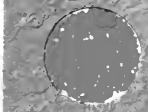
UB
290
H5



UC-NRLF

$B 72 551

YC 62994

MANUAL FOR THE SOLUTION OF MILITARY CIPHERS

BY

PARKER HITT

Captain of Infantry, U. S. A.

PRESS OF
THE ARMY SERVICE SCHOOLS
Fort Leavenworth, Kansas

1916

UB 29
H5

MANUAL FOR THE SOLUTION OF MILITARY CIPHERS

BY

PARKER HITT

Captain of Infantry, United States Army

Introduction

THE history of war teems with occasions where the interception of dispatches and orders written in plain language has resulted in defeat and disaster for the force whose intentions thus became known at once to the enemy. For this reason, prudent generals have used cipher and code messages from time immemorial. The necessity for exact expression of ideas practically excludes the use of codes for military work although it is possible that a special tactical code might be useful for preparation of tactical orders.

It is necessary therefore to fall back on ciphers for general military work if secrecy of communication is to be fairly well assured. It may as well be stated here that no practicable military cipher is mathematically indecipherable if intercepted; the most that can be expected is to delay for a longer or shorter time the deciphering of the message by the interceptor.

The capture of messengers is no longer the only means available to the enemy for gaining information as to the plans of a commander. All radio messages sent out can be copied at hostile stations within radio range. If the enemy can get a fine wire within one hundred feet of a buzzer line or within thirty feet of a telegraph line, the message can be copied by induction. Messages passing over commercial telegraph lines, and even over military lines, can be copied by spies in the offices. On telegraph lines of a permanent nature it is possible to install high speed automatic sending and receiving machines and thus prevent surreptitious copying of messages, but nothing but a secure cipher will serve with other means of communication.

M150947

It is not alone the body of the message which should be in cipher. It is equally important that, during transmission, the preamble, place from, date, address and signature be enciphered; but this should be done by the sending operator and these parts must, of course, be deciphered by the receiving operator before delivery. A special operators' cipher should be used for this purpose but it is difficult to prescribe one that would be simple enough for the average operator, fast and yet reasonably safe. Some form of rotary cipher machine would seem to be best suited for this special purpose.

It is unnecessary to point out that a cipher which can be deciphered by the enemy in a few hours is worse than useless. It requires a surprisingly long time to encipher and decipher a message, using even the simplest kind of cipher, and errors in transmission of cipher matter by wire or radio are unfortunately too common.

Kerckhoffs has stated that a military cipher should fulfill the following requirements:

1st. The system should be materially, if not mathematically, indecipherable.

2d. It should cause no inconvenience if the apparatus and methods fall into the hands of the enemy.

3d. The key should be such that it could be communicated and remembered without the necessity of written notes and should be changeable at the will of the correspondents.

4th. The system should be applicable to telegraphic correspondence.

5th. The apparatus should be easily carried and a single person should be able to operate it.

6th. Finally, in view of the circumstances under which it must be used, the system should be an easy one to operate, demanding neither mental strain nor knowledge of a long series of rules.

A brief consideration of these six conditions must lead to the conclusion that there is no perfect military cipher. The first requirement is the one most often overlooked by those prescribing the use of any given cipher and, even if not overlooked, the indecipherability of any cipher likely to be used for military purposes is usually vastly overestimated by those prescribing the use of it.

If this were not true, there would have been neither material for, nor purpose in, the preparation of these notes. Of the hundreds of actual cipher messages examined by the writer, at least nine-tenths have been solved by the methods to be set forth. These messages were prepared by the methods in use by the United States Army, the various Mex-

ican armies and their secret agents, and by other methods in common use. The usual failure has been with very short messages. Foreign works consulted lead to the belief that many European powers have used, for military purposes, cipher methods which vary from an extreme simplicity to a complexity which is more apparent than real. What effect recent events have had on this matter remains to be seen. It is enough that the cipher experts of practically every European country have appealed to the military authorities of their respective countries time and again to do away with these useless ciphers and to adopt something which offers more security, even at the expense of other considerations.

The cipher of the amateur, or of the non-expert who makes one up for some special purpose, is almost sure to fall into one of the classes whose solution is an easy matter. The human mind works along the same lines, in spite of an attempt at originality on the part of the individual, and this is particularly true of cipher work because there are so few sources of information available. In other words, the average man, when he sits down to evolve a cipher, has nothing to improve upon; he invents and there is no one to tell him that his invention is, in principle, hundreds of years old. The ciphers of the Abbé Tritheme, 1499, are the basis of most of the modern substitution ciphers.

In view of these facts, no message should be considered indecipherable. Very short messages are often very difficult and may easily be entirely beyond the possibility of analysis and solution, but it is surprising what can be done, at times, with a message of only a few words.

In the event of active operations, cipher experts will be in demand at once. Like all other experts, the cipher expert is not born or made in a day; and it is only constant work with ciphers, combined with a thorough knowledge of their underlying principles, that will make one worthy of the name.

Digitized by the Internet Archive
in 2007 with funding from
Microsoft Corporation

http://www.archive.org/details/manualforsolutio00hittrich

Chapter I

Equipment for Cipher Work

SUCCESS in dealing with unknown ciphers is measured by these four things in the order named; perseverance, careful methods of analysis, intuition, luck. The ability at least to read the language of the original text is very desirable but not essential.

Cipher work will have little permanent attraction for one who expects results at once, without labor, for there is a vast amount of purely routine labor in the preparation of frequency tables, the rearrangement of ciphers for examination, and the trial and fitting of letter to letter before the message begins to appear.

The methods of analysis given in these notes cover only the simpler varieties of cipher and it is, of course, impossible to enumerate all the varieties of these. It is believed that the methods laid down are sound and several years of successful work along this line would seem to confirm this belief. For more advanced work there is no recourse but to study the European authorities whose writings are mostly in French, German, and Italian and, unfortunately, are rarely available in English translations.

Under intuition must be included a knowledge of the general situation and, if possible, the special situation which led to the sending of the cipher message. The knowledge or guess that a certain cipher messages contains a particular word, often leads to its solution.

As to luck, there is the old miner's proverb: "Gold is where you find it."

The equipment for an office, where much cipher work is handled, will now be considered. The casual worker with ciphers can get along with much less, but the methods of filing and keeping a record of all messages studied should be followed wherever possible. The interchange of results between individuals and between offices should be encouraged and, in time of active operations, should be mandatory. An enemy may be using the same cipher in widely separated parts of the zone of operations and it is useless labor to have many cipher offices working on intercepted messages, all in the same cipher, when one office may have the solution that will apply to all of them.

Cipher work requires concentration and quiet and often must proceed without regard to hours. The office should be chosen with these points in mind. A clerical force is desirable and even necessary if there is much work to do. The clerk or clerks can soon be trained to do the routine part of the analysis.

It is believed that each Field Army should have such an office where all ciphers intercepted by forces under command of the Field Army Commander should be sent at once for examination. This work naturally falls to the Intelligence section of the General Staff at this headquarters. A special radio station, with receiving instruments only, should be an adjunct to this office and its function should be to copy all hostile radio messages whether in cipher or plain text. Such a radio station requires but a small antenna; one of the pack set type or any amateur's antenna is sufficient, and the station instruments can be easily carried in a suit case. Three thoroughly competent operators should be

provided, so that the station can be "listening in" during the entire twenty-four hours.

The office should be provided with tables of frequency of the language of the enemy, covering single letters and digraphs; a dictionary and grammar of that language; copies of the War Department Code, Western Union Code and any other available ones; types of apparatus or, at least, data on apparatus and cipher methods in use by the enemy; and a safe filing cabinet and card index for filing messages examined. A typewriter is also desirable.

The office work on a cipher under examination should be done on paper of a standard and uniform size. Printed forms containing twenty-six ruled lines and a vertical alphabet are convenient and save time in preparation of frequency tables. Any new cipher methods which are found to be in use by the enemy should, when solved, be communicated to all similar offices in the Army for their information.

Unless an enemy were exceedingly vigilant and changed keys and methods frequently, such an office would, in a few days, be in a position to disclose completely all intercepted cipher communications of the enemy with practically no delay.

Chapter II

Principles of Mechanism of a Written Language

WITH a few exceptions, notably Chinese, all modern languages are constructed of words which in turn are formed from letters. In any given language the number of letters, and their conventional order is fixed. Thus English is written with 26 letters and their conventional order is A, B, C, D, E, etc. Some letters are used very frequently and others rarely. In fact, if ten thousand consecutive letters of a text be counted and the frequency of occurrence of each letter be noted, the numbers found will be practically identical with those obtained from any other text of ten thousand letters in the same language. The relative proportion of occurrence of the various letters will also hold approximately for even very short texts.

Such a count of a large number of letters, when it is put in the form of a table, is known as a frequency table. Every language has its own distinctive frequency table and, for any given language, the frequency table is almost as fixed as the alphabet. There are minor differences in frequency tables prepared from texts on special subjects. For example, if the text be newspaper matter, the frequency table will differ slightly from one prepared from military orders and will also differ slightly from one prepared from telegraph messages. But these differences are very slight as compared with the differences between the frequency tables of two different languages.

Again there is a fixed ratio of occurrence of

every letter with every other for any language and this, put in table form, constitutes a table of frequency of digraphs. In the same way a table of trigraphs, showing the ratio of occurrence of any three letters in sequence, could be prepared, but such a table would be very extensive and a count of the more common three letter combinations is usually used.

Other tables, such as frequency of initial and final letters of words, might be of value but the common practice is to put cipher text into groups of five or ten letters each and eliminate word forms. This is almost a necessity in telegraphic and radio communication to enable the receiving operator to check correct receipt of a message. He must get five letters, neither more nor less, per word or he is sure a mistake has been made. There is little difficulty, as a rule, in restoring word forms in the deciphered message.

We will now take up, in order, the various frequency tables and linguistic peculiarities of English and Spanish. Frequency tables for French, German, and Italian for single letters will follow. All frequency tables have been re-calculated from at least ten thousand letters of text and compared with existing tables. No marked difference has been found in any case between the re-calculated tables and those already in use.

Data for Solution of Ciphers in English

TABLE I.—Normal frequency table. Frequency for ten thousand letters and for two hundred letters. This latter is put in graphic form and is necessarily an approximation. Taken from military orders and reports, English text.

	10,000 Letters		*200 Letters*
A	778	16	1111111111111111
B	141	3	111
C	296	6	111111
D	402	8	11111111
E	1277	26	11111111111111111111111111
F	197	4	1111
G	174	3	111
H	595	12	111111111111
I	667	13	1111111111111
J	51	1	1
K	74	2	11
L	372	7	1111111
M	288	6	111111
N	686	14	11111111111111
O	807	16	1111111111111111
P	223	4	1111
Q	8		
R	651	13	1111111111111
S	622	12	111111111111
T	855	17	11111111111111111
U	308	6	111111
V	112	2	11
W	176	3	111
X	27		
Y	196	4	1111
Z	17		

Vowels AEIOU=38.37%; consonants LNRST=31.86%; consonants JKQXZ=1.77%.

The vowels may be safely taken as 40%, consonants LNRST as 30% and consonants JKQXZ as 2%.

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

TABLE II.—Frequency table for telegraph messages, English text. This table varies slightly from the standard frequency table because the common word "the" is rarely used in telegrams and there is a tendency to use longer and less common words in preparing telegraph messages.

	10,000 Letters		*200 Letters*
A	813	16	1111111111111111
B	149	3	111
C	306	6	111111
D	417	8	11111111
E	1319	26	11111111111111111111111111
F	205	4	1111
G	201	4	1111
H	386	8	11111111
I	711	14	11111111111111
J	42	1	1
K	88	2	11
L	392	8	11111111
M	273	6	111111
N	718	14	11111111111111
O	844	17	11111111111111111
P	243	5	11111
Q	38	1	1
R	677	14	11111111111111
S	656	13	1111111111111
T	634	13	1111111111111
U	321	6	111111
V	136	3	111
W	166	3	111
X	51	1	1
Y	208	4	1111
Z	6		

In this table the vowels AEIOU=40.08%, consonants LNRST=30.77% and consonants JKQXZ=2.25%.

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

TABLE III.—Table of frequency of digraphs, duals or pairs (English). This table was prepared from 20,000 letters, but the figures shown are on the basis of 2,000 letters. For this reason they are, to a certain extent, approximate; that is, merely because no figures are shown for certain combinations, we should not assume that such combinations never occur but rather that they are rare. The letters in the horizontal line at the top and bottom are the leading letters; those in the vertical columns at the sides are the following letters. Thus in two thousand letters we may expect to find AH once and HA twenty-six times.

	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		1	7	10	22	3	2	26	4	2	2	7	8	11	2	9		13	12	9		2	4	1	12	
B	5			1	2				1			1	1	1	2				2	1	3				1	
C	6		1	1	14	2			11					11	3			2	3	1	1		1		1	
D	6			12	30	1			2			4		30	1			4	1	1	1		1		3	
E		11	14	16	12	2	6	33	10	2	6	18	14	12	1	7		36	11	12	2	16	5		1	1
F	3			2	8	2	1		2			2	1	3	25				3	1	1				1	
G	4			1	3				2					11	2			3							1	
H	1		11	2	4	1	4					1		2	1	1		2	10	50			3		2	
I	2	1	4	12	6	5	1	12	1		5	9	8	12	1	3		12	13	22	2	3	6		1	1
J		1																								
K	1		1		2													2	1		1					
L	14	6	2	1	6	1	1	1	6			9		3	6	3		3	2	3	5					
M	7			3	13	2		2	3				4	1	10			4	1	1					2	
N	38			3	25		2	1	31		3		2	2	39			4	3		11		2			
O	1	1	12	4	8	8	3	12	18	2		4	7	8	3	7		13	15	22		2	6	1	5	
P	2			1	8				1			2	4	2	3	2		1	8	1	4			3	1	
Q					2									1	1				1							
R	16	1	3	3	40	3	6	2	6			1	2	1	25	8		2	2	8	11				2	
S	16	1		3	25	1	2		17		1	2	1	12	7	2		9	11	6	11		1		6	
T	25	1	3	12	13	5	2	3	20			2	1	24	8	2		16	20	11	6		2	2	7	
U	1	2	1	6	1	3	2	2		3		3	1		17	1	5	3	5	5				1		
V	3	1			5				5						3			2			5				1	
W	1			2	8		1	1				1	1	2	4				2	3					3	
X	1				4				2						1						1					
Y	3	2		2	4		1	1				8	1	2		1		3	1	7						
Z	1								1					1												
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

TABLE IV.—Order of frequency of common pairs to be expected in a count of 2,000 letters of military or semi-military English text. (Based on a count of 20,000 letters).

TH	50	AT	25	ST	20
ER	40	EN	25	IO	18
ON	39	ES	25	LE	18
AN	38	OF	25	IS	17
RE	36	OR	25	OU	17
HE	33	NT	24	AR	16
IN	31	EA	22	AS	16
ED	30	TI	22	DE	16
ND	30	TO	22	RT	16
HA	26	IT	20	VE	16

TABLE V.—Table of recurrence of groups of three letters to be expected in a count of 10,000 letters of English text.

THE	89	TIO	33	EDT	27
AND	54	FOR	33	TIS	25
THA	47	NDE	31	OFT	23
ENT	39	HAS	28	STH	21
ION	36	NCE	27	MEN	20

TABLE VI.—Table of frequency of occurrence of letters as initials and finals of English words. Based on a count of 4,000 words; this table gives the figures for an average 100 words and is necessarily an approximation, like Table III. English words are derived from so many sources that it is not impossible for any letter to occur as an initial or final of a word, although Q, X and Z are rare as initials and B,I, J, Q, V, X and Z are rare as finals.

Letters	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
Initial	9	6	6	5	2	4	2	3	3	1	1	2	4	2	10	2	-	4	5	17	2	-	7	-	3	-
Final	1	-	-	10	17	6	4	2	-	-	1	6	1	9	4	1	-	8	9	11	1	-	1	-	8	-

It is practically impossible to find five consective letters in an English text without a vowel and we may expect from one to three with two as the general average. In any twenty letters we may expect to find from 6 to 9 vowels with 8 as an average. Among themselves the relative frequency of occurrence of each of the vowels, (including Y when a vowel) is as follows:

A, 19.5%	E, 32.0%	I, 16.7%
O, 20.2%	U, 8.0%	Y, 3.6%

The foregoing tables give all the essential facts about the mechanism of the English language from the standpoint of the solution of ciphers. The use to be made of these tables will be evident when the solution of different types of ciphers is taken up.

Data for the Solution of Ciphers in Spanish

The Spanish language is written with the following alphabet:

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

while the exact sense often depends upon the use of accents over the vowels. However, in cipher work it is exceedingly inconvenient to use the permanent digraphs, CH, LL and RR and they do not appear as such in any specimens of Spanish or Mexican cipher

examined. Accented vowels and Ñ are also not found and we may, in general, say that a cipher whose text is Spanish will be prepared with the following alphabet:

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

and the receiver must supply the accents and the tilde over the N to conform to the general sense.

However, many Mexican cipher alphabets contain the letters K and W. This is particularly true of the ciphers in use by secret service agents who must be prepared to handle words like NEW YORK, WILSON and WASHINGTON. The letters K and W will, however, have a negligible frequency except in short messages where words like these occur more than once.

In this connection, if a cipher contains Mexican geographical names like CHIHUAHUA, MEXICO, MUZQUIZ, the letters H, X and Z will have a somewhat exaggerated frequency.

In Spanish, the letter Q is always followed by U and the U is always followed by one of the other vowels, A, E, I or O. As QUE or QUI occurs not infrequently in Spanish text, particularly in telegraphic correspondence, it is well worth noting that, if a Q occurs in a transposition cipher, we must connect it with U and another vowel. The clue to several transposition ciphers has been found from this simple relation.

TABLE VII.—Normal frequency table for military orders and reports, calculated on a basis of 10,000 letters of Spanish text. The graphic form is on a basis of 200 letters.

	10,000 Letters		*200 Letters*
A	1352	27	111111111111111111111111111
B	102	2	11
C	474	9	111111111
D	524	10	1111111111
E	1402	28	1111111111111111111111111111
F	91	2	11
G	137	3	111
H	102	2	11
I	606	12	111111111111
J	41	1	1
L	517	10	1111111111
M	300	6	111111
N	619	12	111111111111
O	818	16	1111111111111111
P	257	5	11111
Q	87	2	11
R	751	15	111111111111111
S	724	14	11111111111111
T	422	8	11111111
U	387	7	1111111
V	85	2	11
X	6		
Y	103	2	11
Z	42	1	1

In this table the vowels AEIOU=45.65%; consonants LNRST=30.33%; consonants JKQXZ=1.76%.

Order of letters:

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

TABLE VIII.—Table of frequency of digraphs, duals or pairs, Spanish text. Like Table III, this table is on the basis of 2,000 letters although prepared from a count of 20,000 letters. For this reason it is, to a certain extent an approximation; that is, merely because no figures are shown for certain combinations, we should not assume that such combinations never occur but rather that they are rare. The letters in the horizontal lines at the top and bottom are the leading letters; those in the vertical columns at the sides are the following letters. Thus, in two thousand letters, we may expect to find AI twice and IA twenty-three times.

UNIVERSITY OF CALIFORNIA LIBRARY

	A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	
A	9	4	19	11	5		6	17	23		54	18	9	3	20		29	11	21	8	6		2	5	A
B	6								3			1		4											B
C	24		6	6	24				5		3		8	8			9	5		2			2		C
D	31				29				3				19	13			10	9					4		D
E	12	2	6	59	10		1	5	7	2	12	18	22	4	9		38	25	28	25	3		3		E
F	4				4						4		3					3					1		F
G	2				4				8				4											2	G
H	2		12		10													2					1		H
I	2		23	16		5	2				3	11	13				6	10	5		3				I
J	3				2								1												J
L	21	3	6		39	3	3		7		21		5	6			2	2		2					L
M	12				6				5		1		6	15			7	2		6			1		M
N	32				46		2		8					32						12			2		N
O			26	22	2	6	3	4	9		16	2	8		20		15	7	11						O
P	13				3				2		4	9	2	7			4	11							P
Q	11	5									1		2				3	1							Q
R	40				27	2			4		4			36	3		11		17	3					R
S	39				52				10				7	14			2			14			3		S
T	5				13				4		4		18	5			6	30							T
U	2		4	2	6	3	4			5		2	6		4	17		15	2				1		U
V	2				2						2			2				2					2		V
X																									X
Y	5				6									2				5		2				2	Y
Z	1				2								1				4			2					Z
	A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	

TABLE IX.—Order of frequency of common pairs to be expected in a count of 2,000 letters of Spanish military orders and reports. Based on Table VIII.

DE 59	ON 32	AC 24
LA 54	AD 31	EC 24
ES 52	ST 30	CI 23
EN 46	ED 29	IA 23
AR 40	RA 29	DO 22
AS 39	TE 28	NE 22
EL 39	ER 27	AL 21
RE 38	CO 26	LL 21
OR 36	SE 25	PA 20
AN 32	UE 25	PO 20

Alphabetic Frequency Tables

(Truesdell)

Frequency of occurrence in 1,000 letters of text:

Letter	*French*	*German*	*Italian*	*Portuguese*
A	80	52	117	140
B	6	18	6	6
C	33	31	45	34
D	40	51	31	40
E	197	173	126	142
F	9	21	10	12
G	7	42	17	10
H	6	41	6	10
I	65	81	114	59
J	3	1	*	5
K	*	10	*	
L	49	28	72	32
M	31	20	30	46
N	79	120	66	48
O	57	28	93	110
P	32	8	30	28
Q	12	*	3	16
R	74	69	64	64
S	66	57	49	88
T	65	60	60	43
U	62	51	29	46
V	21	9	20	15
W	*	15		
X	3	*	*	1
Y	2	*	*	1
Z	1	14	12	4

* Occurrence rare, usually in proper names.

Order of Frequency

French

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

German

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

Italian

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

Portuguese

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

Graphic Frequency Tables

Frequency of occurrence in 200 letters of text.

French

A	16	1111111111111111
B	2	11
C	6	111111
D	10	1111111111
E	39	111111111111111111111111111111111111111
F	2	11
G	1	1
H	1	1
I	13	1111111111111
J	1	1
K		
L	10	1111111111
M	6	111111
N	16	1111111111111111
O	11	11111111111
P	6	111111
Q	2	11
R	15	111111111111111
S	13	1111111111111
T	13	1111111111111
U	12	111111111111
V	4	1111
W		
X	1	1
Y		
Z		

Italian

A	23	11111111111111111111111
B	1	1
C	9	111111111
D	6	111111
E	25	1111111111111111111111111
F	2	11
G	3	111
H	1	1
I	23	11111111111111111111111
L	14	11111111111111
M	6	111111
N	13	1111111111111
O	19	1111111111111111111
P	6	111111
Q		
R	13	1111111111111
S	10	1111111111
T	12	111111111111
U	6	111111
V	4	1111
X		
Y		
Z	2	11

German

A	10	1111111111
B	4	1111
C	6	111111
D	10	1111111111
E	32	11111111111111111111111111111111
F	4	1111
G	8	11111111
H	8	11111111
I	16	1111111111111111
J		
K	2	11
L	6	111111
M	4	1111
N	24	111111111111111111111111
O	6	111111
P	2	11
Q		
R	14	11111111111111
S	11	11111111111
T	12	111111111111
U	10	1111111111
V	2	11
W	3	111
X		
Y		
Z	3	111

Portuguese

A	28	1111111111111111111111111111
B	1	1
C	7	1111111
D	8	11111111
E	28	1111111111111111111111111111
F	2	11
G	2	11
H	2	11
I	12	111111111111
J	1	1
L	6	111111
M	9	111111111
N	10	1111111111
O	22	1111111111111111111111
P	6	111111
Q	3	111
R	13	1111111111111
S	18	111111111111111111
T	9	111111111
U	9	111111111
V	3	111
X		
Y		
Z	1	1

Chapter III

Technique of Cipher Examination

IN time of active operations it is important that captured or intercepted cipher messages reach the examining office with the least possible delay. The text of messages, captured at a distance from the examining office, should be sent to the office by telegraph or telephone, the original messages being forwarded to the office as soon thereafter as possible.

The preamble, "place from," date, address and signature, give most important clues as to the language of the cipher, the cipher method probably used, and even the subject matter of the message. If the whole of a telegraphic or radio message is in cipher, it is highly probable that the preamble, "place from." etc., are in an operators' cipher and are distinct from the body of the message. As these operators' ciphers are necessarily simple, an attempt should always be made to discover, by methods of analysis to be set forth later, the exact extent of the operator's cipher and then to decipher the parts of the messages enciphered with it.

In military messages, we almost invariably find the language of the text to be that of the nation to which the military force belongs. The language of the text of the message of secret agents is, however, another matter and, in dealing with such messages, we should use all available evidence, both external and internal, before deciding finally on the language used. Whenever a frequency table can be prepared,

such a table will give the best evidence for this purpose.

All work in enciphering and deciphering messages and in copying ciphers should be done with capital letters. There is much less chance of error when working with capitals and, with little practice, it is just about as fast. An additional safeguard is to use black ink or pencil for the plain text and colored ink or pencil for the cipher. A separate color may be used for the key when necessary.

The following blank form is suggested as convenient for keeping a record of a cipher under examination. It should accompany the cipher through the examining process and should be filled in as the facts are determined. This record, the original cipher and all notes of work done during the examination, should be filed together when the examination is completed, whether the cipher has been solved or not. It may be that other ciphers solved later will give clues to the solution of such unsolved ciphers.

The first column of this blank should be filled out from data furnished by the officer obtaining the cipher from the enemy. A general order, emphasizing the importance of promptly forwarding captured or intercepted ciphers to an examining office, could specify that a brief report embodying this data should be forwarded with each cipher.

The second column of the blank should be filled out progressively as the work proceeds. The office number should be a serial one, the first cipher examined being No. 1. The date and hour of receipt at examining office will be a check as to the time required to transmit it from place of capture. The spaces "From" "At," "To," "At," "Date," are for

the information concerning sender and addressee of the cipher and are to be obtained from the message. In case an operators' cipher has been used, these parts of the message will have to be deciphered before the blanks can be filled in.

Intelligence Section, General Staff
1st Field Army

_____
Place, Date

Record of Cipher Examination

This cipher obtained by

_____

_____

at _____ _____

on _____ _____
(date) (hour)

How being transmitted when obtained. (Underscore means used and enter data on sending and receiving stations).

	Sending Station	Receiving Station
Radio		
Telephone		
Telegraph		
Buzzer		
Helio		
Lantern		
Flag		
Cyclist	from	to
Foot Messenger	"	"
Mtd. Messenger	"	"

How obtained. (Underscore means used). Captured before delivery to addressee. Captured after delivery to addressee. Intercepted, not received by addressee. Copied, but received by addressee.

REMARKS:

Office No. _____

Received _____
(Date) (Hour)

From _____

At _____

To _____ _____

At _____ _____

Date _____ _____

Probable language of text _____

Class { Transposition _____ / Substitution _____ / _____

Case _____

Remarks:

Solution completed _____
(date) (hour)

Language of text _____

Key, (if determined) _____

_____

Type _____ File No. _____

_____

_____
Examiner.

The probable language of the text is assumed from the preceding data and, if necessary, from

internal evidence. Thus a cipher from a Mexican source and not containing K or W is probably in Spanish.

The class and case are determined by the rules laid down later. The space for remarks is to permit notation of any special features. When the solution is completed, the date and hour are noted, the language of text and key (if determined) are entered and a type number, to identify it with other ciphers prepared by the same method (but not necessarily the same key), is given to it. The file number is for convenience in filing and in preparation of a card index.

The process of examination in an office with one examiner, one stenographer and one clerk, might be as follows: On receipt of a captured cipher with accompanying report, the stenographer makes four copies of the cipher on the typewriter. The clerk and stenographer then check the work. The stenographer then proceeds to fill out the first column and first two lines of the second column of the record blank from the report of the capturing officer, keeping the original cipher and two copies with the record. He may also fill out the first seven lines of the second column, if this data is on the captured cipher in plain text. In the meantime the clerk is counting and setting down the whole number of letters of the cipher and the occurrence of AEIOU, LNRST, and JKQXZ, while the examining officer is looking over the cipher for possible recurring groups of letters and underlining them when found.

This work being completed, the examining officer is in a position, ordinarily, to decide on the class of the cipher and he may have found something in his examination which will lead him to the case under the class. The clerk in this preliminary count should

keep track of the total occurrence of each of the fifteen check letters and not of the three groups given above. This takes a little longer but when done, the data for fifteen letters of the alphabet for a frequency table is completed, leaving only eleven other letters, and in Spanish, but nine, to be counted, in case it is necessary to prepare a frequency table.

If the examining officer decides the cipher to be of the transposition class, no further work with frequency tables is necessary. The clerk should proceed to count and set down the number of vowels in each line and column and the examining officer should look for any occurrence of the letter Q and try to connect it with U and another vowel. The stenographer may be set to work putting the cipher into rectangles of different dimensions. The clerk's work gives data for possible rearrangement, for if the vowels are much out of proportion at any point, they must be connected with the proper proportion of consonants as a first step in rearrangement. Work with transposition ciphers must necessarily include much of the fit and try method. The details of this work are taken up later.

If a cipher seems to be a substitution cipher, the examining officer should look over the frequency of occurrence of each of the fifteen letters counted. If some letters (it is of no importance at present which ones) occur much more frequently than others and some occur rarely or not at all, we may safely decide on Case 4, 5 or 6 and let the clerk proceed to finish the frequency table for the message. On the other hand, if all the fifteen letters examined occur with somewhere near the same frequency—for example, the most common letter occurring not over three or four times as often as the least common letter—we may at once eliminate the first three cases

and let the clerk proceed to examine the cipher for recurring pairs and groups, counting the intervening letters, so that the examining officer may decide whether Case 7, or some more complicated case, should be chosen.

If something more complicated than Case 7 has been used and other ciphers are on hand awaiting examination, the cipher should go into the unsolved file to be worked on when other work permits, unless the contents of the cipher are believed to be very important. Every opportunity should be taken to clean up the unsolved file and, whenever a message is solved, the methods should be tried, if applicable, to everything remaining in the file.

The first few days or weeks after the establishment of an examining office will be the most trying time. When solved ciphers begin to pile up, the methods of the enemy will be more and more apparent and it will often be possible to determine the method from knowledge of the name of the sender and receiver.

When a cipher has been solved, the solution should be prepared in triplicate and given the serial number of the cipher. Any parts which are not clear, through errors in enciphering or in transmission, should be underlined or otherwise made conspicuous, so that the head of the Intelligence Section may note them and, possibly, from other sources, supply the deficiency.

One of the copies of the cipher and report of examination, with a copy of the solution, should be turned over at once to the head of the Intelligence Section or to the Chief of Staff. The other copies of the solution should be filed with the original cipher, the report of examination, and all work done on the cipher.

Periodically, say once a week or even daily at the begining of active operations, there should be an interchange between all examining offices of solved messages involving new methods used by the enemy. All the examining offices will thus be kept in touch. It may also be possible to assign certain hostile radio stations to each examining office to prevent duplication of work.

Chapter IV

Classes of Ciphers

THERE are, in general, two classes of ciphers. These are the transposition cipher and the substitution cipher.

Substitution ciphers may be made up of substituted letters, numerals, conventional signs or combinations of all three; and furthermore, for a single letter of the original text there may be substituted a single letter, numeral or sign or two or more of each, or a whole word or group of figures, combination of conventional signs, or combinations of all three of these elements. Thus substitution ciphers may vary from those of extreme simplicity to those whose complication defies any ordinary method of analysis and whose solution requires the possession of long messages and much time and study. Fortunately the more difficult substitution ciphers are rarely used for military purposes, on account of the time and care required for enciphering and deciphering.

Transposition ciphers are limited to the characters of the original text. These characters are rearranged singly, according to some predetermined method or key (monoliteral transposition), or whole words are similarly rearranged (route cipher).

There may also be a combination of transposition and substitution methods in enciphering a message but in this case it will fall into the substitution class on first determination and after solution as a substitution cipher it must be handled as a transposition cipher. Examples of this case will be given.

We may also find transposition or substitution methods applied to words taken from a code book, or to numbers which represent these words. Thus cipher methods blend into code work, for a code is, after all, only a specialized substitution cipher.

We can now lay down the rules for determining whether any given cipher belongs to the substitution class or to the transposition class.

Count the number of letters in the message, the number of vowels, AEIOU, the number of the consonants, LNRST, and the number of the consonants, JKQXZ.

If the text is English and the cipher is a transposition cipher, this proportion will hold; vowels AEIOU constitute 40% of the whole; consonants LNRST, 30% and consonants JKQXZ, 3%.

If the text be Spanish the proportions for a transposition cipher will be: vowels AEIOU 45%, consonants LNRST, 30%; consonants JKQXZ, 2%.

If these proportions do not hold within 5%, one way or the other, the cipher is certainly a substitution cipher. Note, however, that often the end of a message is filled with letters like K, X, Z to complete cipher words and it is best to neglect the last word or words in making a count. Also, if the cipher be a long one, this determination can safely be made by taking 100 or 200 consecutive letters of the message, either from the beginning or, if nulls at the beginning are suspected, from the interior of the message.

The distinction between the route cipher (transposition) and the substitution cipher where whole words are substituted for letters of the original text, must be made on the basis of the words actually used. It is better to consider such a message as a route cipher when the words used appear to have some consecutive meaning bearing on the situation

at hand. A substitution cipher of this variety would only be used for transmission of a short message of great importance and secrecy, and then the chances are that certain words corresponding to A, E, N, O and T would appear with such frequency as to point at once to the fact that a substitution cipher was used. Watch the initial or terminal letters in such a cipher; they may spell the message.

In general, the determination of class by proportion of vowels, common consonants and rare consonants may be safely followed. We will now proceed to the examination of the more common varieties of each class of cipher.

Chapter V

Examination of Transposition Ciphers

AFTER having decided that a cipher belongs to the transposition class, it remains to decide on the variety of cipher used. As, by definition, a transposition cipher consists wholly of characters of the original message, rearranged according to some law, we may, in general, say that such a cipher offers fewer difficulties in solution than a substitution cipher. A transposition cipher is like a picture puzzle; the parts are all there and the solution merely involves their correct arrangement.

CASE 1.—Geometrical ciphers. This case includes all ciphers in which a certain number of the characters are chosen so that they will form a square or rectangle of predetermined dimensions; and then these characters are arranged according to a geometrical design.

Taking the message:

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

of twenty-four letters and assuming a rectangle of six letters horizontally, and four letters vertically, we may have:

(*a*) *Simple Horizontal*:

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

(*b*) *Simple Vertical*:

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

(*c*) *Alternate Horizontal*:

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

(*b*) *Alternate Vertical*:

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

(*e*) *Simple Diagonal*:

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

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

(*f*) *Alternate Diagonal*:

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

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

(*g*) *Spiral, clockwise*:

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

(*h*) *Spiral, counter clockwise*:

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

It is simply a matter of inspection to read a message in a cipher of this type, once the dimensions of the rectangles have been determined. We place the whole or a portion of the message in such rectangles and read horizontally, vertically and diagonally forward and backward. Parts of words will at once be apparent and the whole message is soon deciphered. Two examples will show the process.

Message

ILVGIOIAEITSRNMANHMNG

This message contains eight vowels or 38% out of twenty-one letters, and the letters LNRST occur 7 times or 33%, the letters XQJKZ not appearing. It is therefore a transposition cipher. Twenty-one letters immediately suggest seven columns of three letters each or three columns of seven letters each. Trying the former we have:

I L V G I O I
A E I T S R N
M A N H M N G

and reading down each column in succession (Case 1-b) reveals the message to be "I am leaving this morning."

Message

MSIBR ORSEE VUEEM CORER ELIDE TOEPQ
ENRER NSERY ECOLL EREUS PLURC ELOAJ
AEHUH PFASO NNOAA EPIUA PPEAC UQARU
OPOEI IRRMI AFDAA RQUBO ZAEGE RSFSX

There are 120 letters in this message with 57 vowels or 47% vowels, and the letters LNRST occur 31 times or 26% of the whole.

Non-occurrence of K and W and vowel proportion leads us to the assumption that it is a transposition cipher of a Spanish text. The factors of 120 are 5 x 3 x 2 x 2 x 2. We may then have one rectangle of 4 x 30 or one of 5 x 24 or two of 5 x 12, or three of 5 x 8, or four of 5 x 6, of five of 3 x 8, or ten of 3 x 4, or twenty of 3 x 2. The message being in a rectangle of 4 x 30, we can inspect it as it stands and this is clearly not the arrangement if it be a geometrical transposition cipher at all. It is best however to try the largest possible rectangles first so we will put it in the form 5 x 24, thus:

MSIBRORSEEVUEEMCORERELID
ETOEPQENRERNSERYECOLLERE
USPLURCELOAJAEHUHPFASONN
OAAEPIUAPPEACUQARUOPOEII
RRMIAFDAARQUBOZAEGERSFSX

Here an inspection shows this to be Case 1-f, alternate diagonal, and the text to be "ME SITUO SOBRE PARRAL PORQUE ME PRESENCIA FUE REVELADA POR U"; here the sense breaks but note that U is the twelfth letter of the line and continue as if the rectangle were 5 x 12 and we have "NA PAREJA QU." Now inspect the second rectangle of 5 x 12 in the same way and the sense continues "E SE ME ACERCO Y HUBO QUE RECHAZAR POR EL FUEGO ALLI ESRERO ORDENES FINISX".

The practical way of examining a cipher of this type is to have several men prepare rectangles of different dimensions, using the letters of the cipher in the order received. The rectangles can be inspected very rapidly when once prepared. Note that the dimensions of any rectangle will rarely be such as to contain more than fifty letters, on account of the necessity of filling up a rectangle with nulls if the number of letters of the message is just a little greater than a multiple of the rectangle. Also large rectangles give, for all but the diagonal method, whole words in a line or column and these are easily noted.

The following ciphers come under Case 1:

CASE 1-i.—The rail fence cipher, useful as an operators' cipher but permits of no variation and is therefore read almost as easily as straight text when the method is known. The message:

HOSTILE CAVALRY HAS RETIRED

is written:

O T L C V L Y A R T R D
H S I E A A R H S E I E

and is sent:

OTLCV LYART RDHSI EAARH SEIEX

CASE 1-j.

Message

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

To solve this cipher, read down the columns in this order 8, 1, 15, 2, 14, 3, 13, 4, 12, etc. A variation is to arrange the cipher so the columns are read upwards. Another is to arrange the ciphers so the columns are read alternately upward and downward. The factors of the number of letters in this case give the shape of the rectangle as usual.

It will be seen that there are a great number of possible transposition ciphers that come under Case 1 but practically all of them are useless from a military standpoint because they do not depend on a key which can be readily and frequently changed. However such ciphers constantly crop up in cipher examination, being used for special communication between parties who consider the regular military ciphers too complicated. Thus some of these expedients have been used.

REVERSED WRITING.—(Special case of Case 1-a).

LEAVING TONIGHT is enciphered THGINOT GNIVAEL or it may be reversed by words, thus GNIVAEL THGINOT or by groups of five letters, thus IVAEL NOTGN XTHGI.

VERTICAL WRITING.—(Special case of Case I-b). Same message is enciphered,

LT
EO
AN
VI
IG
NH
GT

and is sent, LTEOA NVIIG NHGTX.

CASE 2.—This case includes all transposition ciphers in which lines and columns of the text are rearranged according to some key word or key number. There are many varieties of this case but their solution usually is arrived at through the methods suggested for Case 1, that is, arrangement into appropriate rectangles and examination of lines and columns for words or syllables. Rearrangement of columns or lines follows until the solution is completed.

CASE 2-a. *Message*

HIIGF TNGHI NTCVN IEIOT CYIFY LHAEA ESNBA EEEEN
RWGBN YDELR OAESG RNEBO VNLDA ICAOA LCNDT IRGVA
CDOIE SEREC DVPEI AFIFL RINEH ETT

There are 108 letters in this message and examination shows it to be a transposition cipher, English text. The number of letters, 108, immediately suggests a rectangle of 12 x 9 or 9 x 12 letters. Put into this form we have:

	Vowels
H I I G F T N G H I N T	3
C V N I E I O T C Y I F	5
Y L H A E A E S N B A E	6
E E E N R W G B N Y D E	4
L R O A E S G R N E B O	5
V N L D A I C A O A L C	5
N D T I R G V A C D O I	4
E S E R E C D V P E I A	6
F I F L R I N E H E T T	4

	Vowels
H I I G F T N G H	2
I N T C V N I E I	4
O T C Y I F Y L H	2
A E A E S N B A E	6
E E E N R W G B N	3
Y D E L R O A E S	4
G R N E B O V N L	2
D A I C A O A L C	5
N D T I R G V A C	2
D O I E S E R E C	5
D V P E I A F I F	4
L R I N E H E T T	3

The vowel count of the lines shows the first arrangement to be the more likely. We will now number the columns and try pairing off certain ones which in no line would give impossible combinations of letters.

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

These combinations appear among others:

1	6	2	4	5	2
H	T	I	G	F	I
C	I	V	I	E	V
Y	A	L	A	E	L
E	W	E	N	R	E
L	S	R	A	E	R
V	I	N	D	A	N
N	G	D	I	R	D
E	C	S	R	E	S
F	I	I	L	R	I

The word FIGHT stares at us from the first line; let us arrange the columns thus:

5	2	4	1	6	3
F	I	G	H	T	I
E	V	I	C	I	N
E	L	A	Y	A	H
R	E	N	E	W	E
E	R	A	L	S	O
A	N	D	V	I	L
R	D	I	N	G	T
E	S	R	E	C	E
R	I	L	F	I	F

We have the words FIGHTI(NG), VICIN-(ITY), RENEWE(D), ANDVIL(LA), RDINGT-(O), RECE(IVED). With this to go on, we must choose column 11 as the next one and then in order, columns 8, 10, 7, 12, 9. But note that the order 11, 8, 10, 7, 12, 9, is the same as the order 5, 2, 4, 1, 6, 3. The message was written in twelve columns and the columns have been transposed in that order. We may, although it is entirely unnecessary, speculate on the key word used. It was probably

M	E	X	I	C	O
4	2	6	3	1	5

meaning that the 4th column of the plain text was transferred in enciphering so it became our 1st, the 2d column remained the 2d; the 6th column became our 3d, etc.

Actually, this cipher was solved because the word VILLA was suspected and all the necessary letters were found in line six of the arrangement in

twelve columns. The order 1, 6, 3, 11, 8 was tried and gave this result.

1	6	3	11	8
H	T	I	N	G
C	I	N	I	T
Y	A	H	A	S
E	W	E	D	B
L	S	O	B	R
V	I	L	L	A
N	G	T	O	A
E	C	E	I	V
F	I	F	T	E

The remainder of the solution followed the lines already laid down and, naturally, offered no difficulties, in view of the large number of connected syllables available.

CASE 2-b.

Message

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

This is a transposition cipher, English text, and contains 105 letters. The factors of 105 are 5 x 3 x 7 so that we must investigate the following rectangles; 5 x 21, 15 x 7, three of 5 x 7, five of 3 x 7 and seven of 5 x 3.

21x5

																					Vowels
S	L	C	O	F	W	E	E	T	N	E	B	R	D	O	O	R	V	Y	M	F	6
F	E	D	I	N	M	T	E	C	R	O	I	A	R	P	E	R	H	O	E	S	9
E	T	S	R	F	B	H	L	T	E	N	A	H	O	P	T	A	U	S	O	M	7
T	L	R	T	E	T	T	A	S	C	B	H	N	I	O	D	C	R	E	N	E	6
N	A	A	P	R	D	L	A	C	Y	E	E	C	I	I	E	S	G	U	F	N	9
Vowels	1	2	1	2	1	0	1	4	0	1	3	3	1	3	3	3	1	1	3	2	1

The vowel count of the columns of the rectangle 5 x 21 is very satisfactory. Let us consider it as three blocks of 5 x 7 each, since we must do this ultimately, and make a vowel count of columns for these blocks.

5x21

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

	Column				
	1	2	3	4	5
Vowels, 1st block	2	2	3	2	2
Vowels, 2d block	2	3	2	2	2
Vowels, 3d block	3	4	3	2	2

This is also excellent, so we will try three blocks 5 x 7 and see if rearrangement of *horizontal lines* will give results reading the columns vertically.

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

Among other combinations are:

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

The addition of line 6 above line 3 and line 4 below line 7 will complete this cipher. The successive columns should be read downward.

CASE 2-c. In this case, both lines and columns are rearranged by means of a key word or key words. The method of solution is the same as Case 2-a and 2-b except that the lines must be rearranged after the columns have been correctly arranged, or in some cases, vice versa. This cipher is not infrequently met with because it seems to offer safety by use of two key words and by the great but only apparent complexity of the method.

Message

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

This is a transposition cipher, English text and

the number of letters, 70, leads us to try rectangles of 10 x 7 and 7 x 10.

										Vowels
W	V	G	A	E	E	G	E	N	L	4
T	F	T	O	H	T	E	I	E	F	3
R	B	T	S	E	I	N	E	N	G	3
O	N	W	R	M	G	X	I	X	N	2
G	O	I	T	N	R	O	M	R	O	4
E	S	P	A	L	H	N	E	A	C	4
U	D	N	N	H	D	E	R	M	E	3

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

The first form looks the more likely from the vowel count. We proceed to number the columns and lines and try rearrangement of columns so as to obtain possible letter combinations from every line.

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

Among other combinations we have these:

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

A very casual inspection of the lines shows that they should be rearranged in order 6, 1, 2, 7, 3, 5, 4, as follows:

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

Although of no particular importance, it may be stated that the column key in this case was GRAND

and the line key was CENTRAL, both used as in enciphering Case 2-a.

CASE 3. Route ciphers. In this case, whole words of the message are transposed according to some of the methods of Case 1 or 2 or their equivalents. The route cipher is little used at present. Its development and use during the Civil War was caused by the inability of the telegraphers of that day to handle regular cipher matter correctly and rapidly. It was, even in those days, frankly only a delaying cipher and, to be of any value, had to be filled with meaningless words to conceal the message proper. An example from the Signal Book will suffice to show the general character of route ciphers. To one familiar with monoliteral transposition ciphers, even the best of route ciphers offers but little difficulty.

"To encipher the message 'MOVE DAYLIGHT. ENEMY APPROACHING FROM NORTH. PRISONERS SAY STRENGTH ONE HUNDRED THOUSAND. MEET HIM AS PLANNED.' arrange as follows:

MOVE	STRENGTH	PLANNED	SAY
DAYLIGHT	ONE	AS	PRISONERS
ENEMY	HUNDRED	HIM	NORTH
APPROACHING	THOUSAND	MEET	FROM

Here the route is down the first column, up the fourth, down the second and up the third."

This cipher was often complicated by the introduction of nulls for every fifth word. Thus the above message might be sent:

MOVE STRENGTH PLANNED SAY *NEVER* DAYLIGHT ONE AS PRISONERS *LEAVING* ENEMY HUNDRED HIM NORTH *UNCHANGED* APPROACHING THOUSAND MEET FROM *COME.*

The words in italics are nulls and not a part of

the message and the receiver eliminates them before arranging his message in columns to get the sense of it.

As an additional complication, it was customary for each correspondent to have a dictionary or code in which the names of all prominent generals and places and many of the prominent verbs, —as to march, to sail, to encamp, to attack, to retreat, —were represented by other words.

A route cipher using the code words of the War Department code might have some advantages over the method of enciphering code messages as prescribed in that Code.

General Remarks on Transposition Ciphers

It is the consensus of opinion of experts that the transposition cipher is not the best one for military purposes. It does not fulfill the first, second, and third of Kirckhoff's requirements as to indecipherability, safety when apparatus and method fall into the hands of the enemy, and dependability on a readily changeable key word.

However, transposition ciphers are often encountered. They are favorites with those who find the substitution ciphers too difficult and too tedious to handle and who believe that their transposition methods are either absolutely indecipherable or sufficiently so for the purpose of concealing the text of a message for the time being. They seem to be particularly popular with secret agents and spies, presumably because special apparatus is rarely necessary in enciphering and deciphering.

Although the number of transposition methods is legion, they can practically all be considered under one of the three cases already discussed. It is surprising how often transposition ciphers prepared

by complicated rules, will, on analysis, be seen to be very simple.

To be successful in solving transposition ciphers, one should constantly practice reading backward and up and down columns, so that the common combinations of letters are as quickly identified when seen thus as when encountered in straight text. Combinations like EHT, LLIW, ROF, DNA, etc., should be appreciated immediately as common words written backward.

A study of the table of frequency of digraphs or pairs is also excellent practice and such a table should be at hand when a transposition cipher is under consideration. It assists greatly if Case 2 be encountered and is of considerable use in solving Case 1.

The solution of route ciphers is necessarily one of try and fit, with the knowledge that such ciphers usually are read up and down columns. It is not believed that route ciphers will often be met with at the present day.

Chapter VI

Examination of Substitution Ciphers

WHEN an unknown cipher has been put into the substitution class by the methods already described we may proceed to decide on the variety of substitution cipher which has been used.

There are a few purely mechanical ways of solving some of the simple cases of substitution ciphers but as a general rule some or all of the following determinations must be made:

1. By preparation of a frequency table for the message we determine whether one or more substitution alphabets have been used and, if one only has been used, this table leads to the solution.

2. By certain rules we determine how many alphabets have been used, if there are more than one, and then isolate and analyze each alphabet by means of a frequency table.

3. If the two preceding steps give no results we have to deal with a cipher with a running key, a cipher of the Playfair type, or a cipher where two or more characters are substituted for each letter of the text. Some special cases under this third head will be given but, in general, military ciphers of the substitution class will usually be found to come under the first two heads, on account of the time and care required in the preparation and deciphering of messages by the last named methods and the necessity, in many cases, of using complicated machines for these processes.

CASE 4-a.

Message

OBQFO BPBRP QBAML OBHIF PILFQ FJBOX OFLNR BIXOZ EL

From the recurrence of B, F and O, we may conclude that a single substitution alphabet was used for this message. If so and if the alphabet runs in the same order and direction as the regular alphabet, the simplest way to discover the meaning of the message is to take the first two words and write alphabets under each letter as follows, until some line makes sense:

O B Q F O B P B R P
P C R G P C Q C S Q
Q D S H Q D R D T R
R E T I R E S E U S

The word RETIRESE occurs in the fourth line, and, if the whole message be handled in this way we find the rest of the fourth line to read USTED POR EL MISMO ITINERARIO QUE MARCHO. The message was enciphered using an alphabet where A=X, B=Y, C=Z, D=A, etc. noting that as this message is in Spanish the letters K and W do not appear in the alphabet.

CASE 4-b.

Message

HUJZH UIUPN OZYTS VQXMI SMOMX MQHUD UMREI SESJU AG

This is a message in Spanish. We will handle it as in case 4-a, setting down the whole message.

HUJZHUIUPNOZYTSVQXMISMOMXMQHUDUMREISESJUAG		
IVLAIVJVQOPAZUTXRY	A=A	NYNRIVEVNSFJTFTLVBH
JXMBJXLXRPQBAVUYSZ		OZOSJXFXOTGLUGUMXOI
LYNCLYMYSQRCBXVZTA		PAPTLYGYPUHMVHVNYDJ
MZODMZNZTRSDCYXAUB		QBQUMZHZQVINXIXOZEL
NAPENAOAUSTEDZYBVC		RCRVNAIARXJOYJYPAFM
OBQFOBPB	A=U	AZCXD SDSXOBJBSYLPZLZQBGN
PCRGPCQC		BADYE TETYPCLCTZMQAMARCHO
QDSHQDRD		CBEZF UFUZQDMDUANRB A=S
RETIRESE		DCFAG VGVARENEVBOSC
A=Q		EDGBH XHXBSFOFXCPTD
		FEHCI YIYCTGPGYDQUE
		GFIDJ ZJZDUHQHZEA=O
		HGJEL ALAEVIRIAF
		IHLA=M BMBFXJSJBG
		JIM CNCGYLTLCH
		LJN DODHZMUMDI
		MLO EPEIANVNEJ
		NMP FQFJBOXOFL
		ONQ GRGLCPYPGM
		POR HSHMDQZQHN
		A=E ITINERARIO
		A=D

Here each word of the message comes out on a different line, and noting in each case the letter corresponding to A, we have the word QUEMADOS which is the key. The cipher alphabet changed with each word of the message.

A variation of this case is where the cipher alphabet changes according to a key word but the change comes every five letters or every ten letters of the message instead of every word. The text of the message can be picked up in this case with a little study.

Note in using case 4 that if we are deciphering a Spanish message we use the alphabet without K or W as a rule, altho if the letters K or W appear in

ce = t ?

the cipher it is evidence that the regular English alphabet is used.

CASE 5-a.

Message

DNWLW MXYQJ ANRSA RLPTE CABCQ RLNEC LMIWL
XZQTT QIWRY ZWNSM BKNWR YMAPL ASDAN

This message contains K and W and therefore we expect the English alphabet to be used. The frequency of occurrence of A, L, N, R and W has lead us to examine it under case 4 but without result. Let us set down the first two words and decipher them with a cipher disk set A to A and then proceed as in case 4.

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

The message is thus found to be enciphered with a cipher disk set A to E and the text is: BRITISH GOVERNMENT PLACED CONTRACTS WITH FOLLOWING FIRMS DURING SEPTEMBER.

CASE 5-b.

Same as case 4-b except that the cipher message must be deciphered by means of a cipher disk set A to A before proceeding to make up the columns of alphabets. The words of the deciphered message will be found on separate lines, the lines being indicated as a rule by a key word which can be determined as in case 4-b.

The question of alphabetic frequency has already been discussed in considering the mechanism of language. It is a convenient thing to put the frequency tables in a graphic form and to use a similar graphic form in comparing unknown alphabets with the standard frequency tables. For instance the standard Spanish frequency table put in graphic

form is here presented in order to compare with it the frequency table for the message discussed in case 4-a.

Standard Spanish frequency table			Table for Message Case 4-a		
A	11111111111111111111111111	27	A	1	1
B	11	2	B	1111111	7
C	111111111	9	C		
D	1111111111	10	D		
E	1111111111111111111111111111	28	E	1	1
F	11	2	F	11111	5
G	111	3	G		
H	11	2	H	1	1
I	111111111111	12	I	111	3
J	1	1	J	1	1
L	1111111111	10	L	111	3
M	111111	6	M	1	1
N	111111111111	12	N	1	1
O	1111111111111111	16	O	111111	6
P	11111	5	P	111	3
Q	11	2	Q	111	3
R	111111111111111	15	R	11	2
S	11111111111111	14	S		
T	11111111	8	T		
U	1111111	7	U		
V	11	2	V		
X			X	11	2
Y	11	2	Y		
Z	1	1	Z	1	1

Our first assumption might be that B=A and F=E but it is evident at once that in that case, S, T, U and V (equal to R, S, T and U) do not occur and a message even this short without R, S, T or U is practically impossible. By trying B=E we find that the two tables agree in a general way very well and this is all that can be expected with such a short message. The longer the message the nearer would its frequency table agree with the standard table. Note that if a cipher disk has been used, the alphabet runs the other way and we must count upward in working with a graphic table. Note also that if, in a fairly long message, it is impossible to coördinate the graphic table, reading either up or down, with the standard table and yet some letters occur much more frequently than others and some do not occur at all, we have a mixed alphabet to deal with. The example chosen for case 6-a is of this character. An examination of the frequency table given under that case shows that it bears no graphic resemblance to

the standard table. However, as will be seen in case 7-b, the preparation of graphic tables enables us to state definitely that the same order of letters is followed in each of a number of mixed alphabets.

General Remarks

Any substitution cipher, enciphered by a single alphabet composed of letters, figures or conventional signs, can be handled by the methods of case 6. For example, the messages under case 4-a and 5-a are easily solved by these methods. But note that the messages under case 4-b and 5-b cannot so be solved because several alphabets are used. We will see later that there are methods of segregating the different alphabets in some cases where several are used and then each of the alphabets is to be handled as below.

CASE 6-a.

Message

QDBYP BXHYS OXPCP YSHCS EDRBS ZPTPB BSCSB PSHSZ AJHCD OSEXV HPODA PBPSZ BSVXY XSHCD

This message was received from a source which makes us sure it is in Spanish. The occurrence of B, H, P and S has tempted us to try the first two words as in case 4 and 5 but without result. We now prepare a frequency table, noting at the same time the preceeding and following letter. This latter proceeding takes little longer than the preparation of an ordinary frequency table and gives most valuable information.

Frequency Table

		Prefix		*Suffix*
A	II	2	ZD	JP
B	IIIIIIII	8	DPRPBSPZ	YXSBSPPS
C	IIIII	5	PHSHH	PSSDD
D	IIIII	5	QECOC	BROA
E	II	2	S S	DX
F				
G				
H	IIIIII	6	XSSJVS	YCSCPC
I				
J	I	1	A	H
L				
M				
N				
O	III	3	SDP	XSD
P	IIIIIIII	9	YXCZTBHAB	BCYTBSOBS
Q	I	1		D
R	I	1	D	B
S	IIIIIIIIIII	12	YYCBBCPHOPBX	OHEZCBHZEZVH
T	I	1	P	P
U				
V	II	2	XS	HX
X	IIIII	5	BOEVY	HPVYS
Y	IIII	4	BHPX	PSSX
Z	III	3	SSS	PAB

It is clear from an examination of this table that we have to deal with a single alphabet but one in which the letters do not occur in their regular order.

We may assume that P and S are probably A and E, both on account of the frequency with which they occur and the variety of their prefixes and suffixes. If this is so, then B and H, are probably consonants and may represent R and N respectively. D and X are then vowels by the same method of analysis. Noting that HC occurs three times and taking H as N we conclude that C is probably T. Substitute these values in the last three words of

the message because the letters assumed occur rather frequently there.

```
P B P S Z B S V X Y X S H C D
          I   I       I
A R A E _ R E _ _ _ E N T
              O   O       O
```

Now Z is always prefixed by S and may be L. Taking X=I and D=O, (they are certainly vowels), V=G and Y=M, we have

ARA EL REGIMIENTO

Substituting these values in the rest of the message we have

```
Q D B Y P B X H Y S O X P C P Y S H C S E D R B S Z P T P B
_ O R M A R I N M E _ I A T A M E N T E _ O _ R E L A _ A R
_

B S C S B  P S H S Z  A J H C D  O S E X V H P O D A
R E T E R  A E N E L  _ _ N T O  _ E _ I G N A _ O _
```

We may now take Q=F, O=D, E=S, R=B, T=C, A=P and J=U and the message is complete. We are assisted in our last assumption by noting that S=E and E=S, etc., and we may on that basis reconstruct the entire alphabet. The letters in parenthesis do not occur in the message but may be safely assumed to be correct.

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

It is always well to attempt the reconstruction of the entire alphabet for use in case any more cipher messages written in it are received.

CASE 6-b.

Message

Lt. J. B. Smith, Royal Flying Corps, Calais, France.

DACFT	RRBHA	MOOUE	AENOI	ZTIET
ASMOS	EOHIE	YOCKF	NOHOE	NOUTH
OMEAH	NILGO	OSAHU	OHOUE	APCHS
TLNDA	CFTEN	INTWN	BAFOH	GROHT
AEIOH	ABRIS	ODACF	TRREN	OSTSM
AYBIS	DFTEN	EFAPH	OSMNI	ZTIEA
HLILL	TWSOU	GDENO	UTHOM	EAHBH
AMOOU	EAYOE	QISUU	OLEHA	DENOE
NHOOQ	OBBOR	TSLHO	BAHEO	UBHOB
IHTSW	ENOHO	PAHIH	ITUAS	BIHTL

Graham-White.

The address and signature indicate that this message is in English.

There are 250 letters in the cipher; the vowels AEIOU occur 109 times or 43.6%, the letters LNRST occur 62 times or 24.8%, and the letters KQVXZ occur 5 times or 2%. The proportion in the case of the vowels is somewhat too large and, in the case of the letters LRNST, it is too small. It is then questionable whether this is a transposition cipher altho, at first glance it might appear to be one.

On examination for parts of possible words we are at once struck by the occurrence at irregular intervals of recurring groups, viz:

DACFTRR	ENO	BHAMOOUEA
DACFTEN	ENOUTHOMEAH	BHAMOOUEA
	ENO	
DACFTRR	DENOUTHOMEAH	IZTIE
FTEN	DENO	IZTIE
	ENO	

This is a strong indication that the cipher is a substitution cipher, so, to make an examination a frequency table will be constructed.

Frequency Table

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
23	11	7	6	24	7	3	26	16	0	1	8	8	15	36	3	2	8	14	17	11	1	3	0	3	2

Superficially, this looks like a normal frequency table, but O is the dominant letter, followed by H, E, A, T, I, N, S, in the order named. It is certainly Case 6 if it is a substitution cipher at all.

Let us see what can be done by assuming O=E; the triplet ENO, occurring six times might well be THE and E=T and N=H. A glance at the frequency table shows this to be reasonable. Now substitute these letters in some likely groups. FNOHOENO becomes _HE_ETHE; FTEN becomes _TH; ENOENHO becomes THETH_E; ENOHO becomes THE_E. A bit of study will show that F=W, T=I and H=R and the frequency table bears this out except that H(=R) seems to occur too frequently. The recurring groups containing DAC (see above) occur in such a way that we may be sure DAC is one word, FTRR is another and FTEN(=WITH) is a third. Now FTRR becomes WI__, which can only be completed by a double letter. LL fills the bill and we may say R=L. As DAC starts the message and is followed by FTRR (=WILL) it is reasonable to try DAC=YOU. Looking up DAC in the frequency table it is evident that we strain nothing by this assumption. We now have:

Letters of cipher ONTAHECFD
Letters of message EHIORTUWY

Now take the group ENOUTHOMEAH which occurs twice. This becomes THE_IRE_TOR and if we substitute U=D and M=C we have THE DIRECTOR. Next the group (FTRR)BHAMOOUEA becomes (WILL) _ROCEEDTO and the context gives word with missing letter as PROCEED, from which B=P, Next the group (ENO) IZTIETASMOSEOHIEYOCK(FNOHO) becomes (THE)__I_TIO_CE_-TER_T_EU_(WHERE) and the group (FTEN)EFAPHOSMNIZTIEAHL becomes (WITH)TWO_RE_CH

__I_TOR_. The substitution of A for I, V for Z, N for S and F for P makes the latter group read (WITH TWO FRENCH AVIATORS and the former read (THE)AVIATION CENTER AT_EU_(WHERE).

Now the word YOCK=(_EU_) is the name of a place, evidently. WE find another group containing Y, viz: ENOSTSMAYBISD which becomes THENINCO_PANY so that evidently we should substitute M for Y. The other occurrence of Y (=M) is in the group EAYOEQISU which becomes TOMET_AND. A reasonable knowledge of geography gives us the words MEUX and METZ so that X should be substituted for K and Z for Q.

We now have sufficient letters for a complete deciphering of the message.

Letters of cipher ABCDEFGHIKLMNOPQRSTUVWYZ
Letters of message OPUYTW_RAXSCHEFZLNID__MV

The message deciphers:

YOU WILL PROCEED TO THE AVIATION CENTER AT MEUX WHERE THE DIRECTOR HAS _EEN ORDERED TO FURNISH YOU WITH A HI_H POWER _LERIOT AEROPLANE. YOU WILL THEN IN COMPANY WITH TWO FRENCH AVIATORS ASSI_NED _Y THE DIRECTOR PROCEED TO METZ AND DESTROY THE THREE ZEPPELINS REPORTED PREPARIN_ THERE FOR A RAID ON PARIS.

The substitution of B for G, G for W and K for V completes the cipher. This cipher is difficult only because the cipher alphabet is made up, not haphazard, but scientifically with proper consideration for the natural frequency of occurrence of the letters. In cipher work it is dangerous to neglect proper analysis and jump at conclusions.

In the study of Mexican substitution ciphers, several alphabets have been found which are made up in a general way, like the one discussed in this case.

CASE 6-c.—It is a convenience in dealing with ciphers made up of numbers or conventional signs to substitute arbitrary letters for the numbers and signs. Suppose we have the message:

"??2& 45x15)"8&# &&1x4 %&4&%
6x?&" 8&*x4 6°*°& %"4&"

By arbitrary substitution of letters this is made

ABBCD EFGHF IJKDL DDHGE MDEDM NGBDA
KDOGE NPOPD MAEDA

This message is now in convenient shape to handle as Case 6-a and on solution is found to read:

ALL PERSONS HAVE BEEN ORDERED TO LEAVE FORTIFIED AREA.

In the same way the message

1723 3223 2825 1828 3630 2336 1423 2827 2324 3120 2317 3123
3036 2120 2415 3029 1512 2831 1721 2715 2811 2715 1923 3030
1215 1130 2128 3623

is found to be made up entirely of numbers between 11 and 36 with the numbers 23, 28 and 30 occurring most frequently. This immediately suggests an alphabet made up of the numbers from 11 to 36 inclusive and each cipher group of figures represents two letters. By arbitrary substitution of letters for groups of two numbers we obtain:

AB CB DE FD GH BG IB DJ BK LM BA LB
HG NM OP HQ PR DL AN JP DS JP TB HH
RP SH ND GB

and this message is also in shape to handle as Case 6-a. It reads, on solution,

SEVEN HUNDRED MEN LEFT YESTERDAY FOR POINTS ON LOWER RIO GRANDE.

Chapter VII

WE WILL now consider the class of substitution ciphers where a number of alphabets are used, the number and choice of alphabets depending on a key word or equivalent and being used periodically throughout the message.

In this class belong the methods of Vigenere, Porta, Beaufort, St. Cyr, and many others. These methods date back several hundred years, but variations of them are constantly appearing as new ciphers. The Larrabee cipher, used for communication between government departments, is the Vigenere cipher of the 17th Century. The cipher disk method is practically the Vigenere cipher with reversed alphabets.

In using these ciphers, there is provided a number of different cipher alphabets, usually twenty-six, and each cipher alphabet is identified by a different letter or number. A key word or phrase (or key number) is agreed upon by the correspondents. The message to be enciphered is written in lines containing a number of letters which is a multiple of the number of letters of the key. The key is written as the first line. Then each column under a letter of the key is enciphered by the cipher alphabet pertaining to that letter of the key. For example, let us take the message, "All radio messages must hereafter be put in cipher," with the key GRANT, using the Vigenere cipher alphabets given below. Each of these alphabets is identfied by the first or left hand letter which represents A of the text. We thus will

use in turn the alphabets beginning with G, with R, with A, with N, and with T.

```
G R A N T G R A N T

A L L R A D I O M E
S S A G E S M U S T
H E R E A F T E R B
E P U T I N C I P H
E R
```

Using the alphabet indicated by G, we get

```
G       J
Y       Y
N       L
K       T
K
```

Continuing for the other alphabets, we get

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

This method of arranging the message into lines and columns and then enciphering whole columns with each cipher alphabet is much shorter than the method of handling each letter of the message separately. The chance of error is also greatly reduced.

All these cipher methods can be operated by means of squares containing the various alphabets, cipher disks or arrangements of fixed and sliding alphabets. For example, this was the original cipher of Vigenere:

(See next page.)

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

The first horizontal alphabet is the alphabet of the plain text. Each substitution alphabet is designated by the letter at the left of a horizontal line. For example, if the key word is BAD, the second, first and fourth alphabets are used in turn and the word WILL is enciphered XIOM.

The Larrabee cipher is merely a slightly different arrangement of the Vigenere cipher and is printed on a card in this form:

(See next page.)

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 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	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 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	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 c d e f g h i j k l m n o p q r s t u v w x y z a b

etc.

Y	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 y z a b c d e f g h i j k l m n o p q r s t u v w x
Z	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 z a b c d e f g h i j k l m n o p q r s t u v w x y

The large letters at the left are the letters of the key word. It will be noted that these letters correspond to the first letters of the cipher alphabets (in small letters) as in the Vigenere cipher.

A much simpler arrangement of the Vigenere cipher is the use of a fixed and sliding alphabet. Either the fixed or sliding alphabet must be double in order to get coincidence for every letter when A is set to the letter of the key word.

Fixed Alphabet of Text

ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Movable Alphabet of Cipher

As shown here, A of the fixed or text alphabet coincides with T of the movable cipher alphabet. This is the setting where T is the letter of the key word in use. The lower movable alphabet is moved for each letter of the message and the A of the fixed alphabet is made to coincide in turn with each letter of the key before the corresponding letter of the text is enciphered. It is obviously only a step from this arrangement to that of a cipher disk, where the

fixed alphabet, (a single one will now serve) is printed in a circle and the movable alphabet, also in a circle, is on a separate rotatable disk. Coincidence of any letter on the disk with A of the fixed alphabet is obtained by rotating the disk.

The well known U. S. Army Cipher Disk has just such an arrangement of the fixed alphabet but the alphabet of the disk is reversed. This has several advantages in simplicity of operation but none in increasing the indecipherability of the cipher prepared with it. The arrangement of fixed and sliding alphabets which is equivalent to the U. S. Army cipher disk is this:

Fixed Alphabet

ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ

ZYXWVUTSRQPONMLKJIHGFEDCBA

Movable Alphabet

It will be noticed that with this arrangement of running the alphabets in opposite directions, it becomes immaterial which alphabet is used for the text and which for the cipher for if A=G then G=A. This is not true of the Vigenere cipher.

It is perfectly feasible to substitute a card for the U. S. Army cipher disk. It would have this form:

ABCDEFGHIJKLMNOPQRSTUVWXYZ
1 AZYXWVUTSRQPONMLKJIHGFEDCB
2 BAZYXWVUTSRQPONMLKJIHGFEDC
3 CBAZYXWVUTSRQPONMLKJIHGFED

etc.

25 YXWVUTSRQPONMLKJIHGFEDCBAZ
26 ZYXWVUTSRQPONMLKJIHGFEDCBA

The first horizontal line is the alphabet of the text. The other twenty-six lines are the cipher alphabets each corresponding to the letter of the key word which is at the left of the line.

One of the ciphers of Porta was prepared with a card of this kind:

AB	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
CD	A B C D E F G H I J K L M Z N O P Q R S T U V W X Y
EF	A B C D E F G H I J K L M Y Z A B C D E F G H I J K
etc.	
WX	A B C D E F G H I J K L M P Q R S T U V W X Y Z N O
YZ	A B C D E F G H I J K L M O P Q R S T U V W X Y Z N

In this cipher the large letters at the left correspond to the letters of the key and, in each alphabet, the lower letter is substituted for the upper and vice versa. For example, with key BAD to encipher WILL we would get JVXY. Note that with either B or A as the key letter, the first alphabet would be used.

A combination of the Vigenere and Porta ciphers is this:

A	ABCDEFGHIJKLMNOPQRSTUVWXYZ ABCDEFGHIJKLMNOPQRSTUVWXYZ
BC	ABCDEFGHIJKLMNOPQRSTUVWXYZ BCDEFGHIJKLMNOPQRSTUVWXYZA
DE	ABCDEFGHIJKLMNOPQRSTUVWXYZ CDEFGHIJKLMNOPQRSTUVWXYZAB
etc.	
VW	ABCDEFGHIJKLMNOPQRSTUVWXYZ LMNOPQRSTUVWXYZABCDEFGHIJK
XY	ABCDEFGHIJKLMNOPQRSTUVWXYZ MNOPQRSTUVWXYZABCDEFGHIJKL
Z	ABCDEFGHIJKLMNOPQRSTUVWXYZ NOPQRSTUVWXYZABCDEFGHIJKLM

Here again the large letters at the left correspond to the letters of the key and, in each pair of alphabets, the upper one is that of the plain text and the lower is that of the cipher.

This cipher can also be operated by a fixed and sliding alphabet.

Fixed Alphabet of Text:

ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Sliding Alphabet of Cipher

V **Index**

BDFHJLNPRTVX

A Z **Letters of Key.**

CEGIKMOQSUWY

The other ciphers mentioned are merely variations of these that have been discussed. It is immaterial, in the following analysis, which variety has been used. The analysis is really based on what can be done with a cipher made up with a mixed cipher alphabet which may be moved with reference to the fixed alphabet of the text, (See Case 7-b). Clearly this is a much more difficult proposition than dealing with a cipher in which the cipher alphabets run in their regular sequence, either backward or forward. In fact, in the analysis of Case 7, we may consider any cipher prepared by the method of Vigenere or any of its variations as a special and simple case.

It was long ago discovered that, in any cipher of this class, (1) two like groups of letters in the cipher are most probably the result of two like groups of letters of the text enciphered by the same alphabets and (2) the number of letters in one group plus the number of letters to the beginning of the second group is a multiple of the number of alphabets used. It is evident, of course, that we may have similar groups in the cipher which are not the result of en-

ciphering similar groups of the text by the same alphabets but if we take all recurring groups in a message and investigate the number of intervening letters, we will find that the majority of such cases will conform to these two principles.

Changing the key word and message to illustrate more clearly the above points, the following is quoted from the Signal Book, 1914, with reference to the use of the cipher disk in preparing a message with a key word.*

"—This simple disk can be used with a cipher word or, preferably, cipher words, known only to the correspondents. ....Using the key word 'disk' to encipher the message 'Artillery commander will order all guns withdrawn,' we will proceed as follows: Write out the message to be enciphered and above it write the key word.... letter over letter, thus:

DISK	DISK	DISK	DISK	DISK	DISK	DISK	DISK	DISK	DISK	DIS
ARTI	LLER	YCOM	MAND	ERWI	LLOR	DERA	LLGU	NSWI	THDR	AWN
DRZC	SXOT	FGEY	RIFH	ZRWC	SXET	AEBK	SXMQ	QQWC	KBPT	DMF

"Now bring the 'a' of the upper disk under the first letter of the key word on the lower disk, in this case 'D'. The first letter of the message to be enciphered is 'A': 'd' is found to be the letter connected with 'A', and it is put down as the first cipher letter. The letter 'a' is then brought under 'I' which is the second letter of the key word. 'R' is to be enciphered and 'r' is found to be the second cipher letter. . . . . Proceed in this manner until the last letter of the key word is used and beginning again with the letter 'D', so continue until all letters of

*The method used is not the most satisfactory one for several reasons and a better method is that of writing the message in multiples of the key and enciphering the columns as already described.

the message have been enciphered. Divided into groups of five letters, it will be as follows:

"DRZCS XOTFG EYRIF HZRWC SXETA EBKSX MQQQW CKBPT DMF."

So much for the Signal Book; now let us examine the above message for pairs or similar groups and count the intervening letters to demonstrate principles (1) and (2);

CSX—CSX	16=4x4
SX— SX	16=4x4
SX— SX	8=2x4
WC—WC	16=4x4

The key word might contain 2, 4 or 8 letters from the evidence but we may eliminate 2 as unlikely and preparation of frequency tables of each of the four alphabets would soon show that 4 is the correct number.

A later and more extensive example (Case 7-a) will show pairs not separated by multiples of the number of alphabets used, but the evidence in nearly every case will be practically conclusive. Especially is this so if chance assists us by giving groups of three or more letters like the group CSX in the above example. The number of alphabets having been determined each alphabet is handled by the methods of Case 6 already discussed.

CASE 7-a.—The following message appeared in the "personal" column of a London paper:

"M. B. Will deposit £27 14s 5d tomorrow,"

and the next day we find this one:

(Cipher on next page.)

M.B. CT OSB UHGI TP IPEWF H CEWIL NSTTLE FJNVX XTYLS FWKKHI BJLSI SQ VOI BKSM XMKUL SK NVP-ONPN GSW OL. IEAG NPSI HYJISFZ CYY NPUXQG TPRJA VXMXI AP EHV-PPR TH WPPNEL. UVZUA MMYVSF KNTS ZSZ UAJPQ DLMMJXL JR RA PORTELOGJ CSULTWNI XMKUHW XGLN ELCPOWY OL. ULJTL. BVJ TLBWTPZ XLD K ZISZNK OSY DL RYJUAJSSGK. TLFNS UVD VV FQGCYL FJHVSI YJL NEXV PO WTOL PYYYHSH GQBOH AGZTIQ EYFAX YPMP SQA CI XEYVXNPPAII UV TLFTWMC FU WBWXGUHIWU. AIIWG HSI YJVTI BJV XMQN SFX DQB LRTY TZ QTXLNISVZ. GIFT AII UQSJGJ OHZ XFOWFV BKAI CTWY DSWTLTTT-PKFRHG IVX QCAFV TP DIIS JBF ESF JSC MCCF HNGK ESBP DJPQ NLU CTW ROSB CSM.

The messages in question appeared in an English newspaper. It is fair to presume then that the cipher is in English. This is checked negatively by the fact that it contains the letter W which is not used in any of the Latin languages and that the last fifteen words of the message consist of from two to four letters each, an impossible thing in German. It contains 108 groups which are probably words, as there are 473 letters or an average of 4.4 letters per group, while we normally expect an average of about 5 letters per group. The vowels AEIOU number 90 and the letters JKQXZ number 78. It is thus a substitution cipher (20% of 473=94.6).

Recurring words and similar groups are AIIWG, AII; BKSM, BKAI; CT, CTWY, CTW; DLMMJXL, DL; ESF, ESBP; FJNVX, FJHVSI; NPSI, NPUXQG; OSB, OSY, ROSB; OL, OL; PORTELOGJ, PO; SQ, SQA; TP, TP; TLBWTPZ, TLFNS, TLFTWMC; UVZUA, UVD, UV; XMKUL, XMKUHW; YJL, YJVTI.

Frequency Table for the Message

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
15	13	15	8	13	20	16	16	30	21	13	27	14	19	15	26	13	9	33	30	17	12	19	20	19	11

This clearly eliminates Cases 4, 5 and 6.

Referring to the recurring words and groups above noted, we figure the number of letters between each.

AII...AII	45=3 x 3 x 5	OSB...OSB	465=31 x 3 x 5
BK...BK	345=23 x 3 x 5	PO...PO	105=7 x 3 x 5
CT...CT	403 No factors	SQ...SQ	250=2 x 5 x 5 x 5
CTW...CTW	60=2 x 2 x 3 x 5	TLF...TLF	80=2 x 2 x 2 x 2 x 5
DL...DL	75=3 x 5 x 5	TP...TP	405=3 x 3 x 3 x 3 x 5
ES...ES	14=2 x 7	UV...UV	115=23 x 5
FJ...FJ	187 No factors	XMKU...XMKU	120=2 x 2 x 2 x 3 x 5
NP...NP	14=2 x 7	UV...UV	73 No factors
OL...OL	120=2 x 2 x 2 x 3 x 5	YJ...YJ	85=17 x 5
OS...OS	220=11 x 2 x 2 x 5		

The dominant factor is clearly 5, so we may consider that five alphabets were used, indicating a keyword of five letters. Writing the message in lines of five letters each and making a frequency table for each of the five columns so formed, we find the following:

Frequency Tables

Colum	*Column 2*	*Column 3*	*Column 4*	*Column 5*
A 11	A 111111111	A 1	A 1	A 11
B	B 111	B 111	B	B 1111111
C 1111111	C 1	C 111	C 1111	C
D 11	D 11	D 1	D	D 111
E 1111	E	E 11	E 1111111	E
F 111	F	F 111111111	F III	F 11111
G 111111111	G	G 111	G II	G 11
H 111	H 11111	H 111	H 111	H 11
I 11	I 11	I 1111111	I 11111111111111111	I 11
J 11111	J 1	J 111111	J	J 111111111
K 111111	K 11111	K	K 1	K 1
L	L 1111111111111111111	L 11	L 11111	L 1
M	M	M 1111111	M IIII	M 111
N 1111111	N 111	N 1111	N	N 11111
O 11111	O	O 111111111	O 1	O
P 1111111	P 1111111	P 11111111	P 1111	P
Q 11111	Q	Q	Q 11	Q 111111
R	R 1	R 1	R 111111	R 1
S	S 11111111	S 111111	S 111111111111	S 1111111
T 1111111	T 111	T 11111	T 1	T 11111111111111
U 1111111	U 111	U 111111	U	U 1
V 11111	V	V II	V 11111	V
W 111	W 1111	W	W 11111	W 1111111
X 11	X	X 1111	X 11111111	X 111111
Y 1111	Y 11111	Y	Y 111	Y 1111111
Z	Z 11111	Z 111	Z	Z 111

In the table for Column 1, the letter G occurs 9

times. Let us consider it tentatively as E. Then if the cipher alphabet runs regularly and in the direction of the regular alphabet, C (7 times)=A and the cipher alphabet bears a close resemblance to the regular frequency table. Note TUV (=RST) occurring respectively 7, 7, and 5 times and the non-occurrence of B, L, M, R, S, Z, (=Z, J, K, P, Q, and X respectively.)

In the next table, L occurs 19 times and taking it for E with the alphabet running in the same way, A=H. The first word of our message, CT, thus becomes AM when deciphered with these two alphabets and the first two letters of the key are C H.

Similarly in the third table we may take either F or O for E, but a casual examination shows that the former is correct and A=B (even if we were looking for a vowel for the next letter of the keyword).

In the fourth table, I is clearly E and A=E. The fifth table shows T=14 and J=9. If we take T=E we find that we would have many letters which should not occur. On the other hand, if we take J=E then T=O and in view of the many E's already accounted for in the other columns, this may be all right. It checks as correct if we apply the last three alphabets to the second word of our message, OSB, which deciphers NOW. Using these alphabets to decipher the whole message, we find it to read:

"M. B. Am now safe on board a barge moored below Tower Bridge where no one will think of looking for me. Have good friends but little money owing to action of police. Trust, little girl, you still believe in my innocence although things seem against me. There are reasons why I should not be questioned. Shall try to embark before the mast in some outward bound vessel. Crews will not be scrutinized so sharply as passengers. There are those who will let you know my movements. Fear the police may

tamper with your correspondence but later on when hue and cry have died down will let you know all."

The key to this message is CHBEF which is not intelligible as a word but if put into figures indicating that the 2d, 7th, 1st, 4th, and 5th letter beyond the corresponding letter of the message has been used the key becomes 27145 and we may connect it with the "personal" which appeared in the same paper the day before reading:

"M. B. Will deposit £27 14s 5d tomorrow."

CASE 7-b

Message

DDLRM ERGLM UJTLL CHERS LSOEE SMEJU
ZJIMU DAEES DUTDB GUGPN RCHOB EQEIE
OOACD EIOOG COLJL PDUVM IGIYX QQTOT
DJCPJ OISLY DUASI UPFNE AECOB OESHO
BETND QXUCY LUQOY EHYDU LXPEQ FIXZE
PDCNZ ENELQ MJTSQ ECFIE ARNDN ETSCF
IFQSE TDDNP UUZHQ CDTXQ IRMER GLXBE
IQRXJ FBSQD LDSVI XUMTB AEQEB YLECO
IYCUD QTPYS VOQBL ULYRO YHEFM OYMUY
ROYMU EQBLV UBREY GHYTQ CMUBR EQTOF
VSDDU DAFFS CEBSV TIOYE TCLQX DVNLQ
XYTSI MZULX BAXQR ECVTD ETGOB CCUYF
TTNXL UNEFS IVIJR ZHSBY LLTSI

On the preliminary determination, we have the following count of letters out of a total of 385:

	A 8		L 23		J 9
	E 38		N 11		Q 22
	I 19		R 14		V 9
	O 21		S 20		X 13
	U 24		T 21		Z 6
Total	110	Total	89	Total	59
	28%		23%		15%

Every letter except K and W occurs at least six times. We may say then that it is a substitution cipher, Spanish text, and certainly not Case 4, 5 or 6. We will now analyze it for recurring pairs or groups

to determine, if it be Case 7, how many alphabets were used. The following is a complete list of such recurring groups and pairs with the number of letters intervening and the factors thereof. In work of this kind, the groups of three or more letters are always much more valuable than single pairs. For example, the groups, HOBE, OYMU, RMERGL and UBRE show, without question, that six alphabets were used. It is not necessary, as a rule, to make a complete list like the following:

AE 74=2x37
AE 120=2x2x2x3x5
BE 88=2x2x2x11
CD 132=2x2x3x11
CFI 12=2x2x3
CH 36=2x2x3x3
CO 42=2x3x7
CO 126=2x3x3x7
CU 114=2x3x19
DD 186=2x3x31
DD 116=2x2x29
DE 285=5x57
DL 218=2x109
DN 14=2x7
DQ 120=2x2x2x3x5
DU 36=2x2x3x3
DU 24=2x2x2x3
DU 38=2x19
DU 165=3x5x11
EA 30=2x3x5
EB 78=2x3x13
EC 180=2x2x3x3x5
ECO 126=2x3x3x7
EES 14=2x7
EF 105=3x5x7
EI 8=2x2x2
EI 152=2x2x2x19
EQ 88=2x2x2x11
EQ 264=2x2x2x3x11
EQ 44=2x2x11
EQE 176=2x2x2x2x11
IE 110=2x5x11
IM 302=2x151
IO 250=2x5x5x5
IX 78=2x3x13
LY 158=2x79
JT 150=2x3x5x5
LL 367 No factors
LQ 164=2x2x41
LQX 6=2x3
LU 124=2x2x31
LU 110=2x5x11
LU 234=2x3x3x13
LX 66=2x3x11
LXB 132=2x2x3x11
LY 158=2x79
ME 22=2x11
MU 24=2x2x2x3
MU 240=2x2x2x2x3x5
MU 18=2x3x3
ND 47 No factors
NE 48=2x2x2x2x3
NE 18=2x3x3
NE 192=2x2x2x2x2x2x3
OB 6=2x3
OB 234=2x3x3x13
OE 93=3x31
OI 144=2x2x2x2x3x3
OO 7 No factors
OY 6=2x3
OY 46=2x23
OYMU 6=2x3
RE 50=2x5x5
RMERGL 198=2x3x3x11
SC 132=2x2x3x11
SD 262=2x131
SI 230=2x5x23
SI 34=2x17
SI 264=2x2x2x3x11
SI 12=2x2x3
SL 78=2x3x13
SQ 54=2x3x3x3
SV 27=3x3x3
SV 63=3x3x7
SV 90=2x3x3x5
TD 47 No factors
TD 165=3x5x11
TD 96=2x2x2x2x2x3
TN 239 No factors
TS 14=2x7
TS 156=2x2x3x13
TSI 50=2x5x5
UBRE 12=2x2x3
UD 60=2x2x3x5
UDA 270=2x3x3x3x5
UL 114=2x3x19
ULX 198=2x3x3x11
UY 89 No factors
UZ 162=2x3x3x3x3
VI 148=2x2x37
VT 33=3x11
XQ 114=2x3x19
XQ 144=2x2x2x2x3x3

ER 12=2x2x3	PD 75=3x5x5	XU 99=3x3x11
ES 78=2x3x13	QBL 24=2x2x2x3	YE 184=2x2x2x23
ET 135=3x3x5	QC 95=5x19	YL 106=2x53
ET 9=3x3	QE 108=2x2x3x3x3	YL 144=2x2x2x2x3x3
ET 54=2x3x3x3	QE 68=2x2x17	YM 6=2x3
ET 31 No factors	QR 132=2x2x3x11	YRO 12=2x2x3
HE 245=5x7x7	QTO 210=2x3x5x7	ZE 6=2x3
HOBE 66=2x3x11	QX 198=2x3x3x11	ZH 183=3x61

Out of one hundred and one recurring pairs we have fifty with the factors 2x3=6; out of twelve recurring triplets, nine have these factors; and the four recurring groups of four or more letters all have these factors. The percentages are respectively 49.5%, 75% and 100% and we may be certain from this that six alphabets were used. But, before the six frequency tables are made up, there is one more point to be considered; why are there so many recurring groups which do not have six as a factor? The answer is that one or more of the alphabets is repeated in each cycle; that is, a key word of the form HAVANA has been used. If this were the key word, the second, fourth and sixth alphabets would be the same. We will see later that in this example the second and sixth alphabets are the same and this introduces the great number of recurring groups without the factor 6.

We will now proceed to make a frequency table for each alphabet. As the message is written in thirty columns, we take the first, seventh, thirteenth, etc., as constituting the first alphabet; the second, eighth, fourteenth, etc., as constituting the second alphabet and so on. The prefix and suffix letter is noted for each occurrence of each letter. The importance of this will be appreciated when the form of the frequency tables is examined. None bears any resemblance to the normal frequency table except that each is evidently a mixed up alphabet. The

numbers after "Prefix" and "Suffix" refer to the alphabet to which these belong, for convenience in future reference.

Frequency Tables

First Alphabet

Letter	Prefix (6)	Suffix (2)
A 111	3 DUD	ESF
B 11111111	8 OOOFEEOS	EOESYSCY
C	0	
D 1111	4 TYT	DJUD
E 1	1 E	S
F	0	
G	0	
H	0	
I 11111111	8 EOFFEOVS	OSEFQYJ
J	0	
L 1	1 O	J
M 1	1 F	O
N 1111	4 FEDU	EEEE
O 1	1 E	O
P 11	2 GE	ND
Q 1111	4 UEOE	OFBB
R 1111111	7 EEEYYBB	GSGOOEE
S 1	1 D	V
T 11111111	8 JUJMQYVF	LDSBPQDT
U	0	
V 11	2 UF	MS
X 111111	6 YQTQQA	QUQDYQ
Y 1	1 O	E
Z 111	3 UUM	JHU

Second Alphabet

Letter	Prefix (1)	Suffix (3)
A	0	
B 111	3 TQQ	ALL
C 1	1 B	C
D 111111	6 DTPDXT	LBCNVE
E 11111111111	11 ABNBNINRRYN	EOATLATYQTF
F 111	3 QIA	IQF
G 11	2 RR	LL
H 1	1 Z	O
I	0	
J 1111	4 ZLDI	ILCR
L 1	1 T	L
M 1	1 V	I
N 1	1 P	R
O 1111111	7 OIBQRMR	AOEYYYY
P 1	1 T	Y
Q 11111	5 XXITX	OIRCR
R	0	
S 11111111	8 REIATBVB	LMLIQQDV
T 1	1 T	N
U 111	3 XDZ	CLL
V 1	1 S	I
X	0	
Y 1111	4 BIXB	LCTL
Z	0	

Third Alphabet

Letter	Prefix (2)	Suffix (4)
A 1111	4 OEEB	CERE
B 1	1 D	G
C 111111	6 JUDYQC	PYNUMU
D 1	1 S	D
E 111	3 EOD	SST
F 11	2 FE	SS
G	0	
H	0	
I 111111	6 JMSFQV	MGUXRX
J	0	
L 11111111111111	14 DGLSJSUEG YBBUY	RMCSPYXQ XEUVXL
M 1	1 S	E
N 11	2 DT	PX
O 1	1 O	G
P	0	
Q 1111111	7 EQSFHSE	ETESCDT
R 1111	4 NQQJ	CXEZ
S	0	
T 1111	4 EEEY	NSCS
U	0	
V 11	2 SD	TN
X	0	
Y 111111	6 OPOOOE	ESHMMG
Z	0	

Fourth Alphabet

Letter	Prefix (3	Suffix (5)
A	0	
B	0	
C 11111	5 LRAQT	HHDDL
D 11	2 QD	LU
E 11111111	8 MQAYQALR	JICHCQCC
F	0	
G 1111	4 BOIY	UCIH
H 1	1 Y	E
I	0	
J	0	
L 1	1 L	T
M 11111	5 LIYYC	UUUUU
N 111	3 TCV	DZL
O	0	
P 111	3 LCN	DJU
Q 1	1 L	M
R 111	3 LAI	MNM
S 111111111	9 LEETQYFTF	ODHCEVCII
T 1111	4 QQVE	OOIG
U 1111	4 ICLC	PDLY
V 1	1 L	U
X 1111111	7 LILRILN	PZBUBL
Y 11	2 LC	DLJ
Z 1	1 R	H

FIFTH ALPHABET

Letter	*Prefix (4)*	*Suffix (6)*
A	0	
B 11	2 XX	EA
C 1111111	7 GDDSDSD	OOFFOEV
D 111111	6 SCPYNCU	UEUUQTQ
E 11	2 SH	TF
F	0	
G 1	1 U	T
H 111111	6 CCSDGZ	EOOYYS
I 11111	5 EGTSS	EYOMV
J 111	3 EPX	UOF
L 111111	6 YDUCNX	UDYQQU
M 111	3 RQR	EJE
N 1	1 R	D
O 111	3 STT	ETF
P 11	0 UX	FE
Q 1	1 E	E
R	0	
S	0	
T 1	1 L	S
U 1111111111	10 MMGPXMM VMD	JDGUMYEB BD
V 1	1 S	O
X	0	
Y 1	1 U	F
Z 11	2 XN	EE

SIXTH ALPHABET

Letter	*Prefix (5)*	*Suffix (1)*
A 1	1 B	X
B 11	2 UU	RR
C	0	
D 1111	4 UNLU	ANSA
E 1111111111111	13 MHOIDPZ ZMBQUC	RREOIQPN RIBQB
F 1111111	7 PCCJEOC	NIIBMVT
G 1	1 U	P
H	0	
I	0	
J 11	2 UM	TT
L	0	
M 11	2 UI	TZ
N	0	
O 111111111	9 HCJCHCVIG	BLIBBIQYB
P	0	
Q 1111	4 DDLL	XTXX
R	0	
S 11	2 HT	BI
T 111	3 OED	DDX
U 1111111	7 JDDDLUL	ZTVAQZN
V 11	2 CI	TI
X	0 I	
Y 11111	5 IHLUH	XDRRT
Z	0	

We will now set down some of the determinations which can be made at once from these frequency tables. Clearly several mixed alphabets have been used. As was to be expected from the analysis of the recurring groups, we note that the frequency tables for alphabets 2 and 6 are of so nearly the same general form that certainly these two alphabets are one and the same. If a Spanish word has been used as a key word, this means that A is probably represented by a vowel in these two alphabets and probably equals A or O, because these two letters are such common finals in Spanish.

1st Alphabet. Probable vowels T, X; probable common consonants, B, I, N, R. We conclude this because of the frequency of occurrence of T and X and the variety of their prefixes and suffixes. On the other hand, B, I, N, and R have for prefixes and suffixes, in a majority of cases, E, F, O and S which are the probable vowels in the 2d and 6th alphabets.

2d and 6th Alphabets.—Probable vowels E, F, O, S; probable common consonants, D, J, Q, U, Y.

3d Alphabet.—Probable vowels C, I, L; probable common consonants A, Q, T, Y.

4th Alphabet.—Probable vowels, E, G, S, T; probable common consonants, C, M, N, P, U, X.

5th Alphabet.—Probable vowels, D, L, U; probable common consonants, C, H, I.

Now this cipher may have been made up from five distinct alphabets with letters chosen at random but it is much more likely to have been prepared with a cipher disk or equivalent, having the regular alphabet on the fixed disk and the mixed alphabet on the movable disk. An equivalent form of apparatus (not using the mixed alphabet in question) is one like this:

Fixed Alphabet of Text

ABCDEFGHIJLMNOPQRSTUVXYZABCDEFGHIJLMNOPQRSTUVXYZ

PCJVRQZBAODFSUTMXIYHLGEN

Movable Alphabet of Cipher

Here A of the plain text is enciphered by S and the other letters come as they will. If we move the cipher alphabet one space to the left, A will be enciphered by U and the whole sequence of the alphabet will be changed.

We will therefore use some such form as the above and see if we can insert our letters, as they are determined, in such a way as to have each of the cipher slips identical. We may start thus:

	ABCDEFGHIJLMNOPQRSTUVXYZABCDEFGHIJLMNOPQRSTUVXYZ
1st *Alphabet*	t x
2d	ol qei ms d c u
3d	ol qei ms d c u
4th	ol qei ms d c u
5th	d c u ol qei ms
6th	ol qei ms d c u

In the 1st alphabet, T and X are placed as A and E respectively on the basis of frequency. In the 2d and 6th alphabets, O and E are placed as A and E respectively on the basis of frequency. In the 4th

alphabet, E and S are placed as A and E, and in the 5th, D, U and L are placed as A, E and O for the same reason. We now have an excess of E's and a deficiency of A's, which will be corrected if, in the 3d alphabet, we place L, I and C as A, E and O respectively. As a check, this gives us TOLEDO as the key word.

In the second alphabet, O is four letters to the left of E; we may place O four letters to the left of E in the fourth and it comes under V. Note that in the fourth frequency table O (=V) does not occur. In the same way in the fourth alphabet, S is four letters to the right of E; placing it in the same position with respect to E in the second and sixth, we have S under I. We have already noted that S probably represents a vowel in these two alphabets. In this way, we may add D and U to the third alphabet from their position in the fifth with respect to L and we may add I and O to the fifth from their position in the third with respect to L. In every case we check results from the frequency tables and find nothing unlikely in the results.

Now in the second and sixth, let us try Q, D and U as D, N and R respectively. We may add these letters to the third, fourth and fifth alphabets by the method of observing the number of letters to the right or left of some letter already fixed. We now add L to the second, third, fourth and sixth from its position with reference to D and U in the fifth. M is probably D in the fourth and we may add it to each of the alphabets, except the first, in the same way. The table is now complete as shown.

Let us try these letters on the first line of the message and see if some other letters will be self-evident.

Alphabet	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6
Message	D	D	L	R	M	E	R	G	L	M	U	J	T	L	L	C	H	E	R	S	L	S	O	E
Deciphered	_	N	A	_	U	E	_	_	A	D	E	_	A	B	A	L	_	E	_	I	A	E	N	E

Alphabet	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6
Message	E	S	M	E	J	U																		
Deciphered	_	I	G	A	_	R																		

Referring to our frequency tables as a check on suppositions, we find everything agrees well enough if we assume the first line to read:

UNAFUERZA DE CABALLERIA ENEMIGA

We will now put the newly found letters in the table. The letters previously found are in capitals and the new letters in small letters. The addition of D (=U) to the first alphabet permits us to add all the letters of the other alphabets to the first by the methods already discussed. Each of the other letters may then be added to every alphabet by these methods:

```
ABCDEFGHIJLMNOPQRSTUVXYZABCDEFGHIJLMNOPQRSTUVXYZ
1st                          T   xhgoljqei msr  d c u
2d                    t   xhgOLjQEI MSr  D C U
3d                    t   xhgOLjQEI MSr  D C U
4th              t   xhgOLjQEI MSr   D C U
5th    t   xhgOLjQEI MSr   D C U
6th                    t   xhgOLjQEI MSr  D C U
```

One alphabet checks another in this way and we find everything to fit so far. We will decipher a few words more of the cipher message by the above alphabets and see if we can determine some new letters.

Alphabet

5612345612345612345612345612345612345612345612345612345612

Message

JU ZJ I MUDAEE S DUTD BGU GPN RCHOB EQ E IEO OAC DE I OOGC OL JL PDUVM IGIYXQ

Deciphered

PR CEDEN EDEARAU UEZ ILLA ECASEHA LAENAZUCAICA AR HEUS ED

Again referring to the frequency tables the first word is evidently PROCEDENTE. We have also HALLA and MARCHEUSTED. The letter B may be determined from another cipher group, JFBSQDLD (56123456) =POSICION. The letter N may be determined from BETNDQXUC (123456123) =SERRADERO. The letters F and Y may be determined from JCPJOISLYDUASIUPF (23456123456123456)=

COMPANIA PARTIENDO. The completed alphabets, arranged as before, are:

```
ABCDEFGHIJLMNOPQRSTUVXYZABCDEFGHIJLMNOPQRSTUVXYZ
1st                              TYVNXHGOLJQEIZMSRBADFCPU
2d                          TYVNXHGOLJQEIZMSRBADFCPU
3d                          TYVNXHGOLJQEIZMSRBADFCPU
4th                      TYVNXHGOLJQEIZMSRBADFCPU
5th    TYVNXHGOLJQEIZMSRBADFCPU
6th                         TYVNXHGOLJQEIZMSRBADFCPU
```

The key word is TOLEDO and the completely deciphered message is:

"Una fuerza de caballeria enemiga procedente de Aranjuez y Villaseca se halla en Azucaica. Marche usted con su compania partiendo de la casa de la serradero por las alturas de lo este y norte de Azucaica con el fin de reconocer su numero y clase de fuerzas y en disposicion que se halla. (Q) Esta acantonada (Q) Se hallan otras tropas detras de ella (Q). El resultado del reconocimiento necesito saberlo dentro de tres horas y media cuando mas. Pongo a sus ordenes un ciclista (X) Fin."

Special Solution for Case 7

When a short message is enciphered with a long key word, the methods of analysis already discussed may fail; first, because there will be no recurring pairs to indicate the number of alphabets used and, second, because there will be so few letters in each alphabet that the methods of Case 6 will not be easily applied.

However, if we know or correctly assume one word, preferably a fairly long one, in the cipher text, a solution is very simple. For example, the following message is believed to refer to reënforcements and to contain that word.

```
YANZV   ZNLPP   KQFXI   JBPWA
NRUQP   EPLOM   CCWHM   I
```

Let us assume that REINFORCEMENTS is the first word and that it is represented by the cipher group YANZVZNLPPKQFX. We may put the test in this tabular form, using a cipher disk and a Larrabee cipher card to determine the value of A for each letter under these two systems. Any other alphabets suspected may be tried out at the same time.

If

Y A N Z V Z N L P P K Q F X

equals

R E I N F O R C E M E N T S

then, with cipher disk, A equals

P E R M A N E N T B O D Y P

and, in Vigenere cipher, A equals

H W F M Q L W J L D G D M F

It is evident that the guess as to the appearance of the word REINFORCEMENTS was correct, that it is the first word of the message, that the cipher disk was used in preparing the cipher and that the key words are PERMANENT BODY.

This is, of course, an especially favorable case and we will take one less favorable to show how this method can be applied.

Two Mexican chieftains, A and B, have been communicating with the following cipher alphabet:

Plain text	ABCDEFGHIJLMNOPQRSTUVXYZ
Cipher	PCJVRQZBAODFSUTMXIYHLGEN

This alphabet has been determined from many radio messages from A, the superior, to B, his subordinate, who has a force of about 2,000 men near the border. A uses the form ORDENO QUE instead of the more familiar MANDO QUE in all his messages giving orders to B. The following message is received from A by B's radio station (and other listening stations) and about an hour

later there is a good deal of noise and movement as if B's force were breaking camp.

IIHAH	YDXRP	EGQGV	JJEEE	HOBGV
GJCAG	XAESA	VVXLE	IILHM	PSQAG
BDGAV	GSQAZ			

This is a substitution cipher, but it is not Case 6 using the usual alphabet of the communications from A to B and, in fact, is not Case 6 at all. The recurring pairs and triplets point to a key word of ten letters and this would give us but six letters per alphabet if it is Case 7.

The preparations for a move lead us to believe that A has given an order to B and he has, in that case, probably used the expression ORDENO QUE in the message. We will try the first nine letters of the message as in the other example, first preparing a cipher disk or equivalent sliding arrangement having on it the alphabet usually used between these chieftains or A-B cipher.

Fixed Cipher Alphabet

PCJVRQZBAODFSUTMXIYHLGENPCJVRQZBAODFSUTMXIYHLGEN

ABCDEFGHIJLMNOPQRSTUVXYZ

Sliding Plain Text Alphabet

A-B Cipher

If I equals	O then A equals	R
I	R	C
H	D	X
A	E	R
H	N	B
Y	O	Q

Clearly there is nothing here and the assumed words, if they occur, are in the middle of the message. We may jump to the combination PEGQGV at once since the preceding letters do not make ORDENO QUE. We try this without result and proceed to EGQGVJ, GQGVJJ, QGVJJE, GVJJEE,

VJJEEE, JJEEEH, JEEEHO, EEEHOB, EEHOBG, EHOBGV, HOBGVG, OBGVGJ, BGVGJC, GVGJCA, VGJCAG, all without result. This work requires less time than might be imagined and is the kind of work which can be divided among a number of operators. Now let us come to the next combination GJCAGX. We add the next three letters, AES, against QUE.

If

GJCAGX AES

equals

ORDENO QUE

Then, in the A-B cipher, A equals

ADEROV IVA

The key is found; VIVA _ADERO and a trial of M in the blank space shows correct results. This checks with our theory that a ten letter key word was used and deciphering the message we have:

PARA EL ATAQUE CONTRA TORREON ORDENO QUE SUS TROPAS MARCHEN ESTE NOCHE X.

The reason for breaking camp is now evident.

This method may be used, with some labor, on short words like THE, AND, etc. Parts of the key will appear whenever an assumed word is found in the message and the whole key may be assembled if enough of the parts are available. Even if only part of the key may be so recovered, it will always lead to the ultimate solution of the cipher by trial of the partially recovered key on the message letter by letter.

As an example of recovery of a key by use of short common words, let us refer to the message of Case 7-a. There are twenty-four groups of three letters each in this message and we will try them against THE, ARE and YOU, assuming that the Vigenere cipher is used.

	1	2	3	4	5	6	7	8	9	10	11	12
If	OSB	VOI	GSW	CYY	ZSZ	BVJ	XLD	OSY	UVD	YJL	SQA	HSI
equals	THE	THE	THE	THE	THE	THE	THE	THE	THE	THE	THE	THE
or	ARE	ARE	ARE	ARE	ARE	ARE	ARE	ARE	ARE	ARE	ARE	ARE
or	YOU	YOU	YOU	YOU	YOU	YOU	YOU	YOU	YOU	YOU	YOU	YOU
then A												
equals	VLX	CHE	NLS	JRU	GLV	IOF	EEZ	VLU	BOZ	FCH	ZJW	OLE
or	OBX	VXE	GBS	CHU	ZBV	BEF	XUZ	OBU	UEZ	YSH	SZW	HBE
or	QEH	XAO	IEC	EKE	BEF	DHP	ZXJ	QEE	WHJ	AVR	UCG	JEO

	13	14	15	16	17	18	19	20	21	22	23	24
If	BJV	SFX	DQB	AII	OHZ	IVX	JBF	ESF	JSC	NLU	CTW	CSM
equals	THE	THE	THE	THE	THE	THE	THE	THE	THE	THE	THE	THE
or	ARE	ARE	ARE	ARE	ARE	ARE	ARE	ARE	ARE	ARE	ARE	ARE
or	YOU	YOU	YOU	YOU	YOU	YOU	YOU	YOU	YOU	YOU	YOU	YOU
then A												
equals	ICR	ZYT	KJX	HBE	VAV	POT	QUB	LLB	QLY	UEQ	JMS	JLI
or	BSR	SOT	DZX	ARE	OQV	IET	JKB	EBB	JBY	NUQ	CCS	CBI
or	DVB	URD	FCH	YUO	QTF	KHD	LNL	GEL	LEI	PXA	EFC	EES

In column 5, we have, for YOU, the key BEF; column 6 gives the same key for ARE; column 10 gives the key FCH for THE and column 15 gives the same key for YOU; column 12 gives the key HBE for ARE and column 16 gives the same key for THE; column 23 gives the key EFC for YOU. The only possible key for the message is a five-letter one made up of the letters BEFCH or EFCHB or FCHBE or CHBEF or HBEFC. If the key in this case were a word, we would have no difficulty in determining it; as it is, there is no real difficulty in the matter as we may now divide the message into blocks of five letters and note that ZSZ (=YOU) form the 3d, 4th and 5th letters of a group. The corresponding key letters, BEF, are then the 3d, 4th and 5th letters of the key which must be CHBEF.

This special solution for Case 7 depends so largely on the intuition of the operator in choice of a word that it is not, in general, advisable to use it unless the message is very short and the regular methods of analysis have been tried unsuccessfully. It is, however, a wonderfully short cut in difficult cases where the other methods fail.

Chapter VIII

CASE 8. The Playfair cipher. This is the English military field cipher; as the method is published in English military manuals and as it is a cipher of proven reliability, it may be met with in general cipher work. The Playfair cipher operates with a key word; two letters are substituted for each two letters of the text.

The Playfair cipher may be recognized by the following points: (a) It is a substitution cipher, (b) it always contains an even number of letters, (c) when the cipher is divided into groups of two letters each, no group consists of the repetition of the same letter as SS or BB, (d) there will be recurrence of pairs throughout the message, following in a general way, the frequency table of digraphs of pairs, (e) in short messages there may be recurrence of cipher groups representing words or even phrases, and these will always be found in long messages.

In preparing a cipher by this method, a key word is chosen by the correspondents. A large square, divided into twenty-five smaller squares, is constructed as shown below and the letters of the key word are written in, beginning at the upper left hand corner. If any letter recurs in the key word, it is only used on the first occurrence. The remaining letters of the alphabet are used to fill up the square. It is customary to consider I and J as one letter in this cipher and they are written together in the same square.

If the key word chosen is LEAVENWORTH, then the square would be constructed as follows:

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

The text of the message to be sent is then divided up into groups of two letters each, and equivalents are found for each pair.

Every pair of letters in the square must be: Either (1) in the same vertical line. Thus in the above example each letter is represented in cipher by that which stands next below it, and the bottom letter by the top one of the same column; for instance, TY is represented by FV.

Or (2) in the same horizontal line. Each letter in this case is represented by that which stands next on its right, and the letter on the extreme right by that on the extreme left of the same horizontal line with it; for instance RH is represented by TW.

Or (3) at opposite corners of a rectangle. Each letter of the pair is represented by the letter in the other corner of the rectangle in the same horizontal line with it; for instance TS is represented by WY.

If, on dividing the letters of the text into pairs, it is found that a pair consists of the same letter repeated, a dummy letter, as X, Y, or Z, should be introduced to separate the similar letters.

If the message to be sent were "The enemy moves at dawn," it would be divided into pairs:

TH EX EN EM YM OV ES AT DA WN

and enciphered: HWAU AL AK XP TE LU VR MR HL

The message is then broken up into groups of five letters for transmission.

To decipher such a cryptogram, (knowing the key word), the receiver divides it into pairs, and

from his table finds the equivalent of these pairs, taking the letter immediately above each, when they are in the same vertical line; those immediately on the left, when in the same horizontal line; and those at opposite angles of the rectangle when this is formed.

It is evident, from the foregoing description, that any letter of the plain text may be represented in cipher by one of five letters, viz: The one next below it and the other four letters in the same horizontal line with it in the square. Take, for example, the letter D of the plain text, in combination with each of the other letters of the alphabet. We have, using the key LEAVENWORTH:

DA DB DC DE DF DG DH DI DK DL DM DN DO DP DQ DR DS DT DU DV DW DX DY DZ
MR FC FD CA FG FB GR BM CM BA MX GA CR FM GM MD BX FR CX FA BR MA FX GX

This gives D represented by B C F G M
4 4 8 4 4 times,
and, connected with these five letters representing D,
we have A R D M X B C G
5 5 2 4 5 1 1 1 times.

Note that these letters are those of the vertical column containing D plus the letters B, C and G, of the horizontal line containing D.

Lieut. Frank Moorman, U. S. Army, has developed a method for determining the letters which make up the key word in a Playfair cipher. In the first place, a key word necessarily contains vowels in the approximate proportion of two vowels to three consonants and it is also likely that a key word will contain other common letters. This key word is placed in the first row or rows. Now if a table is made, showing what letters in the cipher occur with every letter, it will be found that the letters having the greatest number of other letters in combination with them are very likely to be letters of the key

word, or in other words, letters occurring in the first or second lines. An example will make this clear:

Message

DB FN EX TZ MF TO VB QB QT OB XA OF PR TZ EQ
RH QK QV DX OK AB PR QI EL TV KE EX XS FS BP
WD BO BY BF RO EA BO RH QK QV TX GU EL AB TH
TR XN ON EA AY XH BO HN EX BS HR QB ZM SE XP
HF GZ UG KC BD PO EA AY XH BO XP HF KR QI AB
PR QI EL BX FZ BI SE FX PB RA PR QI WC BR XD
YG TB QT EA AY XH BO HN EX BS HR QB PR QI EL
BX BT HB QB NF SI SE BX NU XP BU RB XB QR OX
BA TB RH BP WD RP RO GU GX QR SE ZY OX BA EL
AX CW BY BA SX RK RO PR HB OP BD PI CN OX EM
RP KR XT EL AX CW EQ FZ SX EL RH RO PR HB UX
DA SE XN ZN GU EL BX FS DG DB TB ZL VE RH BO
RQ.

From this message, we make up the following table, considering the letters of each pair:

(Table on next page.)

First Letters of Pairs

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

From this table we pick out the letters B, E, F, O, R, T, X, as tentative letters of the key word on account of the variety of other letters with which they occur. As there are but two vowels for seven letters, we will add A to the list on account of its occurrences with B, D, E, R, and X. This leaves the letters for the bottom lines of the square as follows:

·	·	·	·	·
·	·	·	C	D
G	H	IJ	K	L
M	N	P	Q	S
U	V	W	Y	Z

Referring to the table again we find the most frequent combination to be EL, occurring 8 times, with no occurrence of LE. Now, TH is the commonest pair in plain text, and HT is not common. The fact that H occurs in the same horizontal line with L and that E and T are probably in the key, will lead us to put E in the first line over H and T in the first line over L, so as to make EL equal TH.

The next most frequent combination is PR occurring 7 times, with RP occurring twice. In the square as partially arranged, PR equals M_ or N_ or Q_ or I_. We may eliminate all these except N_, and this N_ could only be NO or NA, so that we will put, tentatively the R in the second line over H and the O and A in the same line over IJ. We have then:

·	E	·	·	T
·	R	AO	C	D
G	H	IJ	K	L
M	N	P	Q	S
U	V	W	Y	Z

Let us now check this by picking out the combinations beginning with EL and seeing if the table will solve them. We find, ELTV, ELAB, ELBXFZ, ELBXBT, ELAXCWBY, ELAXCWEQ, ELRH, ELBXFS. Now, on the assumption that the letter after EL represents E, we have it represented by A three times, B three times, R once and T once. This re-

quires that A and B be put in the same horizontal line with E, since T is already there, and R is tentatively under E.

The combination ELTV now equals THEZ. If the T were moved one place to the left, it would be THEY, a more likely combination, but this requires the L to be moved one place to the left also, by putting I or K in the key word and taking out O, R or X and returning it to its place in the alphabetical sequence. The most frequent pairs containing O are B O six times, R O four times, and O X three times. Now these pairs equal respectively E N, E S and H E, if O is put between N and P in the fourth line. We will therefore cease to consider it as a letter of the the key word. The combination ELAB can only be THE_ on the assumption that A is the first letter to the right of E. The combination ELBX occurs three times. If it represents THE _, the B must be the first letter of the first line and the X must now be placed under E where the R was tentatively put. We can get THE _out of ELRH by putting R in the first line or leaving it where it is, but the preponderance of the BX combination should suggest the former alternative.

A new square showing these changes will look like this:

B	E	A	T	R
.	X	.	.	.
G	H	.	L	M
N	O	P	Q	S
U	V	W	Y	X

As I put in the space under B will give the word BEATRIX and as a vowel is clearly necessary there, we will so use the IJ and leave K between H and L. This leaves C, D and F to be placed. It appeared at

first that F was in the key but if it is in the second line, in proximity to the letters of the first line, it will give the same indications. Completing the square then, we have

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

With this square, the message is deciphered without difficulty.

"It is very frequently neces(x)sary to employ ciphers and they have for many centuries been employed in the relations betwe(x)en governments, for com(x)munication betwe(x)en com(x)manders and their subordinates and particularly betwe(x)en governments and their agents in foreign countries; there are many cases in history where the capture of a message not in cipher has made the captors of the message victorious in their military movements."

It will be seen that the method of Lieut. Moorman enabled us to pick out six letters of the key word out of eight letters chosen tentatively. The reason for the appearance of F has already been noted; the letter O occurred with many other letters because it happened to remain in the same line with N and S and to be under H. It thus was likely to represent any of these three letters which occur very frequently in any text.

Two-character Substitution Ciphers

CASE 9.—Two-character substitution ciphers. In ciphers of this type, two letters, numerals, or conventional signs, are substituted for each letter of the text. There are many ways of obtaining the char-

acters to be substituted but, in general, these ciphers may be considered as special varieties of Case 6 or Case 7. The ciphers which come under this case are not well suited to telegraphic correspondence because the cipher message will contain twice as many letters as the plain text. However they are so used; an example is at hand in which two numerals are substituted for each letter and this makes transmission by telegraph very slow.

Case 9 can be recognized by some or all of the following points; the number of characters in the cipher is always an even number; often only a few, say five to ten, of the letters of the alphabet appear; either a frequency table for pairs of the cipher text resembling the normal single letter frequency table can be made, or groups of four letters will show a regular recurrence, from which the cipher can be solved as in Case 7.

CASE 9a.—

Message

RNTGN RAAGR NARNA GTGRA TGAAN NANGG
RARAT NAANR NNNRN AAAGG AANGR NGGNN
NRNAA AANRA TNANN NGGRN RNNRG TTGRG
TGGRN ARNTG NNART GGRNR GRNNT GTGAA
NNARN ARNRT TGAGG GAAAA NANNA RNAGA
NGNAT NNNAT

This message contains 160 letters and it will be noted that the only letters used are A, G, N, R and T.

We may expect a simple two-letter substitution cipher at once. It will simplify the work if we divide the cipher into groups of two letters and then, if we find there are 26 or less recurring groups, to assign an arbitrary letter to each group and work out the cipher by the method of Case 6.

RN TG NR AA GR NA RN AG TG RA TG AA NN AN GG
RA RA TN AA NR NN NR NA AA GG AA NG RN GG NN
NR NA AA AN RA TN AN NN GG RN RN NR GT TG RG
TG GR NA RN TG NN AR TG GR NR GR NN TG TG AA
NN AR NA RN RT TG AG GG AA AA NA NN AR NA GA
NG NA TN NN AT

With arbitrary letters substituted, we have

A B C D E F A G B H B D I J K
H H L D C I C F D K D M A K I
C F D J H L J I K A A C N B O
B E F A B I P B E C E B B D
I P F A Q B G K D D F I P F R
M F L I S

Now, preparing a frequency table, with note of prefixes and suffixes we have:

		Frequency	*Prefix*	*Suffix*
A	7	1111111	FMKAFF	BGKACBQ
B	10	1111111111	AGHNOAPIBQ	CHDOEIEBDG
C	6	111111	BDIIAE	DIFFNE
D	9	111111111	CBLFKFBKD	EICKMJIDF
E	4	1111	DBBC	FFCI
F	8	11111111	ECCEPDPM	ADDAAIRL
G	2	11	AB	BK
H	4	1111	BKJH	BHLL
I	9	111111111	DCKJBEDFL	JCCKPBPP
J	3	111	IDL	KHI
K	5	11111	JDAIG	HDIAD
L	3	111	HHF	DJI
M	2	11	DR	AF
N	1	1	C	B
O	1	1	B	B
P	3	111	III	BFF
Q	1	1	A	B
R	1	1	F	M
S	1	1	I	

A brief study of this table and the distribution in the cipher leads to the conclusion that B, F and C are certainly vowels and are, if the normal frequency holds, equal to E, O, and A or I. Similarly D and I are consonants and we may take them as N and T. I is taken as T because of the combination IP (=possibly TH) occurring three times. The next letter in order of frequency is A; it is certainly a consonant and may be taken as R on the basis of its frequency. Let us now try these assumptions on the first two lines of the message. We have

R E $\begin{smallmatrix}A\\I\end{smallmatrix}$ N _ O R _ E _ E N T _ _ _ _ _ _ N $\begin{smallmatrix}A\\I\end{smallmatrix}$ T $\begin{smallmatrix}A\\I\end{smallmatrix}$ O N _ N _

This is clearly the word REINFORCEMENTS and, using the letters thus found, the rest of the line becomes AMMUNITIONAND. We have then the following letters determined:

Arbitrary letters	A B C D E F G H I J K L M
Plain Text	R E I N F O C M T S A U D

If these be substituted we have for the message:

REINFORCEMENTS AMMUNITION AND RATIONS MUST ARRI E EFORE T E FIFTEENT OR E CANNOT O D OUT .

From this the remainder of the letters are determined:

Arbitrary letters	N O P Q R S
Plain text	V B H W L X

Now let us substitute the two-letter groups for the arbitrary letters:

Arbitrary letters	K O G M B E P C R H D F A J I L N Q S
Two-letter groups	GG RG AG NG TG GR AR NR GA RA AA NA RN AN NN TN GT RT AT
Plain text	A B C D E F H I L M N O R S T U V W X

It is evident that the cipher was prepared with the letters of the word GRANT chosen by means of a square of this kind:

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

Thus TG=E, AN=S, etc., as we have already found.

CASE 9-b

Message

1950492958	3123252815	4418452815	2048115041
2252115345	5849134124	5028552526	5933195222
5245113215	6215584143	2861361265	2945565015
2342455850	6345542019	1550185311	2115415828
1124174553	4554205950	2552454132	1533492048
5018152364			

An examination of the groups of two numerals each which make up this message, shows that we have 11 to 36 and 41 to 65 with eleven groups missing. Now the 11 to 36 combination is a very familiar one in numeral substitution ciphers (See Case 6-c) and it

will be noted that 41 to 66 would give us a similar alphabet. Let us make a frequency table in this form:

Group	*Frequency*	*Group*	*Frequency*
11	11111	41	11111
12	1	42	1
13	1	43	1
14		44	1
15	111111111	45	111111111
16		46	
17	1	47	
18	111	48	11
19	111	49	111
20	1111	50	11111111
21	1	51	
22	11	52	1111
23	111	53	111
24	11	54	11
25	111	55	1
26	1	56	1
27		57	
28	11111	58	11111
29	11	59	11
30		60	
31	1	61	1
32	11	62	1
33	11	63	1
34		64	1
35		65	1
36	1	66	

Each of these tables looks like the normal frequency table except for the position of 20 and 50 which should represent T, by all our rules, and should be apparently 30 and 60. But suppose we put the alphabet and corresponding numerals in this form:

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

Then A=11 or 41, J=10 or 40 and T=20 or 50 as we found. Using the above alphabet, the message may easily be read. Note that this cipher is made up of ten characters only, the Arabic numerals.

CASE 9c—

Message

1156254676	2542294432	1949294015	1423217211	2979703115
4924213511	7424147875	7646252444	5143254845	3179742533
4055461512	7573227945	1627481511	7042351944	1378252149
2514764553	1548342126	7215254075	1611257845	4642217415
4952197929	7015242143	2925444933	1970187531	4079254829
4551491411	7321171554			

An examination of this message shows it to consist of forty-four different two-figure groups running from 11 to 79. Let us prepare a frequency table of these groups.

Group	*Frequency*	*Group*	*Frequency*	*Group*	*Frequency*
11	111111	31	111	51	11
12	1	32	1	52	1
13	1	33	11	53	1
14	1111	34	1	54	1
15	111111111	35	11	55	1
16	11	36		56	1
17	1	37		57	
18	1	38		58	
19	1111	39		59	
20		40	1111	70	1111
21	1111111	41		71	
22	1	42	111	72	11
23	1	43	11	73	11
24	1111	44	1111	74	111
25	11111111111	45	11111	75	1111
26	1	46	1111	76	111
27	1	47		77	
28		48	1111	78	111
29	111111	49	111111	79	11111
30		50			

We at once note the resemblance between the frequency tables for the groups 11 to 19 and 21 to

29; for the groups 30 to 36 and 50 to 56; and for the groups 40 to 49 and 70 to 79. Also the groups 11 to 19 and 21 to 29 have a frequency fitting well with the normal frequency table of the letters A to I; the groups 41 to 49 and 71 to 79 have a frequency fitting well with the normal frequency table of the letters K to S; and the groups 31 to 36 and 51 to 56 have a frequency fitting well with the normal frequency table of the letters U to Z. We have J and T unaccounted for, but note what occurred in Case 9-b and that 40 and 70 would correspond well with T if they followed respectively 49 and 79. We may now make up a cipher table as follows.

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

and this table will solve the cipher message.

In ciphers coming under case 9-b and 9-c, it is not uncommon to assign some of the unused numbers such as 85, 93, etc., to whole words in common use or to names of persons or places. In case such groups are found, the meaning must be guessed at from the context; but if many messages in the same cipher are available, the meaning of these groups will soon be obtained. The appearance of such odd groups of figures in a message does not interfere materially with the analysis, and it will be apparent at once on deciphering the message that they represent whole words instead of letters.

Chapter IX

Other Substitution Methods

The foregoing cases by no means exhaust the possibilities of the substitution cipher but they cover practically all methods which are satisfactory for military purposes, having in mind conservation of time, the minimizing of mental strain, and the requirements that complicated apparatus and rules be avoided, and that the resulting cipher should be adapted to telegraphic correspondence.

A message may be re-enciphered two or more times using a different key word each time or it may be enciphered by one method and re-enciphered by another method, using the same or a different key word. Complicated cipher systems requiring the memorizing of, or reference to, numerous rules have been devised for special purposes. Such systems usually fail utterly if there are any errors in transmission and it will be seen later that such errors are very common.

There are several ingenious cipher machines by which complicated ciphers can be formed, but if the apparatus is available and fairly long messages are at hand for examination, it is usually possible to solve them. Such machines are not, as a rule, simple and small enough for field use; and it must always be remembered that a machine cipher operates on certain mechanical cycles, which can be determined if the machine is available.

A book by Commandant Bazeries, entitled "Etude sur la Cryptographie Militaire," and a series of

articles by A. Collon, entitled "Etude sur la Cryptographie," which appeared in the Revue de L'Armée Belge, 1899-1902, give illustrations and details of operation of several of these cipher machines and the latter goes into the methods of deciphering messages enciphered with them. These methods of analysis require long messages, and as each one is adapted only to the product of a certain machine or apparatus, it is not considered advisable to include a discussion of them here. Those interested in such advanced cipher work must refer to these and other European authors on the subject.

The requirement that cipher messages should be adapted to telegraphic transmission, practically excludes ciphers in which three or more letters or whole words are substituted for each letter of the plain text. Such ciphers might be used for the transmission of very short messages but in no other case.

The cipher of Case 7, with a key word or phrase longer than one-fourth of the message, the cipher after the method of Case 7, using a certain page of a book as a key, and the cipher with a running key, where each letter of the cipher is the key for enciphering the next letter, all look safe and desirable, theoretically, but, practically, the work of enciphering and deciphering is hopelessly slow, and errors in enciphering or transmission make deciphering very difficult. Incidentally the first and second of these ciphers can be solved by the special solution for Case 7, and the third can be solved by trying each of the twenty-six letters of the alphabet as the first key letter, and then continuing the work for five or six letters of the cipher. When the proper primary key letter is found, the solution of the next five or six letters of the cipher will make sense, and thereafter the cipher offers no difficulty.

There are numerous other methods of preparing what is virtually a very long, or even an indefinitely long key from a short key word, but all such cipher methods have the same practical disadvantages of slowness of operation and difficulty in deciphering, if errors of enciphering or transmission have been made.

The ciphers of Napoleon were long series of numbers representing letters, syllables and words. They were really codes; and a code based on these principles, but using letters instead of numerals, might be evolved very easily. The War Department Code, the Western Union Code, and, in fact, all codes are nothing but specialized substitution ciphers in which each code word represents a letter, word or phrase of the plain text.

Combined Transposition and Substitution Methods

It is evident that a message can be enciphered by any transposition method, and the result enciphered again by any substitution method, or vice versa. But this takes time and leads to errors in the work, so that, if such a process is employed, the substitution and transposition ciphers used are likely to be very simple ones which can be operated with fair rapidity.

On preliminary determination, a cipher prepared by such a combination of methods will appear to be a substitution cipher to be solved as such. The frequency table of the result will resemble the normal frequency table, although the message will still be unintelligible and we will know at once that it is a transposition cipher for further solution.

The substitution methods usually found in combination ciphers are those of Case 4, 5 and 6, and the transposition method is nearly always Case 1, and particularly the simple varieties of this case like the

fence rail (Case 1-i), reversed writing or vertical writing.

A few examples will show some of the possible combinations.

The first line of the message of Case 4-a is:

OBQFOBPBRP

We might write it BFBBPOQOPR (Case 1-i),
or PRBPBOFQBO (Case 1, reversed writing),
or OFQBOPRBPB (Case 1, reversed by groups of five).

The first line of the message of Case 2-b is:

SLCOF WEETN EBRDO ORVYM FFEDI

We might write it TMDPG XFFUO FCSEP PSWZN GGFEJ,
or RKBNE VDDSM DAQCN NQUXL EEDCH (Case 4-a, going forward one letter or back one letter).

These examples give an idea of the use of combination methods. It is very rare to find both complicated transposition and substitution methods used in combination, If one is complicated, the other will usually be very simple; and ordinarily both are simple, the sender depending on the combination of the two to attain indecipherability. It is evident how futile this idea is.

Methods of Enciphering Numerals

It is frequently desirable to send numerals in the body of a cipher message. Several cipher systems prescribe that all numerals in the body of a message must be spelled out; and, while there is no doubt but that this insures greater accuracy, it also greatly increases the length of such messages. In most systems in which it is permissible to send numerals, the following system is used. An indicator, one of the little used letters and especially X, is interpolated before and after the numeral or numerals to be enciphered, and then, for each numeral, a letter is substituted using this or a similar table:

1 2 3 4 5 6 7 8 9 0
A B C D E F G H I J

The enciphering of the message then proceeds, dealing with the indicator and substituted letters as if they were the letters of a word. The decipherer arriving at an X, a series of the letters of the above table and another X, casts out the X's and substitutes numbers for the letters.

Sometimes no indicator is used, but the system of substitution of a certain letter for each numeral is followed. Again, the indicator NR may be used instead of a single letter.

Conventional letters may also be substituted for special characters like ? , $, " , - , and periods and commas, but this is rarely done except for the period and question mark. The context will usually determine the meaning of such letters when found. In this connection, the use of X to represent end of a sentence and Q to represent a question mark is quite common.

Chapter X

Errors in Enciphering and Transmission

One of the most difficult tasks before the cipher expert, is the correction of errors which creep into cipher texts in the process of enciphering and transmission by telegraph or radio.

In some cipher methods a mistake in enciphering one letter, or the omission of one letter, will so mix up the deciphering process that only one familiar with such errors can apply the necessary corrections.

The transmission of cipher text over the telegraph or by radio is a slow process, and many fairly good operators cannot receive such matter satisfactorily, because they listen for words and guess at letters at times. The spaced letters in American Morse are the cause of so many errors in code transmission that the War Department Code does not employ any groups using them. In fact, this code is limited to the letters

A B D E F G I K M N S T U X

so that there may be a minimum of such confusion.

In cipher work it is necessary, under ordinary circumstances, to use any or all of the letters of the alphabet. To assist operators in keeping the text straight, it is customary to divide cipher text into groups of four, five, six or ten letters, and usually groups of five letters are used. The receiving operator may then expect five letters per group, and if he receives more or less he is sure that either he or the sending operator has made an error. This division into groups of a constant number of letters eliminates word forms and, in the mind of the non-expert, in-

creases the difficulty of solving the cipher. But the increase in difficulty is more apparent than real; particularly, as a cipher examiner habitually finds himself dealing with ciphers without word forms, and the occurrence of a cipher with word forms usually means that he has an easy one to handle.

Messages are occasionally encountered which consist partly of plain text and partly of cipher. The cipher part may or may not retain its word forms, but, when this method is used, it is clearly impossible to have a fixed number of letters in each cipher group if the word forms are not used. It is almost impossible to prevent errors of transmission in such messages, and it often requires considerable skill and labor to correct them.

For those unfamiliar with the telegraph alphabets, they are given below. Messages sent by commercial or military telegraphs or buzzer lines will be transmitted with the American Morse alphabet. Those sent by radio, visual signalling or submarine cable will be transmitted by Continental Morse, known also as the International Code. Messages may be transmitted by both alphabets in course of transmission. For example, a cablegram from the Philippines to Nome, Alaska, will be transmitted by Continental Morse (commercial cable) from Manila to San Francisco, by American Morse (commercial land line) from San Francisco to Seattle, by Continental Morse (military cable) from Seattle to Valdez, by American Morse (military land line) from Valdez to Nulato and by Continental Morse (military radio) from Nulato to Nome.

Prior to February, 1914, the Mexican government telegraph lines used an alphabet differing slightly from the American and Continental Morse. However, at that time, the Continental Morse alphabet was prescribed for use on these lines and

it is believed that the use of the old alphabet has entirely ceased on Mexican lines. However, skilled American operators would have no difficulty in picking up this alphabet if it were found to be in use.

Radio communication is, by International Convention, invariably in Continental Morse.

Telegraph Alphabets

Character	*American Morse*	*Continental Morse or International Code*
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	. . - - .	. . - - -
3	. . . - .	. . . - -
4	. . . . -	. . . . -
5	- - -	. . . . .
6	. . . . .	- . . . .

7	- - - .	- - - . .
8	- - - - .	- - - - .
9	- - - -	- - - - -
0	——	- - - - -
Period	. . - - - .	. . . . .
Question Mark	- - - - .	. . - - - .
Comma	. - - -	. - . - . -

The following example will show some of the errors that creep into messages prepared with the cipher disk and transmitted by radio:

Message

Radio Douglas de El Paso, 2 H 71, twenty-fifth, 9:00 a.m., Govt. To C.O., Sixth Brigade, Douglas, Arizona:

JPRZI	RDJSG	XTRMJ	USFPC	RECLA	BCPCB	OAXPK
QEQKF	PPZAE	BKUTT	JHWEU	AHPZE	EZOLT	HKXPH
KIHAV	DRODN	IAPZC	LVUMP	KFUBV	VTVNV	EFVZV
TLVQS	BKAHQ	NVKVF	MGJTH	OWBGN	WWEPO	LJKFP
HEXKW	CPDLZ	JWSQC	JVKIG	HTJHT	EGAHA	GDXXK
BSPPK	DIAVZ	VQONC	HOVDA	VZQKW	FNVON	RPVGH
CUFPV	SFPIE	TOZOD	WGYFE	AWNJY	KOEDW	UMELD
NOBUH	MUPQL	GYOPP	ODBAB	UFUUC	AEOJW	RDIPK
WMOKV	OMICW	CKPIH	LUMSY	YOSBG	WOPHV	PKOMO
PHGER						

Smith.

The key word is ATCHISON, the cipher disk being used and the setting changed for every letter of the message. The letter X indicates a period where it is evidently not a letter of a word.

Deciphering the message with this key and method we have:

RELIA	BLEIN	FORGF	TIONF	ROMCA	SASGR	ANDES
RECEI	LEDHE	RETHA	TAMOU	NTEDD	ETACH	MSKTL
EFTTH	ERELA	STNIG	HTTOE	SCORT	SHYMP	ENTOF
ARMSA	NDAMM	UNITI	ONTOB	ESMUG	GLEDA	CRJXS
BORDE	RNEXT	FRIDA	YNIGH	TATAP	OINTT	WELVE
MIENX	FKOSB					

Beyond this point the message, if we continue the deciphering process, is unintelligible. The sense fails at the first P of the cipher group BSPPK. We have translated B as M with disk A to N and S as I with disk A to A. The last words that make sense

are A POINT TWELVE MI; clearly the rest of the last word is LES and this is represented by PPK. Putting P=L then A=A and putting P=E then A=T. In other words, the encipherer forgot to change his disk setting, A to A, after enciphering I into S and enciphered L into P with the same setting, A to A. Continuing the deciphering on this basis, we have:

LES EASTO FDOUG LAS.T HISIS INYOU RDIST RICT. WILLY OUTAK ENECE SSARV STEPS TOPRE VENTT HISSH IPMEN TFROM GOING SKZRX LEADE ROFSM UGGLE RSSAL DTOBE JUANH ERNAN DEZOF NACO.

The minor errors underlined above are not difficult to correct except the sixth word in the eighth line. They will be taken up however for analysis of cause of error.

Line 1, GF should be MA. Putting the latter into cipher we find the letters of the cipher should have been GO instead of MJ. This is clearly a telegrapher's error, - - . - - - becoming - - . - - -

Line 2, L should be V. The corresponding cipher letter should be F instead of P. This is an error of the encipherer in copying.

Line 2, SK should be EN. The corresponding cipher letters should be YU instead of KX. Another telegrapher's error, - . - - . . - becoming - . - - - . -

Line 3, Y should be I. The corresponding cipher letter should be L instead of V. Another error in copying by the encipherer.

Line 4, JX should be OS. The corresponding cipher letters should be FK instead of KF; an error on the part of the encipherer in copying.

Line 7, V should be Y. A mistake in copying.

Line 8, SKZRX. If we take X as a period, then this line might be OVER, the R being correct and

SKZ being in question. The corresponding cipher letters are AEO and if we encipher OVE we get ETJ. Here again we have a telegrapher's error, . - . - - - becoming . - . - - -

Line 9, L should be I. The corresponding cipher letter should be K instead of H; an error in copying by the encipherer.

The errors by the encipherer above noted are fairly common ones. These and similar errors are usually found when a cipher message, prepared as a rough draft by the encipherer, is copied by a clerk and a careful check of the copy is not made. The letters mistaken depend, of course, on the encipherer's hand writing or printing. Other errors, besides those noted, are the confusion of C, G, and Q; I, and J; B and R, etc.

The error by the encipherer, in not changing his disk setting for one letter and thus throwing out the whole process of deciphering, would not have occurred had he put the message into eight columns or a multiple thereof and enciphered each column with one disk setting. This latter method is also very much faster.

Telegraphers' errors in cipher transmission are common and often very confusing. Note should be taken as to whether Continental or American Morse was used for transmission. An analysis along the lines indicated will usually develop the error and correction. If not, a repetition should be demanded, calling attention, if possible, to the particular groups that are not clear.

The deciphered and corrected message is:

"Reliable information from Casas Grandes received here that a mounted detachment left there last night to escort shipment of arms and ammunition to be smuggled across border next Friday night, at a point twelve miles east of Douglas. This is in

your district. Will you take necessary steps to prevent this shipment going over? Leader of smugglers said to be Juan Hernandez of Naco."

Another remarkable example of errors in transmission by American Morse is the following: A message, partly in cipher and partly in plain text, contained the cipher words

GA GTXIEIT EIDISXQ

This, deciphered as far as possible by the alphabet determined by analysis of the rest of the cipher, read

SU SME_Y_M Y_O_GES

It was finally decided that the context required a single word like SUSPENDIO or SUSPENDIOLES for this cipher group. An examination along this line showed that the cipher words should have been received..... GA G L X C U R D P X G
and were received..... GA G T X IE IT EI D IS X Q

and that there were five errors in transmission in these three cipher groups alone.

RETURN TO the circulation desk of any
University of California Library
or to the
NORTHERN REGIONAL LIBRARY FACILITY
Bldg. 400, Richmond Field Station
University of California
Richmond, CA 94804-4698

ALL BOOKS MAY BE RECALLED AFTER 7 DAYS
2-month loans may be renewed by calling
(415) 642-6233
1-year loans may be recharged by bringing books
to NRLF
Renewals and recharges may be made 4 days
prior to due date

DUE AS STAMPED BELOW

FEB 20 1989

Jones, H. C.
1-24-89

AUG 0 2 2004

LD 21A–38*m*-5,'68
(J401s10)476B

General Library
University of California
Berkeley

Gaylord
PAMPHLET BINDER
Syracuse, N. Y.
Stockton, Calif.

YC 62994

GENERAL LIBRARY - U.C. BERKELEY

B000886028