated digraphs $\overline{ET}_p$, $\overline{IN}_p$, $\overline{AD}_p$, $\overline{IG}_p$, etc. In case b, however, the digraphic κ_p would be .0044; and in case c, whereas the κ_p of the digraphs 1-8 and 2-7 would be .0044, the κ_p of the digraph 3-6 would theoretically be a shade above .0044 (a refinement indistinguishable in actual practice), while the digraph 4-5 would of course have a κ_p of .0069.

(4) It follows, then, that given enough material, the digraphic ϕ test may be used to diagnose a periodic digraphic cipher, to include the manner of pairing the plaintext letters to produce the cipher digraphs. Furthermore, the digraphic χ test may be employed to discover whether all the digraphic encipherments are cryptographically unique, or whether the same digraphic treatment has been applied to more than one pairing in the

[12] The κ_r constant is the reciprocal of the number of elements possible in the distribution, thus the usual value for the digraphic κ_r is $\frac{1}{676} = .00148$. In the case of systems employing 4-square or 2-square matrices, the κ_r is $\frac{1}{625} = .00160$; if the system employed Playfair squares, the digraphic κ_r is $\frac{1}{600} = .00167$, since doubled letters are usually excluded in this cipher.

[13] In this example, having a seriation interval of 5, if the last block of 10 letters were incomplete, it would be padded by enough nulls to permit the encipherment of the five vertical digraphs.

[14] The solution of systems such as the one just described will be taken up in Military Cryptanalytics, Part IV.

periodic digraphic system. A résumé of the formulas used in digraphic analysis is given below. When the digraphs are composed of enciphered adjacent letters,

$$_2\phi_p = .0069N(N-1) \qquad _2\chi_m = .0069N_1N_2$$

$$_2\phi_r = .0015N(N-1) \qquad _2\chi_m = .0015N_1N_2$$

For digraphs composed of enciphered separated letters,

$$_2\phi_p \cong .0044N(N-1) \qquad _2\chi_m \cong .0044N_1N_2$$

$$_2\phi_r = .0015N(N-1) \qquad _2\chi_m = .0015N_1N_2$$

(5) A rather important consideration that may be overlooked or forgotten by the student of cryptanalytics, is that the ϕ tests on the initial and final letters of a digraphic substitution employing 4-square, 2-square, or Playfair matrices are far from being random distributions. Since these matrices produce only a partially digraphic encipherment,[15] then the encipherments of $\overline{EN}_p$, $\overline{ER}_p$, $\overline{ES}_p$, $\overline{ET}_p$... may result in a series of cipher digraphs in which the E_p has been enciphered more or less monoalphabetically. However, the use of a well-constructed 26x26 table will yield a digraphic encipherment wherein the uniliteral frequency distributions of the initial letters and final letters have random characteristics.

(6) Some pertinent observations may be made here regarding repetitive phenomena in cases such as a, b, and c of subpar. (2), above. In case a, repetitions will begin predominantly in alphabets 1 and 5, and end in alphabets 4 and 8; in case b, repetitions will usually begin in alphabet 1 and end likewise in alphabet 8; and in case c, the delineations of the repetitions will either be from alphabet 1 to alphabet 8, or alphabet 2 to alphabet 7, or alphabet 3 to alphabet 6. Thus, causal tetragraphic repetitions are possible in case a in the first four or last four letters, and tetragraphic repetitions are also possible in case c in the middle four letters; but in case b, causal tetragraphic repetitions have been effectively suppressed.

b. It might be of interest to point out that periodic cryptosystems have been constructed which contain intermixtures of monographic and digraphic treatment, usually for the purpose of achieving a "complexity" in the cryptographic system and thereby defeating enemy cryptanalysis. Such poor subterfuges are--as we have just said--poor; nevertheless, similar ideas are sometimes encountered in examples of poor cryptography. The monographic encipherments in these systems might be uniliteral in form, or biliteral; and in the latter case, the two cipher elements concerned might be adjacent elements in the cipher text, or separated in the cycle of a period-length--as another cryptographic trick to deter cryptanalysis.

[15] Cf. subpar. 68b, Military Cryptanalytics, Part I.

c. The superimposition of messages enciphered in periodic digraphic systems is accomplished generally in the same manner as is the case with monographic ciphers, i.e., aligning the messages by means of known indicators, or juxtaposing messages so that long polygraphic repetitions present are exactly superimposed. In addition, long messages might be correctly superimposed by means of a modification of the kappa test; this test will be treated in the next chapter.

CHAPTER XIV

CONCLUDING REMARKS

96. Miscellaneous periodic polyalphabetic systems.--a. In all the systems treated thus far in this text, each alphabet was used successively to encipher successive single plaintext elements, monographic or digraphic. There is no reason, however, why each alphabet might not be used to encipher 2, 3, or more successive letters at a time; this has the apparent effect of doubling, tripling, or n-tupling the length of the fundamental period, but at the expense of a corresponding reduction in the cryptographic security of the system.

b. As an example of such a system, we may cite that used by the Russians during World War I and known in cryptologic literature as the "Sprungchiffre"; this is illustrated in Fig. 133, below:[1]

	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ю	Я	Ь	Ъ	Ы	Й	І
3	31	61	81	79	57	35	12	56	46	74	37	41	89	43	45	47	97	65	32	59	24	39	38	86	13	84	23	85	62	17	54	58	14
1	31	21	81	79	42	56	72	26	83	27	37	61	89	43	28	23	97	13	29	59	36	32	38	73	63	24	64	85	41	17	25	51	46
4	15	37	21	64	31	17	67	25	49	69	18	23	35	93	59	86	52	13	46	89	74	98	28	47	72	42	45	24	48	87	34	65	39
5	86	92	52	23	18	97	36	13	46	67	54	71	19	14	65	27	93	85	16	79	12	58	76	48	83	34	26	74	62	38	37	29	81
6	25	31	17	42	38	13	41	61	23	45	89	15	84	75	48	54	34	73	14	53	37	24	64	18	28	12	95	57	93	78	82	76	27
7	41	64	84	43	92	53	85	34	67	71	27	26	46	49	24	58	31	75	18	23	98	29	62	39	42	51	95	65	17	96	13	91	94
8	12	56	82	74	13	38	96	54	61	37	83	26	49	68	39	65	57	16	23	95	48	31	78	17	59	73	14	72	98	52	41	53	69
2	73	86	31	93	42	56	21	62	19	47	75	61	32	59	28	84	14	71	35	91	87	69	16	13	25	76	89	38	64	94	95	83	29

Figure 133.

(1) This basically is a dinome-for-letter substitution with 8 random, unrelated alphabets,[2] used in conjunction with a special indicator procedure. The enciphering clerk begins his message with a 5-digit "stutter" group chosen at random, such as 44444, which indicates how many consecutive plaintext letters are to be enciphered by each alphabet. He then enciphers the first four letters (if 44444 is the indicator) with the alphabet labeled "1", after which he enciphers the next four letters with alphabet "2", and so on, repeating the cycle after alphabet "8" is used. At any point during the encipherment after a block of letters (in this case, 4) has been encrypted, the clerk might introduce a new stutter group, such as 66666, which would indicate that each alphabet from now on (without disturbing the sequence of alphabets) will be used to encipher six consecutive plaintext

[1] The matrix illustrated and a description of the cryptography of the system were taken from Andreas Figl, Systeme des Chiffrierens, Graz, 1926, pp. 84-85 and Appendix 19.

[2] The dinomes in the cipher components did not include the digit 0, nor were there any doublets such as 11, 22, etc.

letters. The final cipher text was transmitted in 5-digit groups. For decipherment, a separate deciphering table was necessary.

(2) Changes of keys in this system were effected merely by changing the designations of the 8 alphabets, the basic matrix remaining fixed for a considerable period; in fact, according to official German historical records, the random cipher components of the matrix seem to have been changed only twice during the life of this cryptosystem.[3]

(3) The cryptanalysis of this system is obvious. If the matrix and details of the system were unknown, the study of even a small amount of traffic in the same key would establish the meaning of the stutter indicator group, disclosing the basic periodicity as 8 alphabets. The general method of attack is then along the lines indicated in subpar. 74b. In this latter connection, we would be aided by the idiomorphisms which will manifest themselves when a single alphabet is used to encipher several consecutive plaintext letters; the word КОМИССИЯ, for instance, will quite likely yield an ABBA pattern in the cipher if the indicator is 44444 or higher. Once the matrix becomes known, new alphabet keys may be recovered by a modification of the usual generatrix method.[4]

c. The 4-level dinome variant system illustrated in subpar. 58c of Military Cryptanalytics, Part I, lends itself to polyalphabetic treatment. The basic system, as the student will recall, involves a matrix with a 25-letter (I=J) plain component, and four cipher sequences consisting of 25 dinomes each (in normal numerical order, 01-25, 26-50, 51-75, and 76-00). These sequences, aligned according to a specific key, constitute a matrix providing four cipher equivalents for each plaintext letter.

(1) In Fig. 134, below, there is illustrated a polyalphabetic modification of this system:

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

Figure 134.

[3] This system, introduced toward the end of 1914, was so clumsy to use and caused so many requests for retransmissions--because the Russians were often unable to read their own traffic--that it was withdrawn even before the year was up. The Russians, unaccustomed to such complications, reverted to the simple substitution ciphers (!) they had previously been using.

[4] We could even identify a particular alphabet from occurrences of certain dinomes which are unique in the matrix (such as, in Fig. 133, the dinome 63 in alphabet "2" and 68 in alphabet "7"), or from the ten different dinomes which occur in only two of the alphabets (such as 15, occuring in alphabets "3" and "5").

The four sequences are printed on sliding strips which are free to slide individually in a frame against a normal plain component. The initial dinomes (01, 26, 51, 76) of the strips are here shown aligned to the letters B, E, A, D, respectively, constituting the first specific key. These strips are now locked into place with respect to each other, and the entire compound strip is moved to provide a feature of polyalphabeticity, controlled by a second specific key. For instance, if the dinome 01 in the now-fixed compound strip were set successively against the letters B, A, S, K, E, T during the encipherment of successive plaintext letters, we will have a periodic polyalphabetic substitution system with variants.

(2) The cryptanalysis of this system, too, is quite apparent. What we have fundamentally is a repeating-key system with standard alphabets. This gives us at once the obvious cue: factor the message, convert the cipher letters of each alphabet into their plain-component equivalents, and complete the plain-component sequence. The particular steps for such a system have been treated in subpars. 60n-p of Military Cryptanalytics, Part I.

(3) If the alphabets had not been standard alphabets, the story would be quite different. Fortunately, in such a case the system would become cryptographically preposterous, with the probable result that the enemy's cryptocommunications would break down if such a system were introduced. But even if such a system with mixed alphabets were used, the application of the principles expounded in this text, and the availability of a reasonable amount of traffic, would lead to solution, albeit laborious.

d. Polyalphabetic systems have been encountered in which vowels have been enciphered by vowels, and consonants by consonants.[5] This feature usually has been prompted for reasons of economy existing in once prevailing telegraph company rates. The following sectional matrix[6] is an example of a system possessing the vowel-to-vowel feature:

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

Figure 135.

Other sectional matrices might be constructed in which the cipher equivalents for plaintext vowels are chosen from a group of six cipher letters.

[5] We have already seen an example of this in the system described in par. 76.

[6] A sectional matrix is, as the term implies, a polyalphabetic substitution matrix with two or more distinct sections. The Porta table is an example of a sectional matrix, as is demonstrated by the equivalent matrix illustrated in subpar. 23a, on p. 59.

In such a system, the plaintext letters AEIOUY, comprising 40% of the text, will be replaced by the six new vowel-equivalents in question. The vowel-equivalents can be picked out of the uniliteral distributions on the basis of their outstanding frequencies; and supporting evidence may be found in the "vowel-like" positional spacing of these letters in the cipher text of a cryptogram. While we're on the subject of sectional matrices, it might be mentioned that matrices with multiple sections are also possible, as exemplified in Fig. 136, below:

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

Figure 136.

e. Periodic cryptosystems have been encountered in which the alphabets used consisted of both direct standard and reversed standard alphabets. The rule governing the choice of one type or the other, might be based (1) on the position of the key letter in the repeating key (e.g., the odd letters of the key to be enciphered with direct standard alphabets, the even letters with reversed standard), or (2) on the parity of the key letter in the normal alphabetical sequence (e.g., key letters in the ACEGI... family to be enciphered with direct standard, and key letters in the BDFHJ... family to be enciphered with reversed standard alphabets). Examples such as these should pose no difficulties; the principles of their cryptanalysis have been covered in Chapter IV.

f. The student has seen that, when the cipher component in a periodic cipher is the normal sequence (or any other known sequence), matching of the individual uniliteral frequency distributions for each alphabet is possible, reducing the polyalphabetic cryptogram to a monoalphabetic cipher.[7] Now let us assume we have at hand a particular periodic polyalphabetic cipher of several hundred letters, factoring to six alphabets. We observe that we are able to slide the uniliteral distributions for alphabets 1 and 2 to an excellent match, confirmed by the χ test; alphabets 3 and 4 are also slid to an excellent fit with respect to each other; and likewise alphabets 5 and 6 are also slid to a correct match. Yet it is impossible to find a good match for the three combined distributions, in spite of the paradoxical fact that the cipher component must have been the normal sequence to enable us to match any distributions at all! The obvious explanation (which incidentally was far from obvious when this situation was first encountered) is that the cipher components for the first two alphabets consisted of the normal sequence; the cipher components for alphabets 3 and 4 consisted of a decimation of the normal sequence; and the cipher components for alphabets 5 and 6 consisted of a different decimation of the normal sequence. (The plain component was a mixed sequence.) This demonstrates to the student

[7] Cf. par. 36.

once again that he must always keep an open mind in explaining phenomena, however "incongruous" or "inexplicable" they may be. It is the "improbable" system which may resist the efforts of the cryptanalyst, until he casts aside preconceived idées fixes and rationalizes the causes of the manifestations present to reach an ultimate solution.[8]

97. Periodic Baudot systems.--a. In the previous text we became familiar with the international Baudot code used in teleprinter communication.[9] This code is reproduced for convenience in Fig. 137, below:

UPPER CASE	WEATHER SYMBOLS	↑	⊕	○	⁄	3	→	↘	↓	8	⁄	←	↘	•	●	9	ø	1	4	△	5	7	①	2	/	6	+	−	(	III
	COMMUNICATIONS	−	?	:	$	3	!	&	£	8	'	(	)	•	,	9	ø	1	4	△	5	7	:	2	/	6	"	≈	(	
LOWER CASE		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	BLANK	C R	L F	SPACE	LTR SHIFT	FIG SHIFT
	1	●	●		●	●	●				●	●						●		●		●		●	●	●	●					●	●
	2	●		●				●		●	●	●	●				●	●	●			●	●	●						●		●	●
	3			●			●		●	●		●		●	●			●	●		●		●	●		●	●					●	●	
	4		●	●	●		●	●			●	●		●	●	●			●				●		●				●			●	●
	5		●					●	●				●	●		●	●	●			●		●	●	●	●	●					●	●

Figure 137.

There are many methods for accomplishing the encryption of teleprinter signals, ranging from primitive switching devices yielding nothing more than a simple substitution, to systems involving complicated apparatus producing encrypted signals of great security.

b. The first encrypted teleprinter system was invented during World War I by an American engineer, Gilbert S. Vernam, who called it the "Cipher Printing Telegraph System." Basically, the Vernam system incorporated a specially prepared tape of random teleprinter characters used to key another tape containing the plain text to be encrypted. The two tapes were fed into a "tape reader", and the impulses from these two tapes were combined by what is known as "encipherment according to the Vernam rule", or, more simply, "Baudot addition." That is, like impulses or bauds combine to form a "mark" (symbolized by +), whereas unlike impulses result in a "space" (symbolized by -). For example, if the character on the keying tape is -+++- (≡ C) and the character on the plaintext message tape is ++--- (≡ A), then the result by Baudot addition is -+--+ (≡ L). Of course, by a simple modification of the electrical circuit, the rule of addition could be changed to one where like bauds produce a space and unlike bauds a mark; but the general nature of Baudot addition remains the same.

c. The Vernam system was designed originally to use a long keying tape of approximately 100,000 characters. If the tape were actually random and if it were used only once (i.e., if no portion of the tape were ever used for more than one message), then the system would impart absolute security to the traffic. However, the practicability of production and distribution

[8] In this connection, the student would do well to spend 60 seconds in meditation on the quotation from Aristotle on the back of the title page of this text (from the Politics, i. 2. 9. 1253 a).

[9] At this point it is recommended that the student review the material covered in par. 56 of Military Cryptanalytics, Part I.

of these tapes becomes quite a problem, especially if the traffic transmitted is large in volume, and if there are a large number of correspondents who must intercommunicate in the system. Therefore Vernam proposed that two key tapes in the form of continuous loops be used together, the lengths of which should be prime to each other; the interaction of these tapes would generate a very long keying sequence. For instance, if the two key loops consisted of 1,000 and 999 characters, respectively, then the resultant key would be the product of the lengths of the tapes, or 999,000 characters. This key would not be, strictly speaking, a purely random key, since it is derived from the interaction of two primary components; nor would the security offered, under actual operating conditions, be as great as might be imagined. For certain types of traffic, Vernam even proposed as a convenience the use of a single tape loop constituting a short repeating key; the security of this scheme is either negligible, or only two or three times that amount.

d. Let us now consider the mechanics of Baudot encipherment. Since the international Baudot code is a known alphabet, it follows that we should be able to read two or more messages enciphered with identical keys. Suppose we have the following beginnings of two messages which possessed identical indicators, and are therefore assumed to be in flush depth:

Msg "A": -+--+ +++++ ++--- ++-++ --+-+ ---+- --+-- -+++- ...

Msg "B": +--++ -+--+ +-+-+ ----- ----- +--+- -+--- +--+- ...

If we assume that the first message begins with RE_p (= -+-+- +----), we will derive as key[10] the fragment +++-- +---- (= UE_k). This key, when applied to the beginning of Message "B", yields +---- --++- (= EN_p). This certainly looks promising, and if we extend the RE_p into REQUEST, we will get ENEMY PA... in Message "B". And so on.

e. In practice, teleprinter signals are not analyzed baud by baud as in the foregoing example; instead, each group of five bauds is transcribed as a single Baudot character, and treatment is applied to the 32 Baudot characters resulting from this transcription.[11] In cryptanalysis, we make use of Baudot combination tables which contain all possible combinations of the 32 characters and their Baudot sum. Such a table is

[10] We are assuming here the keying convention that like impulses produce a "+", unlike a "-". This assumption, however, is (except in certain rare cases) immaterial, the opposite rule might actually have been employed in the encryption, without our either knowing it or being able to prove it.

[11] As mentioned in the previous text, it is customary in cryptanalytic work to symbolize the character representing the carriage return by the digit "3", the line feed by "4", the figure shift by "5", the blank by "7", the letter shift by "8", and the space by "9". The beginner should be careful not to confuse these symbols with plaintext digits.

θ^2

θ^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	3	4	5	7	8	9	$(\theta^1+\theta^2)$
A	8	S	L	Y	X	Z	I	3	G	Q	W	C	7	T	9	R	J	P	B	N	5	4	K	E	D	F	H	V	U	M	A	O	
B	S	8	3	K	U	J	M	L	7	F	D	H	G	R	V	T	Z	N	A	P	E	O	Y	5	W	Q	C	9	X	I	B	4	
C	L	3	8	O	T	M	J	S	Q	G	V	A	F	X	D	U	I	5	H	E	P	K	4	N	9	7	B	W	R	Z	C	Y	
D	Y	K	O	8	Q	5	N	4	T	X	B	9	R	G	C	7	E	M	W	I	Z	3	S	J	A	U	V	H	F	P	D	L	
E	X	U	T	Q	8	W	9	R	O	Y	Z	N	4	L	I	3	D	H	5	C	B	7	F	A	J	K	P	M	S	V	E	G	
F	Z	J	M	5	W	8	3	I	H	B	X	7	C	V	R	9	S	O	Q	4	Y	N	E	K	U	A	G	T	D	L	F	P	
G	I	M	J	N	9	3	8	Z	A	C	R	Q	B	D	X	W	L	K	7	Y	4	5	P	O	T	H	F	U	V	S	G	E	
H	3	L	S	4	R	I	Z	8	F	7	9	B	Q	U	W	X	M	E	C	5	N	Y	O	P	V	G	A	D	T	J	H	K	
I	G	7	Q	T	O	H	A	F	8	L	P	J	S	Y	E	K	C	W	M	D	V	U	R	9	N	3	Z	5	4	B	I	X	
J	Q	F	G	X	Y	B	C	7	L	8	5	I	3	O	N	4	A	V	Z	9	W	R	U	D	E	S	M	P	K	H	J	T	
K	W	D	V	B	Z	X	R	9	P	5	8	4	N	M	3	I	U	G	Y	7	Q	C	A	F	S	E	O	L	J	T	K	H	
L	C	H	A	9	N	7	Q	B	J	I	4	8	Z	E	Y	5	G	U	3	X	R	W	V	T	O	M	S	K	P	F	L	D	
M	7	G	F	R	4	C	B	Q	S	3	N	Z	8	K	5	Y	H	D	I	W	9	X	T	V	P	L	J	E	O	A	M	U	
N	T	R	X	G	L	V	D	U	Y	O	M	E	K	8	J	S	9	B	P	A	H	F	7	C	I	4	5	Z	3	W	N	Q	
O	9	V	D	C	I	R	X	W	E	N	3	Y	5	J	8	Z	T	F	4	Q	7	B	H	G	L	P	K	S	M	U	O	A	
P	R	T	U	7	3	9	W	X	K	4	I	5	Y	S	Z	8	V	A	N	B	C	Q	G	H	M	O	E	J	L	D	P	F	
Q	J	Z	I	E	D	S	L	M	C	A	U	G	H	9	T	V	8	4	F	O	K	P	5	Y	X	B	7	R	W	3	Q	N	
R	P	N	5	M	H	O	K	E	W	V	G	U	D	B	F	A	4	8	T	S	L	J	I	3	7	9	X	Q	C	Y	R	Z	
S	B	A	H	W	5	Q	7	C	M	Z	Y	3	I	P	4	N	F	T	8	R	X	9	D	U	K	J	L	O	E	G	S	V	
T	N	P	E	I	C	4	Y	5	D	9	7	X	W	A	Q	B	O	S	R	8	3	Z	M	L	G	V	U	F	H	K	T	J	
U	5	E	P	Z	B	Y	4	N	V	W	Q	R	9	H	7	C	K	L	X	3	8	1	J	S	F	D	T	G	A	O	U	M	
V	4	O	K	3	7	N	5	Y	U	R	C	W	X	F	B	Q	P	J	9	Z	I	8	L	M	H	T	D	A	G	E	V	S	
W	K	Y	4	S	F	E	P	O	R	U	A	V	T	7	H	G	5	I	D	M	J	L	8	Z	B	X	9	C	Q	N	W	3	
X	E	5	N	J	A	K	O	P	9	D	F	T	V	C	G	H	Y	3	U	L	S	M	Z	8	Q	W	R	7	B	4	X	I	
Y	D	W	9	A	J	U	T	V	N	E	S	O	P	I	L	M	X	7	K	G	F	H	B	Q	8	5	4	3	Z	R	Y	C	
Z	F	Q	7	U	K	A	H	G	3	S	E	M	L	4	P	O	B	9	J	V	D	T	X	W	5	8	I	N	Y	C	Z	R	
3	H	C	B	V	P	G	F	A	Z	M	O	S	J	5	K	E	7	X	L	U	T	D	9	K	4	I	8	Y	N	Q	3	W	
4	V	9	W	H	M	T	U	D	5	P	L	K	E	Z	S	J	R	Q	O	F	G	A	C	7	3	N	Y	8	I	X	4	B	
5	U	X	R	F	S	D	V	T	4	K	J	P	O	3	M	L	W	C	E	H	A	G	Q	B	Z	Y	N	I	8	9	5	7	
7	M	I	Z	P	V	L	S	J	B	H	T	F	A	W	U	D	3	Y	G	K	O	E	N	4	R	C	Q	X	9	8	7	5	
8	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	3	4	5	7	8	9	
9	O	4	Y	L	G	P	E	K	X	T	H	D	U	Q	A	F	N	Z	V	J	M	S	3	I	C	R	W	B	7	5	9	8	

Figure 138a.

illustrated in Fig. 138a, containing Baudot sums combined according to the rule that like bauds produce a "+", unlike a "-".[12] In Fig. 138b we have the complementary table of Baudot sums combined according to the rule that unlike bauds produce a "+", like bauds a "-". As has already been mentioned, it is immaterial which rule of addition is assumed; but once a convention is established, it must be continued in the particular problem under study. For the sake of uniformity, in this and the following texts

[12] The student will note that in Baudot addition, because of the binary basis of the arithmetic, P + K = C, P + C = K, and C + K = P. Thus, in Fig. 138a, it will be seen that any combination of two of the characters A, B, and S will yield the third character given.

θ^2

θ^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	3	4	5	7	8	9	$(\theta^1+\theta^2)$
A	7	G	F	R	4	C	B	Q	S	3	N	Z	8	K	5	Y	H	D	I	W	9	X	T	V	P	L	J	E	O	A	M	U	
B	G	7	Q	T	O	H	A	F	8	L	P	J	S	Y	E	K	C	W	M	D	V	U	R	9	N	3	Z	5	4	B	I	X	
C	F	Q	7	U	K	A	H	G	3	S	E	M	L	4	P	O	B	9	J	V	D	T	X	W	5	8	I	N	Y	C	Z	R	
D	R	T	U	7	3	9	W	X	K	4	I	5	Y	S	Z	8	V	A	N	B	C	Q	G	H	M	O	E	J	L	D	P	F	
E	4	O	K	3	7	N	5	Y	U	R	C	W	X	F	B	Q	P	J	9	Z	I	8	L	M	H	T	D	A	G	E	V	S	
F	C	H	A	9	N	7	Q	B	J	I	4	8	Z	E	Y	5	G	U	3	X	R	W	V	T	O	M	S	K	P	F	L	D	
G	B	A	H	W	5	Q	7	C	M	Z	Y	3	I	P	4	N	F	T	8	R	X	9	D	U	K	J	L	O	E	G	S	V	
H	Q	F	G	X	Y	B	C	7	L	8	5	I	3	O	N	4	A	V	Z	9	W	R	U	D	E	S	M	P	K	H	J	T	
I	S	8	3	K	U	J	M	L	7	F	D	H	G	R	V	T	Z	N	A	P	E	O	Y	5	W	Q	C	9	X	I	B	4	
J	3	L	S	4	R	I	Z	8	F	7	9	B	Q	U	W	X	M	E	C	5	N	Y	O	P	V	G	A	D	T	J	H	K	
K	N	P	E	I	C	4	Y	5	D	9	7	X	W	A	Q	B	O	S	R	8	3	Z	M	L	G	V	U	F	H	K	T	J	
L	Z	J	M	5	W	8	3	I	H	B	X	7	C	V	R	9	S	O	Q	4	Y	N	E	K	U	A	G	T	D	L	F	P	
M	8	S	L	Y	X	Z	I	3	G	Q	W	C	7	T	9	R	J	P	B	N	5	4	K	E	D	F	H	V	U	M	A	O	
N	K	Y	4	S	F	E	P	O	R	U	A	V	T	7	H	G	5	I	D	M	J	L	8	Z	B	X	9	C	Q	N	W	3	
O	5	E	P	Z	B	Y	4	N	V	W	Q	R	9	H	7	C	K	L	X	3	8	I	J	S	F	D	T	G	A	O	U	M	
P	Y	K	O	8	Q	5	N	4	T	X	B	9	R	G	C	7	E	M	W	I	Z	3	S	J	A	U	V	H	F	P	D	L	
Q	H	C	B	V	P	G	F	A	Z	M	O	S	J	5	K	E	7	X	L	U	T	D	9	R	4	I	8	Y	N	Q	3	W	
R	D	W	9	A	J	U	T	V	N	E	S	O	P	I	L	M	X	7	K	G	F	H	B	Q	8	5	4	3	Z	R	Y	C	
S	I	M	J	N	9	3	8	Z	A	C	R	Q	B	D	X	W	L	K	7	Y	4	5	P	O	T	H	F	U	V	S	G	E	
T	W	D	V	B	Z	X	R	9	P	5	8	4	N	M	3	I	U	G	Y	7	Q	C	A	F	S	E	O	L	J	T	K	H	
U	9	V	D	C	I	R	X	W	E	N	3	Y	5	J	8	Z	T	F	4	Q	7	B	H	G	L	P	K	S	M	U	O	A	
V	X	U	T	Q	8	W	9	R	O	Y	Z	N	4	L	I	3	D	H	5	C	B	7	F	A	J	K	P	M	S	V	E	G	
W	T	R	X	G	L	V	D	U	Y	O	M	E	K	8	J	S	9	B	P	A	H	F	7	C	I	4	5	Z	3	W	N	Q	
X	V	9	W	H	M	T	U	D	5	P	L	K	E	Z	S	J	R	Q	O	F	G	A	C	7	3	N	Y	8	I	X	4	B	
Y	P	N	5	M	H	O	K	E	W	V	G	U	D	B	F	A	4	8	T	S	L	J	I	3	7	9	X	Q	C	Y	R	Z	
Z	L	3	8	O	T	M	J	S	Q	G	V	A	F	X	D	U	I	5	H	E	P	K	4	N	9	7	B	W	R	Z	C	Y	
3	J	Z	I	E	D	S	L	M	C	A	U	G	H	9	T	V	8	4	F	O	K	P	5	Y	X	B	7	R	W	3	Q	N	
4	E	5	N	J	A	K	O	P	9	D	F	T	V	C	G	H	Y	3	U	L	S	M	Z	8	Q	W	R	7	B	4	X	I	
5	O	4	Y	L	G	P	E	K	X	T	H	D	U	Q	A	F	N	Z	V	J	M	S	3	I	C	R	W	B	7	5	9	8	
7	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	3	4	5	7	8	9	
8	M	I	Z	P	V	L	S	J	B	H	T	F	A	W	U	D	3	Y	G	K	O	E	N	4	R	C	Q	X	9	8	7	5	
9	U	X	R	F	S	D	V	T	4	K	J	P	O	3	M	L	W	C	E	H	A	G	Q	B	Z	Y	N	I	8	9	5	7	

Figure 138b.

we will always assume the convention that, unless otherwise specified, like bauds produce a "+", unlike a "-".[13]

[13] The reason for the inclusion here of the complementary Baudot table illustrated in Fig. 138b, is for purposes of reference in following other technical treatments in which the inverse convention might be used. The table in Fig. 138b can be derived from that in Fig. 138a by adding +++++ (= 8) to all the values in that table.

f. The complete texts of the two messages in flush depth given in subpar. d, above, are as follows:

Message "A"

L8A5H 39CTB KNMIH KEAFR UGGPZ U3P8Y EE5ZX JBD3K WWV8D 9ZEFE
NOIS7 FPZVG NAXJR NQGVH

Message "B"

BLY77 D4DAG VOD9J KSHCR 8OD77 3LS8Z 45YAU KCCE5 FELG8 TPLWV
CKYRH

Let us suppose that, in order to illustrate the method of sliding a probable word, we had not already made an entry into the texts, and let us assume that the word ARTILLERY is in one of the messages. The first thing we will do is to superimpose the two cipher texts and add these texts together, using the Baudot combination table for this purpose. Since the messages are in depth, this is equivalent to removing the effect of the key.[14] The combined cipher stream is shown below:

L8A5H	39CTB	KNMIH	KEAFR	UGGPZ	U3P8Y	EE5ZX	JBD3K	WWV8D	9ZEFE
BLY77	D4DAG	VOD9J	KSHCR	8OD77	3LS8Z	45YAU	KCCE5	FELG8	TPLWV
HLD9J	VBONM	CJRX7	853M8	UXNDC	TSN85	MSZFS	530PJ	EFWGD	JONE7

NOIS7	FPZVG	NAXJR	NQGVH
CKYRH			
X3NTJ			

Our next step is to use a diagram similar to that in Fig. 15 (in par. 22) to facilitate sliding the probable word. In the diagram below, the first row under the combined cipher stream represents the plaintext equivalents in one of the messages if the other contains the A_p of the probable word; the second row represents the equivalents on the trial that the message in question contains the R_p of the probable word; and so forth for all of the letters of the probable word being tried. If our assumption is correct, the word ARTILLERY, when correctly placed, will yield plain text along a diagonal, representing the plain text of the other message.[15] The beginning of this diagram is illustrated in Fig. 139, below:

[14] This may be demonstrated mathematically by the following:

$$(1)\quad P_1 + C_1 = K = P_2 + C_2$$
$$(2)\quad P_1 + C_1 = P_2 + C_2$$
$$(3)\quad P_1 - P_2 = C_1 - C_2$$
$$(4)\quad P_1 + P_2 = C_1 + C_2$$

(The fourth equation follows from the third because of the fact that in Baudot systems, addition is identical with subtraction.) The sum of the ciphers is proved to equal the sum of their plaintext equivalents; the effect of the key is thereby eliminated. The use of the combined cipher stream makes unnecessary the two-step process of $P_1 + C_1 = K$, followed by $K + C_2 = P_2$.

[15] At this stage we are not sure which message contains the word ARTILLERY; this point will be resolved in the next subparagraph.

```
          5         10        15        20        25        30        35
    H L D 9 J V B O N M C J R X 7 8 5 3 M 8 U X N D C T S N S 5 M S Z F S
A 3 C Y O Q 4 S 9 T 7 L Q P E M A U H 7 A 5 E T Y L N B T B U 7 B F Z B
R   U M Z V J N F B D 5 V 8 3 Y R C X D R L 3 B M 5 S T B T C D T 9 O T
T     I J 9 Z P Q A W E 9 S L K T H U W T 3 L A I E 8 R A R H W R V 4 R
I       X L U 7 E Y S Q L W 9 B I 4 Z S I V 9 Y T Q D M Y M 4 S M 3 H M
L         I W H Y E Z A I U T F L P S Z L R T E 9 A X 3 E 3 P Z 3 M 7 3
L           W H Y E Z A I U T F L P S Z L R T E 9 A X 3 E 3 P Z 3 M 7 3
E             U I L 4 T Y H A V E S P 4 E B A L Q T C 5 L 5 S 4 5 K W 5
R               F B D 5 V 8 3 Y R C X D R L 3 B M 5 S T B T C D T 9 O T
Y                 I P 9 E 7 Q R Y Z 4 P Y F Q I A 9 G K I K Z P K 5 U K
```

Figure 139.

From the plaintext fragment ALLY9ACTI revealed along the diagonal, starting at the 20th position, it is clear that both the presence and placement of the probable word ARTILLERY are confirmed. The two plain texts are now inserted in the messages, arbitrarily assuming that ARTILLERY is in Message "A", and they are extended in both directions, yielding the following decryption:[16]

```
                5         10        15        20        25        30        35
Key:  U E J A R L J Y N K B Y W 8 W M X C P P L Y A 5 M B X M 9 K B 3 L P 3
 C1:  L 8 A 5 H 3 9 C T B K N M I H K E A F R U G G P Z U 3 P 8 Y E E 5 Z X
 P1:  R E Q U E S T 9 A D D I T I O N A L 9 A R T I L L E R Y 9 S U P P O R

 C2:  B L Y 7 7 D 4 D A G V O D 9 J K S H C R 8 O D 7 7 3 L S S Z 4 5 Y A U
 P2:  E N E M Y 9 P A T R O L S 9 U N U S U A L L Y 9 A C T I V E 9 N O R T

                40        45        50        55        60        65        70
Key:  9 4 T 5 H P I 7 E G S 3 N 7 8 Q 4 O H K R A
 C1:  J B D 3 K W W V 8 D 9 Z E F E N O I S 7 F P Z V G N A X J R N Q G V H
 P1:  T 9 I N 9 G R E E N V I L L E 9 S E C T O R

 C2:  K C C E 5 F E L G 8 T P L W V C K Y R H
 P2:  H W E S T 9 O F 9 G R E E N V I L L E 9
```

g. In the preceding subparagraph it was stated that, even after the presence of the probable word ARTILLERY was confirmed, we arbitrarily assumed the crib to be in Message "A". It is important to note that there is an element of ambiguity in reading a Baudot depth of two; if two messages are of the same length, it is possible to recover the entire texts of the messages, but the plain texts corresponding to the particular messages might be inverted, i.e., the plain text recovered for Message "A" really belongs to Message "B", and vice versa. This phenomenon, characteristic of Baudot depths only, is brought about by the binary addition inherent in the cryptographic process. An assurance that we have the right

[16] The last 13 characters of Message "A" cannot be decrypted at this time, since in these positions we do not have a second message upon which to test key obtained from plaintext assumptions. If there is a systematic method for the generation of key, and if this method is successfully analyzed, then it will be possible to read the "depth of one" at the end of Message "A".

plain text with the right cipher is only obtained if (a) one message is longer than the other (in which case the logical continuation of the longer message will indicate which of the two plain texts belongs to the message), or (b) a third message is available on which to test the derived key. For example, if the plain texts to our two messages in the preceding subparagraph had been inverted, we would have obtained the following result, shown only in part:

```
                5         10        50        55        60        65        70
Key:  N N X O V W F L 8 N     7 Y Y J 5 5
C1:   L 8 A 5 H 3 9 C T B.....E N O I S 7 F P Z V G N A X J R N Q G V H
P1:   E N E M Y 9 P A T R     V I L L E 9

C2:   B L Y 7 7 D 4 D A G.....V C K Y R H
P2:   R E Q U E S T 9 A D     E 9 S E C T
```

The last word in the second message, SECT(OR?), seems to have been throttled; unless a group is missing, this is indicative that the plain texts of the messages have been inverted. Further confirmation could be obtained if we had a third message against which to try our derived key. For example, let the third message, starting at the same point[17] in the key as the other two, begin with the cipher text VLTPH 5I8Q7 ... In Fig. 140a, the key derived

```
"Key":  N N X O V W F L 8 N
C3:     V L T P H 5 I 8 Q 7
P3:     F E L Z Y Q H L Q W
```

Figure 140a.

```
Key:    U E J A R L J Y N K
C3:     V L T P H 5 I 8 Q 7
P3:     I N 9 R E P L Y 9 T
```

Figure 140b.

above yields gibberish, whereas in Fig. 140b the key recovered in the preceding subparagraph produces valid plain text for the third message.

h. In subpar. f we recovered 57 elements of key, and the key did not repeat within this stretch. If the key is periodic, we would need additional traffic to establish the length of the period, unless the period is too long to make feasible this determination. But even if the key has a long period, if this key has been produced by the interaction of two short key loops, we will be able to partition the key into its two components and reconstruct two equivalent loops with which we could generate the entire key; thus we would be able to read all messages encrypted with these tapes.[18]

---

[17] If this third message were not in flush depth with the other two, we could use a modification of the diagram in Fig. 139 to test the first few letters of the third message against the recovered key (or its complement), and then, if necessary, the last few letters of the third message against the key (or its complement).

[18] Once we have possession of the entire key, a new message could be read by sliding, say, the first 10 cipher characters of the message against the key stream, in a manner identical to that illustrated in Fig. 139. If the indicator system were known, or if there were a long polygraphic repetition in common with an already solved message, a new message could be read without further ado. See also par. 98 (and, in particular, subpar. 98j) in connection with the kappa test for message placement.

i. Let us assume that the key recovered in subpar. f has been produced by two short loops of unknown lengths between 11 and 50 characters, so that the total key might be from 550 (=11x12) to 2450 (=49x50) characters long. The first thing to be determined is the length of the two tapes concerned. What we will do is write out the key successively on various widths, starting at a width of 11; as soon as we have arrived at the correct length for one of the tapes, the length of the other tape will be manifested by a process described below. Consider the following transcriptions of the key on widths of 11, 12, and 13:

1	2	3	4	5	6	7	8	9	10	11
U	E	J	A	R	L	J	Y	N	K	B
Y	W	8	W	M	X	C	P	P	L	Y
A	5	M	B	X	M	9	K	B	3	L
P	3	9	4	T	5	H	P	I	7	E
G	S	3	N	7	8	Q	4	O	H	K
R	A									

Figure 141a.

1	2	3	4	5	6	7	8	9	10	11	12
U	E	J	A	R	L	J	Y	N	K	B	Y
W	8	W	M	X	C	P	P	L	Y	A	5
M	B	X	M	9	K	B	3	L	P	3	9
4	T	5	H	P	I	7	E	G	S	3	N
7	8	Q	4	O	H	K	R	A			

Figure 141b.

1	2	3	4	5	6	7	8	9	10	11	12	13
U	E	J	A	R	L	J	Y	N	K	B	Y	W
8	W	M	X	C	P	P	L	Y	A	5	M	B
X	M	9	K	B	3	L	P	3	9	4	T	5
H	P	I	7	E	G	S	3	N	7	8	Q	4
O	H	K	R	A								

Figure 141c.

Now if we take each one of the foregoing transcriptions and add the first row of key to the second row, the second row to the third, and so on, we will be negating the effect of the key, producing what amounts to a delta or difference stream.[19] At the correct assumption of the length of one of the tapes, the delta stream will repeat itself at an interval corresponding to the length of the other tape.[20] The deltas at the foregoing three widths are shown below:

1	2	3	4	5	6	7	8	9	10	11
F	F	J	K	D	T	G	M	S	4	W
D	Q	M	Y	V	V	Y	I	T	S	O
R	N	U	9	L	O	K	I	7	Q	N
W	L	W	Z	K	5	M	J	E	J	Z
K	B									

Figure 142a.

1	2	3	4	5	6	7	8	9	10	11	12
J	E	U	7	3	A	4	M	E	S	S	Z
T	B	Z	8	I	V	T	E	8	M	H	7
E	P	B	Q	F	P	I	P	Q	N	8	Q
X	T	W	D	Z	F	T	H	I			

Figure 142b.

1	2	3	4	5	6	7	8	9	10	11	12	13
U	F	3	E	5	5	4	O	I	W	X	P	Y
X	T	U	F	3	E	5	5	4	O	I	W	X
P	Y	X	T	U	F	3	E	5	5	4	O	I
W	X	P	Y	X								

Figure 142c.

It is clear from the repeated delta stream manifested in Fig. 142c that the lengths of the two tapes are 13 and 15 characters.

j. Now that we know the lengths of the tapes, we can reconstruct equivalent tapes which will be cryptographically identical with the original tapes.[21] The 57 elements of recovered key are written on a width of 13 (the length of the shorter tape), allowing space between successive rows; and on this diagram every 15 characters (the length of the longer tape) are blocked off beneath the key. We will now arbitrarily assume that the first character on tape II (the longer tape) is a "U"; since the first key character is also a "U", this would make the first element of tape I (the shorter tape) an "8", in order to satisfy the equation $U_1 + 8_2 = U_k$. The "U's" are written under

[19] As has already been noted, in Baudot arithmetic subtraction is identical with addition.

[20] See also subpar. 88g for an analogous situation involving additive-enciphered monome-dinome systems.

[21] These tapes will differ from the original tapes by a constant Baudot character added to all the elements of each key tape.

the key at every cyclic repetition of tape II, and, adding these U's to their corresponding key letters, we obtain elements belonging to tape I; this is shown in Fig. 143a, below. By continuing this process, we are able

```
          1 2 3 4 5 6 7 8 9 10 11 12 13
Tape I:   8
  Key:    U E J A R L J Y N K B Y W
Tape II:  U
          8 W M X C P P L Y A 5 M B
            ]U
          X M 9 K B 3 L P 3 9 4 T 5
              ]U
          H P I 7 E G S 3 N 7 8 Q 4
                ]U
          O H K R A
```

Figure 143a.

```
          1 2 3 4 5 6 7 8 9 10 11 12 13
Tape I:   8 5 9 U E L X L A 9 H Q H
  Key:    U E J A R L J Y N K B Y W
Tape II:  U S T 5 H 8 D O T H L X O
          8 W M X C P P L Y A 5 M B
          8 Q]U S T 5 H 8 D O T H L
          X M 9 K B 3 L P 3 9 4 T 5
          X O 8 Q]U
          H P I 7 E G S 3 N 7 8 Q 4
                ]U
          O H K R A
```

Figure 143b.

to reconstruct both tapes in their entirety, as is shown in Fig. 143b. With these tapes at hand, we can generate the entire key of 195 characters, the first 90 of which are shown below:

```
                    5         10        15        20        25        30
Tape I:   8 5 9 U E L X L A 9 H Q H]8 5 9 U E L X L A 9 H Q H]8 5 9 U
Tape II:  U S T 5 H 8 D O T H L X O 8 Q]U S T 5 H 8 D O T H L X O 8 Q]
  Key:    U E J A R L J Y N K B Y W 8 W M X C P P L Y A 5 M B X M 9 K

                   35        40        45        50        55        60
          E L X L A 9 H Q H]8 5 9 U E L X L A 9 H Q H]8 5 9 U E L X L
          U S T 5 H 8 D O T H L X O 8 Q]U S T 5 H 8 D O T H L X O 8 Q]
          B 3 L P 3 9 4 T 5 H P I 7 E G S 3 N 7 8 Q 4 O H K R A Y X G

                   65        70        75        80        85        90
          A 9 H Q H]8 5 9 U E L X L A 9 H Q H]8 5 9 U E L X L A 9 H Q
          U S T 5 H 8 D O T H L X O 8 Q]U S T 5 H 8 D O T H L X O 8 Q]
          5 V 5 W 8 8 F A 3 R 8 8 Y A N N F 5 5 T 9 Z I X P 8 E A H 8
```

With the key extended to the 70th position, we are now able to read the end of Message "A" which was previously denied to us because the depth of two did not extend that far. The decryption of the last four groups of Message "A" is now revealed as follows:[22]

```
                   55        60        65        70
Key:      Q 4 O H K R A Y X G 5 V 5 W 8 8 F A 3 R
Cipher:   N O I S 7 F P Z V G N A X J R N Q G V H
Plain:    9 S E C T O R 5 M 8 3 4 B U R N S I D E
```

[22] Note the appearance in the plain text of the punctuation and of the carriage-return and line-feed functions.

98. The κ (kappa) test for the superimposition of messages.--a. In subpar. 65c, in connection with a discussion on placing polyalphabetically enciphered messages in depth, it was stated that "even if an extremely long key is employed and several messages beginning at different initial points are enciphered by such a key, this method of superimposition can be employed, provided the messages can be superimposed correctly, that is, so that the letters which fall in one column really belong to one cipher alphabet." In subpar. 72b, in connection with a discussion on the solution of progressive alphabet systems, it was stated that there are three principal means of superimposing messages, as follows: (1) superimposition by means of known indicators; (2) superimposition by ciphertext repetitions; and (3) superimposition by a comparison of columnar frequency distributions. It was furthermore indicated, in an accompanying footnote to subpar. 72b, that the foregoing three means are also applicable for the superimposition of messages in other types of repeating-key systems. If the repeating key is very long (or, for that matter, if the period is undeterminable), then we can bring to bear a statistical method for placing messages in depth, even if the indicator system is unknown and there are no long polygraphic repetitions in common among the messages. This statistical method will be described in the subparagraphs below.

b. One of the most important techniques in cryptanalytics is that known as the "kappa test." This test is useful for several cryptanalytic purposes and one of the most important of them is to ascertain when two or more sequences of letters are correctly superimposed. By the word "correctly" in this case is merely meant that the sequences are so arranged relative to one another as to facilitate or make possible a solution. The test has for its theoretical basis the following circumstances:

(1) If any two rather lengthy sequences of letters are superimposed, it will be found, on examining both members of the successive pairs of letters brought into vertical juxtaposition, that in a certain number of cases the two superimposed letters will coincide. If both sequences of letters constitute random text taken from a 26-letter alphabet, there will be about 38 or 39 such cases of coincidence per thousand pairs examined. This, of course, is because the "kappa" or repeat rate for single letters (i.e., the probability of monographic coincidence) of random text is the reciprocal of the number of elements in the alphabet; so for a 26-character alphabet the κ_r (kappa random) is $\frac{1}{26} = .0385$. If both sequences of letters constitute English plain text, there will be about 66 or 67 such cases of coincidence per thousand pairs examined. This is because the κ_p or repeat rate for single letters of English plain text is .0667. (The student will note that these two constants, κ_r and κ_p, are the ones he has been using in the monographic ϕ and χ tests when 26-letter text has been involved.)

(2) If the superimposed sequences are wholly monoalphabetic encipherments of plain text by the same cipher alphabet, there will still be about 66 or 67 cases of coincidence in each 1,000 cases examined, because in monoalphabetic substitution there is a fixed or unvarying relationship between plaintext- and ciphertext letters, so that for statistical purposes monoalphabetic cipher text behaves just the same as if it were normal plain text.

(3) Even if the two superimposed sequences are not monoalphabetically enciphered text, but are polyalphabetic in character, there will still be about 66 or 67 cases of identity between superimposed letters per thousand cases examined, provided that the two sequences really belong to the same cryptographic system and are superimposed at the proper point with respect to the keying sequence. The reasons for this will be set forth in the succeeding subparagraphs.

(4) Consider the two messages below. They have been enciphered polyalphabetically by the same two primary components sliding against each other. The two messages use the same keying sequence, beginning at the same initial point in that sequence; that is, they are in flush depth. Consequently, the two messages are identically enciphered, letter for letter, and the only differences between them are those occasioned by differences in plain text.

No. 1	Alphabets	16	21	13	5	6	4	17	19	21	21	2	6	3	6	13	13	1	7	12	6
	Plain text	W	H	E	N	I	N	T	H	E	C	O	U	R	S	E	L	O	N	G	M...
	Cipher	E	Q	N	B	T	F	Y	R	C	X	X	L	Q	J	N	Z	O	Y	A	W...

No. 2	Alphabets	16	21	13	5	6	4	17	19	21	21	2	6	3	6	13	13	1	7	12	6
	Plain text	T	H	E	G	E	N	E	R	A	L	A	B	S	O	L	U	T	E	L	Y...
	Cipher	P	Q	N	T	U	F	B	W	D	J	L	Q	H	Y	Z	P	T	M	Q	I...

Note, now, that (a) in every case in which two superimposed cipher letters are the same, the plaintext letters are identical, and (b) in every case in which two superimposed cipher letters are different, the plaintext letters are different. In such a system, even though the cipher alphabet changes from letter to letter, the number of cases of identity or coincidence in the two members of a pair of superimposed cipher letters will still be about 66 or 67 per thousand cases examined, because the two members of each pair of superimposed letters are in the same cipher alphabet and it has been seen in (2) that in monoalphabetic cipher text κ is the same as for plain text,[23] viz., .0667. The two messages may here be said to be superimposed "correctly," that is, brought into proper juxtaposition with respect to the keying sequence.

(5) But now suppose the same two messages are superimposed "incorrectly," that is, they are no longer in proper juxtaposition with respect to the keying sequence. Thus:

No. 1	Alphabets	16	21	13	5	6	4	17	19	21	21	2	6	3	6	13	13	1	7	12	6
	Plain text	W	H	E	N	I	N	T	H	E	C	O	U	R	S	E	L	O	N	G	M
	Cipher	E	Q	N	B	T	F	Y	R	C	X	X	L	Q	J	N	Z	O	Y	A	W

No. 2	Alphabets		16	21	13	5	6	4	17	19	21	21	2	6	3	6	13	13	1	7	12
	Plain text		T	H	E	G	E	N	E	R	A	L	A	B	S	O	L	U	T	E	L
	Cipher		P	Q	N	T	U	F	B	W	D	J	L	Q	H	Y	Z	P	T	M	Q

[23] The fact that in this case each monoalphabet contains but two letters does not affect the theoretical value of κ; and whether the actual number of coincidences agrees closely with the expected number based upon $\kappa = .0667$ depends upon the lengths of the two superimposed sequences.

It is evident that the two members of every pair of superimposed cipher letters are no longer in the same cipher alphabet, and therefore, if two superimposed cipher letters are identical this is merely an "accident," for now there is no basic or general cause for the similarity, such as is true in the case of the correct superimposition. The similarity, if present, is, as already stated, due to chance and the number of such cases of similarity should be about the same as though the two cipher letters were drawn at random from random text, in which $\kappa_r = .0385$. It is no longer true that (a) in every case in which two superimposed cipher letters are the same, the plaintext letters are identical, or (b) in every case in which two superimposed cipher letters are different, the plaintext letters are different. Note, for example, that the superimposed T_c's represent two different plaintext letters and that the S_p of the word COURSE in the first message gives J_c while the S of the word ABSOLUTELY in the second message gives H_c. Thus, it becomes clear that in an incorrect superimposition two different plaintext letters enciphered by two different alphabets may "by chance" produce identical cipher letters, which on superimposition yield a coincidence having no external indications as to dissimilarity in plaintext equivalents. Hence, if there are no other factors which enter into the matter and which might operate to distort the results to be expected from the operation of the basic factor, the expected number of cases of identical cipher letters brought together by an incorrect superimposition will be determined by the value $\kappa_r = .0385$.

(6) But now note also that in the foregoing incorrect superimposition there are two Z_c's and that they represent the same plaintext letter L. This is occasioned by the fact that the plaintext messages happened to have L's in just those two places and that the cipher alphabet happened to be the same both times. Hence, it becomes clear that the same cipher alphabet brought into play twice may "by chance" happen to encipher the same plaintext letter both times, thus producing identical cipher letters. In some systems this source of identity in superimposed cipher letters is of little importance; in other systems, it may materially affect the actual number of coincidences. For instance, if a system is such that it produces a long secondary keying cycle composed of repetitions of short primary keying cycles, an incorrect superimposition of two cryptograms may bring into juxtaposition many of these short cycles, with the result that the actual number of cases of identical superimposed cipher letters is much greater than the expected number based upon $\kappa_r = .0385$. Thus, this source for the production of identical cipher letters in an incorrect superimposition operates to increase the number of cases to be expected from the fundamental constant $\kappa_r = .0385$.

(7) In some systems, where nonrelated cipher alphabets are employed, it may happen that two identical plaintext letters may be enciphered by two different cipher alphabets which, "by chance", have the same equivalent for the plaintext letter concerned. This is, however, a function of the particular cryptographic system and can be taken into account when the nature of the system is known.

(8) In general, then, it may be said that in the case of a correct superimposition the probability of identity or coincidence in superimposed cipher letters is .0667; in the case of an incorrect superimposition, the probability is at least .0385 and may be somewhat greater, depending upon special circumstances. The foregoing situation and facts make possible what has sometimes been referred to as the "coincidence test." Since this test uses the constant κ, the specific designation "kappa test" is more appropriate.

c. The way in which the kappa test may be applied will now be explained. The statement that $\kappa_p = .0667$ means that in 1,000 cases where two letters are drawn at random from a large volume of plain text, there will be about 66 or 67 cases in which the two letters coincide, that is, are identical. Nothing is specified as to what the two letters shall be; they may be two Z's or they may be two E's. This constant, .0667, really denotes a percentage: if many comparisons of single letters are made, the letters being drawn at random from among those constituting a large volume of plain text, 6.67 per cent of these comparisons made will yield coincidences. So, if 2,000 such comparisons are made, the theory indicates that there should be about .0667 x 2,000 = 133 coincidences; if there is sufficient text to permit making 20,000 comparisons, there should be about 1,334 coincidences, and so on.

d. Another way of handling the matter is to find the ratio of the observed number of coincidences to the total number of cases in which the event in question might possibly occur, i.e., the total number of comparisons of superimposed letters. When this ratio is closer to .0667 than it is to .0385, the correct superimposition has been ascertained. This is true because in the case of a correct superimposition both members of each pair of superimposed letters actually belong to the same monoalphabet and therefore the probability of their coinciding is .0667; whereas in the case of an incorrect superimposition the members of each pair of superimposed letters belong, as a general rule, to different monoalphabets,[24] and therefore the probability of their coinciding is nearer to .0385 than to .0667.

e. From the foregoing, it becomes clear that the kappa test involves ascertaining the total number of comparisons that can be made in a given case, as well as ascertaining the actual number of coincidences in the case under consideration. When only two messages are superimposed, this is easy: the total number of comparisons that can be made is the same as the number of superimposed pairs of letters. But when more than two messages are superimposed in a superimposition diagram it is necessary to make a simple calculation, based upon the fact that n letters yield $\frac{n(n-1)}{2}$ pairs or com-

[24] The qualifying phrase "as a general rule" is intended to cover any distortion in results occasioned by the presence of an unusual number of those cases of coincidence described under subpars. b(6) and (7).

parisons, where n is the number of letters in the column.[25] For example, in the case of a column of 3 letters, there are $\frac{3x2}{2} = 3$ comparisons; in the case of a column of 4 letters, there are $\frac{4x3}{2} = 6$ comparisons; and so on. If a superimposition diagram contains columns of various lengths, one merely adds together the number of comparisons for the columns of different lengths to obtain a grand total.[26]

f. In ascertaining the number of coincidences in the case of a column containing several letters, it is again necessary to use the formula $\frac{n(n-1)}{2}$, only in this case n is the number of identical letters in the column. The reasoning, of course, is the same as before. The total number of coincidences is the sum of the number of coincidences for each case of identity. For example, in a column consisting of the ten letters CKBKZKCBBK, there are 3 B's, 2 C's, 4 K's, and 1 Z. The 3 B's yield 3 coincidences, the 2 C's yield 1 coincidence, and the 4 K's yield 6 coincidences. The sum 3 + 1 + 6 makes a total of 10 coincidences in the $\frac{10x9}{2} = 45$ comparisons.

g. The steps in applying the foregoing principles to a typical case will now be described. Suppose several messages enciphered by the same keying sequence but each beginning at a different point in that sequence are to be solved. The indicated method of solution is that of superimposition, the problem being to determine just where the respective messages are to be superimposed so that the cipher text within the respective columns formed by the superimposed messages will be monoalphabetic. From what has been indicated above, it will be understood that the various messages may be shifted relative to one another to many different points of superimposition, there being but one correct superimposition for each message with respect to all the others. First, all the messages might be numbered according to their lengths, the longest being assigned the number 1. Commencing with messages 1 and 2, and keeping number 1 in a fixed position, message 2 is placed under it so that the initial letters of the two messages coincide. Then the two letters forming the successive pairs of superimposed letters are examined and the total number of cases in which the superimposed letters are identical is noted, this giving the observed number of coincidences. Next, the total number of superimposed pairs is ascertained, and the latter is multiplied by .0667 to find the expected number of coincidences. If the

---

[25] This formula is merely a special case under the general formula for ascertaining the number of combinations that may be made of n different things taken r at a time, which is ${}_nC_r = \frac{n!}{r!(n-r)!}$. In studying coincidences by the method indicated, since only two letters are compared at a time, r is always 2; hence the expression $\frac{n!}{r!(n-r)!}$, which is the same as $\frac{n(n-1)(n-2)!}{2(n-2)!}$, becomes $\frac{n(n-1)}{2}$ when $(n-2)!$ is cancelled.

[26] We have already seen examples of this in subpars. 18e and 86c, in connection with the ϕ test. (By definition, ϕ is twice the number of coincidences.)

observed number of coincidences is considerably below the expected number, or if the ratio of the observed number of coincidences to the total number of comparisons is nearer .0385 than to .0667, the superimposition is incorrect and message 2 is shifted to the next superimposition, that is, so that its first letter is under the second of message 1. Again the observed number of coincidences is ascertained and is compared with the expected number. Thus, by shifting message 2 one space at a time (to the right or left relative to message 1) the kappa test finally should indicate the proper relative positions of the two messages. When the correct point of superimposition is reached, the cryptanalyst is rarely left in doubt, for the results are sometimes quite startling. After messages 1 and 2 have been properly superimposed, message 3 is tested first against messages 1 and 2 separately, and then against the same two messages combined at their correct superimposition.[27] Thus message 3 is shifted a step each time until its correct position with respect to messages 1 and 2 has been found. Then message 4 is taken and its proper point of superimposition with respect to messages 1, 2, and 3 is ascertained. The process is continued in this manner until the correct points of superimposition for all the messages have been found. It is obvious that, as messages are added to the superimposition diagram, the determination of correct points of superimposition for subsequent messages becomes progressively more certain and therefore easier.

h. In the foregoing procedure it is noted that there is necessity for repeated displacement of one message against another or other messages. Therefore, it is advisable to transcribe the messages on long strips of cross-section paper, joining sections accurately if several such strips are necessary to accommodate a long message. Thus, a message once so transcribed can be shifted to various points of superimposition relative to another such message, without repeatedly rewriting the messages.[28]

i. In subpar. d, above, we mentioned that in applying the kappa test we might consider a ratio of the observed number of coincidences to an expected number. Since the statistic δ I.C. is defined as the ratio $\frac{\phi_o}{\phi_r}$ and the ξ I.C. is defined as $\frac{\chi_o}{\chi_r}$, we may express the value of kappa as a "κ I.C.";

[27] At first thought the student might wonder why it is advisable or necessary to test message 3 against messages 1 and 2 separately before testing it against the combination of messages 1 and 2. The first two tests, it seems to him, might be omitted and time saved thereby. The reason for this is that if messages 1 and 2 are correctly superimposed, it might be possible that at an incorrect juxtaposition of message 3 we would still get a high number of coincidences against the combination of messages 1 and 2, whereas if we were to try message 3 separately against message 1 and then against message 2, our superimposition error would be disclosed. Thus, a correct superimposition for one of the three combinations may yield such good results as to mask the bad results for the other two combinations.

[28] Machinery for automatically comparing letters in applying the kappa test has been devised. Such machines greatly facilitate and speed up the procedure, and make possible a comparison of many messages among themselves which would otherwise require enormous labor if performed by manual methods.

this κ I.C. will be defined as the ratio of the observed number of coincidences to the expected number of coincidences for random.[29] The advantage of expressing coincidences as a κ I.C. is particularly evident when we are testing digital traffic, wherein the value of κ_p for the underlying intermediate plain text might be unknown.

j. The κ_r constant for digital text is of course $\frac{1}{10} = .1$, and the κ_r for Baudot text is $\frac{1}{32} = .0313$; these are the constants to be used in deriving the κ I.C. for digital and teleprinter traffic. If the exact nature of digital intermediate plain text is known (such as has been indicated, for example, in subpars. 89a-c with respect to monome-dinome systems), the κ_p for a particular digital system may be calculated. As for the κ_p in Baudot text, an analysis of 300 Western Union teleprinter messages (totalling 53,281 characters) revealed that .0566 is the κ_p for English Baudot text.[30]

k. The student is again cautioned that the kappa test is especially reliable only when the messages to be superimposed are rather long (say, 500 letters or more), so that there are a sufficient number of comparisons to permit unequivocal manifestations of the laws of probability. If the messages are too short, an incorrect superimposition may yield an inordinate number of coincidences; or, worse yet, the correct superimposition may not produce a high enough score. Military Cryptanalytics, Part III, will contain more on the kappa test, to include refinements applicable in certain polygraphic weighting systems. In the meanwhile, the student has been exposed to the basic idea of the kappa test, to round out his general technical perspective.[31]

99. Fundamental principles of aperiodic systems.--a. Virtually all systems based upon the principle of a repeating key can be solved because of cyclic or periodic phenomena, which the use of a repeating key exhibits externally or internally in the cryptograms. There are methods for preventing the external manifestation in the cryptograms of these phenomena, or their suppression and disguise if present internally. In some, the principle is to make the elements of a fixed or invariable-length key apply to variable or irregular-length groupings of the plain text so that no cyclic phenomena are exhibited by the cryptograms. In others, the principle is to apply irregular-lengths of the key, or a variable-length key to regular and fixed groupings of the plain text, with the same object in view.

---

[29] The expression "κ I.C." is introduced here to eliminate the confusion which heretofore existed in designating the I.C. derived from aligning two sequences. In the past, designations such as "I.C." or (incorrectly) "ξ I.C." have given rise to ambiguity; likewise, the term "kappa test" is preferable to the former designations "counting coincidences" or "applying the coincidence test", which are broad expressions covering a multitude of syncracies.

[30] The δ I.C. of English Baudot text is therefore 32(.0566) = 1.81.

[31] The student will be able to use the kappa test if he undertakes the analysis of some of the more complex cryptosystems which form a part of the traffic given in Appendix 8

In still other methods, both principles are combined, or the key itself is of such a nature that it does not repeat itself. This may be brought about by constructing or establishing a nonrepeating key, or by employing the key in a special manner. Systems in which the successive letters of the cipher text (or successive letters of the plain text) after the initial letter serve as successive key letters are also used with the object of avoiding or eliminating periodicity. The subparagraphs following will be devoted to a description and discussion of the methods of suppressing periodicity in cryptosystems. These methods as a class are designated as aperiodic systems, as contrasted with the more simple periodic or repeating-key systems we have been studying in this text.

b. One of the simplest methods of avoiding periodicity is to use as the key for the encipherment of one or more messages a series of letters or characters that does not repeat itself. The running text of a book, identical copies of which are in possession of the correspondents, may serve as the key for this purpose. It is only necessary for the correspondents to agree as to the starting point of the key, or to arrange a system of indicating this starting point by means of an indicator letter or group in a fixed position of a cryptogram, usually at the very beginning. Various types of cipher alphabets may be employed in this system: direct or reversed standard alphabets, mixed alphabets drawn up at random, or secondary alphabets resulting from the interaction of two primary sliding components. Such a system is called a running-key system; other names applied to it are nonrepeating-, continuous-, or indefinite-key systems. Telephone directories, the Bible, novels, long poems, standard reference works, numerical tables such as logarithmic and trigonometric tables, etc., have often been used as source books for such keys.

c. In the preceding subparagraph it was shown how suppression of periodicity could be accomplished by means of a continuous key. However, periodicity may also be avoided by special manipulation of an otherwise finite, repeating key. A key word, though limited in length, may nevertheless be applied to variable or invariable-length sections of the plain text. When, for example, each letter of the key serves to encipher a single letter of the plain text, the encipherment is said to be invariable or fixed in this respect. The same is true even if a single letter of the key serves to encipher regular sets of letters of the plain text; for example, each letter of the key may serve to encipher 2, 3, 4..., letters of the text. In these cases periodicity would be manifested externally by the cryptograms, provided that there is a sufficient amount of text to be examined. But if each letter of the key serves to encipher irregular or variable-length groupings of the plain text, then periodicity cannot appear except under rather remote contingencies. Suppose, for example, that so simple a scheme is used as letting each letter of the key serve to encipher a complete word of the text; since words are of irregular lengths and there is no regularity whatever in the sequence of words with respect only to their lengths, periodicity cannot appear. Or, instead of enciphering according to natural word lengths, the irregular groupings of the text might be regulated by other agreements; for example, it might be agreed that every key letter will be used to encipher a number of letters corresponding to the numerical value

of the key letter in the normal alphabet. If the key word in the foregoing two systems is short and the message is long, periodicity may creep in despite the irregular groupings in the encipherment. Sufficient evidence may even be obtained to lead to a disclosure of the length of the key. But if the key consists of a long word, or of a complete phrase or sentence, the text would have to be very long in order that sufficient evidences of periodicity be found to make possible the determination of the length of the key.

d. In the preceding subparagraph, periodicity was suppressed by enciphering variable-length groupings of the plain text. It will now be shown how periodicity may be avoided by enciphering by variable-length groupings of the key. The method consists in interrupting the key; given a key word, it can become a variable-length key by interrupting it according to some prearranged plan, so that it becomes equivalent to a series of keys of different lengths. Thus, the single key word QUESTIONABLY, for example, might be expanded into a sequence of irregular lengths, such as QUESTIONA/QUESTIONAB/QUE/QUESTI/, etc.[32]

(1) Various schemes for indicating or determining the interruptions may be adopted. For example, suppose it may be agreed that the interruption will take place immediately after and every time that the letter R occurs in the plain text; this is the plaintext interruptor method. If the key word were QUESTIONABLY, it would then be interrupted as shown in the following example:

K: QUEQU QUEST IONAB QUEST QUESQ UE
P: OURFR ONTLI NESAR ENOWR EPORT ED...

Since this scheme is cryptographically objectionable because of a preponderance in the key of the first few letters of the key word, it might be advantageous to use the key interruption (in this case, the presence of an R_p in the text being enciphered) either to cause the key to "stutter", or to skip an element in the key; these effects are shown in the following examples:

K: QUEES STION ABLYQ QUEST TIONN AB
P: OURFR ONTLI NESAR ENOWR EPORT ED...

K: QUETI NABLY QUEST ONABL QUESI ON
P: OURFR ONTLI NESAR ENOWR EPORT ED...

[32] Note that here the key word is being interrupted according to its derived numerical key, i.e., first

8 11 3 9 10 4 7 6 1 2 5 12
Q U E S T I O N A B L Y

after the digit 1, then after the digit 2, etc. The example in this subparagraph shows how a long key sequence may be derived from a short basic key.

(2) An alternative to the foregoing method is that employing the idea of a ciphertext interruptor letter. In this case, the interruption of the key takes place every time a designated letter shows up in the cipher text.

(3) It is possible to apply an interrupted key to variable-length groupings of the plain text. In illustrating this method, an indicator (for instance, the letter X) will be inserted in the plain text to show when the interruption takes place. For example, if the plain text is polyalphabetically enciphered by word lengths and one letter of the key word QUESTIONABLY is skipped when the interruptor letter is used, we would have the following:

K: QUE STIONA LYQUE STI ONAB YQUESTIO
P: OUR FRONTX LINES ARE NOWX REPORTED...

Many other variations of the interrupted method are of course possible; Military Cryptanalytics, Part III, will contain more on the cryptography of these systems, as well as include detailed treatment of their cryptanalysis.

e. The last major class of aperiodic systems is that of autokey systems in which the key is automatically derived either from the cipher text (in the case of ciphertext autokey systems) or from the plain text (in plaintext autokey systems).

(1) Suppose, for example, that two correspondents agree to use the word TRUE as an initial key in a ciphertext autokey system, in conjunction with reversed standard alphabets, and the message to be enciphered begins HEAVY INTERDICTION FIRE FALLING AT... The first four letters are enciphered as follows:

K: TRUE
P: HEAVY INTER DICTI ONFIR EFALL INGAT...
C: MNUJ

The cipher letters MNUJ now form the key letters for enciphering the next four plaintext letters, $YINT_p$, yielding $OFHQ_c$. The latter then form the key letters for enciphering the next four letters, and so on, resulting in the following:

K: TRUEM NUJOF HQKOE IIVWU VQODR LOSGD
P: HEAVY INTER DICTI ONFIR EFALL INGAT...
C: MNUJO FHQKO EIIVW UVQOD RLOSG DBMGK

(2) Instead of using the cipher letters in sets, as shown above, the last cipher letter given by the use of the key word may become the key letter for enciphering the next plaintext letter; this new cipher resultant then becomes the key letter for enciphering the following letter, and so on to the end of the message. Thus:

K: TRUEJ LDQXT CZRPW OANIA JFAAP EWJDA
P: HEAVY INTER DICTI ONFIR EFALL INGAT...
C: MNUJL DQXTC ZRPWO ANIAJ FAAPE WJDAH

It is obvious that an initial key word is not necessary; a single prearranged letter will do.

(3) In plaintext autokey systems, the plain text itself serves as the key, after an initial group or an initial letter. This is shown in the following example, wherein the text of the message itself, after the prearranged initial key word TRUE, forms the key text (the enciphering alphabets, as before, are reversed standard alphabets):

K: TRUEH EAVYI NTERD ICTIO NFIRE FALLI
P: HEAVY INTER DICTI ONFIR EFALL INGAT...
C: MNUJJ WNCUR KICYV UPOAX JAIGT XNFLP

(4) One serious objection to plaintext autokey systems is that the results of errors are cumulative; one error affects all the succeeding letters, and if several errors are made, the messages are difficult to decrypt. (This disadvantage can be minimized by the use of automatic cipher devices suitably constructed to accomplish the encipherment with speed and accuracy.) The serious weakness of ciphertext autokey systems, on the other hand, is that the key of an intercepted message is already in the possession of the enemy cryptanalyst, since the cipher text itself is the key. How these systems are solved merits detailed treatment; their cryptanalysis will be discussed in the next volume.

f. There are many elementary cryptomechanisms and cipher devices which have as their principle the suppression of periodicity. A description of some of the more important of these is contained in Appendix 6, "Cryptographic Supplement."

100. Final remarks.--a. In subpars. 13f-h we stated that there are twelve different equations possible for establishing the manner in which two sliding primary components may be used. It was furthermore stated that twelve square tables, equivalent to the twelve different equations, can readily be constructed. Using the two components given in the example,

(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

and the twelve enciphering equations

(1) $\theta_{k/2} = \theta_{i/1}$; $\theta_{p/1} = \theta_{c/2}$

(2) $\theta_{k/2} = \theta_{i/1}$; $\theta_{p/2} = \theta_{c/1}$

(3) $\theta_{k/1} = \theta_{i/2}$; $\theta_{p/1} = \theta_{c/2}$

(4) $\theta_{k/1} = \theta_{i/2}$; $\theta_{p/2} = \theta_{c/1}$

(5) $\theta_{k/2} = \theta_{p/1}$; $\theta_{i/1} = \theta_{c/2}$

(6) $\theta_{k/2} = \theta_{c/1}$; $\theta_{i/1} = \theta_{p/2}$

(7) $\theta_{k/2} = \theta_{p/1}$; $\theta_{i/2} = \theta_{c/1}$

(8) $\theta_{k/2} = \theta_{c/1}$; $\theta_{i/2} = \theta_{p/1}$

(9) $\theta_{k/1} = \theta_{p/2}$; $\theta_{i/1} = \theta_{c/2}$

(10) $\theta_{k/1} = \theta_{c/2}$; $\theta_{i/1} = \theta_{p/2}$

(11) $\theta_{k/1} = \theta_{p/2}$; $\theta_{i/2} = \theta_{c/1}$

(12) $\theta_{k/1} = \theta_{c/2}$; $\theta_{i/2} = \theta_{p/1}$

we can produce the corresponding twelve square tables, the first four rows of which are shown below:[33]

Table No. 1[34]

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

Table No. 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
A	A	H	L	U	R	G	P	S	O	V	Y	B	X	D	E	I	M	K	Q	T	W	Z	C	F	J	N
B	T	A	E	N	K	Z	I	L	H	O	R	U	Q	W	X	B	F	D	J	M	P	S	V	Y	C	G
C	P	W	A	J	G	V	E	H	D	K	N	Q	M	S	T	X	B	Z	F	I	L	O	R	U	Y	C
D	G	N	R	A	X	M	V	Y	U	B	E	H	D	J	K	O	S	Q	W	Z	C	F	I	L	P	T

Table No. 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
A	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
B	X	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
C	O	X	F	B	P	Y	R	C	Q	Z	I	G	S	E	H	T	D	J	U	M	K	V	A	L	W	N
D	N	O	X	F	B	P	Y	R	C	Q	Z	I	G	S	E	H	T	D	J	U	M	K	V	A	L	W

Table No. 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
A	U	B	F	O	L	A	J	M	I	P	S	V	R	X	Y	C	G	E	K	N	Q	T	W	Z	D	H
B	V	C	G	P	M	B	K	N	J	Q	T	W	S	Y	Z	D	H	F	L	O	R	U	X	A	E	I
C	W	D	H	Q	N	C	L	O	K	R	U	X	T	Z	A	E	I	G	M	P	S	V	Y	B	F	J
D	X	E	I	R	O	D	M	P	L	S	V	Y	U	A	B	F	J	H	N	Q	T	W	Z	C	G	K

[33] It is understood that the plaintext letters are to be found in the normal sequence above the square proper, the key letters in the sequence to the left of the square, and the resultant cipher letters within the square.

[34] This table is cryptographically identical with that given in Fig. 9 on p. 21, even though for comparison purposes the horizontal rows of the latter have been interchanged so as to begin successive alphabets with the successive letters of the normal sequence.

Table No. 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
A	A	V	K	M	U	J	D	T	H	E	S	G	I	Z	Q	C	R	Y	P	B	F	X	O	N	W	L
B	B	F	X	O	N	W	L	A	V	K	M	U	J	D	T	H	E	S	G	I	Z	Q	C	R	Y	P
C	C	R	Y	P	B	F	X	O	N	W	L	A	V	K	M	U	J	D	T	H	E	S	G	I	Z	Q
D	D	T	H	E	S	G	I	Z	Q	C	R	Y	P	B	F	X	O	N	W	L	A	V	K	M	U	J

Table No. 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
A	A	T	P	G	J	U	L	I	M	F	C	Z	D	X	W	S	O	Q	K	H	E	B	Y	V	R	N
B	H	A	W	N	Q	B	S	P	T	M	J	G	K	E	D	Z	V	X	R	O	L	I	F	C	Y	U
C	L	E	A	R	U	F	W	T	X	Q	N	K	O	I	H	D	Z	B	V	S	P	M	J	G	C	Y
D	U	N	J	A	D	O	F	C	G	Z	W	T	X	R	Q	M	I	K	E	B	Y	V	S	P	L	H

Table No. 7

	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	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
B	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
C	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
D	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

Table No. 8

	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	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
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	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
D	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

Table No. 9[35]

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

Table No. 10[36]

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

[35] An interesting fact about this case is that if the plain component is made identical with the cipher component (both being the sequence FBPY...), and if the enciphering equations are the same as for Table No. 1, then the resultant cipher square is identical with Table No. 9, except that the key letters at the left are in the order of the reversed mixed component, FXON... In other words, the secondary cipher alphabets produced by the interaction of two identical mixed components are the same as those given by the interaction of a mixed component and the normal component.

[36] The foregoing footnote also applies to this table, except that the key letters at the left will follow the order of the direct mixed component.

Table No. 11

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

Table No. 12

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

b. When these tables are examined carefully, certain interesting points are noted. In the first place, the tables may be paired so that one of a pair may serve for enciphering and the other of the pair may serve for deciphering, or vice versa. For example, Tables 1 and 2 bear this reciprocal relationship to each other; similarly, Tables 3 and 4, 5 and 6, 7 and 8, 9 and 10, and 11 and 12 also show this relationship. In the second place, although the tables are derived from the same pair of components, the internal dispositions of the letters are quite diverse. For example, in Table 1 the horizontal sequences are identical with those of the square in Fig. 9 (on p. 21), but are merely displaced to the right and to the left at different intervals according to the successive key letters. Hence Table 1 shows a horizontally displaced, direct symmetry of the cipher component. Vertically, no symmetry is in evidence;[37] but when Table 1 is more carefully examined, a latent symmetry may be discerned where at first glance it is not apparent. If one takes any two columns of the table, it is found that the interval between the members of any pair of letters in one column is the same as the interval between the member of the homologous pair of letters in the other column, if the distance is measured on the cipher component. For example, consider the 2d and 15th columns (headed by L and I, respectively); take the letters P and G in the 2d column, and J and W in the 15th column. The distance between P and G on the cipher component is 7; the distance between J and W on the same component is also 7. This, of course, is a manifestation of indirect symmetry inherent in the cipher square. It follows, then, that every table which sets forth in systematic fashion the various secondary alphabets, derivable by sliding two primary sequences through all points of coincidence to find cipher equivalents, must show some kind of symmetry both horizontally and vertically. The symmetry is termed visible or direct, if the sequences of letters in the rows (or columns)are the same throughout and are identical with that of one of the primary components; it is termed hidden or indirect if the sequences of letters in the rows or columns are different, apparently not related to either of the components, but which are in reality decimations of one of the primary components.

[37] It is true that the first column within the table shows the plain-component sequence, but this is merely because the method of finding the equivalents in this case is such that this sequence is bound to appear in that column, since the successive key letters are A, B, C, ... Z, and this sequence happens to be identical with the plain component in this case. The same is true of Table Nos. 5 and 11; it is also applicable to the first row of Table Nos. 9 and 10.

c. When the twelve tables are examined in the light of the foregoing remarks, the type of symmetry found in each may be summarized in the following manner:

Table	Horizontal				Vertical			
	Direct symmetry		Indirect symmetry		Direct symmetry		Indirect symmetry	
	Follows plain component	Follows cipher component	Follows plain component	Follows cipher component	Follows plain component	Follows cipher component	Follows plain component	Follows cipher component
1	.....	x	.....	.....	.....	.....	.....	x
2	.....	.....	x	.....	.....	.....	x	.....
3	.....	x	.....	.....	.....	x	.....	.....
4	.....	.....	x	.....	x	.....	.....	.....
5	.....	x	.....	.....	.....	.....	.....	x
6	.....	.....	x	.....	.....	.....	x	.....
7	x	.....	.....	.....	.....	.....	x	.....
8	x	.....	.....	.....	.....	.....	x	.....
9	.....	.....	.....	x	.....	.....	.....	x
10	.....	.....	.....	x	.....	.....	.....	x
11	.....	.....	x	.....	x	.....	.....	.....
12	.....	x	.....	.....	.....	x	.....	.....

Of these twelve types of cipher squares, corresponding to the twelve different ways of using a pair of sliding primary components to derive secondary alphabets, the ones best known and most often encountered in cryptologic studies are Tables 1 and 2, referred to as being of the Vigenère type; Tables 5 and 6, referred to as being of the Beaufort type; and Tables 9 and 10, referred to as being of the Delastelle type.[38] The foregoing exposition might serve to clarify the relationships present among the twelve different cryptographic equations and their associated derived tables.

d. Not much has been said in this text concerning the use of word separators in polyalphabetic systems. This usage is not often encountered in periodic systems; nevertheless, a few words on the subject may not be amiss. Word separators may be incorporated in the cryptosystem in both enciphered and unenciphered form, as follows:

(1) A rare letter, such as X_p, might be used as a word separator in the plain text of a message; this separator would then be enciphered by the alphabets used in the polyalphabetic system. In such a case, the cipher equivalents of X_p, when the periodic cipher text is allocated into its constituent monoalphabetic distributions, will have a predominant frequency.[39]

[38] It will be noted that the tables of the Delastelle type show no direct or visible symmetry, either horizontally or vertically, and because of this fact some authors have declared that they yield more security than do any of the other types of tables, this supposed increase in security is, as the student has come to learn, more illusory than real.

[39] See footnote 8 on p. 96, Military Cryptanalytics, Part I, for the frequency characteristics of English plain text which includes a word separator.

(2) A 25-letter cipher alphabet might be used, with, say, the letter X_c missing in the cipher component; this X_c could then be used as a word separator during the course of the periodic encipherment, without disturbing the period (i.e., as if X_c was the ciphertext equivalent of a word separator in all the alphabets). In such a case, the overwhelming frequency of X_c in the over-all cipher text, together with its characteristic positional appearance spaced throughout the cipher text, would at once proclaim what is going on.

(3) If the X_c in subpar. (2), above, were inserted in the cipher text after periodic encipherment, it would disturb the cyclic phenomena that otherwise might be present in the cryptogram, giving the impression (on hasty analysis) of an aperiodic system. Nevertheless, as in the preceding case, the startling frequency of X_c in the over-all cipher text, coupled with its positional appearance, would enable the cryptanalyst to interpret its significance. Once the X_c's have been eliminated, the cryptogram would be back in periodic form--with the added help of the now known word divisions!

(4) Unenciphered word separators need not be as unsophisticated as in cases (2) and (3), above. For example, in a 25-letter alphabet with a missing X_c, this X_c might be used to replace the second letters of all cipher-text doublets; then the last cipher letter of every word is doubled, to indicate word divisions. (If a word ends in a doubled cipher letter, the second letter of the doublet is replaced by an X_c, followed in this case by another X_c to indicate the end of a word.) In other words, there will be 26 different letters used for word separators, in what appears to be a random selection. Such a case, when first encountered, might be hard to diagnose because of possible mental blocks on the part of the cryptanalyst; nevertheless, the manifestations of the extraordinarily high doublet rate in the cipher text (16% instead of the expected 3.8% for random), the absence of any tripled letters in the cipher text, and the positional appearance of the doublets scattered throughout the text, should be enough clues to enable the correct interpretation of these phenomena.

(5) In polyalphabetic systems yielding digits for the cipher text, a particular digit, not otherwise used in the cryptographic scheme, might be reserved as a word separator, which is then enciphered along with the rest of the text, similar to case (1), above. Or, in the case of additive-enciphered systems, using a monome-dinome system as an example, the digit "9" might be missing in the row and column coordinates; the addition of the key would be performed mod 9 (producing cipher text containing only the digits 0 through 8). The digit 9 is then inserted in the cipher text, to show word divisions, disturbing the cyclic repetitions of the key in the process, similar to case (3), above. Such a scheme might be troublesome, especially since, with a 10-element alphabet, the frequency of the digit 9 might be very close to the random expectation of 10%; but the absence of doubled 9's, and the positional appearance of the 9's in the cipher text, would once again lead to a correct interpretation of the phenomena.

e. The student has seen in subpar. 97f how we are able to read a depth of two in a Baudot system where the key is longer than either of the two messages. The reason this is possible with such a shallow depth is, of course, that the alphabet is a known alphabet. If our depth of two were in a literal system with known alphabets (say, reversed standard alphabets), solution would still be possible, regardless of the length of the total key or its composition; likewise, in a digital system, such as an additive-enciphered monome-dinome system, wherein the matrix and coordinates are known, solution of a depth of two is also possible. In certain situations, it is even possible to read a single message enciphered with an unknown long, non-repeating key, if the key is a plaintext key or is derived from plain text;[40] in effect what we really have is a depth of two in these situations, since a correct plaintext assumption in the message will yield plain text in the key, and vice versa.[41]

f. Now that the formal part of this second volume in a comprehensive series of six basic texts on cryptanalytics is drawing to a close, there are still several topics which must be included if, as indicated at the end of Military Cryptanalytics, Part I, the first two volumes are to contain most of the necessary fundamentals of the science; this information is included in some of the appendices which follow.

(1) Although considerable treatment has been devoted to the solution of monoalphabetic and polyalphabetic substitution ciphers, we have not yet

---

[40] As an example of key derived from plain text, consider an additive-enciphered monome-dinome system in which the key consists of plain text taken from a book in the possession of the correspondents; this key text is then converted into digital form by enciphering it through the same matrix used for encrypting the message.

[41] Perhaps this is as good a place as any to make some observations which are of general interest in connection with the running-key principle, and which have no doubt been the subject of speculation on the part of some students. Suppose a basic, unintelligible, random sequence of keying characters which is not derived from the interaction of two or more shorter keys and which never repeats is employed but once as a key for encipherment. Can a cryptogram enciphered in such a system be solved? The answer to this question must unqualifiedly be this: even if the cipher alphabets are known sequences, cryptanalytic science is certainly powerless to attack such a cryptogram. Furthermore, so far as can now be discerned, no method of attack is likely ever to be devised. Short of methods based upon the alleged phenomena of telepathy--the very objective existence of which is denied by most "sane" investigators today--it is impossible for the author to conceive of any way of attacking such a cryptogram.

This is a case (and perhaps the only case) in which the impossibility of cryptanalysis is mathematically demonstrable. Two things are involved in a complete solution in mathematics: not only must a satisfactory (logical) answer to the problem be offered, but also it must be demonstrated that the answer offered is unique, that is, the only possible one. (The mistake is often made that the latter phase of what constitutes a valid solution is overlooked--and this is the basic error which numerous alleged Bacon-Shakespeare "cryptographers" commit.) To attempt to solve a cryptogram enciphered in the manner indicated is analogous to an attempt to find a unique solution for a single equation containing two unknowns, with absolutely no data available for solution other than those given by that equation itself. It is obvious that no unique solution is possible in such a case, since any one quantity whatsoever may be chosen for one of the unknowns and the other will follow as a consequence. Therefore an infinite number of different answers, all equally valid, is possible. In the case of a cryptogram enciphered in the manner indicated, there is the equivalent of an equation with two unknowns;

touched upon, except for a few remarks of a very general nature, that other large and important class of ciphers, viz., transposition. The fourth volume in this series will deal extensively with these latter systems; in the meanwhile, the student can learn the general methods of solution of some of the more elementary types of transposition systems by studying Appendix 5, "Introduction to the solution of transposition ciphers."

(2) In order to round out the student's background in the cryptography of codes,[42] and of certain aperiodic systems and representative machine ciphers, this information is contained in Appendix 6, "Cryptographic supplement."

(3) In this and the preceding volume there have been numerous references on the importance of the assistance rendered by machine aids in cryptanalysis.[43] In modern communication intelligence operations, these aids play a paramount role, just as they do in other scientific and technological fields. At this point in our studies, it is desirable to have an appreciation of the potentialities of some of the more elementary aids, viz., punched card business machines; Appendix 4, "Applications of electrical tabulating equipment in cryptanalysis", provides this background.

(4) Appendix 7, "Introduction to traffic analysis," will give the student a basic understanding of the fundamentals of this important branch of cryptology, and will make him realize the close bond between cryptanalysis and traffic analysis. Appendix 8, "The ZENDIAN Problem: an exercise

---

the key is one of the unknowns, the plain text is the other. One may conjure up an infinite number of different plain texts and offer any one of them as a "solution." One may even perform the perfectly meaningless labor of reconstructing the "key" for this selected "solution", but since there is no way of proving from the cryptogram itself, or from the reconstructed key (which is unintelligible) whether the "solution" so selected is the actual plain text, all of the infinite number of "solutions" are equally valid. Now since it is inherent in the very idea of cryptography as a practical art that there must and can be only one actual solution (or plain text), and since none of this infinite number of different solutions can be proved to be the one and only correct solution, therefore, our common sense rejects them one and all, and it may be said that a cryptogram enciphered in the manner indicated is absolutely impossible to solve.

It is perhaps unnecessary to point out that the foregoing statement is no longer true when the running key constitutes intelligible text, or if it is used to encipher more than one message, or if it is the secondary resultant of the interaction of two or more short primary keys which go through cycles themselves. For in these cases there is additional information available for the delimitation of one of the pair of unknowns, and hence a unique solution becomes possible.

Now although a true "one-time" system represents the ultimate goal of cryptographic security and is the ideal toward which cryptographic experts have striven for a long time, there is a wide abyss to be bridged between the recognition of a theoretically perfect system and its establishment as a practical means of secret intercommunication. For the mere mechanical details involved in the production, reproduction, and distribution of such keys present difficulties which are so formidable as to destroy the effectiveness of the method as a system of secret intercommunication suitable for groups of correspondents engaged in a voluminous exchange of messages.

[42] Elementary principles of code solution have in effect been touched upon in the discussion on cryptosystems employing syllabary squares and code charts, in par. 80 of Military Cryptanalytics, Part I.

[43] Cf. the first reference on machine aids in subpar. 2f (6), Military Cryptanalytics, Part I.

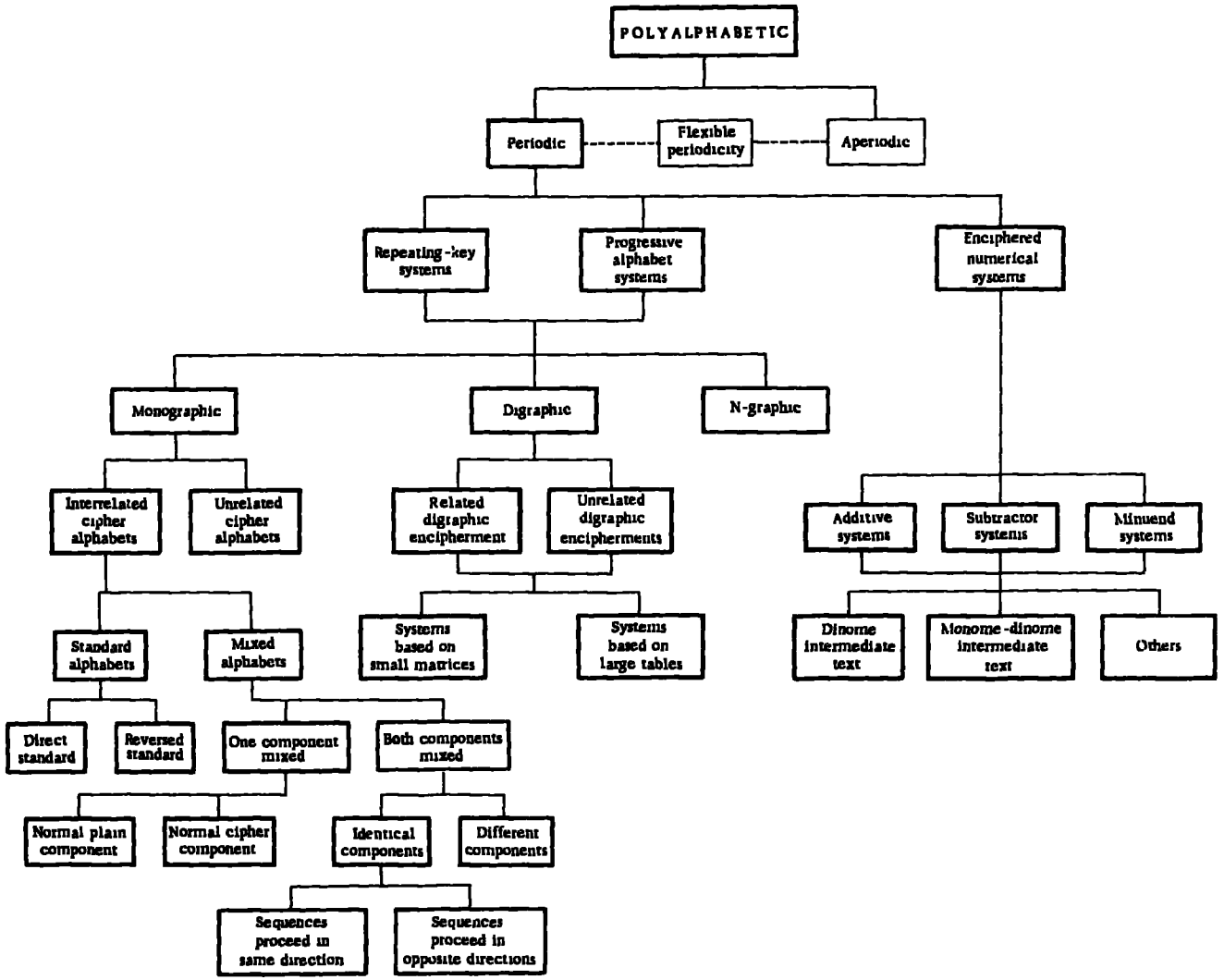
in communication intelligence operations," presents a simulated operational situation involving traffic analysis and cryptanalysis on a volume of traffic intercepted during a hypothetical amphibious operation.

g. As was the case with the previous text, mere reading of the methods of solution of the various types of cryptosystems covered in this volume is not enough to insure complete understanding of the principles and techniques presented. It is therefore strongly recommended that the student solve the problems contained in Appendix 9, "Problems - Military Cryptanalytics, Part II", as a means of acquiring facility and adroitness in the solution of periodic polyalphabetic ciphers. For further study, the messages of the Zendian Problem will provide valuable experience in attacking unknown cryptosystems of all classes, especially as regards cryptanalytic diagnosis.

h. The formal portion of this text will be closed with a synoptic chart of cryptography (continuing the series of charts established in the first volume), found on p. 373, showing the relationships among the various cryptosystems treated in Military Cryptanalytics, Part II. This chart is a continuation of the chart on p. 227 of Military Cryptanalytics, Part I, if we consider the present chart as an amplification of the box labelled "Polyalphabetic" in the previous chart.

* * * * *

YYJIU KDPRJ ZCZUO OVHTR BEFLA E



Synoptic chart of cryptography for Military Cryptanalytics, Part II

(BLANK)

APPENDICES

(BLANK)

APPENDIX 1

GLOSSARY FOR MILITARY CRYPTANALYTICS, PART II

This glossary is limited in scope to cryptologic terms actually appearing in this text, terms likely to be encountered in other cryptologic literature of approximately the same level as this text, and a few other terms considered necessary to complement or to clarify certain definitions.

~~CONFIDENTIAL~~

(BLANK)

GLOSSARY FOR MILITARY CRYPTANALYTICS, PART II

accidental repetition. A repetition produced fortuitously, and not by encipherment of identical plaintext characters by identical keying elements. Cf. CAUSAL REPETITION.

additive, n. A single digit, a numerical group, or a series of digits which for the purpose of encipherment, is added to a numerical cipher unit, code group, or plain text, usually by cryptographic arithmetic.

additive book. A book comprising a group of additive tables.

additive method. The method of encipherment wherein the cryptographic equations are $P + K = C$, and $P = C - K$. Cf. MINUEND METHOD and SUBTRACTIVE METHOD.

additive system. A cryptosystem in which encipherment is accomplished through the application of additives.

additive table. A tabular arrangement of additives.

anagram, n. Plain language reconstructed from a transposition cipher by restoring the letters of the cipher text to their original order.--v. t. To cryptanalyze a transposition cipher in whole or in part by combining one series of characters with another series from the same message to produce plain text, plain code, or intermediate plain text.

analytical machine technique. In the solution of a cryptologic problem, an approach using data processing machinery, computers, or special purpose high-speed electrical or electronic devices.

aperiodic, adj. Characterized by absence of cyclic attributes or usage, as of key in an aperiodic system, q. v.

aperiodic system. A system in which the method of keying results in the suppression of cyclical phenomena in the cryptographic text.

autoencipherment, n. Encipherment by means of an autokey system, q. v.

autokey system. An aperiodic substitution system in which the key, following the application of a previously arranged initial key, is generated from elements of the plain or cipher text of the message.

ban, n. A fundamental scoring unit for the odds on, or the probability of, one of a series of hypotheses. In order that multiplication may be replaced by addition, the ban is expressed in logarithms.

baud, n. The unit impulse of the code employed. Normally the impulse of shortest duration which can appear alone in a given telegraphic system, e.g., the dot in the Morse code, the impulse of teleprinter systems.

Baudot alphabet. A five-unit code applied to teleprinter systems by Jean Maurice Émile Baudot (1845-1903). It employs a 32-element alphabet designed particularly for telecommunications wherein each symbol intended for transmission is represented by a unique arrangement of five mark or space impulses, q. v.

Beaufort system. In cryptology, a polyalphabetic substitution system employing a key word in connection with a Vigenère square, but differing from the normal Vigenère method in its rules for application of the key.

biliteral, adj. Of or pertaining only to cryptosystems, cipher alphabets, and frequency distributions which involve cipher units of two letters or characters. See the more inclusive term DIGRAPHIC; see also BILITERAL FREQUENCY DISTRIBUTION.

biliteral alphabet. A cipher alphabet having a cipher component composed of two-character units.

biliteral frequency distribution. A frequency distribution of pairs formed by combining successive letters or characters. Thus, a biliteral distribution of ABCDEF would list the following pairs: AB, BC, CD, DE, EF. Cf. DIGRAPHIC FREQUENCY DISTRIBUTION.

bipartite alphabet. A multiliteral alphabet in which the cipher units may be divided into two separate parts whose functions are clearly defined, e.g., row indicators and column indicators of a matrix.

bipartite system. A substitution system involving the use of a bipartite alphabet.

blank expectation test. Cf. LAMBDA TEST.

book cipher. A cipher system, utilizing any agreed-upon book, in which the cipher identifies a plain element present in the book.

bust message. A message or set of related messages containing an error in encipherment or violating standard cryptographic security practices so as to jeopardize the security of the message or the system and thus be of potential value to the cryptanalyst.

call sign. Any combination of letters, numbers, or a combination of both, used as the identification for a communications facility, command, authority, activity, or unit; used for establishing and maintaining communications. In U.S. military practice used also for the purpose of identifying message originators and addressees.

callsign, adj. Of or pertaining to a call sign or call signs; as, the callsign generation.

causal isomorph. An isomorph produced by different encipherments of identical plain text.

causal repetition. A repetition produced by the encipherment of identical plaintext characters by identical keying elements. Cf. ACCIDENTAL REPETITION.

cell, n. An individual small square on cross-section paper, grilles, etc.

centiban, n. A scoring unit for probability equal to one one-hundredth of a ban, q. v. A logarithm multiplied by 100.

chain, n. In its cryptologic application, a series, usually cyclic, of letters or other textual symbols following one another according to some rule or law.--v. t. To form into chains.

chi-square (χ^2) table. A mathematical table listing the probabilities of occurrence by chance of a chi-square value higher than those observed in a given case; an adjunct to the chi-square test.

chi-square (χ^2) test. A mathematical means for determining the relative likelihood that two distributions derive from the same source. For example, the test can be used to aid in the determination of whether a distribution is more likely to be random than not; in this usage, the observed distribution is compared with a theoretical distribution representing that which is expected for random. The end result of the test is a value representing the discrepancy between the two distributions which have been compared. This value, called a "chi-square value" may be interpreted as it is, or it may be interpreted through the use of a chi-square table.

chi (χ) test. A test applied to the distributions of the elements of two cipher texts either to determine whether the distributions are the result of encipherment by identical cipher alphabets, or to determine whether the underlying cipher alphabets are related. Also called the cross-product sum.

cifrario militare tascabile. "Pocket military cipher", an Italian World War I cryptosystem involving a Vigenère table with a 36-element cipher component consisting of the dinomes 10-45 in normal order.

cipher, n. 1. A cipher system. 2. A cryptogram produced by a cipher system.--adj. Pertaining to that which enciphers or is enciphered. See also CIPHER TEXT.

cipher alphabet. An ordered arrangement of the letters (or other conventional signs, or both) of a written language and of the characters which replace them in a cryptographic process of substitution. Also called a substitution alphabet.

cipher component. The sequence of a cipher alphabet containing the symbols which replace the plaintext symbols in the process of substitution.

cipher device. A relatively simple mechanical contrivance for encipherment and decipherment, usually hand-operated or manipulated by the fingers, such as sliding strips or rotating disks.

cipher disk. A cipher device consisting of two or more concentric disks, each bearing on its periphery one component of a cipher alphabet.

cipher machine. A relatively complex apparatus or mechanism for encipherment and decipherment, usually equipped with a keyboard and often requiring an external power source.

cipher square. An orderly arrangement or collection of sequences set forth in a rectangular form, commonly a square (e.g., a Vigenère square), and employed in a cipher system.

cipher system. Any cryptosystem in which cryptographic treatment is applied to plaintext units of regular length, usually monographic or digraphic. Cf. CODE SYSTEM.

cipher text. The text of a cryptogram which has been produced by means of a cipher system.

ciphertext, adj. Of or pertaining to the encrypted text produced by a cipher system or to the elements which comprise such text; as the ciphertext distribution. Often shortened to cipher.

ciphertext autokey system. An aperiodic substitution system in which the key, following the application of a previously arranged initial key, is generated from elements of the cipher text of the message.

ciphertext interruptor. In certain aperiodic substitution systems, a specific cipher letter which, by prearrangement, serves to interrupt the keying cycle and thus suppresses periodicity.

code, n. 1. A code system, q. v. 2. A code book, q. v. 3. A system of signals used in electrical or electronic communication.--adj. Pertaining to that which encodes or is encoded.

code book. A book or document used in a code system, arranged in systematic form, containing units of plain text of varying length (letters, syllables, words, phrases, or sentences) each accompanied by one or more arbitrary groups of symbols used as equivalents in messages.--adj. Codebook.

code chart. A chart in the form of a matrix containing letters, syllables, numbers, words, and occasionally, phrases. The matrix has row and column coordinates for the purpose of designating the plaintext elements within.

code group. A group of letters or numbers, or a combination of both, assigned (in a code system) to represent a plaintext element.

code message. A cryptogram produced by encodement.

code system. A cryptosystem in which arbitrary groups of symbols represent plaintext units of varying length, usually syllables, whole words, phrases, and sentences.

code text. The text of a cryptogram which has been produced by means of a code system.

coincidence, n. A recurrence of textual elements (single letters, digits, digraphs, etc.) occurring within a message or between messages.

coincidence test. The kappa test, a statistical test applied to two ciphertext messages to determine whether or not they both involve encipherment by the same sequence of cipher alphabets.

column equating. The process of reduction to monoalphabetic terms of an array of columns of additive-enciphered intermediate plain text, where each different column represents monoalphabetic encipherments by a unique additive.

columnar transposition. A method of transposition in which the cipher text is obtained by inscribing the plain text into a matrix in any way except vertically and then transcribing the columns of the matrix.

common logarithms. Logarithms to the base 10. Also known as Briggsian logarithms.

communication intelligence. Information derived from the study of intercepted communications. Abbr. COMINT.

communication security. The protection resulting from all measures designed to deny to unauthorized persons information of value which might be derived from a study of communications. Cryptosecurity and transmission security are the components of communication security. Abbr. COMSEC.

commutative, adj. As applied to cipher matrices, so constructed as to permit coordinates to be read in either row-column or column-row order without cryptographic ambiguity.

complementary key. Key elements which differ from a derived or true key by their complements, mod n; e.g., 1524 is complementary to 9586, mod 10.

complementary plain text. Intermediate plain text which differs from a derived or true plain text by the complements, mod n.

component, n. 1. One of the two sequences (plain and cipher) which compose a cipher alphabet. 2. An independent or semi-independent part of a machine or device.

compromise, n. The availability of classified material to unauthorized persons through loss, theft, capture, recovery by salvage, defections of individuals, unauthorized viewing, or any other physical means.

computer, n. A machine for executing prescribed programs, especially a high-speed automatically sequenced machine.

continuity, n. Identity with respect to a series of changes. In cryptanalytic procedure, the maintenance of continuity involves keeping current a systematic record of changes in such variable elements as indicators, keys, discriminants, code books, etc., on a given cryptochannel. In traffic analysis, the maintenance of continuity involves the tracing of changes in call signs, frequencies, schedules, or other variable elements assigned to a given radio station, link, or net.

crib, n. 1. Plain text assumed or known to be present in a cryptogram. 2. Keys known or assumed to have been used in a cryptogram.--v. t. 1. To fit assumed or known plain text or keys into the proper position in an encrypted message. 2. In traffic analysis, to equate an unknown element, particularly call signs and addresses, to one that is already known, especially applicable in case of compromise.

cross I.C. The ratio of the observed value of a cross-product sum to that expected for random. Abbr. ξ I.C.

cross-product sum. See CHI TEST.

crypt-, crypto-. In general, a combining form meaning "hidden," "covered," or "secret." Used as a prefix in compound words, crypt-, crypto-, pertains to cryptologic, cryptographic, or cryptanalytic, depending upon the use of the particular word as defined.

cryptanalysis, n. The analysis of encrypted messages; the steps or processes involved in converting encrypted messages into plain text without initial knowledge of the key employed in the encryption. Abbr. C/A.

cryptanalyst, n. A person versed in the art of cryptanalysis.

cryptanalytic, adj. Of, pertaining to, or used in cryptanalytics.

cryptanalytics, n. That branch of cryptology which deals with the principles, methods, and means employed in the solution or analysis of cryptosystems.

cryptanalyze, v. t. To solve by cryptanalysis.

cryptochannel, n. A complete system for encrypted communications between two or more holders.

cryptogram, n. A communication in visible writing which conveys no intelligible meaning in any known language, or which conveys some meaning other than the real meaning.

cryptographic, adj. Of, pertaining to, or concerned with cryptography.

cryptographic ambiguity. Uncertainty as to the method of decryption or as to the meaning intended after decryption; created by a fault in the structure of a cryptosystem.

cryptographic arithmetic. The method of modular arithmetic used in cryptographic procedures which involves no carrying in addition and no borrowing in subtraction.

cryptographic depth. See DEPTH.

cryptographic equation. In cryptosystems involving sliding primary components, the rules determining the derivation of plaintext or ciphertext equivalents in encryption and decryption.

cryptographic security. See CRYPTOSECURITY.

cryptographic system. See CRYPTOSYSTEM.

cryptographic text. Encrypted text; the text of a cryptogram.

cryptography, n. That branch of cryptology which treats of the means, methods, and apparatus for converting or transforming plaintext messages into cryptograms, and for reconverting the cryptograms into their original plaintext form by a simple reversal of the steps used in their transformation.

cryptolinguistics, n. The study of those characteristics of languages which have some particular application in cryptology, (e.g., frequency data, word patterns, unusual or impossible letter combinations, etc.).

cryptologic, adj. Of, pertaining to, or concerned with cryptology.

cryptology, n. That branch of knowledge which treats of hidden, disguised, or encrypted communications. It embraces all means and methods of producing communication intelligence and maintaining communication security; for example, cryptology includes cryptography, cryptanalytics, traffic analysis, interception, specialized linguistic processing, secret inks, etc.

cryptomaterial, n. All documents, devices, and machines employed in encrypting and decrypting messages.

cryptomathematician, n. One versed in cryptomathematics.

cryptomathematics, n. Those portions of mathematics and those mathematical methods which have cryptologic applications.

cryptoperiod, n. The specific length of time throughout which there is no change in cryptographic procedure (keys, codes, etc.).

cryptosecurity, n. That component of communication security which results from the provision of technically sound cryptographic systems and from their proper use.

cryptosystem, n. The associated items of cryptomaterial and the methods and rules by which these items are used as a unit to provide a single means of encryption and decryption. A cryptosystem embraces the general cryptosystem and the specific keys essential to the employment of the general cryptosystem.

cyclic, adj. Periodic; continuing or repeating so that the first term of a series follows the last; characterized by a ring or closed-chain formation.

cyclic additive. A sequence of key digits used as a repeating additive.

cyclic permutation. Any rearrangement of a sequence of elements which merely involves shifting all the elements of common distance to the right or left of their initial positions in the sequence, the relative order remaining undisturbed; such a rearrangement requires that one consider the basic sequence as being circular in nature so that, for example, shifting that element which occupies the left-most position in the sequence one place to the left places this element in the right-most position.

cyclic phenomena. Periodic ciphertext repetitions in a cryptogram enciphered with a repeating key.

daily keying element. That part of the specific key that changes at predetermined intervals, usually daily.

deciban, n. A scoring unit for probability factors equal to one-tenth of a ban, q. v. A logarithm multiplied by 10.

decimated alphabet. An alphabet produced by decimation, q. v.

decimation, n. The process of selecting members of a series by counting off at an arbitrary interval, the original series being treated as cyclic; or the result of the foregoing process.

decimation-mixed sequence. A mixed sequence produced by decimation, q. v.

decipher, v. t. To convert an enciphered message into its equivalent plain text by a reversal of the cryptographic process used in the encipherment. (This does not include solution by cryptanalysis.)

deciphering alphabet. A cipher alphabet in which the sequence of symbols in the cipher component is arranged in normal order for convenience in decipherment.

deciphering equation. In cryptosystems involving sliding primary components, the rules determining the derivation of plaintext equivalents of cipher elements.

decipherment, n. 1. The process of deciphering. 2. The plain text of a deciphered cryptogram. 3. In an enciphered code system, the code text resulting from the removal of the encipherment.

decode, n. 1. That section of a code book in which the code groups are in alphabetical, numerical, or other systematic order. 2. The decoded, but not translated, version of a code message.--v. t. To convert an encoded message into its plain text by means of a code book. (This does not include solution by cryptanalysis.)

decodement, n. 1. The process of decoding. 2. The decoded, but not translated, version of a cryptogram.

decrypt, n. A decrypted, but not translated, message.--v. t. To transform an encrypted communication into an intelligible one by a reversal of the cryptographic process used in encryption. (This does not include solution by cryptanalysis.)

decryption, n. The act of decrypting.

degarble, v. t. To make emendations in a garbled text.

Delastelle system. In cryptology, a polyalphabetic substitution system employing a key word in connection with a Vigenère square, but differing from the normal Vigenère method in its rules for application of the key.

delta, n. Lateral differences either of consecutive elements of text, or of textual elements at a constant interval apart. v. t. To derive lateral differences of a text.

delta (δ) I.C. The ratio of the observed number of coincidences to that expected for random; the index of coincidence applied to a small sample. See INDEX OF COINCIDENCE.

delta stream. The stream derived by taking lateral differences of a text.

depth, n. 1. The condition which results when two or more sequences of encrypted text have been correctly superimposed with reference to the keying thereof. Sequences so superimposed are said to be in depth. 2. The number of such superimposed sequences, as a depth of three.

depth reading. The cryptanalysis of messages in cryptographic depth.

derived numerical key. A key produced by assigning numerical values to a selected literal key.

diagnosis, n. In cryptanalysis, a systematic examination of cryptograms with a view to discovering the general system underlying these cryptograms.

digraph, n. A pair of letters.

digraphic, adj. Of or pertaining to any combination of two characters.

digraphic frequency distribution. A frequency distribution of successive pairs of letters or characters. A digraphic distribution of ABCDEF would list the pairs: AB, CD, EF. Cf. BILITERAL FREQUENCY DISTRIBUTION.

digraphic substitution. Encipherment by substitution methods in which the plaintext units are pairs of characters and their cipher equivalents usually consist of two characters.

dinome, n. A pair of digits.

direct standard cipher alphabet. A cipher alphabet in which both the plain and cipher components are the normal sequence, the two components being juxtaposed in any of the noncrashing placements. Cf. REVERSED STANDARD CIPHER ALPHABET.

direct symmetry. A property of a cipher square in which the sequence of characters in the rows or the columns is the same throughout and is visibly identical with that of one of the primary components, (i.e., patent symmetry as opposed to the latent symmetry of a cipher square exhibiting indirect symmetry).

discriminant, n. A group of symbols indicating the specific cryptosystem used in encrypting a given message. Also called system indicator.

distribution, n. See FREQUENCY DISTRIBUTION.

doublet, n. A digraph or dinome in which a letter or a digit is repeated (e.g., LL, EE, 22, 66, etc.).

double transposition. A cryptosystem in which the characters of a first or primary transposition are subjected to a second transposition.

encipher, v. t. To convert a plaintext message into unintelligible language or signals by means of a cipher system.

enciphered code. A cryptographic system in which a cipher system is applied to encoded text.

enciphering alphabet. A cipher alphabet in which the sequence of letters in the plain component is arranged in normal order for convenience in encipherment.

enciphering equation. In cryptosystems involving sliding primary components, the rules determining the derivation of ciphertext equivalents of plaintext elements.

encipherment, n. 1. The process of enciphering. 2. Text which has been enciphered.

encode, n. That section of a code book in which the plaintext equivalents of the code groups are in alphabetical, numerical, or other systematic order.--v. t. To convert a plaintext message into unintelligible language by means of a code book.

encodement, n. 1. The act or process of encrypting plain text with a code system. 2. The text produced by encoding plain text.

encrypt, v. t. To convert a plaintext message into unintelligible language or signals by means of a cryptosystem.

encrypted text. The text produced by the application of a cryptosystem to a plaintext message.

encryption, n. 1. The act of encrypting. 2. Encrypted text.

equivalent primary component. A sequence which has been or can be developed from the original sequence, or basic primary component, by applying a decimation process to the latter.

factoring, n. 1. An arithmetical process of determining the period of a periodic polyalphabetic cipher by a study of the intervals between repetitions. 2. In transposition, the process of determining column lengths by studying intervals between elements.

flat, adj. As a characteristic of a frequency distribution, implies statistically not rough. Cf. SMOOTHNESS.

flush depth. 1. The condition which results when two or more encrypted messages have been correctly superimposed, each starting at the same point in the key. 2. The number of such superimposed sequences, as a flush depth of three.

fractionation, n. A cryptographic system in which plaintext units are represented by two or more cipher symbols which in turn are dissociated and subjected to further encipherment by substitution or transposition or both.

frequency, n. In cryptology, the number of actual occurrences of a textual element within a given text. Cf. RELATIVE FREQUENCY.

frequency distribution. A tabulation of the frequency of occurrence of plaintext, ciphertext, or codetext units in a message or a group of messages. A frequency count.

frequency weight. A weight established for a key, plaintext, or ciphertext element on the basis of its arithmetical frequency.

gamma (γ) I.C. Index of coincidence applied to a universe, i.e., a very large sample. See INDEX OF COINCIDENCE.

garble, n. An error in transmission, reception, encryption, or decryption which renders incorrect or undecryptable a message or transmission or a portion thereof.--v. t. To make an error in transmission, reception, encryption, or decryption of a message.

general cryptosystem. The basic invariable method of encryption of a cryptosystem, excluding the specific keys essential to its employment.

general solution. A solution dependent on exploiting the inherent weaknesses of the cryptographic system arising from its own mechanics, without the presence of any specialized circumstances.

general system. See GENERAL CRYPTOSYSTEM.

generatrix, n. 1. One decipherment or encipherment out of a set of decipherments or encipherments of the same text, the set being exhaustive on a given hypothesis or given cryptographic principle. The elements of a generatrix are at a constant alphabetic (normal or cipher) interval from those of another generatrix of the set, (e.g., as in a strip system). 2. In connection with the method of completing the plain component sequence, any one of the rows, each of which represents a trial "decipherment" of the original cryptogram.

grid, n. In a transposition system, a form or matrix over which a grille is placed for the purpose of enciphering or deciphering.

grille, n. 1. A sheet of paper, cardboard, thin metal, plastic, or like material in which perforations have been made for the uncovering of spaces in which textual units or key may be written or read on a grid. 2. A matrix in which certain squares are blocked out or otherwise marked so as not to be used. Also called a stencil.

Gronsfeld system. A polyalphabetic substitution system employing the first 10 alphabets of a direct standard Vigenere table in conjunction with a numerical key. The cipher equivalent of a given plaintext letter is found by counting down the normal sequence the number of positions indicated by the numerical key; thus A_p with key of 4 is E_c.

group, n. 1. A number of digits, letters, or characters forming a unit for transmission or for cryptographic treatment. 2. In radio, one or more links whose stations work together as a communication entity under a common operating control.

high-echelon, adj. Pertaining to organizational units at the army divisional level or higher, or their equivalents in other Services.

high-grade, adj. Pertaining to a cryptosystem which offers a maximum of resistance to cryptanalysis; for example: (1) complex cipher machines, (2) one-time systems, (3) two-part codes enciphered with an additive book. Cf. LOW-GRADE and MEDIUM-GRADE.

I.C. Index of coincidence, q. v.

identification, n. 1. In cryptanalysis, determination of the plaintext value of a cipher element or code group. 2. In traffic analysis, determination of the specific unit, aircraft, ship, or Order of Battle involved in a given instance, but not its location.

identify, v. t. 1. In cryptanalysis, to determine the plaintext value of a cipher element or code group. 2. In traffic analysis, to determine the specific unit, aircraft, ship, or Order of Battle involved in a given instance, but not its location.

idiomorph, n. A plaintext, cipher, or key sequence which contains or shows a pattern in its construction as regards the number and positions of repeated elements.

idiomorphic, adj. Exhibiting the phenomenon of idiomorphism.

idiomorphism, n. In a plaintext, cipher, or key sequence, the phenomenon of showing a pattern as regards the number and positions of repeated letters.

index letter. That letter of a component of a cipher alphabet against which the key letter in the other component is juxtaposed.

index of coincidence. The ratio of the observed number of coincidences in a given body of text or keys to the number of coincidences expected in a sample of random text of the same size. Commonly known as I.C. See also DELTA (δ) I.C. and GAMMA (γ) I.C.

indicator, n. In cryptography, an element inserted within the text or heading of a message which serves as a guide to the selection or derivation and application of the correct system and key for the prompt decryption of the message. See also the more precise terms DISCRIMINANT and MESSAGE INDICATOR.

indirect symmetry. A property of a cipher square in which a pair of rows or pair of columns may be united to give a decimation of one of the primary components; i.e., latent symmetry as opposed to the patent symmetry of a cipher square exhibiting direct symmetry. Cf. DIRECT SYMMETRY.

initial key. In autokey systems, the key element or elements which are used to encipher the beginning of a message before autokeying takes place.

inscription, n. 1. In a transposition system, the process of writing a message into a matrix. 2. The process of writing a series of numbers, letters, or coded meanings into a code chart or table.

intelligence, n. The product resulting from the collecting and processing of information concerning actual and potential situations and conditions relating to foreign activities and to foreign or enemy-held areas. This processing includes the evaluation and collation of the information obtained from all available sources, and the analysis, synthesis and interpretation thereof for subsequent presentation and dissemination.

intercept, n. A copy of a message obtained by interception.--v. t. To engage in interception.

interception, n. The process of gaining possession of communications intended for others without obtaining the consent of the addressees and ordinarily without delaying or preventing the transmission of the communications to those addressees.

intermediate plain text. Plain text enciphered by elements of a multiliteral substitution (such as that produced by a dinome matrix or a monome-dinome matrix), which "intermediate plain text" is then subjected to further encipherment.

internal text. In concealment systems, the secret text which is enveloped by open or apparently innocent text.

interrelated cipher alphabets. Cipher alphabets most commonly produced by the interaction of two primary components which, when juxtaposed at various points of coincidence, can be made to yield secondary alphabets.

interrupted-key columnar transposition. A columnar transposition system in which the plaintext elements are inscribed in a matrix in rows of irregular length as determined by a numerical key.

interruptor system. A polyalphabetic substitution system in which the key is interrupted upon the occurrence of a prearranged letter or letters of the plain text or of the cipher text.

interval, n. A distance between two points or occurrences, especially between recurrent conditions or states. The number of units between a letter, digraph, code group, etc., and the recurrence of the same letter, digraph, code group, etc., counting either the first or second occurrence but not both. Frequently called cryptanalyst's interval.

intuitive method. A method of solution making use of probable words, probable keys, the supposed psychology of the encipherer, the reports of espionage services, and all other factors derivable from a given situation.

inverse matrix. In the cryptanalysis of a polyalphabetic substitution system, a reconstruction matrix in which the cipher elements are located in the row above the matrix, and the plaintext equivalents are placed within the matrix.

isolog, n. A cryptogram in which the plain text is identical or nearly identical with that of a message encrypted in another system, key, code, etc.

isologous, adj. Pertaining to or having the nature of an isolog.

idiomorph, n. A sequence of plain, cipher, or key elements which exhibits an idiomorph identical with that of another sequence.

isomorphic, adj. Of or pertaining to ismorphism or isomorphs.

isomorphism, n. The existence of two or more identical idiomorphs.

Jefferson cipher. A polyalphabetic substitution system invented by Thomas Jefferson and independently at a later date by the French cryptographer Bazeries. It provided for encipherment by means of a manually operated device involving a number of revolvable disks, each bearing a mixed alphabet on its periphery.

kappa (κ) I.C. In comparing two superimposed sequences of text, the ratio of the observed number of coincidences to that expected for random.

kappa plain (κ_p) constant. A mathematical constant employed in coincidence tests such as the phi test, to denote the probability of coincidence of a given plaintext element or unit. It is the sum of the squares of the probabilities of occurrence of the different textual elements or units as they are employed in writing the text; for example, in English telegraphic plain text, the monographic and digraphic plain constants are .0667 and .0069, respectively.

kappa random (κ_r) constant. A mathematical constant employed in coincidence tests such as the phi test to denote the probability of coincidence of a given textual element in random text. It is merely the reciprocal of the total number of characters used in writing the text. If a 26-letter alphabet were employed, for instance, the constant denoting the probability of coincidence of various textual elements would be derived as follows:

a.	single letters	1/26 = .0385
b.	digraphs	1/676 = .00148
c.	trigraphs	1/17,576 = .000057

kappa (κ) test. A test applied to two superimposed sequences of text to determine whether or not they are correctly superimposed. See KAPPA (κ) I.C.

key, n. 1. In cryptography, a symbol or sequence of symbols applied to successive textual elements of a message to control their encryption or decryption. 2. A specific key.

key book. A book containing key text, or plain text forming specific keys.

keyed columnar transposition. A transposition system in which the columns of a matrix are taken off in the order determined by the specific key, which is often a derived numerical key.

key letter. A letter of key; especially in polyalphabetic ciphers, the letter determining which of the available cipher alphabets is used to encipher a particular letter.

key phrase. An arbitrarily selected phrase used as a key or from which a key is derived.

key recovery. The cryptanalytic reconstruction of a key.

key text. Text from which a key is derived.

key word. An arbitrarily selected word used as a key per se, or from which a key is derived.

keyword, adj. Of or pertaining to a key word or key words; as, the keyword recovery.

keyword-mixed alphabet. An alphabet constructed by writing a prearranged key word or key phrase (repeated letters, if present, being omitted after their first occurrence), and then completing the sequence from the unused letters of the alphabet in their normal sequence.

lambda (Λ) test. A test for monoalphabeticity in a message, based on a comparison of the observed number of blanks in its frequency distribution with the theoretically expected number of blanks both in (a) a normal plaintext message of equal length and (b) a random assortment of an equal number of letters. Also called the blank-expectation test.

latent repetition. A plaintext repetition not apparent in cipher text but susceptible of being made patent as a result of analysis.

lateral difference. See DELTA.

Latin square. A cipher square in which no row or column contains a repeated symbol.

lexical, adj. Of, pertaining to, or connected with words. In its cryptologic sense, the word is used to characterize those cryptographic methods (chiefly codes) which deal with plaintext elements comprising complete words, phrases, and sentences.

link, n. The existence of direct communication facilities between two points.

literal key. A key composed of a sequence of letters. Cf. NUMERICAL KEY.

logarithmic score. The sum of a set of logarithmic weights of a given sample of text.

logarithmic weights. Numerical weights assigned to units of text, which weights are actually logarithms of the probabilities of the textual units, and which are used to evaluate the results of certain cryptanalytic operations.

low-echelon, adj. Pertaining to organizational units below the level of the army division or its equivalent in the other Services.

low-grade, adj. Pertaining to a cryptosystem which offers only slight resistance to cryptanalysis; for example: (1) Playfair ciphers, (2) single transposition, (3) unenciphered one-part codes. Cf. MEDIUM-GRADE and HIGH-GRADE.

mark impulse. One of the two types of impulses used in teleprinter transmission; normally, that impulse during which current flows through the teleprinter receiving magnet. The other type of impulse is the space impulse, q. v.

matching, adj. Shifting of two or more monoalphabetic frequency distributions so as to bring them into proper alignment for amalgamation into a single monoalphabetic distribution.

matrix, n. A geometric form or pattern. In transposition systems, the figure or diagram in which the various steps of the transposition are effected; in substitution systems, the figure or diagram containing the sequence or sequences of plain text or cipher symbols.

medium-grade, adj. Pertaining to a cryptosystem which offers considerable resistance to cryptanalysis; for example: (1) strip ciphers, (2) double transposition, (3) unenciphered two part-codes. Cf. LOW-GRADE and HIGH-GRADE.

message, n. Any thought or idea expressed in plain or secret language, prepared in a form suitable for transmission by any means of communication.

message indicator. A group of letters or numbers placed within an encrypted message to designate the keying elements applicable to that message.

message keying element. That part of the key which changes with every message.

minuend method. The method of encipherment wherein the cryptographic equations are K - P = C, and K - C = P. Cf. ADDITIVE METHOD and SUBTRACTIVE METHOD.

minuend system. A system in which encipherment is accomplished by subtracting the plain text from the key; in the process of decipherment, the enciphered text is subtracted from the key. Cf. SUBTRACTIVE SYSTEM.

mixed cipher alphabet. A cipher alphabet in which the sequence of letters or characters in one or both of the components is not the normal sequence.

mixed-length system. A cryptosystem in which the units of cipher text or code text are of irregular or nonconstant length, as for example, a monome-dinome system, or a code system employing both 4-letter and 5-letter groups.

mnemonic key. A key so constructed as to be easily remembered.

modular, adj. Pertaining to a modulus, q. v.

modulo, adv. With respect to a modulus, q. v. (Abbr. mod; e.g., mod 10, mod 26, etc.)

modulus, n. Scale or basis of arithmetic; the number n is called the modulus when all numbers which differ from each other by n or a multiple of n are considered equivalent.

monoalphabet, n. Monoalphabetically enciphered text. Also a frequency distribution exhibiting monoalphabeticity, q. v.

monoalphabetic, adj. Of or pertaining to monoalphabeticity, q. v.

monoalphabeticity, n. A characteristic of encrypted text which indicates that it has been produced by means of a single cipher alphabet or an unenciphered code system using a single code book. It is normally disclosed by frequency distributions which display "roughness," or pronounced variation in relative frequencies.

monoalphabetic substitution. A type of substitution employing a single cipher alphabet by means of which each cipher equivalent, composed of one or more elements, invariably represents one particular plaintext unit, wherever it occurs throughout any given message.

monograph, n. A single letter.

monographic, adj. Of or pertaining to any units comprising single characters.

monographic substitution. Encipherment by substitution methods in which the plaintext units are single characters and their cipher equivalents usually consist of single characters.

monome, n. A single digit. A contraction of mononome.

monome-dinome system. A substitution system in which certain plaintext elements have single-digit cipher equivalents, while others are represented by pairs of digits.

multiliteral, adj. Of or pertaining only to cryptosystems, cipher alphabets, and frequency distributions which involve cipher units of two or more letters or characters. See also POLYGRAPHIC.

multiliteral cipher alphabet. A cipher alphabet in which one plaintext letter is represented by cipher units of two or more elements.

multiliteral system. A substitution system involving one or more multiliteral cipher alphabets.

multiple-alphabet system. A type of substitution in which successive lengthy portions of a message are each monoalphabetically enciphered by a different alphabet; monoalphabetic encipherment by sections.

multiple anagramming. A process of anagramming simultaneously several transposition messages of the same length that have been enciphered with the same key.

natural logarithms. Logarithms to the base e (= 2.71828...). Also known as Napierian logarithms.

Nihilist system. A system employing a 5x5 square with numerical coordinates for bipartite encipherment, followed by additive encipherment with a key derived by enciphering plain text with the square.

noncarrying sum. A sum produced in cryptographic (mod 10) arithmetic.

noncommutative, adj. As applied to bipartite matrices, so constructed that row and column coordinates must be read in a certain prescribed order, for example, in row-column order.

noncrashing, adj. A term used to describe that feature of the structure of certain cryptosystems which does not permit a plaintext unit to be represented in the cipher text by the same unit.

normal alphabet. The conventional sequence of letters which form the elements of written language and are used to represent approximately the sounds of the spoken language. The direct standard alphabet beginning with "A" and ending with "Z".

normal frequency. The standard frequency of a textual unit or letter relative to other textual units or letters, as disclosed by the statistical study of a large volume of homogeneous text. Also called characteristic frequency.

normal sequence. The normal alphabetical sequence of those letters which are used in the written text of any particular language, or any cyclic permutation thereof.

normal uniliteral frequency distribution. A distribution showing the standard relative frequency of single plaintext symbols as disclosed by statistical study of a large volume of text.

null, n. In cryptography, a symbol or unit of encrypted text having no plaintext significance.

numerical key. A key composed of a sequence of numbers. Cf. LITERAL KEY.

numerically-keyed columnar transposition. A columnar transposition system in which the columns of a matrix are taken off in the order determined by a numerical key.

off the cut. As applied to the division of cipher text into polygraphs, beginning elsewhere than with the initial character of a bona fide polygraph.

one-part code. A code in which the plaintext elements are arranged in alphabetical, numerical, or other systematic order accompanied by their code groups also arranged in alphabetical, numerical, or other systematic order.

one-time pad. A form of key book used in a one-time system, so designed as to permit the destruction of each page of key as soon as it has been used.

one-time system. A cryptosystem in which the key, normally of a random nature, is used only once.

on the cut. As applied to the division of text into polygraphs, beginning with the first texual character.

padding, n. Extraneous text added to a message for the purpose of concealing its length and beginning or ending or both.

paraphrase, v. t. To change the phraseology of a message without changing its meaning.

partially-digraphic system. A digraphic substitution system in which the encipherment of certain members of the polygraphs show group relationships; small matrix systems, such as the four-square, two-square and Playfair systems involve such group relationships and are therefore partially-digraphic systems.

partition, n. Resolution of an integer into a set of integers (e.g., representation of the integer 6 as 1 and 5, 2 and 4, or 3 and 3.--v. t. In key analysis, to resolve the actual key into the separate key contributions made by the component factors.

patent repetition. A repetition which is externally visible in encrypted text. Cf. LATENT REPETITION.

pentagraph, n. A set of five letters.

pentanome, n. A set of five digits.

periodic, adj. Characterized by cyclic attributes or usage, as of key in a periodic system, q. v.

periodic digraphic system. A system involving a multiplicity of digraphic systems, used cyclically.

periodic polyalphabetic substitution. A method of encipherment involving the cyclic use of two or more alphabets. Also called repeating-key method.

periodic system. A system in which the enciphering process is repetitive in character and which usually results in the production of cyclic phenomena in the cryptographic text.

permutation table. A table designed for the systematic construction of code groups. It may also be used to correct garbles in groups of code text.

phi (ϕ) test. A test applied to a frequency distribution to determine whether it is monoalphabetic or not. See also KAPPA PLAIN CONSTANT and KAPPA RANDOM CONSTANT.

physical security. That component of security which results from all physical measures necessary to safeguard classified equipment and material from access by unauthorized persons.

plain, adj. Of or pertaining to that which is unencrypted. See also PLAINTEXT.

plain code. Unenciphered code.

plain component. The sequence of plaintext symbols in a cipher alphabet.

plain component equivalents. In connection with the method of completing the plain component sequence, the plaintext equivalents for cipher units derived from an arbitrary juxtaposition of the components of a cipher alphabet.

plain language. Plain text, q. v.

plain text. 1. Normal text or language which, with no hidden or secret meaning, conveys knowledge. 2. The intelligible text underlying a cryptogram.

plaintext, adj. Of or pertaining to that which conveys an intelligible meaning in the language in which it is written with no hidden meaning; as the plaintext equivalents. Often shortened to plain.

plaintext autokey system. An aperiodic substitution system in which the key, following the application of a previously arranged initial key, is generated from elements of the plain text of the message.

plaintext interruptor. In certain aperiodic substitution systems, a specific plaintext letter which, by prearrangement, serves to interrupt the keying cycle and thus suppress periodicity.

Playfair system. A type of digraphic substitution using a single matrix normally of 25 cells.

Poisson table. Table of the Poisson distribution. A special type of mathematical table containing probability data applicable to the phenomena of repetitions expected to obtain in samples of random text; used in cryptanalysis to determine whether or not the repetitions observed in a given sample of cryptographic text are causal or random repetitions.

polyalphabeticity, n. A characteristic of encrypted text which indicates that it has been produced by more than one cipher alphabet. It is normally disclosed by frequency distributions which display "smoothness", or lack of pronounced variation in relative frequencies.

polyalphabetic substitution. A type of substitution in which the successive plaintext elements of a message, usually single letters, are enciphered

primary component. The basic component from which other components may be derived or which may be slid against another basic component to produce secondary alphabets.

probable word. A word assumed or known to be present in the underlying plain text of a cryptogram. A crib.

probable-word method. The method of solution involving the trial of plain text assumed to be present in a cryptogram.

proforma message. A message in standardized form, designed to convey intelligence by conventions of arrangement and abbreviation.

progressive alphabet system. A periodic polyalphabetic substitution system in which the successively used cipher alphabets are produced by successively sliding a pair of sequences through all possible juxtapositions.

proportion, v. t. In cryptology, to derive additional values in an indirect symmetry reconstruction matrix by comparing patent four-element proportions with other proportions in which only one of the elements is missing.

pseudo-digraphic system. A digraphic substitution system in which one of the letters in each digraph is enciphered monoalphabetically.

random, adj. 1. In mathematics, pertaining to unsystematic or chance variations from an expected norm. 2. In cryptanalysis, pertaining to any situation in which a statistical analysis will show variations from a calculated expected norm which variations are indistinguishable from those due to chance.

random text. Text which appears to have been produced by chance or accident, having no discernible patterns or limitations.

rapid analytical machinery. Any high-speed cryptanalytic machinery, usually electronic or photoelectric in nature. Abbr. RAM.

raw traffic. Intercepted traffic showing no evidence of processing for communication intelligence purposes beyond sorting by clear address elements, elimination of unwanted messages, and the inclusion of an arbitrary traffic designator.

read, v. t. 1. To decrypt, especially as the result of successful cryptanalytic investigation.--v. i. To yield intelligible plain text when decrypted.

readable, adj. Pertaining to those code and cipher systems in which sufficient plaintext values or keys have been recovered to permit the reading of messages encrypted in these systems.

reciprocal cipher alphabet. A cipher alphabet in which either of the two sequences may serve as plain or cipher since the equivalents exhibit reciprocity.

reciprocity, n. As used in cryptology, interchangeability of plain-cipher relationships (e.g., $A_p = B_c$ and $B_p = A_c$).

reconstruction matrix. A skeleton matrix employed in the solution of cryptosystems involving a substitution matrix. It aids in the correct relative placement of plaintext or ciphertext values as recovered, and thus often affords clues as to the internal arrangement of the original matrix.

related alphabets. Any of the several secondary cipher alphabets which are produced by sliding any given pair of primary components against each other.

relative code. Code text from which an encipherment has been removed in relative terms, but not reduced to plain-code text, so that the groups differ from the actual original plain code by an interval constant for every group, thus the difference between two relative code groups is the same as that between their plain-code equivalents.

relative frequency. In its cryptologic application, the ratio of the actual occurrences of a textual element to the number of possible occurrences within a given text.

repeating key. A key used cyclically, which therefore repeats.

repeating-key system. Periodic polyalphabetic substitution, q. v.

repetitive encipherment. A type of encipherment in which the primary cipher text of a cryptogram is subjected to further encipherment with either the same or a different system. Double transposition is a frequently encountered example of repetitive encipherment.

reversed standard cipher alphabet. A cipher alphabet in which both the plain and cipher components are the normal sequence, the cipher component being reversed in direction from the plain component.

revolving grille. A type of grille in which the apertures are so distributed that when the grille is turned successively through four angles of 90 degrees and set in position on the grid, all the cells on the grid are disclosed only once. Also called rotating grille.

rotating grille. See REVOLVING GRILLE.

rotor, n. A disk designed to rotate within a cipher machine and which controls the action of some other machine component or produces a variation in some textual or keying element.

roughness, n. A pronounced variation in relative frequencies of the elements considered in a frequency distribution. Cf. SMOOTHNESS.

route transposition. A method of transposition in which the ciphertext equivalent of a message is obtained by transcribing, according to any prearranged route, the letters inscribed in the cells of a matrix into which the message was inscribed earlier according to some prearranged route.

running-key system. A polyalphabetic substitution system which employs a nonperiodic key arbitrarily prepared or obtained from a book or any continuous text.

score, n. The sum of the weights of a given set of characters.--v. t. To derive the sum of such weights in cryptomathematics.

scoring method. A method of assigning weights to elements of plain text, cipher text, or key, as a means of establishing thresholds or criteria in cryptomathematics.

secondary alphabet. An enciphering or deciphering alphabet resulting from the juxtaposition of two primary components, at least one of which is mixed. A secondary alphabet, though different in appearance from the primary alphabet, is cryptographically equivalent to the primary alphabet.

sectional matrix. In polyalphabetic substitution systems, an enciphering matrix consisting of two or more sections, such as in the case of separate vowel and consonant encipherment.

separator, n. See WORD SEPARATOR.

sequence, n. An ordered arrangement of symbols (letters, digits, etc.) having continuity. Specifically, the members of a component of a cipher alphabet in order; the symbols in a row, column, or diagonal of a cipher square in order, key letters or key figures in order.

setting, n. The arrangement and alignment of the variable elements of a cryptographic device or machine at any moment during its operation.

sigma (σ), n. A symbol for the standard deviation.

sigmage, n. As used in cryptomathematics, a measure of the deviation from the normal, expressed in terms of numbers of sigmas (σ).

simple substitution. Monoalphabetic uniliteral substitution.

simple transposition. See SINGLE TRANSPOSITION.

single transposition. A transposition in which only one inscription and one transcription are effected.

sliding alphabet. A pair of components which may be slid to any point of juxtaposition.

sliding strip. A strip of cardboard or similar material which bears a sequence and which can be slid against other such strips to various juxtapositions.

smoothness, n. The lack of pronounced variation in relative frequencies of the elements considered in a frequency distribution. Cf. ROUGHNESS.

solution, n. In its cryptanalytic application, the process or result of solving a cryptogram or cryptosystem by cryptanalysis.

solve, v. t. To cryptanalyze. To find the plain text of encrypted communications by cryptanalytic processes, or to recover by analysis the keys and the principles of their application.

space impulse. One of the two types of impulses used in teleprinter transmission; normally, that impulse during which no current flows through the teleprinter receiving magnet. The other type of impulse is the mark impulse, q. v.

special solution. A solution which depends on circumstances which are not caused by the inherent principles of the particular cryptosystem. For example, solution of a periodic system by exploiting a pair of isologs which have been produced by identical sliding components but which use two different repeating keys; solution of a double transposition system by simultaneously anagramming the corresponding elements of several cryptograms which are of identical length and which all use the same specific key; etc.

specific key. An element which is used with a specific cryptosystem to determine the encipherment of a message and which includes both the message keying element and the daily keying element. It may consist of a letter, number, word, phrase, sentence, a special document, book, or table, etc., usually of a variable nature and easily changeable at the will of the correspondents, or prearranged for them or for their agents by higher authority.

square, n. See MATRIX.

square table. A cipher square (e.g., a Vigenere table).

stagger, n. The situation characterizing a pair of isologs enciphered by identical keys, where the two plain texts are identical except for the addition or deletion of a letter or letters.

standard cipher alphabet. A cipher alphabet in which the sequence of letters in the plain component is the normal, and in the cipher component is the same as the normal, but either reversed in direction or shifted from its point of coincidence with the plain component.

standard uniliteral frequency distribution. See NORMAL UNILITERAL FREQUENCY DISTRIBUTION.

stencil, n. See GRILLE.

stereotype, n. A word, number, phrase, abbreviation, etc., which as a result of language habits, has a high probability of occurrence, especially at the beginning or ending of a message.

stereotyped messages. Related encrypted messages which are recognizable as such because of distinctive characteristics of the underlying plain text.

strip-cipher device. A cipher device employing sliding alphabet strips.

strip-cipher system. A polyalphabetic substitution system employing sliding strips in conjunction with the variable-generatrix principle as in the Jefferson cipher.

stutter group. A group consisting of a repeated single character, as 55555 or EEEEE, usually a four or five character group.

substitution alphabet. See CIPHER ALPHABET.

substitution cipher. 1. A cipher system in which the elements of the plain text are replaced by other elements. 2. A cryptogram produced by enciphering a plaintext message with a substitution system.

substitution system. A system in which the elements of the plain or code text are replaced by other elements.

subtractive method. The method of encipherment wherein the cryptographic equations are P - K = C, and C + K = P. Cf. ADDITIVE METHOD and MINUEND METHOD.

subtractive system. A system in which encipherment is accomplished by subtracting the key from the plain text; in the process of decipherment, the enciphered text is added to the key. Cf. MINUEND SYSTEM.

sum check. A digit of a textual group which is the sum (mod 10) of the other digits in the group.--v. i. To exhibit the property of a sum check.

sum-checking digit. A preselected digit (normally the final digit) in a code or cipher group which is the noncarrying sum of the other digits in the group.

superencipherment, n. A form of superencryption in which the final step involves encipherment.

superencryption, n. A further encryption of the text of a cryptogram for increased security. Enciphered code is a frequently encountered example of superencryption.

syllabary, n. In a code book, a list of individual letters, combination of letters, or syllables, accompanied by their equivalent code groups, usually provided for spelled-out words or proper names not present in the vocabulary of a code; a spelling table.

syllabary square. A cipher matrix containing individual letters, digits, syllables, frequent digraphs, trigraphs, etc., which are encrypted by the row and column coordinates of the matrix.

syllabic, adj. Of, pertaining to, or denoting syllables.

system, n. See CRYPTOSYSTEM.

system indicator. See DISCRIMINANT.

tail, v. i. Of two messages, to exhibit tailing, q. v.

tailing, n. 1. The practice of beginning the encipherment of one message with the element of key immediately following the element of key used to encipher the last textual groups of the preceding message. 2. The practice of beginning the encipherment of one message with machine components aligned as they were after processing of the last textual group of the preceding message.

telecommunications, n. Any transmission, emission, or reception of signs, signals, writing, images and sounds, or intelligence of any nature by wire, radio, visual, electronic, or other means.

teleprinter, n. An electrically-operated instrument used in the transmission and reception-printing of messages by proper sensing and interpretation of electrical signals. Also called teletypewriter, radioprinter. A specific variety of teleprinter is the Teletype, a trademarked machine manufactured by the Teletype Corporation.

tetragraph, n. A set of four letters.

tetranome, n. A set of four digits.

text, n. The part of a message containing the basic information which the originator desires to be communicated.

traffic, n. All transmitted and received communications. Abbr. tfc.

traffic analysis. The branch of cryptology which deals with the study of the external characteristics of signal communications and related materials for the purpose of obtaining information concerning the organization and operation of a communication system. Abbr. T/A.

traffic intercept. A copy of a communication obtained through interception.

transcription, n. 1. In a transposition system, the process of removing the text from a matrix or grid by a method or route different from that used in the inscription. 2. A written copy of a previously recorded radio transmission; also the process of preparing such copy from tapes or records.

transmission security. That component of communication security which results from all measures designed to protect transmissions from interception, traffic analysis, and imitative deception.

transposition cipher. 1. A transposition system. 2. A cryptogram produced by enciphering a message with a transposition system.

transposition system. A cryptosystem in which the elements of plain text, whether individual letters, groups of letters, syllables, words, phrases, sentences or code groups or their components undergo some change in their relative positions without a change in their identities.

trigraph, n. A set of three letters.

trigraphic, adj. Of or pertaining to any three-character group.

trigraphic frequency distribution. A frequency distribution of successive trigraphs. A trigraphic frequency distribution of ABCDEF would consider only the trigraphs ABC and DEF. Cf. TRILITERAL FREQUENCY DISTRIBUTION.

triliteral, adj. Of or pertaining only to cryptosystems, cipher alphabets, and frequency distributions which involve cipher units of three letters or characters. See the more inclusive term TRIGRAPHIC; see also TRILITERAL FREQUENCY DISTRIBUTION.

triliteral frequency distribution. A distribution of the characters in the text of a message in sets of three, which will show: (a) each character with its two preceding characters or (b) each character with its two succeeding characters, or in its most usual form, (c) each character with one preceding and one succeeding character. A triliteral frequency distribution of ABCDEF would consider the groups ABC, BCD, CDE, DEF.

trinome, n. A set of three digits.

trinome-digraphic system. A substitution system in which plaintext digraphs are represented by 3-digit cipher elements.

tripartite alphabet. A multiliteral alphabet in which the cipher units may be divided into three separate parts whose functions are clearly defined, viz., page, row, and column indicators of a dictionary system.

triplet, n. A group of three like symbols.

two-category weights. Weights of ϕ and 1 assigned to units of text or key used to evaluate the results of certain cryptanalytic operations.

two-element differential. The characteristic incorporated in certain codes in which the groups differ from one another by a minimum of two elements, either in identity or the position occupied. When the elements are letters, the characteristic is called a two-letter differential; when the elements are digits, it is called a two-digit differential.

two-part code. A randomized code, consisting of an encoding section in which the plaintext groups are arranged in an alphabetical or other systematic order accompanied by their code groups arranged in a non-alphabetical or random order; and a decoding section, in which the code groups are arranged in alphabetical or numerical order and are accompanied by their meanings as given in the encoding section.

uniliteral, adj. Of, or pertaining only to cryptosystems, cipher alphabets and frequency distributions which involve cipher units of single letters or characters. See the more inclusive term MONOGRAPHIC; see also UNILITERAL FREQUENCY DISTRIBUTION.

uniliteral frequency distribution. A simple tabulation showing the frequency of individual characters of a text.

uniliteral substitution. A cryptographic process in which the individual letters of a message text are replaced by single-letter cipher equivalents.

uniselector switch. A multipole-multilevel switch such as that used in automatic dialing telephone systems.

variant, n. 1. One of two or more cipher or code symbols which have the same plain equivalent; also called variant value. 2. One of several plaintext meanings which may be represented by a single code group.

variant system. A substitution system in which some or all plaintext letters may be represented by more than one cipher equivalent.

variant value. See VARIANT.

Vernam system. A cipher teleprinter system employing a prepared tape of random teleprinter characters used to key another tape containing the plain text to be encrypted.

Vigenère square. The cipher square commonly attributed in cryptographic literature to the French cryptographer Blaise de Vigenère (1523-1596), having the normal sequence at the top (or bottom) and at the left (or right), with cyclic permutations of the normal sequence forming the successive rows (or columns) within the square.

Vigenère system. A cryptosystem employing a Vigenère square, q. v.

weight, n. A value assigned to units of text or key, used to evaluate the results of certain cryptanalytic operations.

Wheatstone cipher device. A cipher device consisting essentially of two rings mounted concentrically in a single plane, the outer (and larger) ring being the plain component of the device and comprising 27 equisized divisions, the inner (and smaller) ring being the cipher component, comprising 26 smaller divisions. The device incorporates two hands (similar to those on a clock) pivoted at the center of the device--the larger hand serving the outer ring and the smaller hand the inner--so geared together that for each complete revolution of the larger, the smaller turns through one complete revolution plus one twenty-sixth.

word pattern. The characteristic arrangement of repeated letters in a word which tends to make it readily identifiable when enciphered monoalphabetically. See IDIOMORPHISM.

word separator. A unit of one or more characters employed in certain cryptosystems to indicate the space between words. It may be enciphered or unenciphered. Also called a word spacer.

word transposition. A cryptosystem in which whole words are transposed according to a certain prearranged route or pattern.

xi (ξ) I.C. See CROSS I.C.

ZENDIAN Problem. A large-scale problem in cryptanalysis and traffic analysis performed on a volume of traffic intercepted during an amphibious operation against the hypothetical country of Zendia.

(BLANK)

APPENDIX 2

SUMMARY OF BASIC FORMULAS AND USEFUL TABLES

(BLANK)

SUMMARY OF BASIC FORMULAS AND USEFUL TABLES

A. Formulas

1. $\phi_o = \Sigma f_i(f_i-1)$, where f_i = frequency of each element in distribution.

2. $\phi_r = \frac{N(N-1)}{c}$, where N = total number of tallies in distribution and c = number of categories in alphabet.

3. $\phi_p = \kappa_p N(N-1)$, where κ_p = repeat rate for the particular language; for English, the monographic $\kappa_p = .0667$.

4. δ I.C. $= \frac{\phi_o}{\phi_r} = \frac{c\Sigma f(f-1)}{N(N-1)}$

5. $\chi_o = \Sigma f_i f_i'$, where f_i and f_i' are frequencies of corresponding elements in two distributions being matched.

6. $\chi_r = \frac{N_1 N_2}{c}$, where N_1 and N_2 are the total number of tallies in two distributions being matched.

7. $\chi_m = \kappa_p N_1 N_2$

8. ξ I.C. $= \frac{\chi_o}{\chi_r} = \frac{c\Sigma f_i f_i'}{N_1 N_2}$

9. $\sigma = \frac{\sqrt{2(c-1)}}{\sqrt{N(N-1)}}$ = standard deviation of δ I.C. of samples drawn from a flat population.

10. $S = \frac{\text{observed I.C.} - 1.00}{\sigma}$ = sigmage of δ I.C. of samples drawn from a flat population.

B. Handy slide rule settings[1]

1. ϕ_r for 26-letter text:

   To N on D set 26 on C; under (N-1) on C read ϕ_r on D.

2. ϕ_p for English plain text:

   To N on D set (N-1) on CI; under .0667 on C read ϕ_p on D.[2]

3. δ I.C. for 26-letter text:

   To 26 on A set (N - 0.5) on C; over ϕ_o on B read δ I.C. on A.[3]

4. χ_r for 26-letter text:

   Use settings in (1), above, substituting N_2 for (N-1).

5. χ_m for English plain text:

   Use settings in (2), above, substituting N_2 for (N-1).

6. ξ I.C. for 26-letter distributions:

   To 26 on D set N_1 on C; move hairline to χ_o on C; slide N_2 on C to hairline, under index of C read ξ I.C. on D.

7. σ, for flat population (26-letter text):

   To 7.07 on D set (N - 0.5) on C; under index of C read σ on D.

8. σ, for flat population (digital text):

   To 4.24 on D set (N - 0.5) on C; under index of C read σ on D.

---

[1] The expressions below, except for No. 6, are solvable with one setting of the slide.

[2] For languages other than English, substitute the appropriate κ_p instead of the .0667 given.

[3] In this formula, $(N - 0.5)^2$ is used as a convenient approximation to N(N-1); the error is negligible for slide rule computation, since $(N - 0.5)^2 = N(N-1) + 0.25$.

C. Expected number of repetitions

No. 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	0.298	0.011						
200	21.8	2.12	0.154	0.009					
300	42.5	6.23	0.683	0.060	0.004				
400	65.3	12.8	1.87	0.220	0.022	0.002			
500	88.1	21.6	3.97	0.582	0.071	0.008			
600	110	32.3	7.11	1.25	0.184	0.023	0.003		
700	129	44.3	11.4	2.35	0.403	0.059	0.008	0.001	
800	145	57.1	16.8	3.96	0.777	0.130	0.019	0.003	
900	158	70.1	23.2	6.16	1.36	0.257	0.043	0.006	0.001
1000	169	83.0	30.6	9.03	2.21	0.466	0.085	0.014	0.002

No. of letters	Expected number of trigraphs		
	E(2)	E(3)	E(4)
100	0.269	0.001	
200	1.10	0.004	
300	2.48	0.014	
400	4.40	0.033	
500	6.85	0.064	
600	9.81	0.111	0.001
700	13.3	0.175	0.002
800	17.3	0.261	0.003
900	21.8	0.371	0.005
1000	26.8	0.505	0.008

No. of letters	Tetragraphs	
	E(2)	E(3)
100	0.010	
200	0.043	
300	0.096	
400	0.171	
500	0.270	
600	0.389	
700	0.530	
800	0.693	
900	0.877	
1000	1.08	0.001

No. of letters	Pentagraphs
	E(2)
100	
200	0.002
300	0.004
400	0.007
500	0.011
600	0.015
700	0.021
800	0.027
900	0.034
1000	0.042

D. Expected values of ϕ_r and ϕ_p

N	ϕ_r	ϕ_p	N	ϕ_r	ϕ_p	N	ϕ_r	ϕ_p	N	ϕ_r	ϕ_p	N	ϕ_r	ϕ_p
11	4.23	7.34	29	31	54	47	83	144	65	160	277	83	262	454
12	5.08	8.80	30	33	58	48	87	150	66	165	286	84	268	465
13	6.00	10.4	31	36	62	49	90	157	67	170	295	85	275	476
14	7.00	12.1	32	38	66	50	94	163	68	175	304	86	281	488
15	8.08	14.0	33	41	70	51	98	170	69	180	313	87	288	499
16	9.23	16.0	34	43	75	52	102	177	70	186	322	88	294	511
17	10.5	18.1	35	46	79	53	106	184	71	191	331	89	301	522
18	11.8	20.4	36	48	84	54	110	191	72	197	341	90	308	534
19	13.2	22.8	37	51	89	55	114	198	73	202	351	91	315	546
20	14.6	25.3	38	54	94	56	118	205	74	208	360	92	322	558
21	16.2	28.0	39	57	99	57	123	213	75	213	370	93	329	571
22	17.8	30.8	40	60	104	58	127	221	76	219	380	94	336	583
23	19.5	33.8	41	63	109	59	132	228	77	225	390	95	343	596
24	21.2	36.8	42	66	115	60	136	236	78	231	401	96	351	608
25	23.1	40.0	43	69	120	61	141	244	79	237	411	97	358	621
26	25.0	43.4	44	73	126	62	145	252	80	243	422	98	366	634
27	27.0	46.8	45	76	132	63	150	261	81	249	432	99	373	647
28	29.1	50.4	46	80	138	64	155	269	82	255	443	100	381	660

E. Standard deviation of δ I.C. (for 10 and 26 categories)

N	c_{10}	c_{26}	N	c_{10}	c_{26}	N	c_{10}	c_{26}	N	c_{10}	c_{26}	N	c_{10}	c_{26}
11	.41	.67	29	.15	.25	47	.09	.15	65	.07	.11	83	.05	.09
12	.37	.62	30	.14	.24	48	.09	.15	66	.06	.11	84	.05	.08
13	.34	.57	31	.14	.23	49	.09	.15	67	.06	.11	85	.05	.08
14	.31	.52	32	.13	.22	50	.09	.14	68	.06	.10	86	.05	.08
15	.29	.49	33	.13	.22	51	.08	.14	69	.06	.10	87	.05	.08
16	.27	.46	34	.13	.21	52	.08	.14	70	.06	.10	88	.05	.08
17	.26	.43	35	.12	.20	53	.08	.13	71	.06	.10	89	.05	.08
18	.24	.40	36	.12	.20	54	.08	.13	72	.06	.10	90	.05	.08
19	.23	.38	37	.12	.19	55	.08	.13	73	.06	.10	91	.05	.08
20	.22	.36	38	.11	.19	56	.08	.13	74	.06	.10	92	.05	.08
21	.21	.35	39	.11	.18	57	.08	.13	75	.06	.09	93	.05	.08
22	.20	.33	40	.11	.18	58	.07	.12	76	.06	.09	94	.05	.08
23	.19	.31	41	.10	.17	59	.07	.12	77	.06	.09	95	.04	.07
24	.18	.30	42	.10	.17	60	.07	.12	78	.05	.09	96	.04	.07
25	.17	.29	43	.10	.17	61	.07	.12	79	.05	.09	97	.04	.07
26	.17	.28	44	.10	.16	62	.07	.11	80	.05	.09	98	.04	.07
27	.16	.27	45	.10	.16	63	.07	.11	81	.05	.09	99	.04	.07
28	.15	.26	46	.09	.16	64	.07	.11	82	.05	.09	100	.04	.07

F. Interpretation of sigmage of δ I.C.

Sigmage (S), calculated by $\frac{\delta \text{I.C.} - 1.00}{\sigma}$	Values of x		
	Chi-square distribution		Normal distribution
	10 categories	26 categories	
1	6.6	6.4	6.3
1½	12	13	15
2	24	28	44
2½	49	64	161
3	100	160	740
3½	220	430	4,310
4	480	1,200	31,500

The sigmage in the first column will be equaled or exceeded by pure chance, on the average, once every x times as shown in the table. Since the distribution of the δ I.C. is closely approximated by the χ^2 distribution (up to about 4σ), this latter is a good measure for evaluating the sigmage of the δ I.C. For example, a distribution of 60 random letters has (from table E, above) a standard deviation of .12; now if a 60-letter sample under study has an observed δ I.C. of 1.36, the sigmage $S = \frac{1.36 - 1.00}{.12} = 3$, which is then found in the table above as representing one chance in 160 of equaling or exceeding this deviation if the sample were drawn from a random population. The Normal distribution appended here for comparison purposes has often been used, incorrectly so, for evaluating the sigmage of the δ I.C.; after a sigmage of 1 1/2, the Normal distribution is a very poor approximation of the distribution of the δ I.C.

G. Factor table
(numbers 1-400)

1	
2	
3	
4	2
5	
6	2 3
7	
8	2 4
9	3
10	2 5
11	
12	2 3 4 6
13	
14	2 7
15	3 5
16	2 4 8
17	
18	2 3 6 9
19	
20	2 4 5 10
21	3 7
22	2 11
23	
24	2 3 4 6 8 12
25	5
26	2 13
27	3 9
28	2 4 7 14
29	
30	2 3 5 6 10 15
31	
32	2 4 8 16
33	3 11
34	2 17
35	5 7
36	2 3 4 6 9 12 18
37	
38	2 19
39	3 13
40	2 4 5 8 10 20
41	
42	2 3 6 7 14 21
43	
44	2 4 11 22
45	3 5 9 15
46	2 23
47	
48	2 3 4 6 8 12 16 24
49	7
50	2 5 10 25
51	3 17
52	2 4 13 26
53	
54	2 3 6 9 18 27
55	5 11
56	2 4 7 8 14 28
57	3 19
58	2 29
59	
60	2 3 4 5 6 10 12 15 20 30
61	
62	2 31
63	3 7 9 21
64	2 4 8 16 32
65	5 13
66	2 3 6 11 33
67	
68	2 4 17 34
69	3 23
70	2 5 7 10 14 35
71	
72	2 3 4 6 8 9 12 18 24 36
73	
74	2 37
75	3 5 15 25
76	2 4 19 38
77	7 11
78	2 3 6 13 26 39
79	
80	2 4 5 8 10 16 20 40
81	3 9 27
82	2 41
83	
84	2 3 4 6 7 12 14 21 28 42
85	5 17
86	2 43
87	3 29
88	2 4 8 11 22 44
89	
90	2 3 5 6 9 10 15 18 30 45
91	7 13
92	2 4 23 46
93	3 31
94	2 47
95	5 19
96	2 3 4 6 8 12 16 24 32 48
97	
98	2 7 14 49
99	3 9 11 33
100	2 4 5 10 20 25 50

101	
102	2 3 6 17 34 51
103	
104	2 4 8 13 26 52
105	3 5 7 15 21 35
106	2 53
107	
108	2 3 4 6 9 12 18 27 36 54
109	
110	2 5 10 11 22 55
111	3 37
112	2 4 7 8 14 16 28 56
113	
114	2 3 6 19 38 57
115	5 23
116	2 4 29 58
117	3 9 13 39
118	2 59
119	7 17
120	2 3 4 5 6 8 10 12 15 20 24 30 40 60
121	11
122	2 61
123	3 41
124	2 4 31 62
125	5 25
126	2 3 6 7 9 14 18 21 42 63
127	
128	2 4 8 16 32 64
129	3 43
130	2 5 10 13 26 65
131	
132	2 3 4 6 11 12 22 33 44 66
133	7 19
134	2 67
135	3 5 9 15 27 45
136	2 4 8 17 34 68
137	
138	2 3 6 23 46 69
139	
140	2 4 5 7 10 14 20 28 35 70
141	3 47
142	2 71
143	11 13
144	2 3 4 6 8 9 12 16 18 24 36 48 72
145	5 29
146	2 73
147	3 7 21 49
148	2 4 37 74
149	
150	2 3 5 6 10 15 25 30 50 75
151	
152	2 4 8 19 38 76
153	3 9 17 51
154	2 7 11 14 22 77
155	5 31
156	2 3 4 6 12 13 26 39 52 78
157	
158	2 79
159	3 53
160	2 4 5 8 10 16 20 32 40 80
161	7 23
162	2 3 6 9 18 27 54 81
163	
164	2 4 41 82
165	3 5 11 15 33 55
166	2 83
167	
168	2 3 4 6 7 8 12 14 21 24 28 42 56 84
169	13
170	2 5 10 17 34 85
171	3 9 19 57
172	2 4 43 86
173	
174	2 3 6 29 58 87
175	5 7 25 35
176	2 4 8 11 16 22 44 88
177	3 59
178	2 89
179	
180	2 3 4 5 6 9 10 12 15 18 20 30 36 45 60 90
181	
182	2 7 13 14 26 91
183	3 61
184	2 4 8 23 46 92
185	5 37
186	2 3 6 31 62 93
187	11 17
188	2 4 47 94
189	3 7 9 21 27 63
190	2 5 10 19 38 95
191	
192	2 3 4 6 8 12 16 24 32 48 64 96
193	
194	2 97
195	3 5 13 15 39 65
196	2 4 7 14 28 49 98
197	
198	2 3 6 9 11 18 22 33 66 99
199	
200	2 4 5 8 10 20 25 40 50 100

201	3 67
202	2 101
203	7 29
204	2 3 4 6 12 17 34 51 68 102
205	5 41
206	2 103
207	3 9 23 69
208	2 4 8 13 16 26 52 104
209	11 19
210	2 3 5 6 7 10 14 15 21 30 35 42 70 105
211	
212	2 4 53 106
213	3 71
214	2 107
215	5 43
216	2 3 4 6 8 9 12 18 24 27 36 54 72 108
217	7 31
218	2 109
219	3 73
220	2 4 5 10 11 20 22 44 55 110
221	13 17
222	2 3 6 37 74 111
223	
224	2 4 7 8 14 16 28 32 56 112
225	3 5 9 15 25 45 75
226	2 113
227	
228	2 3 4 6 12 19 38 57 76 114
229	
230	2 5 10 23 46 115
231	3 7 11 21 33 77
232	2 4 8 29 58 116
233	
234	2 3 6 9 13 18 26 39 78 117
235	5 47
236	2 4 59 118
237	3 79
238	2 7 14 17 34 119
239	
240	2 3 4 5 6 8 10 12 15 16 20 24 30 40 48 60 80 120
241	
242	2 11 22 121
243	3 9 27 81
244	2 4 61 122
245	5 7 35 49
246	2 3 6 41 82 123
247	13 19
248	2 4 8 31 62 124
249	3 83
250	2 5 10 25 50 125
251	
252	2 3 4 6 7 9 12 14 18 21 28 36 42 63 84 126
253	11 23
254	2 127
255	3 5 15 17 51 85
256	2 4 8 16 32 64 128
257	
258	2 3 6 43 86 129
259	7 37
260	2 4 5 10 13 20 26 52 65 130
261	3 9 29 87
262	2 131
263	
264	2 3 4 6 8 11 12 22 24 33 44 66 88 132
265	5 53
266	2 7 14 19 38 133
267	3 89
268	2 4 67 134
269	
270	2 3 5 6 9 10 15 18 27 30 45 54 90 135
271	
272	2 4 8 16 17 34 68 136
273	3 7 13 21 39 91
274	2 137
275	5 11 25 55
276	2 3 4 6 12 23 46 69 92 138
277	
278	2 139
279	3 9 31 93
280	2 4 5 7 8 10 14 20 28 35 40 56 70 140
281	
282	2 3 47 94 141
283	
284	2 4 71 142
285	3 5 15 19 57 95
286	2 11 13 22 26 143
287	7 41
288	2 3 4 6 8 9 12 16 18 24 32 36 48 72 96 144
289	17
290	2 5 10 29 58 145
291	3 97
292	2 4 73 146
293	
294	2 3 6 7 14 21 42 49 98 147
295	5 59
296	2 4 8 37 74 148
297	3 9 11 27 33 99
298	2 149
299	13 23
300	2 3 4 5 6 10 12 15 20 25 30 50 60 75 100 150

301 | 7 43
302 | 2 151
303 | 3 101
304 | 2 4 8 16 19 38 76 152
305 | 5 61
306 | 2 3 6 9 17 18 34 51 102 153
307 |
308 | 2 4 7 11 14 22 28 44 77 154
309 | 3 103
310 | 2 5 10 31 62 155
311 |
312 | 2 3 4 6 8 12 13 24 26 39 52 78 104
313 |
314 | 2 157
315 | 3 5 7 9 15 21 35 45 63 105
316 | 2 4 79 158
317 |
318 | 2 3 6 53 106 159
319 | 11 29
320 | 2 4 5 8 10 16 20 32 40 64 80 160
321 | 3 107
322 | 2 7 14 23 46 161
323 | 17 19
324 | 2 3 4 6 9 12 18 27 36 54 81 108 162
325 | 5 13 25 65
326 | 2 163
327 | 3 109
328 | 2 4 8 41 82 164
329 | 7 47
330 | 2 3 5 6 10 11 13 22 30 33 55 66 110 165
331 |
332 | 2 4 83 166
333 | 3 9 37 111
334 | 2 167
335 | 5 67
336 | 2 3 4 6 7 8 12 14 16 21 24 28 42 48 56 84 112 168
337 |
338 | 2 13 26 169
339 | 3 113
340 | 2 4 5 10 17 20 34 68 84 170
341 | 11 31
342 | 2 3 6 9 18 19 38 57 114 171
343 | 7 49
344 | 2 4 8 43 86 172
345 | 3 5 15 23 69 115
346 | 2 173
347 |
348 | 2 3 4 6 12 29 58 87 116 174
349 |
350 | 2 5 7 10 14 25 35 50 70 175
351 | 3 9 13 27 39 117
352 | 2 4 8 11 16 22 32 44 88 176
353 |
354 | 2 3 6 59 118 177
355 | 5 71
356 | 2 4 89 178
357 | 3 7 17 21 51 119
358 | 2 179
359 |
360 | 2 3 4 5 6 8 9 10 12 15 18 20 24 30 36 40 45 60 72 90 120 180
361 | 19
362 | 2 181
363 | 3 11 33 121
364 | 2 4 7 13 14 26 28 52 91 182
365 | 5 73
366 | 2 3 6 61 122 183
367 |
368 | 2 4 8 16 23 46 92 184
369 | 3 9 41 123
370 | 2 5 10 37 74 185
371 | 7 53
372 | 2 3 4 6 12 31 62 93 124 186
373 |
374 | 2 11 17 22 34 187
375 | 3 5 15 25 75 125
376 | 2 4 8 47 94 188
377 | 13 29
378 | 2 3 6 7 9 14 18 21 27 42 54 63 126
379 |
380 | 2 4 5 10 19 20 38 76 95 190
381 | 3 127
382 | 2 191
383 |
384 | 2 3 4 6 8 12 16 24 32 48 64 96 128
385 | 5 7 11 35 55 77
386 | 2 193
387 | 3 9 43 129
388 | 2 4 97 194
389 |
390 | 2 3 5 6 10 13 15 26 30 39 65 78 130 195
391 | 17 23
392 | 2 4 7 8 14 28 49 56 98 196
393 | 3 131
394 | 2 197
395 | 5 79
396 | 2 3 4 6 9 11 12 18 22 33 36 44 66 99 132 198
397 |
398 | 2 199
399 | 3 7 19 21 57 133
400 | 2 4 5 8 10 16 20 25 40 50 80 100 200

H. Table of primes up to 2000

1	139	337	557	769	1013	1249	1493	1741
2	149	347	563	773	1019	1259	1499	1747
3	151	349	569	787	1021	1277	1511	1753
5	157	353	571	797	1031	1279	1523	1759
7	163	359	577	809	1033	1283	1531	1777
11	167	367	587	811	1039	1289	1543	1783
13	173	373	593	821	1049	1291	1549	1787
17	179	379	599	823	1051	1297	1553	1789
19	181	383	601	827	1061	1301	1559	1801
23	191	389	607	829	1063	1303	1567	1811
29	193	397	613	839	1069	1307	1571	1823
31	197	401	617	853	1087	1319	1579	1831
37	199	409	619	857	1091	1321	1583	1847
41	211	419	631	859	1093	1327	1597	1861
43	223	421	641	863	1097	1361	1601	1867
47	227	431	643	877	1103	1367	1607	1871
53	229	433	647	881	1109	1373	1609	1873
59	233	439	653	883	1117	1381	1613	1877
61	239	443	659	887	1123	1399	1619	1879
67	241	449	661	907	1129	1409	1621	1889
71	251	457	673	911	1151	1423	1627	1901
73	257	461	677	919	1153	1427	1637	1907
79	263	463	683	929	1163	1429	1657	1913
83	269	467	691	937	1171	1433	1663	1931
89	271	479	701	941	1181	1439	1667	1933
97	277	487	709	947	1187	1447	1669	1949
101	281	491	719	953	1193	1451	1693	1951
103	283	499	727	967	1201	1453	1697	1973
107	293	503	733	971	1213	1459	1699	1979
109	307	509	739	977	1217	1471	1709	1987
113	311	521	743	983	1223	1481	1721	1993
127	313	523	751	991	1229	1483	1723	1997
131	317	541	757	997	1231	1487	1733	1999
137	331	547	761	1009	1237	1489		

I. Four-place

N	0	1	2	3	4	5	6	7	8	9	Proportional Parts 1	2	3	4	5	6	7	8	9
10	0000	0043	0086	0128	0170	0212	0253	0294	0334	0374	4	8	12	17	21	25	29	33	37
11	0414	0453	0492	0531	0569	0607	0645	0682	0719	0755	4	8	11	15	19	23	26	30	34
12	0792	0828	0864	0899	0934	0969	1004	1038	1072	1106	3	7	10	14	17	21	24	28	31
13	1139	1173	1206	1239	1271	1303	1335	1367	1399	1430	3	6	10	13	16	19	23	26	29
14	1461	1492	1523	1553	1584	1614	1644	1673	1703	1732	3	6	9	12	15	18	21	24	27
15	1761	1790	1818	1847	1875	1903	1931	1959	1987	2014	3	6	8	11	14	17	20	22	25
16	2041	2068	2095	2122	2148	2175	2201	2227	2253	2279	3	5	8	11	13	16	18	21	24
17	2304	2330	2355	2380	2405	2430	2455	2480	2504	2529	2	5	7	10	12	15	17	20	22
18	2553	2577	2601	2625	2648	2672	2695	2718	2742	2765	2	5	7	9	12	14	16	19	21
19	2788	2810	2833	2856	2878	2900	2923	2945	2967	2989	2	4	7	9	11	13	16	18	20
20	3010	3032	3054	3075	3096	3118	3139	3160	3181	3201	2	4	6	8	11	13	15	17	19
21	3222	3243	3263	3284	3304	3324	3345	3365	3385	3404	2	4	6	8	10	12	14	16	18
22	3424	3444	3464	3483	3502	3522	3541	3560	3579	3598	2	4	6	8	10	12	14	15	17
23	3617	3636	3655	3674	3692	3711	3729	3747	3766	3784	2	4	6	7	9	11	13	15	17
24	3802	3820	3838	3856	3874	3892	3909	3927	3945	3962	2	4	5	7	9	11	12	14	16
25	3979	3997	4014	4031	4048	4065	4082	4099	4116	4133	2	3	5	7	9	10	12	14	15
26	4150	4166	4183	4200	4216	4232	4249	4265	4281	4298	2	3	5	7	8	10	11	13	15
27	4314	4330	4346	4362	4378	4393	4409	4425	4440	4456	2	3	5	6	8	9	11	13	14
28	4472	4487	4502	4518	4533	4548	4564	4579	4594	4609	2	3	5	6	8	9	11	12	14
29	4624	4639	4654	4669	4683	4698	4713	4728	4742	4757	1	3	4	6	7	9	10	12	13
30	4771	4786	4800	4814	4829	4843	4857	4871	4886	4900	1	3	4	6	7	9	10	11	13
31	4914	4928	4942	4955	4969	4983	4997	5011	5024	5038	1	3	4	6	7	8	10	11	12
32	5051	5065	5079	5092	5105	5119	5132	5145	5159	5172	1	3	4	5	7	8	9	11	12
33	5185	5198	5211	5224	5237	5250	5263	5276	5289	5302	1	3	4	5	6	8	9	10	12
34	5315	5328	5340	5353	5366	5378	5391	5403	5416	5428	1	3	4	5	6	8	9	10	11
35	5441	5453	5465	5478	5490	5502	5514	5527	5539	5551	1	2	4	5	6	7	9	10	11
36	5563	5575	5587	5599	5611	5623	5635	5647	5658	5670	1	2	4	5	6	7	8	10	11
37	5682	5694	5705	5717	5729	5740	5752	5763	5775	5786	1	2	3	5	6	7	8	9	10
38	5798	5809	5821	5832	5843	5855	5866	5877	5888	5899	1	2	3	5	6	7	8	9	10
39	5911	5922	5933	5944	5955	5966	5977	5988	5999	6010	1	2	3	4	5	7	8	9	10
40	6021	6031	6042	6053	6064	6075	6085	6096	6107	6117	1	2	3	4	5	6	8	9	10
41	6128	6138	6149	6160	6170	6180	6191	6201	6212	6222	1	2	3	4	5	6	7	8	9
42	6232	6243	6253	6263	6274	6284	6294	6304	6314	6325	1	2	3	4	5	6	7	8	9
43	6335	6345	6355	6365	6375	6385	6395	6405	6415	6425	1	2	3	4	5	6	7	8	9
44	6435	6444	6454	6464	6474	6484	6493	6503	6513	6522	1	2	3	4	5	6	7	8	9
45	6532	6542	6551	6561	6571	6580	6590	6599	6609	6618	1	2	3	4	5	6	7	8	9
46	6628	6637	6646	6656	6665	6675	6684	6693	6702	6712	1	2	3	4	5	6	7	7	8
47	6721	6730	6739	6749	6758	6767	6776	6785	6794	6803	1	2	3	4	5	5	6	7	8
48	6812	6821	6830	6839	6848	6857	6866	6875	6884	6893	1	2	3	4	4	5	6	7	8
49	6902	6911	6920	6928	6937	6946	6955	6964	6972	6981	1	2	3	4	4	5	6	7	8
50	6990	6998	7007	7016	7024	7033	7042	7050	7059	7067	1	2	3	3	4	5	6	7	8
51	7076	7084	7093	7101	7110	7118	7126	7135	7143	7152	1	2	3	3	4	5	6	7	8
52	7160	7168	7177	7185	7193	7202	7210	7218	7226	7235	1	2	2	3	4	5	6	7	7
53	7243	7251	7259	7267	7275	7284	7292	7300	7308	7316	1	2	2	3	4	5	6	6	7
54	7324	7332	7340	7348	7356	7364	7372	7380	7388	7396	1	2	2	3	4	5	6	6	7

logarithms

N	0	1	2	3	4	5	6	7	8	9	Proportional Parts 1	2	3	4	5	6	7	8	9
55	7404	7412	7419	7427	7435	7443	7451	7459	7466	7474	1	2	2	3	4	5	5	6	7
56	7482	7490	7497	7505	7513	7520	7528	7536	7543	7551	1	2	2	3	4	5	5	6	7
57	7559	7566	7574	7582	7589	7597	7604	7612	7619	7627	1	2	2	3	4	5	5	6	7
58	7634	7642	7649	7657	7664	7672	7679	7686	7694	7701	1	1	2	3	4	4	5	6	7
59	7709	7716	7723	7731	7738	7745	7752	7760	7767	7774	1	1	2	3	4	4	5	6	7
60	7782	7789	7796	7803	7810	7818	7825	7832	7839	7846	1	1	2	3	4	4	5	6	6
61	7853	7860	7868	7875	7882	7889	7896	7903	7910	7917	1	1	2	3	4	4	5	6	6
62	7924	7931	7938	7945	7952	7959	7966	7973	7980	7987	1	1	2	3	3	4	5	6	6
63	7993	8000	8007	8014	8021	8028	8035	8041	8048	8055	1	1	2	3	3	4	5	5	6
64	8062	8069	8075	8082	8089	8096	8102	8109	8116	8122	1	1	2	3	3	4	5	5	6
65	8129	8136	8142	8149	8156	8162	8169	8176	8182	8189	1	1	2	3	3	4	5	5	6
66	8195	8202	8209	8215	8222	8228	8235	8241	8248	8254	1	1	2	3	3	4	5	5	6
67	8261	8267	8274	8280	8287	8293	8299	8306	8312	8319	1	1	2	3	3	4	5	5	6
68	8325	8331	8338	8344	8351	8357	8363	8370	8376	8382	1	1	2	3	3	4	4	5	6
69	8388	8395	8401	8407	8414	8420	8426	8432	8439	8445	1	1	2	2	3	4	4	5	6
70	8451	8457	8463	8470	8476	8482	8488	8494	8500	8506	1	1	2	2	3	4	4	5	6
71	8513	8519	8525	8531	8537	8543	8549	8555	8561	8567	1	1	2	2	3	4	4	5	5
72	8573	8579	8585	8591	8597	8603	8609	8615	8621	8627	1	1	2	2	3	4	4	5	5
73	8633	8639	8645	8651	8657	8663	8669	8675	8681	8686	1	1	2	2	3	4	4	5	5
74	8692	8698	8704	8710	8716	8722	8727	8733	8739	8745	1	1	2	2	3	4	4	5	5
75	8751	8756	8762	8768	8774	8779	8785	8791	8797	8802	1	1	2	2	3	3	4	5	5
76	8808	8814	8820	8825	8831	8837	8842	8848	8854	8859	1	1	2	2	3	3	4	5	5
77	8865	8871	8876	8882	8887	8893	8899	8904	8910	8915	1	1	2	2	3	3	4	4	5
78	8921	8927	8932	8938	8943	8949	8954	8960	8965	8971	1	1	2	2	3	3	4	4	5
79	8976	8982	8987	8993	8998	9004	9009	9015	9020	9025	1	1	2	2	3	3	4	4	5
80	9031	9036	9042	9047	9053	9058	9063	9069	9074	9079	1	1	2	2	3	3	4	4	5
81	9085	9090	9096	9101	9106	9112	9117	9122	9128	9133	1	1	2	2	3	3	4	4	5
82	9138	9143	9149	9154	9159	9165	9170	9175	9180	9186	1	1	2	2	3	3	4	4	5
83	9191	9196	9201	9206	9212	9217	9222	9227	9232	9238	1	1	2	2	3	3	4	4	5
84	9243	9248	9253	9258	9263	9269	9274	9279	9284	9289	1	1	2	2	3	3	4	4	5
85	9294	9299	9304	9309	9315	9320	9325	9330	9335	9340	1	1	2	2	3	3	4	4	5
86	9345	9350	9355	9360	9365	9370	9375	9380	9385	9390	1	1	2	2	3	3	4	4	5
87	9395	9400	9405	9410	9415	9420	9425	9430	9435	9440	0	1	1	2	2	3	3	4	4
88	9445	9450	9455	9460	9465	9469	9474	9479	9484	9489	0	1	1	2	2	3	3	4	4
89	9494	9499	9504	9509	9513	9518	9523	9528	9533	9538	0	1	1	2	2	3	3	4	4
90	9542	9547	9552	9557	9562	9566	9571	9576	9581	9586	0	1	1	2	2	3	3	4	4
91	9590	9595	9600	9605	9609	9614	9619	9624	9628	9633	0	1	1	2	2	3	3	4	4
92	9638	9643	9647	9652	9657	9661	9666	9671	9675	9680	0	1	1	2	2	3	3	4	4
93	9685	9689	9694	9699	9703	9708	9713	9717	9722	9727	0	1	1	2	2	3	3	4	4
94	9731	9736	9741	9745	9750	9754	9759	9763	9768	9773	0	1	1	2	2	3	3	4	4
95	9777	9782	9786	9791	9795	9800	9805	9809	9814	9818	0	1	1	2	2	3	3	4	4
96	9823	9827	9832	9836	9841	9845	9850	9854	9859	9863	0	1	1	2	2	3	3	4	4
97	9868	9872	9877	9881	9886	9890	9894	9899	9903	9908	0	1	1	2	2	3	3	4	4
98	9912	9917	9921	9926	9930	9934	9939	9943	9948	9952	0	1	1	2	2	3	3	4	4
99	9956	9961	9965	9969	9974	9978	9983	9987	9991	9996	0	1	1	2	2	3	3	3	4

(BLANK)

APPENDIX 3

LIST OF WORDS CONTAINING LIKE LETTERS REPEATED AT VARIOUS INTERVALS

(BLANK)

~~CONFIDENTIAL~~

LIST OF WORDS CONTAINING LIKE LETTERS REPEATED AT VARIOUS INTERVALS

AA	RU	BBER	AA	CR	EEK
AA	RU	BBLE	AA	DECR	EE
AA	A	CCEPT	AA	DEGR	EE
AA	A	CCEPTABLE	AA	EIGHT	EEN
AA(5)A	A	CCEPTANCE	AA	EIGHT	EENTH
AA	A	CCESS	AA	EMPLOY	EE
AA	A	CCESSORY	AA	ENGIN	EER
AA	A	CCIDENTAL	AA	ENGIN	EERING
AA	A	CCOMPANY	AA	F	EEL
AA	A	CCOMMODATION	AA	F	EET
AA(5)A	A	CCORDANCE	AA	FIFT	EEN
AA	A	CCORDING	AA	FIFT	EENTH
AA	O	CCUPATION	AA	FL	EE
AA	O	CCUPY	AA	FL	EET
AA	SU	CCEEDED	AA	FOURT	EEN
AA	SU	CCESS	AA	FOURT	EENTH
AA	SU	CCESSFUL	AA	HASB	EEN
AA	SU	CCESSFULLY	AA	HAVEB	EEN
AA	SU	CCESSIVE	AA	IND	EED
AA	TOBA	CCO	AA	K	EEP
AA	UNSU	CCESSFUL	AA(1)A	K	EEPER
AA	A	DD	AA	M	EET
AA	A	DDITIONAL	AA	NINET	EEN
AA	A	DDRESSES	AA	NINET	EENTH
AA	A	DDRESS	AA	PROC	EED
AA(5)A	A	DDRESSED	AA(1)A	PROC	EEDED
AA	BE	DDING	AA	QU	EEN
AA	LA	DDER	AA(5)A	R	EENFORCE
AA	SU	DDEN	AA(5)A(1)A	R	EENFORCEMENT
AA(1)A	AGR	EEMENT	AA	R	EENLIST
AA	B	EEN	AA(5)A	R	EENLISTED
AA(1)A	BEENN	EEDED	AA(6)A	R	EENLISTMENT
AA(2)AA(1)A	B	EENNEEDED	AA	REFUG	EE
AA(2)A	B	EETLE	AA	SCR	EEN
AA	BETW	EEN	AA	SCR	EENING
AA(1)A	BR	EEZE	AA	S	EE
AA(1)A	CH	EESE	AA	S	EEN
AA	COFF	EE	AA	SEVENT	EEN
AA	COMMAND	EER	AA	SEVENT	EENTH
AA	COMMITT	EE	AA	SIXT	EEN

AA		SIXT EENTH	AA		ACTUA LLY
AA		SMOKESCR EEN	AA		A LL
AA		SP EED	AA		A LLEGE
AA		ST EEL	AA		A LLEGIANCE
AA		STR EET	AA		A LLIED
AA(1)A		SUCC EEDED	AA		A LLIES
AA		SW EEPING	AA		A LLOCATION
AA		THIRT EEN	AA		A LLOTMENT
AA		THIRT EENTH	AA		A LLOWANCE
AA		THR EE	AA		A LLOW
AA		W EEK	AA		A LLY
AA		WH EEL	AA		ARTI LLERY
AA		A FFAIR	AA		BA LLISTICS
AA		CHAU FFEUR	AA		BA LLOON
AA		COE FFICIENT	AA		BE LLIGERENT
AA		CO FFEE	AA		BI LLET
AA		DI FFERENCE	AA		BI LLETED
AA		DI FFERENT	AA		BU LLETIN
AA		DI FFICULT	AA		CA LL
AA		DI FFICULTIES	AA		CANCE LLATION
AA		E FFECT	AA		CANCE LLED
AA		E FFECTED	AA		CE LL
AA		E FFECTIVE	AA		CHA LLENGE
AA		E FFICACY	AA		CO LLAPSED
AA		E FFICIENT	AA		CO LLECT
AA		E FFICIENCY	AA		CO LLECTION
AA		E FFORT	AA		CO LLEGE
AA		GENERALSTA FF	AA		CO LLISION
AA		INE FFICIENCY	AA		COMPE LLED
AA		JUMPO FF	AA		DISTI LL
AA		O FF	AA		DO LLAR
AA		O FFEND	AA		DRI LL
AA		O FFENDED	AA		ENRO LL
AA		O FFENSE	AA		ENRO LLED
AA		O FFENSIVE	AA		ENRO LLMENT
AA		O FFICE	AA		EXPE LLED
AA		O FFICER	AA		FA LL
AA		O FFICIAL	AA		FA LLING
AA		POSTO FFICE	AA		FE LL
AA		STA FF	AA		FI LLING
AA		SU FFER	AA		FO LLOW
AA		SU FFERED	AA		FU LL
AA		SU FFICIENT	AA		HI LL
AA		TRA FFIC	AA		I LL
AA(1)A		BA GGAGE	AA(3)A		I LLEGAL
AA		FO GGY	AA		I LLITERATE
AA		STRA GGLER	AA		I LLNESS
AA		SU GGEST	AA		I LLUMINATE
AA		TRI GGER	AA		I LLUMINATING
AA		BEAC HHEAD	AA		I LLUMINATION

AA	I LLUSTRATE
AA	I LLUSTRATION
AA	INSTA LL
AA	INSTA LLATIONS
AA	INTE LLIGENCE
AA	INTE LLIGENT
AA	KI LLED
AA	KI LLING
AA	MI LLIMETER
AA	MISCE LLANEOUS
AA	OSCI LLATE
AA	PARA LLAX
AA(1)A	PARA LLEL
AA	PATRO LLING
AA	PAYRO LL
AA	RA LLY
AA	REBE LLION
AA	REFI LL
AA	REFI LLING
AA	REPE LLED
AA	RESPECTFU LLY
AA	SHE LL
AA	SHE LLED
AA	SHE LLFIRE
AA	SHE LLING
AA	SHE LLS
AA	SIGNA LLING
AA	SMA LL
AA	SPE LL
AA	SUCCESSFU LLY
AA	VA LLEY
AA	VI LLAGE
AA	WE LL
AA	WI LL
AA	WI LLATTACK
AA	WI LLIAM
AA	ACCO MMODATION
AA	A MMETER
AA	A MMUNITION
AA	CO MMA
AA	CO MMAND
AA	CO MMANDANT
AA	CO MMANDED
AA	CO MMANDEER
AA	CO MMANDER
AA	CO MMANDING
AA	CO MMENCE
AA(4)A	CO MMENCEMENT
AA	CO MMEND
AA	CO MMENDATION

AA	CO MMENT
AA	CO MMERCE
AA	CO MMISSARY
AA	CO MMISSION
AA	CO MMISSIONER
AA	CO MMIT
AA(2)A	CO MMITMENT
AA	CO MMITTEE
AA	CO MMON
AA	CO MMUNICATE
AA	CO MMUNICATION
AA	CO MMUNIQUE
AA	CO MMUTE
AA	HA MMER
AA	I MMEDIATE
AA	I MMIGRATION
AA	INFLA MMABLE
AA	RECO MMEND
AA	RECO MMENDATION
AA	RECO MMENDED
AA	SU MMARY
AA	SU MMER
AA	SU MMIT
AA	SU MMON
AA	SWI MMING
AA	A NNEX
AA	A NNOUNCE
AA(2)A(4)A	A NNOUNCEMENT
AA	A NNUAL
AA	ANTE NNA
AA	BA NNER
AA	BEE NNEEDED
AA(1)A	BEGI NNING
AA	CA NNOT
AA	CHA NNEL
AA(4)A	CO NNECTING
AA(5)A	CO NNECTION
AA	GU NNER
AA	MA NNER
AA(1)A	MA NNING
AA	PERSO NNEL
AA(1)A	PLA NNING
AA(5)A	RECO NNAISSANCE
AA	RECO NNOITER
AA(6)A	RECO NNOITERING
AA	RU NNER
AA(1)A	RU NNING
AA	TO NNAGE
AA	AFTERN OON
AA	ASS OONAS

AA	BALL	OON	AA	A	PPROXIMATE
AA	B	OOK	AA	CLI	PPER
AA	B	OOTH	AA	DISA	PPEAR
AA	CODEB	OOK	AA	DISA	PPEARANCE
AA	C	OOK	AA	DISA	PPEARED
AA	C	OOPERATE	AA	DRO	PPED
AA(6)A	C	OOPERATION	AA	HA	PPEN
AA	C	OORDINATE	AA	MA	PPING
AA(7)A	C	OORDINATION	AA	O	PPOSE
AA(2)A	F	OOTHOLD	AA	O	PPOSITE
AA	FOREN	OON	AA	O	PPOSITION
AA	H	OOK	AA	PHILI	PPINES
AA	L	OOK	AA	REA	PPOINTED
AA(1)A	L	OOKOUT	AA	REA	PPOINTMENT
AA	N	OON	AA	SHI	PPING
AA	PLAT	OON	AA	STO	PPED
AA	PONT	OON	AA	SU	PPLIES
AA	PR	OOF	AA	SU	PPLY
AA	SCH	OOL	AA	SU	PPORT
AA	SCH	OOLHOUSE	AA	SU	PPORTING
AA	SHARPSH	OOTER	AA	SU	PPOSE
AA	S	OON	AA	A	RRANGE
AA	SP	OOLS	AA	A	RRANGEMENT
AA	SP	OONS	AA	A	RREST
AA	TATT	OO	AA	A	RRESTED
AA	T	OO	AA	A	RRIVAL
AA	T	OOK	AA	A	RRIVE
AA	T	OOL	AA	BA	RRACKS
AA	TR	OOPS	AA	BA	RRAGE
AA	TR	OOPSHIP	AA	CA	RRIAGE
AA	TR	OOPSHIPS	AA(2)A	CA	RRIER
AA	UNDERST	OOD	AA	CA	RRY
AA	W	OODED	AA	CONFE	RRED
AA	W	OODS	AA	CO	RRECT
AA	AIRSU	PPORT	AA	CO	RRECTED
AA	A	PPARATUS	AA	CO	RRECTION
AA	A	PPARENT	AA	CO	RRECTNESS
AA	A	PPARENTLY	AA	CO	RRESPONDENCE
AA	A	PPEAR	AA	CO	RRESPONDING
AA	A	PPEARANCE	AA(3)A	CO	RRIDOR
AA	A	PPEARED	AA	CU	RRENT
AA	A	PPLICATION	AA	DEFE	RRED
AA	A	PPLY	AA	DE	RRICK
AA	A	PPOINT	AA(1)A	E	RROR
AA	A	PPOINTED	AA	FE	RRY
AA	A	PPOINTMENT	AA	GA	RRISON
AA	A	PPROACH	AA	HU	RRICANE
AA(2)A	A	PPROPRIATE	AA	INTE	RRUPT
AA	A	PPROVAL	AA	INTE	RRUPTED
AA	A	PPROVE	AA	INTE	RRUPTION

~~CONFIDENTIAL~~

AA(5)A	I	RREGULAR
AA(5)A	I	RREGULARITIES
AA(5)A	I	RREGULARITY
AA	I	RRIGATION
AA(1)A	MI	RROR
AA	PREA	RRANGED
AA	PREFE	RRED
AA(4)A	SU	RRENDER
AA(4)A	SU	RRENDERED
AA	SU	RROUND
AA	TE	RRAIN
AA	TE	RRIBLE
AA	TE	RRIFIC
AA(3)A	TE	RRITORY
AA(1)A	TE	RROR
AA	TOMO	RROW
AA	TRANSFE	RRED
AA	TRANSFE	RRING
AA	TU	RRET
AA	ACCE	SS
AA	ACCE	SSORY
AA	ACRO	SS
AA	ADDRE	SSED
AA	ADDRE	SS
AA(1)A	ADDRE	SSES
AA	ADMI	SSION
AA	AMBA	SSADOR
AA	ASPO	SSIBLE
AA	A	SSAULT
AA	A	SSEMBLE
AA	A	SSEMBLY
AA(6)A	A	SSEMBLIES
AA(1)AA(4)A	A	SSESSMENTS
AA(4)A	ASSE	SSMENTS
AA	A	SSET
AA(2)A	A	SSETS
AA	A	SSIGNED
AA	A	SSIGNMENT
AA(7)A	A	SSIGNMENTS
AA(1)A	A	SSIST
AA(1)A	A	SSISTANT
AA(1)A	A	SSISTANCE
AA	A	SSOCIATE
AA	A	SSOCIATION
AA(4)A	A	SSOONAS
AA	A	SSURANCE
AA	A	SSURE
AA	BUSINE	SS
AA	CARELE	SS
AA(2)AA	CARELE	SSNESS
AA	CARELESSNE	SS
AA(1)A	CHA	SSIS
AA	CLA	SSIFICATION
AA	COMMI	SSARY
AA	COMMI	SSION
AA	COMMI	SSIONER
AA	COMPA	SS
AA	COMPLETENE	SS
AA	COMPRE	SSED
AA	CONCE	SSION
AA	CONFE	SSION
AA	CONGRE	SS
AA	CONGRE	SSIONAL
AA	CORRECTNE	SS
AA	CRO	SS
AA	CRO	SSING
AA(4)A	CRO	SSROADS
AA	DARKNE	SS
AA	DEPRE	SSION
AA	DISCU	SS
AA	DISCU	SSED
AA	DISCU	SSION
AA	DISMI	SS
AA	DISMI	SSAL
AA	DI	SSEMINATED
AA	DI	SSEMINATION
AA	DISTRE	SS
AA	DISTRE	SSED
AA	DRE	SS
AA	DRE	SSING
AA(2)A	EMBA	SSIES
AA	EMBA	SSY
AA	EXCE	SS
AA	EXCE	SSIVE
AA	EXPRE	SS
AA	FORTRE	SS
AA	GA	SSING
AA(1)A	GLA	SSES
AA(1)A	HEAVYLO	SSES
AA	ILLNE	SS
AA	IMPA	SSABLE
AA	IMPO	SSIBLE
AA	IMPRE	SSED
AA	IMPRE	SSION
AA	IMPRE	SSIVE
AA	I	SSUE
AA(2)A	I	SSUES
AA	I	SSUING
AA	LE	SS
AA	LE	SSON

~~CONFIDENTIAL~~

AA	LO	SS
AA(1)A	LO	SSES
AA	MA	SS
AA	ME	SS
AA	ME	SSAGE
AA(3)A	ME	SSAGES
AA	ME	SSENGER
AA	ME	SSING
AA	MI	SSING
AA	MI	SSION
AA(3)A	MI	SSIONS
AA	NECE	SSARY
AA	NECE	SSITY
AA	NECE	SSITATE
AA	PA	SS
AA	PA	SSAGE
AA	PA	SSED
AA	PA	SSENGER
AA(1)A	PA	SSES
AA	PA	SSIVE
AA	PA	SSPORT
AA	PERMI	SSION
AA	POSSE	SSION
AA(1)AA	PO	SSESSION
AA	PO	SSIBLE
AA	PREPAREDNE	SS
AA	PRE	SS
AA	PRE	SSED
AA	PRE	SSURE
AA	PROGRE	SSIVE
AA	PROGRE	SS
AA	READINE	SS
AA	RECONNAI	SSANCE
AA	REDCRO	SS
AA	SE	SSION
AA	STRE	SS
AA	SUBMI	SSION
AA	SUCCE	SS
AA	SUCCE	SSFUL
AA	SUCCE	SSFULLY
AA	SUCCE	SSIVE
AA	TRANSMI	SSION
AA	UNLE	SS
AA	UNSUCCE	SSFUL
AA	USELE	SS
AA	VE	SSEL
AA(2)A	VE	SSELS
AA	WIRELE	SS
AA	WITNE	SS
AA(1)A	WITNE	SSES

AA	A	TTACH
AA(6)A	A	TTACHMENT
AA	A	TTACK
AA	A	TTAIN
AA(6)A	A	TTAINMENT
AA(3)A	A	TTEMPT
AA(3)A	A	TTEMPTED
AA(2)A	A	TTENTION
AA	BA	TTALION
AA	BA	TTEN
AA	BA	TTERED
AA	BA	TTERIES
AA	BA	TTERY
AA	BA	TTLE
AA	BA	TTLEFIELD
AA	BA	TTLESHIP
AA	BE	TTER
AA	BI	TTER
AA	BO	TTOM
AA	BOYCO	TT
AA	CIGARE	TTE
AA	COMMI	TTEE
AA	COUNTERA	TTACK
AA	FI	TTING
AA	GE	TTING
AA	LE	TTER
AA	LE	TTERED
AA	LI	TTER
AA	LI	TTLE
AA	NAVALA	TTACK
AA	NAVALBA	TTLE
AA	OMI	TTED
AA	SE	TTLE
AA	SPO	TTING
AA	SUBMI	TTED
AA	TA	TTOO
AA	THA	TTHE
AA	WILLA	TTACK
AA	WRI	TTEN
AA	MU	ZZLE
AA	NO	ZZLE
A-A		ABANDON
A-A		AGAIN
A-A		AGAINST
A-A		ALARM
A-A(2)A		ALASKA
A-A	ALM	ANAC
A-A		ANALYSIS
A-A		ANALYZE
A-A	APP	ARATUS

~~CONFIDENTIAL~~

A-A	APPE	ARANCE
A-A(2)A		ARABIA
A-A(2)A		AVAILABLE
A-A		AWAIT
A-A		AWARD
A-A		AWAY
A-A	C	ALAMITY
A-A(1)A	C	ANADA
A-A	CAN	ADA
A-A	C	ANAL
A-A	C	APABILITY
A-A	C	APACITY
A-A	C	ATASTROPHE
A-A	C	AVALRY
A-A	CH	ARACTER
A-A	CH	ARACTERISTIC
A-A	CLE	ARANCE
A-A	COMB	ATANT
A-A	CONTR	ABAND
A-A	D	AMAGE
A-A	D	AMAGED
A-A	D	AMAGING
A-A	DISAPPE	ARANCE
A-A	EXC	AVATE
A-A	EXC	AVATION
A-A	EXPL	ANATION
A-A	F	ATAL
A-A	F	ATALITY
A-A	FIRE	ALARM
A-A	G	ARAGE
A-A(1)A	GENER	ALALARM
A-A	GENERAL	ALARM
A-A	J	APAN
A-A	M	ANAGE
A-A	M	ANAGEMENT
A-A	N	AVAL
A-A(1)A(2)A	N	AVALATTACK
A-A(2)A	NAV	ALATTACK
A-A(2)A	N	AVALBASE
A-A(2)A	N	AVALBATTLE
A-A	N	AVALFORCES
A-A	NONCOMB	ATANT
A-A(1)A	P	ANAMA
A-A	PAN	AMA
A-A	P	ARACHUTE
A-A	P	ARADE
A-A(2)A	P	ARAGRAPH
A-A(2)A	P	ARALLAX
A-A	P	ARALLEL
A-A	PREP	ARATION
A-A	PROCL	AMATION
A-A	QU	ARANTINE
A-A	S	ALARY
A-A	SEP	ARATE
A-A	SEP	ARATION
A-A	T	AXATION
A-A	V	ACANCY
A-A	WITHDR	AWAL
A-A	PRO	BABLE
A-A	PRO	BABLY
A-A	BI	CYCLE
A-A		CYCLONE
A-A	EFFI	CACY
A-A	MOTOR	CYCLE
A-A	BEENNEE	DED
A-A	BLOCKA	DED
A-A	BOMBAR	DED
A-A	COMMAN	DED
A-A	DECI	DED
A-A		DEDICATE
A-A		DEDICATION
A-A	DEFEN	DED
A-A	DEMAN	DED
A-A	ENCO	DED
A-A	EXPAN	DED
A-A	EXPEN	DED
A-A	EXTEN	DED
A-A	GROUN	DED
A-A	GUAR	DED
A-A	INVA	DED
A-A	LAN	DED
A-A	OFFEN	DED
A-A	PROCEE	DED
A-A	RAI	DED
A-A	RECOMMEN	DED
A-A	SUCCEE	DED
A-A	SUSPEN	DED
A-A	UNEXPEN	DED
A-A	WOO	DED
A-A	WOUN	DED
A-A		DID
A-A	AGRE	EMENT
A-A	ALL	EGE
A-A	AMM	ETER
A-A	AMUS	EMENT
A-A	ANNOUNC	EMENT
A-A	ARRANG	EMENT
A-A	BAROM	ETER
A-A	BATT	ERED
A-A	BEENNE	EDED

~~CONFIDENTIAL~~

A-A	BELLIG ERENT
A-A	BESI EGED
A-A	BILL ETED
A-A	BRE EZE
A-A	BRIDG EHEAD
A-A	CAR ELESS
A-A(3)A	CAR ELESSNESS
A-A	CEM ETERY
A-A(1)A	C EMETERY
A-A	CENT ERED
A-A	CHE ESE
A-A	COLL EGE
A-A	COMMENC EMENT
A-A	COMPL ETELY
A-A	COMPL ETE
A-A	COMPLET ENESS
A-A(1)A	COMPL ETENESS
A-A	CONCR ETE
A-A(2)A	CONF ERENCE
A-A	CONFIN EMENT
A-A	CONQU ERED
A-A	COV ERED
A-A	CR EDENTIAL
A-A(2)A	D ECEMBER
A-A(7)A	D ECENTRALIZE
A-A(7)A	D ECENTRALIZED
A-A	DECIPH ERED
A-A	D EFEAT
A-A(2)A	D EFEATED
A-A	D EFECT
A-A(4)A	D EFECTIVE
A-A	D EFEND
A-A(2)A	D EFENDER
A-A(2)A	D EFENDED
A-A(2)A	D EFENSE
A-A(4)A	D EFENSIVE
A-A	D EFER
A-A(2)A	D EFERRED
A-A	D EPEND
A-A	D EPENDABILITY
A-A(5)A	D EPENDABLE
A-A(2)A	D EPENDENT
A-A	D ESERT
A-A(2)A	D ESERTED
A-A(2)A	D ESERTER
A-A	D ETECTOR
A-A	D ETENTION
A-A(6)A	D ETERIORATE
A-A	D ETERMINATION
A-A(4)A	D ETERMINE
A-A(4)A	D ETERMINED
A-A	D EVELOP
A-A(3)A	D EVELOPED
A-A(4)A	D EVELOPMENT
A-A	DIFF ERENT
A-A(2)A	DIFF ERENCE
A-A	DISPLAC EMENT
A-A	DYNAMOM ETER
A-A	ELECTRICITY
A-A	EL EMENT
A-A	EL EMENTARY
A-A(1)A	ELEMENT
A-A(1)A	ELEMENTARY
A-A(3)A	ELEVATE
A-A	ELEVATION
A-A(1)A	ELEVEN
A-A	EL EVEN
A-A	ELSEWH ERE
A-A(2)A	EMERGENCY
A-A	EMPLAC EMENT
A-A	ENCIPH ERED
A-A	ENCOUNT ERED
A-A(2)A	ENEMIES
A-A	ENEMY
A-A(6)A	ENEMYPLANES
A-A	ENEMYTANKS
A-A	ENFORC EMENT
A-A	ENGAG EMENT
A-A	ENTANGL EMENT
A-A	EVERY
A-A	EXCIT EMENT
A-A(5)A	EXECUTIVE
A-A(4)A	EXERCISE
A-A	EXTR EME
A-A	EYE
A-A	F EDERAL
A-A	G ENERAL
A-A	G ENERALALARM
A-A	G ENERALSTAFF
A-A	GONIOM ETER
A-A	GYROM ETER
A-AA	HAV EBEEN
A-A	H ERE
A-A	HIND ERED
A-A	HYDROM ETER
A-A	HYGROM ETER
A-A	IC EBERG
A-A	IMPROV EMENT
A-A(2)A	INCOMP ETENCE
A-A	INCOMP ETENT

A-A(2)A	IND EPENDENT
A-A(6)A	IND ETERMINATE
A-A	INT EREST
A-A	INT ERESTING
A-A	INTERF ERE
A-A(2)A	INTERF ERENCE
A-A	INTERPR ETER
A-A	INTERV ENE
A-A	KE EPER
A-A	KILOM ETER
A-A	LETT ERED
A-A	L EVEL
A-A	MANAG EMENT
A-A	MANGAN ESE
A-A	MEASUR EMENT
A-A	MEASUR EMENTS
A-A	M ETEOROLOGICAL
A-A	M ETER
A-A	MILLIM ETER
A-A	MOV EMENT
A-A	N ECESSARY
A-A	N ECESSITY
A-A(6)A	N ECESSITATE
A-AA	NIN ETEEN
A-AA	NIN ETEENTH
A-A	OBSOL ETE
A-A	ORD ERED
A-A	PARENTH ESES
A-A	P ENETRATION
A-A(4)A	P ENETRATE
A-A	P ETER
A-A	PLAC EMENT
A-A	PREC EDE
A-A(1)A	PR ECEDE
A-A(2)A	PREC EDENCE
A-A(1)A(2)A	PR ECEDENCE
A-A	PR ECEDING
A-A	PR EFER
A-A(2)A	PREF ERENCE
A-A(1)A(2)A	PR EFERENCE
A-A(2)A	PR EFERRED
A-A	PR ESENT
A-A	PR ESERVATION
A-A(2)A	PR ESERVE
A-A	PROCE EDED
A-A	PSYCHROM ETER
A-A	R EBELLION
A-A	R ECEIPT
A-A(2)A	R ECEIVE
A-A(2)A	R ECEIVER
A-A	R ECEIVING
A-A(5)A	R ECEPTACLE
A-A	REENFORC EMENT
A-A	R EFER
A-A(2)A	REF ERENCE
A-A(1)A(2)A	R EFERENCE
A-A	REIMBURS EMENT
A-A	REINFORC EMENT
A-A	REINSTAT EMENT
A-A	R EJECT
A-A(2)A	R EJECTED
A-A	R EJECTOR
A-A(2)A	R ELEASE
A-A	RELI EVE
A-A(2)A	R EMEDIES
A-A	R EMEDY
A-A(2)A	R EMEMBER
A-A(2)A	R EPEATED
A-A(2)A	R EPEATER
A-A	R EPEL
A-A(2)A	R EPELLED
A-A	REPLAC EMENT
A-A	REPR ESENT
A-A	REPR ESENTATION
A-A(6)A	REPR ESENTATIVE
A-A	REQUIR EMENT
A-A	R ESEARCH
A-A	R ESERVATION
A-A(2)A	R ESERVE
A-A	R ETENTION
A-A(2)A	R EVENUE
A-A(2)A	R EVERSE
A-A	REVI EWED
A-A	SCH EME
A-A	SEAL EVEL
A-A	S ELECT
A-A(2)A	S ELECTED
A-A	S EVEN
A-A(2)AA	S EVENTEEN
A-A(2)AA	S EVENTEENTH
A-A	S EVENTH
A-A	S EVENTY
A-A(6)A	S EVENTYFIVE
A-A	S EVERAL
A-A	SEV ERE
A-A(1)A	S EVERE
A-A	SI EGE
A-A	SPH ERE
A-A	STAT EMENT
A-A	SUCCE EDED

A-A	SUFF	ERED
A-A	SURREND	ERED
A-A	T	ELEGRAM
A-A(4)A	T	ELEPHONE
A-A	TH	ERE
A-A(3)A	TH	EREFORE
A-A	THERMOM	ETER
A-A	TH	ESE
A-A	THREAT	ENED
A-A	US	ELESS
A-A	V	ETERINARIAN
A-A	W	ERE
A-A	WH	ERE
A-A	WIR	ELESS
A-A		FIFTEEN
A-A		FIFTEENTH
A-A		FIFTH
A-A		FIFTY
A-A	BAG	GAGE
A-A	EN	GAGE
A-A	EN	GAGEMENT
A-A(2)A	EN	GAGING
A-A	EIG	HTH
A-A	WIT	HTHE
A-A	ACT	IVITY
A-A	ACTIV	ITIES
A-A(1)A	ACT	IVITIES
A-A	ADD	ITIONAL
A-A(5)A	ADM	INISTRATIVE
A-A(5)A	ADM	INISTRATION
A-A	ADV	ISING
A-A	AMMUN	ITION
A-A	ANT	IAIRCRAFT
A-A	ANT	ICIPATE
A-A(3)A	ANT	ICIPATION
A-A	ARTIF	ICIAL
A-A(1)A	ART	IFICIAL
A-A	AUDIB	ILITY
A-A(1)A	AUD	IBILITY
A-A	CAPAB	ILITY
A-A	CERT	IFICATE
A-A	CIV	ILIAN
A-A(1)A	C	IVILIAN
A-A(3)A	CLASS	IFICATION
A-A	COAL	ITION
A-A	COEFF	ICIENT
A-A	COLL	ISION
A-A	COLL	ISIONS
A-A	COMPET	ITION
A-A	COMPOS	ITION
A-A(2)A	CONC	ILIATION
A-A	COND	ITION
A-A	CR	ISIS
A-A	CR	ITIC
A-A	CR	ITICAL
A-A	CRIT	ICISE
A-A(1)A	CR	ITICISE
A-A	CR	ITIQUE
A-A	DEC	ISION
A-A	DEF	ICIENCY
A-A	DEF	ICIENT
A-A	DEF	INITE
A-A	DEFIN	ITION
A-A(1)A	DEF	INITION
A-A	DEMOB	ILIZE
A-A(3)A	DEMOB	ILIZATION
A-A	DEPENDAB	ILITY
A-A	DETRA	INING
A-A	DIET	ITIAN
A-A	DIM	INISH
A-A(1)A	D	IMINISH
A-A	DIR	IGIBLE
A-A(1)A	D	IRIGIBLE
A-A	D	ISINFECT
A-A	D	ISINFECTED
A-A	DISPOS	ITION
A-A	D	IVIDE
A-A	DIV	IDING
A-A(1)A	D	IVIDING
A-A	DIV	ISION
A-A(1)A	D	IVISION
A-A	EFF	ICIENT
A-A	EFF	ICIENCY
A-A	ELECTR	ICITY
A-A	EL	IGIBLE
A-A	ENTERPR	ISING
A-A	EXH	IBITED
A-A	EXHIB	ITION
A-A(1)A	EXH	IBITION
A-A	EXPED	ITING
A-A	EXPED	ITION
A-A	FACIL	ITIES
A-A(1)A	FAC	ILITIES
A-A	F	ILING
A-A	F	INISH
A-A	F	IRING
A-A	FORT	IFIED
A-A	HOST	ILITY
A-A	HOSTIL	ITIES
A-A(1)A	HOST	ILITIES

~~CONFIDENTIAL~~

A-A(3)A	IDENT IFICATION
A-A	IGN ITION
A-A	INCL INING
A-A	IND IVIDUAL
A-A	INEFF ICIENCY
A-A	IN ITIAL
A-A(1)A	INITIAL
A-A	IN ITIATE
A-A(1)A	INITIATE
A-A	IRREGULAR ITIES
A-A	LIAB ILITY
A-A	L IAISON
A-A	L IMIT
A-A(3)A	L IMITATION
A-A(1)A	L IMITING
A-A	LIM ITING
A-A	L INING
A-A	MAR ITIME
A-A	MED ICINE
A-A	M ILITARY
A-A(1)A	M ILITIA
A-A	MIL ITIA
A-A	M INIMUM
A-A	M INING
A-A(3)A	MOB ILIZATION
A-A	MOB ILIZE
A-A	MUN ITIONS
A-A	OBTA INING
A-A	OFF ICIAL
A-A	OP INION
A-A	OPPOS ITION
A-A	PAC IFIC
A-A	PART ITION
A-A(2)A	PH ILIPPINES
A-A	POL ITICAL
A-A	POL ITICS
A-A	POS ITION
A-A	POS ITIONS
A-A	POS ITIVE
A-A	PRA IRIE
A-A(3)A	PREL IMINARIES
A-A	PREL IMINARY
A-A	PROH IBIT
A-A	PROV ISION
A-A	PROV ISIONS
A-A	PROX IMITY
A-A(3)A	QUAL IFICATION
A-A	RA IDING
A-A	RA INING
A-A	RECE IVING
A-A	RECOGN ITION
A-A	RECRU ITING
A-A	REMA INING
A-A	REQU IRING
A-A(1)A	REQU ISITION
A-A	REQUIS ITION
A-A(1)A	RESPONS IBILITY
A-A	RESPONSIB ILITY
A-A	RET IRING
A-A	R IDING
A-A	R IGID
A-A	RIT ICISM
A-A(1)A	R ITICISM
A-A	SEMIR IGID
A-A(1)A	SEM IRIGID
A-A	SERV ICING
A-A	SIGN IFICANT
A-A	SIGN IFICANCE
A-A	S IMILAR
A-A(3)A	S IMILARITY
A-A	SPEC IFIC
A-A(3)A	SPEC IFICATION
A-A	SUFF ICIENT
A-A	SUITAB ILITY
A-A	SUSP ICION
A-A	SUSP ICIONS
A-A	SUSP ICIOUS
A-A	TERR IFIC
A-A	TRAD ITIONAL
A-A	TRA INING
A-A	TRANSPAC IFIC
A-A	UNIDENT IFIED
A-A	UT ILITY
A-A(3)A	VER IFICATION
A-A	VIC INITY
A-A(1)A	V ICINITY
A-A	VISIB ILITY
A-A(1)A	VIS IBILITY
A-A(1)A(1)A	V ISIBILITY
A-A	V ISIBLE
A-A	V ISIT
A-A	V ISITOR
A-A	V ISITS
A-A	W IRING
A-A	GENERA LALARM
A-A	PARAL LEL
A-A	AR MAMENT
A-A	DYNA MOMETER
A-A	MAXI MUM
A-A	MEMBER

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

A-A		MEMORANDA
A-A(6)A		MEMORANDUM
A-A		MEMORIAL
A-A	MINI	MUM
A-A	RE	MEMBER
A-A	THER	MOMETER
A-A	A	NONYMOUS
A-A	BEGIN	NING
A-A	CONCER	NING
A-A	CONTI	NENTAL
A-A	DETRAI	NING
A-A	DOMI	NANCE
A-A	DOMI	NANT
A-A	INCLI	NING
A-A	INTERVE	NING
A-A	LIEUTE	NANT
A-A	LI	NING
A-A	MAINTE	NANCE
A-A	MAN	NING
A-A	MI	NING
A-A	MOR	NING
A-A		NAN
A-A		NINE
A-A(4)A		NINETEEN
A-A(4)A		NINETEENTH
A-A		NINETY
A-A		NINTH
A-A(7)A		NONCOMBATANT
A-A	OBTAI	NING
A-A	ORD	NANCE
A-A	PERMA	NENT
A-A	PLAN	NING
A-A	RAI	NING
A-A	REMAI	NING
A-A	RETUR	NING
A-A	RUN	NING
A-A	SCREE	NING
A-A	TRAI	NING
A-A(2)A	U	NKNOWN
A-A	AUT	OMOBILE
A-A	CHRON	OLOGICAL
A-A(1)A	CHR	ONOLOGICAL
A-A	C	OLON
A-A	C	OLONEL
A-A	C	OLORS
A-A	EC	ONOMIC
A-A	H	ONOR
A-A	LOC	OMOTIVE
A-A(1)A	L	OCOMOTIVE
A-A	LO	OKOUT

A-A	METEOR	OLOGICAL
A-A(1)A	METE	OROLOGICAL
A-A	MON	OPOLY
A-A(1)A	M	ONOPOLY
A-A	M	OTOR
A-A	M	OTORCYCLE
A-A	M	OTORIZED
A-A		OBOE
A-A	PH	OTOGRAPHY
A-A	PR	OMOTE
A-A(2)A	PR	OMOTION
A-A(3)A	PR	OPORTION
A-A	PR	OPOSALS
A-A	PR	OPOSE
A-A	PROT	OCOL
A-A(1)A	PR	OTOCOL
A-A	PR	OVOST
A-A	RIG	OROUS
A-A	SEMIC	OLON
A-A(2)A	T	OMORROW
A-A	T	OPOGRAPHIC
A-A	VIG	OROUS
A-A	NEWS	PAPER
A-A	NEWS	PAPERS
A-A		PIPE
A-A		POPULATED
A-A		POPULATION
A-A	AI	RCRAFT
A-A	AI	RDROME
A-A	ANTIAI	RCRAFT
A-A	ARBIT	RARY
A-A	CA	RTRIDGE
A-A	D	RYRUN
A-A	ENTE	RPRISE
A-A	ENTE	RPRISING
A-A	ER	ROR
A-A	FINGE	RPRINT
A-A	FO	RTRESS
A-A	INTE	RPRETATION
A-A(3)A	INTE	RPRETER
A-A	LIB	RARY
A-A	MIR	ROR
A-A	NEA	RER
A-A	SU	RPRISE
A-A	TER	ROR
A-A	ADDRES	SES
A-A	ANALY	SIS
A-AA	AS	SESSMENT
A-AA(4)A	AS	SESSMENTS
A-A	AS	SIST

~~CONFIDENTIAL~~

A-A	AS	SISTANT
A-A	AS	SISTANCE
A-A	CA	SES
A-A	CHAS	SIS
A-A	CRI	SIS
A-A	DEFEN	SES
A-A	DI	SASTER
A-A	EXERCI	SES
A-A	EXPEN	SES
A-A	CLAS	SES
A-A	HEAVYLOS	SES
A-A	LOS	SES
A-A	OUTPO	STS
A-A	PARENTHE	SES
A-A	PARENTHE	SIS
A-A	PAS	SES
A-A	PER	SISTENT
A-AA	POS	SESSION
A-A	PROTE	STS
A-A	PURPO	SES
A-A	RE	SIST
A-A	RE	SISTANCE
A-AA		SESSION
A-A	SUB	SISTENCE
A-A		SUSPECTED
A-A		SUSPEND
A-A		SUSPENDED
A-A(3)A		SUSPENSE
A-A(3)A		SUSPENSION
A-A		SUSPICION
A-A(6)A		SUSPICIONS
A-A(6)A		SUSPICIOUS
A-A		SYSTEM
A-A	WITNES	SES
A-A	AL	TITUDE
A-A	AN	TITANK
A-A	CI	TATION
A-A	COMPE	TITION
A-A	COMPU	TATION
A-A	CONSTI	TUTE
A-A	CONSTI	TUTING
A-A(1)A	CONS	TITUTING
A-A	CONSTI	TUTION
A-A(1)A	CONS	TITUTE
A-A(1)A	CONS	TITUTION
A-A	DESTI	TUTE
A-A(1)A	DES	TITUTE
A-A	DIC	TATED
A-A	DIC	TATOR
A-A	DIE	TITIAN

A-A	INSTI	TUTION
A-A(1)A	INS	TITUTION
A-A	INTERPRE	TATION
A-A	INVI	TATION
A-A	LA	TITUDE
A-A	LIMI	TATION
A-A	NECESSI	TATE
A-A	PAR	TITION
A-A	RADIOS	TATION
A-A	REINS	TATE
A-A(4)A	REINS	TATEMENT
A-A	REPRESEN	TATIVE
A-A	REPRESEN	TATIONS
A-A	SANI	TATION
A-A(4)A	S	TATEMENT
A-A	S	TATES
A-A	S	TATION
A-A	S	TATIONS
A-A(2)A	S	TATISTICS
A-A	S	TATUS
A-A	SUBSTI	TUTE
A-A	SUBSTI	TUTION
A-A(1)A	SUBS	TITUTE
A-A(1)A	SUBS	TITUTION
A-AA		TATTOO
A-A	TEN	TATIVE
A-A		TITLE
A-A		TOTAL
A-A		TOTALING
A-A	TRANSPOR	TATION
A-A	UNITEDS	TATES
A-A	WI	THTHE
A-A	A	UGUST
A-A	CONTIN	UOUS
A-A	F	UTURE
A-A	INA	UGURATION
A-A	UN	USUAL
A-A(1)A		UNUSUAL
A-A		USUAL
A-A	SUR	VIVED
A-A	A	WKWARD
A(2)A		ADJACENT
A(2)A		ADVANCING
A(2)A	ADV	ANTAGEOUS
A(2)A	ADV	ANTAGE
A(2)A(2)A		ADVANTAGE
A(2)A(2)A		ADVANTAGEOUS
A(2)A		ADVANCE
A(2)A		ADVANCED
A(2)A		AFFAIR

~~CONFIDENTIAL~~

A(2)A	AL	ASKA
A(2)A(1)A		ALMANAC
A(2)A		ALWAYS
A(2)A	AMB	ASSADOR
A(2)A(2)A		AMBASSADOR
A(2)A(1)A		APPARATUS
A(2)A		APPARENT
A(2)A		APPARENTLY
A(2)A	AR	ABIA
A(2)A		AREA
A(2)A		ARMAMENT
A(2)A		ARRANGE
A(2)A		ARRANGEMENT
A(2)A		ASIA
A(2)A		ASIATIC
A(2)A		ASSAULT
A(2)A		ATLANTIC
A(2)A		ATTACH
A(2)A		ATTACHMENT
A(2)A		ATTACK
A(2)A		ATTAIN
A(2)A		ATTAINMENT
A(2)A	AV	AILABLE
A(2)A		AVIATION
A(2)A		AVIATOR
A(2)A	B	AGGAGE
A(2)A	B	ARRACKS
A(2)A	B	ARRAGE
A(2)A	B	ATTALION
A(2)A	C	AMPAIGN
A(2)A	C	ANVAS
A(2)A	C	APTAIN
A(2)A	C	ASUAL
A(2)A	C	ASUALTIES
A(2)A	C	ASUALTY
A(2)A	CH	APLAIN
A(2)A	CO	ASTAL
A(2)A	COMM	ANDANT
A(2)A	COUNTER	ATTACK
A(2)A	DEB	ARKATION
A(2)A	DI	AGRAM
A(2)A	EMB	ARKATION
A(2)A	EV	ACUATE
A(2)A	EV	ACUATING
A(2)A	EV	ACUATION
A(2)A	EV	ALUATION
A(2)A	GR	ADUAL
A(2)A	INFL	AMMABLE
A(2)A	INST	ALLATIONS
A(2)A	INST	ANTANEOUS

A(2)A	J	ANUARY
A(2)A	M	ANDATE
A(2)A	M	ANDATED
A(2)A	M	ANGANESE
A(2)A	M	ANUAL
A(2)A	MEMOR	ANDA
A(2)A	NAVAL	ATTACK
A(2)A	NAV	ALBASE
A(2)A	NAV	ALBATTLE
A(2)A	P	ACKAGE
A(2)A	PAR	AGRAPH
A(2)A	PAR	ALLAX
A(2)A	P	ASSAGE
A(2)A	PRE	ARRANGED
A(2)A	R	ADIAL
A(2)A	R	ADIATE
A(2)A	R	ADIATION
A(2)A	RET	ALIATION
A(2)A	SE	APLANES
A(2)A	ST	ANDARD
A(2)A	ST	ANDARDS
A(2)A	TH	ATHAVE
A(2)A	TRANS	ATLANTIC
A(2)A(2)A	TR	ANSATLANTIC
A(2)A	V	ARIATION
A(2)A	VETERIN	ARIAN
A(2)A	W	ARFARE
A(2)A	WILL	ATTACK
A(2)A	ATOMIC	BOMB
A(2)A		BARBED
A(2)A		BOMB
A(2)A		BOMBARD
A(2)A		BOMBARDED
A(2)A		BOMBARDMENT
A(2)A		BOMBER
A(2)A		BRIBE
A(2)A		BRIBERY
A(2)A		BULB
A(2)A	DIVE	BOMBER
A(2)A	HEAVY	BOMBER
A(2)A	LIGHT	BOMBER
A(2)A	MEDIUM	BOMBER
A(2)A		CANCEL
A(2)A		CANCELLATION
A(2)A		CANCELLED
A(2)A		CHECK
A(2)A		CIRCLE
A(2)A		CIRCUIT
A(2)A		CIRCUITOUS
A(2)A		CIRCULAR

~~CONFIDENTIAL~~

A(2)A	CIRCULATE
A(2)A	CIRCULATION
A(2)A	CIRCUMSTANTIAL
A(2)A(6)A	CIRCUMSTANCES
A(2)A	CONCEAL
A(2)A	CONCEALMENT
A(2)A	CONCENTRATE
A(2)A	CONCENTRATING
A(2)A	CONCENTRATION
A(2)A	CONCERNING
A(2)A	CONCESSION
A(2)A	CONCILIATION
A(2)A	CONCLUDE
A(2)A	CONCLUSION
A(2)A	CONCRETE
A(2)A	EN CIRCLE
A(2)A	EN CIRCLING
A(2)A	IMPRA CTICABLE
A(2)A	PRA CTICAL
A(2)A	SE CRECY
A(2)A	SIGNIFI CANCE
A(2)A	TA CTICAL
A(2)A	TA CTICS
A(2)A	VA CANCY
A(2)A	HUN DRED
A(2)A	IN DEED
A(2)A	ONEHUN DRED
A(2)A	STAN DARD
A(2)A	STAN DARDS
A(2)A	ABS ENCE
A(2)A	ADDR ESSED
A(2)A	ADDR ESSES
A(2)A	AGR EEMENT
A(2)A	APP EARED
A(2)A	ARR ESTED
A(2)A	BATT ERIES
A(2)A	BATTL EFIELD
A(2)AA(1)A	BE ENNEEDED
A(2)A	BEENN EEDED
A(2)A	BE ETLE
A(2)A(1)A	B ESIEGED
A(2)A	B ETTER
A(2)AA	B ETWEEN
A(2)A	BR EEZE
A(2)A	CANC ELLED
A(2)A	C EASE
A(2)A	C ENTER
A(2)A(1)A	C ENTERED
A(2)A	C ENTERING
A(2)A	CHALL ENGE

A(2)A	CH EESE
A(2)A	CIGAR ETTE
A(2)A	COINCID ENCE
A(2)A	COMM ENCE
A(2)A(1)A	COMM ENCEMENT
A(2)A	COMM ERCE
A(2)A	COMP ELLED
A(2)A	COMPR ESSED
A(2)A	COND EMNED
A(2)A	COND ENSED
A(2)A	CONFER ENCE
A(2)A	CONF ERRED
A(2)A	CONFID ENCE
A(2)A	CONVAL ESCENT
A(2)A	CONV ENIENT
A(2)A	CORR ECTED
A(2)A	CORRESPOND ENCE
A(2)A	DEC EMBER
A(2)A	DECIPH ERMENT
A(2)A	DECR EASE
A(2)A	DECR EASED
A(2)A(2)A	D ECREASE
A(2)A(2)A	D ECREASED
A(2)AA	D ECREE
A(2)A	DEF EATED
A(2)A	DEF ENDER
A(2)A	DEF ENDED
A(2)A	DEF ENSE
A(2)A	DEF ENSES
A(2)A	DEF ERRED
A(2)AA	D EGREE
A(2)A	DEP ENDENT
A(2)A	D EPRESSION
A(2)A	DES ERTED
A(2)A	DES ERTER
A(2)A	DIFFER ENCE
A(2)A	DISAPP EARED
A(2)A	DIS EASE
A(2)A	DISINF ECTED
A(2)A	DISP ERSED
A(2)A	DISP ERSE
A(2)A	DISTR ESSED
A(2)A	EAGER
A(2)A	ECHELON
A(2)A(3)A	ECHELONED
A(2)A(4)A	ECHELONMENT
A(2)A	EDGE
A(2)A	EFFECT
A(2)A	EFF ECTED
A(2)A(2)A	EFFECTED

~~CONFIDENTIAL~~

A(2)A(4)A	EFFECTIVE
A(2)A(1)A ELS	EWHERE
A(2)A(2)A(1)A	ELSEWHERE
A(2)A EM	ERGENCY
A(2)A ENCIPH	ERMENT
A(2)A EN	EMIES
A(2)A ENT	ENTE
A(2)A(2)A	ENTENTE
A(2)A	ENTER
A(2)A	ENTERING
A(2)A	ENTERPRISING
A(2)A(5)A	ENTERPRISE
A(2)A(6)A	ENTERTAINMENT
A(2)A	ENVELOP
A(2)A(3)A	ENVELOPE
A(2)A	ETHER
A(2)A	EXCEPT
A(2)A	EXCESS
A(2)A(4)A	EXCESSIVE
A(2)A	EXPECT
A(2)A	EXPEDITING
A(2)A	EXPEDITION
A(2)A(3)A	EXPEDITE
A(2)A EXP	ELLED
A(2)A(2)A	EXPELLED
A(2)A	EXPEND
A(2)A EXP	ENDED
A(2)A(2)A	EXPENDED
A(2)A EXP	ENSES
A(2)A(2)A	EXPENSES
A(2)A(4)A	EXPENSIVE
A(2)A EXPERI	ENCE
A(2)A(2)A EXP	ERIENCE
A(2)A(2)A(2)A	EXPERIENCE
A(2)A(3)A	EXPERIMENT
A(2)A	EXTEND
A(2)A EXT	ENDED
A(2)A(2)A	EXTENDED
A(2)A	EXTENDING
A(2)A	EXTENSION
A(2)A(4)A	EXTENSIVE
A(2)A	EXTENT
A(2)A	EXTERIOR
A(2)A	EXTERMINATION
A(2)A(6)A	EXTERMINATE
A(2)A FI	ERCE
A(2)A GR	EASE
A(2)A HAV	EBEEN
A(2)A H	ELPER
A(2)A IMPR	ESSED
A(2)A INCID	ENCE
A(2)A INCOMPET	ENCE
A(2)A INCR	EASED
A(2)A INDEP	ENDENT
A(2)A INF	ECTED
A(2)A INFLU	ENCE
A(2)A INTELLIG	ENCE
A(2)A INT	ERCEPT
A(2)A INTERC	EPTED
A(2)A(2)A INT	ERCEPTED
A(2)A INTERFER	ENCE
A(2)A INT	ERFERING
A(2)A(1)A INT	ERFERE
A(2)A(1)A(2)A INT	ERFERENCE
A(2)A INT	ERMENT
A(2)A(4)A INT	ERMEDIATE
A(2)A INT	ERVENING
A(2)A(1)A INT	ERVENE
A(2)A INT	ERVENTION
A(2)A INV	ENTED
A(2)A K	EEPER
A(2)A L	EADER
A(2)A L	EAVE
A(2)A L	ETTER
A(2)A(1)A L	ETTERED
A(2)A LIC	ENSE
A(2)A LI	EUTENANT
A(2)A MAN	EUVER
A(2)A MAT	ERIEL
A(2)A M	EAGER
A(2)A M	EMBER
A(2)A MESS	ENGER
A(2)A(2)A M	ESSENGER
A(2)A N	EARER
A(2)A N	EAREST
A(2)A NEGLIG	ENCE
A(2)A NIN	ETEEN
A(2)A NIN	ETEENTH
A(2)A NORTHW	ESTERN
A(2)A NOV	EMBER
A(2)A OBS	ERVE
A(2)A OBS	ERVER
A(2)A OFF	ENDED
A(2)A OFF	ENSE
A(2)A OVERWH	ELMED
A(2)A PASS	ENGER
A(2)A PRECED	ENCE
A(2)A PREFER	ENCE
A(2)A PREF	ERRED
A(2)A PREPAR	EDNESS

~~CONFIDENTIAL~~

A(2)A	PRES ERVE
A(2)A	PR ESSED
A(2)A	PROC EEDED
A(2)A	PROT ECTED
A(2)A	PROT ESTED
A(2)A	REC EIVE
A(2)A	REC EIVER
A(2)A	RECOMM ENDED
A(2)A	R ECREATION
A(2)A	R ECREATIONAL
A(2)A	REFER ENCE
A(2)A	REJ ECTED
A(2)A	REL EASE
A(2)A	R ELIEF
A(2)A(1)A	R ELIEVE
A(2)A	REM EDIES
A(2)A	REM EMBER
A(2)A	REP EATED
A(2)A	REP EATER
A(2)A	REP ELLED
A(2)A(1)A	R EPRESENT
A(2)A(1)A	R EPRESENTATION
A(2)A(1)A(6)A	R EPRESENTATIVE
A(2)A	R EQUEST
A(2)A	REQU ESTED
A(2)A(2)A	R EQUESTED
A(2)A	RES ERVE
A(2)A	RES ERVES
A(2)A	R ESPECT
A(2)A	R ESPECTFULLY
A(2)A	R ESPECTS
A(2)A	R ETREAT
A(2)A	REV ENUE
A(2)A	REV ERSE
A(2)A	R EVIEW
A(2)A(1)A	R EVIEWED
A(2)A	R EVIEWING
A(2)A(1)A	S EALEVEL
A(2)A	S EAMEN
A(2)A	S ECRECY
A(2)A	S ECRETARY
A(2)A	S EIZE
A(2)A	SEL ECTED
A(2)A	SENT ENCE
A(2)A(2)A	S ENTENCE
A(2)A	SEPT EMBER
A(2)A(2)A	S EPTEMBER
A(2)A	S ERGEANT
A(2)AA	SEV ENTEEN
A(2)AA	SEV ENTEENTH
A(2)A	SH ELLED
A(2)A	SOUTHW ESTERN
A(2)A	ST EAMER
A(2)A	SUBSIST ENCE
A(2)A	SUCC EEDED
A(2)A	SURR ENDER
A(2)A(1)A	SURR ENDERED
A(2)A	SUSP ECTED
A(2)A	SUSP ENDED
A(2)A	SUSP ENSE
A(2)A(5)A	T EMPERATURE
A(2)A(1)A	THR EATENED
A(2)A	TRANSF ERRED
A(2)A	TRANSV ERSE
A(2)A	TRAV ERSE
A(2)A	TW ELVE
A(2)A	UNEXP ENDED
A(2)A(2)A	UN EXPENDED
A(2)A	V ESSEL
A(2)A	V ESSELS
A(2)A	W EDNESDAY
A(2)A	W ESTERLY
A(2)A	W ESTERN
A(2)A	WH ETHER
A(2)A	WITN ESSES
A(2)A	WR ECKED
A(2)A	Y ESTERDAY
A(2)A	BA GGAGE
A(2)A	DAMA GING
A(2)A	ENGA GING
A(2)A	FOR GING
A(2)A	GAUGE
A(2)A	GEOGRAPHIC
A(2)A	GEOGRAPHICAL
A(2)A	LAN GUAGE
A(2)A	NE GLIGENT
A(2)A	NE GLIGENCE
A(2)A	ZI GZAG
A(2)A	HIGH
A(2)A	HIGHER
A(2)A	HIGHEST
A(2)A	T HATHAVE
A(2)A	W HETHER
A(2)A	W HICH
A(2)A	ADM ISSION
A(2)A	A IRFIELD
A(2)A	AS IATIC
A(2)A	ASSOC IATION
A(2)A	AV IATION
A(2)A	BALL ISTIC

~~CONFIDENTIAL~~

A(2)A	BALL	ISTICS
A(2)A	BEG	INNING
A(2)A	B	INDING
A(2)A	BU	ILDING
A(2)A	CHARACTER	ISTIC
A(2)A	CO	INCIDENCE
A(2)A	COMM	ISSION
A(2)A	COMM	ISSIONER
A(2)A	CONCIL	IATION
A(2)A	CONSCR	IPTION
A(2)A	DESCR	IPTIVE
A(2)A	DESCR	IPTION
A(2)A(1)A	D	IETITIAN
A(2)A	D	IFFICULT
A(2)A(4)A	D	IFFICULTIES
A(2)A	DISC	IPLINE
A(2)A(2)A	D	ISCIPLINE
A(2)A	D	ISMISS
A(2)A	D	ISMISSAL
A(2)A	D	ISTILL
A(2)A(3)A	D	ISTINCTION
A(2)A	DISTINGU	ISHING
A(2)A(3)A	D	ISTINGUISH
A(2)A(3)A	D	ISTINGUISHED
A(2)A(3)A(2)A	D	ISTINGUISHING
A(2)A	DR	IFTING
A(2)A	ENL	ISTING
A(2)A	F	ILLING
A(2)A	F	INDING
A(2)A	F	ISHING
A(2)A	F	ITTING
A(2)A(1)A		IGNITION
A(2)A		ILLITERATE
A(2)A(4)A		IMMIGRATION
A(2)A		INCIDENCE
A(2)A		INCIDENT
A(2)A		INDICATE
A(2)A		INDICATED
A(2)A(3)A		INDICATING
A(2)A(3)A		INDICATION
A(2)A		INDIRECT
A(2)A(1)A		INDIVIDUAL
A(2)A	INFL	ICTING
A(2)A	INS	IGNIA
A(2)A(2)A		INSIGNIA
A(2)A	INTERD	ICTION
A(2)A(3)A		INVITATION
A(2)A(3)A		IRRIGATION
A(2)A	K	ILLING
A(2)A(1)A	L	IABILITY
A(2)A	L	IFTING
A(2)A	L	IQUID
A(2)A	LOG	ISTICS
A(2)A	M	IDNIGHT
A(2)A	M	ILLIMETER
A(2)A	M	ISFIRE
A(2)A	M	ISFIRES
A(2)A	M	ISSING
A(2)A	M	ISSION
A(2)A	M	ISSIONS
A(2)A	PATR	IOTIC
A(2)A	PERM	ISSION
A(2)A	PHIL	IPPINES
A(2)A	PR	INCIPAL
A(2)A	PR	INCIPLE
A(2)A	PR	INTING
A(2)A	PR	IORITY
A(2)A	RAD	IATION
A(2)A	REF	ILLING
A(2)A	RESTR	ICTION
A(2)A	RETAL	IATION
A(2)A	REV	IEWING
A(2)A	SH	IPPING
A(2)A(1)A	S	IGNIFICANT
A(2)A(1)A	S	IGNIFICANCE
A(2)A	S	IGNIFY
A(2)A	S	INKING
A(2)A	SK	IRMISH
A(2)A	STAT	ISTICS
A(2)A	SUBM	ISSION
A(2)A	SUPER	IORITY
A(2)A	SW	IMMING
A(2)A	TRANSM	ISSION
A(2)A	VAR	IATION
A(2)A	V	ICTIM
A(2)A	W	ILLIAM
A(2)A	W	ITHIN
A(2)A	AVAI	LABLE
A(2)A	FUE	LOIL
A(2)A	PARA	LLEL
A(2)A	COM	MITMENT
A(2)A		MAIM
A(2)A	MEDIU	MBOMBER
A(2)A	ABA	NDON
A(2)A	ADVA	NCING
A(2)A	AFTER	NOON
A(2)A	AN	NOUNCE
A(2)A(4)A	AN	NOUNCEMENT
A(2)AA	A	NTENNA
A(2)A	ASSIG	NMENT

~~CONFIDENTIAL~~

A(2)A	ASSIG NMENTS
A(2)A	ATTAI NMENT
A(2)A	BEGI NNING
A(2)A	BI NDING
A(2)A	COMMA NDANT
A(2)A	COMMA NDING
A(2)A	CO NCENTRATE
A(2)A(5)A	CO NCENTRATING
A(2)A(6)A	CO NCENTRATION
A(2)A	CO NDENSED
A(2)A	CO NFINE
A(2)A(3)A	CO NFINEMENT
A(2)A(1)A	CO NTINENTAL
A(2)A(2)A	CO NTINGENT
A(2)A	CONTI NGENT
A(2)A	CO NTINUAL
A(2)A	CO NTINUE
A(2)A	CO NTINUOUS
A(2)A(5)A	CO NTINUATION
A(2)A	CONVE NIENT
A(2)A(2)A	CO NVENIENT
A(2)A	CORRESPO NDENCE
A(2)A	CORRESPO NDING
A(2)A	DEPE NDENT
A(2)A	DISCONTI NUANCE
A(2)A	DISCO NTINUE
A(2)A(2)A	DISCO NTINUANCE
A(2)A	ECHELO NMENT
A(2)A	E NGINE
A(2)A	E NGINEER
A(2)A(4)A	E NGINEERING
A(2)A(5)A	E NTANGLEMENT
A(2)A	E NTENTE
A(2)A	ENTERTAI NMENT
A(2)A	EXTE NDING
A(2)A	FI NDING
A(2)A	FLA NKING
A(2)A	FORE NOON
A(2)A	GOVER NMENT
A(2)A	I NCENDIARY
A(2)A	I NCENTIVE
A(2)A	INDEPE NDENT
A(2)A	I NFANTRY
A(2)A	I NLAND
A(2)A	INSTA NTANEOUS
A(2)A	I NTEND
A(2)A	I NTENSIVE
A(2)A	I NTENT
A(2)A(3)A	I NTENTION
A(2)A	INTER NMENT
A(2)A	I NVENT
A(2)A	I NVENTED
A(2)A(3)A	I NVENTION
A(2)A	LA NDING
A(2)A(1)A	MAI NTENANCE
A(2)A	MA NGANESE
A(2)A	MA NNING
A(2)A	NOON
A(2)A	OPI NION
A(2)A	PAI NTING
A(2)A	PLA NNING
A(2)A	PO NTON
A(2)A	PRI NTING
A(2)A	QUARA NTINE
A(2)A	RU NNING
A(2)A	SE NTENCE
A(2)A	SE NTINEL
A(2)A	SI NKING
A(2)A	SU NKEN
A(2)A	U NION
A(2)A	UNK NOWN
A(2)A	U NTENABLE
A(2)A(4)A	ACC OMMODATION
A(2)A	AER ODROME
A(2)A	B OTTOM
A(2)A	B OYCOTT
A(2)A	C OMMON
A(2)A	C OMPOSED
A(2)A(4)A	C OMPOSITION
A(2)A(5)A	C ONFORMATION
A(2)A	C ONVOY
A(2)A	C ORPORAL
A(2)A(4)A	C ORPORATION
A(2)A	CUST OMHOUSE
A(2)A	D OCTOR
A(2)A	EN ORMOUS
A(2)A	EXPL OSION
A(2)A	EXPL OSIONS
A(2)A	F OGHORN
A(2)A	F OLLOW
A(2)A	FO OTHOLD
A(2)A	G ONIOMETER
A(2)A	GYR OSCOPIC
A(2)A	L OOKOUT
A(2)A	N ONCOMBATANT
A(2)A	OBSOLETE
A(2)A	OCTOBER
A(2)A	OPPOSE
A(2)A	OPPOSITE
A(2)A(4)A	OPPOSITION

~~CONFIDENTIAL~~

A(2)A	P OISON
A(2)A	P ONTON
A(2)AA	P ONTOON
A(2)A	P OSTOFFICE
A(2)A	PROM OTION
A(2)A	REC ONNOITER
A(2)A	REC ONNOITERING
A(2)A	SCHO OLHOUSE
A(2)A	TOM ORROW
A(2)A	VICT ORIOUS
A(2)A	AP PROPRIATE
A(2)A	IM PROPER
A(2)A	PREPARATION
A(2)A	PREPARE
A(2)A	PREPAREDNESS
A(2)A	PREPARING
A(2)A	PROPER
A(2)A	PROPORTION
A(2)A	PROPOSALS
A(2)A	PROPOSE
A(2)A	PUMP
A(2)A	PURPOSE
A(2)A	PURPOSES
A(2)A	AE RODROME
A(2)A	AI RBORNE
A(2)A	APP ROPRIATE
A(2)A	A RMOR
A(2)A(4)A	A RMOREDCAR
A(2)A	A RMORY
A(2)A	CAR RIER
A(2)A	CO RPORAL
A(2)A	CO RPORATION
A(2)A	COU RIER
A(2)A	DEPA RTURE
A(2)A	DESE RTER
A(2)A	DETE RIORATE
A(2)A	E RROR
A(2)A	EXTE RIOR
A(2)A(4)A	EXT RAORDINARY
A(2)A	FEB RUARY
A(2)A	FO RWARD
A(2)A	HA RBOR
A(2)A	HEADQUA RTERS
A(2)A	HYD ROGRAPHIC
A(2)A	INTE RFERE
A(2)A	INTE RFERENCE
A(2)A	INTE RFERING
A(2)A	INTE RIOR
A(2)A	MI RROR
A(2)A	MO RTAR
A(2)A	MU RDER
A(2)A	OBSE RVER
A(2)A	O RDER
A(2)A	O RDERED
A(2)A	O RDERS
A(2)A	PA RAGRAPH
A(2)A	PE RFORMANCE
A(2)A	P RAIRIE
A(2)AA	P REARRANGED
A(2)A	P RIOR
A(2)A	P RIORITY
A(2)A	P ROGRAM
A(2)A	P ROGRESS
A(2)A	P ROGRESSIVE
A(2)A	QUA RTER
A(2)A	QUA RTERS
A(2)A(5)A	QUA RTERMASTER
A(2)A	REAR
A(2)A(3)A	REARGUARD
A(2)A	RECO RDER
A(2)A	RECREATION
A(2)A	RECREATIONAL
A(2)A	RECRUIT
A(2)A	RECRUITING
A(2)A	REORGANIZATION
A(2)A	REPRESENT
A(2)A	REPRESENTATIVE
A(2)A	REPRESENTATION
A(2)A	REPRISAL
A(2)A	REPRISALS
A(2)A	RETREAT
A(2)A	RETROACTIVE
A(2)A	STA RTER
A(2)A	SUPE RIOR
A(2)A	SUPE RIORITY
A(2)A	TE RROR
A(2)A	WA RFARE
A(2)A	ADDRE SSES
A(2)AA	A SPOSSIBLE
A(2)A	AS SESSMENT
A(2)A	AS SESSMENTS
A(2)AA	A SSESSMENT
A(2)AA	A SSESSMENTS
A(2)A	AS SETS
A(2)A	A SSIST
A(2)A	A SSISTANT
A(2)A	A SSISTANCE
A(2)AA	CARELES SNESS
A(2)A	CEN SORSHIP
A(2)A	CHA SSIS

A(2)A	CRUI SERS
A(2)AA	DI SCUSS
A(2)AA	DI SCUSSED
A(2)AA	DI SCUSSION
A(2)A	DI SEASE
A(2)AA	DI SMISSAL
A(2)AA	DI SMISS
A(2)A	DI SPOSITION
A(2)A	EMBAS SIES
A(2)A	GLA SSES
A(2)A	HEAVYLO SSES
A(2)A	IS SUES
A(2)A	LO SSES
A(2)A	PA SSES
A(2)A	POS SESSION
A(2)AA	PO SSESSION
A(2)A	PROPO SALS
A(2)A	REPRI SALS
A(2)A	SESSION
A(2)A(1)A	SUBSISTENCE
A(2)A	SUBSTITUTE
A(2)A	SUBSTITUTION
A(2)A	SUNSET
A(2)AA	TRAN SMISSION
A(2)A	VES SELS
A(2)A	VI SITS
A(2)A	WITNE SSES
A(2)A	ADJU TANT
A(2)A	ADMINIS TRATIVE
A(2)A	ADMINIS TRATION
A(2)A	ARBI TRATION
A(2)A	ASSIS TANT
A(2)A	AT TENTION
A(2)A	CA TASTROPHE
A(2)A	CIRCUMS TANTIAL
A(2)A	COMBA TANT
A(2)A	CONCEN TRATE
A(2)A	CONCEN TRATING
A(2)A	CONCEN TRATION
A(2)A	CON TACT
A(2)A	DEMONS TRATE
A(2)A	DEMONS TRATED
A(2)A	DEMONS TRATION
A(2)A	DE TECTOR
A(2)A	DE TENTION
A(2)A	EN TENTE
A(2)A(6)A	EN TERTAINMENT
A(2)A	EX TENT
A(2)A	ILLUS TRATE
A(2)A	ILLUS TRATION
A(2)A	IMPOR TANT
A(2)A	INCOMPE TENT
A(2)A	INI TIATE
A(2)A	INS TANT
A(2)A	INS TANTANEOUS
A(2)A	INS TANTLY
A(2)A	IN TENT
A(2)A	IN TENTION
A(2)A	NONCOMBA TANT
A(2)A	OU TPUT
A(2)A	PENE TRATE
A(2)A	PENE TRATION
A(2)A	PERSIS TENT
A(2)A	PRO TECT
A(2)A	PRO TECTED
A(2)A	PRO TECTION
A(2)A	PRO TECTOR
A(2)A	PRO TEST
A(2)A	PRO TESTED
A(2)A	PRO TESTS
A(2)A	REGIS TRATION
A(2)A	RE TENTION
A(2)A	SI TUATION
A(2)A	S TART
A(2)A	S TARTER
A(2)A	STA TISTICS
A(2)A	S TRATEGIC
A(2)A	S TRATEGICAL
A(2)A	S TRATEGY
A(2)A	TACTICAL
A(2)A	TACTICS
A(2)A	TATTOO
A(2)A	TENT
A(2)A(1)A	TENTATIVE
A(2)A	TENTH
A(2)A	TEXT
A(2)A	THAT
A(2)A	THATHAVE
A(2)AA	THATTHE
A(2)A	TWEN TIETH
A(2)A	WA TERTANK
A(2)A	AGRIC ULTURAL
A(2)A	D UGOUT
A(2)A	O UTGUARD
A(2)A	O UTPUT
A(2)A	P URSUE
A(2)A	P URSUIT
A(2)A(6)A	UNSUCCESSFUL
A(2)A	UNSUITABLE
A(2)A	RE VOLVE

A(2)A	RE VOLVER
A(2)A	AN YWAY
A(2)A	ZIGZAG
A(3)A	ACTUALLY
A(3)A	ANIMAL
A(3)A	ANNUAL
A(3)A(4)A	ANTIAIRCRAFT
A(3)A	ANYWAY
A(3)A	APPEAR
A(3)A(1)A	APPEARANCE
A(3)A	APPEARED
A(3)A	AVERAGE
A(3)A	AWKWARD
A(3)A	C ANADA
A(3)A	C ARRIAGE
A(3)A	CENTR ALIZATION
A(3)A	CIRCUMST ANTIAL
A(3)A	DIS APPEAR
A(3)A	DIS APPEARED
A(3)A	E ASTWARD
A(3)A	EL ABORATE
A(3)A	ESTIM ATEDAT
A(3)A	EX AMINATION
A(3)A	GENER ALALARM
A(3)A	GENER ALSTAFF
A(3)A	HE ADQUARTERS
A(3)A	L ABORATORY
A(3)A	L ANGUAGE
A(3)A	M AINTAIN
A(3)A	M AINTAINED
A(3)A	M ANUFACTURE
A(3)A	M ARSHAL
A(3)A	M ARTIAL
A(3)A	N ATURAL
A(3)A	N ATURALIZE
A(3)A	NATUR ALIZATION
A(3)A(3)A	N ATURALIZATION
A(3)A	N AVIGATION
A(3)A	ORG ANIZATION
A(3)A	P ANAMA
A(3)A	R AILWAY
A(3)A	RE ARGUARD
A(3)A	RECONN AISSANCE
A(3)A	REORG ANIZATION
A(3)A	S ABOTAGE
A(3)A	S ANITARY
A(3)A	S ANITATION
A(3)A	SPE ARHEAD
A(3)A	TR ANSPACIFIC
A(3)A	CAPACITY
A(3)A	CHURCH
A(3)A(4)A	COINCIDENCE
A(3)A	CONSCRIPTION
A(3)A	COUNCIL
A(3)A	DEFI CIENCY
A(3)A	EFFI CIENCY
A(3)A	ELE CTRICITY
A(3)A	GYROS COPIC
A(3)A	INEFFI CIENCY
A(3)A	PA CIFIC
A(3)A	SPE CIFIC
A(3)A	SPE CIFICATION
A(3)A	TE CHNICAL
A(3)A	TRANSPA CIFIC
A(3)A	DECIDE
A(3)A(1)A	DECIDED
A(3)A	DECODE
A(3)A	DIVIDE
A(3)A	DIVIDING
A(3)A	HIN DERED
A(3)A	IN DIVIDUAL
A(3)A	MAN DATED
A(3)A	OR DERED
A(3)A	RE DUCED
A(3)A	SURREN DERED
A(3)A	WE DNESDAY
A(3)A	WIN DWARD
A(3)A	ASS EMBLE
A(3)A	ASS ESSMENT
A(3)A	ASS ESSMENTS
A(3)A	ATT EMPTED
A(3)A	AV ERAGE
A(3)AA(1)A	B EENNEEDED
A(3)A(1)A	BE ENNEEDED
A(3)A	B EETLE
A(3)A	B EFORE
A(3)A	B ETWEEN
A(3)A	CAREL ESSNESS
A(3)A	C EMETERY
A(3)A	COMPL ETENESS
A(3)A	CONC EALMENT
A(3)A	COOP ERATE
A(3)A	CORR ECTNESS
A(3)A	D ECIDE
A(3)A	D ECIDED
A(3)A	D ECODE
A(3)A	D ECREE
A(3)A	D EGREE
A(3)A	D ELAYED
A(3)A	D ELIVER

~~CONFIDENTIAL~~

A(3)A	DEV	ELOPE
A(3)A	DEV	ELOPED
A(3)A	D	EVICE
A(3)A	D	EVISE
A(3)A		EASTERLY
A(3)A		EASTERN
A(3)A	ECH	ELONED
A(3)A		EITHER
A(3)A		ELEMENT
A(3)A		ELEMENTARY
A(3)A	EL	EVATE
A(3)A		ELEVEN
A(3)A		ENTRENCH
A(3)A(3)A		ENTRENCHED
A(3)A	ENTR	ENCHED
A(3)A	ENV	ELOPE
A(3)A		ERASE
A(3)A		ERASER
A(3)A	EXP	EDITE
A(3)A	EXP	ERIMENT
A(3)A		EXPRESS
A(3)A(1)A		EXTREME
A(3)A	FUS	ELAGE
A(3)A	G	EORGE
A(3)A	GOV	ERNMENT
A(3)A	GR	ENADE
A(3)A	H	EAVIER
A(3)A	ILLIT	ERATE
A(3)A	IMP	EDIMENTA
A(3)A	INS	ECURE
A(3)A	INT	ERNMENT
A(3)A	INT	ERPRETATION
A(3)A(1)A	INT	ERPRETER
A(3)A	INT	ERVIEW
A(3)A	L	EAGUE
A(3)A	OP	ERATE
A(3)A(2)A	OV	ERWHELMED
A(3)A	PAR	ENTHESIS
A(3)A(1)A	PAR	ENTHESES
A(3)A	PR	ECEDE
A(3)A(2)A	PR	ECEDENCE
A(3)A(2)A	PR	EFERENCE
A(3)A	PR	EPARE
A(3)A(2)A	PR	EPAREDNESS
A(3)A	PR	ESIDENT
A(3)A	PR	ESIDENTIAL
A(3)A	PROC	EDURE
A(3)A	R	EACHED
A(3)A	R	ECOVER
A(3)A	R	EDUCE
A(3)A	R	EDUCED
A(3)A(2)A	R	EFERENCE
A(3)A	R	EFUGE
A(3)AA	R	EFUGEE
A(3)A	R	EFUSE
A(3)A	R	EGIMENTAL
A(3)A	R	EGIMENT
A(3)A	R	ESCUE
A(3)A	R	ESUME
A(3)A	R	ETIRE
A(3)A	SCH	EDULE
A(3)A	S	ECURE
A(3)A	S	ETTLE
A(3)A	SEV	ENTEEN
A(3)A	SEV	ENTEENTH
A(3)A	S	EVERE
A(3)AA	SMOK	ESCREEN
A(3)A	SP	EARHEAD
A(3)A	THER	EFORE
A(3)A	TW	ENTIETH
A(3)A	W	EATHER
A(3)A		GARAGE
A(3)A		GEORGE
A(3)A		GOING
A(3)A	C	HURCH
A(3)A	FLAS	HLIGHT
A(3)A	P	HOSPHORUS
A(3)A	SC	HOOLHOUSE
A(3)A	SEARC	HLIGHTS
A(3)A	T	HATTHE
A(3)A	T	HOUGH
A(3)A	ACT	IVITIES
A(3)A	ANTIC	IPATION
A(3)A	APPL	ICATION
A(3)A	ART	IFICIAL
A(3)A	AUD	IBILITY
A(3)A	BR	IGADIER
A(3)A	CENTRAL	IZATION
A(3)A	C	IRCUIT
A(3)A	C	IRCUITOUS
A(3)A	C	ITATION
A(3)A	CLASSIF	ICATION
A(3)A	COMMUN	ICATION
A(3)A	CONST	ITUTING
A(3)A	CONST	ITUTION
A(3)A	COORD	INATION
A(3)A	CR	ITICISE
A(3)A	DED	ICATION
A(3)A	DEF	INITION
A(3)A	DEMOBIL	IZATION

~~CONFIDENTIAL~~

A(3)A	DETERM	INATION
A(3)A	D	IMINISH
A(3)A	D	IRIGIBLE
A(3)A	DISSEM	INATION
A(3)A	DIST	INCTION
A(3)A	DIST	INGUISH
A(3)A	DIST	INGUISHED
A(3)A(2)A	DIST	INGUISHING
A(3)A	D	ISTRIBUTE
A(3)A	DISTR	IBUTING
A(3)A	DISTR	IBUTION
A(3)A(3)A	D	ISTRIBUTING
A(3)A(3)A	D	ISTRIBUTION
A(3)A	D	ISTRICT
A(3)A	D	ISTRICTS
A(3)A	D	IVIDING
A(3)A	D	IVISION
A(3)A	D	IVISIONS
A(3)A	DOM	INATION
A(3)A	ENC	IRCLING
A(3)A	EST	IMATION
A(3)A	EXAM	INATION
A(3)A	EXH	IBITION
A(3)A	EXTERM	INATION
A(3)A	EXT	INGUISH
A(3)A	FAC	ILITIES
A(3)A	F	IGHTING
A(3)A	HOST	ILITIES
A(3)A	IDENTIF	ICATION
A(3)A	ILLUM	INATING
A(3)A	ILLUM	INATION
A(3)A(1)A		INCLINING
A(3)A	IND	ICATING
A(3)A	IND	ICATION
A(3)A		INFLICT
A(3)A(2)A		INFLICTING
A(3)A		INITIATE
A(3)A		INQUIRE
A(3)A		INQUIRY
A(3)A	INSP	IRATION
A(3)A(3)A		INSPIRATION
A(3)A		INSPIRE
A(3)A	INST	ITUTION
A(3)A(3)A		INSTITUTION
A(3)A	INVEST	IGATION
A(3)A	INVEST	IGATIONS
A(3)A	INV	ITATION
A(3)A	IRR	IGATION
A(3)A		ISSUING
A(3)A	LIM	ITATION
A(3)A	L	IMITING
A(3)A	MA	INTAIN
A(3)A	MA	INTAINED
A(3)A	M	ILITIA
A(3)A	MOBIL	IZATION
A(3)A	NATURAL	IZATION
A(3)A	NAV	IGATION
A(3)A	ORGAN	IZATION
A(3)A	PRELIM	INARIES
A(3)A	QUALIF	ICATION
A(3)A	RECONNO	ITERING
A(3)A	REORGAN	IZATION
A(3)A	REQU	ISITION
A(3)A	RESPONS	IBILITY
A(3)A	R	ITICISM
A(3)A	SAN	ITATION
A(3)A	SEM	IRIGID
A(3)A	S	IGHTING
A(3)A	SIM	ILARITY
A(3)A	SPECIF	ICATION
A(3)A	SUBST	ITUTION
A(3)A(1)A	SU	ITABILITY
A(3)A	VERIF	ICATION
A(3)A	VETER	INARIAN
A(3)A	V	ICINITY
A(3)A	VIS	IBILITY
A(3)A(1)A	V	ISIBILITY
A(3)A	CO	LONEL
A(3)A	COMP	LETELY
A(3)A	F	LASHLIGHT
A(3)A	IL	LEGAL
A(3)A		LEVEL
A(3)A		LITTLE
A(3)A		LOCAL
A(3)A	SEA	LEVEL
A(3)A	A	MUSEMENT
A(3)A	CO	MMITMENT
A(3)A(1)A		MAXIMUM
A(3)A(1)A		MINIMUM
A(3)A		MOVEMENT
A(3)A	ALTER	NATING
A(3)A(4)A	A	NNOUNCEMENT
A(3)A	A	NTENNA
A(3)A	APPOI	NTMENT
A(3)A	ASCE	NSION
A(3)A	ATTE	NTION
A(3)A(1)A	CO	NCERNING
A(3)A	CO	NDEMN
A(3)A	CO	NDEMNED
A(3)A	CONFI	NEMENT

~~CONFIDENTIAL~~

A(3)A	CO NTAIN
A(3)A	DETE NTION
A(3)A	DIME NSION
A(3)A	E NCOUNTERED
A(3)A	E NTRENCH
A(3)A	E NTRENCHED
A(3)A	EXPA NSION
A(3)A	EXTE NSION
A(3)A	ILLUMI NATING
A(3)A	I NDEMNITY
A(3)A	I NSIGNIA
A(3)A	I NSTANT
A(3)A	I NSTANTLY
A(3)A(2)A	I NSTANTANEOUS
A(3)A	INTE NTION
A(3)A	I NTERNAL
A(3)A(4)A	I NTERNATIONAL
A(3)A(2)A	I NTERNMENT
A(3)A	INTERVE NTION
A(3)A	I NTRENCH
A(3)A	INVE NTION
A(3)A	LAU NCHING
A(3)A	MACHI NEGUN
A(3)A	MAI NTAIN
A(3)A	MAI NTAINED
A(3)A	MOU NTAIN
A(3)A	NOTING
A(3)A	O NEHUNDRED
A(3)A	PO NTOON
A(3)A	REAPPOI NTMENT
A(3)A	RETE NTION
A(3)A	SEVE NTEEN
A(3)A	SEVE NTEENTH
A(3)A	SUSPE NSION
A(3)A	U NIDENTIFIED
A(3)A	AIRC ONTROL
A(3)A	AN ONYMOUS
A(3)A	CHR ONOLOGICAL
A(3)AA	C ODEBOOK
A(3)A	C ONTROL
A(3)A	C ONTROVERSY
A(3)A	CR OSSROADS
A(3)A	FIREC ONTROL
A(3)A	F OOTHOLD
A(3)AA	F ORENOON
A(3)A	H ORIZON
A(3)A	LAB ORATORY
A(3)A	L OCOMOTIVE
A(3)A	METE OROLOGICAL
A(3)A	M ONOPOLY
A(3)A	OUTBOARD
A(3)A	OUTPOST
A(3)A	OUTPOSTS
A(3)A	PH OSPHORUS
A(3)A	P ONTOON
A(3)A	P OSTPONE
A(3)A	PROP ORTION
A(3)A	PR OTOCOL
A(3)A	A PPROPRIATE
A(3)A	PASSPORT
A(3)A	PHOSPHORUS
A(3)A	POSTPONE
A(3)A	PROMPT
A(3)A	TROO PSHIP
A(3)A	TROO PSHIPS
A(3)A	A RBITRATION
A(3)A	B RIBERY
A(3)A	CA RRIER
A(3)A	CONT ROVERSY
A(3)A	COR RIDOR
A(3)A	C ROSSROADS
A(3)A	DEST ROYERS
A(3)A	DEST ROYER
A(3)A	E RASER
A(3)A	FA RTHER
A(3)A	FU RTHER
A(3)A	IMP ROPER
A(3)A	INTERP RETER
A(3)A	LABO RATORY
A(3)A	NO RTHERN
A(3)A	NO RTHERLY
A(3)A	OPE RATOR
A(3)A	P REARRANGED
A(3)A	P REFER
A(3)A	P REFERENCE
A(3)AA	P REFERRED
A(3)A	P REPARATION
A(3)A	P REPARE
A(3)A	P REPAREDNESS
A(3)A	P REPARING
A(3)A	P RESCRIBED
A(3)A	P RESERVATION
A(3)A	P RESERVE
A(3)A	P RIMARY
A(3)A	P ROPER
A(3)A	P ROPORTION
A(3)A	RAILROAD
A(3)A	REA RGUARD
A(3)A	RECORD
A(3)A(2)A	RECORDER

~~CONFIDENTIAL~~

A(3)A	REDCROSS
A(3)A	REFER
A(3)A	REFERENCE
A(3)A	REGARDING
A(3)A	REPORT
A(3)A	REPORTED
A(3)A	RESERVATION
A(3)A	RESERVE
A(3)A	RESERVES
A(3)A	RESTRAINT
A(3)A	RESTRICTED
A(3)A	RESTRICTION
A(3)A	RETIRE
A(3)A	RETIRING
A(3)A	RETURN
A(3)A	RETURNED
A(3)A	RETURNING
A(3)A	REVERSE
A(3)A	RIGOROUS
A(3)A	RIVER
A(3)A	ROGER
A(3)A	SEC RETARY
A(3)A	TEMPE RATURE
A(3)A	TER RITORY
A(3)A	THE REFORE
A(3)A	T RAVERSE
A(3)A	VETE RINARIAN
A(3)A	A SCENSION
A(3)A	A SPOSSIBLE
A(3)A	A SSESSMENT
A(3)A(4)A	A SSESSMENTS
A(3)A	A SSETS
A(3)A	BALLI STICS
A(3)A	BATTLE SHIPS
A(3)AA	BU SINESS
A(3)AA	CARELE SSNESS
A(3)A	CARELES SNESS
A(3)A	COLLI SIONS
A(3)A	DI SCUSS
A(3)A	DI SCUSSED
A(3)A	DI SCUSSION
A(3)A	DI SMISSAL
A(3)A	DI SMISS
A(3)A	DI SPERSE
A(3)A	DI SPERSED
A(3)A	DI SPERSION
A(3)AA	DI STRESS
A(3)AA	DI STRESSED
A(3)A	DIVI SIONS
A(3)A	EMBA SSIES
A(3)A	EXPLO SIONS
A(3)A	I SSUES
A(3)A	LOGI STICS
A(3)A	MARK SMANSHIP
A(3)A	MES SAGES
A(3)A	MIS SIONS
A(3)A	PO SSESSION
A(3)A	PROVI SIONS
A(3)A	RE SPONSIBLE
A(3)A	RE SPONSIBILITY
A(3)A	SATISFACTORY
A(3)A	SATISFY
A(3)A	SHIPS
A(3)A	STATI STICS
A(3)AA	STRESS
A(3)A	SU SPENSE
A(3)A	SU SPENSION
A(3)A	TRAN SMISSION
A(3)A	TRAN SVERSE
A(3)A	TROOP SHIPS
A(3)AA	U SELESS
A(3)A	VE SSELS
A(3)A	WAR SHIPS
A(3)A	AC TIVITY
A(3)A	AC TIVITIES
A(3)A	ALLO TMENT
A(3)A	AN TEDATING
A(3)A	APPOIN TMENT
A(3)A	A TLANTIC
A(3)A	AT TEMPT
A(3)A	AT TEMPTED
A(3)A	A TTENTION
A(3)A	AU TOMATIC
A(3)A	COMMI TMENT
A(3)A	COMPAR TMENT
A(3)A	CONS TITUTE
A(3)A	CONS TITUTION
A(3)A	CONS TRUCTION
A(3)A	CON TRACT
A(3)AA	COUN TERATTACK
A(3)A	DEPAR TMENT
A(3)A	DEPAR TMENTAL
A(3)A	DES TITUTE
A(3)A	DES TRUCTION
A(3)A	DE TONATE
A(3)A	DE TONATED
A(3)A	DE TONATION
A(3)A	DIS TINCTION
A(3)A	DIS TRICT
A(3)A	DIS TRICTS

A(3)A	EIGH	TEENTH
A(3)A	ENLIS	TMENT
A(3)A	ES	TIMATE
A(3)A	ES	TIMATION
A(3)A	ESTIMA	TEDAT
A(3)A	ES	TIMATES
A(3)A(3)A	ES	TIMATEDAT
A(3)A	EX	TRACT
A(3)A	FA	TALITY
A(3)A	FIF	TEENTH
A(3)A	FOUR	TEENTH
A(3)A	HOS	TILITY
A(3)A	HOS	TILITIES
A(3)A	ILLI	TERATE
A(3)A	INS	TITUTION
A(3)A	INS	TRUCT
A(3)A	INS	TRUCTION
A(3)A	INS	TRUCTIONS
A(3)A	INS	TRUCTOR
A(3)A	INVES	TIGATE
A(3)A	INVES	TIGATION
A(3)A	INVES	TIGATIONS
A(3)A	NINE	TEENTH
A(3)A	OBS	TRUCTIONS
A(3)A	OU	TPOST
A(3)A	OU	TPOSTS
A(3)A	PA	TRIOTIC
A(3)A	REAPPOIN	TMENT
A(3)A	RECONS	TRUCTION
A(3)A	REENLIS	TMENT
A(3)A	RES	TRICTED
A(3)A	RES	TRICTION
A(3)A	RE	TREAT
A(3)A	SEVEN	TEENTH
A(3)A	SIX	TEENTH
A(3)A	S	TREET
A(3)A	SUBS	TITUTE
A(3)A	SUBS	TITUTION
A(3)A		TAXATION
A(3)A		THATTHE
A(3)A		THIRTEEN
A(3)A	THIR	TEENTH
A(3)A(3)A		THIRTEENTH
A(3)A		THIRTY
A(3)A		TRACT
A(3)A		TRACTOR
A(3)A	TRANSA	TLANTIC
A(3)A(2)A		TWENTIETH
A(3)A		TWENTY
A(3)A		TWENTYFIVE
A(3)A(1)A	UNI	TEDSTATES
A(3)A	U	TILITY
A(3)A	WARDEPAR	TMENT
A(3)A	WI	THOUT
A(3)A	B	UREAU
A(3)A	CHA	UFFEUR
A(3)A	CIRC	UITOUS
A(3)A	COMM	UNIQUE
A(3)A	S	URPLUS
A(3)A	S	URROUND
A(3)A		UNUSUAL
A(3)A		WESTWARD
A(3)A		WINDWARD
A(4)A		ADJUTANT
A(4)A		AERONAUTICS
A(4)A		AIRCRAFT
A(4)A		AIRPLANE
A(4)A		ALASKA
A(4)A		ALLOCATION
A(4)A		ALLOWANCE
A(4)A		ALMANAC
A(4)A		AMBULANCE
A(4)A		ANTEDATING
A(4)A	ANTI	AIRCRAFT
A(4)A		ANTITANK
A(4)A		APPARATUS
A(4)A		APPROACH
A(4)A		ARABIA
A(4)A		ARRIVAL
A(4)A		ASSURANCE
A(4)A		AUTOMATIC
A(4)A		AVAILABLE
A(4)A	BE	ACHHEAD
A(4)A	C	AUSEWAY
A(4)A	CO	ASTGUARD
A(4)A	GEOGR	APHICAL
A(4)A	IMPR	ACTICABLE
A(4)A	IN	AUGURATION
A(4)A	INTERN	ATIONAL
A(4)A	M	ARKSMANSHIP
A(4)A	M	ATERIAL
A(4)A	N	ATIONAL
A(4)A	N	ATIONALISM
A(4)A	N	ATIONALITY
A(4)A	N	AUTICAL
A(4)A	NAV	ALATTACK
A(4)A	N	AVALBASE
A(4)A	N	AVALBATTLE
A(4)A	P	ARAGRAPH
A(4)A	P	ARALLAX

A(4)A	PR ACTICAL
A(4)A	R AILHEAD
A(4)A	R AILROAD
A(4)A	RECRE ATIONAL
A(4)A	S ATISFACTORY
A(4)A	S ATURDAY
A(4)A	T ACTICAL
A(4)A	W ARDEPARTMENT
A(4)A	W ATERTANK
A(4)A	BLOCKBUSTER
A(4)A	CHARACTER
A(4)A(7)A	CHARACTERISTIC
A(4)A	CHEMICAL
A(4)A	CLERICAL
A(4)A	COIN CIDENCE
A(4)A	COLLECT
A(4)A	COLLECTION
A(4)A	CONDUCT
A(4)A	CONNECTING
A(4)A	CONNECTION
A(4)A	CONTACT
A(4)A	CORRECTED
A(4)A	CORRECTION
A(4)A	CORRECTNESS
A(4)A	CORRECT
A(4)A	CRITIC
A(4)A	CRITICAL
A(4)A	CRITICISE
A(4)A	IN CIDENCE
A(4)A	ME CHANIC
A(4)A	PRE CEDENCE
A(4)A	RE CEPTACLE
A(4)A	CRITICISM
A(4)A	CON DEMNED
A(4)A	CON DENSED
A(4)A	DEFEND
A(4)A	DEFENDER
A(4)A(1)A	DEFENDED
A(4)A(1)A	DEMANDED
A(4)A	DEPEND
A(4)A	DEPENDABLE
A(4)A	DEPENDABILITY
A(4)A	DEPENDENT
A(4)A	DISLODGE
A(4)A	DOWNED
A(4)A	IN DEPENDENT
A(4)A	ALT ERNATE
A(4)A	ASS EMBLIES
A(4)A	B EACHHEAD
A(4)A	B ECAUSE
A(4)A(1)A	B EENNEEDED
A(4)A(1)A	B ELLIGERENT
A(4)A	B ESIEGED
A(4)A	C ENTERED
A(4)A	COMM ENCEMENT
A(4)A	COMP ENSATE
A(4)A	CONF ERENCE
A(4)A	CONSID ERABLE
A(4)A	D ECEMBER
A(4)A	D ECIPHER
A(4)A(1)A	D ECIPHERED
A(4)A(2)A	D ECIPHERMENT
A(4)A	D ECLARE
A(4)A	D ECLARED
A(4)A	D EFEATED
A(4)A	DEF ECTIVE
A(4)A	D EFENDER
A(4)A	D EFENDED
A(4)A	D EFENSE
A(4)A	D EFENSES
A(4)A	DEF ENSIVE
A(4)A	D EFERRED
A(4)A	D EFICIENT
A(4)A	D EFICIENCY
A(4)A	D EMANDED
A(4)A	D EPARTED
A(4)A	D EPENDENT
A(4)A	D EPLOYED
A(4)A	D EPORTED
A(4)A	D ESERTED
A(4)A	D ESERTER
A(4)A	D ETACHED
A(4)A	DET ERMINE
A(4)A	DET ERMINED
A(4)A	DEV ELOPMENT
A(4)A	DIFF ERENCE
A(4)A	DIV EBOMBER
A(4)A	ECH ELONMENT
A(4)A	EFF ECTIVE
A(4)AA	EIGHTEEN
A(4)AA	EIGHTEENTH
A(4)A	ELS EWHERE
A(4)A	EMERGENCY
A(4)A	ENCODE
A(4)A	ENCODED
A(4)A	ENEMIES
A(4)A	ENGAGE
A(4)A(1)A	ENGAGEMENT
A(4)A	ENGINE
A(4)AA	ENGINEER

A(4)AA	ENGINEERING
A(4)A	ENTIRE
A(4)A	EUROPE
A(4)A	EUROPEAN
A(4)A	EXC ESSIVE
A(4)A	EXCITE
A(4)A(1)A	EXCITEMENT
A(4)A	EX ERCISE
A(4)A	EX ERCISES
A(4)A	EXP ENSIVE
A(4)A	EXT ENSIVE
A(4)A	FL EXIBLE
A(4)A	IMM EDIATE
A(4)A	IMPR ESSIVE
A(4)A	INC ENTIVE
A(4)A	INCOMP ETENCE
A(4)A	IND EPENDENT
A(4)A	INT ELLIGENT
A(4)A(2)A	INT ELLIGENCE
A(4)A	INT ENSIVE
A(4)A	INTERF ERENCE
A(4)A	INT ERFERE
A(4)A(2)A	INT ERFERENCE
A(4)A	INTERM EDIATE
A(4)A	INT ERPOSE
A(4)A	INT ERVENE
A(4)A	L ECTURE
A(4)A	L ETTERED
A(4)A	MAINT ENANCE
A(4)A(1)A	M EASUREMENT
A(4)A(1)A	M EASUREMENTS
A(4)A	M ESSAGE
A(4)A	M ESSAGES
A(4)A	MISC ELLANEOUS
A(4)A	N EGLIGENT
A(4)A(2)A	N EGLIGENCE
A(4)A	OBJ ECTIVE
A(4)A	OFF ENSIVE
A(4)A	PEN ETRATE
A(4)A	P ERMANENT
A(4)A	PREC EDENCE
A(4)A	PREF ERENCE
A(4)A	PR EFERRED
A(4)A	PR ESERVE
A(4)A	PR ESSURE
A(4)A	PROGR ESSIVE
A(4)A	RANG EFINDER
A(4)A	R EADINESS
A(4)A	R ECEIVE
A(4)A	R ECEIVER
A(4)A	R ECOMMEND
A(4)A	R ECOMMENDATION
A(4)A(2)A	R ECOMMENDED
A(4)A	R ECORDER
A(4)A	REF ERENCE
A(4)A	R EFUGEE
A(4)A	R EGISTER
A(4)A	R EJECTED
A(4)A	R ELEASE
A(4)A	R ELIEVE
A(4)A	R EMEDIES
A(4)A	R EMEMBER
A(4)A	R EPAIRED
A(4)A	R EPEATED
A(4)A	R EPEATER
A(4)A	R EPELLED
A(4)A	R EPLACE
A(4)A(1)A	R EPLACEMENT
A(4)A	R EPORTED
A(4)A	R EPRESENT
A(4)A	R EPRESENTATION
A(4)A(6)A	R EPRESENTATIVE
A(4)A	R EPULSED
A(4)A	R EQUIRE
A(4)A(1)A	R EQUIREMENT
A(4)A	R ESERVE
A(4)A	R ESERVES
A(4)A	R ESTORED
A(4)A	R ETURNED
A(4)A	R EVENUE
A(4)A	R EVERSE
A(4)A	R EVIEWED
A(4)A	R EVOLVE
A(4)A	R EVOLVER
A(4)A	S EALEVEL
A(4)A	S ELECTED
A(4)A	S ENTINEL
A(4)A	S ERVICE
A(4)AA	S EVENTEEN
A(4)AA	S EVENTEENTH
A(4)A	SMOK ESCREEN
A(4)A	SUCC ESSIVE
A(4)A	SURR ENDERED
A(4)A	TEL EPHONE
A(4)A(1)A	TH ERMOMETER
A(4)A	THR EATENED
A(4)A	UNT ENABLE
A(4)A	V EHICLES
A(4)A	FORTIFIED
A(4)A	EN GAGING

A(4)A	FI GHTING
A(4)A	SI GHTING
A(4)A	BREAKT HROUGH
A(4)A	S HARPSHOOTER
A(4)A	T HROUGH
A(4)A	ARB ITRATION
A(4)A	CONC ILIATION
A(4)A	CONF IDENTIAL
A(4)A	CONF IRMATION
A(4)A	CONF ISCATION
A(4)A	CONT INUATION
A(4)A	DES IGNATION
A(4)A	D IETITIAN
A(4)A	DIFF ICULTIES
A(4)A	D IMENSION
A(4)A	D IRECTION
A(4)A(1)A	D ISPOSITION
A(4)A	D ISSEMINATED
A(4)A(3)A	D ISSEMINATION
A(4)A	ENG INEERING
A(4)A	IDENTICAL
A(4)A	IDENTIFY
A(4)A(1)A(3)A	IDENTIFICATION
A(4)A	IGNITION
A(4)A	ILLUMINATE
A(4)A(3)A	ILLUMINATING
A(4)A(3)A	ILLUMINATION
A(4)A	IMMEDIATE
A(4)A	IMM IGRATION
A(4)A	IMPEDIMENTA
A(4)A	INDIVIDUAL
A(4)A(1)A	INEFFICIENCY
A(4)A	INHABITED
A(4)A	INTERIOR
A(4)A	INVADING
A(4)A	INVASION
A(4)A	LEG ISLATION
A(4)A	L IABILITY
A(4)A	NAT IONALISM
A(4)A	NAT IONALITY
A(4)A	PH ILIPPINES
A(4)A	PRES IDENTIAL
A(4)A	RES IGNATION
A(4)A	S IGNIFICANT
A(4)A	S IGNIFICANCE
A(4)A	S ITUATION
A(4)A(1)A	UN IDENTIFIED
A(4)A	V ICTORIOUS
A(4)A	AGRICU LTURAL
A(4)A	BATT LEFIELD
A(4)A	E LIGIBLE
A(4)A	F LEXIBLE
A(4)A	I LLEGAL
A(4)A	LEGISLATION
A(4)A	LIABILITY
A(4)A	NAVA LBATTLE
A(4)A	ATO MICBOMB
A(4)A	BO MBARDMENT
A(4)A	COM MENCEMENT
A(4)A	CO MPARTMENT
A(4)A	E MPLOYMENT
A(4)A	I MPEDIMENTA
A(4)A	MARKSMANSHIP
A(4)A	MEDIUM
A(4)A(2)A	MEDIUMBOMBER
A(4)A	MILLIMETER
A(4)A	AMMU NITION
A(4)A	ANNOU NCEMENT
A(4)A	A NTITANK
A(4)A	ARRA NGEMENT
A(4)A	CE NTERING
A(4)A	COI NCIDENCE
A(4)A	COMME NCEMENT
A(4)A	CO NFERENCE
A(4)A	CO NFIDENCE
A(4)A	CO NFIDENT
A(4)A	CO NFIDENTIAL
A(4)A	CON NECTING
A(4)A	CO NTINENTAL
A(4)A	COORDI NATION
A(4)A	DEFI NITION
A(4)A	DESIG NATION
A(4)A	DETERMI NATION
A(4)A	DETO NATION
A(4)A	DISSEMI NATION
A(4)A	DISTI NCTION
A(4)A	DOMI NATION
A(4)A	E NDURANCE
A(4)A	E NGAGING
A(4)A	ENGI NEERING
A(4)A	E NTERING
A(4)A	E NTRAIN
A(4)A	E NTRAINED
A(4)A	EXAMI NATION
A(4)A	EXPLA NATION
A(4)A	EXTERMI NATION
A(4)A	IG NITION
A(4)A	ILLUMI NATION
A(4)A	I NCIDENT
A(4)A	I NCIDENCE

A(4)A(2)A	I NDEPENDENT
A(4)A	I NFLUENCE
A(4)A	INTER NATIONAL
A(4)A	I NVADING
A(4)A	JU NCTION
A(4)A	MAI NTENANCE
A(4)A	MU NITIONS
A(4)A	NATIONALITY
A(4)A	NATIONAL
A(4)A	NATIONALISM
A(4)A	NI NETEEN
A(4)A	NI NETEENTH
A(4)A	NOTHING
A(4)A	RA NGEFINDER
A(4)A	RECOG NITION
A(4)A	RESIG NATION
A(4)A	ROADJU NCTION
A(4)A	SIG NALLING
A(4)A	SY NCHRONIZE
A(4)A	U NEXPENDED
A(4)A	U NKNOWN
A(4)A	VETERI NARIAN
A(4)A	ACCOMM ODATION
A(4)A	ALL OCATION
A(4)A	AT OMICBOMB
A(4)A	C ODEBOOK
A(4)A	COMP OSITION
A(4)A	CORP ORATION
A(4)A	C ORRIDOR
A(4)A	DEC ORATION
A(4)A	DET ONATION
A(4)A	DISP OSITION
A(4)A	F ORENOON
A(4)A	INTR ODUCTORY
A(4)A	L OCATION
A(4)A	OPINION
A(4)A	OPP OSITION
A(4)A	OVERCOMING
A(4)A	P OSITION
A(4)A	P OSITIONS
A(4)A	PR OJECTOR
A(4)A	PR OMOTION
A(4)A	PR OTECTOR
A(4)A	PR OVISION
A(4)A	PR OVISIONS
A(4)A	REV OLUTION
A(4)A	REV OLUTIONARY
A(4)A	T OBACCO
A(4)A	T OMORROW
A(4)A	T ORPEDO

A(4)AA	PHILIPPINES
A(4)A	TO POGRAPHIC
A(4)A	AI RCONTROL
A(4)A	ARMO REDCAR
A(4)A	CHA RACTER
A(4)A	CHA RACTERISTIC
A(4)A	CI RCULAR
A(4)A	CO RRIDOR
A(4)A	C RUISER
A(4)A	C RUISERS
A(4)A	DI RECTOR
A(4)A	EXTRAO RDINARY
A(4)A	FI REALARM
A(4)A	INST RUCTOR
A(4)A	NO RTHWARD
A(4)A	P REFERRED
A(4)A	P RESSURE
A(4)A	REPAIR
A(4)A	REPAIRED
A(4)A	REQUIRE
A(4)A	REQUIREMENT
A(4)A	REQUIRING
A(4)A	RESEARCH
A(4)A	RESOURCES
A(4)A	RESTORED
A(4)A	RUBBER
A(4)A	RUNNER
A(4)A	SUR RENDER
A(4)A	SUR RENDERED
A(4)A	TE RRITORY
A(4)A	T RACTOR
A(4)A	T RAILERS
A(4)A	T RAWLER
A(4)A	T RIGGER
A(4)A	WA RDEPARTMENT
A(4)A	ASSES SMENTS
A(4)A	AS SOONAS
A(4)A	BU SINESS
A(4)A	CARELE SSNESS
A(4)A	CROS SROADS
A(4)A	DI STRESS
A(4)A	DI STRESSED
A(4)A	I SLANDS
A(4)A	ME SSAGES
A(4)A	MI SFIRES
A(4)A	MI SSIONS
A(4)A	OUT SKIRTS
A(4)A	PRI SONERS
A(4)A	RE SERVES
A(4)A	RE SPECTS

~~CONFIDENTIAL~~

A(4)A	SHARPSHOOTER
A(4)A	SHELLS
A(4)A	SMOKESCREEN
A(4)A	SPOOLS
A(4)A	SPOONS
A(4)A	STATES
A(4)A(3)A	STATISTICS
A(4)A	STATUS
A(4)A	STRESS
A(4)A	STRIPS
A(4)AA	SUBMISSION
A(4)A	SUBSISTENCE
A(4)AA	SUCCESSIVE
A(4)AA	SUCCESS
A(4)AA	SUCCESSFUL
A(4)AA	SUCCESSFULLY
A(4)A	SUGGEST
A(4)A	SUNRISE
A(4)A	SUPPOSE
A(4)A	TRAN SPORTS
A(4)A	UNITED STATES
A(4)AA	UN SUCCESSFUL
A(4)A	U SELESS
A(4)A	AL TERNATING
A(4)A	AL TERNATE
A(4)A	A TTEMPT
A(4)A	A TTEMPTED
A(4)A	CHARAC TERISTIC
A(4)A	CON TINENTAL
A(4)A	CON TINUATION
A(4)A	COUN TERATTACK
A(4)A	DIS TRIBUTE
A(4)A	DIS TRIBUTION
A(4)A	DIS TRIBUTING
A(4)A	ELEC TRICITY
A(4)A	EXCI TEMENT
A(4)A	INS TALLATIONS
A(4)A	IN TEGRITY
A(4)A	IN TEREST
A(4)A	IN TERESTING
A(4)A	IN TERNATIONAL
A(4)A	LIEU TENANT
A(4)A	NOR THEAST
A(4)A	NOR THWEST
A(4)A	NOR THWESTERN
A(4)A	OU TSKIRTS
A(4)A	REINSTA TEMENT
A(4)A	RES TRAINT
A(4)A	RE TALIATION
A(4)A	RE TROACTIVE

A(4)A	SOU THEAST
A(4)A	SOU THWEST
A(4)A	SOU THWESTERN
A(4)A	STA TEMENT
A(4)A	S TATISTICS
A(4)A	TARGET
A(4)A	TENTATIVE
A(4)A	TERRITORY
A(4)A	THREAT
A(4)A	THREATENED
A(4)A	TRADITIONAL
A(4)A	TURRET
A(4)A	TWELFTH
A(4)A	L UMINOUS
A(4)A	MAN UFACTURE
A(5)A	ACCEPTANCE
A(5)A	ACCEPTABLE
A(5)A	ACCOMPANY
A(5)A	ACCORDANCE
A(5)A	ADVANTAGEOUS
A(5)A	ADVANTAGE
A(5)A	AEROPLANE
A(5)A	ALLEGIANCE
A(5)A	ALTERNATING
A(5)A	ALTERNATE
A(5)A	AMBASSADOR
A(5)A	AMERICAN
A(5)A	ANTENNA
A(5)A	APPEARANCE
A(5)A	APPLICATION
A(5)A	APPROVAL
A(5)A	ARBITRARY
A(5)A	ARBITRATION
A(5)A	ASSISTANT
A(5)A	ASSISTANCE
A(5)A	ASSOCIATE
A(5)A	ASSOCIATION
A(5)A	ASSOONAS
A(5)A	C ABLEGRAM
A(5)A	C AMOUFLAGE
A(5)A	C ANCELLATION
A(5)A	DIS APPEARANCE
A(5)A	EXTR AORDINARY
A(5)A	M AINTENANCE
A(5)A	QU ALIFICATION
A(5)A	QU ARTERMASTER
A(5)A	R ADIOGRAM
A(5)A	R ADIOSTATION
A(5)A	STR ATEGICAL
A(5)A	TR ANSATLANTIC

A(5)A	AC CEPTANCE
A(5)A	AC CORDANCE
A(5)A	CHRONICAL
A(5)A	COEFFICIENT
A(5)A	COMMENCE
A(5)A	COMMENCEMENT
A(5)A	COMMERCE
A(5)A	CONFISCATION
A(5)A	CONFLICT
A(5)A	CONTRACT
A(5)A	DIS CREPANCIES
A(5)A	DIS CREPANCY
A(5)A	E CONOMIC
A(5)A	AD DRESSED
A(5)A	A DVANCED
A(5)A	BRI DGEHEAD
A(5)A	DAMAGED
A(5)A	DECIDED
A(5)A	DELAYED
A(5)A	DROPPED
A(5)A	IN DICATED
A(5)A	ACC EPTANCE
A(5)A	ACC EPTABLE
A(5)A	ALL EGIANCE
A(5)A	APP EARANCE
A(5)A	CAR ELESSNESS
A(5)A	CL EARANCE
A(5)A	CO EFFICIENT
A(5)A	CONC ENTRATE
A(5)A(2)A	CORR ESPONDENCE
A(5)A	D ECREASE
A(5)A	D ECREASED
A(5)A	D EDICATE
A(5)A	D EFINITE
A(5)A	D EPARTMENT
A(5)A	D EPARTMENTAL
A(5)A	DEP ENDABLE
A(5)A	D EPLOYMENT
A(5)A	D ESCRIBE
A(5)A	D ESCRIBED
A(5)A	D ESTROYERS
A(5)A	D ESTROYED
A(5)A	D ESTROYER
A(5)A	D ETACHMENT
A(5)A	D ETONATE
A(5)A	D ETONATED
A(5)A	D ETRAINED
A(5)A	D EVELOPE
A(5)A	D EVELOPED
A(5)A	DISAPP EARANCE
A(5)A	DISCR EPANCIES
A(5)A	DISS EMINATED
A(5)A	EFFECTED
A(5)A	EFFICIENT
A(5)A	EFFICIENCY
A(5)A	EIGHTEEN
A(5)A	EIGHTEENTH
A(5)A	ELEVATE
A(5)A	ELSEWHERE
A(5)A(1)A	EMPLACEMENT
A(5)AA	EMPLOYEE
A(5)A	EMPLOYER
A(5)A(2)A	ENCIPHERMENT
A(5)A(1)A	ENCIPHERED
A(5)A	ENCIPHER
A(5)A(1)A	ENFORCEMENT
A(5)A	ENFORCE
A(5)A	ENGINEER
A(5)A	ENGINEERING
A(5)A	ENLISTED
A(5)A	ENROLLED
A(5)A	ENTENTE
A(5)A	ENT ERPRISE
A(5)A	EQUIPMENT
A(5)A	ESCORTED
A(5)A	EXCLUDE
A(5)A	EX ECUTIVE
A(5)A	EXPANDED
A(5)A	EXPELLED
A(5)A	EXPENDED
A(5)A	EXPENSES
A(5)A	EXP ERIENCE
A(5)A(2)A	EXPERIENCE
A(5)A	EXTENDED
A(5)A	EXTREME
A(5)A	FIGHT ERPLANE
A(5)A	IN EFFICIENCY
A(5)A	INT ERCEPTED
A(5)A	INT ERPRETER
A(5)A	INT ERRUPTED
A(5)A	J ETPLANE
A(5)A	M EDICINE
A(5)A	M ESSENGER
A(5)A	N EWSPAPER
A(5)A	N EWSPAPERS
A(5)A	ON EHUNDRED
A(5)A	PAR ENTHESES
A(5)A	P ERSISTENT
A(5)A	P ERSONNEL
A(5)A	PR EMATURE

~~CONFIDENTIAL~~

A(5)A	PR	ESCRIBED
A(5)A	QUART	ERMASTER
A(5)A	REC	EPTACLE
A(5)A(1)A	RE	ENFORCEMENT
A(5)A	RE	ENFORCE
A(5)A	RE	ENLISTED
A(5)A	R	EMAINDER
A(5)A	R	EQUESTED
A(5)A	R	ESOURCES
A(5)A	S	EABORNE
A(5)A	S	EAPLANES
A(5)A	S	ENTENCE
A(5)A	S	EPARATE
A(5)A	S	EPTEMBER
A(5)A	S	EVENTEEN
A(5)A	S	EVENTEENTH
A(5)A	SH	ELLFIRE
A(5)A	TEMP	ERATURE
A(5)A	T	ERRIBLE
A(5)A	TH	EREFORE
A(5)A	UN	EXPENDED
A(5)A	UNID	ENTIFIED
A(5)A	UNIT	EDSTATES
A(5)A	WARD	EPARTMENT
A(5)A	BE	GINNING
A(5)A		GASSING
A(5)A		GETTING
A(5)A	RE	GARDING
A(5)A	EIG	HTEENTH
A(5)A	ADMIN	ISTRATIVE
A(5)A	ADMIN	ISTRATION
A(5)A	ANT	ICIPATION
A(5)A	CLASS	IFICATION
A(5)A	CONS	IDERATION
A(5)A	DEMOB	ILIZATION
A(5)A	D	ISCIPLINE
A(5)A	D	ISCONTINUE
A(5)A	D	ISCONTINUANCE
A(5)A	D	ISCUSSION
A(5)A	D	ISPERSION
A(5)A	IDENT	IFICATION
A(5)A		IMPASSIBLE
A(5)A		IMPOSSIBLE
A(5)A		INCENDIARY
A(5)A		INCENTIVE
A(5)A		INCLINING
A(5)A		INCLUDING
A(5)A		INCLUSIVE
A(5)A		INDEMNITY
A(5)A		INFLATION

A(5)A		INSIGNIA
A(5)A		INTEGRITY
A(5)A		INTELLIGENCE
A(5)A		INTELLIGENT
A(5)A		INTENSIVE
A(5)A		INTENTION
A(5)A(2)A		INTERDICTION
A(5)A		INTERDICT
A(5)A		INTERVIEW
A(5)A		INVENTION
A(5)A(3)A		INVESTIGATION
A(5)A(3)A		INVESTIGATIONS
A(5)A		INVESTIGATE
A(5)A	L	IMITATION
A(5)A	MOB	ILIZATION
A(5)A	PREL	IMINARIES
A(5)A	QUAL	IFICATION
A(5)A	RAD	IOSTATION
A(5)A	REG	ISTRATION
A(5)A	S	IGNALLING
A(5)A	S	IMILARITY
A(5)A	SPEC	IFICATION
A(5)A	SU	ITABILITY
A(5)A	VER	IFICATION
A(5)A	V	ISIBILITY
A(5)A	CHRONO	LOGICAL
A(5)A	C	LERICAL
A(5)A	INF	LAMMABLE
A(5)A		LOGICAL
A(5)A	METEORO	LOGICAL
A(5)A	PO	LITICAL
A(5)A	CO	MMENCEMENT
A(5)A	E	MPLACEMENT
A(5)A	I	MPROVEMENT
A(5)A		MANAGEMENT
A(5)A		MARITIME
A(5)A		MAXIMUM
A(5)A		MINIMUM
A(5)A	REI	MBURSEMENT
A(5)A	COMME	NDATION
A(5)A	COMPE	NSATION
A(5)A	CONCE	NTRATING
A(5)A	CO	NCERNING
A(5)A	CO	NDITION
A(5)A	CO	NNECTING
A(5)A	CON	NECTION
A(5)A	CO	NTINGENT
A(5)A	CONTI	NUATION
A(5)A	CO	NTRABAND
A(5)A	CO	NVENIENT

A(5)A	DISCO NTINUANCE
A(5)A	E NEMYTANKS
A(5)A	E NLISTING
A(5)A	ENTA NGLEMENT
A(5)A	FOU NDATION
A(5)A	I NCLINING
A(5)A	I NCLUDING
A(5)A	I NTERMENT
A(5)A(3)A	I NTERVENTION
A(5)A(1)A	I NTERVENING
A(5)A	I NTERVENE
A(5)A	I NVASION
A(5)A	MA NAGEMENT
A(5)A	RECOMME NDATION
A(5)A	RECON NAISSANCE
A(5)A	REPRESE NTATION
A(5)A	SIG NIFICANCE
A(5)A	SIG NIFICANT
A(5)A	TRA NSATLANTIC
A(5)A	ASS OCIATION
A(5)A	C OALITION
A(5)A	C OLLISION
A(5)A	C OLLISIONS
A(5)A	C ONDITION
A(5)A	CONF ORMATION
A(5)A	C ONTINUOUS
A(5)A	C ORRESPONDENCE
A(5)A	C ORRESPONDING
A(5)A	F ORMATION
A(5)A	INF ORMATION
A(5)A	INTR ODUCTION
A(5)A	OPERATOR
A(5)A	PR OPORTION
A(5)A	PR OTECTION
A(5)A	RADI OSTATION
A(5)A	REC OGNITION
A(5)A	TRANSP ORTATION
A(5)A	PHILIPPINES
A(5)A	PRINCIPAL
A(5)A	PRINCIPLE
A(5)A	AI RSUPPORT
A(5)A	A RBITRARY
A(5)A	A RTILLERY
A(5)A	BA ROMETER
A(5)A	B REAKTHROUGH
A(5)A	FI RECONTROL
A(5)A	GENE RALALARM
A(5)A	GY ROMETER
A(5)A	HYD ROMETER
A(5)A	HYG ROMETER

A(5)A	INTE RPRETER
A(5)A	IR REGULAR
A(5)A	IR REGULARITIES
A(5)A	IR REGULARITY
A(5)A	P REMATURE
A(5)A	P RISONER
A(5)A	P RISONERS
A(5)A	P ROCEDURE
A(5)A	PSYCH ROMETER
A(5)A	QUARTE RMASTER
A(5)A	RADIOGRAM
A(5)A	RECOVER
A(5)A	REENFORCE
A(5)A	REENFORCEMENT
A(5)A	REGISTRATION
A(5)A	REGULAR
A(5)A	REIMBURSEMENT
A(5)A	REINFORCE
A(5)A	REINFORCEMENT
A(5)A	ST RAGGLER
A(5)A	SU RRENDER
A(5)A	SU RRENDERED
A(5)AA	T RANSFERRED
A(5)AA	T RANSFERRING
A(5)A	T RANSFER
A(5)A	T RANSPORT
A(5)A	T RANSPORTATION
A(5)A	T RANSPORTS
A(5)A	T RANSVERSE
A(5)A	ASSE SSMENTS
A(5)A	A SSOONAS
A(5)A	CIRCUM STANCES
A(5)A	CRO SSROADS
A(5)A	DI STRICTS
A(5)A	E STABLISH
A(5)A	E STABLISHED
A(5)A	E STABLISHMENT
A(5)A	NEW SPAPERS
A(5)A	PHO SPHORUS
A(5)A	PO SITIONS
A(5)A	RE SOURCES
A(5)A	SAILORS
A(5)A	SECTORS
A(5)A	SERIOUSLY
A(5)A	SKIRMISH
A(5)A	SUBMISSION
A(5)A	SUCCESSIVE
A(5)A	SUCCESS
A(5)A	SUCCESSFUL
A(5)A	SUCCESSFULLY

A(5)A	SURPLUS
A(5)A	SURPRISE
A(5)A	SUSPENSE
A(5)A	SUSPENSION
A(5)A	UN SUCCESSFUL
A(5)A	AN TICIPATE
A(5)A	AN TICIPATION
A(5)A	CER TIFICATE
A(5)A	CON TINGENT
A(5)A	IDEN TIFICATION
A(5)A	INS TRUMENT
A(5)A	INS TRUMENTS
A(5)A	IN TERCEPT
A(5)A	IN TERCEPTED
A(5)A	IN TERDICT
A(5)A	IN TERDICTION
A(5)A	IN TERMENT
A(5)A(1)A	IN TERPRETATION
A(5)A	IN TERPRETER
A(5)A	IN TERRUPT
A(5)A	IN TERRUPTED
A(5)A	IN TERRUPTION
A(5)A	IN TERVENTION
A(5)A	IN TRODUCTION
A(5)A	IN TRODUCTORY
A(5)A	QUAR TERMASTER
A(5)A	SA TISFACTORY
A(5)A	SUI TABILITY
A(5)A	TONIGHT
A(5)A	TRAJECTORY
A(5)A(3)A	TRANSATLANTIC
A(5)A	UNI TEDSTATES
A(5)A	S UBSTITUTE
A(5)A	S UBSTITUTION
A(6)A	ANTICIPATE
A(6)A	ANTICIPATION
A(6)A	CL ASSIFICATION
A(6)A	DEP ARTMENTAL
A(6)A	TR ADITIONAL
A(6)A	TR ANSPORTATION
A(6)A	A CCEPTANCE
A(6)A	A CCORDANCE
A(6)A	CERTIFICATE
A(6)A	CIR CUMSTANCES
A(6)A	CLEARANCE
A(6)A	COMMUNICATE
A(6)A	COMMUNICATION
A(6)A	CONSTRUCTION
A(6)A	RE CONSTRUCTION
A(6)A	A DDRESSED
A(6)A	DECLARED
A(6)A	DEFEATED
A(6)A	DEFENDED
A(6)A	DEFERRED
A(6)A	DEMANDED
A(6)A	DEPARTED
A(6)A	DEPLOYED
A(6)A	DEPORTED
A(6)A	DESERTED
A(6)A	DETACHED
A(6)A	DICTATED
A(6)A	DISARMED
A(6)A	UN DERSTAND
A(6)A	UN DERSTOOD
A(6)A	A ERODROME
A(6)A	A EROPLANE
A(6)A	B EENNEEDED
A(6)A	B ELLIGERENT
A(6)A	D ECIPHERED
A(6)A	D EFECTIVE
A(6)A	D EFENSIVE
A(6)A	D EPARTURE
A(6)A	D ESIGNATE
A(6)A	D ESIGNATED
A(6)A	D ESPATCHES
A(6)A	D ESPATCHED
A(6)A	D ESTITUTE
A(6)A	DET ERIORATE
A(6)A	D ETERMINE
A(6)A	D ETERMINED
A(6)A	D EVELOPMENT
A(6)A	ECHELONED
A(6)A	ELIGIBLE
A(6)A	EMBASSIES
A(6)A	EMPLOYEE
A(6)A	EMPLOYMENT
A(6)A	ENCIRCLE
A(6)A(1)A	ENCOUNTERED
A(6)A	EN EMYPLANES
A(6)A	ENFILADE
A(6)A	ENGAGEMENT
A(6)A	ENLISTMENT
A(6)A	ENROLLMENT
A(6)A(1)A	ENTANGLEMENT
A(6)A	ENT ERTAINMENT
A(6)A	ENTRAINED
A(6)A	ENVELOPE
A(6)A	EQUALIZE
A(6)A	EQUIPAGE
A(6)A	EQUIVALENT

A(6)A	ESTIMATE
A(6)A	ESTIMATEDAT
A(6)A	ESTIMATES
A(6)A	EVACUATE
A(6)A	EXCAVATE
A(6)A	EXCHANGE
A(6)A	EXCITEMENT
A(6)A	EXERCISE
A(6)A	EXERCISES
A(6)A	EXHIBITED
A(6)A	EXPEDITE
A(6)A	EXPERIMENT
A(6)A	EXT ERMINATE
A(6)A	INDET ERMINATE
A(6)A	INV ESTIGATE
A(6)A	M EASUREMENT
A(6)A	M EASUREMENTS
A(6)A	M ECHANIZED
A(6)A	NEC ESSITATE
A(6)A	OV ERWHELMED
A(6)A	P ENETRATE
A(6)A	PR EARRANGED
A(6)A	PR ECEDENCE
A(6)A	PR EFERENCE
A(6)A	PR EPAREDNESS
A(6)A	R ECOGNIZE
A(6)A	R EENFORCE
A(6)A(1)A	R EENFORCEMENT
A(6)A	R EENLISTED
A(6)A	RE ENLISTMENT
A(6)A	R EFERENCE
A(6)A(1)A	R EIMBURSEMENT
A(6)A(1)A	R EINFORCEMENT
A(6)A	R EINFORCE
A(6)A(1)A	R EINSTATEMENT
A(6)A	R EINSTATE
A(6)A	R EPLACEMENT
A(6)A	REPRES ENTATIVE
A(6)A	R EQUIREMENT
A(6)A	R ESTRICTED
A(6)A	SEV ENTYFIVE
A(6)A	T ECHNIQUE
A(6)A	T ELEPHONE
A(6)A	T ENTATIVE
A(6)A	TH ERMOMETER
A(6)A	TW ENTYFIVE
A(6)A	DISTIN GUISHING
A(6)A	GROUPING
A(6)A	GUARDING
A(6)A	SI GNALLING

A(6)A	C IRCULATION
A(6)A	D IPLOMATIC
A(6)A	D ISORGANIZED
A(6)A	D ISPOSITION
A(6)A	D ISTINCTION
A(6)A	D ISTINGUISH
A(6)A	D ISTINGUISHED
A(6)A(2)A	D ISTINGUISHING
A(6)A	DIST INGUISHING
A(6)A	F INGERPRINT
A(6)A(3)A	IDENTIFICATION
A(6)A	IMPRACTICABLE
A(6)A	IMPRESSION
A(6)A	IMPRESSIVE
A(6)A	INDICATING
A(6)A	INDICATION
A(6)A	INEFFICIENCY
A(6)A	INFLICTING
A(6)A	INSECURITY
A(6)A	INSPECTION
A(6)A	INVITATION
A(6)A	IRRIGATION
A(6)A	UN IDENTIFIED
A(6)A	W ITHDRAWING
A(6)A	MEASUREMENT
A(6)A	MEASUREMENTS
A(6)A	ME MORANDUM
A(6)A	A NTEDATING
A(6)A	COMMU NICATION
A(6)A	CO NCEALMENT
A(6)A	CONCE NTRATION
A(6)A	CO NCESSION
A(6)A	CO NCLUSION
A(6)A	CO NFESSION
A(6)A	CO NFINEMENT
A(6)A	CO NNECTION
A(6)A	DISTI NGUISHING
A(6)A	E NCIRCLING
A(6)A	E NEMYPLANES
A(6)A	E NLISTMENT
A(6)A	E NROLLMENT
A(6)A(2)A	E NTERTAINMENT
A(6)A	E NTRUCKING
A(6)A	FI NGERPRINT
A(6)A	I NDICATING
A(6)A	I NFLATION
A(6)A	I NFLICTING
A(6)A	I NSTANTANEOUS
A(6)A	I NSTRUMENT
A(6)A	I NSTRUMENTS

A(6)A	I NTENTION
A(6)A	I NTERNMENT
A(6)A	I NVENTION
A(6)A	NEGLIGENT
A(6)A	NEGLIGENCE
A(6)A	NINETEEN
A(6)A	NINETEENTH
A(6)A	NORTHERN
A(6)A	NUMBERING
A(6)A	ORGA NIZATION
A(6)A	RECO NNAISSANCE
A(6)A	RECON NOITERING
A(6)A	REE NLISTMENT
A(6)A	REORGA NIZATION
A(6)A	SA NITATION
A(6)A	TRA NSFERRING
A(6)A	U NDERSTAND
A(6)A	C OLLECTION
A(6)A	C OMMISSION
A(6)A	C OMMISSIONER
A(6)A	C ONCESSION
A(6)A	C ONCLUSION
A(6)A	C ONFESSION
A(6)A	C ONNECTION
A(6)A	CO OPERATION
A(6)A	C ORRECTION
A(6)A	D OMINATION
A(6)A	F OUNDATION
A(6)A	OBJECTION
A(6)A	OPERATION
A(6)A	P OPULATION
A(6)A	P OSSESSION
A(6)A	PARAGRAPH
A(6)A	AG RICULTURAL
A(6)A	B RIGADIER
A(6)A	INT RODUCTORY
A(6)A	I RREGULAR
A(6)A	I RREGULARITIES
A(6)A	I RREGULARITY
A(6)A	P ROJECTOR
A(6)A	P ROTECTOR
A(6)A	REARGUARD
A(6)A	RECEIVER
A(6)A	RECONSTRUCTION
A(6)A	RECORDER
A(6)A	REGISTER
A(6)A	REJECTOR
A(6)A	REMEMBER
A(6)A	REPEATER
A(6)A	REVOLVER
A(6)A	THE RMOMETER
A(6)A	T RAJECTORY
A(6)A	T RANSFERRED
A(6)A	T RANSFERRING
A(6)A	AS SEMBLIES
A(6)A	CA SUALTIES
A(6)A	CU STOMHOUSE
A(6)A	DE SPATCHES
A(6)A	DE STROYERS
A(6)A	DI SPATCHES
A(6)A	DI STINGUISH
A(6)A	DI STINGUISHED
A(6)A	DI STINGUISHING
A(6)A	E STIMATES
A(6)A	SOLDIERS
A(6)A	SOUTHEAST
A(6)A	SOUTHWEST
A(6)A	SOUTHWESTERN
A(6)A	STATIONS
A(6)A	SUPPLIES
A(6)A	SU SPICIONS
A(6)A	SU SPICIOUS
A(6)A	AT TACHMENT
A(6)A	AT TAINMENT
A(6)A	CEN TRALIZATION
A(6)A	DE TACHMENT
A(6)A	DE TERIORATE
A(6)A	DE TERMINATION
A(6)A	ENTER TAINMENT
A(6)A	EX TERMINATE
A(6)A	EX TERMINATION
A(6)A	INDE TERMINATE
A(6)A	IN TERNMENT
A(6)A	NA TIONALITY
A(6)A	REINS TATEMENT
A(6)A	S TATEMENT
A(6)A	TEMPERATURE
A(6)A	TWENTIETH
A(6)A	C USTOMHOUSE
A(6)A	SIM ULTANEOUS
A(6)A	S UCCESSFUL
A(6)A	S UCCESSFULLY
A(6)A	S USPICIOUS
A(6)A	UNS UCCESSFUL
A(6)A	SE VENTYFIVE
A(6)A	WITHDRAW
A(6)A	WITHDRAWAL
A(6)A	WITHDRAWING
A(6)A	WITHDREW
A(7)A	ACCIDENTAL

~~CONFIDENTIAL~~

A(7)A	ACCOMMODATION
A(7)A	ADDITIONAL
A(7)A	APPROPRIATE
A(7)A	APPROXIMATE
A(7)A	ARMOREDCAR
A(7)A	ARTIFICIAL
A(7)A	N ATURALIZATION
A(7)A	CHARA CTERISTIC
A(7)A	CLASSIFICATION
A(7)A	CONFERENCE
A(7)A	CONFIDENCE
A(7)A	CONSPIRACY
A(7)A	CONVALESCENT
A(7)A	IN COMPETENCE
A(7)A	DECREASED
A(7)A	DESCRIBED
A(7)A	DESTROYED
A(7)A	DETONATED
A(7)A	DETRAINED
A(7)A	DEVELOPED
A(7)A	DISCUSSED
A(7)A	DISPERSED
A(7)A	DOMINATED
A(7)A	UNI DENTIFIED
A(7)A	C ENTRALIZE
A(7)A	DEC ENTRALIZE
A(7)A	DEC ENTRALIZED
A(7)A	D ECIPHERMENT
A(7)A	D EMOBILIZE
A(7)A	D EPENDABLE
A(7)A	ECHELONMENT
A(7)A	EFFECTIVE
A(7)A	ELABORATE
A(7)A	EMPLACEMENT
A(7)A	ENCIPHERED
A(7)A	ENDURANCE
A(7)A	ENFORCEMENT
A(7)A	ENTRENCHED
A(7)A	EXCESSIVE
A(7)A	EXCLUSIVE
A(7)A	EXECUTIVE
A(7)A	EXPANSIVE
A(7)A	EXPENSIVE
A(7)A	EXPLOSIVE
A(7)A	EXTENSIVE
A(7)A	H EADQUARTERS
A(7)A	H EAVYBOMBER
A(7)A	H EAVYLOSSES
A(7)A	INT ELLIGENCE
A(7)A	INT ERMEDIATE

A(7)A	N EGLIGENCE
A(7)A	R EAPPOINTED
A(7)A	R ECEPTACLE
A(7)A	R ECOMMENDED
A(7)A	R ECONNOITER
A(7)A	R ECONNOITERING
A(7)A	RE ENFORCEMENT
A(7)A	R EENLISTMENT
A(7)A	R ESISTANCE
A(7)A	EN GINEERING
A(7)A	P HOTOGRAPHY
A(7)A	T HIRTEENTH
A(7)A	ADM INISTRATIVE
A(7)A	ADM INISTRATION
A(7)A	D IFFICULTIES
A(7)A	D ISTRIBUTING
A(7)A	D ISTRIBUTION
A(7)A	IMMIGRATION
A(7)A	INDETERMINATE
A(7)A	INFORMATION
A(7)A	INSPIRATION
A(7)A	INSTITUTION
A(7)A	INSTRUCTION
A(7)A	INSTRUCTIONS
A(7)A	INTERESTING
A(7)A	INTERFERING
A(7)A	INTERMEDIATE
A(7)A	INTERNATIONAL
A(7)A	INTERVENING
A(7)A	MECHANISM
A(7)A	MEDIUMBOMBER
A(7)A	AN NOUNCEMENT
A(7)A	CO NGRESSIONAL
A(7)A	CO NSTITUTING
A(7)A	CO NSUMPTION
A(7)A	CO NVALESCENT
A(7)A	DEMO NSTRATION
A(7)A	E NFORCEMENT
A(7)A	E NGINEERING
A(7)A	I NCOMPETENT
A(7)A	I NCOMPETENCE
A(7)A	I NDEPENDENT
A(7)A	I NDETERMINATE
A(7)A	I NDICATION
A(7)A	I NEFFICIENCY
A(7)A	I NSPECTION
A(7)A	I NTELLIGENCE
A(7)A	I NTELLIGENT
A(7)A	I NTERESTING
A(7)A	I NTERFERENCE

~~CONFIDENTIAL~~

A(7)A	I NTERFERING
A(7)A	I NTERVENING
A(7)A	I NVITATION
A(7)A	NO NCOMBATANT
A(7)A	PE NETRATION
A(7)A	RECO NNOITERING
A(7)A	REE NFORCEMENT
A(7)A	REI NFORCEMENT
A(7)A	REI NSTATEMENT
A(7)A	TRA NSMISSION
A(7)A	ACC OMMODATION
A(7)A	C OMPETITION
A(7)A	C OMPOSITION
A(7)A	C OMPUTATION
A(7)A	C ONGRESSIONAL
A(7)A	C ONSUMPTION
A(7)A	C OOPERATION
A(7)A	CO ORDINATION
A(7)A	C ORPORATION
A(7)A	DEM ONSTRATION
A(7)A	OCCUPATION
A(7)A	OPPOSITION
A(7)A	PR OCLAMATION
A(7)A	PHOTOGRAPHY
A(7)A	A RMOREDCAR
A(7)A	EXT RAORDINARY
A(7)A	NO RTHWESTERN
A(7)A	P RELIMINARIES
A(7)A	P RELIMINARY
A(7)A	REMAINDER
A(7)A	SHA RPSHOOTER
A(7)A	A SSEMBLIES
A(7)A	AS SESSMENTS
A(7)A	AS SIGNMENTS
A(7)A	HO STILITIES
A(7)A	IN STRUMENTS
A(7)A	MEA SUREMENTS
A(7)A	SEAPLANES
A(7)A	STANDARDS
A(7)A	A TTACHMENT
A(7)A	A TTAINMENT
A(7)A	ES TIMATEDAT
A(7)A	IN TELLIGENT
A(7)A	IN TERMEDIATE
A(7)A	IN TERPRETATION
A(7)A	NA TURALIZATION
A(7)A	THERMOMETER
A(7)A	THIRTEENTH
A(7)A(1)A	TRANSPORTATION
A(7)A	TRANSPORT
A(7)A	TRANSPORTS
A(7)A	YESTERDAY
A(8)A	ADMINISTRATIVE
A(8)A	ADMINISTRATION
A(8)A	ANTIAIRCRAFT
A(8)A	COINCIDENCE
A(8)A	DIS CONTINUANCE
A(8)A	DECIPHERED
A(8)A	DESIGNATED
A(8)A	DESPATCHED
A(8)A	DETERMINED
A(8)A	DISPATCHED
A(8)A	DISTRESSED
A(8)A	C ERTIFICATE
A(8)A	CORR ESPONDENCE
A(8)A	D EMONSTRATE
A(8)A	D EMONSTRATED
A(8)A	D ESCRIPTIVE
A(8)A	D ETERIORATE
A(8)A	ENCIPHERMENT
A(8)A	ENCOUNTERED
A(8)A	ENEMYPLANES
A(8)A	ENTANGLEMENT
A(8)A	ENTERPRISE
A(8)A	ESTABLISHED
A(8)A	IND ETERMINATE
A(8)A	IRR EGULARITIES
A(8)A	M EDIUMBOMBER
A(8)A	N ECESSITATE
A(8)A	P ERFORMANCE
A(8)A	PR ELIMINARIES
A(8)A	R EAPPOINTMENT
A(8)A	R EENFORCEMENT
A(8)A	R EIMBURSEMENT
A(8)A	R EINFORCEMENT
A(8)A	R EINSTATEMENT
A(8)A	REPR ESENTATIVE
A(8)A	R ESPONSIBLE
A(8)A	R ETROACTIVE
A(8)A	S EVENTYFIVE
A(8)A	T EMPERATURE
A(8)A	HYDROGRAPHIC
A(8)A	D ISCREPANCIES
A(8)A	ILLUSTRATION
A(8)A	INAUGURATION
A(8)A	INSTALLATIONS
A(8)A	INTERDICTION
A(8)A	INTERRUPTION
A(8)A	INTERVENTION
A(8)A	INTRODUCTION

~~CONFIDENTIAL~~

(7)A	I NTERFERING
(7)A	I NTERVENING
(7)A	I NVITATION
(7)A	NO NCOMBATANT
(7)A	PE NETRATION
(7)A	RECO NNOITERING
(7)A	REE NFORCEMENT
(7)A	REI NFORCEMENT
(7)A	REI NSTATEMENT
(7)A	TRA NSMISSION
(7)A	ACC OMMODATION
(7)A	C OMPETITION
(7)A	C OMPOSITION
(7)A	C OMPUTATION
(7)A	C ONGRESSIONAL
(7)A	C ONSUMPTION
(7)A	C OOPERATION
(7)A	CO ORDINATION
(7)A	C ORPORATION
(7)A	DEM ONSTRATION
(7)A	OCCUPATION
(7)A	OPPOSITION
(7)A	PR OCLAMATION
(7)A	PHOTOGRAPHY
(7)A	A RMOREDCAR
(7)A	EXT RAORDINARY
(7)A	NO RTHWESTERN
(7)A	P RELIMINARIES
(7)A	P RELIMINARY
(7)A	REMAINDER
(7)A	SHA RPSHOOTER
(7)A	A SSEMBLIES
(7)A	AS SESSMENTS
(7)A	AS SIGNMENTS
(7)A	HO STILITIES
(7)A	IN STRUMENTS
(7)A	MEA SUREMENTS
(7)A	SEAPLANES
(7)A	STANDARDS
(7)A	A TTACHMENT
(7)A	A TTAINMENT
(7)A	ES TIMATEDAT
(7)A	IN TELLIGENT
(7)A	IN TERMEDIATE
(7)A	IN TERPRETATION
(7)A	NA TURALIZATION
(7)A	THERMOMETER
(7)A	THIRTEENTH
(7)A(1)A	TRANSPORTATION
(7)A	TRANSPORT

A(7)A	TRANSPORTS
A(7)A	YESTERDAY
A(8)A	ADMINISTRATIVE
A(8)A	ADMINISTRATION
A(8)A	ANTIAIRCRAFT
A(8)A	COINCIDENCE
A(8)A	DIS CONTINUANCE
A(8)A	DECIPHERED
A(8)A	DESIGNATED
A(8)A	DESPATCHED
A(8)A	DETERMINED
A(8)A	DISPATCHED
A(8)A	DISTRESSED
A(8)A	C ERTIFICATE
A(8)A	CORR ESPONDENCE
A(8)A	D EMONSTRATE
A(8)A	D EMONSTRATED
A(8)A	D ESCRIPTIVE
A(8)A	D ETERIORATE
A(8)A	ENCIPHERMENT
A(8)A	ENCOUNTERED
A(8)A	ENEMYPLANES
A(8)A	ENTANGLEMENT
A(8)A	ENTERPRISE
A(8)A	ESTABLISHED
A(8)A	IND ETERMINATE
A(8)A	IRR EGULARITIES
A(8)A	M EDIUMBOMBER
A(8)A	N ECESSITATE
A(8)A	P ERFORMANCE
A(8)A	PR ELIMINARIES
A(8)A	R EAPPOINTMENT
A(8)A	R EENFORCEMENT
A(8)A	R EIMBURSEMENT
A(8)A	R EINFORCEMENT
A(8)A	R EINSTATEMENT
A(8)A	REPR ESENTATIVE
A(8)A	R ESPONSIBLE
A(8)A	R ETROACTIVE
A(8)A	S EVENTYFIVE
A(8)A	T EMPERATURE
A(8)A	HYDROGRAPHIC
A(8)A	D ISCREPANCIES
A(8)A	ILLUSTRATION
A(8)A	INAUGURATION
A(8)A	INSTALLATIONS
A(8)A	INTERDICTION
A(8)A	INTERRUPTION
A(8)A	INTERVENTION
A(8)A	INTRODUCTION

A(9)A	TRANSPORTATION	A(10)A	NORTHWESTERN
A(9)A	UNSUCCESSFUL	A(10)A	REVOLUTIONARY
A(10)A	COUNTERATTACK	A(10)A	SEARCHLIGHTS
A(10)A	DEMONSTRATED	A(10)A	SIMULTANEOUS
A(10)A	DISORGANIZED	A(11)A	CORRESPONDENCE
A(10)A	DISSEMINATED	A(11)A	DECENTRALIZED
A(10)A	INTERPRETATION	A(11)A	DISTINGUISHED
A(10)A	IRREGULARITIES	A(11)A	R ECONNAISSANCE
A(10)A	CE NTRALIZATION	A(11)A	I NTERPRETATION
A(10)A	I NVESTIGATION	A(12)A	NATURALIZATION
A(10)A	I NVESTIGATIONS		

~~CONFIDENTIAL~~