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

RECORDS CHARGE-OUT

96

DATE OF REQUEST	BY
25 Jan 61	10

FILE OR SERIAL NUMBER AND SUBJECT	From File of Special Consultant (Friedman) German Military Ciphers from February to November 1918 Register No. 117 Serial No. 1016 ~~Confidential~~
TO	NAME AND EXTENSION OF PERSON REQUESTING FILE: Mr. William Friedman LI 6-8520 — ORGANIZATION, BUILDING, AND ROOM NUMBER:
RETURN TO	Mrs. Christian, AG-24, NSA, Ft. Geo. G. Meade, Md. — DATE RET'ND. — INITIAL HERE
INSTRUCTIONS	WHEN TRANSFERRING FILE TO ANOTHER PERSON, COMPLETE SELF-ADDRESSED TRANSFER COUPON BELOW, DETACH, STITCH TO BLANK LETTER-SIZE PAPER AND PLACE IN OUT-GOING MAIL SERVICE.

~~Confidential~~ Register No. 117

WAR DEPARTMENT

OFFICE OF THE CHIEF SIGNAL OFFICER

WASHINGTON

GERMAN MILITARY CIPHERS FROM FEBRUARY TO NOVEMBER 1918

30 April 1959

This document is re-graded "CONFIDENTIAL" UP of DOD Directive 5200.1 dated 8 July 1957, and by authority of the Director, National Security Agency.

Paul S. Willard
Colonel, AGC
Adjutant General

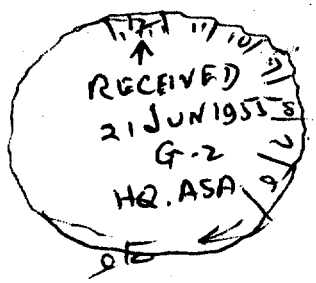
Classification changed to ~~RESTRICTED~~
By Authority of
HAROLD G. HAYES, Col., Signal Corps
Acting Chief, Army Security Agency

By JASON G. CAMPBELL, 1st Lt., SigC
1 April 1946

crossed in pencil in LC copy

~~NO ACCOUNTING NECESSARY~~

REGISTRATION CANCELED
by
Authority Hqs, ASA ltr dated 27 Feb 46
2d Ind 11 Mar 46, signed:
HAROLD G. HAYES, Col., Signal Corps
Acting Chief, Army Security Agency



~~Register~~ No. 117

WAR DEPARTMENT

OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

GERMAN MILITARY CIPHERS FROM FEBRUARY TO NOVEMBER, 1918

J. R. Childs

TECHNICAL PAPER

OF THE

SIGNAL INTELLIGENCE SECTION
WAR PLANS AND TRAINING DIVISION

of p. 24(n)

UNITED STATES
GOVERNMENT PRINTING OFFICE
WASHINGTON: 1935

FOREWORD

The following report on the military ciphers used by the Germans from February to November 1918, was written about December 1918 by First Lt. J. R. Childs, Infantry, and except for minor changes is in the form in which he prepared it. There have been added note 7, by First Lt. H. C. Skinner, M.I.D., entitled "Note on Reconstruction of an Incomplete ADFGVX Message", and note 12, entitled "A Mechanical Method for Determining the Key for the Transposition in the ADFGVX Cipher, Given Two Messages Having Similar Endings", prepared in January 1919 by the undersigned, then First Lieut., Military Intelligence Division, U.S.A.

WILLIAM F. FRIEDMAN,
Cryptanalyst, Chief of Signal Intelligence Section.

Office of the Chief Signal Officer,
War Department,
Washington, June 25, 1934.

CONTENTS

GERMAN MILITARY CIPHERS FROM FEBRUARY TO NOVEMBER, 1918

This survey of German Military Ciphers is intended to be very brief. A knowledge of the principles contained in Hitt's Manual for the Solution of Military Ciphers is presupposed.

One of the most outstanding features in the use of cipher by the Germans, whether on the Western or Eastern Front, was their predilection for transposition methods. Of all their systems which have come under our observation, there were only two of purely substitution methods.

I. SUBSTITUTION CIPHERS

One of these, strange to say, was a single mixed alphabet substitution used by Gen. Kress von Kressenstein in communication with Helferich. Several very important messages were sent in this very simple cipher. This cipher was preceded by the preamble "777." This was an identification to the recipient of the system which had been employed. The life of the "777" Cipher was not of long duration. The system was too simple; the wonder is that it was ever used at all. A message sent in the "RICHI" Cipher a few days after the "777" had been solved, directed an immediate discontinuation of its use.

"The cipher prepared by General von Kress was solved here at once. Its further use and operation is forbidden. (Signed) Chief Signal Officer, Berlin."

The second cipher based upon substitution principles and perhaps the only one which was ever made extensive use of, was the so-called "Wilhelm" or "Fuer God" Cipher. This cipher was used over a longer period of time than any other cipher which the Germans were ever known to have employed.

The cipher was known as the "Fuer God" for the reason that all messages in this cipher contained the address "Fuer God", "GOD" being the call sign of the wireless station to which the messages were directed. The messages were sent by POZ, a station at Nauen, just outside of Berlin. They were numbered serially from the first of the year to December the 31st, and were sent at more or less irregular intervals, an average of about three a week.

These ciphers were identified as substitution ciphers from the resemblance which the frequency tables of the cipher letters bore to the common type of substitution frequencies. Further evidence was contained in the repetitions which occurred in the body of the messages. These repetitions were factored as an ordinary substitution cipher; and they established the fact that the number of alphabets in messages numbered from 1 to 30 varied between 11 and 18, and that from 31 to 60, inclusive, the number of alphabets employed reverted to the same cycle as from 1 to 30. In other words, there were but 30 keys and messages from 31 to 60, and from 61 to 90 were enciphered by the same keys as those numbered from 1 to 30.

It was also ascertained that the number of alphabets was limited; and that not only was the same alphabet oftentimes repeated in the 13 alphabets, for example, in the 13 of message number 1, but that the same alphabet also reappeared in the 13 alphabets of number 2, in the 12 of 3, and in the 18 of number 4, and so forth.

The number of alphabets finally reduced themselves to 22. They formed a modified Vigenère Table.

TABLE—1.—THE ALPHABETS FOR THE "WILHELM" CIPHER

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

Numbers were expressed by the following letters bracketed between "Q's":

1	2	3	4	5	6	7	8	9	0
H	P	J	W	D	Y	V	R	A	F

The alphabet beginning "SQRYV" was known as the "A" alphabet, that beginning "LOPNM" as the "B" alphabet, etc.

Messages numbered 1, 31, 61, etc., were decipherable by the 13 alphabets in the order "JVCEPQHCMPQGP".

Messages numbered 2, 32, 62, etc., were decipherable by the 13 alphabets in the order "TBUULENFKEQGC".

The horizontal sequence above the table is the plain-text sequence. The vertical alphabet on the extreme left gives the arbitrary symbol by which the different alphabets were known n the 30 keys. Attached is a list of these 30 keys:

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

It will be noticed that the same letter, as P, for instance, in key no. 1, is repeated four different times. Again, the E and Q and G which occur in 1 occur also in 2. These facts pointed to the use in these 30 keys of intelligible German words. The arbitrary letters, which the keys in their present form contained, represented a simple substitution. This appeared from the frequency, for example, of G and the inseparable combinations NF and NA, N never appearing unless followed by F or A. It was therefore extremely probable that these letters, arbitrarily chosen to represent the 22 different alphabets, in reality represented keywords in German text.

N was assumed to be the value of C, and F, H; and G, the most frequent letter which was never absent from any of the series, E. This simple substitution was continued until familiar German syllables began to appear and finally the complete keywords themselves.

68652—35——2

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

II. TRANSPOSITION CIPHERS

Reference has been made to the predilection for transposition methods on the part of the Germans. Even substitution methods, when resorted to, usually contained in them some form of transposition, such as in the "RICHI", the most important military cipher used by the Germans.

One of the most common forms of transposition cipher used by the Germans was the double transposition. Occasionally, the simple columnar transposition was used, but this was extremely rare as such a system of encipherment in a language such as the German, which contains the common invariable combination CH, offers very little security.

The solution of a simple columnar transposition involves merely putting together the columns containing the C's with the columns containing the H's with which they belong. If, as often happens, in a transposition cipher, two C's occur in the same column, there must also be two H's which occur the same number of letters apart as the two C's in a similar single column.

As an example of a simple transposition, there was intercepted by the high-powered station at General Headquarters in May, a cipher which read as follows:

ALTMARK 41 GRUPPEN

B E L N S M E U A G H R L N V R S N D C D C N O A A C E F N
F N F P E O S G A A B N B D E D M W L R R T H N A T O S O N
S N Ü I K L N I G P U S U S S H F E I N R A A D N H N R N E
F A E U N E H B A S R T A R R N U E R I M G U R E K C O B T
A I T O F I L T A N N U A E M E I O D E D E H Z K G N T C H
N A D Ü G U R S R T E D L Z R I C A U N Z D M R F A L C N L
N E U L U B E S B H T E N A H D N U S T Ä N M S Z.

A frequency of the cipher letters in which the most frequent German letters, E, A, N, I, etc., appeared in approximately the same proportion as in German text and the absence of Q, J, and Y indicated that the principle upon which the message had been enciphered was that of transposition.

In the fourth cipher group of 5 letters there is a C which is followed at an interval of 2 letters by a C in the fifth group. A third C follows the second C at an interval of 5 letters.

In the thirteenth group from the end there is an H followed by a K at a similar interval of 2 letters, as was observed between the first 2 C's, and, further, there is another H which follows the K at an interval of 5 letters.

There can be but one conclusion, and that is that these 3 C's belong in a column which will directly precede the column which contains the 2 H's and the K.

C H
D Z
C K
N G
O N
A T
A C
C H

As yet the length of the columns is still unknown, though there can be no doubt that the length must be at least such as to include the 8 lines which are contained in the series of the 3 C's.

If a count is made of the letters which occur between the first C in the fourth group and the H in the fourteenth group from the end (2 letters which it is believed are paired together) the number will be found to be 123. This number is divisible only by 3 and 41. There are 205 letters in the entire message. If the message is divided into columns of 41 letters in length, precisely 5 columns will result.

Again, one might have chosen to place a third column against the original two which had been selected

C H
D Z
C K
N G
O N
A T
A C
C H

by putting a column containing an H or K against the AC which appeared as a result of the matching of the three C's. There are a number of H's from which to choose but the proper H would have readily proved itself from the kind of syllables which would have resulted when the letters immediately preceding it appeared in conjunction with those which were already possessed.

Compare two such combinations, one in which the correct H has been placed against the AC which it follows and the other an H selected at random.

(1)	(2)
C H L	C H S
D Z U	D Z M
C K B	C K E
N G E	N G U
O N S	O N A
A T B	A T G
A C H	A C H
C H T	C H R

In the first, the German word ZU has appeared. The second contains in its second line a combination "DZM" which, unless an error, is impossible in German. A count of the letters between the C and H in "ACH" in the first gives also 41 which is a factor of the number 123 which was found to separate the other CH's.

There is no other conclusion but that the columns are five in number and are 41 letters in length. The columns are accordingly cut as follows:

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

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

By fitting the remaining C's with H's which appear in the same horizontal lines the completely reconstructed key becomes:

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

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

The message is now in the original form in which it appeared before encipherment. The translation reads: "Do not let Reservist Wenzel and Mrs. Margaret Fuhrman Lelea, who are on board, disembark, but bring them back to Germany. Notify Consulate. Confirm at once to the Admiralty Staff the receipt and carrying out of this wireless message."

In the case of a double transposition, which is the double application of the same columnar key, it is impossible to attempt to reconstruct the key by the method of fitting together the C's with the H's. The cipher letters in a double transposition are inextricably mixed together in a way that has led a mathematician to say that the only principle which remains in the order of the letters after their double encipherment is the fact that there is no principle.

There is but one method of solution. This is accomplished when two or more messages are to be had of the same length and enciphered by the same key. This is only possible in the case of two messages of identical length where the number of letters does not exceed 50 in each message. If the number is more, the solution is only possible with three messages of identical length. The method of solution is that of writing out the messages of identical length under each other. The vertical columns which are thus formed are cut up and the messages are then anagrammed.

The principle of anagraming two messages is made possible by reason of the fact that, in any transposition or rearrangement of letters in messages of equal length enciphered by the same key, the letters which occupy the same relative positions in each of the clear text messages of

similar length will pass through identically the same permutations when put through the process of encipherment.

The double transpositions which were used by the Germans in 1918—notably, the Alachi, Gechi, Omochi, Itochi, all modifications in one unimportant way or another of a double application of a single transposition key—were never used in sufficient quantity to make the method of solution by means of anagraming two messages of equal length possible.

It however happened on more than one occasion in messages sent by some of the smaller stations in the Black Sea area which made use of the Alachi and Itochi, etc., in communication with Berlin and Constantinople, that, instead of making a double application of the key in the encipherment of messages, only a single application of the key was employed. This had the effect of leaving the message in the form of a simple columnar transposition.

Thus, on July 24, two messages were intercepted by our stations—one of them sent by LP (Berlin) to COS (Tiflis) by way of NKJ (Nicolaiev) and the other sent to OSM (Constantinople) by COS (Tiflis).

NKJ v LP
FUER COS ALACHI-266

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

OSM v COS
ALACHI-152

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

The first message resisted all efforts at a solution directed along simple principles. The C's which were matched for trial with the H's gave no promising syllables.

In the second message there were 2 C's and 5 H's.

There was nothing to do but try each against the other. The columns were run tentatively a distance of two or more letters in either direction from the C.

(First set)					(Second set)				
R	O	R	E	R A R S	E	O	E	E	E A E S E R
R	M	R	U	R H R G	T	M	T	U	T H T G T S
S	G	S	A	S B S M	R	G	R	A	R B R M R C
C	H	C	H	C H C H	C	H	C	H	C H C H C H
H	N	H	B	H R H B	A	N	A	B	A R A B A N
N	E	N	H	N S N A	E	E	E	H	E S E A E S
S	N	S	R	S E S T	R	N	R	R	R E R T R E

In the first set the last pair of columns was finally chosen from amongst the four. It was hardly probable that the C would precede the H which immediately followed it in the cipher in the first group. If this pair of columns was correct the syllables formed as a result of the conjunction of the letters should suggest parts of German words. "NA" in the second line below the CH seemed to offer the best suggestion. "NA" might be the first letters in "NACH".

Since the "NA" was taken from a pair of columns in which one of the two CH's in the message had been formed, there was the single alternative of fitting the "NA" in this pair of columns against the proper CH combination of columns which was to be found somewhere among the five pairs in the second set.

The column chosen in the first set, was placed against each of the five columns in the second set in succession, the "NA" being placed each time in the same horizontal line with the CH in order to form the word "NACH". The correct pairs should prove themselves by the appearance of other German words or syllables when once the two pairs were correctly fitted.

The first CH in the second set when placed against the NA in the last column of the first set gave no result.

R S
R G
S M E O
C H T M
H B R G
N A C H
S T A N

The combination "HBRG" which appeared in the line above "NACH" eliminated this choice.

The second attempt appeared much better:

R S
R G
S M E E
C H T U
H B R A
N A C H
S T A B

Another German word "STAB" had appeared in addition to the syllables "BRA", "CH" "TU", and "MEE".

A count was made of the number of letters which separated the "C" from the "H", the "H" from the "T", and the "T" from the "U" in "CHTU". This gave 145, 76, and 21 letters, respectively. The latter was divisible by 7, the 76 was one short of a seven factor and the 145 two short. The columns were probably 7 letters in length. There were 152 letters in the message which would give 20 columns of 7 letters in length and 2 of 6. This would account for the discrepancy of two and one in the count between "C" and "H" and "T".

These deductions were soon afterwards confirmed. The word "STAB" was a word of frequent occurrence in the signature "GENERAL STAB POLITIK BERLIN," with which we were familiar. This enabled us to reconstruct the entire rectangle.

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

The cipher was a simple columnar transposition. The message read when translated:

"Lieut. Colonel Baron von der Goltz and Major Count Graf Jolfsmeel, with staff, will arrive in Braila on July 28th; they will then continue their journey to Tiflis. General Staff, Political Section, Berlin."

The key once solved by the reconstruction of the transposition in the one "Alachi", the second message should be decipherable by the application of the same key.

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

This operation was now repeated. The message was written under the same series of numbers, reading from the first horizontal line of the first transposition and writing the letters in succession vertically down the columns in numerical order from 1 to 22.

68652—35——3

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

"ZU FUENF VIER EINS. AN HEERES GR. EICHHORN IST GEDRAHTET ABNAHME DES ANGEKOMMENEN TRANSPORTES DRINGEND ERFORDERLICH. WEITERE TRANSPORTS MUESSEN FOLGEN SOBALD EINRICHTUNG VON QUARANTAENE STATIONEN IN UKRAINE ERFOLGT IST. ICH BITTE MIR VORSCHLAEGE HIERUEBER BESCHLEUNIGT ZU MACHEN. LUDENDORFF O P ZWEI ANG."

When translated:

"Referring to no. 541. Army Group Eichhorn has been advised by wire that the unloading of the transport which has arrived is urgently necessary. Further transports must follow as soon as arrangement of quarantine stations in Ukraine is made. Please expedite suggestions to me in regard to this. Ludendorff. O P 2 ANG."

The "Alachi" was a double transposition. Every deduction which had been made had proved correct.

Until the day of the armistice and for some few days afterwards the "Alachi" double transposition cipher continued to pass between Berlin and the East. Although it was never possible to anagram any two messages since no messages were ever found identical in length, yet on more than this one occasion after having solved the key from a single operation of the transposition, it was possible to read all other messages for the same day without further experimentation by the mere double application of the solved key.

It was never the Berlin operator who was guilty of this error, but always the encipherer from one of the numerous smaller stations at Poti, Nicolaiev, Constantinople, or Sebastopol located in the area of the Black Sea.

The encipherer at Constantinople was probably indifferent enough to consider that a single transposition was sufficient for security.

III. THE ADFGVX CIPHER (WESTERN FRONT)

This cipher which combined the use of transposition and substitution methods, was probably one of the most intricate and most widely used systems of cipher ever employed by the Germans in the course of their military operations from 1914 to 1918. The system first sprang into use on March 1, 1918, 3 weeks before the initial spring drive of the Germans. Its appearance was almost coincident with that of a number of new codes and ciphers such as the Trinumeral Code, which suddenly came into existence at this time. At first, only 5 letters were used in this cipher A, D, F, G, and X. These letters formed the radicals of a square which contained the letters of the alphabet with J omitted. Twenty-five 2-letter combinations were possible with these 5 letters. The digraphs thus formed such as AA, AD, AF, AG, AX, etc., were substitutions for the various letters of the alphabet. After the substitution had been effected, the letters were then subjected to a simple columnar transposition. The keys were found to change daily.

The number of messages which were intercepted in the cipher varied from 25 a day upon the inception of the system to as great a number as 148 during the last days of May.

The first solution of a key in this cipher was made by Capt. George Painvin of the French Cipher Bureau on April 6 and was the key for messages of the 1st of April.

The cipher continued to be extensively used as late as the last offensive operations of the Germans in June. From that time until the conclusion of the armistice, the volume of messages diminished very considerably. Although only 10 keys covering a period of 10 days were ever solved the proportion of the messages which were deciphered by means of these keys was about 50 percent of the total number of messages which were ever received. This was true because of the fact that the keys which were solved, were those for days on which the greatest number of messages were received.

The cipher was used by the Germans in their communications between higher headquarters, principally, between the headquarters of divisions and army corps.

Much valuable information was contained in these ciphers. On one occasion, the solution of a key was accomplished so rapidly by the French that it was possible for an important movement which the Germans had given notice of in an order enciphered by this system, to be completely frustrated.

On June 1, the additional letter "V" was added to the other five. By the use of this additional radical, a total of 6, ADFGVX, a rectangle 6 by 6 was substituted for the 5 by 5 square which permitted the additional substitution of the numbers 0 to 9 and the letter J which had previously been omitted from the square.

On account of the fact that this cipher was used principally by army corps in the communication of orders and directions for an advance, it became possible to forecast the approximate time of some of the later German offensives of the spring and summer of 1918 from an activity chart of the cipher. Several days prior to an operation the volume of messages which were intercepted always increased noticeably above the normal.

IV. THE ADFGVX CIPHER (EASTERN FRONT)

In the month of July 1918, this cipher, which had formerly been used exclusively on the Western Front, began to be employed for the first time by Berlin in communication with the German occupied territories of Russia, the station OSM (Constantinople), and the German controlled Black Sea ports, Sebastopol, Nicolaiev, Poti, and other stations in the vicinity of the region. The only difference in the similarity of this cipher with that which was used on the Western Front was the preamble of the messages. Those which were sent to the eastern theater of war were distinguished by the prefatory word "RICHI" from the western ADFGVX messages, which were prefaced by "CHI."

The keys of the western ADFGVX messages changed daily; those of the eastern, the RICHI messages, had a life at first of 2 days and beginning September 1, they commenced to run in 3-day cycles. A total of 17 keys, covering a total of 44 days was solved in this cipher from its beginning in July to the end of November.

The first few messages which were solved, in August, contained information that was of little value. That is often the surprise which a cipher holds in store. Ciphers which prove a puzzle for weeks and months oftentimes when solved contain nothing more than a barren summary of statistics of station call signs or reports of wireless traffic. One of the most important messages which was solved by the cipher section was enciphered by simple substitution methods.

From the time of the debacle of Bulgaria and Turkey, until a few weeks after the conclusion of the armistice, the content of the solved messages increased in importance. On November 2, the key for November 2 and 3 was successfully solved within a period of an hour and a half by the method which similar endings in two messages makes possible, and which is described in one of the enclosed notes. A message in 13 parts which was deciphered by means of this key contained the entire plans by which General Mackensen proposed to retreat from Rumania.

V. MISCELLANEOUS NOTES

The following notes on the solution of the ADFGVX and other ciphers are appended:

1. Known solutions for the ADFGVX cipher.
2. Note on "RICHI" ADFGVX Cipher: Messages for the month of September.
3. Note on "RICHI" ADFGVX Cipher: The "exact factor" method of solution.
4. Note on "RICHI" ADFGVX Cipher: Solution of key of October 28, 29, 30, 31.
5. Note on "RICHI" ADFGVX Cipher: Solution of key of November 1, 2, 3.
6. Special note on "RICHI" ADFGVX Cipher.
7. Note by First Lt. H. C. Skinner, M.I.D.: "Reconstruction of an incomplete ADFGVX message."
8. Note on ADFGVX Cipher (Western Front): Solution of key of October 8.
9. Special report on the double transposition cipher.
10. Special report on ciphers.
11. Translation of a captured German document: "Instructions for Grill Ciphers."
12. Note by First Lt. William F. Friedman, M.I.D.: "A mechanical method for determining the key for the transposition in ADFGVX Ciphers, given two messages with similar endings."

1. KNOWN SOLUTIONS FOR THE ADFGVX CIPHER

(A) SOLUTION BY SIMILAR BEGINNINGS

The first step in this solution is to identify the number of columns employed in the transposition by the comparison of two messages whose text begins the same and runs so over two or more lines of transposition.

To understand how this is done, let us study first, two specimen messages whose beginnings are the same and which have been enciphered and transposed without however destroying the identity which originally characterized them.

No. 1. "150 TAUSEND R PATRONEN MOEGLICHT GEGUERTET"

No. 2. "150 TAUSEND S PATRONEN EMPFANGEN"

Effecting the cipher substitution according to the following key:

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

and the following transposition, the messages are written out thus:

	5	11	8	18	3	10	4	15	7	9	14	16	17	2	12	1	6	13
No. 1.	X	X	A	D	G	A	X	G	V	A	G	D	G	G	G	V	A	X
	A	G	D	G	F	A	D	G	V	X	V	A	X	G	F	A	D	D
	A	X	G	V	A	X	D	F	D	D	G	V	X	D	V	D	X	F
	X	V	D	A	X	G	D	G	X	D	G	V	X	D	G	D	G	V
	F	A	X	G	G	V	X	G	D	G								
No. 2.	X	X	A	D	G	A	X	G	V	A	G	D	G	G	G	V	A	X
	A	G	D	G	G	G	D	G	V	X	V	A	X	G	F	A	D	D
	A	X	G	V	A	X	G	V	D	F	V	X	F	D	V	A	A	X
	X	D	G	V	A	X												

It will be noticed that as they stand the first, all but two letters of the second horizontal lines and a part of the third are identical in the two messages.

Beginning with column 1 and reading down the successive columns in numerical order the messages are then communicated as follows:

12 H 40 – DJL v DFM – CHI–82

V A D D G G D D G F A X G X D D D X X A A X F A D X G V V D
X D A D G D X A X D D G A A X G V X G X V A G F V G X D F V
G V G G G G F G G D A V V G X X X D G V A G

12 H 40 – DJL v DFM – CHI–60

V A A G G D G G A A X D G X A A X A D A V V D A D G G A X F
A G X X X G X D G F V X D X G V V G G V D A X G X F D G V V

They are now in the form in which intercepted.

It will be noticed that in these messages the first two letters VA are identical. Now the first message (CHI–82) is longer by 22 than the second (CHI–60). Then we shall look for a longer interval in the first separating the letters which are the same as those in the second. Suppose we divide the two messages roughly by 20, as the columnar transposition usually employed runs between 16–21. In that case if we count four in the first message we find GGD and if we count three in the second we also find GGD. To check this let us see if the letter preceding GGD is identical in the two messages. It is not. Therefore, we take for the point of division VADD–GGD, etc., in the one message and VAA–GGD, etc., in the other.

Continuing from the points of division, we count four as before in the first message and find GFA, and counting three in the second message we find GGA. Here the second letter is not the same in both cases but the first is identical and so also the third. We are safe in assuming then that the second letter in one case may be an error and that we have again three letters which are identical. However, a new difficulty confronts us. The letter preceding GFA and GGA is in both cases D. Are we to include this in the series with GFA and GGA?

One of two courses is open to us. Either we can count a multiple of our factor 4 in the one message and a multiple of 3 in the other and leave this doubtful division for the present, or we can begin from the ends of the messages and work backwards.

Suppose for the moment we choose the latter course. Counting backwards four in the first message, we reach GV, and in the second, GV. But we are confronted here again with the difficulty we have just left. There is another letter D which precedes GV in both messages. Are we

to include it or not? Since we are unable then to overcome our difficulties here as before, let us choose the alternative method as outlined above and instead of counting four from the end in the first message, we shall count eight, and instead of three in the second, six. This count gives us in the first message XXX, etc., and in the second XFD, etc. Again in both cases a G precedes the X. Shall we include it? First let us multiply our count and count for the sake of further check, 12 in the first message and 9 in the second. We have AVV, etc., in the first message and AXG in the second. Again the letter D preceding is common to both. Let us include this D then in our division and we have DAV, etc., and DAX, etc. Counting four forward from DAVV, we strike the next division at GXXX and in the second message after counting three our division corresponding GXF. Again counting forward four in the first message we strike the next division between X and D in the one message and F and D in the other. There remain, at the end of the first message, 5 letters and at the end of the second 4.

We are enabled now, therefore, to conclude that the columns of the first message are of 4 and 5 letters in length and the second of 3 and 4 letters.

We return now to the beginning of the message and we have no hesitation in making our divisions

CHI.–82. |V A D D |G G D D |G F A etc.
CHI.–60. |V A A |G G D |G G A etc.

since we know now that the third division cannot include a D, as that would restrict the second division of the second message to two letters and that is manifestly impossible since the columns have been proven to be 4 and 5 letters in length in the one message and 3 and 4 in the other.

We now have the messages divided thus:

CHI–82

|V A D D|G G D D|G F A X G|X D D D X|X A A X F|A D X G|V V D
X D|A D G D X|A X D D G|A A X G V|X G X V A|G F V G|X D F V
|G V G G|G G F G G|D A V V|G X X X|D G V A G

CHI–60

|V A A|G G D|G G A A |X D G|X A A X|A D A |V V D|A D G G|A X F
|A G X X|X G X D|G F V |X D X|G V V|G G V |D A X|G X F D|G V V

Having completed our divisions along these lines, we now write the messages in vertical columns, beginning a new column with each new division.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
CHI.–82.	V	G	G	X	X	A	V	A	A	A	X	G	X	G	G	D	G	D
	A	G	F	D	A	D	V	D	X	A	G	F	D	V	G	A	X	G
	D	D	A	D	A	X	D	G	D	X	X	V	F	G	F	V	X	V
	D	D	X	D	X	G	X	D	D	G	V	G	V	G	G	V	X	A
			G	X	F		D	X	G	V	A				G			G
CHI.–60.	V	G	G	X	X	A	V	A	A	A	X	G	X	G	G	D	G	D
	A	G	G	D	A	D	V	D	X	G	G	F	D	V	G	A	X	G
	A	D	A	G	A	A	D	G	F	X	X	V	X	V	V	X	F	V
			A		X			G		X	D							V

Some of these columns are found to be longer than others; these are columns which will take positions to the left. The long columns which are common to the two messages will fall to the extreme left, followed by the remaining long columns.

It will be noticed that in both set-ups all of the letters of the first line are identical, all but 2 of the second and 9 of the third. The two in the second which are not the same may be accepted as telegraphic errors. The nine letters of the third line which are identical and which are not in the long columns will be placed naturally on the left and will take precedence after the long columns have been placed.

The steps then would be as follows:

(1) The placing of the long columns common to both messages 3—5—8—10—11—18 on the extreme left.

(2) The placing of the long columns remaining, 4—7—9—15, after these.

(3) Following these the columns [1] 2—12.

(4) After these the remaining six, 1—6—13—14—16—17.

The columns will then stand:

	3	5	8	10	11	18	4	7	9	15	2	12	1	6	13	14	16	17
CHI—82.	G	X	A	A	X	D	X	V	A	G	G	G	V	A	X	G	D	G
	F	A	D	A	G	G	D	V	X	G	G	F	A	D	D	V	A	X
	A	A	G	X	X	V	D	D	D	F	D	V	D	X	F	G	V	X
	X	X	D	G	V	A	D	X	D	G	D	G	D	G	V	G	V	X
	G	F	X	V	A	G	X	D	G	G								
CHI—60.	G	X	A	A	X	D	X	V	A	G	G	G	V	A	X	G	D	G
	G	A	D	G	G	G	D	V	X	G	G	F	A	D	D	V	A	X
	A	A	G	X	X	V	G	D	F	V	D	V	A	A	X	V	X	F
	A	X	G	X	D	V												

We are reasonably certain that these columns will be found to fall within the limits indicated.

Having completed, then, the determination of the number of columns and their relative positions our next task is to ascertain their exact positions by a study of digraphic frequencies.

Beginning with the left hand group column 3 is selected and placed against 5, 8, 10, 11, 18 in turn and frequencies made of the digraphs in the vertical column. For this purpose all messages which factor evenly for 18 and also those which run $4\times18+10$ as the CHI–82 and $3\times18+6$ as the CHI–60 are selected.

Having made these frequencies we next choose a column from the series 4—7—9—15 and match it with the three others and make frequencies of the digraphs resulting.

We have now to match each of these three frequencies with the five previously made in the series 3—5—8—10—11—18. Having found two pairs whose frequencies compare favorably we assume these as correctly matched and with these as a basis for our frequency the operation is repeated for each of the other columns until all have been successfully paired.

Having paired all columns the next step is to place the pairs in their proper position. For this purpose messages which factor 2 over 18 are selected and are put up in turn with each of the three pairs (3–5, 8–10, 11–18, assuming that these are the proper pairs) placed successively on the left. Suppose for instance that when the pair 3—5 is placed as the first pair on the left the frequency of the digraphs in the messages in which it is thus placed, gives us a frequency which compares most favorably with our original table of frequency.

[1] Reference to the known key will show that this is not correct. The letters D and V which are common to these two columns in both messages are not part of the identical beginnings and hence may be accidental repetitions.—Editor's Note.

This pair is then assumed as correctly placed and the operation is repeated with messages which factor 4 over 18.

A somewhat less accurate method in case there are no messages of this description to be found, is to attempt to place the columns with reference to the pair representing H which would most usually follow the pair representing C. This method however is best adapted to use when one or more pairs have been correctly placed.

B. SOLUTION BY "EXACT FACTOR" METHOD

This solution depends, not upon two messages whose beginnings are identical but upon finding enough messages which factor precisely for the number of columns employed.

For instance, on June 3, the key of which was determined by this method there were 11 messages found which factored for 18. The number of columns was then assumed to be 18 and having made frequencies of these columns and compared them amongst themselves, this supposition was confirmed.

Work from this point proceeded along the lines indicated in solution A. Further details will be found on pages 26 to 29 below.

C. SOLUTION BY SIMILAR ENDINGS

It will be convenient to describe this method by quoting from a report rendered by the w iter on August 13, 1918.

AUGUST 13, 1918.

Report to Major Moorman:

In accordance with instructions I proceeded first to Paris, where I acquainted Captain Painvin with what I had done on the ADFGVX. We talked over in detail the result of my solution and he suggested that in the final placing of pairs in position it would be convenient to determine their position after the position of the first pair had been determined by tables of suffixes which would show up any CH combination. He seemed very much interested in what I had written him of the apparent weekly rotation in the length of the transposition key, and in the face of the three coincidences of keys falling at intervals of 7 days, was inclined to accept it.

Since June 1, Captain Painvin has developed two new solutions of the cipher, one of which, however, is a combination of his old solution of "cutting" similar beginnings with his latest method.

The following two messages were sent on June 1 by the same station:

(1) "14 ID XX OBERBEFEHLSHABER KOMMT NICHT NACH SELENS 7 A K"

Translation: "14th Infantry Division: Commander-in-Chief is not coming to Selens. 7 A K"

(2) "211 ID XX OBERBEFEHLSHABER KOMMT NICHT NACH SELENS 7 A K"

Translation: "211th Infantry Division: Commander-in-Chief is not coming to Selens. 7 A K"

NEUFCHATEL.

7 H 9 – DAX v GGI – 0005 – CHI 106

|G A F F A| |F V A A G| |A V F(b) G X| |X V F X D| |X X X A A| |V X V D X
F| |A D F D F| |A X A D D| |G G A X X| |X G X V G| |D F X V A| |X G F V
A| |A X F G X| |F X V D A| |A D X X X| |D A X A A| |G A X V A| |F D G G
X| |F G G G(a) F| |D A A X D| |X A G X F|

68652—35—4

CHALONS

7 H 41 DTD v GGI – 0055 – CHI 108

GGAXX DXXAA AXADD VAGXF DAXAA XDAAX
DVXVD XFXGF VAXGX VGFVA AGFGG GFGAF
FAADX XXGAX VAFXV DAVFD GGXVD FDFDF
XVAXV FXD AVFGX AXFGX
(b) (a)

6 16 7 5 17 2 14 10 15 9 13 1 21 12 4 8 19 3 11 20 18
V D A X G F F X A G A G X X X A F A D D F
X A D X A V X G D G X A A G V X G V F A D
V X F X X A V X X A F F G F F A G F X A G
D A D A V A D V X X G F X V X D G G V X G
X A F A A G A G X X X A F A D D F X A D X
F

X V V D V D G F F X A G A G V X X A F A D
D F X A D X A V X G D G X A A G V X G V F
A D V X F X X A V X X A F F G F F A G F X
A G D A D A V A D V X X G F X V X D G G V
X G X A F A A G A G X X X A F A D D F X A
D X F

It will be noticed that when the messages have been set up and transposed we may expect to have two messages which are practically identical but whose identities we shall have to look for in different parts of the two messages.

If we take the two messages as they are intercepted and take the last 5 letters of message (2), AXFGX, this same series is found in the body of message (1). Marking off this part we take the 5 letters preceding AXFGX in (2) and identify and mark off these same 5 letters in (1), AVFGX. Continuing this we soon have all the positions identified in the 2 messages with the exception of 2 letters, the 2 letters in the message of 108 letters which are in excess of 106.

(1) CHI – 106

GAFFA FVAAG AVFGX XVFXD XXXAA VXVDX
FADFD FAXAD DGGAX XXGXV GDFXV AXGFV
A AXFGX FXVD AADXX XDAXA AGAXV AFDGG
(b) (a)
XFGGG FDAAX DXAGX F

(2) CHI – 108

GGAXX DXXAA AXADD VAGXF DAXAA XDAAX
DVXVD XFXGF VAXGX VGFVA AGFGG GFGAF
FAADX XXGAX VAFXV DAVFD GGXVD FDFDF
XVAXV FXD AVFGX AXFGX
(b) (a)

Writing these messages then, as follows:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
(1)	G	F	A	X	X	V	A	A	G	X	D	X	A	F	A	D	G	F	F	D	X
	A	V	V	V	X	X	D	X	G	G	F	G	X	X	D	A	A	D	G	A	A
	F	A	F	F	X	V	F	A	A	X	X	F	F	V	X	X	X	G	G	A	G
	F	A	G	X	A	D	D	D	X	V	V	V	G	D	X	A	V	G	G	X	X
	A	G	X	D	A	X	F	D	X	G	A	A	X	A	X	A	A	X	F	D	F
						F															
(2)	G	D	A	V	D	(X)	V	X	X	F	F	G	A	G	F	(V)	V	D	X	A	A
	G	X	X	A	A	D	X	G	G	V	G	A	D	A	X	F	D	F	V	V	X
	A	X	A	G	X	A	V	F	X	A	G	F	X	X	V	D	F	X	F	F	F
	X	A	D	X	A	A	D	V	V	A	G	F	X	V	D	G	D	V	X	G	G
	X	A	D	F	A	X	X	A	G	G	F	A	X	A	A	G	F	A	D	X	X
						D	F								(V)	X					

we find that in (1), column 6, as the only long column, fixes itself on the extreme left. Hence this disposes of the extra X between columns 5 and 6, as 6 must be a long column in (2) also and therefore will be included in column 6. The extra V between column 15–16 must remain unsettled as yet, as there is nothing to indicate whether it belongs with 15 or 16.

Rearranging our columns therefore we shall have column 6 on the extreme left.

Now, before proceeding further we should speculate as to what sort of phenomena we have to deal with. For one thing it will be observed that there are five columns whose initial letters do not agree. 5, 7, 18, 20, 21 in (1), and 2, 4, 6, 16, 17 in (2).

Assuming that one of these is a telegraphic error, what we have is probably 2 digraphs which represent an address, and 2 identical messages have been sent to 2 different stations with the difference of only 2 letters in the address.

Aligning the column 6 on the left therefore we shall have to choose for the next column from either columns 7 and 15 or 16 and following this from amongst those columns whose initial letters are not in agreement.

Now since the messages will end the same, and as (1) ends with F, column 7, as it ends with F, must be placed the third from the left in (2). We have then only to determine whether 15 or 16 is a long column to decide which column falls between 6 and 7. If 15 is chosen we should have the digraph VF ending message (2). Since F in (1) is on the extreme left, the V which should accompany it in case this supposition is correct, should be found and placed on the extreme right. But there is nowhere in the fifth horizontal line of (1) a V. Hence we must accept 16 as the long column which falls between 6–7 and which gives us an XF as ending message (2). An X is sought for in the fifth horizontal line of (1) to complete the similar digraph

XF in (2). As there are several we return to (2) and find that reading vertically upwards we have $\begin{bmatrix}G\\G\\X\end{bmatrix}$ in column 16 in (2). Thus:

(1)

6	16	7																			
V																					
X																					
V																					
D																					
X																					
F																					

(2)

X	V	V																		
D	F	X																		
A	D	V																		
A	(G)	D																		
X	(G)	X																		
D	(X)	F																		

As $\begin{bmatrix}G\\G\\X\end{bmatrix}$ unites with $\begin{bmatrix}D\\X\\F\end{bmatrix}$ in (2) so also ought a $\begin{bmatrix}G\\G\\X\end{bmatrix}$ to be found in one of the columns in (1) which when placed on the extreme right will unite also with $\begin{bmatrix}D\\X\\F\end{bmatrix}$ in (1).

This is found in column 18 and this column is placed on the extreme right and the process repeated until all the columns thus fall correctly into place. (For another example of this method, see "Note on 'Richi' ADFGVX cipher: Solution of October 28, 29, 30, 31", p. 29.)

While working with Captain Painvin he gave me access to the voluminous quantity of cipher notes which he has accumulated since 1914. I interested myself principally in double transposition as this is the method frequently employed by the Germans between Berlin and Constantinople, the East and Russia.

From Paris I proceeded to London where I reported to Colonel Slocum and put myself in touch with Major Hay. He immediately put me in the hands of Captain Brooke-Hunt, who has been working at ciphers in the East for 2 years and who has recently come to London. I found him working on the ADFGVX messages, particularly those which pass between Berlin and Constantinople. He was also working on the von Kress double transposition messages, so many of which have been received here recently. In the case of a double transposition the only possible method of solution is to find two or more messages which are equal in length and, writing them under each other, attempt to anagram them. For example, if after writing

two messages, one under the other we found on cutting them into columns, a column as follows:

C
E

we should look for a column with an H and an N or R to form two digraphs.

C H
E N

Such a method as this is of course greatly simplified with the addition of more messages. Having anagrammed the messages the method employed may then be reconstructed.

The double transposition is effected by transposing a message according to a simple transposition key.

A message:

"Forty-sixth Infantry Division: Objective for tomorrow Montigny"

would be written out according to the key.

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

The dummy letters or signature OSM will now be added[1] and the message transposed as follows, according to the same key:

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

reading down the columns 1—11 in order and writing out horizontally.

The message would now be sent NYYTM TINFR etc.

In solving, the process is reversed. After anagramming and having discovered the dummy letters we are enabled to determine by the position of the dummy letter in the text after some experimentation the position of the columns under which they fall and whether long or short columns. Having determined this we have the letters in the columns fixed in both transpositions, and by a process of trying and fitting the whole system is built up.

[1] The writer was certainly in error in regard to when the dummy letters were added, if such addition took place. A memorandum by Capt. Brooke-Hunt (referred to on p. 22) shows that the dummy letter (or letters) were added to the end of the *second* transposition rectangle. This makes a very important difference. However, the double transposition ciphers solved during the time of A. E. F. participation in the World War failed to contain any cases in which dummy letters were added, *either* at the end of the first *or* the second transposition rectangle. See also, in this connection the quoted statement on p. 47.—*W. F. F.*

I have also discovered while in London that a cipher intercepted some time ago by us passing between the Turkish Embassies in Berlin and Madrid was enciphered in Turkish and not in French as we had supposed. The British have a cipher man who is acquainted with Turkish and I suggest that any such messages intercepted here should be turned over to them as we have at present no one with a knowledge of Turkish in our office.

Captain Brooke-Hunt was attempting his solution of ADFGVX along the lines first laid down by Captain Painvin: That of finding two identical beginnings and failing that, along the lines by which I arrived at a solution, of looking for this identity within the body of the messages, having once determined the length of transposition. Since leaving London we have received a solution from him which indicates from the contents of the messages solved that his solution was accomplished along these lines.

Captain Painvin and Captain Brooke-Hunt both agreed that as yet no general method had been evolved and that solution must depend as it has in the past upon constant study and experimentation with new ideas and methods.[1]

From Major Hay I learned that work was continuing on the FLG in his office and that his study has revealed three FLG codes instead of the original assumption of one. Solution of the whole is dependent upon the arrival of certain maps which will give the names of towns and geographical points already located. Major Hay expects to be able to send us these solutions shortly.

While in London I arranged to have a copy of all cipher keys solved there forwarded to us and promised in return that we should send them any solutions we made.

At British G.H.Q., I found that very little cipher work was done there, as they depended more or less upon their office in London for this. The man who had been working on cipher was absent but I spent my time instructing the man to whom they had assigned this work in what I knew, particularly of ADFGVX.

The British acknowledge that they have had difficulty with the German 3-letter codes, both on account of the increasing complexity of the German code methods and also from the small quantity of text received. There was one code which was, however, proceeding very satisfactorily.

I learned of several matters in connection with their handling of codes which I shall briefly outline and to illustrate which I submit three memoranda given me by them.

1. This is the form in which information obtained from decoded messages is submitted to the proper authorities. This form, for example, excludes practice messages or other information which can be of interest to no one but the parties to whom the messages are addressed.

2. This is a map issued daily, showing in a visualized form the position of stations in divisions in the region which a particular code may include and indicates also stations which have been in communication with one another.

3. Captain Hitchins informed me that he had found that it was imperative that a check be kept upon the work of solution done at the armies. Each day each army sends to him a form such as this containing all solutions made and any suggestions as to other possible values. These are then checked up by the men in charge of the codes affected. While at G.H.Q., I visited the Second and Fifth British Armies with one of Captain Hitchins' officers who wished to correct the careless work which these forms were bringing to light.

While at British G.H.Q., a message in the KRUSA Code was received in blocks of five letters, sent as such obviously to resemble cipher. Such practice may be looked for in our own work.

---

[1] It is a strange and interesting fact that no *general* solution for this cipher system was evolved by the cryptanalytic services of any of the Allies during the World War, despite almost a full year's concentrated study. See S. I. S. Technical Paper *A General Solution for the ADFGVX Cipher System.*—*W. F. F.*

Returning to Paris I found that in my absence Captain Painvin had solved one of the messages passing between Eichhorn and Berlin and also one from von Kress, the latter a simple transposition. This was the only message, however, which yielded to a simple transposition and that this was not their general practice is indicated in the decipherment of one of the ADFGVX messages sent to Tiflis which reads:

"The cipher method prepared by General von Kress was solved here at once. Its further use by OP is forbidden. ALACHI method, is only to be used in cases which employ the 'dividing system' (in ciphers). For other cases, the new ITOCHI method, with dividing system, has been on the way to Kress since July 18. New instructions regarding double transposition are shown.—Wireless Section, General Staff." (Berlin.)

2. NOTE ON "RICHI" ADFGVX CIPHER

(Employed between Berlin and the Black Sea area)

MESSAGES FOR THE MONTH OF SEPTEMBER

A study of the RICHI messages for the month of September indicates the following facts:

(a) The same key was employed for a period of 3 successive days beginning September 1, 2, and 3, and the keys ran in cycles of three throughout the month: 4, 5, 6; 7, 8, 9; 10, 11, 12; 13, 14, 15; 16, 17, 18; 19, 20, 21; 22, 23, 24; 25, 26, 27; 28, 29, 30—a total of 10 keys for the month.

(b) A study of messages previously solved indicates that the length of the transposition key may be determined by excluding all numbers between 15–22, inclusive, for which messages sent by LP may be factored (LP has never been known to send a filled-up rectangle), and isolating from those numbers which remain the number for which the majority of messages sent by NKJ may be factored. (NKJ in contradistinction to LP makes a practice of filling up the rectangle when the enciphered message falls 2, 3, or 4 digraphs short of the end.)

(c) Previous study of the messages for September 13, 14, 15 had indicated that the length of transposition key was 22 and also that the key for the series of September 10, 11, 12 was 21. Work has also shown that the transposition key for September 19, 20, 21 is 22. We have here, therefore, a recurrence of the transposition key, 22 separated by a space of 3 days, September 16, 17, 18. This would indicate the use of two transposition lengths 21 and 22 recurring alternately over a 3-day period.

If the messages of LP and NKJ are checked it will be found, if the series is arranged as follows:

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

that in not one of these series in which the transposition length is assumed has LP made use of an exact rectangle of that length, and further, that so far as the material at hand is concerned, the majority of the messages of NKJ which factor on those days indicates the factor which we have assumed.

Enough material is not yet at hand to postulate any theories of the practice for October, but so far it would seem that the key continues to run for a period of 3 days, October 1, 2, and 3, and that it is likely that two different factors have been substituted for 21 and 22.

OCTOBER 6, 1918.

3. NOTE ON "RICHI" ADFGVX CIPHER

THE "EXACT FACTOR" METHOD OF SOLUTION

In partial confirmation of our note of October 6 (see previous note), the key for September 19, 20, 21 has been solved and the supposition established that the key was not only the same for the 3 days, but that the length of the transposition was 22.

The method employed in solution was the same as the one with which we succeeded in solving the Western Front ADFGVX messages of June 3.

A count of the letters of the messages for September 20 and 21 had indicated that the same key was employed on both days. In confirmation, the factor 22 appeared to predominate in the messages of NKJ for both days. The messages for September 19 were examined next, and a count of the letters also indicated that these messages had been enciphered by the same key as those of September 20 and 21. In the order of frequency the letters for the 3 days were as follows:

September 19	F X G D A V
September 20	X F G D V A
September 21	G X F D V A

As on the 20th and 21st, 22 was again the predominant factor.

There were 7 messages for the 3 days which factored for 22. When set up in vertical columns, there were 61 horizontal lines from which to make frequencies for the pairing of the columns.

The frequencies were made by setting column 1 against the remaining 21 columns in succession, and following this, the operation was repeated with column 2, and so on throughout the 21 columns. Column 1 was easily matched with 13, and 12 with 2, and from these 2

pairs the prominent digraphs; FG, XD, XF, XX were identified as common to both pairs and thus capable of being used as a test for other pairs. A final frequency of pairs was as follows:

	1—13	12—2	5—15	6—16	21—8	7—20	11—12	14—4	3—17	9—18	10—19
AA	///	𝍸 ////	///		//	///	//	/	/		///
AD	/	/	/	/	/			/		//	
AF		/							/	/	/
AG					/	/	/		/	/	
AV					/	/					
AX					/						
DA								/			/
DD	//		/	/		/	//	/	/	/	/
DF	////	//	//			/		/	//	/	/
DG	////	//	𝍸	𝍸 ////	𝍸	𝍸	//	𝍸 /	///	////	𝍸
DV	//	///	///	//	//	𝍸 /	///	////	//	///	/
DX	/		/	/		/	/		/		
FA	///	///		//	//	/		/	//	𝍸	//
FD		/	/				//				/
FF	///							/			
FG	𝍸 //	𝍸 ////	𝍸 /	𝍸𝍸	𝍸 /	𝍸 /	///	////	𝍸 ///	////	////
FV	//		///	/	///	𝍸	𝍸 ///	𝍸𝍸	//	𝍸	
FX	/	𝍸	///	//	//	/	///	//	///	//	///
GA			//		/		/		/		
GD	////	////	//	/	//	////		//	//	////	//
GF	𝍸	//	//	𝍸 /	𝍸	///	/	///	/	//	𝍸
GG	///	//		/	/	//			//	//	/
GV		/	//		//	/	/	/	//	//	/
GX	/	/	///		/		/	/	//	/	/
VA	/					/	/		/	/	/
VD		/	//	//	/	//	/	/	/	/	/
VF	/		////		/	/	/		///	/	
VG		/			///				/	/	
VV		////	/	//	///				/	///	/
VX	/		//	////	//		/	/	//		//
XA					/	/		//	//		//
XD	𝍸 //	𝍸	//	/	//	///	//	////	///	///	𝍸
XF	𝍸	///		////	////	𝍸 /	////	///	𝍸	/	//
XG		/		//	//	/	𝍸	///		/	////
XV	/		/				//		/	/	//
XX	𝍸 /	////	𝍸 //	////	𝍸	////	𝍸 ////	////	////	𝍸	𝍸 /

A consolidated frequency of the whole was as follows:

AA 𝍸𝍸𝍸𝍸 // (D)
AD 𝍸 /// (5)
AF //// (8)
AG 𝍸 (I)
AV / (3)
AX / (Q)
DA 𝍸 (9)
DD 𝍸𝍸 (K)
DF 𝍸𝍸𝍸 // (B)
DG 𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸 (N)
DV 𝍸𝍸𝍸𝍸𝍸 (O)
DX 𝍸 / (0) Zero
FA 𝍸𝍸𝍸𝍸 // (H)
FD /// (Y)
FF //// (8)
FG 𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸 / (E)
FV 𝍸𝍸𝍸𝍸𝍸𝍸𝍸 /// (I)
FX 𝍸𝍸𝍸𝍸𝍸 // (S)
GA 𝍸 (J)
GD 𝍸𝍸𝍸𝍸𝍸𝍸𝍸 // (U)
GF 𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸 /// (T)
GG 𝍸𝍸 // (Z)
GV 𝍸𝍸 /// (F)
GX 𝍸𝍸 // (C)
VA 𝍸 / (W)
VD 𝍸𝍸 /// (7)
VF 𝍸𝍸 // (V)
VG 𝍸 / (P)
VV 𝍸𝍸𝍸 (M)
VX 𝍸𝍸 //// (L)
XA 𝍸 /// (2)
XD 𝍸𝍸𝍸𝍸𝍸𝍸𝍸 /// (A)
XF 𝍸𝍸𝍸𝍸𝍸𝍸𝍸 /// (R)
XG 𝍸𝍸𝍸 //// (G)
XV 𝍸 / (4)
XX 𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸 / (X)

The greatest difficulty was experienced in pairing 3—17, 11—22, and 14—4. In two of these FG totaled but 7, while FV, an almost unknown digraph, appeared a total of 18 times. The final selection was made after setting up several messages which fell two short of an even factor and observing the behavior of the different doubtful pairs. In this manner 3—10, 14—16, which had been originally selected, were discarded; and 3—17, the poorest of the 11 pairs, proved by elimination.

Early in the work, having established the length of the transposition as 22, two messages, RICHI–168 and 222, from LP to OSM, were discovered which bore evidence of possessing similar beginnings over a line or part of a line. It was almost impossible to attempt to make the correct cuts in the columns by means of this identity, small as it was, but it seemed evident enough from the messages when a tentative division was made, that in RICHI–222, 12 and 2 were the long columns. A substantiation was afforded by setting up RICHI–222 with each of the 11 pairs in succession on the left, and as 12—2 alone gave XX as a final digraph, which had been previously identified as X, the position of 12—2 was thus fixed. After our solution it was proved that the difficulty of establishing the division of columns by means of the identity which we correctly assumed as existing, had been further complicated by the fact that the identity ran for 14 cipher letters at the beginning and there ceased, and was resumed after an interval of two digraphs and ran over 6 additional letters.

The fact that XX was X, was determined from its frequency which followed almost parallel with DG (N) and after having observed that in the last lines of the 7 messages that factored 22, XX appeared in the same vertical columns, in 5—15 twice and 1—12 three times.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
1	F	F	G	V	D	G	F	G	D	D	F	D	G	F	G	F	G	G	G	G	F	G
2	V	F	D	A	X	F	F	G	G	V	F	G	X	A	X	G	G	D	X	G	X	X
3	G	G	X	V	D	G	D	G	F	X	F	F	D	D	X	F	X	A	D	G	V	V
4	X	D	D	X	G	D	D	A	D	X	D	X	X	X	A	G	D	G	X	G	G	D
5	F	A	–	X	X	X	V	G	–	V	X	A	G	V	X	–	V	F	V	A	F	X
6	X	V	X	V	F	D	X	V	D	X	D	V	X	F	F	A	F	G	V	X	X	X
7	X	G	F	D	F	D	D	V	D	X	F	D	X	X	G	G	X	V	D	D	V	V

Arranged in proper order the columns fell as follows:

	12–2	7–20	10–19	1–13	9–18	3–17	21–8	14–4	6–16	11–22	5–15
1	DF	FG	DG	FG	DG	GG	FG	FV	GF	FG	DG
2	GF	FG	VX	VX	GD	DG	XG	AA	FG	FX	XX
3	FG	DG	XD	GD	FA	XX	VG	DV	GF	FV	DX
4	XD	DG	XX	XX	DG	DD	GA	XX	DG	DD	GA
5	AA	VA	VV	FG	–F	–V	FG	VX	X–	XX	XX
6	VV	XX	XV	XX	DG	XF	XV	FV	DA	DX	FF
7	DG	DD	XD	XX	DV	FX	VV	XD	DG	FV	FG

From the appearance of XX in the first table it was deduced that either 5—15 or 1—13 fell on the extreme right. RICHI–152 which factored for 22 less 2, was set up and frequencies of the pairs taken, first with 1—13 on the right and then 5—15. The latter gave a very much better frequency, and a frequency of the digraphs made with 5—15 on the right and 12—2 on the left gave excellent results. The digraph GX was followed two out of three times by FA. GX–FA was assumed as CH and working upon this clue the pairs very quickly thereafter fell into their proper positions in the rectangle.

OCTOBER 9, 1918.

4. NOTE ON "RICHI" ADFGVX CIPHER

SOLUTION OF KEY OF OCTOBER 28, 29, 30, 31

The solution of this key was accomplished in the space of 2 hours and was obtained without the use of a single frequency tabulation. The method employed was the one which has been described in a former note: the method formulated by Captain Painvin, where two messages enciphered by the same key are found to possess similar endings.

On October 30 it was observed that two messages had been sent from LP to NKJ for COS addressed to the Kaukasus Delegation, the one RICHI 338 and the other RICHI 274. It was found upon inspection that the RICHI 274 was a duplicate of RICHI 338 minus three prefatory lines in the RICHI 338.

The messages were divided as follows:

```
RICHI 338   V A X V V   V A X G A   F A A A D   A A X V| |V   A A A G A
            D V G V V   D A A A V   V X D| |D D   F V X D A   X F A X X
            G V F X V   V| |A D G A   G X A A A   X F F A X   V A A V D|
            |F F V F X   F G X F A   F V G F X   F D A V| |V   A A D X D
            F G D X X   D F X X A   G A D| |A A   V D A A F   A A D A V
            D A X A A   D X| |X X X   X F D A V   A V F G A   F F A D A
            A F D X A   A G V G D   X X V G A   A V D A| |D   A X G X D
            X G X F X   X V V D X   G V A D G   V X G F X   V F D A F
            F A D F A   G D D A X   F D X G X   A D X X X   D X F X X|
            |A X G A G   F D G D V   X F F D D   X X X X| |D   A F X F X
            F D F X X   D A X V D   X A A| |G X   A D A D A   V A A A D
            G F X D X   A D| |D F X   X A A X F   A V D X F   D D A G A
            A| |G F F D   F F A A F   X G A D D   F G V A X|  |X G G A F
            V A F X X   X A F F F   A G F|
```

RICHI 274

A A X F A V D X F D D A G A A A A F A A D A V D A
X A A D X G X A A A X F F A X V A A V D A A G V G
D X X V G A A V D A G X D X G X F X X V V D X G V
V X G F X V F D A F F A D F A G V X D A X F A X X
G V F X V V A D A V A A A D G F X D X A D F D A V
A V F G A F F A D A A F X F D F X X D A X V D X A
A F D X G X A D X X X D X F X X D F F A A F X G A
D D F G V A X X D F G D X X D F X X A G A D A F V
A F X X X A F F F A G F V V V A X G A F A A A D A
A X V A G A D V G V V D A A A V V X D X F G X F A
F V G F X F D A V G F D G D V X F F D D X X X X

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
RICHI 274	A	A	G	A	G	V	V	A	F	F	F	D	X	A	V	A	X	G
	A	A	X	A	X	X	X	D	D	X	D	F	D	F	V	G	F	F
	X	F	A	G	D	G	D	A	A	F	X	F	F	V	V	A	G	D
	F	A	A	V	X	F	A	V	V	D	G	A	G	A	A	D	X	G
	A	A	A	G	G	X	X	A	A	F	X	A	D	F	X	V	F	D
	V	D	X	D	X	V	F	A	V	X	A	F	X	X	G	G	A	V
	D	A	F	X	F	F	A	A	F	X	D	X	X	X	A	V	F	X
	X	V	F	X	X	D	X	D	G	D	X	G	D	X	F	V	V	F
	F	D	A	V	X	A	X	G	A	A	X	A	F	A	A	D	G	F
	D	A	X	G	V	F	G	F	F	X	X	D	X	F	A	A	F	D
	D	X	V	A	V	F	V	X	F	V	D	D	X	F	A	A	X	D
	A	A	A	A	D	A	F	D	A	D	X	F	A	F	D	A	F	X
	G	A	A	V	X	D	X	X	D	X	F	G	G	A	A	V	D	X
	A	D	V	D	G	F	V	A	A	A	X	V	A	G	A	V	A	X
	A	X	D	A	V	A	V	D	A	A	X	A	D	F	X	X	V	X
						G						X			V	D		

RICHI 338

V V D A F V A X F D A D A D G D G X
A A D D F A A X D A D D X A X F F G
X A F G V A V X X X G A G F A X F G
V A V A F D D X A G V X A X D X D A
V G X G X X A F A X X F G F A A F F
V A D X F D A D G D G D F X D A F V
A D A A G F F A V X F X D F A X A A
X V X A X G A V G G X G G D V F A F
G G F A F D A A D X V X D F A A F X
A V A X A X D V X F F A V X A V X X
F V X F F X A F X X D D X X A D G X
A D X F V D V G V X A X F D D X A A
A A G A G F D A G V F X F A G F D F
A A V X F X A F A V F X D X F D D F
D A F V X A X F A D A D D V X D F F
A V X A F A A A V X D X X D D A G A
A V V A D G A D D G F F X X X G V G
X X V V A A D A A V A X X A A A A F
V D D V D X A G X X A D A X

When set up, the length of the transposition key proved to be 18, giving 4 long columns in one message and 14 in the other. The difficulty which confronted us now was the determination of the relative position of the 4 long columns 6—12—15—16 which naturally placed themselves on the extreme left. To accomplish this without the laborious compilation of frequency tables was our aim.[1] This we succeeded in doing in the following manner:

(1) In RICHI 274, the 4 long columns 6—12—15—16 were placed on the extreme left. The position of these columns was thus limited to the first 4 columns.

(2) If RICHI 274 ended GXVD, RICHI 338 must end the same and the columns which corresponded to these in RICHI 338 (2—1—17—11) therefore aligned themselves within the limits of the numerical order 11—14, inclusive.

(3) In RICHI 338 there were four short columns, 3—9—10—18, which placed themselves on the extreme right and which thus fixed DAAX as immediately preceding GXVD in RICHI 274.

(4) If DAAX preceded GXVD in RICHI 274 it must also precede GXVD in RICHI 338. These columns were found to be 4—8—13—14 and their limits were fixed within columns 7—10, inclusive.

(5) Two columns remained, 5—7, and thus these were proven by elimination to be the fifth and sixth columns.

	6	12	15	16	5	7	4	8	13	14	2	1	17	11	3	9	10	18
RICHI 274	V	D	V	A	G	V	A	A	X	A	A	A	X	F	G	F	F	G
	X	F	V	G	X	X	A	D	D	F	A	A	F	D	X	D	X	F
	G	F	V	A	D	D	G	A	F	V	F	X	G	X	A	A	F	D
	F	A	A	D	X	A	V	V	G	A	A	F	X	G	A	V	D	G
	X	A	X	V	G	X	G	A	D	F	A	A	F	X	A	A	F	D
	V	F	G	G	X	F	D	A	X	X	D	V	A	A	X	V	X	V
	F	X	A	V	F	A	X	A	X	X	A	D	F	D	F	F	X	X
	D	G	F	V	X	X	X	D	D	X	V	X	V	X	F	G	D	F
	A	A	A	D	X	X	V	G	F	A	D	F	G	X	A	A	A	F
	F	D	A	A	V	G	G	F	X	F	A	D	F	X	X	F	X	D
	F	D	A	A	V	V	A	X	X	F	X	D	X	D	V	F	V	D
	A	F	D	A	D	F	A	D	A	F	A	A	F	X	A	A	D	X
	D	G	A	V	X	X	V	X	G	A	A	G	D	F	A	D	X	X
	F	V	A	V	G	V	D	A	A	G	D	A	A	X	V	A	A	X
	A	A	X	X	V	V	A	D	D	F	X	A	V	X	D	A	A	X
	G	X	V	D														

[1] See in this connection note 12, *A Mechanical Method for Determining the Key for the Transposition in ADFGVX Ciphers, Given Two Messages Having Identical Endings.—W. F. F.*

	6	12	15	16	5	7	4	8	13	14	2	1	17	11	3	9	10	18
RICHI 338	V	D	G	D	F	A	A	X	A	D	V	V	G	A	D	F	D	X
	A	D	X	F	F	A	D	X	X	A	A	A	F	D	D	D	A	G
	A	A	A	X	V	V	G	X	G	F	A	X	F	G	F	X	X	G
	D	X	D	X	F	D	A	X	A	X	A	V	D	V	V	A	G	A
	X	F	A	A	X	A	G	F	G	F	G	V	F	X	X	A	X	F
	D	D	D	A	F	A	X	D	F	X	A	V	F	G	D	G	D	V
	F	X	A	X	G	F	A	A	D	F	D	A	A	F	A	V	X	A
	G	G	V	F	X	A	A	V	G	D	V	X	A	X	X	G	G	F
	D	X	A	A	F	A	A	A	D	F	G	G	F	V	F	D	X	X
	X	A	A	V	A	D	X	V	V	X	V	A	X	F	A	X	F	X
	X	D	A	D	F	A	F	F	X	X	V	F	G	D	X	X	X	X
	D	X	D	X	V	V	F	G	F	D	D	A	A	A	X	V	X	A
	F	X	G	F	G	D	A	A	F	A	A	A	D	F	G	G	V	F
	X	X	F	D	F	A	X	F	D	X	A	A	D	F	V	A	V	F
	A	D	X	D	X	X	V	F	D	V	A	D	F	A	F	A	D	F
	A	X	D	A	F	A	A	A	X	D	V	A	G	D	X	V	X	A
	G	F	X	G	D	A	A	D	X	X	V	A	V	F	V	D	G	G
	A	X	A	A	A	D	V	A	X	A	X	X	A	A	V	A	V	F
	D	X	D	A	V	X	D	A	X	A	D	V	X	G				

(6) Having thus fixed the position of two columns there remained simply to place together in RICHI 338 the columns which contained the same letters and which would naturally take position as the sixteenth and seventeenth columns or, 10 columns removed from the fixed columns, 5 and 7 in RICHI 274. (This followed from the fact that the text of RICHI 338 ran 10 letters ahead of the similar text of RICHI 274.) These columns were 3—10.

(7) The placing of the remaining pairs was accomplished by continuing to build up upon this sequence by the same sort of cross fire between the two messages.

(8) Inspection of 5—7 had indicated FA as E and therefore the arrangement of columns, when once paired in their relative order, was very easily determined by pairing them in such a way as to bring out FA as the prominent digraph. Thus 10—3 was chosen in preference to 3—10 because of the number of AF's which would appear if the pair was placed in the latter order.

(9) To return to the system of cross fire building up of the pairs in the rectangle, the position of 5—7 having been fixed as columns 5 and 6, respectively, in RICHI 274, the columns corresponding or those which contained the identical letters with 5—7 in RICHI 274 were identified in RICHI 338 as columns 10—3 and were placed for reasons which we have stated in a previous paragraph as the fifteenth and sixteenth columns.

(10) Our skeleton rectangles appeared then as follows:

RICHI 274

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
				5	6	7								10	8		
				G	V									F	G		
				X	X									X	X		
				D	D									F	A		
				X	A									D	A		
				G	X									F	A		
				X	F									X	X		
				F	A									X	F		
				X	X									D	F		
				X	X									A	A		
				V	G									X	X		
				V	V									V	V		
				D	F									D	A		
				X	X									X	A		
				G	V									A	V		
				V	V									A	D		

RICHI 338

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
				5	6	7								10	8		
				F	A									D	D		
				F	A									A	D		
				V	V									X	F		
				F	D									G	V		
				X	A									X	X		
				F	A									D	D		
				G	F									X	A		
				X	A									G	X		
				F	A									X	F		
				A	D									F	A		
				F	A									X	X		
				V	V									X	X		
				G	D									V	G		
				F	A									V	V		
				X	X									D	F		
				F	A									X	X		
				D	A									G	V		
				A	D									V	V		
				V	X												

(11) Our 10—3 having been properly placed in RICHI 338 as the fifteenth and sixteenth columns, the 10 and 3 columns in RICHI 274 quite naturally place themselves in the same numerical order of columns, i.e., 15 and 16.

(12) There remain now in the last of our five divisions in RICHI 274 columns 9—18 which cannot take position as the fifteenth and sixteenth columns since these are occupied by 10—3. They therefore fall into position as the seventeenth and eighteenth columns, in the order 18—9 rather than 9—18 for the sake of the greater number of FA's in the former, a digraph which has been identified as having the highest frequency.

(13) The process just outlined is now repeated. The columns which are identical with 18—9 in RICHI 274 are sought for in RICHI 338. Since the text of these columns in RICHI 274 contain in their last line the digraph, XA, 4 letters removed from the end of the message, the same text must appear in RICHI 338, 4 letters removed from the end. XA is found in columns 13—8, which therefore fall into columns 9 and 10. Columns 14—4, which are left in this, the third of our five divisions, accordingly take the position of columns 7 and 8.

(14) The final position of the columns was as follows:

	6	15	12	16	5	7	14	4	13	8	11	1	17	2	10	3	18	9
RICHI 274	V	V	D	A	G	V	A	A	X	A	F	A	X	A	F	G	G	F
	X	V	F	G	X	X	F	A	D	D	D	A	F	A	X	X	F	D
	G	V	F	A	D	D	V	G	F	A	X	X	G	F	F	A	D	A
	F	A	A	D	X	A	A	V	G	V	G	F	X	A	D	A	G	V
	X	X	A	V	G	X	F	G	D	A	X	A	F	A	F	A	D	A
	V	G	F	G	X	F	X	D	X	A	A	V	A	D	X	X	V	V
	F	A	X	V	F	A	X	X	X	A	D	D	F	A	X	F	X	F
	D	F	G	V	X	X	X	X	D	D	X	X	V	V	D	F	F	G
	A	A	A	D	X	X	A	V	F	G	X	F	G	D	A	A	F	A
	F	A	D	A	V	G	F	G	X	F	X	D	F	A	X	X	D	F
	F	A	D	A	V	V	F	A	X	X	D	D	X	X	V	V	D	F
	A	D	F	A	D	F	F	A	A	D	X	A	F	A	D	A	X	A
	D	A	G	V	X	X	A	V	G	X	F	G	D	A	X	A	X	D
	F	A	V	V	G	V	G	D	A	A	X	A	A	D	A	V	X	A
	A	X	A	X	V	V	F	A	D	D	X	A	V	X	A	D	X	A
	G	V	X	D														

	6	15	12	16	5	7	14	4	13	8	11	1	17	2	10	3	18	9
RICHI 338	V	G	D	D	F	A	D	A	A	X	A	V	G	V	D	D	X	F
	A	X	D	F	F	A	A	D	X	X	D	A	F	A	A	D	G	D
	A	A	A	X	V	V	F	G	G	X	G	X	F	A	X	F	G	X
	D	D	X	X	F	D	X	A	A	X	V	V	D	A	G	V	A	A
	X	A	F	A	X	A	F	G	G	F	X	V	F	G	X	X	F	A
	D	D	D	A	F	A	X	X	F	D	G	V	F	A	D	D	V	G
	F	A	X	X	G	F	F	A	D	A	F	A	A	D	X	A	A	V
	G	V	G	F	X	A	D	A	G	V	X	X	A	V	G	X	F	G
	D	A	X	A	F	A	F	A	D	A	V	G	F	G	X	F	X	D
	X	A	A	V	A	D	X	X	V	V	F	A	X	V	F	A	X	X
	X	A	D	D	F	A	X	F	X	F	D	F	G	V	X	X	X	X
	D	D	X	X	V	V	D	F	F	G	A	A	A	D	X	X	A	V
	F	G	X	F	G	D	A	A	F	A	F	A	D	A	V	G	F	G
	X	F	X	D	F	A	X	X	D	F	F	A	D	A	V	V	F	A
	A	X	D	D	X	X	V	V	D	F	A	D	F	A	D	F	F	A
	A	D	X	A	F	A	D	A	X	A	D	A	G	V	X	X	A	V
	G	X	F	G	D	A	X	A	X	D	F	A	V	V	G	V	G	D
	A	A	X	A	A	D	A	V	X	A	A	X	A	X	V	V	F	A
	D	D	X	A	V	X	A	D	X	A	G	V	X	D				

5. NOTE ON "RICHI" ADFGVX CIPHER

SOLUTION OF KEY OF NOVEMBER 1, 2, 3

As this last solution was accomplished by principles involving an interesting combination of several familiar methods, it has been thought worth while to include this in a further memorandum.

At 4 a.m., on November 1 a first and second part of a RICHI ADFGVX was communicated to OSM by LP, the second part of which contained 264 letters.

On November 2 this second part was repeated but bearing a preamble RICHI 266 instead of 264.

The text of the two messages follows:

2–TL RICHI 264	D	V	D	V	F	D	V	F	A	G	X	V	X	F	F	F	V	G	G	G
	A	G	G	X	A	X	D	X	G	F	X	V	V	D	D	G	F	G	F	D
	F	A	V	G	V	D	A	F	G	F	G	X	D	X	V	D	F	A	A	D
	G	X	D	F	D	X	V	V	D	G	D	G	V	F	F	G	D	X	D	G
	A	X	A	X	V	G	V	A	A	A	V	F	V	G	V	F	D	G	D	X
	A	X	G	V	F	A	G	D	D	D	V	G	D	V	V	G	G	D	G	G
	G	V	A	A	D	D	G	D	V	F	V	D	D	D	X	D	V	X	D	X
	D	V	D	V	A	V	G	X	V	V	D	F	V	F	D	A	X	D	G	D
	A	V	G	X	D	D	D	A	D	G	F	V	G	D	G	A	V	A	X	D
	A	D	D	G	G	F	D	F	A	G	G	F	A	X	G	F	F	X	D	G
	G	G	V	G	A	F	D	X	A	A	F	D	V	V	F	G	X	G	F	V
	F	D	X	A	A	V	A	G	A	G	A	A	V	G	D	G	G	G	F	D
	V	A	G	G	V	X	A	A	D	D	D	D	A	V	A	V	V	A	D	G
	D	G	D	D																

2-TL RICHI 266

D V V D F D V D V G D V V G F F V G G G A X D A D
D G G G F X V V D D A A D D G D V V G V D A F G G
F G F D F A V V D G D G V D F V V D A X G A X A X
V G D D D A D G F V G V F D G D F G X D F D X G V
F A G D D V G A A A V F G D G G G V G A X G V F X
D F F D D D X G F A G X V X F V A V G X V X G G X
A X D X D G D A V G X D F F X D A G V G D G A V A
A D G D G D D F D F A G G F V X D X D V D G G G V
G A F G X G F V F D A V G D V V F V F F G D X D X
A A V A G A G V X A A D D G G F D V A G X A F D X
A X D D A V A V V G A A V G D G

It was at once concluded from a comparison of the two messages that the RICHI 266 was the correct version of RICHI 264 which had probably been garbled in its encipherment. If this were the case then we might expect to find an identical beginning in the two messages which would extend as far as the garbled portion and from there, following an hiatus of 2 letters (266–264), a similar ending which would extend in RICHI 266 in an order 2 letters removed from the same similar ending in RICHI 264.

The messages were therefore divided off or cut with reference to their identical beginnings. The cuts indicated a transposition key length of 19. This meant that RICHI 266 was an exact factor of 19 (19×14). We had then, therefore, but to set up RICHI 266 in 19 columns of 14 letters in length and follow the division thus made as a check in the cutting of RICHI 264.

The messages were then set up as follows:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
RICHI 266	D	F	G	V	V	G	V	G	G	F	V	D	V	F	G	A	X	G	D
	V	F	F	G	V	A	G	V	D	F	A	G	G	D	G	V	A	G	D
	V	V	X	V	D	X	V	F	G	D	V	D	D	G	G	G	A	F	A
	D	G	V	D	G	A	F	A	G	D	G	A	G	A	V	D	V	D	V
	F	G	V	A	D	X	D	G	G	D	X	V	A	G	G	V	A	V	A
	D	G	D	F	G	V	G	D	V	X	V	G	V	G	A	V	G	A	V
	V	A	D	G	V	G	D	D	G	G	X	X	A	F	F	F	A	G	V
	D	X	A	G	D	D	F	V	A	F	G	D	A	V	G	V	G	X	G
	V	D	A	F	F	D	G	G	X	A	G	F	D	X	X	F	V	A	A
	G	A	D	G	V	D	X	A	G	G	X	X	G	D	G	F	X	F	A
	D	D	D	F	V	A	D	A	V	X	A	X	D	X	F	G	A	D	V
	V	D	G	D	D	D	F	A	F	V	X	D	G	D	V	D	A	X	G
	V	G	D	F	A	G	D	V	X	X	D	A	D	V	F	X	D	A	D
	G	G	V	A	X	F	X	F	D	F	X	G	D	D	D	D	D	X	G

RICHI 264

D F G V V G V G G F V D V F G A X G D
V F F G V A G V D V A G G D G V A G D
D V X V D X V F G D V D D F G G A F A
V G V D G A F A G D G A G A V D V D V
F G V A D X D G G D X V A G G V A V A
D G D F G V G D V X V G V G A V G A V
V A D G V G D D A D V X A F F F A G V
F G G F F V X D A V D D X A D G G G A
A G F G F G A V D X F D D X F X A V D
G X G X G A F G D D V D A G X G A X G
X A F D D A D D G X F A D V X F V A D
V X D F X A X V D D D D D D F D V G A G
X D F D D V A V V V A G G X A F D D D
F X A X F X G D X F G D C D G D D

In cutting RICHI 264 we had only to follow the beginning of the columns as cut in RICHI 266. The division between columns 1 and 2 in RICHI 264 followed naturally from the identity with the similar beginnings in RICHI 266. Since column 2 in RICHI 266 began FFVGGGA (providing, of course, that our theory was correct) column 2 in RICHI 266 must likewise begin FFVGGGA.

A further check, if further check were needed, was given by the possession of the two messages of identical endings. Having cut columns 1 and 2 in RICHI 264 by means of a comparison of the beginnings, we had now to look in RICHI 266 for a column ending as column 1 in RICHI 264 with AGXVXF. This column was found in RICHI 266 in the position of the tenth column ending with these identical letters. In the same way when column 2 had been cut in RICHI 264 its ending GGXAXDX was found in RICHI 266, in the eleventh column. Employing this double check, the columns in their proper length in RICHI 264 were very quickly reconstructed and the short columns fixed upon as 5 and 9.

From this point the solution followed as described in our last note of November 1. The successive steps were, in their order:

First: The short columns 5 and 9 in RICHI 264 were placed on the extreme right of the rectangle. It was, of course, impossible to determine immediately the relative order of 5 and 9 but it was enough for the present to know that 5 and 9 would occupy in one order or another the position as the eighteenth and nineteenth columns taken in the numerical succession of the columns.

To avoid a repetition of an unnecessary number of letters we subjoin only the three final lines of each message.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18 (5)	19 (9)
RICHI 266																		D	F
																		A	X
																		X	D
RICHI 264																		X	D
																		D	V

Second: If columns 5 and 9 occupied the position of columns 18 and 19 in RICHI 264, then the columns containing at their ends the same letters as 5—9 would, in RICHI 266, occupy

the position of the first and second columns, since the concluding text of RICHI 266 ran two letters in advance of the same text in RICHI 264. These columns were identified in RICHI 266 as columns 16 and 3 and they were accordingly placed in the position of the first and second columns.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
	16	3																5	9
RICHI 266	D	G																D	F
	X	D																A	X
	D	V																X	D
RICHI 264	V	D																X	D
	F	F																D	V
	D	A																	

Third: With columns 16 and 3 placed in position in RICHI 266, the same columns must occupy a position as the first and second columns in RICHI 264. We had then to look in RICHI 266 for the columns which ended similarly to 16 and 3 in RICHI 264. These columns were found to be 15 and 4, and for reasons which we had stated in the former paragraph they must follow 16 and 3, since the identity of RICHI 264 will follow two spaces removed from RICHI 266.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
	16	3	15	4														5	9
RICHI 266	D	G	V	D														D	F
	X	D	F	F														A	X
	D	V	D	A														X	D
RICHI 264	V	D	D	F														X	D
	F	F	A	D														D	V
	D	A	G	X															

Fourth: In the same way columns 12 and 7 were placed in their positions as the fifth and sixth columns in RICHI 266 following the identity contained in columns 15—4 in RICHI 264.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
	16	3	15	4	12	7												5	9
RICHI 266	D	G	V	D	D	F												D	F
	X	D	F	F	A	D												A	X
	D	V	D	A	G	X												X	D
RICHI 264	V	D	D	F	D	X												X	D
	F	F	A	D	G	A												D	V
	D	A	G	X	F	X													

Fifth: This criss-cross building up was continued by the same process as has been described. It can be followed without the necessity of further explanation from the outlines as given:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
	16	3	15	4	12	7	6	18										5	9
RICHI 266	D	G	V	D	D	F	D	X										D	F
	X	D	F	F	A	D	G	A										A	X
	D	V	D	A	G	X	F	X										X	D
RICHI 264	V	D	D	F	D	X	A	A										X	D
	F	F	A	D	G	A	V	D										D	V
	D	A	G	X	F	X	F	D											

Sixth:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
	16	3	15	4	12	7	6	18	8	17								5	9
RICHI 266	D	G	V	D	D	F	D	X	A	A								D	F
	X	D	F	F	A	D	G	A	V	D								A	X
	D	V	D	A	G	X	F	X	F	D								X	D
RICHI 264	V	D	D	F	D	X	A	A	V	G								X	D
	F	F	A	D	G	A	V	D	V	D								D	V
	D	A	G	X	F	X	F	D	G	G									

Seventh:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
	16	3	15	4	12	7	6	18	8	17	1	19						5	9
RICHI 266	D	G	V	D	D	F	D	X	A	A	V	G						D	F
	X	D	F	F	A	D	G	A	V	D	V	D						A	X
	D	V	D	A	G	X	F	X	F	D	G	G						X	D
RICHI 264	V	D	D	F	D	X	A	A	V	G	V	G						X	D
	F	F	A	D	G	A	V	D	V	D	X	D						D	V
	D	A	G	X	F	X	F	D	G	G	F	D							

Eighth:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
	16	3	15	4	12	7	6	18	8	17	1	19	10	13				5	9
RICHI 266	D	G	V	D	D	F	D	X	A	A	V	G	V	G				D	F
	X	D	F	F	A	D	G	A	V	D	V	D	X	D				A	X
	D	V	D	A	G	X	F	X	F	D	G	G	F	D				X	D
RICHI 264	V	D	D	F	D	X	A	A	V	G	V	G	D	D				X	D
	F	F	A	D	G	A	V	D	V	D	X	D	V	G				D	V
	D	A	G	X	F	X	F	D	G	G	F	D	D	G					

Ninth:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
	16	3	15	4	12	7	6	18	8	17	1	19	10	13	14	2		5	9
RICHI 266	D	G	V	D	D	F	D	X	A	A	V	G	V	G	D	D		D	F
	X	D	F	F	A	D	G	A	V	D	V	D	X	D	V	G		A	X
	D	V	D	A	G	X	F	X	F	D	G	G	F	D	D	G		X	D
RICHI 264	V	D	D	F	D	X	A	A	V	G	V	G	D	D	F	X		X	D
	F	F	A	D	G	A	V	D	V	D	X	D	V	G	X	D		D	V
	D	A	G	X	F	X	F	D	G	G	F	D	D	G	D	X			

Tenth:

	1 16	2 3	3 15	4 4	5 12	6 7	7 6	8 18	9 8	10 17	11 1	12 19	13 10	14 13	15 14	16 2	17 11	18 5	19 9
RICHI 266	D	G	V	D	D	F	D	X	A	A	V	G	V	G	D	D	X	D	F
	X	D	F	F	A	D	G	A	V	D	V	D	X	D	V	G	D	A	X
	D	V	D	A	G	X	F	X	F	D	G	G	F	D	D	G	X	X	D
RICHI 264	V	D	D	F	D	X	A	A	V	G	V	G	D	D	F	X	D	X	D
	F	F	A	D	G	A	V	D	V	D	X	D	V	G	X	D	A	D	V
	D	A	G	X	F	X	F	D	G	G	F	D	D	G	D	X	X		

Having located the precise position of column 11 in RICHI 266 as the seventeenth column, our task was now a very simple one. Column 2 in RICHI 264 which corresponded in the identity of its letters with column 11 in RICHI 266 or the seventeenth column must occupy a position in RICHI 264 two columns removed from the seventeenth column. Accordingly upon the identification of this column in RICHI 264 as column 2 it was placed in its position as the fifteenth column. Column 14 adjusted itself by elimination, within the limits set by the division which has been described above, as the sixteenth column.

Column 14, now that it had been fixed as the sixteenth column, fixed also column 10 in the division alongside as the fourteenth column since the identity DVD in column 14 or the sixteenth column in RICHI 266 must be preceded by two columns in RICHI 264 with the same identity. This, therefore, at the same time fixed the position of column 13 as the thirteenth column since column 10 had been proved to be the fourteenth column as the columns were limited to one of the two columns, the thirteenth or fourteenth by the limits which had been fixed earlier in the study.

The two messages as they finally appeared were as follows:

	3	16	4	15	7	12	18	6	17	8	19	1	13	10	2	14	11	9	5
RICHI 266	G	A	V	G	V	D	G	G	X	G	D	D	V	F	F	F	V	G	V
	F	V	G	G	G	G	G	A	A	V	D	V	G	F	F	D	A	D	V
	X	G	V	G	V	D	F	X	A	F	A	V	D	D	V	G	V	G	D
	V	D	D	V	F	A	D	A	V	A	V	D	G	D	G	A	G	G	G
	V	V	A	G	D	V	V	X	A	G	A	F	A	D	G	G	X	G	D
	D	V	F	A	G	G	A	V	G	D	V	D	V	X	G	G	V	V	G
	D	F	G	F	D	X	G	G	A	D	V	V	A	G	A	F	X	G	V
	A	V	G	G	F	D	X	D	G	V	G	D	A	F	X	V	G	A	D
	A	F	F	X	G	F	A	D	V	G	A	V	D	A	D	X	G	X	F
	D	F	G	G	X	X	F	D	X	A	A	G	G	G	A	D	X	G	V
	D	G	F	F	D	X	D	A	A	A	V	D	D	X	D	X	A	V	V
	G	D	D	V	F	D	X	D	A	A	G	V	G	V	D	D	X	F	D
	D	X	F	F	D	A	A	G	D	V	D	V	D	X	G	V	D	X	A
	V	D	A	D	X	G	X	F	D	F	G	G	D	F	G	D	X	D	X

DEM NACH GEHEN NUMEHR SAEMTLICHE
SCHIFFE VON KOSPOLI NACH ODESSA BEZW. NIKOLAJEW.

	3	16	4	15	7	12	18	6	17	8	19	1	13	10	2	14	11	9	5			
RICHI 264	G	A	V	G	V	D	G	G	X	G	D	D	V	F	F	F	V	G	V			
	F	V	G	G	G	G	A	A	V	D	V	G	V	F	D	A	D	V				
	X	G	V	G	V	D	F	X	A	F	A	D	D	D	V	F	V	G	D			
	V	D	D	V	F	A	D	A	V	A	V	V	G	D	G	A	G	G	G			
	V	V	A	G	D	V	V	X	A	G	A	F	A	D	G	G	X	G	D			
	D	V	F	A	G	G	A	V	G	D	V	D	V	X	G	G	V	V	G			
	D	F	G	F	D	X	G	G	A	D	V	V	A	D	A	F	V	A	V			
	G	G	F	D	X	D	G	V	G	D	A	F	X	V	G	A	D	A	F			
	F	X	G	F	A	D	V	G	A	V	D	A	D	X	G	X	F	D	F			
	G	G	X	X	F	D	X	A	A	G	G	G	A	D	X	G	V	D	G			
	F	F	D	X	D	A	A	A	V	D	D	X	D	X	A	V	F	G	D			
	D	V	F	D	X	D	A	A	G	V	G	V	D	D	X	F	D	D	X			
	F	F	D	A	A	G	D	V	D	V	D	X	G	V	D	X	A	V	D			
	A	D	X	G	X	F	D	F	G	G	D	F	G	D	X	D	X					

DEM NACH GEHEN NUMEHR SAEMTLICHE SCHIFFE
VON KOSPOLI NACH ODESSA BEZW. NIKOLJEW.

The omission of the letter A in "NIKOLAJEW" in RICHI 264 was the only difference, beyond a few errors in transmission which distinguished the two messages.

It is interesting to add that work on the solution of the key was begun in the afternoon of November 2 and completed within an hour and a half.

Although we had no confirmation as to the number of days for which the key ran since we had received up to November 2 only messages of November 1, we had no hesitation in notifying the French and British Cipher Bureaus in Paris and London that the key which we telegraphed them was the key for November 2 and 3 as well as the 1st. Our supposition proved correct and we were enabled to decipher the messages for the following 2 days as soon as they were received from our wireless station.

NOVEMBER 4, 1918.

6. SPECIAL NOTE ON "RICHI" ADFGVX CIPHER

(*a*) The activity of the RICHI ADFGVX Cipher, although having abated somewhat since the conclusion of the armistice, continues greatly above its former normal record of August and September.

The solution of the key for messages of November 16, 17, 18 brings the total number of successive days for which the messages have been read to 22. The solutions comprise 7 different keys, 4 of which were solved by our office.

Since, from December 1 to the 21st of the month, messages will have been ciphered by the same keys as those of November 10–30, according to directions from the Chief Signal Officer in Berlin to the Black Sea stations as embodied in a deciphered telegram, it will be possible without further work to translate the messages of December 1–9, inclusive, with the keys which we have now solved.

(*b*) Commencing several days prior to the conclusion of the armistice, RICHI ADFGVX messages began to be intercepted which proved upon translation to indicate that stations in the rear of the German lines had begun to use this cipher in communication with German General Headquarters and amongst themselves. The same key in use between Berlin and the Black Sea area was employed. Traffic of this kind was particularly noted between two

stations, CM and CZ in the region of Metz, and between SY (Spa) and neighboring stations. This communication continued simultaneously with the use of the CHI ADFGVX Cipher which had been employed on the Western Front since March. While the key for RICHI ADFGVX has a life of 3 days, the keys for CHI ADFGVX have never been known to continue in use for more than 1 day.

(*c*) At the same time that the RICHI ADFGVX Cipher appeared on the Western Front, a form of transposition cipher suddenly appeared and was employed from a period beginning shortly before the armistice until only several days since.

The fact that the principle employed was that of a double transposition was confirmed in a message sent in the RICHI ADFGVX Cipher recently deciphered.

From station SY (Spa) to station RVV (location unknown), via station N4 (location unknown)
Sent at 21:03, 9 November; intercepted by station at G.H.Q., American E.F.
German text:

"UEBER 2 BAYRISCHE GENERAL-KOMMANDO, MUENCHEN: AN 7 RESERVENDIVISION: LANDWEHR REGIMENT; AN FECH: NICHT DURCH KABEL. ARMEESCHLUESSEL DOPPELT. EMPFANG BESTAETIGEN: O.H.L. ROEM. 1 ANR. 11338. GEHEIMORDRE."

Translation:

"To the 7th Reserve Division, Landwehr Rgt., for the Director of Railways, via the 2d Bavarian Army Staff: Do not send by cable. Key for the army is a double encipherment. Acknowledge receipt: Higher Command, 1 ANR 11338. Secret Order."

NOVEMBER 20, 1918.

7. NOTE ON RECONSTRUCTION OF AN INCOMPLETE ADFGVX MESSAGE

On November 3, 1918, a 13-part message from NKJ to LP (Constantinople to Berlin) was intercepted. Two of the parts were missing and the thirteenth, RICHI 222, lacked the last 67 and 11 additional letters. It was, however, translated without great difficulty, and it is worth while quoting as an interesting example of the treatment of the numerous garbled ADFGVX messages which are intercepted.

The message when properly set up appeared as follows:

3	16	4	15	7	12	18	6	17	8	19	1	13	10	2	14	11	9	5
F	–	V	–	–	D	–	F	–	G	–	G	G	A	V	G	D	A	D
X	–	F	–	–	D	–	X	–	D	–	V	D	V	G	V	G	G	A
V	–	G	–	V	D	–	G	–	A	–	V	D	D	V	F	G	A	A
A	–	A	–	D	V	–	A	–	G	–	F	F	X	G	D	A	G	G
X	–	A	–	A	V	–	G	–	V	–	G	D	A	D	–	D	D	V
F	–	F	–	G	D	–	A	–	V	–	–	G	X	G	–	G	D	F
A	–	F	–	–	A	–	G	–	X	–	G	G	G	D	–	V	G	A
D	–	G	–	–	V	–	D	–	D	–	F	X	–	G	–	G	G	G
G	–	G	–	–	D	–	V	–	V	–	G	D	A	G	–	V	G	F
X	–	G	–	–	–	–	D	–	–	–	D	X	V	V	–	X	V	–
D	–	D	–	V	D	–	X	–	F	–	X	X	G	X	–	X	F	F
F	–	A	–	D	D	–	A	–	V	–	D	X						

Now, by reference to the key-square which had already been obtained by the solution of the ADFGVX key for November 1, 2, and 3, it is evident that the initial combination (F–) may stand for any one of six letters or numbers, i.e., Ø, 2, G, 7, Q, or T, and so on for the remaining pairs. Fortunately, the missing letters fall in such a way that in all cases but five we are limited to a choice among six values. Therefore, by setting up the translation in the following fashion it was possible to pick out the correct letter by a process of elimination.

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

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

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

R U J
C I M
Z L H X
V O E
S F K
X 9 P
```

A study of the message when set up in this manner produced the following translation, in which there are two doubtful values, both of which are numbers:

(Continuation of Teil XII)

TEILEN DER X 11 X ARMEE DEN MARSCH DURCH UNGARN AUF OBER SCHLESIEN ANZUTRETEN X EINVERSTAENDNISS ERBETEN XX O X K X M X RM X 1 X A–GR –X OPX

ADFGVX KEY FOR NOVEMBER 1, 2, AND 3

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

H. C. SKINNER,
First Lieutenant, M.I.D.

NOVEMBER 4, 1918.

8. NOTE ON ADFGVX CIPHER
(Western Front)

STUDY OF KEY OF OCTOBER 8

The following trench messages were identified upon their interception as having similar beginnings. The third message, CHI 92 which factored similarly to the first message CHI 136 when a transposition length of 22 was assumed, was found to possess a signature of 26 letters which agreed with 26 of the 36 letters which formed the identical beginnings of CHI 136 and CHI 164.

Although five more lines were to be had in a message of CHI 110 which factored precisely for 22, experimentation with a few frequencies proved that, without more material, further work was useless. This was true despite the fact that frequencies were limited in one division to four columns, the long columns 1—14—21—22 and in another division to 4—18—20—15.

These facts more or less demonstrated the impossibility of a solution of ADFGVX where the number of lines fall short of 45—50. (The method of solution with similar endings where the key may be solved with but two messages is, of course, excepted.)

Previous work on the RICHI messages of September 13, 14, 15, where the transposition length was clearly 22, had proved that even with 35 lines, hope of a successful solution might be vain, particularly in this case where E was evidently the doublet VV and the text of the messages available for our purposes varied so greatly in subject matter as indicated by a count of the cipher letters.

Certainly, so far as the method of solution with a number of messages which factor exactly for the assumed transposition length is concerned, from experience with a number of such problems it would seem that, without as many as 40 lines at the least from which to base frequencies, one may entertain little hope of a solution.

The following numbers of lines were used in the three solutions by the exact factor method:

	Lines
June 3	87
Sept. 19, 20, 21	61
Oct. 4, 5, 6	69

I. SOUILLY 07.43 PPN v DOD 08.20

CHI-136

A X V D X G V F G A V D D V D X A A D X V D V G A V F X V V
A F V X A G D V V X X A A G G D X X G A X G X V D F X G V A
G X A G A X A G G G V X A G A D V G X X V G D V G X X V G
A A V G D V X D A G A D F G X G V G X A D G A X A X G G D V
X X D V A V D V V V V D V A X D N F D O D U M

II. G.H.Q. 09.36 DOD v —— 09.35

CHI-164

A X A V X V G A F G F V A D V D V V X F X V G X V V A X X G
V X A D D D D F X G F X V G V V F X V V A V G G V V A V – G
A G F X G G A F A V V V X D X A V V F D V A G V V D D G X G
A A F V G V X X V V V X F X A X V X X X G D V V A F A V A A
X X V F D D X G X X X X X D G F G A A X A G G V F A X A D V
A X G G A D V V X V X A A G

III. FRENCH STA. 18.47 —— v PPN 19.15

CHI-92

D A A A X G A A F D F X V X D V X V X – V A A X F V G A V D
V V G A A V A X A V F D V V X X V F D A D V D X X F X V G V
X X G D A V D A V A D V U X G V D G G V V G D D G D V D A X
V V

	1	14	21	22	2	7	8	11	18	19	4	18	20	15	3	5	6	9	10	12	16	17
CHI-136	A	X	D	V	F	V	G	X	G	D	X	X	G	X	V	V	F	A	F	G	V	A
PPN v DOD	X	V	V	V	G	V	G	A	A	G	V	G	G	V	D	F	V	V	X	G	G	G
	V	G	A	D	A	X	D	G	D	A	D	V	D	V	X	X	X	G	G	G	D	A
	D	D	V	V	V	X	X	A	V	X	V	G	V	G	A	V	A	X	V	V	V	D
	X	V	D	A	D	A	X	X	G	A	G	X	X	A	A	V	G	V	A	X	X	F
	G	G	V	X	D	A	G	A	X	X	A	A	X	A	D	A	D	D	G	A	D	G
	V	X	V	D																		

	1	14	21	22	2	7	8	11	18	19	4	18	20	15	3	5	6	9	10	12	16	17
CHI-164	A	X	D	V	F	V	G	X	G	D	X	X	G	X	V	V	F	A	F	G	V	A
DOD v ---	X	V	V	V	G	V	G	A	A	G	V	G	G	V	V	X	X	G	A	V	V	X
	A	V	A	X	F	F	V	V	A	G	V	X	V	X	X	A	G	F	V	V	A	X
	V	V	X	V	V	X	V	V	F	G	A	X	F	X	F	D	F	X	V	D	F	V
	X	X	G	X	A	V	A	F	V	A	X	X	A	X	X	D	X	G	V	D	A	F
	V	F	G	A	D	V	V	D	G	A	X	X	X	G	V	D	V	G	X	G	V	D
	G	X	A	A	V	A	–	V	V	X	G	X	A	D	G	D	G	A	D	X	D	D
	A	A	D	G	D	V	G	A	X	A												

CHI–92	D X D D G V D D A G X D G G D V A A X X G D
— v PPN	A X D A A G V V D V D V V V F X A A A V D A
	A F G X A A V V V D V V V X X – X V V F A V
	A X D V F V G X G G X X G X V V F A F D V A
	X V V V

NOVEMBER 4, 1918.

9. SPECIAL REPORT ON THE DOUBLE TRANSPOSITION CIPHER

(Employed between the German General Staff and General von Kress, Tiflis)

The inference that the transposition ciphers, which have been passing between Berlin and Tiflis were double transpositions, has been confirmed by two telegrams of July 23.

On July 23 two of these ALACHI telegrams were intercepted; One sent by LP (Berlin) to COS (Tiflis), and the other sent by OSM (Constantinople). This latter telegram was solved, having been found to consist of a simple transposition only. The first telegram, however, failed to yield to the same method.

The telegram was then subjected to a double operation of the transposition by which the one message had been solved, and it was found to yield itself immediately to solution.

Following are the two messages:

From LP to NKJ for COS. ALACHI 266:

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

From OSM to COS. ALACHI 152:

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

The key for solution of the second message was the simple transposition:

16–4–5–1–22–11–14–21–8–3–19–13–7–20–10–6–12–18–15–2–9–17

The first step in the solution of the first message was to transpose it thus:

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

The transposition is then repeated, as follows:

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

The encipherer at Constantinople was probably indifferent enough to consider that a single transposition was sufficient for security. That the practice, however, of using a single transposition in the ALACHI is not an isolated occurrence is indicated by a communication from the British which says:

"ITO CHI and ALACHI are both double transpositions for certain. The Boche has been making the error of using ALACHI as a single transposition in the Black Sea area; the keys change daily, and when used as a double transposition, no 'dummy' letter is inserted."

It is interesting to note the contrast between the careful methods of the encipherers at Berlin and those in the East. In the ADFGVX telegrams, Berlin never sends a filled-up rectangle, or if the rectangle fills itself up naturally, it is run over with the addition of X's. Among the Black Sea stations, the practice has generally been to fill the rectangle.

September 10, 1918.

10. SPECIAL REPORT ON CIPHERS

During the week of August 12–19, quite a few miscellaneous ciphers were intercepted by the high-powered station located at G.H.Q.

One of these was a simple substitution cipher passing between General von Kress at Tiflis, and Helferich at Moscow. It was probably the use of this system by General von Kress which was referred to in the solved messages of ADFGVX of August 8 and 9 in the following terms:

"The cipher method prepared by General von Kress was solved here at once. Its further use by OP is forbidden."

This same cipher had been noted previously as passing between SEW, a Russian station at Nicolave, and Army Group Eichhorn at Kieff. It would seem to indicate, therefore, that the use of this cipher was in more or less general use among German representatives in the Caucasus. No simple substitution ciphers have ever before been intercepted by us, so far as we are aware; in fact, the use of purely substitution methods of encipherment by the Germans on the Western Front is, and has been, since 1914, with the exception of a very short period, a thing utterly unknown.

A key for the ADFGVX cipher, employed between Berlin and Constantinople and the East, for July 22 was solved by means of the method formulated by Captain Painvin of the French Cipher Section in Paris, and explained in the report of last week. By this method it is possible to arrive at a solution with the text of but two messages, and without the labor of preparing great numbers of frequency tables. In fact, at the time of the first application of this method by Capt. Painvin on June 1, he completed the entire solution of the key within less than an hour, and from information contained in the telegrams he was able to warn the French of a heavy attack impending north of Montdidier.

Since July 3 messages passing between Berlin and General von Kress have been intercepted every few days. These messages give every appearance of being transposition ciphers, and in the opinion of the French and British experts, they are most probably a form of double transposition which the Germans have been known to make use of at various times since 1914. The system was in fact, the first employed by them on the Western Front.

Some hints as to the nature of the method are contained in the ADFGVX messages which were solved for August 8 and which read as follows:

"* * * The Alachi method is only to be used in communicating with places which employ the 'dividing system' (in ciphers). For other places, the new Itochi method with 'dividing system' was sent to Kress on July 18. New instructions regarding double transposition are shown. Wireless section, General Staff" (Berlin).

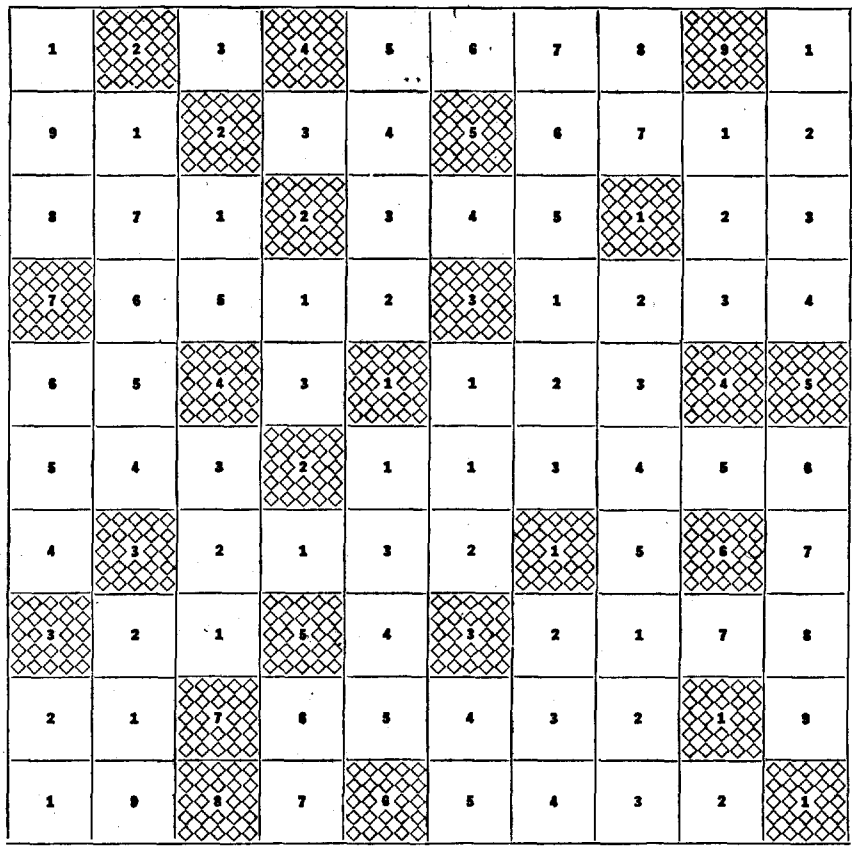
From this information it would seem that the preamble "Alachi", "Gechi", "Itochi", "Richi", etc., which always accompanies the German transposition ciphers, indicates in each case the particular method employed.

AUGUST 20, 1918.

11. TRANSLATION OF A CAPTURED GERMAN DOCUMENT

INSTRUCTIONS FOR GRILL CIPHERS

Preparation of the Grill.—(1) A square sheet of paper is taken and divided into smaller or larger squares, according to whether it is to serve as a grill for long or short messages. The following grill is for 100 letters, its sides being equal to 10 small squares. It is advisable to prepare the grill from colored paper, e.g., a cover for legal documents.



EXAMPLE

(2) The squares are then numbered consecutively in rings from the outside to the center, always with one figure less than that of the number of the small squares forming the outer edge.

(3) Each figure is then cut out once from each receding ring (lettered from outside to center as (*a*), (*b*), (*c*), (*d*), and (*e*)), thus: 1 once, 2 once, etc. Nine grill-holes are thus formed in the outermost ring (*a*) through the removal of figures 1–9, seven holes in the ring (*b*) (figs. 1–7), five holes in the ring (*c*), three in the ring (*d*), through the removal of 1, 2, and 3, and lastly, one hole in the center ring (*e*) through the removal of 1.

Since each figure appears once in each square, and a great many methods of arrangement are consequently possible, this system is proof against incompetent or unauthorized attempts at decipherment.

In the example, the small squares which, as a possible form, are cut out, are inked over.

(4) The following should be written at the corners of the grill: Left top 1; left bottom 2; right bottom 3; right top 4.

(5) If the side of the square is composed of an uneven number of small squares, the inner ring will not, as in the illustration, consist of four squares, but of one only, which, if the grill be turned, remains in the center. Such a single square is *not* to be cut out. The vacant space thus left is to be filled in with ink.

(6) Grills for 25, 36, 49, 64, 81, and 100 letters are to be prepared each week, and marked (25)Anna, (36) Berta, (49) Clara, (64) Dora, (81) Emil, (100) Franz.

Preparation of the cipher.—(7). The grill is chosen according to the length of the text, thus: for 38 letters, the Berta grill, for 55 letters, the Dora grill, for more than 100 letters, the Franz grill, etc. The grill is laid on a squared paper, as described in (1), the corner figure 1 at left top. The letters of the plain text are then written through the holes of the grill, from left to right, as in ordinary writing, up to the last hole. CH is taken as a single letter, there being a special Morse sign for it. The corner figure 2 is then placed at left top and the following plain text letters written through the holes which remain. The corner figure 3 is next placed at left top and writing resumed, the corner figure 4 finally being placed at left top, writing being continued through the holes.

(8) With a text longer than 100 letters, a new square is described in the same way, the corner figure 1 at left top, the grill being the same, or a smaller size. This second square may, or may not, be filled with text letters. When the clear text is finished, the word "End", or an X, may be written through the unfilled holes, the grill removed and the remaining space filled out with nulls.

(9) If a hole has inadvertently been omitted and remains unfilled at the end, an X is inserted in it.

(10) If the text contains fewer than 100 letters, so that not all the holes are filled, the word "End" or an X should be inserted in them and the process at the end of (8) continued. In the case of nulls, letters are not used in alphabetical sequence, as e.g., X, Y, Z, but in their order of frequency, thus many E's fewer N's, T's, etc., or, words quite irrelevant to the text are written in after the word "End."

(11) When the cipher is finished, a different figure, chosen at random, is each time attached to the null and the whole divided into groups, of 5, regardless of square and grill.

(12) Grills vary according to the length of the cipher text. Each telegram must therefore begin with the name in clear text of the grill or grills used. If "Franz, Anna" be used, the telegram must contain more than 100 letters, etc. The large Franz-grill is used for messages up to 100 letters, then the Berta-grill.

(13) The cipher-text follows in groups of five letters, with a period after each group. The receiving station returns each group as received to insure correctness; but the telegram is not repeated in entirety at the end.

(14) *Reception and decipherment of cipher.*—Paper squared in conformity with grills is kept in readiness at stations. The cipher letters, as received are written cross-wise on squared paper in the form of the grill whose name, in clear text, is the first word of the message. This name is noted down, but not spelled out nor recorded in the plain text.

(15) If the grill is now laid on the text, first with figure 1 at left top, the beginning of the message can be read through the holes. Thereupon, 2, 3, and 4 are laid in turn at left top, until the entire text has been read.

(16) This grill-process is adapted as well to telephonic conversations and to correspondence in which secret orders are given and in which the so-called "General Staff Process" must not be employed.

Translated OCTOBER 23, 1918.

12. A MECHANICAL METHOD FOR DETERMINING THE KEY FOR THE TRANSPOSITION IN ADFGVX CIPHERS, GIVEN TWO MESSAGES WITH SIMILAR ENDINGS

This memorandum will use for its examples the messages given in the memoranda dated November 1, and November 4, 1918, this office.

MEMORANDUM OF NOVEMBER 1.

After having identified the similar sections, the messages were set up as shown below (cf. pp. 36 and 37):

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
RICHI 374	A	A	G	A	G	V	V	A	F	F	F	D	X	A	V	A	X	G
	A	A	X	A	X	X	X	D	D	X	D	F	D	F	V	G	F	F
	X	F	A	G	D	G	D	A	A	F	X	F	F	V	V	A	G	D
	F	A	A	V	X	F	A	V	V	D	G	A	G	A	A	D	X	G
	A	A	A	G	G	X	X	A	A	F	X	A	D	F	X	V	F	D
	V	D	X	D	X	V	F	A	V	X	A	F	X	X	G	G	A	V
	D	A	F	X	F	F	A	A	F	X	D	X	X	X	A	V	F	X
	X	V	F	X	X	D	X	D	G	D	X	G	D	X	F	V	V	F
	F	D	A	V	X	A	X	G	A	A	X	A	F	A	A	D	G	F
	D	A	X	G	V	F	G	F	F	X	X	D	X	F	A	A	F	D
	D	X	V	A	V	F	V	X	F	V	D	D	X	F	A	A	X	D
	A	A	A	A	D	A	F	D	A	D	X	F	A	F	D	A	F	X
	G	A	A	V	X	D	X	X	D	X	F	G	G	A	A	V	D	X
	A	D	V	D	G	F	V	A	A	A	X	V	A	G	A	V	A	X
	A	X	D	A	V	A	V	D	A	A	X	A	D	F	X	X	V	X
						G						X			V	D		
RICHI 338	V	V	D	A	F	V	A	X	F	D	A	D	A	D	G	D	G	X
	A	A	D	D	F	A	A	X	D	A	D	D	X	A	X	F	F	G
	X	A	F	G	V	A	V	X	X	X	G	A	G	F	A	X	F	G
	V	A	V	A	F	D	D	X	A	G	V	X	A	X	D	X	D	A
	V	G	X	G	X	X	A	F	A	X	X	F	G	F	A	A	F	F
	V	A	D	X	F	D	A	D	G	D	G	D	F	X	D	A	F	V
	A	D	A	A	G	F	F	A	V	X	F	X	D	F	A	X	A	A
	X	V	X	A	X	G	A	V	G	G	X	G	G	D	V	F	A	F
	G	G	F	A	F	D	A	A	D	X	V	X	D	F	A	A	F	X
	A	V	A	X	A	X	D	V	X	F	F	A	V	X	A	V	X	X
	F	V	X	F	F	X	A	F	X	X	D	D	X	X	A	D	G	X
	A	D	X	F	V	D	V	G	V	X	A	X	F	D	D	X	A	A
	A	A	G	A	G	F	D	A	G	V	F	X	F	A	G	F	D	F
	A	A	V	X	F	X	A	F	A	V	F	X	D	X	F	D	D	F
	D	A	F	V	X	A	X	F	A	D	A	D	D	V	X	D	F	F
	A	V	X	A	F	A	A	A	V	X	D	X	X	D	D	A	G	A
	A	V	V	A	D	G	A	D	D	G	F	F	X	X	X	G	V	G
	X	X	V	V	A	A	D	A	A	V	A	X	X	A	A	A	A	F
	V	D		D	V	D	X	A			G	X	X	A	D	A	X	

Let us now draw up a table showing the equivalency of the various columns, upon the basis of each pair of columns whose last three or four letters are identical.

RICHI 274 RICHI 338

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

As regards the mathematical relations alone, the sequence of numbers in the transposition key may be regarded in the nature of a cycle. The determination of the transposition key, therefore, consists of two steps:

1. Building up the numerical sequence in the key, i.e., the cycle.
2. Finding the exact position of one column in the cycle.

1. Since RICHI 338 has 14 long columns, and RICHI 274 has 4 long columns, then it is evident that the identities in these two messages run along at an interval of 14 minus 4, or 10 spaces. The columns whose equivalencies are shown in the preceding table, therefore, will be 10 spaces apart in the cycle. That is, for example, if we begin to build up the numerical sequence by placing column 1 under a space marked "1", on cross-section paper, then the equivalent of column 1, which is column 16, should be placed 10 spaces removed from the position occupied by column 1 in the cycle, i.e., under the space marked "11"; and the equivalent of column 16, which is column 2, should be placed 10 spaces removed from the position occupied by column 16, etc. Since the numerical sequence is in the nature of a cycle, as stated above, when one arrives at the extreme right of the series, one merely comes back to the extreme left and continues. To make the procedure perfectly clear the successive placements for six columns, beginning arbitrarily with column 1, are shown herewith:

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

Continuing this procedure, the completed cycle is as follows:

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

2. Referring to the set-up of RICHI 274 as shown above, it is seen that the long columns are 6, 12, 15, and 16, and therefore they constitute the first four columns on the left. The cycle shows that column 6 precedes the others in the sequence; that is, it is on the extreme left in the transposition key. The completed key may be written, therefore, merely by advancing the series of numbers in the cycle so that 6 comes first. Thus:

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

MEMORANDUM OF NOVEMBER 4

The two messages, after the identities had been found, were set up as follows:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
RICHI 264	D	F	G	V	V	G	V	G	G	F	V	D	V	F	G	A	X	G	D
	V	F	F	G	V	A	G	V	D	V	A	G	G	D	G	V	A	G	D
	D	V	X	V	D	X	V	F	G	D	V	D	D	F	G	G	A	F	A
	V	G	V	D	G	A	F	A	G	D	G	A	G	A	V	D	V	D	V
	F	G	V	A	D	X	D	G	G	D	X	V	A	G	G	V	A	V	A
	D	G	D	F	G	V	G	D	V	X	V	G	V	G	A	V	G	A	V
	V	A	D	G	V	G	D	D	A	D	V	X	A	F	F	F	A	G	V
	F	G	G	F	F	V	X	D	A	V	D	D	X	A	D	G	G	G	A
	A	G	F	G	F	G	A	V	D	X	F	D	D	X	F	X	A	V	D
	G	X	G	X	G	A	F	G	D	D	V	D	A	G	X	G	A	X	G
	X	A	F	D	D	A	D	D	G	X	F	A	D	V	X	F	V	A	D
	V	X	D	F	X	A	X	V	D	D	D	D	D	F	D	V	G	A	G
	X	D	F	D	D	V	A	V	V	V	A	G	G	X	A	F	D	D	D
	F	X	A	X		F	X	G		D	X	F	G	D	G	D	G	D	D
RICHI 266	D	F	G	V	V	G	V	G	G	F	V	D	V	F	G	A	X	G	D
	V	F	F	G	V	A	G	V	D	F	A	G	G	D	G	V	A	G	D
	V	V	X	V	D	X	V	F	G	D	V	D	D	G	G	G	A	F	A
	D	G	V	D	G	A	F	A	G	D	G	A	G	A	V	D	V	D	V
	F	G	V	A	D	X	D	G	G	D	X	V	A	G	G	V	A	V	A
	D	G	D	F	G	V	G	D	V	X	V	G	V	G	A	V	G	A	V
	V	A	D	G	V	G	D	D	G	G	X	X	A	F	F	F	A	G	V
	D	X	A	G	D	D	F	V	A	F	G	D	A	V	G	V	G	X	G
	V	D	A	F	F	D	G	G	X	A	G	F	D	X	X	F	V	A	A
	G	A	D	G	V	D	X	A	G	G	X	X	G	D	G	F	X	F	A
	D	D	D	F	V	A	D	A	V	X	A	X	D	X	F	G	A	D	V
	V	D	G	D	D	D	F	A	F	V	X	D	G	D	V	D	A	X	G
	V	G	D	F	A	G	D	V	X	X	D	A	D	V	F	X	D	A	D
	G	G	V	A	X	F	X	F	D	F	X	G	D	D	D	D	D	X	G

The table of equivalents is as follows:

RICHI 264 Column		RICHI 266 Column
1	equals	10
2	equals	11
3	equals	4
4	equals	7
5	equals	16
6	equals	8
7	equals	18
8	equals	1
9	equals	3
10	equals	14
11	equals	5
12	equals	6
13	equals	2
14	equals	9
15	equals	12
16	equals	15
17	equals	19
18	equals	17
19	equals	13

The identities in these two messages run along at an interval of two spaces (RICHI 266 may be considered as having 19 long columns, RICHI 264, 17). Therefore, the equivalents will have to be placed two spaces apart. The completed cycle is as follows:

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

The set-up of RICHI 264 shows that columns 5 and 9, being the only short ones, fall on the extreme right. The cycle shows that column 5 follows column 9 in the sequence. The completed key may be written, therefore, by advancing the series of numbers in the sequence so that number 5 occupies the position on the extreme right. Thus:

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

The interval, i.e., the number of spaces which must be left between equivalents in constructing the cycle, will be even in number in all cases, since it takes two cipher letters to make one clear-text letter. In cases where the number of columns and the interval possess a common factor, the condition might arise where the cycle cannot be completed in one step, for after a few placements have been made, one comes back to the starting point. In such a case, however, one can complete it by taking advantage of such clues as are offered by the set-up of the messages, specifically, the number and identities of long and short columns. It may be well to

illustrate by one artificial example. Given two messages in which the interval is 2, the long columns 9, 10, 14, and 18, and the following table of equivalents:

TABLE 3

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

Starting with column 1, the following partial sequence is constructed:

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

The equivalent of column 4 is column 1, and we are then brought back again at our starting point. The cycle shows, however, that column 10 succeeds column 9, with one column intervening. Since columns 14 and 18 are long also, and since the table shows column 18 to be the equivalent of column 14, it is evident that the latter must be placed between columns 9 and 10, and column 18 between columns 10 and 4. From there on the sequence can be completed without further difficulty.

The advantage of this method is that it is almost entirely a mechanical one, and may save time in determining the transposition-key in this cipher. It is also evident that it may be used in ordinary simple, transposition ciphers of the columnar type.

WILLIAM F. FRIEDMAN,
First Lieutenant, M.I.D.

January 6, 1919.

○