~~CONFIDENTIAL~~

315

Record taken from WFF's home

~~CONFIDENTIAL~~

Declassified and approved for release by NSA on 01-22-2014 pursuant to E.O. 13526

REF ID:A60198

~~CONFIDENTIAL~~

ARMY EXTENSION COURSES

SUBCOURSE

MILITARY CRYPTANALYSIS, PART III

SIMPLE TYPES OF APERIODIC SUBSTITUTION SYSTEM

1938-39

(Introduction and Lesson 1)

OFFICE OF THE CHIEF SIGNAL OFFICER
WAR DEPARTMENT
WASHINGTON, 1938

~~CONFIDENTIAL~~

REF ID:A60198

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

REF ID:A60198

~~CONFIDENTIAL~~

ARMY EXTENSION COURSES

Subcourse--Military Cryptanalysis, Part III
Simple Types of Aperiodic Substitution Systems

Introduction

Purpose and Scope:

The purpose of this subcourse is to teach the methods of analysis of some of the more simple varieties of aperiodic substitution systems. To a lesser degree it is intended also to develop the student's ability to ascertain, by cryptanalytic methods, the general system upon which a cryptogram that is to be solved is based.

The scope of the subcourse is: More complex types of poly-alphabetic substitution systems; auto-key systems; interrupted, variable, and non-periodic key systems; systems employing lengthy keying sequences.

Number of Lessons and Approximate Time Required:

This subcourse consists of 12 lessons each of which will probably require approximately 5 hours of work by the average student.

The time indicated above is only an estimate and should be considered merely as a guide. It does not in any way limit the time that may be devoted to each lesson or to the subcourse as a whole. No further mention of the time required will be made in the lesson assignments.

Texts Required:

Military Cryptanalysis, Part III, Aperiodic Substitution Systems, 1938, as prepared under the direction of the Chief Signal Officer.

Materials Required:

Since only the usual cross-section paper and frequency table forms will be required, no further mention of these items will be made in the lesson assignments.

Special Instructions and Information:

Each lesson assignment has a maximum weight of 100. So far as practicable, detailed work sheets which usually form a part of the solution should be submitted with the solutions. They will be returned to the student for file or further study. DO NOT RETURN THE LESSON

SHEETS UNLESS WORK IS SHOWN THEREON. In all cases show the primary components and keys from which derived.

It is essential that the student first read the entire text before attempting to solve any of the problems. This will give him a general background of all the principles and methods covered in the subcourse and will materially assist in the solution of the specific problems in the various lessons. Of course, further study of specific portions of the text will be necessary but the student will have to use his own judgment in this regard. No text assignment will be indicated as specifically applicable to any lesson. Nor will the subject-matter to be covered by each lesson be indicated, as is usually the case in these subcourses, the purpose being to give the student a little practice in ascertaining, by cryptanalytic methods, the cryptographic system involved in a cryptogram to be solved. Of course, no lesson contains a problem involving principles beyond the scope of this and the preceding two texts in cryptanalysis.

The student is urged to apply the principles explained in the text in solving the problems, even though solutions may be obtained in some cases by other means. Only by understanding each principle in turn will progressive results be obtained.

A guiding principle in the solution of any problem should be: ALWAYS TRY THE SIMPLEST THING FIRST.

The text of all messages will be military unless otherwise stated.

****

LESSON ASSIGNMENT

SUBCOURSE - Military Cryptanalysis, Part III

LESSON - 1

Weight:

15 1a. Solve the following message:

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

Q D U O F Z C P M Z Q R Q G E X O G O F Z P Y W N W O C F H

K K J G X T B G T C Q D Z Q R

5 b. What is the keyword for the message?

REF ID:A60198

Weight:

30 2. Solve the following cryptogram, in which the text has been allowed to remain in its bonafide word lengths:

N P M E S S E V Z A X M P E C E N G Q A N T J O L A B W Y S

V K V R J J Z O D Z L A K V E F H E L S B A F I X

J U X M C E N T S B G T F P P B D D R L C E Q S B E B P V E K S

E J V J Z D J X T B L E Q E U P Z Z P S J F S O D

R I Y K J R X B B T N K K B C P Z E J U L Z B N M K Z N R J E

40 3a. Solve the following cryptograms which are in the same key:

No. 1

S I I S A J C I O L A H S X V Z C G E W E A E A D X T V F A

L P T I B K T Q W G T A V T A J V R Z D S R I T Q D G L W M

M S G U X K P P R S A R J S U O Z T G U R U Z G A E D I X N

I T L M I Q Z K R M P J C G T Q T A M A Y A C W R A L A H A

Z M V L M P G D G A S E A G H I T L C K E Z H L M K C E F G

S F M E S H X L C V H P M P B N L B Z R S S I B G W G S M S

A I Z O W E A Z R S N R J M T S Q S E C K D H S G H V F Z V

F M H G Z E K E E V R K D A G S E A A E V I X W B Z G N L Z

N R J M E W E S C K D H S C H

No. 2

W G W H P L B Z R S S I B G V S R W W X B F J C G P R X Q A

Q R D L C V H H P D G Z V K U T A T A M Y Z Y I M N R J R M

R K A H I K R B R U C Q X C R J M L Y X

5 3b. What relation, if any, can you find between Problem 2 and 3a?

Weight:

5 3c. The following cryptogram was sent later on the same day by the same headquarters that sent the one given in Problem 3a. Solve it.

M S O W S A E N Q R K S U B W W N Y O Y W Z E H M B P N Z R

A X N D Q D G X X X

REF ID:A60198

ARMY EXTENSION COURSES

LESSON ASSIGNMENT

SUBCOURSE - Military Cryptanalysis, Part III.

LESSON - 2

C O R R E C T I O N

Problem 3 should read - "The enemy is using the word-length keying system exemplified in Problem 2, but the primary components are differently mixed sequences. The letter Z_p is employed as word separator. The following message has been intercepted. Solve it, reconstruct the primary component and the key for the message."

REF ID:A60198

ARMY EXTENSION COURSES

LESSON ASSIGNMENT

SUBCOURSE - Military Cryptanalysis, Part III

LESSON - 2

Weight:

30 1. Accompanying this lesson sheet is a paper entitled "Instructions relative to a cryptographic system originated by Mr. X." These instructions describe one of the many systems submitted to the War Department for consideration for military use. The description is in the "inventor's" own language and includes one sample message, the key for which he gives, and one test message concerning which he says: "As I alone know the key words of the message below, it should prove a good example to test the efficiency of my cipher." You are to solve his test message.

30 2. The following has been enciphered by means of a disk similar to the obsolete U.S. Army disk except that both primary components are the same mixed sequence, proceeding in the same direction. The successive plain-text words are enciphered by successive keyletters of a keyword. Solve the message, reconstruct the primary component and find the keyword for the message.

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

Military Cryptanalysis-Part III, 2-p.l.,1938.

Weight:

2. Continued:

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

	5				6				
K.	D	J	Q	X	B				
L.	P	P	N	X	A				
M.	J	D	C	W	Y				
N.	I								

40 3. The enemy is using the word-length keying system exemplified in Problem 2, but the primary components are differently mixed sequences, the letter Z_p being employed for this purpose. The following message has been intercepted. Solve it, reconstruct the primary component and the key for the message.

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

"INSTRUCTIONS RELATIVE TO A CRYPTOGRAPHIC SYSTEM ORIGINATED BY MR. X"

- - - - -

!

Lay out the working form as follows:

(Material required: Pencil, Paper and Dividers.)

1. On stiff paper, scribe a circle 3 or 4 inches in diameter.
Divide the circle into 26 equal spaces.
Letter into these spaces the letters of the alphabet, A to Z, pointing the base of the letter toward the center of the circle.

Inside of the line of letters, number the spaces 1 to 26, starting with A.
Now cut out the circle and lay it aside.

2. Scribe another circle of same size, on another piece of paper.
Divide this into 26 divisions, with the dividing marks on the outside of the periphery of the circle.
Into these spaces letter in the letters arranged in a form specified in the following paragraph:

3. On a scrap of paper, set down the letters of the alphabet.
Under these letters, set down the prearranged secret key word or sentence. (In enciphering the enclosed message, I used GIMPY FURBELOW.)
Cancel out of the full alphabet all of the letters contained in the key word.
Now set down the first letter of the key, and follow it with the first letter remaining uncancelled in the alphabet. Then the second letter of the key, followed by the second remaining uncancelled letter in the alphabet above. Continue until all the letters have been used in both. Example:

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

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

Now, keeping A near the top, letter into the spaces, from left to right, the letters formed by the combination above. (It will be found easier to read if the letters are inserted with the bases all pointing toward the bottom of the sheet of paper. The sheet of paper does not move, as is the case with the circular out-put.)

You are now ready to start to encipher.

4. Place cut-out circle on top of circle on sheet, pinning at centers so the cut-out will revolve and the respective letters of each circle will match up.

A

Set the space 1 on the rotating circle opposite A on the stationary circle.

Now move the rotating circle (top) to the left as many spaces as the date of the month. (In the sample message it is the 6th.) Moving the top of the circle to the left progresses up in numbers and toward Z in the alphabet.

This brings us to $\frac{A}{7}$, from which point we encipher our first word of our sample message, the rotating circle being used for the regular word, and the code word being derived from the stationary or outer circle.

When the word is finished, add the code letter for Z.

Now move the rotating circle ahead (top to left) as many spaces as there were letters in the word immediately preceding, not including the added Z.

(In dividing cryptographic messages into letter groups of five, the addition of the letter Z to each word minimizes possibility of error in deciphering. Also the words ending in Z are very few, and in ZZ, none. If such an ending were encountered in foreign proper names, the instances would be so rare as to make the verification of same necessary.)

In the message dated August 6th, we start at $\frac{A}{7}$, and our first word KUMPE will encipher DQHFZL. Moving five spaces ahead brings us to $\frac{A}{12}$, and COLONEL becomes EMAMCLAQ. Grouped into fives, we have DQHFZ LEMAM CLAQ etc. Note that E was Z in Kumpe, but is L in Colonel.

And so the enciphering process continues until the message is completed.

5. DECIPHERING is simply a reversal of the foregoing.

The receiving operator builds up his daily layout along the identical lines employed by the sending operator.

6. The key word, words or sentence may be made up of a thousand different combinations of 13 letters.

The key word for tomorrow, or next changing date, can also be incorporated in any regularily ciphered message with safety.

REF ID:A60198

SAMPLE MESSAGE

August 6th, 1930.

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

As I alone know the key words of the message below, it should prove a good example to test the efficiency of my cipher. Exactly following the layout of the other one, and enciphered by employing the same system, it may give the "enemy" something to do to decipher it.

TEST MESSAGE

August 5th, 1930.

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

Military Cryptanalysis-Part III, 2-p.5,1933.

REF ID:A60198

LESSON ASSIGNMENT SHEET

SUBCOURSE - Military Cryptanalysis, Part III

LESSON - 3

Weight:

8 1a. Solve the following cryptogram:

A X K B Y L B L X K L G B J O B V X Q X K R V G E C U C U O

P H Q D Q D Y U G X K L V A X K J G D D M D F Q R Y X E J Y

Z R Z Z D D E R Z Y Z V V F M C J V U Z Y W J P L B N M O K

Z D Q

2 b. What is the keyword and how does it control the shifting of the primary components?

8 2a. Solve the following cryptogram:

X J H F E U S R B B I T L R N F Y Q R Y I J S Z G G F J Z B

Q W V R Q W C Q R Q J M U J T W R D S I W A M P L O L

2 b. What is the keyword and how does it control the shifting of the primary components?

30 3a. Solve the following cryptogram:

Z S I I F Q V Z O R V S Q Q X U T Y V L B R A A X H X Y C R

I E C N N F B H C D G R Y Z A Y M L E M Y Z A U C M Y L Z B

K L L Z S I J F Q V Z O R V S Q S F C P C M C X H H C Z C D

C R I Y I B D T K Z Y B O C Y L U B D N C F B U V Y U W V Q

Q V Q W O R K U F B M V F B W X K V M V F B Y S X C G S X T

H C R D C N B Y T L X A U U N L G N W L K O L E M Y Z A M Z

S Q R O Z R P V R N U B D U N P T D F B B I Q T H B D S R U

I D Y C H U R R Z S D H E B D U S I D T M Y U D U X R D V Z

R U L U B P Z Y B O G U V S X R X S Y Q X B V Y C X B Q B I

S D

Weight:

b. Having found the primary components, solve the following cryptogram which is enciphered according to the same system but with a different key.

C W I E Q G E R O M V S Q P V M M O X X D U H E D G K E W G

U K F Q Z R V S Q A V G U U V O P C G D S M J H O K J R D O

Q X B S D R O R V S B I C M V I E K Y O E E J B I

c. What are the keys upon which the cryptograms under a and b are based and what controls the number of letters enciphered by each alphabet?

4a. The enemy is using the system exemplified by Problem 3a. The primary components and the keyword change every day. From cryptanalytic work on his previous traffic it has been noted that three stations in a certain radio net always begin their messages with the enciphered serial number of the message. (Example: N U M B E R T W E L V E X) The last deciphered messages exchanged among these particular stations were found to begin with the serial numbers shown below:

From Station	To Station	Serial No.
A	B	17
A	C	15
B	A	14
B	C	16
C	A	21
C	B	11

The next day the following were the first cryptograms to be intercepted between the stations indicated. Solve the messages, ascertain the primary components and the daily keyword.

No. 1

From B to A

U H O K B D Q F Q E H U I A U I O U M U I F S D C O Q G C C

O Y Z F C I P H D B L Z P B I T C A B P B U I J K X G I U O

Y

Weight:

No. 2

From C to A

U H O K B D P N B F E N Y P G A O C O U M I D B R W I C O Y

S I P O X J G C P B L J H I G J O O C U L I J M E A P B V V

U H P O

No. 3

From A to C

U H O K B D Z F M E H U I A I U O K Z A H U H B O F H R D O

Y H L K F A F Z F J U Q F R X L G J L B U H O T H O K G F O

5 4b. What principal lesson does this particular problem teach you as a cryptographer? As a cryptanalyst?

ARMY EXTENSION COURSES

Subcourse--Military Cryptanalysis, Part III,
Aperiodic Substitution Systems.

LESSON ASSIGNMENT

SUBCOURSE - Military Cryptanalysis, Part III.

LESSON - 4

Weight:

30 1a. Solve the beginnings of the 35 messages given in Paragraph 20b of the text. A work-sheet copy is attached.

1 b. What is the keyword for the messages?

3 c. Indicate the primary components.

1 d. What is the interruptor and upon what does it act?

35 2a. The thirty-five messages just solved were the traffic of the eighth of the month. The first message intercepted on the ninth is below. Solve the message and determine the key.

C. O. 95th Infantry

J T K F L Q J D L F I J R H R P M T O K W A H C B T G D H H

L S O S R P K H T I X S D I F L U F R S Z Z S Q V S F Q H C

S H J S B D Z M K P E W I D M I X G C K X

Smith, Brigadier General

30 3. The following message was intercepted on the tenth of the month (the next succeeding day after the message of 2 in this lesson). Solve the message and determine the key word.

P V E S K W V H B P Y I R I S X H H T H J Z K U G U G L W Z

Z S Z P D J A V E A I E C W H Y Y I J I Z V Q H H M L A A M

H K D H Z U Z O T Q L E U E G C E Q W G E U U C X L J U X Q

A P M P X M V Q H H M L X Q J Z Q U R R R U L L O L D P N M

Weight:

M V X S V U Q W O Q V E V C H K K B B U M O F A S S H G X P

W V L S H K K D B L X O H Q H S F J J C B U M F D B I K W V

H B P L F E S R B S B Q W A B C P L G H H K T L D G F Q X V

N D E V B P G O V Q H H M L R O U R D C D S K U W Q W V N V

X S V U E U D K R S

Military Cryptanalysis, Part III, 4-p.2, 1938.

LESSON 4 - Problem 1

MESSAGES WORK SHEET.

(1) Z C T F Z W Z P E F Z Q X

(2) W T E Q M X Z S Y S P R C

(3) T C R W C X T B H H

(4) E F K C S Z R I H A

(5) Y A N C I H Z N U W

(6) V Z I E T I R R G X

(7) H C Q I C K G U O N

(8) Z C F C L X R K Q W

(9) H W W P T E W C I M J S

(10) E P D O Z C L I K S J

(11) W T S S Q Z P Z I E T

(12) Z C G G Y F C S B G

(13) C W Z A O O E M H W T F

(14) C I Y G I F B D T V X

(15) E A Q D R D N S R C A P D T

(16) Y F W C Q Q B Z C W C

(17) W T E Z Q S K U H C

(18) Z C V X Q Z K Z Y D W L K

(19) A F E O J T D T I T

(20) K P V F Q W P K T E V

(21) Z A B G R T X P U Q X

(22) Y H E O C U H M D T

(23) C L C P Z I K O T H

(24) A F L W W Z Q M D T

(25) Z C W A F M B S A W L

(26) H F L M H R Z N A P E C E I

(27) C L Z G E M K Z T O

(28) T P Y F K O T I Z U H

(29) Z C C P S N E O P H D Y L

(30) C I I G I F T S Y T L E

(31) I T S V W V D G H P G U Z

(32) N O C A I F B J B L G H Y

(33) X X X F L F E G J L

(34) Z C T M M B Z J O O

(35) H C Q I W S Y S B P H C Z V

Military Cryptanalysis, Part III, 4-p.3, 1938.

REF ID:A60198

ARMY EXTENSION COURSES

LESSON ASSIGNMENT SHEET

SUBCOURSE - Military Cryptanalysis, Part III

LESSON - 5

Weight:

10 1. Solve the following:

K G G L N G S A H Z O K K T A S H W S P D Y Q Z V E A L X G

N J G F B I M I E R F M D P R P I O Y V O O B Y X X G V H L

G P B P W A M T M E N U W D P W P Y U Q Q E

NOTE: ADDITIONAL MESSAGES, IF FOUND NECESSARY, WILL BE GIVEN UPON REQUEST.

30 2. The following are the beginnings of 45 military-text messages. Solve them, reconstruct the primary components, and briefly describe the system of encipherment employed. Submit the beginnings of the first 5 messages only.

1. S C O P A K F B U C G I M J V

2. H H T G M G Y H K G Q G N I C

3. S R L E N T R C T R A R U B W

4. V L R E N M L U T J D Q E X O

5. L Z V S I E O O A T G U N V T

6. H Y L V D A O T E X W W T A I

7. Y O Q N M P D Q B Q Y I Z U A

8. Z O W K X R K I V R W K K C J

9. C G U Q V R B H O S S X O X R

10. S R R K M A L W Z J A K K M X

11. C A U E J Q T L E Z V H J E U

12. C Y U Q N C H A X X U N R F A

Military Cryptanalysis, Part III, 5-p.1, 1938.

Weight:

13. U O I S V R O J H E J B R H I
14. N R I G F U W Z P A H Z C D T
15. Y O K E R H N S G Z O B A C N
16. O Y T Y R D G C N E J Q H N G
17. V B L S Q Z B D J Q I K P Z V
18. T H N P R B O E F L H X S M K
19. O Y U X I R B W B E L J I M S
20. S R L M R Q F Y T S V V I T Q
21. M H T C Y D G Y Y J V V E B Z
22. C M W E X L R O X M Q V V I T
23. S R L I K D K Q T V W S D X K
24. N O R K G X I W I W M I Z W W
25. Y T B U M N I X Y W V D H E Z
26. W T T G Y C T L M R U I Y W B
27. C W J Y I H H J O I A T S G T
28. Y O P X I Q K A Q R W A R A H
29. C M W Q G H Q A J F N Z R Z F
30. F T W Q G R C E N B F Z E E F
31. T O T I F Z T H U Y R S O W J
32. E Z V W N K P V O W K R L C R
33. T Z W K D C T K O W T L K G Z
34. V B L S G N N J U O B U P X B
35. U Z B N I K B F U I O Z R D M
36. E Z K V F W G G E G O U Y Q K
37. N R L W B H N P U U L A U H Y

Military Cryptanalysis, Part III, 5-p.2, 1938.

Weight:

38. D O R K F H K H I F M D H M J

39. Z A I G R K Q O O W O L I A W

40. C S J E N V M Z X D X M U X T

41. E H W E V S E H E M Q X W I V

42. O Y B E X D O A Y X F Z W U L

43. Y O T K I T T H C P D A T H D

44. Z L P Y V C E D J S K E S S H

45. Y H U Q Y H N P Z E W A U C I

50 3. Solve the following messages, which are all enciphered by the same primary components.

1 2 3 4 5

I.

A. T R S P W G K X G X G J C X Z I R L T K E V V L X

B. L Y L L Y D X Z Z P U A M H Z X L N C Q J T X Y L

C. B P Y M V Z B Q B B F U V V A S F S B N V S P P M

D. P X Y G W C W L J A Z J A Q A W C R N D D C C I M

E. H J A U P U N S D L C L J A D K X X H G F Z C W S

F. B A U V G H P T F U M K K H M X G E X X

II.

G. Z S O P P R R Y N P G D U N S H H A L I P P Q H D

H. W X Y L B P W W G C B T T G D V A B M W D C G Y D

J. X D B Q U T Q U J U D V P W W N G M H Q S S F S K

K. S R M H J O F Q W R F R R M W U E I G J M H Y E G

L. J J K S H B H Q X E A K K N N Y M H B X

REF ID:A60198

Weight:

III.

A. H N F D R E R R Z T S X X Z P F L J Q U E F I X K

B. H J F Q X Z N T B T B M W S H C Y B S K O N E O R

C. R N K E D H R Y E E

IV.

D. Z J D O H H N D K W G Y G L C B S K O X H J Y B E

E. G H G G U U L I I P U Z K E T T Z B G A A A P P G

F. F V E T J Y N S K M H J V P I K P W D C W X X X X

V.

G. T K K L S G D C W G D O F V A U T W S D S O B G H

H. H C M S V E V V S X P V W P R G G L R R E O W S Q

VI.

J. J U Z P C C G H G G A L I R G G T N P W J T F I Z

K. C F F Z I B L Q Z D W P U V V V H C B G B B F M S

L. C C T B F M X X X X

VII.

M. V V W J K S R L K S E R Z L F G W E A Q X C T S O

N. V I B L I Y Y X X X

VIII.

O. S E P B O Z R N V D Y E H H B C R R N K A C Y F W

P. P R K C I I R K E T T Y I X X

IX.

Q. E I H T X G L R Q Z S S A C B X T T L C R F U V X

R. G L Z L R K M W P X T Z J F X M Q S F U A P E I E

S. E H N G T E E D Z J U S D D K W P V O M M J J X X

Military Cryptanalysis, Part III, 5-p.4, 1938.

Weight:

X.

A. L I I W T Q I E A P Q Q E A O L L L I Y U U H X X

B. A O Z T U N N S D Q X E G H J P O R V Z T O Y H Q

C. J A Q J X R G H A B E E X X X

XI.

D. U B H Z L Y K V N O K X C A T O Y K S B X D R N G

E. Y H H P P G G L Y Q J X Y M J T X R G H A B E E A

F. Q L F F V V W P U Z K K X X Y

10 4. The following message was intercepted on the same day as that on which those in Problem 3 were intercepted. This message uses an introductory key of unknown length (but is of several letters). Solve the cryptogram.

N U U B K O C R V S Q I F X Y M P A I Q G B M R T

S P Y C J V E S F O

REF ID:A60198

ARMY EXTENSION COURSES

LESSON ASSIGNMENT SHEET

SUBCOURSE - Military Cryptanalysis, Part III

LESSON - 6

Weight:

10 1. Solve the following message:

K X I V N L Y B S L N K V V H B X E T I V Q Z F N X A M Z T

Z Q D Q L D B L E U D M L S M Z F J T Y V A P N Z

80 2. Solve the following message:

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

Weight:

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

10 3. The following message was the reply to that in Problem 2. Solve it.

V A L L B A V P J X A H E O D H O O F H G M I S E B H Q X D

H C V P V T H T P R Y J

REF ID:A60198

ARMY EXTENSION COURSES
LESSON ASSIGNMENT SHEET

SUBCOURSE - Military Cryptanalysis, Part III

LESSON - 7

Weight:

40 1a. The following represent the beginnings of 20 cryptograms enciphered by means of the obsolete U. S. Army disk with a running key. All the messages begin at the same point in the key. Solve the first two groups of each message.

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

Weight:

	1	2	3	4
18.	O B T W C	E L N K N	H B X M Z	T W J H K
19.	B K X Q C	P O Q Y C	S Q J W Z	L N B W K
20.	A K R A C	I B P S A	Q Q Q M B	P M A X R

b. What are the first 15 letters of the running-key text?

2. The following was enciphered by the same means as above, with a different running key. The running key is presumed to have been taken from an ordinary book in English. Circumstances surrounding the transmission of the message suggest the presence of one of the words BATTALION, BAGGAGE, and UNLOAD in the plain text. Solve the message and reconstruct the running key.

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

REF ID:A60198

ARMY EXTENSION COURSES
LESSON ASSIGNMENT SHEET

SUBCOURSE - Military Cryptanalysis, Part III

LESSON - 8

Weight:

100 1. Solve the following messages, all intercepted on the same date. Prisoners state that the enemy is using a cipher machine, but nothing is known about its operation.

MESSAGE NO. 1

R X O W Z U Z U L I K T O G D F C J T G F M K L R

R E A V H J V S M A Y T I Z G A A F W G E H N C C

A C Y A E E D G P A I J N Q F T G T X L K Y B E O

H J Q Q S D P P K G H U N R S U Q I R K M O U P J

M C T Y V W O T X D S C X C K X C P R A C X X X X

MESSAGE NO. 2

I W K W X Y O K C F S O N S F H S R F V O N Z K U

N D Y A Z M Z H N C C A C Y A

MESSAGE NO. 3

W L W T L O H C H N M Q R Y O N D X J Y J G U V G

Q C J S I O O Z D V V M B M Y D A S X H Y C Q O M

L O T W R C E U Z N V C N T P Y Q N J H T T Z K N

Q G M S W R V P W R F W G A N C R D C T C J T G F

P O N M Q D E M B V D Z K Y N N R X C C A H I H Y

Z P O N L O Y T D G W R G A G O I S G Q D O H S T

I J L I F N N R W S I F Q J I J J Z K U D T W E W

P X Z U A Q J A J S I O C R F K V M B M M I V K B

Weight:

MESSAGE NO. 3 (Continued)

A F X N M J N H I Z S Y O Z H N F G Z Z M Y A X T

Z Z X Y H K C F F T I Q D G D E G P G M T A O B Y

F S D P G L I E Q A T Z X O V D Z I P L K I C V P

N E I H K B P D K V A V M P S P F H Z R W K I S C

G R F F D F W B U A V M J R I L O P D P X O X F X

MESSAGE NO. 4

R U J J N G O T F E I I H Q J P C C G Q W Z S E D

H G W R Y T I C T V F X J T U M D A R H

MESSAGE NO. 5

B H A E X X H E L U O A R B Z Z R B P F W Z I A U

S G D X P O N B J L C S T J W G N D H G G S G L P

B Y U N V Z U T G R G C S J Y X M N F Z N P L I Z

A R U V J V C P O P N Q F X T R X S P X G S C X C

K X C L V

MESSAGE NO. 6

X Q V N M Q R Y D A B H K L Y M D G Q Y O H S Y Q

O Z S M X C L A I W X A V B S H A C M C S H K T C

W W O X K T K Z S Y I Y Q C D P X Q S V C A O R X

P M X E S S L K O D O B T Y F F N F G A A N A T N

MESSAGE NO. 7

P G S A W O G T I Q G B C U Y I L P H F H V I L G

E D X S W A G I K U D T W T I J J T P K C X N K T

V M V X Q U H K Z E R Q T E H T J B X K U F X X X

Military Cryptanalysis, Part III, 8-p.2, 1938.

Weight:

MESSAGE NO. 8

Z U N X W K Z T G C T W F D E K K I O L F T Z T S

O U X X X

REF ID:A60198

ARMY EXTENSION COURSES
LESSON ASSIGNMENT SHEET

SUBCOURSE - Military Cryptanalysis, Part III.

LESSON - 9

Weight:

85 1. The following three cryptograms have been enciphered by a cipher machine employing two primary components which are shifted according to a very long keying sequence. Each message starts at a different point in the keying sequence. For purposes of simplification, it will be stated that the starting points of Messages No. 2 and 3 are not more than 10 intervals forward or behind the starting point of Message No. 1. Find the proper points of superimposition of these cryptograms and show the actual and expected number of coincidences for the various superimpositions you try, using diagrams such as those given in the text and specifying in each test the messages and superimposition points involved.

No. 1

K D G I O J T P L O S K W A P H U C B C J Y M C S V L W A H

V Z C Q U H O D C C R P N T X N A D I H M J X K P P X C O T

X U M T L H G W A H N P W Q J P N T O M F Z T A I F B J D H

M B Z V V C A U S Y Q S I K Q O P M U X X X U N T F F K Y T

N N S C J Z N Z C G C K O R P Z U B S N T Y E Q L N Z E W D

Z P Q Q V X N R B X S J A G A A A U G A Y W B D G C Z F G M

U B H D A W W W K I K F I E B G N F F E O O O I L Q L X E D

D N H A T J G G X J V U W Z Z G A H K K U P J T U K X V F D

V T M J N G W H Z X G L O U O I U Y M J W V W E X P U G G C

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

D N G F C W J R W C Q C A P C S I E A S S X J L A L L B J J

N Z V Z P Z S J E V P Z W T L R K Q O U V W V P O O H I H E

O P N M M A Q I E D L W J H D X T J H J Z I O D V S T D E I

Military Cryptanalysis, Part III, 9-p.1, 1938.

Weight:

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

U K J F H V O Z L V G Y X N W I V R T F I U Q H V X X U C Z

F L X Q W G Q I V V M C U H P T B V L X C R V M O N X M W O

G K B V Y X A B F V R H Y F Z B U U R O

No. 2

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

K J A S R J P Z L X S N Z I B W N B H P P H Z X L K G S S T

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

K V L M W W R E I V D H . H O L B H U I E B D H K E C D Z P

C I H S Q L P Y F R P G T Z F F A O P F B H Q Y H T A M V C

D X N N X H F G W I Y K H I I W X G O B E C M X F K E K M N

V P W F A X V F T H X T P B V I I O R V F K Y M Y Q V T U W

J F V P S A E U O O A G R Q K M Q D D I U A T V C S M M G G

W T K W I N G G E K M E T J Z J O Z X I C T O G Z C X T G H

S Z E T J T Z H M A V B F F T W C E O I Y R T U O K Y Z G E

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

Y R S E E T B V O I L S H Z C P Z H S N R P Z L V K M K N S

Q Y U I D Z L G I W X N G X H Q N V Y O K T A X O T N J F G

N F F K Y H Z R S Q Q C Q C C P F K C Z B P R A X J A U M E

H V S V N D J U C T L P H W D X M O Q D T U Q M H D F M H W

M Z N S D Q M N T H P I Y D V S T F R Q J N D G R B T Y N V

D U K X P

Military Cryptanalysis, Part III, 9-p.2, 1938.

Weight:

No. 3

C H U V O X B D B O C Y M N L U Q F U V R Y Q U M H U U A Q

W R E L F A S R N V Z U G S Q V D X J K C X U F X I Z D B U

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

O X P G H J S Z V T H Z Z N O Y V I B Z L Z A P Z Z T W U Y

J E R O Q C Q L L F U W K A X Y W G D J L W N Z W Z G T W O

L W K M U C E L C O J S Q Y V B H P C P P G W U Q H N V N Q

C R V X Z O I L N P D D A N U D I I U Q L D Z D Y F X J W W

C T R U O B F Z Z E R B F I S Z X D B Y R W L N X L M W B T

B Z M H L D R K T X U M J E V X Y M M D D Z G U I A F A P F

T Y Q L G S J X W A K Z X H Z A E H V A W T K C L A A D X W

C Y Y C H O J V S E Y O R O O Z P V L B I S Z F L U O V M T

N Z A B F T T M R K Q P Q H B B N V Z G Y J A F D P H V Y F

A I B P T K C S X Y X N E X R P Y Y O U Z I I U U C S O E K

J J T P K T Q M O N N S E M N G H M M X L U Y W F Z J X Z S

B W W V P C L N A V B Z X N W U U X D G R E N Q I X J Y J J

I O E O Z U L K Y T B E G S F D Q A R R Q V R D E

15 2. The primary components involved in the three cryptograms of Problem 1 are reversed standard alphabets. Solve the first few groups in each message. The text is strictly military and may be expected to contain such words as ARTILLERY, BATTALION, BRIGADE, etc.

REF ID:A60198

ARMY EXTENSION COURSES
LESSON ASSIGNMENT SHEET

SUBCOURSE - Military Cryptanalysis, Part III.

LESSON - 10

Weight:

40 1a. Of the following 10 frequency distributions the majority are monoalphabetic. Find them and indicate your answer by placing a check mark in the appropriate place in the diagram below.

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

Weight:

Distribution	Ð	Monoalphabetic		Non Monoalphabetic		Decision
		Surely	Probably	Surely	Probably	Suspended
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

b. Using the X-test, answer the following questions, showing the results of your calculations and presenting a summary of the reasoning which lead to your conclusions:

5 (1) Which distributions are monoalphabetic and which are not?

5 (2) How many different cipher alphabets are there in the distributions classified as monoalphabetic?

50 (3) Allocate the distributions to their respective cipher alphabets.

ARMY EXTENSION COURSES
LESSON ASSIGNMENT SHEET

SUBCOURSE - Military Cryptanalysis, Part III.

LESSON - 11

Weight:

85 1. The enemy is using a cipher disk similar to the obsolete U. S. Army cipher disk but with two differently-mixed primary components which are changed every day. The method of using the device is to set the two sequences according to a prearranged initial position and step the revolvable disk one letter forward in a clockwise direction after the encipherment of every letter. The following message was intercepted at 8:00 P.M. and was the first message of a new day's traffic. Solve the message showing the solution of the first 25 letters of the message only. Reconstruct the primary components, determine the keywords upon which they are based and their initial juxtaposition.

NOTE: When you have decided how to go about solving this problem, open the accompanying envelope.

O B D Z R D R U A J P O D B J R Y Y D R A O X Y X W B M A J

O Q N E Y F J V R M K H R L Q P C Q U O S L R X N E W W T E

O U V Z H N K A O A Q F N Q O U S J I F I D E G M B Y M L U

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

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

M E W A S Q B L J U M S V T S H M L K H Q M S A L V B Z Q L

O M M L H I S W H P N K L K G Q E U C K J K H O G T H P M S

P Z V D H U D N L W H D H V I C I T U X J Z B K R O I S E S

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

L U K G L I Z L K V X D Z Z X J Q B O O U O M U X C S E N N

B F Z B Z S P M U D S O R D J C E W T L E D Z Y O E G U U E

X W M F X V Q J Y A N Z T K Q A K A X X J C X V U M V T D B

Weight:

X R I Q E F X I C A U Q E Z R Y K T Z K V Z D V D Q X Y F P

M M A O T I I M A W U Z Q N T X T H A V B I N R I P W T B P

L Q P T K U A Q Q U Z X N Y Y W Y I N V K P V E J S E S Z G

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

P D H X F C K P D I D R L Q U S I V E Q S J T Q P Z G T P X

L R Q R M L I C W I W G V P L Q V E A A I K G C F A O A Q O

H J U Y B U T F N S E S Z Z K E U Q F P A V R P E V B K T R

G D W S J D B H P C T Q U T A C A N S L D T D B V Y C J Y Y

H T S R P A E R N U K P A Y R D Q P A K U O C I T H G U Y F

R O O H L H F G Z F I B F W G B W T B P O B D Z R D R U E V

P L R H T K B K L U R M J C K L E L H V Y

10 2. The foregoing message was one of many transmitted by enemy stations from 7:00 P.M. until 11:30 P.M., 10 June. Then at 11:45 P.M., 10 June, the message labeled No. 1 below was intercepted, after which all enemy stations were silent until 4:00 A.M., 11 June, when the single short message labeled No. 2 below was intercepted. Solve these two messages:

No. 1

11:45 P.M., 10 June.

(5) A G S U H H P R C S A R A A K O I Y E B L T Y H D R S A R K

S I T L O X W Q H M A D H D W E L U S X U U X Z Z M G G V K

N E A G I S F U H G O D H N L D L E O O Q U C R X X Y L F Y

M J W P J O D F

No. 2

4:00 A.M., 11 June.

(5) B B I X J N Y L V G C Q V V O U P K C A

5 3. What important principle of cryptographic security does Problem 2 teach?

Military Cryptanalysis, Part III, 11-p.2, 1938.

DO NOT OPEN
SEE NOTE
ON PROBLEM

REF ID:A60198

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

O B D Z R D R U A J P O D B J R Y Y D R A O X Y X W

B M A Z O Q N E Y F J V R M K H R L Q P C Q U O S L

R X N E W W T E O U V Z H N K A O A Q F N Q O U S J.

I F I D E G M B Y M L U K G Z F Q Z Z W C B O Z C Q

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

D T N X H H P A O N S Q A K J O I Z P R M E W A S Q

B L J U M S V T S H M L K H Q M S A L V B Z Q L O M

M L H I S W H P N K L K G Q E U C K J K H O G T H P

M S P Z V D H U D N L W H D H V I C I T U X J Z B K

R O I S E S Z Q O R L H H D H V D S K I M B N R B U

T F N D E G M B Y M L U K G L I Z L K V X D Z Z X J

Q B O O U O M U X C S E N N B F Z B Z S P M U D S O

R D J C E W T L E D Z Y O E G U U E X W M F X V Q J

Y A N Z T K Q A K A X X J C X V U M V T D B X R I Q

E F X I C A U Q E Z R Y K T Z K V Z D V D Q X Y F P

M M A O T I I M A W U Z Q N T X T H A V B I N R I P

W T B P L Q P T K U A Q Q U Z X N Y Y W Y I N V K P

V E J S E S Z G T G U B C B L N F Z Y N M P Z D K L

E X H Z Y A D X R J P O P D H X F C K P D I D R L Q

U S I V E Q S J T Q P Z G T P X L R Q R M L I C W I

W G V P L Q V E A A I K G C F A O A Q O H J U Y B U

T F N S E S Z Z K E U Q F P A V R P E V B K T R G D

W S J D B H P C T Q U T A C A N S L D T D B V Y C J

Y Y H T S R P A E R N U K P A Y R D Q P A K U O C I

T H G U Y F R O O H L H F G Z F I B F W G B W T B P

O B D Z R D R U E V P L R H T K B K L U R M J C K L

E L H V Y

Military Cryptanalysis, Part III, 11-p.la 1938.

REF ID:A60198

PROBLEM 11 - CRYPTANALYSIS III
FREQUENCY DISTRIBUTION TABLE

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
A	0	1	2	0	0	2	0	3	4	2	1	0	2	0	3	2	0	3	1	0	2	0	0	1	0	0	29
B	2	3	1	0	1	0	0	2	0	0	0	1	0	2	1	0	1	2	0	0	3	5	0	1	4	0	29
C	0	0	0	1	1	0	0	1	0	1	0	0	1	3	0	0	2	2	0	0	2	0	0	2	3	0	19
D	1	1	2	3	0	4	1	0	1	1	0	0	2	3	0	0	1	1	3	0	4	1	1	2	0	2	34
E	4	1	0	1	7	0	0	3	4	1	0	1	0	1	1	0	0	1	1	0	0	1	0	0	0	0	27
F	0	4	0	0	0	1	0	0	0	1	0	0	2	0	1	3	2	0	1	1	0	1	0	0	1	0	18
G	0	1	1	0	0	2	0	1	0	1	0	0	3	3	1	0	0	0	0	0	2	0	1	0	1	0	17
H	0	1	4	0	1	2	2	0	0	2	0	2	3	2	3	1	0	1	0	0	2	0	0	0	1	0	27
I	1	0	3	2	0	1	1	0	0	0	1	0	0	0	0	1	3	0	1	1	0	4	1	0	2	2	24
J	0	0	4	0	0	0	0	1	1	2	1	0	1	0	2	0	0	0	1	0	0	1	2	0	0	4	20
K	0	0	0	0	0	1	0	0	3	1	0	2	5	1	2	2	0	2	3	1	0	2	0	0	3	1	29
L	0	3	0	0	2	0	0	1	0	0	6	2	0	0	2	0	1	3	3	0	0	1	0	1	1	3	29
M	3	2	0	0	1	0	3	1	0	2	1	0	0	1	0	1	0	2	0	0	5	2	0	0	0	1	25
N	0	0	6	0	0	0	1	0	1	3	1	0	1	3	0	2	1	0	0	1	1	0	3	0	0	0	24
O	2	1	1	2	1	1	0	1	4	0	0	2	1	0	0	1	2	0	0	1	0	2	2	2	1	1	28
P	0	0	1	2	0	0	4	1	0	0	4	0	1	2	2	0	0	1	1	3	1	1	0	0	0	5	29
Q	1	0	0	0	0	4	1	2	0	2	0	3	2	1	1	0	1	0	5	0	0	3	1	0	1	4	32
R	3	1	0	0	2	1	3	1	1	2	1	0	2	0	0	1	3	1	0	3	1	0	0	5	0	0	31
S	0	3	0	3	2	4	1	0	1	0	2	0	0	0	0	0	2	1	0	1	0	0	0	0	5	0	25
T	3	2	0	1	2	0	3	2	2	0	1	1	0	2	2	0	1	0	0	3	0	0	1	2	0	0	28
U	1	0	0	3	1	0	1	4	0	2	4	3	0	1	0	2	2	0	0	1	1	0	4	1	0	2	33
V	1	0	1	2	1	0	2	0	0	1	1	1	0	1	0	4	1	0	1	5	0	0	2	2	0	0	26
W	3	0	0	0	1	3	0	0	0	1	0	1	0	0	0	1	0	0	0	4	0	0	2	0	1	1	18
X	0	2	1	1	1	0	0	1	1	0	1	1	0	0	1	4	0	0	1	0	1	2	4	0	2	0	24
Y	2	1	0	0	3	0	0	0	3	0	0	3	0	0	0	1	1	2	2	1	1	0	0	4	0	0	24
Z	0	0	0	6	0	0	3	1	0	1	1	3	0	0	4	0	2	4	2	0	0	0	2	3	0	0	32

681

Letters Arranged
According to Frequency

34	D	28	O T	22	
33	U	27	E H	21	
32	Q Z	26	V	20	J
31	R	25	M S	19	C
30		24	I N X Y	18	F W
29	A B K L P	23		17	G

Military Cryptanalysis, Part III, 11-p.2a, 1938.

REF ID:A60198

ARMY EXTENSION COURSES
LESSON ASSIGNMENT SHEET

SUBCOURSE - Military Cryptanalysis, Part III.

LESSON - 12

DETAILS OF SYSTEM

The enemy is using a cipher system (possibly a machine) concerning which the following information has been deduced from cryptanalytic work:

a. In general the system is like an ordinary repeating-key cipher. It uses two differently-mixed primary components which slide against each other to produce a set of 26 secondary cipher alphabets. (The primary components are derived from key-words, by key-number transposition, and the keywords change monthly.)

b. Each radio net is daily assigned a different message-keyword for enciphering messages within the net. These key-words vary from 5 to 20 letters in length; their composition determines the specific secondary alphabets to be used in enciphering messages.

c. The encipherment of a message can start with any one of the letters of the message-keyword, there being an indicator in each message which tells the recipient with which letter of the key the message begins. The indicator is usually the 1st group in the text and the meaning of every indicator is known. The indicator AMASS, for example, means that the 1st letter of the message is enciphered by the 1st letter of the keyword. The complete list of indicators and their values, is as follows:

Indicator	Letter of keyword with which encipherment of message commences
A M A S S	1st
A M I T Y	2nd
A R R O W	3rd
A S S A Y	4th
A U R A L	5th
A V A S T	6th
A X I O M	7th
A Z T E C	8th
B R I C K	9th
B R O I L	10th
B R O O D	11th

Indicator	Letter of keyword with which encipherment of message commences
B R U T E	12th
B U G G Y	13th
B U G L E	14th
B U M P S	15th
B U R L Y	16th
B U S H Y	17th
B U X O M	18th
C A B I N	19th
C A L Y X	20th

d. After this initial appearance of the keyword (either in whole or in part), each subsequent cycle of this key uses the same set of cipher alphabets but in a different order. That is, the order varies from cycle to cycle and does not repeat for a long time. For example, suppose that on a certain day the keyword for messages originating at Station A is HARVEST, a 7-letter word. A certain message begins with an indicator that shows that the initial key-letter employed is the R. The sequence of alphabets for the initial cycle is therefore R-V-E-S-T. For the second cycle the order of use of the 7 alphabets might be T-A-V-H-R-S-E; for the third cycle it might be V-H-S-A-R-E-T, and so on. In this case there are 8! (8x7x6x5x4x3x2x1 = 40,320) different arrangements or orders possible. Just what determines which arrangement will be used, that is, the sequence of orders is unknown. It seems to be governed by a long and complex key.

* *

Weight:

90 1. On a certain day 25 messages were exchanged by the radio stations within one of the radio nets of a certain division. The beginnings of these messages follow. Solve the first three groups of each message and reconstruct the primary components.

1) A V A S T J E X T W Y C K G E E X W X V I C N R J G U M S F

2) A X I O M X Z J O R D V N H N E Q P E M I H Y I Q E G K V I

3) A U R A L S J E C Q M Y K C A S E E C A N S F S Y I X O K J

4) A S S A Y N G L W R S W B Y A J Q O E K F I M R Z F X U E U

5) A Z T E C W J O K K R R E Z D W I C H Y D R R V E J L B M Z

6) A X I O M E B D K K K P O E H U M I V H N R N J E E Y J H E

7) A S S A Y Q F N E H G W F R H Z J A G G H N C R S X C S S A

Military Cryptanalysis, Part III, 12-p.2, 1938.

Weight:

8) A U R A L G Q E B H T B W C C I S X A L M O W N K O K H U E

9) A M A S S Y H X D K A E Y P U Y G M J D S J J N X D J E G R

10) A M I T Y U H N W P Y D L I P K U V L E D C J I A K U N J D

11) A M A S S Y T X Q I V B W J T F U H A R D E O D X T N G C C

12) A X I O M E B D K K M B W M U Y C J Q D K H R E S S A J C J

13) A V A S T J E X T O C A B I C T W D D X S J N D Q E S J L B

14) A Z T E C V W E R U Z I Q Z X K T K F Q D G N J W E D B E R

15) A R R O W F T V X L B A W B B C S G X C C J I H S Z N Z J O

16) A S S A Y H I C Y K N I F A C H J J Q I P I M V S C O Z I C

17) A V A S T J E H D C R R F I W L O V X P O R D R P S O A D N

18) A V A S T G E B A M Z U N I W S O A L P C K E F I P C C C K

19) A S S A Y H K F Y R P K S V X K X X J R W H S Z L B I S D C

20) A M A S S Y T Z Z Z J T L P M Y K L F L D Q C P I B I G V [illegible]

21) A U R A L A J E L P C R A C J D V L R H N T Z T B X U M R D

22) A S S A Y H I E M S D I G M L R E D E U K N P K E R F Z S E

23) A U R A L G Q E B P K R U V B L E X U L C F O C W P S Q C P

24) A V A S T J E H D C Y G X X X T B M J H N R Z L F T O C L E

25) A U R A L G Q E Y D T Y C I I C T O H P X S W C D R G V M I

5 2. What is the message keyword for this unit?

5 3. What are the keywords from which the primary components are derived?

REF ID:A60198

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE - Military Cryptanalysis, Part III

LESSON 1 - Aperiodic keying by word lengths.

Weight:

15 1a. Solution is obtainable by finding the plain-component equivalents (reversed standard sequence set against the normal sequence) and then completing the plain-component sequences. Each plain-text word comes out on a single generatrix but the successive words reappear on different generatrices. The letter-for-letter decipherment:

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

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

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

5 b. Keyword: T U E S D A Y

30 2. Since the cipher text is grouped according to the original word lengths, idiomorphic words such as ATTACK, FIFTEEN, etc., can readily be spotted. Assuming a mixed cipher component sliding against the normal plain component, and applying the principles of direct symmetry of position in the reconstruction of the former component solution is obtained as follows:

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

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

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

Solutions
Military Cryptanalysis-Part III, 1-p.1, 1938.

Weight:

2. Continued:

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

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

The primary components are as follows:

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

The mixed component is derived by transcribing the columns (from left to right) of a simple transposition rectangle based upon the keyword XYLOPHONE. Thus:

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

Sequence: X A K W Y B M Z L C Q etc.

40 3a. In Message No. 1 the sequence LBZRSSIBG is repeated in Message No. 2. This idiomorph suggests the word ARTILLERY. Immediately preceding this sequence in No. 2 is the sequence WGWHP, which is isomorphic with the sequence PMPBN which precedes the LBZRSSIBG sequence in No. 1. The word ENEMY suggests itself. With these words and sequences as a start, the reconstruction of the primary mixed cipher component is not difficult. The letter-for-letter decipherments are as follows:

No. 1

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

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

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

Solutions
Military Cryptanalysis-Part III, 1-p.2,1938.

REF ID:A60198

Weight:

3a. Continued:

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

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

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

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

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

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

No. 2

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

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

   I     D     E     L
T A K E N B Y H I S T A N K S
H I K R B R U C Q X C R J M L X X
```

The keyword for the message is SLIDERULE and the primary components are as follows:

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

Solutions
Military Cryptanalysis-Part III, 1-p.3,1938.

REF ID:A60198

Weight:

5 3b. Noting that the cipher component shows sections identical with sections in the cipher component of Problem 2, it is possible to block off the identical sections. Thus:

For No. 1:

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

For No. 2:

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

It soon becomes obvious that the cipher component for No. 2 is based upon the same keyword and rectangle as the cipher component for No. 1, but the columns in the transposition rectangle have been transcribed in key number order. Thus:

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

Sequence: E J V H G T L C Q etc.

5 c. Having reconstructed the mixed cipher component, the solution of a subsequent message enciphered by the same components but in a different key is a simple matter. Converting the first few cipher letters into their plain-component equivalents and then completing the plain-component sequences, the solution is as follows:

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

T		
O N L	N I N E	
A X N	D Q D G	X X X

Solutions
Military Cryptanalysis-Part III, 1-p.4,1938.

REF ID:A60198

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE - Military Cryptanalysis, Part III

LESSON 2 - Aperiodic keying by word lengths, continued.

Weight; -

30 1. This problem is no different in principle from that in Problem 3a of Lesson 1, but was introduced in order to give the student an opportunity to take what appears to be a complex scheme of enciphorment and remove the extraneous "trimmings" which cryptographic inventors usually employ with the idea that these additional elements impart cryptographic security to their scheme. The solution of the "challenge" message is as follows:

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

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

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

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

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

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

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

The primary cipher component is based upon the phrase A FROWZY PHLLGM and the components are as follows:

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

30 2a. The mean length of words in English telegraphic text is 5.2 letters. When separators are used the mean length becomes 6.2. Since a keyword is used in this case, then if we should find a repetition of significant length the interval between its 1st and 2nd appearances should give a fair indication of the length of the key.

Weight:

key. For example, note the sequence PBUVGI repeated at an interval of 44 letters. If the mean word length is 6 it follows that the keyword in this case should be 7 or 8 letters in length. Now, since the repeated sequence PBUVGI seems about in the middle of the message, if the text is written out in lines of about 45 to 50 letters before and after the repetition, then each such line will contain about 7 or 8 words each monoalphabetically enciphered by this keyword, and perhaps by careful scrutiny one can pick out the successive word separators. Note in the following transcription how the repeated sequence PBUVGI has been used as a sort of base for writing out the text in superimposed lines; how the word separators P and I appear in the lines above and below the lines with this repetition; how certain letters (E, Q, P, I, Z, M, D, L) appear to be distributed on each line more or less in accordance with the intervals to be expected of word lengths.

ANCKGEHWYJEFVWJQOVDWPBNFNLUZIURWRPOIZQVNYVBLIMKQHYWRKQBDJDBL

YJJNIATEJDZDVQZLXZPUMNAPIMRYJARPOZYBBIKUOTMGQDKBUIL

YJEJYQDVVFDGQ3GKGIGDCPBUVGIHJMUOZCJSOKBQEOMZOVDVWKKL

JNZAEDPEQOGKUPBUVGIOIRJMZVOMBMGFNMHLKXMDVWNVL

CTYXSMEVZJDQDOPQSPBMIFMRRNZZBCWMIKAVLDJQXBSIWTBL

YJEEDGVWQZLVUUPPNXAQNLUBIPLMOIZYVTMVGWLJDCWYNBL

GKTYXCKEWEKFUQZDFI

b. Once the sequence of cipher equivalents for the word separators has been ascertained, this enables one to block out words and these having been enciphered monoalphabetically, solution comes rather easily. For example, immediately preceding the 1st appearance of the sequence PBUVGI is the sequence QSGKGIGDC. The Q is, of course, the separator terminating the word in front of SGKGIGDC; the latter suggests DIVISION.

c. The primary components are based upon the keyword DERMATOLOGY and are as follows:

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

d. The keyword for the message is MUSKETRY.

Solutions
Military Cryptanalysis-Part III, 2-p.2, 1938.

Weight:

e. The complete text is as follows:

```
 M      U       S      K       E       T       R       Y
ANCKGEHWYJEFVWJQOVDWPBNFNLUZIURWRPCIZQVNYVBLIMKQHYWRKQBDJDBL
EIGHT PRISONERS FROM SEVENTY SEVENTH DIVISION INCLUDING ONE

   M      U      S      K      E       T      R      Y
YJJNIATEJDZDVQZLXZPUMNAPIMRYJARPOZYPBYKUOTMGQDKBUIL
OFFICER STATE THAT THEIR REGIMENT ATTACHED ON LEFT

M      U       S       K     E       T       R     Y
YJEJYQDVVFDGQSGKGIGDCPBUVGIIIJMUOZCJSOKBQEOMZOVDVWKKL
OF SIXTEENTH DIVISION STOP FIRST OBJECTIVE WAS HILL

   M   U   S     K     E   I       R       Y
JNZAEDPEQOGKUPBUVGIOIRJMZVOMBMGFNMHLKXMDVWNVL
FIVE TWO FIVE STOP THEIR NEXT OBJECTIVE HIGH

   M    U    S    K     E     T    R       Y
CTYXSMEVZJDQDOPQSPBMIFMRRNZZECWMIKAVLDJQXBSIWTBL
GROUND EAST OF MARSH CREEK STOP FIRST OBJECTIVE

 M   U      S       K       E    T    R     Y
YJEEDGVWQZLVUUPPNXAQNLUBIPLMOIZYVTMVGWLJDCWYNBL
OF OTHER THREE REGIMENTS NORTH AND SOUTH RIDGE

  M      U     S
GKTYXCKEWEKFUQZDFI
THROUGH ROUND TOPS
```

40 3. Examination of the text discloses four isomorphic sequences. They are superimposed for study.

		1	2	3	4	5	6	7	8	9	10	11
Isomorphs	A –	U	O	N	N	Y	S	F	M	L	U	T
	B –	K	V	D	D	G	Z	Q	U	S	K	A
	C –	M	D	W	W	R	L	G	C	B	M	V
	D –	D	Y	J	J	B	K	S	N	U	D	F

These sequences contain all the letters of the alphabet except these 5: E, H, I, P, and X; so that even if we can construct a chain of 26 places, we will have at least 5 blanks in it.

The application of the principles of indirect symmetry of position to the lines of the superimposition diagram yields the following data:

Isomorphs A&B	Isomorphs A&C	Isomorphs A&D
MUK	UMC	LUD
OV	OD	OYB
ND	NW	MNJ
YG	YR	TFSK
ISZ	SLB	
TA	FG	
	TV	

The data from isomorphs A and C may be immediately amalgamated with those from A and B. By careful study of the columns of the superimposition diagram we may add data as shown below:

Isomorphs A&B, A&C	Isomorphs A&D
CMUK	AQZ.VGLUDR.CW
WNDOVTA	TFSKOYBMNJ
JRYGFQ	
BLSZ	

As for the data under isomorphs A and D, it is obvious that we are here confronted with one of two conditions:

(1) Either the two sequences, by chance, are the nearly complete halves of a single sequence of 26 letters, in which case we should put the two sequences together according to one of the following 13 arrangements:

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

or else

(2) The two sequences (AQZ ... and TFS ...) represent two half-chains of 13 letters each, the letters of which must be properly dovetailed in order to produce a single sequence of 26 letters. The former hypothesis is not so likely as the latter. We could proceed to test out the former hypothesis, trying all 13 arrangements mentioned above and seeing if the interval relationships can be made consistent with those given by the actual data. This would be a lengthy and laborious procedure. On the other hand, we may assume the latter hypothesis to be true (that we have two half-chains) and try to dovetail them properly so as to produce a single chain of 26 places, which is not so difficult a process.

Solutions
Military Cryptanalysis-Part III, 2-p.4,1938.

Suppose we superimpose the AQZ ... half-chain over the TFS ... half-chain so as to give values that will correspond to any one of the values given in the partial chains CMUK, WNDOVTA, JRYGFQ, or BLSZ. Thus, selecting VT in the WDNOVTA chain:

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

It will be seen that this yields values consistent with those given by the partial chains under isomorphs A&B. Now since we are probably really dealing with half chains of 13 letters, we may repeat the AQZ ... half chain in its superimposition with the TFS ... half chain. Thus:

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

Since this gives the value AJ, we conclude that the WNDOVTA and JRYGFQ partial chains can be combined at once into one chain:

W N D O V T A J R Y G F Q

In the same way the other partial chains may be added to this sequence until a complete sequence (lacking only the 5 originally missing letters) has been completed, as follows:

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

The problem states that the letter Z is being used as the word separator, hence the letter immediately preceding each isomorph and the last letter of each isomorph should be the equivalent of Z_p, the separator. By studying the various cipher equivalents of this separator letter before and at the tail end of each isomorph the following pairs can be constructed, which give the sequent values of letter Z_p in sequent cipher alphabets, according to sequent key letters. Thus

N	U	O	N	N	Y	S	F	M	L	U	T	gives	NT	as	sequent	values	for	Z_p		
F	K	V	D	D	G	Z	Q	U	S	K	A	"	FA	"	"	"	"	"		
A	M	D	W	W	R	L	G	C	B	M	V	"	AV	"	"	"	"	"		
T	D	Y	J	J	B	K	S	N	U	D	F	"	TF	"	"	"	"	"		

Uniting the sequent values in a chain, one gets the sequence NT TF FA AV = NTFAV as the successive values of Z_p, corresponding to successive key letters. Whether this is the entire sequence of separator values, that is, whether the key is but

5 letters in length cannot yet be ascertained definitely. However, one might make a try at blocking out some or all of the words in the message by means of this sequence of 5 separator values. Simply go through the text and underline places where letters of the sequence NTFAV occur in proper order. Thus:

Y R M L T G C T J H H P F P F B B A O B J S D D A

? ?

V K V N U O N N Y S F M L U T I L T F K V D D G Z ...

Now let us work backward from a known point. It is obvious that immediately preceding the isomorph UONNYSFMLUT there is, in the plain text, a separator letter, Z_p. Hence Z_p must be Nc. Therefore, the V immediately preceding this N cannot be a separator. The V before the K must be Z_p, the separator. If this is correct, then the A immediately in front of that V cannot be a separator; the A in BBAOB must be the separator, Z_p. If this is correct, then the 1st of the two F's in HPFPF must be the separator and not the 2nd, since if the latter were the separator, one would have a 2-letter word with both letters identical (corresponding to BB_c), which is impossible in English. By proceeding along those lines, by careful observation and deduction, the entire text can be blocked off into word lengths. Thus:

Y R M L T G C T J H H P F P F B B A O B J S D D A V K V N

U O N N Y S F M L U T I L T F K V D D G Z Q U S K A O Y P D V

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

C A Q P N D P Z G H G N G O S T K J H G F I V C Z Y S A

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

The cipher text can now be converted into monoalphabetic terms and solved quite rapidly. One might, to satisfy curiosity, find the keyword to the message. It is DRONE. The solution is as follows:

D R O N E

Y O U R Z P L A T C O N Z W I L L P R O C E E D Z T O Z

Y R M L T G C T J H H P F P F B B A O B J S D D A V K V N

D R O N

G E T T Y S B U R G Z V I A Z G E T T Y S B U R G Z P I K E Z

U O N N Y S F M L U T I L T F K V D D G Z Q U S K A O Y P D V

Solutions
Military Cryptanalysis-Part III, 2-p.6, 1938.

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

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

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

The primary components are:

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

These two components were derived, by (key number) columnar transposition from the keywords WISHFUL and THINKING.

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

Solutions
Military Cryptanalysis-Part III, 2-p.7, 1938.

REF ID:A60198

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE - Military Cryptanalysis, Part III

LESSON 3 - Irregular-length plain-text groupings.

Weight:

8 1a. This problem is easily read by converting the cipher letters into normal alphabet equivalents (using a standard reversed sequence against a direct) and then completing the plain component sequences. The plain text reappears in irregular length sequences on different generatrices, the latter corresponding with the successive letters of the key FOGHORN. The solution is as follows:

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

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

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

     F         O
Q U E S T R  E P L Y
P L B N M O  K Z D Q
```

2 b. The successive letters of the keyword FOGHORN have the following numerical values (in the normal alphabet):

F O G H O R N
6 13 7 8 15 18 14

Each keyletter is then used for enciphering as many plain-text letters as its numerical value. Thus, the setting $A_p = F_c$ is used for the first 6 letters; $A_p = O_c$, for the next 15 letters, and so on.

8 2a. This problem is identical in principle with Problem 1, but the primary components shift much sooner than in Problem 1, making the solution more difficult. The primary components are

Weight:

both direct standard sequences. The keyword is FRIDAY and the solution is as follows:

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

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

  I     D  A
O S E H  I L  L
W A M P  L O  L
```

2 b. The letters of the keyword are given numerical values corresponding to their relative order in the normal sequence. Thus:

```
F R I D A Y
3 5 4 2 1 6
```

Each keyletter then enciphers as many letters as its numerical value, the F secondary alphabet being used for the first 3 letters, the R secondary alphabet for the next 5 letters, and so on. Ascertaining the method in which the keyword controls the shifting of the components in cases like this and the foregoing is a matter of observation and experience, with the application of simple reasoning. The student should always try to resolve a problem into its simplest terms, for in practical work it will often be found of great assistance in solving unknown systems.

30 3a. The idiomorphic repetition and its isomorph underscored in the cryptogram suggest the word COMMUNICATION. Immediately beyond the first two appearances of this word (1st and 3rd lines of text) are the sequences:

Line 1

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

Line 3

```
Z S I I F Q V Z O R V S Q S F C P C M C X H H C Z C D C R I Y I
C O M M U N I C A T I O N
```

Weight:

These two sequences certainly suggest that the same or nearly the same words follow COMMUNICATION both times, and that their different external appearances are occasioned by difference in the key. The word which commonly follows COMMUNICATION is WITH. The form of the sequences suggests:

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

Z S I I F Q V Z O R V S Q  S F C P C  M C X H H C Z C D C R I Y I
C O M M U N I C A T I O N  W I T H T  H I R D D I V I S I O N
```

When these hypothetical values are inserted within the cells of a sequence-reconstruction diagram, together with the values given by the isomorphic sequence pointed out above, one has the following:

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

From these values it is possible to reconstruct the primary cipher component based upon LAWN TENNIS:

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

From this point on solution can be promptly reached by decipherment. It is as follows:

```
          M(13)                          O(15)
C O M M U N I C A T I O N  W I T H S E C O N D D I V I S
Z S I I F Q V Z O R V S Q  Q X U T Y V L B R A A X H X Y

          N(14)                              U(21)
I O N W I L L B E D I S C O  N T I N U E D U N T I L J U N E T H R E
C R I E C N N F B H C D G R  Y Z A Y M L E M Y Z A U C M Y L Z B K L

          M(13)              E(5)              N(14)
C O M M U N I C A T I O N  W I T H T  H I R D D I V I S I O N U N
Z S I I F Q V Z O R V S Q  S F C P C  M C X H H C Z C D C R I Y I

                    T(20)                              M(13)
T I L F U R T H E R N O T I C E S T O P  B E G I N N I N G A T Z E
B D T K Z Y B C C Y S U B D H C F B U V  Y U W V Q Q V Q W O R K U
```

Solutions
Military Cryptanalysis--Part III, 3-p.3, 1938.

REF ID:A60198

Weight:

```
          O(15)                                   N(14)
R O Z E R O F I V E Z E R O S  T R I C T R A D I O S I L E
F B M V F B W X H V M V F B Y  S X C G S X T H C R D C N B

                    U(21)                                   M(13)
N C E W I L L B E O B S E R V E D U N T I  L C O N T A C T W I T H E
Y T L X A U U N L G N W L K O L E M Y Z A  M Z S Q R O Z R P V R N U

   E(5)              N(14)
N E M Y H  A S B E E N M A D E S T O P
B D U N P  T D F B B I Q T H B D S R U

                   T(20)                                    M(13)
W I R E C O M M U N I C A T I O N W I L  L B E R E S T R I C T E D
I D Y C H U R R Z S D H E B D U S I D T  M Y U D U X R D V Z R U L

          O(15)                                   N(14)
T O A B S O L U T E M I N I M  U M R E Q U I R E M E N T S
U B P Z Y B O G U V S X R X S  Y Q X B V Y C X B Q B I S D
```

10 b. Solution of this message is accomplished by employing the LAWNTEIS ... sequence and completing plain-component sequences. The text is as follows:

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

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

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

5 c. The keyword for Problem 3a is MONUMENT each letter of which not only determines the secondary alphabet to be employed, but also for how many plain-text letters, according to the key:

```
M  O  N  U  M  E  N  T
13 15 14 21 13 5  14 20
```

In Problem 3b the keyword is F A M E , used in exactly the same manner. 6 1 13 5

Solutions
Military Cryptanalysis-Part III, 3-p.4, 1938.

Weight:

30 4a. From the data given it is clear that -
Message 1 should start with NUMBERFIFTEENX,
Message 2 should start with NUMBERTWENTYTWOX,
Message 3 should start with NUMBERSIXTEENX.

Placing these plain-text beginnings under the proper messages, and applying principles of indirect symmetry of position, the primary component based upon PAN AMERICAN UNION is reconstructed. The solutions are as follows:

From B to A

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

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

From C to A

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

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

From A to C

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

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

5 b. The principal lesson which this problem holds for the cryptographer is the danger (to cryptographic security) of following a fixed procedure in enciphering and especially of enciphering reference numbers in so conspicuous a manner.

Solutions
Military Cryptanalysis-Part III, 3-p.5, 1938.

Weight:

The principal lesson the problem holds for the cryptanalyst is that he should be quick to note weaknesses such as the foregoing and take advantage of them so far as concerns enemy traffic. He should do all in his power to prevent procedures of this kind in our own traffic and to call attention to such weaknesses when he finds them in our own traffic.

Solutions
Military Cryptanalysis-Part III, 3-p.6, 1938.

REF ID:A60198

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE - Military Cryptanalysis, Part III.

LESSON 4 - Variable-length keying; interruptions in keying sequence.

Weight:

30 1a. Messages with their plain texts:

(1) R E P O R T T O C O R P S
z c t p z w z p e p z q x

(2) P R E P A R E T O M O V E
w t e q m x z s y s p r c

(3) N E X T T R A I N W I L L
t c r w c x t b h h

(4) C H I E F S I G N A L
e f k c s z r i h a

(5) T A K E S T E P S T O
y a n c i h z n u w

(6) O R D E R S W I L L
v z i e t i r r g x

(7) S E N D T H R E E M E N
h c q i c k g u o n

(8) R E F E R R I N G T O
z c f c l x r k q w

(9) S T P O N G R E S I S T
h w w p t e w c i m j s

(10) C O U N T E R A T T A C K
e p d o z c l i k s j

(11) P R O M P T O R D E R
w t s s q z p z i e t

Solutions
Military Cryptanalysis, Part III, 4-p.1, 1938.

Weight:

(12) R E G I M E N T W I L L
z c g g y f c s b g

(13) A T T A C K P O S T P O N E D
c w z a o o e m h w t p

(14) A D V I S E O U R Q U
c i y g i f b d t v x

(15) C A N Y O U M O V E Y O U R
e a q d r d n s r c a p d t

(16) T H R E E M O R E R E
y f w c q q b z c w c

(17) P R E V E N T E N E M Y
w t e z q s k u h c

(18) R E Q U E S T Y O U T A K E
z c v x q z k z y d w l k

(19) W H E N Y O U R B R I G A D E
a f e o j t d t i t

(20) G O O D P R O G R E S S
k p v f q w p k t e v

(21) R A D I O N U M B E R
z a b g r t x p u q x

(22) T W E N T Y F O U R
y h e o c u h m d t

(23) A C C O R D I N G T O
c l c p z i k o t h

(24) W H A T I S Y O U R
a f l w w z q m d t

(25) R E R A D I O M A R C H
z c w a p m b s a w l

(26) S H A L L W E P R O C E E D
h f l m h r z n a p e c e i

(27) A C T I V I T Y I N C R E A S I N G
c l z g e m k z t o

Solutions
Military Cryptanalysis, Part III, 4-p.2, 1938.

Weight:

(28) N O T H I N G S E E N
t p y f k o t i z u h

(29) R E C O M M E N D T H A T
z c c p s n e o p h d y l

(30) A D V I S E A T O N C E
c i y g i f t s y t l e

(31) T R O O P S W I L L R E M A I N
y t s v w v d g h p g u z

(32) I N C A S E O F F A I L U R E
n o c a i f b j b l g h y

(33) R U S H R E P L A C E M E N T S
x x x f l f e g j l

(34) R E P L A C E M E N T S
z c t m m b z j o o

(35) S E N D I N G T W O S E T S
h c q i w s y s b p h c z v

1 b. Key for messages: CALAMITY JANE

3 c. Primary components: Plain . . .ABCDEFGHIJKLM...Z
Cipher . . .HYDRAULICBCEF...Z

1 d. Interrupter: O_p.

35 2a. Same primary components as in Problem 1. Key MISSISSIPPI RIVER, applied to irregular lengths of text, starting at beginning of keyword after encipherment of each R_p. Solution most easily obtained by guessing the probable word RECIMENT, the indications of the probable presence of this word being the address and signature.

C. O. 95th Infantry

Plain:	Y	O	U	R	R	E	G	I	M	E	N	T	W	I	L	L	M	O	V
Key:	M	I	S	S	M	M	I	S	S	I	S	S	I	P	P	I	R	I	V
Cipher:	J	T	K	F	L	Q	J	D	L	F	I	J	R	H	R	P	M	T	O

Plain:	E	U	P	T	O	P	O	S	I	T	I	O	N	O	N	H	I	L	L
Key:	E	R	M	I	S	S	I	S	S	I	P	P	I	R	I	V	E	R	M
Cipher:	W	A	H	C	B	T	G	D	H	H	L	S	O	S	R	P	K	H	T

Plain:	O	N	E	A	N	E	N	I	N	E	O	N	E	A	N				
Key:	I	S	S	I	P	I	S	S	I	S	S	I	P	P	I				
Cipher:	X	S	D	I	F	L	U	F	R	S	T	I	X	S	D				

Solutions
Military Cryptanalysis, Part III, 4-p.3, 1938.

Weight:

```
Plain:   D P R E P  A R E T O  A T T A C  K H I L L  O N E N I
Key:     V E R M I  S S M I S  S I S S I  P P I R I  V E R M I
Cipher:  Z Z S Q V  S F Q H C  S H J S B  D Z M K P  E W I D M

Plain:   N E F O U  R
Key:     S S I S S  I
Cipher:  I X G C K  X
```

Smith, Brigadier General.

30 3. Same primary components as in Problems 1 and 2; each word begins with a new juxtaposition of the primary components, the keyword JAPAN being used for this purpose. The letter X is used as a word separator, and is treated as though it were an ordinary letter. Within each word the cipher component is shifted to the left after the encipherment of each letter, including the X separator. The latter then serves as a signal to shift the cipher component to the next keyletter before beginning to encipher the next word.

Solution is most readily obtained by converting the first ten cipher letters into their plain-component equivalents, completing the plain-component sequences initiated thereby, and noting plain-text on a diagonal line: FIVEXTRUCK.

Message

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

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

Plain:   X S O U T  H X O N X  N A N K I  N G X R O  A D X S T
Key:     D A U L I  C B N O P  J K M N O  P Q S A U  L I C P Q
Cipher:  Z V Q H H  M L A A M  H K D H Z  U Z O T Q  L E U E G

Plain:   O P X T H  E Y X S H  O U L D X  R E A C H  X S O U T
Key:     S T V A U  L I C N O  P Q S T V  J K M N O  P A U L I
Cipher:  C E Q W G  E U U C X  L J U X Q  A P M P X  M V Q H H

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

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

Solutions
Military Cryptanalysis, Part III, 4-p.4, 1938.

Weight:

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

Solutions
Military Cryptanalysis, Part III, 4-p.5, 1938.

REF ID:A60198

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE - Military Cryptanalysis, Part III.

LESSON 5 - Cipher-text auto-keying.

Weight:

10 1. The solution of this message requires only the use of two normal sequences, one direct, the other reversed. The usual simple steps having been tried, without success, cipher-text auto-keying is assumed. Since the initial keyletter is unknown, we may disregard the first plain-text letter of the message (which will be found easily enough later, from the context) and start with K as the keyletter. Then the 1st cipher group yields the following:

K G G L N
- E A V Y

Obviously the word is HEAVY.

30 2. A frequency distribution for each of the first 5 columns of letters is made. Each distribution shows monoalphabeticity, and shows crests and troughs in the same order but at different points along the normal sequence. These frequency distributions are solved by applying the principles of direct symmetry of position and the mixed primary component is reconstructed. The five secondary cipher alphabets are as follows:

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

The beginnings of some words (as in Nos. 7, 18, 42, etc.) indicate definitely what plain-text letters follow in columns succeeding column 5. From these values, the system is quickly determined to be cipher-text auto-key with 1st letter keying 6th, 2d keying the 7th, etc. Note the initial keyword for the messages (CHIEF) reappearing under A_p in the reconstruction skeleton.

The plain text of the first 20 messages follows:

Weight:

1.	TWO HUNDRED PRISO	11.	ATTACK PLANES HAV
2.	EASTERN SLOPES OF	12.	ANTI-TANK GUNS ON H
3.	THE ATTACK PLANNE	13.	NEARLY ALL OUR GAS
4.	OUR ATTACK JUMPED	14.	WHAT ARE YOUR DISP
5.	YOUR REQUEST FOR A	15.	REMAIN ON THE DEFE
6.	ENEMY TROOPS HAVE	16.	IN SPITE OF REPEAT
7.	REQUEST ADDITION	17.	OVERHEAD MACHINE
8.	SEVENTY FIVE AMMU	18.	MACHINE GUN FIRE I
9.	ARTILLERY FIRE IS	19.	INTERDICTING FIR
10.	THREE ENEMY AIRPL	20.	THE FIRST FIELD AR

This problem illustrates how easy it is to solve cases of this type when a sufficient number of messages is available to permit of this method of attack by superimposition. If this were not possible, solution would become much more difficult.

50 3. These messages being only 11 in number, the method of solution by superimposition is impracticable. Frequency distributions based upon the letters immediately following each different cipher letter must be prepared and these are solved by applying the principles of indirect symmetry of position. The mixed primary components are based upon the keyphrase ENGLISH-JAPANESE DICTIONARY. They are as follows:

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

The initial keyletters for the messages are as follows:

1)	N	4)	R	7)	F	10)	L
2)	U	5)	E	8)	E	11)	B
3)	N	6)	F	9)	E		

The texts of the messages are as follows:

Solutions
Military Cryptanalysis, Part III, 5-p.2, 1938.

REF ID:A60198

Weight:

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

Solutions
Military Cryptanalysis, Part III, 5-p.3, 1938.

REF ID:A60198

Weight:

IV.

A. C A L L M E U P A S S C O N A S Y O U C A N A N D
Z J D O H H N D K W G Y G L C B S K O X H J Y B E

B. G I V E M E A N E S T I M A T E O F T H E E N E M
G H G G U U L I I P U Z K E T T Z B G A A A P P G

C. Y S I T U A T I O N O N Y O U R F R O N T
F V E T J Y N S K M H J V P I K P W D C W X X X X

V.

D. T H E C G W A N T S A L I S T O F C A S U A L T I
T K K L S G D C W G D O F V A U T W S D S O B G H

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

VI.

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

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

H. H E N I N G
C C T B F M X X X X

VII.

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

K. P A T O N C E
V I B L I Y Y X X X

VIII.

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

M. T S I M M E D I A T E L Y
P R K C I I R K E T T Y I X X

Solutions
Military Cryptanalysis, Part III, 5-p.4, 1938.

Weight:

IX.

A. E I G H T I N C H S H E L L S A R E F A L L I N G
   E I H T X G L R Q Z S S A C B X T T L C R F U V X

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

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

X.

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

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

F. O N T O F B R I G A D E
   J A Q J X R G H A B E E X X X

XI.

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

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

J. T P R E S E N T T I M E
   Q L F F V V L P U Z K K X X X

10 4. Having reconstructed the primary components used in Problem 3, the solution of this message represents merely a special application of the method used in solving Problem 1, despite the fact that an introductory keyword of 7 letters is used. By trying introductory keys of 1, 2, 3, ... letters the solution is solution is reached when IZNFU is used for keying the 8th, 9th, 10th ... letters beyond.

```
.....  ..IZN  FUQGK  TIZRG  BSATB  KOXKT  IXSC
.....  ..OND  ITION  WIREL  INESI  NYOUR  AREA
IZNFU  QGKTI  ZRGBS  ATBKO  XKTIX  SCTTL  IYPCX
```

The text is seen to begin with

```
IZNFU  QGKTI  ZRGBS  etc.
.....  ..OND  ITION  etc.
```

Solutions
Military Cryptanalysis, Part III, 5-p.5, 1938.

Weight:

The 2d word of the message is obviously CONDITION. When $G_C = C_P$, the keyletter is E. The introductory keyword ends in E, then. By assuming various words, when REPORT is tried, the keyword OUTLINE is found. The beginning of the text:

OUTLINE IZN...
REPORTC OND...
IZNFUQG KTI...

Solutions
Military Cryptanalysis, Part III, 5-p.6, 1938.

REF ID:A60198

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE - Military Cryptanalysis, Part III

LESSON 6 - Plain-text auto-keying.

Weight:

10 1. This message represents a case of simple plain-text auto-key encipherment with two normal sequences, one direct, the other reversed. The usual simple steps having been tried, without success, plain-text auto-keying is assumed. Since the initial keyletter is unknown, we may assume the first cipher letter of the message to be A, B, C, ... and try to build up text. It happens that the first plain-text letter is A, and yields ADVAN for the cipher group K X I V N.

80 2. The following repetitions (and many others) are noted:

Group	No. of Occurrences
FC	9
KVHQRMH	2
KOA	4
DJZ	4
DJZMH	6
TJB	2
GCZ	3
GCZBFVBB	2
FCBFVBB	2

The large number of repetitions together with non-monoalphabeticity denoted by a frequency table of a few lines of cipher text, strongly indicates a plain-text auto-key system. In such a system, the plain-text repetitions are one letter longer than the cipher-text repetitions. Consider the third and fourth lines of cipher text. So many repetitions occur here that we can lay off the word lengths with a fair degree of assurance that they are correct. Beginning back in the third line, we have:

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

Colons indicate probable word separations.

Solutions
Military Cryptanalysis, Part III, 6-p.1, 1938.

Weight:

Now consider the 8 plain-text letters represented by JKVHQRMH. An excellent "probable word" to assume for this is DIVISION.

Suppose we assume:

D I V I S I O N to be enciphered by
J K V H Q R M H

Now if the plain component is standard and if we assume the base letter to be A_p, we would have from consideration of letters following I_p:

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

That M, Q, and V should fall in such order if something were not controlling their positions, would be quite a coincidence, particularly as there is just the right number of spaces between M and Q for N, O, and P to be inserted.

Let us tentatively insert N, O, and P in place, and then slide V_c under A_p, in which case $I_p = H_c$. We have:

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

This position of H is not inconsistent with its occurring in the keyword.

Now the digraph FC_c which precedes the cipher equivalents of DIVISION, occurs no less than 9 times. This might well then be the encipherment of the HE_p of THE. If it were, when H_c is under A_p, then C_c is under E_p. We would have:

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

This location of C near end of keyword is excellent. Our assumptions seem to work out too well to be incorrect.

Now since the cipher letter following the encipherment of DIVISION is N_c, the plain-text letter following DIVISION must be A_p.

We have nine letters, perhaps one word, perhaps several, beginning with A, following the word DIVISION. The word ARTILLERY immediately arises for consideration.

Solutions
Military Cryptanalysis, Part III, 6-p.2, 1938.

Weight:

Suppose the word ARTILLERY is enciphered by
NWUGJZPBB

Setting the I_c under A_p, we have $L_p = J_c$

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

which is excellent--too good to be wrong. We can also insert K_c and L_c, a very important addition as we can put L_c under A_p and use values of $Z_c = L_p$ and $P_c = E_p$. We have:

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

P_c checks and Z_c falls into place.

Now since H and I are in the keyword, G_c might well just precede J_c. If it did, then from encipherment of I_p in ARTILLERY to be G_c, we would have T_c falling in front of H_c, forming a very high frequency digraph.

Experimentation quickly shows the correct placement of the remaining letters and develops the cipher sequence:

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

The foregoing procedure represents only one of perhaps several different lines of attack. Other openings are possible, just as in chess or checkers.

The plain text is:

HEAVY ENEMY FORCES HAVE BEEN PRESSING OUR DIVISION VIGOROUSLY BUT HAVE BEEN STOPPED AT THE BLUE RIVER STOP THE DIVISION ARTILLERY WILL MOVE ALL UNITS UP AS CLOSE TO THE RIVER AS PRACTICABLE IN ORDER TO BE ABLE TO COVER AS MUCH TERRITORY ACROSS THE RIVER AS POSSIBLE DURING THE COUNTERATTACK WHICH WILL BE MADE WITHIN TWO DAYS STOP AMMUNITION DUMPS WILL BE MOVED FORWARD AND SUPPLIES OF GASOLINE STORED IN CLOSE PROXIMITY TO THE UNITS IN ORDER THAT NO TIME WILL BE LOST WHEN WE BEGIN OUR ADVANCE ACROSS THE RIVER STOP PONTOON BRIDGES ACROSS BLUE RIVER WILL BE BUILT AT COSTER AND BLUEFIELD BY THE TENTH ENGINEERS TONIGHT.

10 3. The solution of this message follows along the lines of that in Problem 1, since the primary components are now known. It is as follows:

Solutions
Military Cryptanalysis, Part III, 6-p.3, 1938.

Weight:

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

V I S E W H E N C O M P L E T E D
B H Q X D H C V P V T H T P R Y J

Solutions
Military Cryptanalysis, Part III, 6-p.4, 1938.

REF ID:A60198

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE - Military Cryptanalysis, Part III

LESSON 7 - Running key ciphers.

Weight:

40 1a. Superimposition of the 20 beginnings provides more than sufficient material for the solution of the first two or three columns. Since the cipher alphabets are known, frequency distributions of columns of the text can be solved quite readily, aided by a study of the repetitions of digraphs and trigraphs appearing within consecutive columns. The key text can be reconstructed simultaneously with the solution of the cryptographic text. Solution is as follows:

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

Solutions
Military Cryptanalysis, Part III, 7-p.l, 1938.

Weight:

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

10 b. The first 15 letters of the running-key text are as follows: S O M E T I M E S T H E B E S

50 2. By assuming the presence of the word THE in the key-text or the presence of the word BATTALION in the cipher text, a start is made in the solution. By working forward and backward from this initial entering wedge, solution can be completed in the manner stated in the text. The solution is as follows:

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

Solutions
Military Cryptanalysis, Part III, 7-p.2, 1938.

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

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

   G R A D E
E. E H A R H
   C K A M X
```

Solutions
Military Cryptanalysis, Part III, 7-p.3, 1938.

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE - Military Cryptanalysis, Part III

LESSON 8 - Progressive-alphabet systems.

Weight:

100 1. Other methods of attack ending in failure, all the messages are rewritten, one under the other.

By means of the repetition of N M Q R Y (messages 1 and 6), C J T G F (message 1 and line 4 of message 3), K U T D W (message 7 and line 6 of message 3), C X C K X C (ends of messages 1 and 5), and other repetitions, the messages are all lined up in proper columns.

From the repetition in message 3 of J S I O . . . . V M B M (lines 1 and 7) at interval of 156, and from other shorter repetitions, it is determined that 26 alphabets are used.

The messages are rewritten in lines of 26 letters long, using message 3 as a base, and starting the other messages at the proper places to bring the repetitions into alignment.

Frequency tables are made of the letters in each column of the superimposition diagram and the messages solved as a poly-alphabetic substitution cipher of 26 secondary alphabets, using indirect symmetry to assist in determining values and building up the primary components. A start is probably most easily made in message 3 where the repetitions indicate the lengths of three four-letter words in sequence. A guess that these words are numbers follows.

Noting that all the secondary alphabets are reciprocal, this fact is found to be of material assistance. All are derived from the sequence based on P U G N A C I T Y slid against itself. The initial setting of column 1 of message 3 is:

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

Each succeeding secondary alphabet is derived by moving the cipher component one place to the right.

The messages and plain text follow:

MESSAGE NO. 1

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

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

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

I T I O N  A L A R T  I L L E R  Y S U P P  O R T C O  M
Q Q S D P  P K G H U  N R S U Q  I R K M O  U P J M C  T

M A A D V  I S E G D  A S H T H  R E E
Y V W O T  X D S C X  C K X C P  R A C
```

MESSAGE NO. 2

```
                                  Y O U R R  E G I M E  N
                                  I W K W X  Y O K C F  S

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

R O W
C Y A
```

MESSAGE NO. 3

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

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

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

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

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

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

Solutions
Military Cryptanalysis, Part III, 8-p.2, 1938.

MESSAGE NO. 3 (Continued)

```
V I A T W  O F O U R  S E V E N  T O C R O  S S R O A  D
N R W S I  F Q J I J  J Z K U D  T W E W P  X Z U A Q  J

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

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

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

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

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

E I S F E  A S I B L  E X
J R I L O  P D P X O  X F
```

MESSAGE NO. 4

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

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

MESSAGE NO. 5

```
                                C G F I R  S T D I V  I
                                B H A E X  X H E L U  O

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

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

E O N E P  O I N T O  N E T O F  O U R F O  U R O N E  P
J Y X M N  F Z N P L  I Z A R U  V J V C P  O P N Q F  X

O I N T N  I N E G D  A S H T W  O
T R X S P  X G S C X  C K X C L  V
```

Solutions
Military Cryptanalysis, Part III, 8-p.3, 1938.

MESSAGE NO. 6

```
          T H E C  O M M A N  D I N G G  E N E R A  L
          X Q V N  M Q R Y D  A B H K L  Y M D G Q  Y

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

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

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

O W
T N
```

MESSAGE NO. 7

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

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

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

MESSAGE NO. 8

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

O U R T E  N
T Z T S O  U
```

Solutions
Military Cryptanalysis, Part III, 8-p.4, 1938.

ARMY EXTENSION COURSES
SOLUTIONS

SUBCOURSE - Military Cryptanalysis, Part III.

LESSON 9 - Theory of Coincidences; the Kappa-test; general solution for cryptograms with long keys.

Weight:

85 1. By applying the K-test, it is found that the three cryptograms should be superimposed thus:

(1) K D G I O J T P L O S K W A P . . .
(2) B P D I N I I J W L I . . .
(3) C H U V O X B D . . .

The data for all tests are shown below:

Relative Settings Message #1 (504)	Message #2 (485)	Coincidences	No. of Comparisons	Relative Settings Message #1	Message #2	Coincidences	No. of Comparisons
1	1	16	485	1	1	16	485
1	2	17	484	2	1	18	"
1	3	20	483	3	1	11	"
1	4	12	482	4	1	20	"
1	5	15	481	5	1	56	"
1	6	17	480	6	1	21	"
1	7	12	479	7	1	19	"
1	8	16	478	8	1	20	"
1	9	16	477	9	1	22	"
1	10	22	476	10	1	11	"
#1	#3			#1	#3		
1	1	25	475	1	1	25	475
1	2	15	474	2	1	18	"
1	3	13	473	3	1	16	"
1	4	14	472	4	1	17	"
1	5	10	471	5	1	19	"
1	6	15	470	6	1	19	"
1	7	13	469	7	1	27	"
1	8	25	468	8	1	42	"
1	9	14	467	9	1	14	"
1	10	18	466	10	1	17	"

Solutions
Military Cryptanalysis, Part III, 9-p.1, 1938.

REF ID:A6011963

Weight:

Relative Settings Message #2	Relative Settings Message #3	Coincidences	No. of Comparisons	Relative Settings Message #2	Relative Settings Message #3	Coincidences	No. of Comparisons
1	1	15	475	1	1	15	475
1	2	15	474	2	1	16	"
1	3	18	473	3	1	14	"
1	4	22	472	4	1	32	"
1	5	12	471	5	1	20	"
1	6	21	470	6	1	11	"
1	7	14	469	7	1	21	"
1	8	15	468	8	1	19	"
1	9	23	467	9	1	7	"
1	10	19	466	10	1	14	"

15 2. The solution of the first few groups in each message:

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

(2) B P D I N I I J W L I U O U V H M K H L E
E N E M Y O B S E R V A T I O N P O S T S

(3) C H U V O X B D B O C Y M N L U Q F
S E C O N D B A T T A L I O N F O R

Solutions
Military Cryptanalysis, Part III, 9-p.2, 1938.

REF ID:A60198

ARMY EXTENSION COURSES

SOLUTION

SUBCOURSE - Military Cryptanalysis, Part III.

LESSON 10 - The Φ and X tests; ascertaining by statistical methods whether a distribution is monoalphabetic or polyalphabetic.

Weight:

40 1a. All the distributions have 35 letters each. For plain text, the value of $E(\Phi_p)$ is .0667x35x34 = 79; for random text $E(\Phi_r)$ is .0385x35x34 = 46. The midway point between 79 and 46 is 62.5. Consequently we may begin by saying that any distribution which gives a value for Φ which is 63 or more will tentatively be classified as being monoalphabetic; any distribution which gives a value which is below 63 will tentatively be classified as being not monoalphabetic. Accordingly, the results of this first examination are as follows:

Distribution	Φ	Monoalphabetic		Non Monoalphabetic		Decision
		Surely	Probably	Surely	Probably	Suspended
1	106	✓				
2	54				✓	
3	64					✓
4	44			✓		
5	108	✓				
6	70		✓			
7	58					✓
8	104	✓				
9	48			✓		
10	68		✓			

60 b. To answer the questions asked we could begin by testing only the distributions which were classified under a above as being "surely monoalphabetic", and then add to the data thus obtained the results of testing the distributions whose classification

REF ID:A60198

is indicated as probably correct and then treating the distributions whose classification is in doubt. But we might as well systematize the work and make all the tests at once. Moreover, it is possible that the X-test may corroborate or substantiate the results obtained from the ⊕ test; the X-test may even cast some doubt upon the accuracy of the results obtained from the ⊕ test in certain cases. Hence, we draw up a diagram as follows:

RESULTS OF X-TEST

	1	2	3	4	5	6	7	8	9	10
1		52	64	29	46	56	85	119	74	50
2			38	52	32	47	44	44	38	43
3				40	76	81	64	65	55	78
4					57	48	38	46	36	49
5						82	66	45	34	88
6							51	50	45	81
7								87	66	65
8									77	53
9										48

Since all the distributions have 35 letters each, the values of X for plain text and for random text are:

$X_p = 35 \times 35 \times .0667 = 81.7075 = 82$

$X_r = 35 \times 35 \times .0385 = 47.1625 = 47$

The midway point between the two values is 64.5. Examining the values of X for the various comparisons shown in the diagram above we may set down the following reasoning:

Examining the first line in this diagram, we may say that distributions 1 and 8 are certainly similar and belong to the same monoalphabet (X = 119); distributions 1 and 7 (X = 85) most probably belong to the same monoalphabet, too, in which case 1, 7, and 8 are similar and belong together. If this is correct then 7 and 8 when tested against each other should give a high value for X. Reference to the table shows that X in this case equals 87, which corroborates the idea that 1, 7, and 8 belong together. Returning to line 1 of the diagram, the values of X for distributions 1-9 and 1-10 are 74 and 50, respectively.

Weight:

The first of these values is considerably above the midpoint value (64.5) and we may feel that there is good evidence for thinking that distribution 9 also belongs to the same monoalphabet with 1, 7, and 8. Furthermore, if 9 does belong with 1, 7, and 8, then the X values for 7-9, and 8-9 should be high. They are 66 and 77, respectively. The value 77 for the combination 8-9 is high enough to be considered as substantiating the idea that 9 belongs with 1, 7, and 8, but the value for the combination 7-9 is pretty low and casts some doubt upon the matter. However, let us assume tentatively that 1, 7, 8, and 9 belong together. As for distribution 10, it hardly looks as though it belongs with 1, 7, 8, and 9; moreover the X values for 7-10, 8-10, and 9-10 should be low. They are 65, 53, and 48. These certainly corroborate the idea that distribution 10 does not belong with 1, 7, 8, and 9.

Still referring to line 1 of the diagram, we may say that distributions 1 and 4, with X = 29, are certainly not alike. But we have already concluded in a above that distribution 4 is "surely not monoalphabetic." Obviously, if distribution 4 is non monoalphabetic it cannot be similar to distribution 1, which is monoalphabetic. Next we consider 1 and 5, with X = 46. Now in the Φ test distribution 5 gave a very high value (108) so that there can be no doubt about its being monoalphabetic. Hence, the low value of X, when 1 and 5 are compared, must be due to a dissimilarity in monoalphabeticity, and we conclude that distributions 1 and 5 belong to different monoalphabets.

Likewise, as regards distributions 1 and 6 (X = 56) we conclude that they belong to different monoalphabets. Thus we have reached the conclusion that 1 and 5 are different, and that 1 and 6 are different. Now look at the value of X for combination 5-6; it is 82, indicating that distributions 5 and 6 are similar.

We have now disposed of these distributions:

Nos. 1, 7, 8 and 9 belong together
Nos. 5, 6 " "
No. 4 is not monoalphabetic.

There remain distributions 2, 3, and 10 to be classified.

Now 1 and 2 do not go together, since X = 52. But from our work under a above, distribution 2 was classified as "probably not monoalphabetic." Hence, the X test corroborates that conclusion. This is further substantiated by the fact that distribution 2 when tested against all the other distributions (line 2 of the diagram) shows low X values throughout. So we have disposed of distribution 2: it is surely not monoalphabetic and does

Weight:

not belong with either the 1-7-8-9 group or the 5-6 group.

As for distribution 3, it gives a fairly high value for X when tested against distributions 5 and 6 (76 and 81, respectively). It also gives a fairly high value when tested against distribution 10 (X = 78). Do 3, 5, 6, and 10 go together? Note the values:

X for 3-5 = 76	X for 5-6 = 82
" 3-6 = 81	" 5-10= 88
" 3-10= 78	" 6-10= 81

The foregoing leaves no doubt that 3, 5, 6, and 10 are similar distributions.

All distributions have now been accounted for, with the following conclusions:

(1) Distributions 1, 3, 5, 7, 8, 9, and 10 are monoalphabetic; 2 and 4 are not.

(2) There are but 2 monoalphabets represented among the 8 distributions which are monoalphabetic.

(3) Distributions 1, 7, 8, and 9 belong to one of these monoalphabets; distributions 3, 5, 6, and 10 belong to the other.

REF ID:A60198

ARMY EXTENSION COURSES

SOLUTION

SUBCOURSE - Military Cryptanalysis, Part III.

LESSON 11 - Progressive-alphabet systems, continued.
Matching frequency distributions; the X-test.

Weight:

85 1. It is clear that the message involves 26 secondary cipher alphabets employed in progression. Transcribing the text in lines of 26 letters, a distribution is made of the cipher letters with reference to the columns in which they appear. This yields the distribution square which has already been furnished.

By using this distribution square it becomes possible to build up the primary cipher component by successively matching pairs of distributions, and applying the X-test. We begin with the D and and U distributions, since they have the most data. The expected value of X is: 34x33x.0667 = 74.8. None of the juxtapositions of the two distributions gives a cross-product sum that approximates 75; the juxtaposition giving the greatest value for X is as follows:

	1																								
D	1	1	2	3	0	4	1	0	1	1	0	0	2	3	0	0	1	1	3	0	4	1	1	2	0	2
U	0	0	1	1	0	4	1	0	2	1	0	0	3	1	0	1	4	0	2	4	3	0	1	0	2	2
Pro-ducts	0	0	2	3	0	16	1	0	2	1	0	0	6	3	0	0	4	0	6	0	12	0	1	0	0	4

Sum of cross-products (X) = 61

But there are several/other juxtapositions which give values close to this, so that it is inadvisable to assume without further corroboration that this juxtaposition is the correct one.

The next largest distribution is that for Q. This distribution is tested against the D and the U distributions separately and then against the two distributions combined at the various possible juxtapositions. By such procedure it becomes easy to pick out the correct juxtaposition from among several possibilities.

The final result is that the following sequence is constructed:

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

Solutions
Military Cryptanalysis, Part III, 11-p.1, 1938.

Weight:

The cipher text can now be converted into monoalphabetic terms and solved as a monoalphabetic substitution cipher, whereupon the plain component can be constructed. It is found to be as follows:

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

These two primary components were derived from the following transposition rectangles:

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

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

The solution is as follows:

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

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

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

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

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

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

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

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

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

Solutions
Military Cryptanalysis, Part III, 11-p.2, 1938.

REF ID:A60198

- Weight:

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

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

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

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

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

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

N F I F T Y T W O P O I N T F I V E P A R E N T H E
M M A O T I I M A W U Z Q N T X T H A V B I N R I P

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

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

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

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

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

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

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

H A T Y O U R D I V I S I O N M A K E N E C E S S A
Y Y H T S R P A E R N U K P A Y R D Q P A K U O C I

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

Solutions
Military Cryptanalysis, Part III, 11-p.3, 1938.

Weight:

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

E C T O R
E L H V Y

2. By "deciphering" the first few letters (that is, setting the reconstructed cipher component against the reconstructed plain component at any point and converting the cipher letters into their plain-component equivalents, sliding the cipher component one space to the left each time), and then completing the plain-component sequence, the first word of the message is found to be R A D I O. This gives the correct initial juxtaposition of the two components and the entire message can now be read without further delay. It is as follows:

(5) R A D I O S I L E N C E U N T I L F U R T H E R N O T I C E
A G S U H H P R C S A R A A K O I Y E B L T Y H D R S A R K

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

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

R E A C H Y O U
M J W P J O D F

The text of this message then shows what must be done in order to read No. 2. When the primary components are interchanged and the principle explained above is then applied, the message is found to read as follows:

(5) A T T A C K B E G I N S A T F I V E A M
B B I X J N Y L V G C Q V V O U P K C A

3. Problem 2 illustrates the grave danger of communicating, by radio or any other interceptible agency and especially by means of a current cipher system and cipher key, the key to a future message or set of messages. Current ciphers and keys should never be used for such a purpose; nor should such information be communicated by means susceptible of interception.

Solutions
Military Cryptanalysis, Part III, 11-p.4, 1938.

REF ID:A60198

ARMY EXTENSION COURSES
SOLUTION

SUBCOURSE - Military Cryptanalysis, Part III.

LESSON 12 - The X-test and its application in the solution of a practical example involving the matching of alphabets.

Weight:

90 1. The first step is, of course, to superimpose the messages properly. This can readily be done by means of the message indicators. Also, since the indicators give the various starting points, the number of different indicators should correspond with the length of the keyword employed by the stations within the net. Only 8 different indicators appear and hence it is safe to assume a key of 8 letters. The superimposition diagram is shown in Fig. 1. Since there are 32 columns we may mark off the varying keying "blocks" (i.e., permuted arrangements of the 8-letter cycles) as shown at the top of Fig. 1.

Frequency distributions are then made for the individual columns of the superimposition diagram, beginning with column 4 and ending with column 29. (Columns 1-3, 30-32 contain so few letters they may be neglected.) The distributions are shown in Fig. 2.

The next step is to apply the X-test to these distributions for the purpose of combining those which belong to the same cipher alphabets, in order to facilitate the analysis of the latter. The process is likely to be a laborious one and we prepare a table so as to systematize the work. In this table there are pairs of lines, the upper one of each pair giving the expected values of X, the lower one the actual values for each test. Whenever we find a case wherein the actual value is high, indicating a possible similarity in the two distributions being tested, we mark it by an asterisk or by underscoring it. The result is shown in Table 1, which forms the basis for the analysis of the data from the X-tests.

In order to eliminate possible aberrations in frequency occasioned by the presence of words repeatedly occurring at the beginning of messages, we may start our analysis with column 9, the first column in the second cycle of the key. Immediately we note the high value of X for the matching of columns 9 and 19 (X = 55, whereas the expected value is 42). Also, in this same pair of lines we note the value of X for

Weight:

combination 9-29 (X = 36, expected value 25). Let us, then, assume that 9, 19, and 29 belong to the same cipher alphabet. If 9, 19 and 29 are really similar, then the X-test for the combination 19-29 should yield a high value. It is 34, whereas the expected value is only 25. Thus we find excellent corroboration for assuming that columns 9, 19 and 29 belong to the same cipher alphabet. We may now look for that column among columns 1 to 8, inclusive, which belongs with 9, 19 and 29. Of course, it may be that column 1, or 2, or 3 belongs in that group but if it does we cannot test the idea because these columns contain so few letters. So we can only start with column 4. The matching of columns 4 and 9 gives a close approximation to the expected value (X = 15, expected value 17) but the values for 4-19 and 4-29 are so low as to make it certain that 4 does not belong with 9-19-29. Columns 5 and 9 certainly do not belong together. But columns 6 and 9 give a high value for X; moreover, the combinations 6-19 and 6-29 give excellent corroboration for the amalgamation of 6-9-19-29. If this is correct we have isolated from among all the 29 columns four which belong in the same cipher alphabet; moreover, we have one representative of this alphabet in each cycle of the key -- which is as it should be.

Now take column 10. There are several candidates for combination with it, so many, indeed, that we are going to have to be very careful. Columns 10-12 give a value of 40; 10-18, a value of 45; 10-22, a value of 36; columns 10-21, a value of 30. None seems to be really outstanding; if we take the combination 10-18 we cannot corroborate its correctness. Let us, therefore, suspend judgment on this column for a few minutes.

Take column 11; certainly it goes with column 24. Now see how good a value the combination 8-11 gives as against 4-11, 5-11, or 7-11 (column 6 can be passed over since it has already been classified with columns 9, 19, 29). Let us assume that 8, 11, and 24 belong together. Then 8-24 should give a high X-value; it is 38, not as high as we would like to have it, but not bad, since it is only 4 points below the expected value. However, notice how much lower the other values are in this same line of data for the combination of column 8 with most of the other columns. For these reasons we may regard it as fairly well established that columns 8, 11, and 24 belong together; moreover, that the alphabet to which they pertain is not represented in the section containing columns 25-29.

Next take column 12. Here is an excellent case presenting no difficulty. It obviously goes with columns 18 and 28. Corroboration is immediately seen in the high value for the matching of 18 and 28 (expected value 33, actual 46). Does column 4, or 5, or 7 belong in this group? Certainly neither 4 nor 7 does; but 5 may,

Weight:

for its value, 23, is quite close to the expected value, 25. However, 5 and 14 give a better match, so that we cannot assume 5 belongs with 12, 18, and 28. Let us be content at this point to group only 12, 18, and 28, leaving 5 for further consideration.

Thus far, we have definitely tied together the following columns:

Group 1: 6-9-19-29
" 2: 8-11-24
" 3: 5-12-18-28

Looking these over we note that we have allocated several columns which are adjacent. Perhaps we can dispense with further X-tests if we have enough data to solve these adjacent columns. Specifically we note that columns 5, 6, 8 and 9 fall within the three groups of columns definitely combined. Therefore, if we can find the group into which column 7 falls we will have 5 adjacent columns, with more than enough data in the respective alphabets to permit of solution of these alphabets. Consequently, let us study column 7 and see what we can do with it.

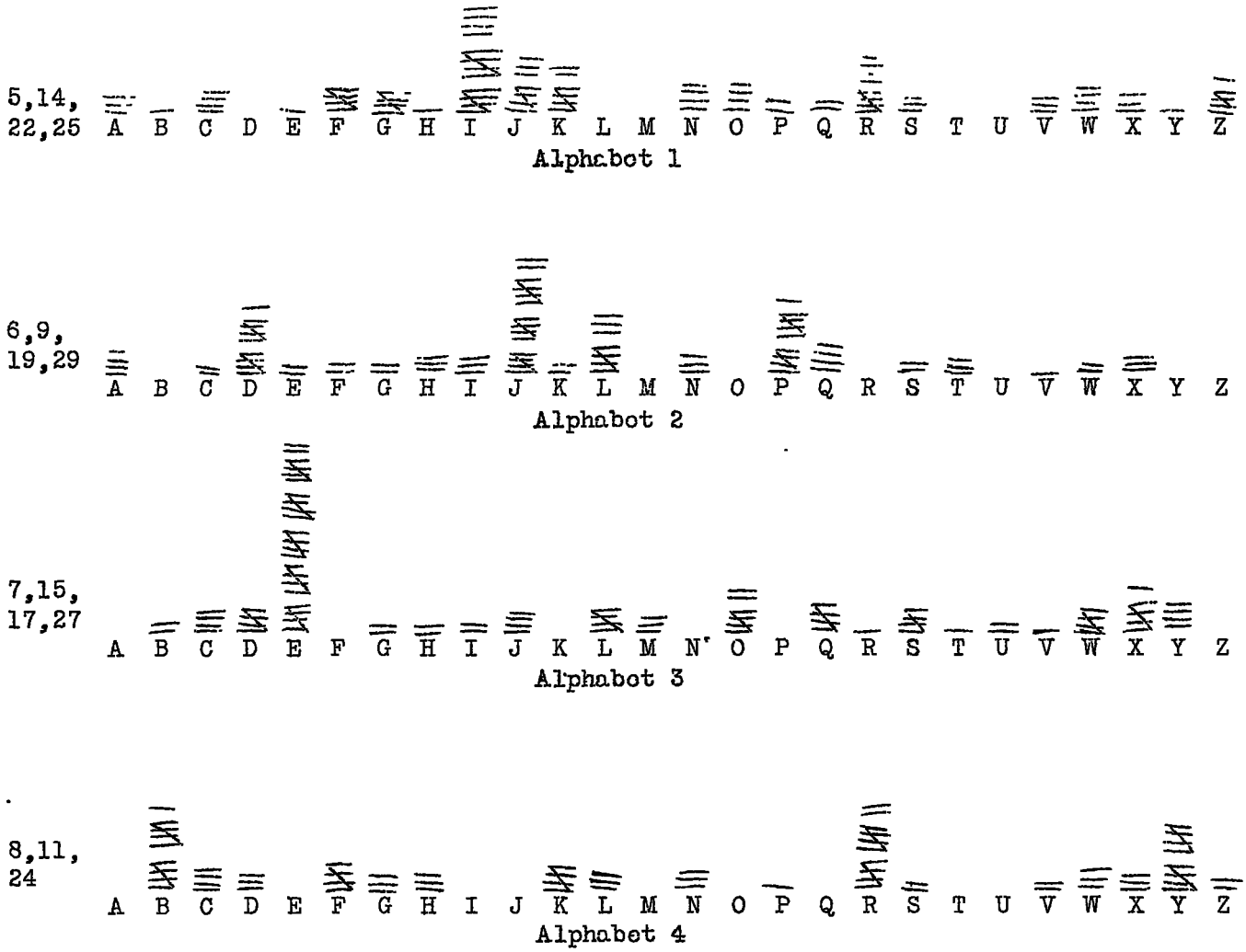
Certainly column 7 belongs with 17. Columns 15 and 16 with values of 64 and 62 respectively also appear to belong in the same group with 7 and 17. But there are several more candidates: columns 23 (X = 44), 26 (X = 30), 27 (X = 58), and 28 (X = 33). Testing columns 15, 16, 23, 26, 27, 28 against column 17, it becomes clear that only columns 15 and 27 belong with 7 and 17. Thus we have again found a group of 4 columns which go together, with a representative in each keying block.

We have four groups of alphabets with the following columns in each group:

Group 1: 5-12-18-28
" 2: 6-9-19-29
" 3: 7-15-17-27
" 4: 8-11-24

The respective small distributions are now combined to yield four larger distributions which can be solved by recourse to principles of frequency and indirect symmetry. These distributions are shown below in Fig. 3

FIGURE 3



Obviously in alphabet 3, $E_c = E_p$. The repeated pentagraph E B D K K in messages 23 and 24, beginning with E_p certainly seems to be E N E M Y, with D_c in column 9 (alphabet 2) equalling E_p, which is corroborated nicely by the frequency of D_c in that alphabet. Also, B_c in alphabet 4 is N_p and the frequency of B is excellent. Once an entering wedge of this kind has been forced into the problem, the rest follows without difficulty.

A reconstruction diagram for the recovery of the cipher component is drawn up and the following sequence is reconstructed:

Solution
Military Cryptanalysis, Part III, 12-p.4, 1938.

REF ID:A60198

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

which is seen to be derived from the key NO SMOKING:

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

The plain component is then quickly recovered: '

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

which is seen to be derived from the key POSITIVELY:

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

The keyword for the unit whose messages have been solved is CONSIDER.

The letter-for-letter solution of the messages is as follows:

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29
C O N S I D E R D O R C N I E S E C D N O I S R I S E C D N O

1) R E Q U I R E T W E N T Y M I N U T E A D V A N C
AVAST J E X T W Y C K G E E X W X V I C N R J G U M S F

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

3) F R E S H T R O O P S N E E D E D H E R E I N O R
AURAL S J E C Q M Y K C A S E E C A N S F S Y I X O K J

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

5) A R E Y O U R E A D Y T O O B S E R V E F O R T H
AZTEC W J O K K R R E Z D W I C H Y D R R V E J L B M Z

6) E N E M Y O B S E R V A T I O N P L A N E C R A S
AXIOM E B D K K K P O E H U M I V H N R N J E E Y J H E

7) C H I E F S I G N A L O F F I C E R R E Q U E S T
ASSAY Q F N E H G W F R H Z J A G G H N C R S X C S S A

8) W H E N C A N Y O U G E T T O G E T T Y S B U R G
AURAL G Q E B H T B W C C I S X A L M O W N K O K H U E

Solution
Military Cryptanalysis, Part III, 12-p.5, 1938.

REF ID:A60198

```
          1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29
          C O N S I D E R D O R C N I E S E C D N O I S R I S E C D N C

 9)       C O N S I D E R A B R I D A D E O F I N F A N T R
   AMASS  Y H X D K A E Y P U Y G M J D S J J N X D J E G R

10)         B A T T A L I O N C O M M A N D E R S W I L L A S
   AMITY    U H N W P Y D L I P K U V L E D C J I A K U N J D

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

12)                E N E M Y A R T I L L E R Y F I R E D E S T R O Y
   AXIOM           E B D K K M B W M U Y C J Q D K H R E S S A J C J

13)              R E Q U E S T R E C O M M E N D A T I O N S F O R
   AVAST         J E X T O C A B I C T W D D X S J N D Q E S J L B

14)                 O B S E R V E R A T O U T P O S T N U M B E R S E
   AZTEC            V W E R U Z I Q Z X K T K F Q D G N J W E D B E R

15)         C O M M A N D I N G O F F I C E R S O F A L L U N
   ARROW    F T V X L B A W B B C S G X C C J I H S Z N Z J O

16)           R E P L Y I N G T O Y O U R L A S T M E S S A G E
   ASSAY      H I C Y K N I F A C H J J Q I P I M V S C O Z I C

17)              R E F E R E N C E M Y N U M B E R S E V E N T E E
   AVAST         J E H D C R R F I W L O V X P O R D R P S O A D N

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

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

20)      C A V A L R Y P A T R O L H A S R E A C H E D O L
   AMASS Y T Z Z Z J T L P M Y K L F L D Q C P I B I G V Z

21)            P R E P A R E T O A D V A N C E A L O N G L I N E
   AURAL       A J E L P C R A C J D V L R H N T Z T B X U M R D

22)           R E G I M E N T A L R E S E R V E L I N E H A S B
   ASSAY      H I E M S D I G M L R E D E U K N P K E R F Z S E

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

24)              R E F E R R I N G T O P A R A G R A P H O N E O F
   AVAST         J E H D C Y G X X X T B M J H N R Z L F T O C L E

25)            W H E R E A R E S E C O N D A N D T H I R D B A T
   AURAL       G Q E Y D T Y C I I C T O H P X S W C D R G V M I
```

Solution
Military Cryptanalysis, Part III, 12-p.6, 1938.

REF ID:A60198

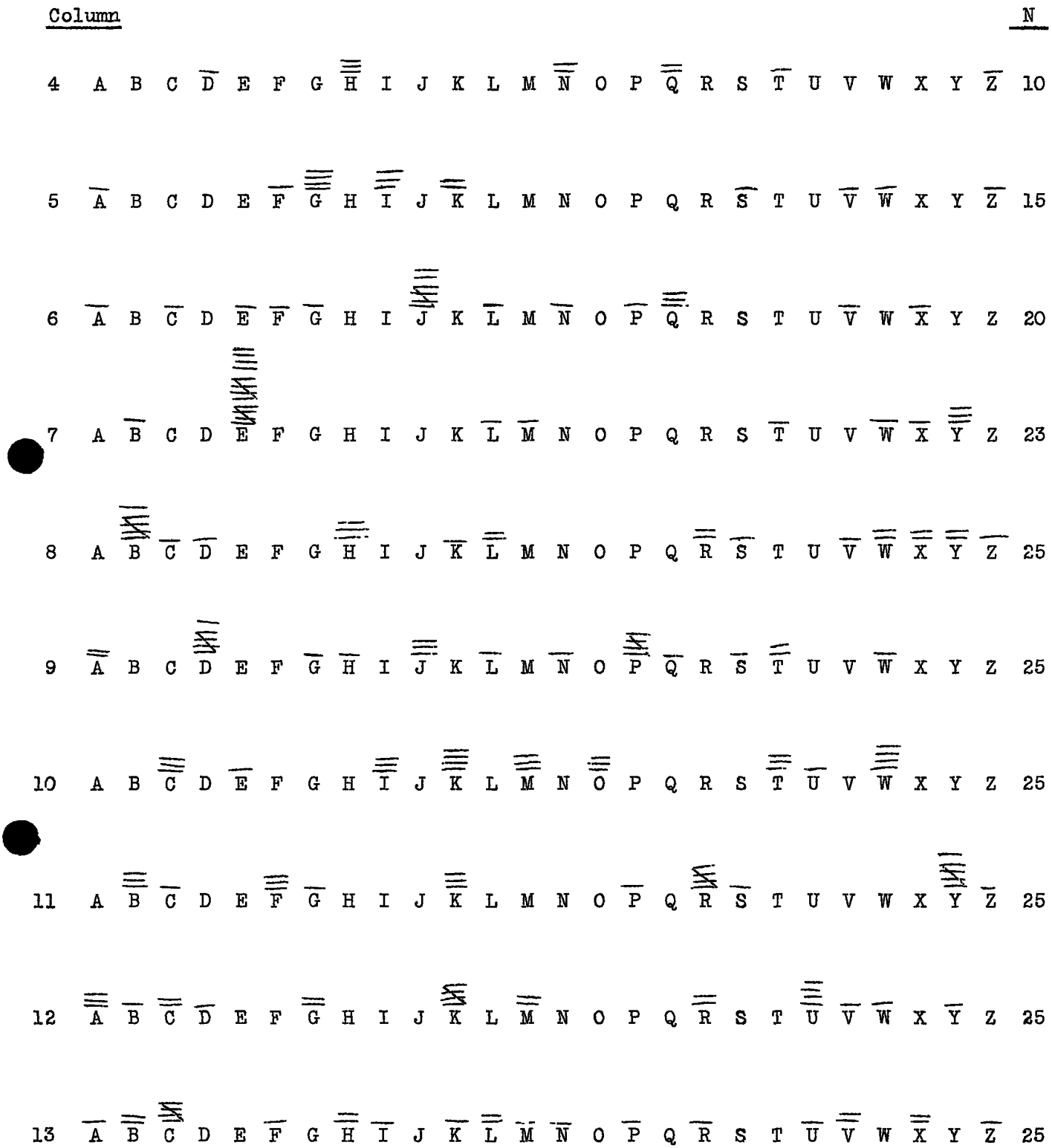
FIGURE 1

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

Solution
Military Cryptanalysis, Part III, 12, p7, 1938

REF ID:A60198

FIGURE 2



Solutions
Military Cryptanalysis, Part III, 12,p8, 1938

FIGURE 2 (continued)

Column																									N
14	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	25
15	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	25
16	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	25
17	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	25
18	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	25
19	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	25
20	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	25
21	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	25
22	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	25
23	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	25

Solutions
Military Cryptanalysis, Part III, 12,p.9-1938

REF ID:A60198

FIGURE 2 (continued)

Column																									N
24	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	25
25	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	25
26	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	22
27	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	21
28	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	20
29	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	15

Solutions
Military Cryptanalysis, Part III, 12 p.10, 1938

REF ID:A60198

TABLE 1

Column	Column N′	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
		15	20	23	25																		22	21	20	15
4	N	10	13	15	17	17	17	17	17	17	17	17	17	17	17	17	17	17	17	17	17	17	15	14	13	10
	10	1	8	1	11	15	3	1	1	9	6	9	13	6	6	11	16	15	8	19	8	6	6	6	0	3
5	15		19	23	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	22	21	19	15
			7	1	5	8	21	15	23	10	28	10	7	5	16	11	19	10	21	14	14	16	18	9	9	6
6	20			31	33	33	33	33	33	33	33	33	33	33	33	33	33	33	33	33	33	33	29	28	27	20
				16	6	34	4	6	8	15	29	32	17	32	19	40	18	7	22	11	12	34	24	9	25	27
7	23				39	39	39	39	39	39	39	39	39	39	39	39	39	39	39	39	39	39	34	32	31	23
					18	4	24	21	7	7	3	64	62	80	4	7	19	6	5	44	11	16	30	58	33	17
8	25					42	42	42	42	42	42	42	42	42	42	42	42	42	42	42	42	42	37	35	33	25
						14	15	46	23	37	22	24	18	23	20	21	19	23	23	21	38	14	12	12	10	12
9	25						42	42	42	42	42	42	42	42	42	42	42	42	42	42	42	42	37	35	33	25
							10	7	15	12	18	28	35	23	18	55	17	31	12	31	19	23	27	13	13	36
10	25							42	42	42	42	42	42	42	42	42	42	42	42	42	42	42	37	35	33	25
								15	40	26	29	24	17	22	45	17	29	30	36	13	14	25	11	30	29	11
11	25								42	42	42	42	42	42	42	42	42	42	42	42	42	42	37	35	33	25
									38	24	23	9	5	11	22	10	7	16	45	15	56	27	13	5	20	6
12	25									42	42	42	42	42	42	42	42	42	42	42	42	42	37	35	33	25
										30	22	14	11	13	48	11	13	16	34	17	31	10	19	11	41	10
13	25										42	42	42	42	42	42	42	42	42	42	42	42	37	35	33	25
											26	25	15	18	40	24	39	27	22	24	32	28	10	12	34	13
14	25											42	42	42	42	42	42	42	42	42	42	42	37	35	33	25
												22	16	17	29	32	40	20	39	17	25	46	18	17	21	17
15	25												42	42	42	42	42	42	42	42	42	42	37	35	33	25
													35	48	27	31	26	19	19	33	22	27	25	31	26	29
16	25													42	42	42	42	42	42	42	42	42	37	35	33	25
														41	11	24	20	31	13	46	13	18	40	38	15	22
		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

Solution
Military Cryptanalysis, Part III, 12.-p.11, 1938

REF ID:A60198

TABLE 1 (Continued)

Column	Column N'	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
		15	20	23	25																		22	21	20	15
17	25																42	42	42	42	42	42	42	37	35	33	25
																	19	24	25	13	13	27	18	29	26	39	23	21
18	25																	42	42	42	42	42	42	42	37	35	33	25
																		16	24	26	32	21	29	26	13	20	46	14
19	25																		42	42	42	42	42	42	37	35	33	25
																			35	22	21	17	16	35	18	7	12	34
20	25																			42	42	42	42	42	37	35	33	25
																				24	27	23	23	42	12	17	15	11
21	25																				42	42	42	42	37	35	33	25
																					14	33	17	19	25	35	19	14
22	25																					42	42	42	37	35	33	25
																						21	39	39	19	15	18	14
23	25																						42	42	37	35	33	25
																							29	19	37	32	21	20
24	25																							42	37	35	33	25
																								28	9	6	20	12
25	25																								37	35	33	25
																									17	19	21	18
26	22																									31	29	22
																										33	15	18
27	21																										28	21
																											17	13
28	20																											19
																												14
		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

Solution
Military Cryptanalysis, Part III, 12.-p.12, 1938