ARMY EXTENSION COURSES

Subcourse-Military Cryptanalysis Part I
Monoalphabetic Substitution Systems

Introduction.

Purpose and Scope:

The purpose of this subcourse is to teach the student the methods of analysis of the more simple military cipher systems.

The scope of this subcourse is: Fundamental principles; monoliteral substitution; polyliteral substitution; polygraphic substitution; and miscellaneous monoalphabetic substitution systems.

Number of Lessons and Approximate Time Required:

This subcourse consists of 10 lessons and will probably require approximately 41 hours of work by the average student.

The time listed for this subcourse and for each lesson 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 the lesson or subcourse.

Texts Required:

Military Cryptanalysis-Part I-Monoalphabetic Substitution Systems (1936). As prepared under the direction of the Chief Signal Officer.

Materials Required :

Cross-section paper.

Special Instructions and Information:

This subcourse and the text used therewith were prepared under the direction of the Chief Signal Officer.

So far as practicable, detailed work sheets which usually form a part of the solution should be submitted with the solutions.

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

~~CONFIDENTIAL~~

ARMY EXTENSION COURSES

LESSON ASSIGNMENT SHEET

SUBCOURSE -Military Cryptanalysis-Part I.

LESSON 1 -Fundamental Principles.

ESTIMATED TIME -4 hours.

TEXT ASSIGNMENT -Text, Sections I and II.

MATERIALS REQUIRED -Cross-section paper of 1/4 inch squares.

MAXIMUM WEIGHT -100.

SUGGESTIONS -None.

EXERCISE

Weight:

4 1. a. What four things were thought by Capt. Hitt to be essential to cryptanalytic success?

5 b. What five additional elements are also highly desirable?

4 2. What four fundamental operations are involved in the solution of practically every cryptogram?

4 3. Indicate the language in which you would expect the plain-text of the cryptographed portion of the following message to be written. Give your reasons for your answer.

From: Felipe Madrazo, Mexico City, Mexico.
To: Andres Gonzales, New York City.

Su telegrama relativo. DIRLTIR DI MTI INXEQMTI TRSID LEQE TJK DI JTIRSQKR LTIQSKR GE HEMTAJEQAE MTI SIJIHKR IJ IRE LTIDI TRSID REGAQ LEQE IRSE

1 4. In the solution of cryptograms involving a form of substitution to what simple terms is it necessary to reduce them in order to reach a solution?

2 5. Is it always necessary to determine the specific key in order to reconstruct the plain text?

20 6. In the following passage each dash indicates the omission of a word or part of a word. Complete the passage by writing on the printed paper over each dash the word or part which seems to you the most appropriate.

Weight: Shortly after the disastrous ------ of Camden, Washington ----- to the President of Congress, "What we need is a good ----, not a ----- one." Unfortunately for the -------, the object sought by this -----tion, so thoroughly in h------ with our cherished institutions, has only been --------- attained in ---- of peace.

In view of the ----th of our neighbors, the vast ex---- of our territory, and the rapid in------ of our floating population, the time must ------ly arrive when intelligent and law-abiding ------ will accept, and adhere to, the ----ion of John Adams that the National ------- is one of the cardinal duties of a s-----man.

Our military ------, or as ---- would affiem, our want of it, has now been tested during ---- than a century. It has been tried in foreign, ------ic, and Indian ----, and while military men, from painful ex--------, are united as to its de----- and dangers, our final ------- in each conflict has so blinded the popular ----, as to induce the belief that as a ------ we are in--------.

With the greater mass of ------, who have neither the time nor the in--------- to study the -------ments of -------- science, no ----- is more common than to mis---- military resources for military --------, and particularly is this the case with ---selves.

History records our triumph in the ------tion, in the War of ----, in the Florida War, in the M------ War, and in the Great ------ion, and as nearly all of ----- wars were largely begun by ------- and volunteers, the conviction has been pro------ that with us a ------- army is not a necessity.

7. a. In the following examples the words of sentences have been transposed. Rearrange the words to make plain text.

1 (1) FRONT VERY IN ENEMY OUR QUIET IS
1 (2) OFF ATTACK TIME ON JUMPED OUR

b. In the following examples the letters of several words of each sentence have been transposed. Rearrange the letters to make good words that will give intelligible plain text.

3 (1) Enemy OPPRSTU line DEIINS of woods is AEHILVY manned.

3 (2) Am CEEGIINRV heavy EFIR from apple ACDHORR.

c. In the following examples the words of each sentence have been transposed and in the case of several words the letters have also been transposed. Reconstruct the plain text.

4 (1) VICINITY AFINNRTY OF IS BDEGIR ENEMY GIMNOV STONE FMOR.

3 (2) ATTACK CDENOS NOW IINOOPSST IN ABDEGIR.

Military Cryptanalysis, Part I, 1-p 3
1936-37.

Weight:

d. In the following examples the letters of each word of each sentence have been rearranged in the order in which they appear in the normal standard alphabet.. Reconstruct the plain text.

10 (1) EHILOST AACKTT AHS ADEM NO EGOPRRSS AAGINST HIST CEORST.

10 (2) AACCEKNORTTTU BY ABDEGIR EEERRSV ILLW BE ACDEHLNU AT AABDEKRY.

e. In the following examples the plain text has been broken up into groups of five letters and then in each group of five the letters have been rearranged in the order in which they appear in the normal standard alphabet. Reconstruct the plain text.

10 (1) EEMNY ISSPU GHHIN AITTS ACIKW GHITV OR

15 (2) EGIMV EORUY CEMOR ADEMN INOST CCENO GINNR EFOSU CENOS ADKNT ACMOP NY.

ARMY EXTENSION COURSES

LESSON ASSIGNMENT SHEET

SUBCOURSE - Military Cryptanalysis, Part I.

LESSON II - Frequency distributions.

ESTIMATED TIME - 4 hours.

TEXT ASSIGNMENT - Text, Sections III and IV, and attached memorandum.

MATERIALS REQUIRED - Cross-section paper of 1/4 inch squares.

MAXIMUM WEIGHT - 100.

SUGGESTIONS - None.

EXERCISE

Weight:

6 1. Using cross-section paper prepare a monoliteral frequency bar distribution of the letters of the following news item:

"Rulers are part of the equipment of Chinese railway conductors. Children are paid for by the foot. Those under two feet six inches ride free, those between that height and four feet four inches pay half fare, and taller ones are classed as adults."

2 2. a. What are the four most frequent consonants in English telegraphic text?

3 b. What are the five least frequent letters in English telegraphic text?

1 c. What percent (in round numbers) of the letters in English telegraphic text are vowels?

3 d. Why are the frequencies of letters in English literary text different from those in telegraphic text?

8 3. What four facts can be determined from a study of the monoliteral frequency distribution of a cryptogram?

4. Determine the class to which the cipher systems, which were used in enciphering the following messages, belong:

Weight:

4 a. E I Y T R T N S Q I F E E V U N R T M E I O O I Y
R E U N O

4 b. Q W T C V V C E M L W O R G F Q H H Q P V K O G X

4 c. S Z P V X Z F R H B V W S Q L L A Q C E V B G
G J V

5. Which of the following substitution ciphers are monoalphabetic?

5 a. N H M Q A D S E Q Q E P C N E M F E O S G H J L H
T L S M M E T E A G M Q I L H G Q H I X L A T E O
S M S P Q H L O R L A G T Q N S D E M Q N H R L X

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

5 c. T R E V N V B L F I I V X L N N V M W Z G R L M H
U L I I V K O Z X R M T W R E R E R L M I V H V I
E V D S V M H Z N V S Z H Y V V M X L N N R G G V
W G L Z X G R L M X

6. The following messages were enciphered monoalphabetically. Determine in each case whether the cipher alphabet used was a standard or mixed alphabet and if standard, whether direct or reversed.

10 a. A T P O Z W D Z U C H U O Q J L Z O A O H U X P Z
P V T M Z U B D H P O C Q T V O A D Q H M Z U D L
D P O T C Q L A D D W D Q X X

Weight:

10 b. W R I F S G H I.P Q L I I J O N H W J J L I W R M
P I L G W Q N I H E O Q N G W Q E D Q I A E W A I
S Q W A W Q Q W F N I H N O R L I O O N H T Q M E
M N T M T L I S H D E W O Q I P C N H T U N F F E

10 c. H P B G Z M H M K T Y Y B V V H G Z X L M B H G T
M P X L M X K G X Q B M L H Y Z X M M R L U N K Z
K X V H F F X G W I K X I T K T M B H G H Y V B K
V N E T M B H G F T I U X X Q I X W B M X W X X X

7. From the intercepted traffic of three intercept stations operating in the same sector of the front, the following messages were selected for study by a member of the code and cipher solution section at GHQ. They are undoubtedly three versions of one enemy cipher message, but there appears to be a number of differences, due no doubt to operating difficulties at the several stations. Study the messages and reconstruct from them the actual message sent by the enemy station.

20 I. Time intercepted 10:05 a.m. by X Y D A X V X A R

G R 35 B T

N R 1 7 D Y B I E D U F T O A M E J A K I B O N
S G C O Y F O B A K D O D L A L U F Y D K A W A L
A P A Y N C O D A P K E D U R J O P I D J E N O X
M E H A Z L O G I S K U T E G E V A U K I P B E M
K E H Z A H O B W E A V D U Z F O F A E M C O Z
E G B L O D O F Y O E N C - - M A W E N - - - - -
- -

II. Time intercepted 10:03 a.m. by L K D A X V X A A

G R 3 5 B T

N R I - D Y B I E B U F T O A M E J A K I B O N

I P K O - F - B A K D O D L A L U F Y L K A W A L

A P A Y N - - - - - - - - D U A - - P I D J E N O X

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

K E H Z A S O B W E V A D U Z F O F E T E M C O Z

E G B L O D O F Y O A E C D A M A W E N - - - O M

E M C O Z A C F A H L O F I R 0 9 3 5

III. Time intercepted 10:05 a.m. by K Z D A X V X A R

G R - - B T

N R 1 7 D Y B I E D U F T O A M E J A K S B O N

I P C O Y - - - A - D O - - - L U F Y L K A W A L

A P E T Y N C O D A P K E D U R W O P I D J E N O X

M E H A Z L O G H K U T E G E V A U K I P B E M

K E H Z A H O B W E A V D U Z F O F E T E M C O Z

E G B L O D O F Y O E N C O A M A W E N M A W E N

E X F O M E M C O Z A C F A H L O F I R 0 9 3 5

MEMORANDUM

Before a military cryptanalyst can begin the analysis of an enemy cryptographic system, it is necessary for him to study the intercept material that is available to him, isolate the messages that have been enciphered by means of the cryptographic system to be studied, and to arrange the latter in a systematic order for easy analysis. This work, although apparently very simple, may require a great deal of time and effort.

Since, whenever practicable, two or more intercept stations are provided to copy traffic emanating from the stations of one enemy radio net, it is natural that there should be a certain amount of duplication in the work of the several stations. This is desirable since it provides the cryptanalysts with two or more sets of the same messages so that when one intercept station fails to receive all the messages completely and correctly, because of set difficulties, local static, or poor operation, it is possible by studying the other sets to reconstruct accurately the entire traffic of the enemy net.

In all intercept activities where operators are used for copying the traffic, one of the most likely errors to be found is caused by the human error in reception. For this reason cryptanalysts and their assistants should be familiar with the Morse telegraph alphabets and the most common errors of wire and radio transmission methods so as to be able to correct garbled groups when they occur. In this work the following table will be found useful:

MOST COMMON ERRORS IN TELEGRAPHIC TRANSMISSION

Continental Morse alphabet (used in radio, cables, and outside U. S.)			American Morse alphabet (used in the United States, Except for radio)		
Letters and figures	Alphabet	Frequent errors	Letters and figures	Alphabet	Frequent errors
A	.-	i, m, t, et	A	.-	i, t, et
B	-...	d, ts	B	-...	d, h, ts
C	-.-.	f, k, j, r, nn	C	.. .	s, z, ie
D	-..	b, s, l, ti	D	-..	b, ti
E	.	t, a, i	E	.	t
F	..-.	q, r, in	F	.-.	r, q, en
G	--.	m, n, o, q, me	G	--.	n, c, me
H	....	s, v, b, se	H	....	s, p, z, y, es
I	..	a, n, s	I	..	a, o, e
J	.---	w, o, eo, am	J	-.-.	c, k, ke
K	-.-	a, n, d, o, ta	K	-.-	j, n, ta
L	.-..	x, r, d, ed	L	——	t, n
M	--	a, n, i, tt	M	--	n, a, tt
N	-.	i, m, t, te	N	-.	o, t, te
O	---	g, k, m, w, mt	O	. .	n, i, ee
P	.--.	j, w, g, l, r, an	P	.....	h, s
Q	--.-	g, k, o, x, z, ma	Q	..-.	f, g, u, in
R	.-.	a, n, f, g, s, l, w	R	. ..	s, i, ei
S	...	h, d, i, r, u, v	S	...	h, r, i
T	-	a, e, n	T	-	l, e, n
U	..-	a, s, v, it	U	..-	v, a, w, it
V	...-	h, u, x, st	V	...-	u, st
W	.--	a, m, o, r, u, at	W	.--	f, a, u, m, at
X	-..-	d, v, u, k, y, tu	X	.-..	l, y, f, ai
Y	-.--	x, w, k, c, nm	Y	.. ..	h, ii
Z	--..	b, d, g, q, mi	Z	... .	h, c, se
1	.----	0, 2	1	.--.	p
2	..---	1, 3	2	..-..	3
3	...--	2, 4	3	...-.	4
4	....-	3, 5	4	....-	3
5	.....	4, 6	5	---	
6	-....	5, 7	6	.....	p
7	--...	6, 8	7	--..	
8	---..	7, 9	8	-....	
9	----.	8	9	-..-	x
0	-----	9	0	——	L

Errors frequent in both systems:
. is omitted
- is omitted
. is transmitted as -
- is transmitted as .

Military Cryptanalysis,
Part I, 2-p 6
1936-37.

ARMY EXTENSION COURSES

LESSON ASSIGNMENT SHEET.

SUBCOURSE - Military Cryptanalysis Part I.

LESSON III - Monoliteral substitution with standard cipher alphabets.

ESTIMATED TIME - 3 hours.

TEXT ASSIGNMENT - Text, Section V.

MATERIALS REQUIRED - Cross-section paper of 1/4 inch squares.

MAXIMUM WEIGHT - 100.

SUGGESTIONS - None.

EXERCISE

Weight:

60 1. a. Solve the following cryptogram:

K D Z Y J G N R Y Y R P H K R Z Q N N E Z Y D C C

N O J E M A D E Y D M Q R Y Y R G J D E A N Z N A

W N G J E N J E A J L K Y P N E Y N A D M A N Z J

Z Y R E P N D M Y K J A O J E M R E Y A T Z Y D C

Y K J A O J E M R E Y A T J Z P D X E Y N A R Y Y

R P H J E L V J Y K A N L J F N E Y R G A N Z N A

W N Y D A N N Z Y R Q G J Z K M A D E Y G J E N

10 b. What is the specific key?

5 c. Name two methods of solving ciphers of this type.

10 2. a. In the solution of a substitution cipher by completing the plain component sequence involving reversed standard alphabets, what are the successive steps?

Weight:

5 b. If a short cryptogram is enciphered by means of a cipher alphabet of which the plain component is a known mixed sequence, can it be solved by completing the plain component sequence?

5 3. a. What is the first step one should take in attempting to solve an unknown cryptogram that is obviously a substitution cipher?

5 b. If this step is unsuccessful and the cryptogram is obviously monoalphabetic in character, what type of cipher alphabet may be assumed to have been used?

ARMY EXTENSION COURSES

LESSON ASSIGNMENT SHEET

SUBCOURSE - Military Cryptanalysis Part I.

LESSON IV - Monoliteral substitution with mixed cipher alphabets.

ESTIMATED TIME - 5 hours.

TEXT ASSIGNMENT - Text, pars. 23-31, Section VI.

MATERIALS REQUIRED - Cross-section paper of 1/4 inch squares.

MAXIMUM WEIGHT - 100.

SUGGESTIONS - None.

EXERCISE

Weight:

5 1. Why do monoalphabetic cryptograms involving standard cipher alphabets yield such a low degree of cryptographic security?

40 2. a. Construct a triliteral frequency distribution showing one prefix and one suffix of the following cryptogram and indicate by underscoring all repetitions of three or more letters:

I F I E X Q M H H J P D W T I O I I F P A G D Q I

K H F D A G D G M H S F K I W P Q H N G M I I F T

A C C I W F K A F Q D I T A R A F A Q X H N I W G

C I C W B I P Q H J P I T I M W C R H E O W Q J W

Q M H C P D W T I O I I F P I F Q H S Q Q H G W A

F R H F Q W R Q U A Q D Q D I I F I E X W F K G W

A F A F N H M E W Q A H F W P Q H D A P I V W R Q

J H P A Q A H F P Q H J U A C C M I J H M Q N S M

Q D I M H F Q D I A M M I Q S M F

Weight:

10 b. Prepare a condensed table of repetitions of trigraphs and digraphs appearing more than twice in the cryptogram given in a.

55 c. Using the data obtained in a and b above, complete the solution of the cryptogram.

10 d. Determine the cipher alphabet and the keyword used.

ARMY EXTENSION COURSES

LESSON ASSIGNMENT SHEET

SUBCOURSE - Military Cryptanalysis Part I.

LESSON V - Monoliteral substitution with mixed cipher alphabets.

ESTIMATED TIME - 8 hours.

TEXT ASSIGNMENT - Text, Pars. 32-34, Section VI.

MATERIALS REQUIRED - Cross-section paper of 1/4 inch squares.

MAXIMUM WEIGHT - 100.

SUGGESTIONS - None.

EXERCISE

Weight:

8 1. What two places in every message lend themselves more readily to successful attack by the assumption of words than do any other places? Why?

10 2. What is meant by the "probable word method" of solution?

7 3. a. What is meant by the word formula: A B B A C D A ?

b. For each formula given below indicate one good English word that fits exactly:

5 (1) A B C B D B E F

5 (2) A B B A C D

5 (3) A B C D B C E

60 4. Using the cipher alphabet applying to the cryptogram given in problem 2 of lesson IV, solve the following by means of it:

W V Q H M V G V N M S Q B B Q Z V D G X

B D G E D X C V T D G U O G X Q G E B M

ARMY EXTENSION COURSES

LESSON ASSIGNMENT SHEET

SUBCOURSE - Military Cryptanalysis, Part I.

LESSON VI - Polyliteral substitution with mono-equivalent cipher alphabets.

ESTIMATED TIME - 4 hours.

TEXT ASSIGNMENT - Text, Section VII.

MATERIALS REQUIRED - Cross-section paper of 1/4 inch squares.

MAXIMUM WEIGHT - 100.

SUGGESTIONS - None.

EXERCISE

Weight:

70 1. a. Solve the following:

U A K E Y K Y K C E Y K C R L A Y E C A U K C E U

A Y K U R B U A U A Y B Y E K K K E Y B U E Y R

Y K Y K C E Y A Y K K B K A C E K A U A Y K C B L

A U E U A C A C K C K Y K Y A Y K Y B U E U A C A

K B L R K E Y A U A Y K U R U K C E U E U A C A C

K C R L A C B K A C E Y K C E C A L R Y K L E U A

Y K C E Y A U E K B U R C A C R U R C A Y B Y A K

A U K C E Y E U A K A C A C E U A L R C A U A K E

U R Y K Y K Y K K A K R K E U A U A C A U A K E Y

K Y E U R C A U E U E U R C A Y B Y A Y K Y B U E

U A C A K B K B Y B K A U R C K C B Y B L A X X X

Weight:

b. Determine the keywords used.

30 2. Find the secret text in the following message:

March 15th

Dear George:

When you read this letter I will probably be basking in the sun of southern California. I thought I would leave today but Mary wanted me to remain here for her birthday party so now I am planning to take an early train tomorrow. I hope you will be able to join me in a few weeks. Give my love to everyone at home.

Cordially yours,

Marion.

Military Cryptanalysis, Part I, 6-p 2
1936-37.

ARMY EXTENSION COURSES

LESSON ASSIGNMENT SHEET

SUBCOURSE - Military Cryptanalysis Part I.

LESSON VII - Polyliteral substitution with poly-equivalent cipher alphabets.

ESTIMATED TIME - 5 hours

TEXT ASSIGNMENT - Text, Section VIII.

MATERIALS REQUIRED - Cross section paper of 1/4 inch squares.

MAXIMUM WEIGHT - 100

SUGGESTIONS - None.

EXERCISE

Weight:

5 1. a. What is the purpose of providing variants in a cipher system?

5 b. From the cryptanalytic point of view, how does simple monoalphabetic substitution differ from monoalphabetic substitution with variants?

85 2. a. Solve the following:

D Z F V J X R W D X Q W H Z L V L W L X B T P Z B

Z K W N T F X D V C X Q T K T N Z L V P T H T R V

K V P W K X R Z R W B Z H T R V H Z P T F V K X K

V R X J W N Z L X C W P X R V N X B V B T L X F X

H T D T J X Q X D W J T P X C T F X J W P X K W P

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

X K W N Z F V L W R W L X B T R X N Z R X P W H T

F X L X C W B Z F W H Z H W K X Q W H X B V B T F

Weight:

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

5 b. From the cryptographic point of view, what serious disadvantage does this type of system have?

Military Cryptanalysis, Part I, 7-p 2
1936-37.

ARMY EXTENSION COURSES

LESSON ASSIGNMENT SHEET

SUBCOURSE - Military Cryptanalysis, Part I.

LESSON VIII - Polygraphic substitution systems - 4 - square checkerboard designs.

ESTIMATED TIME - 4 hours

TEXT ASSIGNMENT - Text, pars. 41 - 44, Section IX.

MATERIALS REQUIRED - Cross section paper of 1/4 inch squares.

MAXIMUM WEIGHT - 100.

SUGGESTIONS - None.

EXERCISE

Weight:

4 1. a. What is polyliteral substitution? What is polygraphic substitution?

4 b. In true digraphic substitution, if $\overline{ER}_p$ yields $\overline{XN}_c$, is it possible for $\overline{EN}_p$ to yield $\overline{AB}_c$?

2 c. What is the fundamental purpose of polygraphic substitution?

90 2. Solve the following:

L O Q M E E C Q N K G G Q A S B N P R M E L N A T

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

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

Q R G X D S T Q N R X D H M X O G L S R D T S H G

S E R D K M F A H G T Q B F Q Q C C T Y E K C P K

F R L O U K U Q A U O C B Q I E P T H V T R O Q M

L P Q A F A Q A E Q F T C P R G K Q D U X A S V S

H S Y C C I U T P H A F G T P D U R D T S S H R M

FABNF CHGTQ NMIHU UZSHM RGGQE

BNGCI MTFSK UELNA TSEQC QEQZS

QNSVS HFCIO CICIO ODOEP CQMIR

AGNAG RMLGK BGNQA IHLUK WTSVS

HUSHR PBNUF KAKMR MLGTA YERNH

GUOUU MWCQO UZSIO CIKDZ STPLG

HPBPB GFUKC GNRMU OECKE LUDPR

MSHRM FABNF CHGCI AGIHN ABMXX

Military Cryptanalysis, Part I, S-p . 2
1936-37.

ARMY EXTENSION COURSES

LESSON ASSIGNMENT SHEET

SUBCOURSE - Military Cryptanalysis, Part I.

LESSON IX - Polygraphic substitution systems - Playfair cipher system.

ESTIMATED TIME - 5 hours.

TEXT ASSIGNMENT - Text, pars. 45 - 46, Section IX.

MATERIALS REQUIRED - Cross section paper of 1/4 inch squares.

MAXIMUM WEIGHT - 100.

SUGGESTIONS - None.

EXERCISE

Weight:

5 1. What are the characteristics of a Playfair cipher which make it recognizable?

95 2. Solve the following:

V F L Q G E A S K Q M Z Y S Q K C H U I Q W A H V

F S Y O Y I B I X S M C D K O S Y R N S K L C O S

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

M C D R G X P X K A H V X D L R G S O S V Z V W F

K Q W X C H Y X Y N Z C Z E T K M P O X M G Y W R

D T S L C B U P M U M Z C S Y R O R G R D X M S G

V U P T V E T H S Y Y K M G Y P G O Y N H U U B Y

T M C I X S Y D M X U A H G Q Y X F U I Y K R V F

S Y M T M C R C O S A R C R C P Y D V F N B C Z Y

D V F K O T K X V H K C A Y S K Q S O Y R X L A H

V F Y P V W N B S M S Y C I P T G P S G K U K Y G

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

ARMY EXTENSION COURSES

LESSON ASSIGNMENT SHEET

SUBCOURSE - Military Cryptanalysis, Part I.

LESSON X - Miscellaneous monoalphabetic substitution systems.

ESTIMATED TIME - 4 hours.

TEXT ASSIGNMENT - Text, Section X.

MATERIALS REQUIRED - Cross section paper of 1/4 inch squares.

MAXIMUM WEIGHT - 100.

SUGGESTIONS - None.

EXERCISE

Weight:

2 1. a. What characters are most used in practical cryptography today?

2 b. What is the usual preliminary procedure in solving cryptograms involving symbols?

4 c. In monoalphabetic substitution with variants, what characters are most commonly used? Why?

2 2. What is the primary purpose of an analytical key?

90 3. Solve the following:

V X O I H N O N Y N X W R I Y I R O I D P X W F I

T W H I R F X O I R X J R N H K I I D Y P X J Q D

F X E Y P X G W P X Z X Y N P N X W D U X W K Y P

R I D V U N W I Q T Y P I D Y P X J L N U U X W I

W N W I P L R I I S T O P U S E M A C C A N J U S

F J X Z C E S H J S E E X Z J Z V N A B E D R S D

E X O U R X B U Q Q A S D Z C U V O U R Q A O A S

C J B J V A C E E A X N O B U R S C E X A T T A C

K P C O D W D S D K J Q G S G Q W G A Q K I J G Y

Q B D H H K J G U X K K J G Y M Y D J S U G J G I

C S Y H D G J U S U K L D J A K Q I T K I I Y J O

D J M M G J G Q Y H S G T K J O P Q D M Y O G K A

C K V Q I K W G

Military Cryptanalysis, Part I, 10-p 2
1936-37.

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE -Military Cryptanalysis-Part I.

LESSON 1 -Fundamental Principles.

Weight:
4 1. a. (1) perseverance, (2) careful methods of analysis, (3) intuition, (4) luck.

5 b. (1) A broad general education.
(2) Access to a large library of current literature and direct contacts with sources of collateral information.
(3) Proper coordination of effort.
(4) Faculty of being able to concentrate on a problem for rather long periods of time without distraction, nervous irritability, and impatience.
(5) A retentive memory, especially in the solution of code.

4 2. (1) The determination of the language employed in the plain-text version.
(2) The determination of the general system of cryptography employed.
(3) The reconstruction of the specific key in the case of a cipher system, or the reconstruction, partial or complete, of the code book, in the case of a code system; or both, in the case of an enciphered code system.

(4) The reconstruction of the plain text.

4 3. Spanish: The correspondents are apparently Spaniards or Mexicans and it is natural to expect them to use their native language. Furthermore, the plain-text words in the message are Spanish so it is probable that the enciphered text is also.

1 4. Monoalphabetic terms.

2 5. No.

20 6. Shortly after the disastrous battle of Camden, Washington wrote to the President of Congress, "What we need is a good Army, not a large one." Unfortunately for the country, the object sought by this assertion, so thoroughly in harmony with our cherished institutions, has only been partially attained in time of peace.

In view of the growth of our neighbors, the vast extent of our territory, and the rapid increase of our floating population, the time must speedily arrive when intelligent and law-abiding people will accept, and adhere to, the opinion of John Adams that the National defense is one of the cardinal duties of a statesman.

Weight:

Our military policy, or as many would affirm, our want of it, has now been tested during more than a century. It has been tried in foreign, domestic, and Indian wars, and while military men, from painful experience, are united as to its defects and dangers, our final success in each conflict has so blinded the popular mind, as to induce the belief that as a nation we are invincible.

With the greater mass of people, who have neither the time nor the inclination to study the requirements of military science, no error is more common than to mistake military resources for military strength, and particularly is this the case with ourselves.

History records our triumph in the Revolution, in the War of 1812, in the Florida War, in the Mexican War, and in the Great Rebellion, and as nearly all of these wars were largely begun by militia and volunteers, the conviction has been produced that with us a regular army is not a necessity.

1 7. a. (1) ENEMY IS VERY QUIET IN OUR FRONT.

1 (2) OUR ATTACK JUMPED OFF ON TIME.

5 b. (1) ENEMY SUPPORT LINE INSIDE OF WOODS IS HEAVILY MANNED.

5 (2) AM RECEIVING HEAVY FIRE FROM APPLE ORCHARD.

4 c. (1) ENEMY INFANTRY IS MOVING FROM VICINITY OF STONE BRIDGE.

5 (2) SECOND BRIGADE NOW IN ATTACK POSITIONS.

10 d. (1) HOSTILE ATTACK HAS MADE NO PROGRESS AGAINST THIS SECTOR.

10 (2) COUNTERATTACK BY BRIGADE RESERVE WILL BE LAUNCHED AT DAYBREAK.

10 e. (1) ENEMY IS PUSHING HIS ATTACK WITH VIGOR.

15 (2) GIVE ME YOUR RECOMMENDATIONS CONCERNING USE OF SECOND TANK COMPANY.

Solutions
Military Cryptanalysis,1-p 2
1936-37.

ARMY EXTENSION COURSES

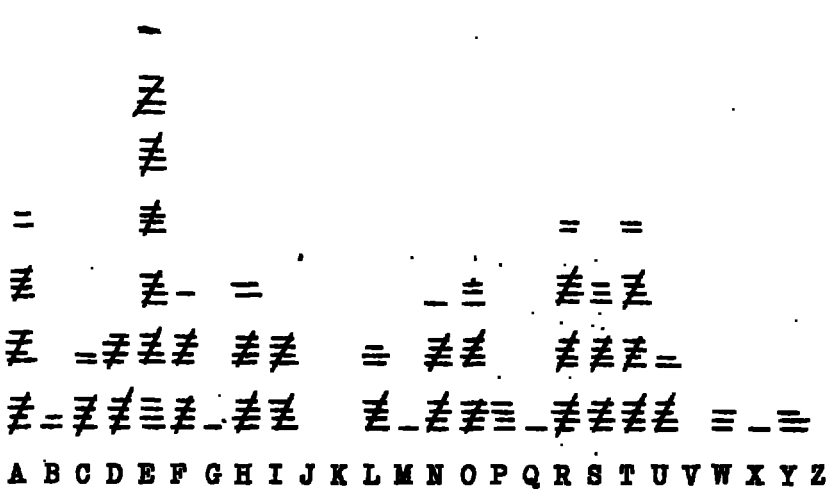
SOLUTIONS

SUBCOURSE - Military Cryptanalysis, Part I.

LESSON II - Frequency distributions.

Weight:

6 1.



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

2 2. a. N, R, S, and T.

3 b. J, K, Q, X, and Z.

1 c. 40 per cent.

3 d. Because (1) in telegraphic text words which are not strictly essential for intelligibility are omitted; (2) certain essential words, such as "stop", "period", "comma", etc., must be spelled out in telegraphic text and occur frequently; and (3) telegraphic text often employs longer and more uncommon words than ordinary literary text.

8 3. (1) Whether the cipher belongs to the substitution or the transposition class;
(2) If a substitution cipher, whether it is monoalphabetic or polyalphabetic in character;
(3) If monoalphabetic, whether the cipher alphabet is a standard cipher alphabet or a mixed cipher alphabet;
(4) If standard, whether it is a direct or reversed standard cipher alphabet.

4 4. a. Transposition.

4 b. Substitution.

4 c. Substitution.

Weight:

15 5. a and c are monoalphabetic. b is polyalphabetic.

10 6. a. Reversed standard.

10 b. Mixed.

10 c. Direct Standard.

20 7. D A X V X A R G R 3 5 B T

N R 1 7 D Y B I E D U F T O A M E J A K I B O N

I P C O Y F O B A K D O D L A L U F Y L K A W A L

A P A Y N C O D A P K E D U R J O P I D J E N O X

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

K E H Z A H O B W E A V D U Z F O F E T E M C O Z

E G B L O D O F Y O E N C O A M A W E N M A W E N

E X F O M E M C O Z A C F A H L O F I R 0 9 3 5

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE - Military Cryptanalysis, Part I.

LESSON III - Monoliteral substitution with standard cipher alphabets.

Weight:

60 1. a. Plain text:

HOSTILE ATTACK HAS BEEN STOPPED IN FRONT OF BATTALION RESERVE LINE IN RIGHT CENTER OF RESISTANCE OF THIRD INFANTRY STOP THIRD INFANTRY IS COUNTERATTACKING WITH REGIMENTAL RESERVE TO REESTABLISH FRONT LINE.

10 b. Reversed standard alphabet with $A_p = R_c$.

5 c. Any two of:-
(1) Frequency method.
(2) Completing the plain-component sequence method.
(3) Fitting the distribution to the normal.

10 2. a. (1) Convert the cipher letters into their plain-component equivalents.
(2) Complete the plain-component sequence.

5 b. Yes.

5 3. a. Try the mechanical method of solution by completing the plain-component sequence, using the normal alphabet, first direct, then reversed.

5 b. Mixed cipher alphabet.

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE - Military Cryptanalysis, Part I.

LESSON IV - Monoliteral substitution with mixed cipher alphabets.

Weight:

5 1. Because both components of the cipher alphabet are composed of known sequences. As a consequence it is sufficient to make but a single correct assumption. They can be solved by completing the plain component.

40 2. a. Triliteral frequency distribution:

A
P D T K T R F W U W F Q D P Q U I
G G C F R F Q F Q F F H P Q H C M

B
W
I

C
A C G I W H A C
C I I W R P C M

D
P G F G Q P Q Q H Q Q
W Q A G I W Q I A I I

E
I H I M
X O X W

F
I I H S I W A A I I A H I W A A H H H M
I P D K T K Q A P Q R Q I K A N W P Q -

G
A A D N W H K
D D M M C W W

H
M H K M Q X Q R M Q Q R N A Q J A Q J M
H J F S N N J E C S G F M F D P F J M F

I
- F T O I Q K M I C D N C B P T T O I P D I F P M D D M
F E O I F K W I F W T W C P T M O I F F I F E V J M A Q

J
H H Q Q H I
P P W H U H

Solutions
Military Cryptanalysis, Part I, 4-p '1
1936-37.

Weight:

K
I F F F
H I A G

L

M
Q G G I Q H C H S I A M W
H H I W H E I Q Q H M I F

N
H H F Q
G I H S

O
I E I
I W I

P
J F W I J C F W A H F
D A Q Q I D I Q I A Q

Q
X D P F A P W W F S Q F R A D W P R A P M M F I
M I H D X H J M H Q H W U D D A H J A H N D D W

R
A C F W W
A H H Q Q

S
H H N
F Q M

T
W F I I W
I A A I I

U
Q J
A A

V
I W
W

W
D I I I C M O J D G Q X G E F V Q
T P F G B C Q Q T A R F A Q P R M

X
E Q E
Q H W

Y

Z

Solutions
Military Cryptanalysis, Part I, 4-p 2
1936-37.

Weight:

Repetitions:

I F I E X Q M H H J P D W T I O I I F P A G D Q I

K H F D A G D G M H S F K I W P Q H N G M I I F T

A C C I W F K A F Q D I T A R A F A Q X H N I W G

C I C W B I P Q H J P I T I M W C R H E O W Q J W

Q M H C P D W T I O I I F P I F Q H S Q Q H G W A

F R H F Q W R Q U A Q D Q D I I F I E X W F K G W

A F A F N H M E W Q A H F W P Q H D A P I V W R Q

J H P A Q A H F P Q H J U A C C M I J H M Q N S M

Q D I M H F Q D I A M M I Q W W F

b. Trigraphs:- P Q H - 4
Q D I - 4
I I F - 4

Digraphs:-

I F - 6	D I - 4	A Q - 3			
Q H - 6	F Q - 4	F K - 3			
A F - 5	I I - 4	F P - 3			
H F - 5	M H - 4	H J - 3			
Q D - 5	P Q - 4	I W - 3			
		M I - 3			
		P I - 3			
		T I - 3			
		W Q - 3			

c. Plain text:

ENEMY TROOPS HAVE BEEN SIGHTED ON HIGH GROUND EAST OF GREEN-
VILLE AND IN THE VICINITY OF EAGLE LAKE STOP SEVERAL COMBAT
PATROLS HAVE BEEN SENT OUT TO GAIN CONTACT WITH THE ENEMY
AND GAIN INFORMATION AS TO HIS EXACT POSITION STOP WILL
REPORT FURTHER ON THEIR RETURN.

d. Cipher alphabet:

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

Keyword: WORKING DAY.

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE - Military Cryptanalysis, Part I.

LESSON V - Monoliteral substitution with mixed cipher alphabets.

Weight:

8 1. The beginning and the end of a message. Because although words may begin and end with almost any letter of the alphabet, they usually begin and end with but a few very common digraphs and trigraphs.

10 2. The "probable word method" of solution is one in which solution is obtained by the assumption of one or more words of plain text without the use of analysis.

7 3. a. This formula indicates a seven-letter word in which the first, fourth, and seventh letters are the same but different from the second, third, fifth and sixth; the second and third letters are the same but different from the first, fourth, fifth, sixth, and seventh; and the fifth and sixth are different from each other and all others.

5 b. (1) Any word that fits the formula such as: cemetery, vicinity, monopoly, division, civilian.

5 (2) Any word that fits the formula such as: affair, attack, effect.

5 (3) Any word that fits the formula such as: warfare, secrecy, whether.

60 4. Plain text:

HEAVY ENEMY BARRAGE ON FRONT OF SECOND INFANTRY.

Specific key: $A_p = Q_o$

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE - Military Cryptanalysis, Part I.

LESSON VI - Polyliteral substitution with mono-equivalent cipher alphabets.

Weight:

70 1. a. Diagram:

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

Plain text:

THE ENEMY COUNTERATTACK HAS BEEN DEFINITELY STOPPED EAST OF WHITE RUN STOP MY LINE NOW EXTENDS FROM ROAD JUNCTION TWO THREE EIGHT TO THE CROSS-ROAD EAST OF FAUPLAY.

b. Keywords: LUCKY; BREAK.

30 2. Biliteral cipher.
Plain text:
FOURTH DIVISION SAILED FROM NEW YORK MARCH FIFTEENTH

CARL

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE - Military Cryptanalysis Part I.

LESSON VII - Polyliteral substitution with poly-equivalent cipher alphabets.

Weight:

5 1. a. The purpose of providing variants in a cipher system is to disguise or suppress the manifestations of monoalphabeticity in a monoalphabetic substitution cipher.

5 b. In simple monoalphabetic substitution:

(1) The same letter of the plain text is invariably represented by but one and always the same character of the cryptogram, and

(2) The same character of the cryptogram invariably represents one and always the same letter of the plain text.

While in monoalphabetic substitution with variants:

(1) The same letter of the plain text may be represented by one or more different characters of the cryptogram, but

(2) The same character of the cryptogram nevertheless invariably represents one and always the same letter of the plain text.

85 2. a. Diagram:

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

Plain text:

PRISONERS TAKEN AT MILLER FARMHOUSE ARE FROM THE THIRD

BATTALION FIFTH INFANTRY. PRISONERS STATE THAT THE SECOND

BATTALION FIFTH INFANTRY IS IN POSITION ALONG RIDGE WEST

Weight:

OF CROSSROAD THREE ONE SEVEN. ABOUT ONE PLATOON COUNTER-

ATTACKED AGAINST THE LEFT FLANK OF THE SECOND INFANTRY.

THIS COUNTERATTACK WAS STOPPED BY OUR ADVANCE.

Note: The five letters A E I O U were inserted between sentences.

.5 b. The cryptographic text is more than twice as long as the plain text.

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE - Military Cryptanalysis, Part I.

LESSON VIII - Polygraphic substitution systems - 4 - square checkerboard designs.

Weight:

4 1. a. Polyliteral substitution is that type of substitution in which each single element (one letter) of the plain text is replaced by a group of two or more cipher elements.

Polygraphic substitution is that type of substitution in which plain-text units consisting of two or more elements (letters) forming an indivisible compound are replaced by cipher text units which usually consist of a corresponding number of elements.

4 b. Yes.

2 c. The suppression of the frequency characteristics of plain text.

90 2. Checkerboard design:

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

Plain text:

MESSAGES FROM THE FIRST BRIGADE SHOW THAT THE ENEMY HAS

ATTACKED IN FORCE ALONG THE PROSPERTOWN DASH SYKESVILLE

ROAD ON A FRONT OF ONE THOUSAND YARDS NORTH AND THREE

HUNDRED YARDS SOUTH OF THE ROAD STOP THEY HAVE ADVANCED

TO HOLD THE ROAD EAST OF HILL ONE THREE SEVEN STOP REG-
IMENTAL AND BRIGADE RESERVES HAVE ALL BEEN ENGAGED RESULT-
ING IN STOPPING THE ENEMY ADVANCE AT THIS POINT STOP
DIVISION RESERVES HAVE BEEN MOVED TO POSITION ALONG STREAM-
LINE JUST EAST OF HILL ONE NINE EIGHT.

Solutions
Military Cryptanalysis, Part I, 8-p 2.
1936-37.

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE - Military Cryptanalysis, Part I.

LESSON IX - Polygraphic substitution systems - Playfair cipher system.

Weight:

5 1. The Playfair cipher may be recognized by virtue of the fact that it always contains an even number of letters and that, when divided into groups of two letters each, no group contains a repetition of the same letter, as NN or EE.

95 2. Transposition rectangle:

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

Cipher square:

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

Plain text:

THIRTY PRISONERS INCLUDING THREE OFFICERS WERE CAPTURED AT HILL SEVEN ONE ZERO. PRISONERS ARE BEING FORWARDED TO DIVISION COMMAND POST. ENEMY HOLDS SPUR NINE HUNDRED YARDS NORTHWEST OF GREELY. HEAVY MACHINE GUN FIRE COMING FROM HILL THREE HUNDRED YARDS NORTH AND NORTHWEST OF TURNER IS DELAYING THE ADVANCE. REQUEST ARTILLERY SUPPORT AND REENFORCEMENTS FROM THE RESERVE.

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE - Military Cryptanalysis, Part I.

LESSON X - Miscellaneous monoalphabetic substitution systems.

Weight:

2 1. a. The 26 letters of the English alphabet.

2 b. Substitute letters for the sysbols consistently throughout the message.

4 c. Figures. Because (1) the use of numerical groups seems more natural or easier to the uninitiated than does the use of varying combinations of letters, and (2) it is easy to draw up cipher alphabets in which some of the letters are represented by single digits and others by pairs of digits thus complicating cryptanalysis.

2 2. To indicate by means of an outline the relationship existing among the various cryptographic systems.

90 3. Monoalphabetic substitution with three different mixed cipher alphabets.

Cipher alphabets:

Plain text:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher (1):	D	E	F	H	I	J	K	L	N	Q	S	U	V	W	X	Z	C	R	Y	P	T	O	G	A	M	B
" (2):	A	M	B	D	E	F	H	I	J	K	L	N	Q	S	U	V	W	X	Z	C	R	Y	P	T	O	G
" (3):	Y	P	T	O	G	A	M	B	D	E	F	H	I	J	K	L	N	Q	S	U	V	W	X	Z	C	R

Plain text:

MOVE DIVISION RESERVE AT ONCE UNDER COVER OF RIDGE EAST OF

JACOBSTOWN TO POSITION ALONG STREAMLINE JUST EAST OF HILL ONE

NINE THREE STOP ONE BATTALION FIRST ENGINEERS IS PLACED UNDER

YOUR COMMAND STOP YOU MAY ANTICIPATE EARLY COUNTERATTACK BY

DIVISION RESERVE FROM NEAR HILL ONE TWO ONE AGAINST ENEMY

SALIENT STOP INFORM COMMANDING GENERAL SECOND BRIGADE OF

YOUR MOVE.

Note: Underlined words were not enciphered. They indicate a change in alphabet.