

~~CONFIDENTIAL~~

CTC

record taken from  
WFF's home

~~CONFIDENTIAL~~

313

~~CONFIDENTIAL~~ 146451

ARMY EXTENSION COURSES

Subcourse--Military Cryptanalysis Part II  
Simpler Varieties of Polyalphabetic Substitution Systems.

Introduction.

Purpose and Scope:

The purpose of this subcourse is to teach the student the methods of analysis of the simpler polyalphabetic substitution systems.

The scope of this subcourse is: Primary classification of polyalphabetic systems; kinds of cipher alphabets; repeating key systems--factoring; mixed cipher alphabets; direct symmetry; high frequency generatrices; and indirect symmetry.

Number of Lessons and Approximate Time Required:

This subcourse consists of ten lessons and will probably require approximately 40 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 II--Simpler Varieties of Polyalphabetic Substitution Systems, 1937, 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. They will be returned to the student for file or further study.

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.

~~CONFIDENTIAL~~

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*  
Paul S. Willard  
Colonel, AGC  
Adjutant General

LESSON ASSIGNMENT SHEET

- SUBCOURSE -- Military Cryptanalysis, Part II
- LESSON I -- Repeating Key Systems, with standard and reversed standard alphabets.
- ESTIMATED TIME - 3 hours.
- TEXT ASSIGNMENT - Text, Sections I to IV, inclusive.
- MATERIALS REQUIRED - Cross-section paper of 1/4 inch squares.
- MAXIMUM WEIGHT - 100.
- SUGGESTIONS - None.

EXERCISE

Weight:

- 5 1. a. In a message of 180 letters, what is the approximate probability of two similar trigrams occurring by chance?
- 5 b. In a message of 1,200 letters, what is the approximate probability of two similar pentagrams occurring by chance?
- 40 2. Solve the following and recover the keyword:

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

Weight:

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

25            3.    Solve the following and recover the keyword:

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

Note: The enemy has been using reversed standard alphabets.

25            4.    Solve the following. It is suspected that the word PLEASANTON occurs in this message. Recover the keyword.

HEADQUARTERS THIRD ARMY  
 ACofS G-4  
 1500 Sept. 23, 1936.

To: CG Provisional Cavalry Corps

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

## ARMY EXTENSION COURSES

## LESSON ASSIGNMENT SHEET

SUBCOURSE - Military Cryptanalysis, Part II

LESSON II - Repeating-key systems with mixed cipher alphabets .

ESTIMATED TIME - 4 hours

TEXT ASSIGNMENT - Text, Section V.

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

MAXIMUM WEIGHT - 100

SUGGESTIONS - Prepare "box" comparable to Fig. 7, Page 26  
of text, and fill in each value as assumed.

## EXERCISE

Weight:

60 1. Solve the following and recover the keyword:

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

Weight:

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

20

2. The following is believed to be enciphered by the same components as those used in Problem 1 above. Solve and determine the keyword.

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

20

3. Solve the following. It is suspected that the word CROSSROADS occurs in this message and that the same cipher alphabet employed in Problem 1 above was used. Determine the keyword.

To 4th Corps, Dewees Ranch, Texas  
 From: G-3, 3rd Army

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

## ARMY EXTENSION COURSES

## LESSON ASSIGNMENT SHEET

SUBCOURSE - Military Cryptanalysis, Part II  
LESSON III - Repeating-key systems, mixed plain component.  
ESTIMATED TIME - 3 hours.  
TEXT ASSIGNMENT - Text, Section VI.  
MATERIALS REQUIRED - Cross-section paper of 1/4 inch squares.  
MAXIMUM WEIGHT - 100.  
SUGGESTIONS - None  
EXERCISE

Weight:

- 2 1. Direct symmetry can be used only when the plain component is known . (Line out incorrect one.)  
unknown
- 2 2. Which component must be known in order to make possible the matching of distributions of cipher alphabets?
- 6 3. If the first and fifth cipher alphabets show similar frequency distributions, what can be deduced as to the nature of the keyword:
- 90 4. Solve the following and recover the keyword:

TO: CG THIRD ARMY  
FROM: IV CORPS DEWEES RANCH, TEXAS

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



Weight:

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

## ARMY EXTENSION COURSES

## LESSON ASSIGNMENT SHEET

SUBCOURSE - Military Cryptanalysis, Part II;  
 LESSON IV - Indirect symmetry; secondary alphabets.  
 ESTIMATED TIME - 4 hours.  
 TEXT ASSIGNMENT - Text, Sections VII. and VIII.  
 MATERIALS REQUIRED - Cross-section paper of 1/4" squares:  
                           5 sheets 8" x 10 1/2"  
                           1 sheet 8" x 21 "  
                           1 frequency table form  
 MAXIMUM WEIGHT - 100  
 SUGGESTIONS - None

## EXERCISE

Weight:

1. What are the keys on which the following secondary alphabets are based:
  - 5     a. N G S U H T R I V Y K W B L X C M Z D O J E P A F Q
  - 5     b. O M D K U G N C J S Z R B I Q Y E A H P X V T F L W
  - 5     c. J R H U F P Z M B E X K T I V G O C Q D S Y L A N W
  - 5     d. Z Y A S D G K Q W C P N I E H M U X R T L B F J O V
- 5     2. Decimation of a primary alphabet at what 11 fundamental intervals only will give complete secondary alphabet chains?
- 30    3. Two messages, Message A and Message B, have been intercepted. It is suspected they contain the same plain text. The enemy has been using a mixed sequence slid against itself. Factoring indicates that message B is composed of 5 cipher alphabets. Pairs of values are obtained as follows:

Weight:

<u>Pairs from Alphabet 1</u>	<u>Pairs from Alphabet 2</u>	<u>Pairs from Alphabet 3</u>	<u>Pairs from Alphabet 4</u>	<u>Pairs from Alphabet 5</u>
AD	QE	AU	IO	SL
EV	TW	EG	AN	HM
IJ	AR	TA	TD	IP
VG	IX	HX	HT	FA
CR	WQ	IY	EL	MN
BQ	CH	WR	OE	RO
KZ	KO		XA	WJ
			WI	

Determine the primary alphabet and the keyword on which it is based.

- 10 4. From what decimation interval of the primary alphabet are the pairs of:

1st alphabet \_\_\_\_; 2d alphabet \_\_\_\_; 3d alphabet \_\_\_\_;  
4th alphabet \_\_\_\_; 5th alphabet \_\_\_\_.

- 5 5. Make up two strips as indicated in sketch and lay them aside for later use. The sequences on both strips will be the mixed sequence you recovered from the pairs given in Question 3 above.

Plain: θ ϕ p r . . etc. . . . .

mixed sequence <sup>↑</sup> 26 letters long

Cipher: θ ϕ p r . . etc. . . . . θ ϕ p r . . etc. . . .

same mixed <sup>↑</sup> sequence repeated - 52 letters long

- 10 6. Part of message B follows. Make up frequency table for each alphabet.

MESSAGE "B".

```

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

Weight:

Consider the frequency table for the second alphabet. Cipher letters A, N, W, X, and Y are high, with A highest. In general, these letters should represent most of the letters E, T, O, A, I, N, .. etc., that is, the high-frequency letters.

Now take the sliding strips prepared in Question 3. Put the A on the cipher (long) strip under the E on the plain (short) strip, and note what plain-text values of N, W, X, and Y are concomitant with  $A_c = E_p$ . Place the  $A_c$  on the cipher strip under T, O, A, etc., (on the plain strip) in turn, noting what plain-text values of the other cipher letters correspond to each setting. When the correct juxtaposition is made, the values of all the cipher letters in alphabet 2 become known, and the frequencies of the plain-text letters will be according to their normal frequencies.

Enter the correct values for the cipher letters of alphabet 2 in their proper places in the message. (NOTE: It is often of considerable assistance to enter the plain-text letters in red, green, or some other bright color.)

Decipher what is given of message "B".

- 5 7. Make up a "box" in the following form:

Plain	(Mixed sequence derived in Question 3)
Cipher 1	(Same sequence with starting point determined from text)
Cipher 2	( " " " " " " " " )
Cipher 3	( " " " " " " " " )
Cipher 4	( " " " " " " " " )
Cipher 5	( " " " " " " " " )

What is the keyword?

- 15 8. From the "box" in Question 7 and the list of pairs given in Question 3, what can you say Message "A" was?  
Note: This is an important point - note the weight of this question.

## ARMY EXTENSION COURSES

## LESSON ASSIGNMENT SHEET

SUBCOURSE - Military Cryptanalysis, Part II

LESSON V - Mixed components; indirect symmetry.

ESTIMATED TIME - 4 hours

TEXT ASSIGNMENT - Text, to include Section VIII.

MATERIALS REQUIRED - Cross-section paper, frequency table form, and trigraphic frequency table forms.

MAXIMUM WEIGHT - 100

SUGGESTIONS - None.

## EXERCISE

Weight:

- 95 1. Solve the message on the next page and reconstruct the alphabets. Determine the keyword for the cipher alphabet.

NOTE: As soon as you have determined the number of alphabets, make frequency tables for each alphabet and then lay out the "box" for the alphabets. (See Fig. 35, Page 86) Whenever you make an assumption of a plain-text value for a cipher letter, be sure to finish four things before you make any further guesses: (1) Enter the clear value below all occurrences of the cipher letter; (2) enter the value in the "box"; (3) see if any inconsistencies are produced (a) in the clear text or (b) in the "box"; and (4) see if you can get any new values from proportions in the "box".

Proceeding in the above orderly manner will save you much time in the end.

- 3 2. If two of the cipher-alphabet frequency distributions match, what is indicated concerning the keyword?
- 1 3. What is the keyword in the message given?
- 1 4. Does the keyword necessarily have to be under the letter "A" in the "box"?

## LESSON FIVE MESSAGE

XJITZ FVYV MNNTL CJIDT FNHTL XVWZT  
 HJOKH BZEYE VPNHZ NMAEA RWHXA BFWKK  
 VGAKH BSWMR DLGNC UAJEF QNSQC IVLJK  
 XZKNX CPXZX KLJLH RYQKE MBDXK HNFJE  
 AZUKH BSCZL BPNXD BAXMR BBHQC PPPCF  
 EJLGT GRXPE SBOLH HNVMO URGAV BFSPS  
 NWUZZ COLZP KJHPL JRKET HXTHR JWFDK  
 IITKH BSIZJ ANHAW NPJTE ABDXX JYFZO  
 ANKKK PAHYT TNNAL NVLPK CJDLH HNVMO  
 UCBKH BZHIZ DBDKH BSYES NBDXF PYZHT  
 TBLHC CWLRZ BNHXB BAHIZ BQGYW JWHCS  
 LIBXC PWLRZ BRHWH KYIEO MWBMS EVQML  
 ENUAW XWLRZ BCBTZ XYZWT FBPZL CYXVP  
 KBDXW XNJMJ KSTYW JWHIN RBDXH RYIZO  
 KNCHD PAIZN ALURL QKWMS MJCQA UYHTS  
 NNCDR XYAZE TRGMH RAHMR DTLKU BOAVW  
 YGLKO BARIL DQGR L YAHWK XJIAW WKBMT  
 BIGBW XVMMJ DMDAW QGIGW DUPXL XVMZE  
 YGBMU XYKEM KNHXW XYFCF NULPL CYBMJ  
 YGNXL YKCTS ALBNC NMCUE RJUQM YKCTS  
 VJSXC

## LESSON FIVE MESSAGE

XJITZ FVYV MNNTL CJIDT FNHTL XVWZT  
 HJOKH BZEYE VPNHZ NMAEA RWHXA BFWKK  
 VGAKH BSWMR DLCNC UAJEF QNSQC IVLJK  
 XZKNX CPXZX KLJLH RYQKE MBDXK HNFJE  
 AZUKH BSCZL BPNXD BAXMR BBHQC PPPCF  
 EJLGT GRXPE SBOLH HNVMO URGAV BFSPS  
 NWUZZ COLZP KJHPL JRKET HXTHR JWIDK  
 IITKH BSIZJ ANHAW NPJTE ABDXX JYFZO  
 ANKKK PAHYT TNNAL NVLPK CJOLH HNVMO  
 UCRKH BZHIZ DBDKH BSYES NBDXF PYZHT  
 TBLHC CWLRZ BNHXB BAHIZ BQGYW JWHCS  
 LIBXC PWLRZ BRHWH KYIEO MWBMS EVQML  
 ENUAW XWLRZ BCBTZ XYZWT FBPZL CYXVP  
 KBDXW XNJMJ KSTYW JWHIN RBDXH RYIZO  
 KNCHD PAIZN ALURE QKWMS MJCQA UYHTS  
 NNCDR XYAZE TRGMH RAHMR DTLKU BOAVW  
 YGLKO BARIL DQGR L YAHWK XJIAW WKBMT  
 BIGBW XVMMJ DMDAW QGIGW DUPXL XVWZE  
 YGBMU XYKEM KNHXW XYFCF NULPL CYBMJ  
 YGNXL YKCTS ALBNC NMCUE RJUQM YKCTS  
 VJSXC

## LESSON FIVE MESSAGE

XJITZ FPVYV MNNTL CJIDT FNHTL XVWZT  
 HJOKH BZEYE VPNHZ NMAEA RWHXA BFWKK  
 VGAKH BSWMR DLCNC UAJEF QNSQC IVLJK  
 XZKNX CPXZX KLJLH RYQKE MBDXK HNFJE  
 AZUKH BSCZL RPNXD BAXMR BBHQC PPPCF  
 EJLGT GRXPE SBOLH HNVMO URGAV BFFPS  
 NWUZZ COLZP KJHPL JRKET HXTHR JWIDK  
 IITKH BSIZJ ANHAW NPJTE ABDXX JYFZO  
 ANKKK PAHYT TNNAL NVLPK CJOLH HNVMO  
 UCBKH BZHIZ DBDKH BSYES NBDXF PYZHT  
 TBLHC CWLRZ BNHXB BAHIZ BQGYW JWHCS  
 LIBXC PWLRZ BRHWH RYIEO MWBMS EVQML  
 ENUAW XWLRZ BCBTZ XYZWT FBPZL CYXVP  
 KBDXW XNJMJ KSTYW JWHIN RBDXH RYIZO  
 KNCHD PAIZN ALURL QKWMS MJCQA UYHTS  
 NNCDR XYAZE TRGMH RAHMR DTLKU BOAVW  
 YGLKU BARIL DQGR L YAHWK XJIAW WKBMT  
 BIGBW XVMMJ DMDAW QGIGW DUPXL XVMZE  
 YGBMU XYKEM KNHXW XYFCF NULPL CYBMJ  
 YGNXL YKCTS ALBNC NMCUE RJJQM YKCTS  
 VJSXC



## ARMY EXTENSION COURSES

## LESSON ASSIGNMENT SHEET

SUBCOURSE - Military Cryptanalysis, Part II.  
 LESSON VI - Indirect Symmetry.  
 ESTIMATED TIME - 5 hours.  
 TEXT ASSIGNMENT - Text, Sections IX and X to include Par. 44.  
 MATERIALS REQUIRED - Cross-section paper; frequency table forms.  
 MAXIMUM WEIGHT - 100  
 SUGGESTIONS - Use the message sheets provided.

## EXERCISE

Weight:

- 60 1. The following two messages have been intercepted. Solve them, reconstruct the alphabets and keywords employed.

## Message A

DNC to DBA 2:15 pm.

MUOUV	DSWKN	ICHGL	BJSIM	XOPJC	IWNUR
MTOGG	SDNOO	IAHTP	ZKXKE	ONNVM	GQOKJ
QCKAE	YQSSO	MOCBM	HKJQC	THSJJ	OYWUY
HOJKN	EJZJM	LCZEO	NNERJ	OOMVI	OHMQH
MCKGU	JRICW	NKOMY	MMQHI	YYUUF	ICMKX
KEONN	GZMJK	NHYOH	MRUFO	PNRFT	MIMMJ
DNORQ	XJMXR	QXAFM	VECHT		

## Message B.

DNC to DBB 2:30 pm.

UQOCL	OHTBP	UAZFF	FHDDJ	KTOXF	UCPQJ
UPQJF	DWMQT	UMZPU	UCKGV	QPHGU	FVTCX
AIBDV	SAZDT	JQFAY	MCXAI	IMKXQ	NSYQS
ZNXLM	HQYXO	SARVQ	PMHOH	QTJGD	NWUZW
UIBJQ	XOUAY	MBCJS	OJVZU	SQOEX	UAUCK
GVQPM	TRJXL	MWENW	OEEHN	UPEPS	JRUJX
WMQBZ	KQJKB	ZKPDY	RVAZP		

Weight:

40

2. Solve the following message and determine the keyword.

## Message C

DNC to DBC 4:00 pm.

WFKQF QRXLQ TFCCX GWELC PSAKW  
 FAQRU TFFAK ICCKG OCDKR EDJOQ  
 PCWFK QFEXC

## Worksheet for Problem 1

MUOUV DSWKN ICHGL BJSIM XOPJC IWNUR  
 UQQCL OHTBP UAZFF FHDDJ KTOXF UCPQJ

MTOGG SDN00 IAHTP ZKXKE ONNVM GQOKJ  
 UPQJF DWMOT UMZPU UCKGV QPMGU FVTCX

QCKAE YQ0S0 MOCBM HKJQC THSJJ OYWUY  
 AIBDV SAZDT JQFAY MCXAI IMKXQ NSYQS

HOJKN EJZJM LCZEO NNERJ QOMVI OHMQH  
 ZNXLM HQYXO SARVQ PMHOH QTJGD NWUZW

MCKGU JRICW NKOMY MM0HI YYUUF ICMKX  
 UIBJQ XOUAY MBCJS OJVZU SQ0EX UA0CK

KE0NN GZMJK NHYOH MRUFO PNRFT MIMMJ  
 GVQPM TRJXL MWENW OEEXN UPEPS JROJX

DNORQ XJM XR QXAFM VECHT  
 WMQBZ KQJKB ZKPDY RVAZP

## Worksheet for Problem 1

## Message A

MUOUV	DSWKN	ICHGL	BJSIM	XOPJC	IWNUR
MTGG	SDNOO	IAHTP	ZKXKE	ONNVM	GQOKJ
QCKAE	YQQSO	MOCBM	HKJQC	THSJJ	OYWUY
HOUKN	EJZJM	LCZEO	NNERJ	OOMVI	OHMQH
MCKGU	JRICW	NKOMY	MMQHI	YYUUF	ICMKX
KEONN	GZMJK	NHYOH	MRUFO	PNRFT	MIMMJ
DNORO	XJMXR	QXAFM	VECHT		

## Message B

UQQCL	OHTBP	UAZFF	FHDDJ	KTOXF	UCPQJ
UPQJF	DWMQT	UMZPU	UCKGV	QPMGU	FVTCX
AIBDV	SAZDT	JWFAY	MCXAI	IMKXQ	NSYQS
ZNXLM	HQYXO	SARVQ	PMHOH	QTJGD	NWUZW
UIBJQ	XOUAY	MBCJS	OJVZU	SQQEX	UAOCK
GVQPM	TRJXL	MWENW	QEEYN	UPEPS	JRUJX
WMQBZ	KQJKB	ZKPDY	RVAZP		

## ARMY EXTENSION COURSES

## LESSON ASSIGNMENT SHEET

SUBCOURSE - Military Cryptanalysis, Part II

LESSON VII - Indirect symmetry.

ESTIMATED TIME - 4 hours

TEXT ASSIGNMENT - Text, Section X.

MATERIALS REQUIRED - Cross-section paper; frequency table forms.

MAXIMUM WEIGHT - 100

SUGGESTIONS - Study Par. 45, text.

## EXERCISE

Weight

- 100 1. Solve the following two messages, and determine the alphabets used and the keywords.

## Message A

BZA to BZC 9:55 am.

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

## Message B

BZA to BZD 10:00 am.

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

LESSON ASSIGNMENT SHEET

SUBCOURSE - Military Cryptanalysis, Part II  
LESSON VIII - Indirect symmetry.  
ESTIMATED TIME - 4 hours.  
TEXT ASSIGNMENT - All of text.  
MATERIALS REQUIRED - Cross-section paper, frequency table forms.  
MAXIMUM WEIGHT - 100.  
SUGGESTIONS - Study remarks on solution of Problem 1 of Lesson VII.  
EXERCISE

Weight:

100

1. Solve the following messages, reconstruct the alphabets, and determine the keywords:

Message No. 1

JXA to JXB 4:55 am

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

Message No. 2

JXA to JXC 5:00 am

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

## ARMY EXTENSION COURSES

## LESSON ASSIGNMENT SHEET

- SUBCOURSE - Military Cryptanalysis, Part II.
- LESSON IX - Indirect Symmetry.
- ESTIMATED TIME - 5 hours.
- TEXT ASSIGNMENT - All of text.
- MATERIALS REQUIRED - Cross section paper, frequency table forms.
- MAXIMUM WEIGHT - 100.
- SUGGESTIONS - Note that you can only take "proportions" from outside the "box" to the inside when you know the plain component sequence. Until you know this, you can only work within the "box".

## EXERCISE

Weight

100

1. Solve the message given on page two of this lesson, determine the alphabets employed, the keys upon which they are based, and the key-word within the "box". As the message readily factors to indicate seven alphabets, it is given already laid out in that manner to save copying.

## Problem for Lesson IX.

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

## ARMY EXTENSION COURSES

## LESSON ASSIGNMENT SHEET.

- SUBCOURSE - Military Cryptanalysis, Part II.
- LESSON X - Indirect Symmetry.
- ESTIMATED TIME - 5 hours.
- TEXT ASSIGNMENT - All of text.
- MATERIALS REQUIRED- Cross section paper; frequency table forms.
- MAXIMUM WEIGHT - 100.
- SUGGESTIONS - Note that when you get a complete secondary alphabet, some decimation of it will give the primary alphabet. This primary alphabet may be standard, mixed in any number of ways, or it may be random. For this problem, see Par. 46, Section IX, TEXT No. 165. See also Par. 33, d and e, Military Cryptanalysis, Part I.

## EXERCISE

Weight

100

1. The message given on page two of this lesson contains a repeat in the plain text eighty nine letters long.

Solve the message, reconstruct the plain and cipher alphabets, and determine the key-words used.



LIUDB USNYE BIDDK BZULA XMQZP  
QKUCW SLCWL SLVUX IMM L P ANULP  
ANUWY INCZO LQRDG YSHBS YNZPC  
SSPYY STWHO GBGMW IBRID SLWHA  
TUPHK JODPW BKGZK JODPK YLARN  
IBCUC AUWCY IYDLG IQNEE JTRPA  
TUPIA TDNJK BRDDQ DBDDQ DBPKK  
DUUAY ELHPF JMICF DJKWA JTSKA  
XEWAN YNELK YLXXA TEWUO LTWHW  
CSKLP ANUHW CSKSH

## ARMY EXTENSION COURSES

## SOLUTIONS

- SUBCOURSE - Military Cryptanalysis, Part II
- LESSON 1 - Repeating Key Systems, with standard and reversed standard alphabets.

Weight:

- 5 1. a. Approximately 1/100
- 5 b. Approximately 1/10,000
- 40 2. Polyalphabetic substitution with five normal alphabets.

Keyword: SOUND

Plain text:

COMMANDING OFFICER FIRST FIELD ARTILLERY STOP

YOU WILL MOVE TO POSITIONS ON SOUTH MOUNTAIN TOMORROW  
 COMMA COMPLETING MOVE BY TEN PM STOP RED FORCES ESTIMATED  
 AT A REINFORCED DIVISION ARE MOVING ON GETTYSBURG DASH  
 HANOVER ROAD STOP THIS DIVISION WILL CONTINUE TO GUARD  
 THE RIGHT FLANK OF OUR CORPS STOP AMMUNITION WILL CON-  
 TINUE TO BE FURNISHED IN ANY AMOUNTS DESIRED BOTH FOR  
 SEVENTY FIVES AND FOR LARGER GUNS STOP GASOLINE FOR  
 TRACTORS WILL BE OBTAINABLE AT FOUR CORNERS AT ANY TIME  
 AFTER EIGHT A(X)M TOMORROW STOP

CG SECOND DIVISION

- 25 3. Polyalphabetic substitution with six reversed standard alphabets.

Keyword: ORANGE

Plain text:

THIRD ARMY DEFENDING POSITION GENERALLY SOUTH AND EAST  
 OF TORDILLAS HILL STOP THE EIGHTH CORPS WILL EXTEND  
 POSITION TO THE RIGHT.

Weight:

- 25      4. Polyalphabetic substitution with seven normal standard alphabets.

Keyword: MACHINE

Plain text:

HEADQUARTERS THIRD ARMY  
ACofS G-4  
1500 Sept. 23, 1936

To: CG PROVISIONAL CAVALRY CORPS

YOUR RAILHEAD AT PLEASANTON WILL BE OPERATED  
BY RAILHEAD COMPANY NOW ESTABLISHED THERE.

## ARMY EXTENSION COURSES

## SOLUTIONS

SUBCOURSE

- Military Cryptanalysis, Part II

LESSON 2

- Repeating-key systems with mixed cipher alphabets.

Weight:

- 60 1. Polyalphabetic substitution with four mixed cipher alphabets, based on the word BALTIMORE.  
Cipher alphabets:

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

Keyword: CITY

Plain text:

CORPS SUMMARY OF OPERATIONS G DASH THREE PROVISIONAL  
CAV CORPS AT ZERO FIVE ZERO ZERO CAV CORPS HELD GENERAL  
LINE CHRISTINE DASH COMPELLTON WITH DIVISIONS ABREAST  
AND WITH CORPS RESERVE OF TWO CAV BRIGS AND ONE MECHANIZED  
REGIMENT PERIOD DURING FORENOON LEFT DIVISION FORCED BACK  
BY STRONG BLACK INFANTRY ATTACK ESTIMATED TWO DIVISIONS  
RIGHT DIVISION IN CONTACT WITH COVERING FORCES ONLY PERIOD  
EARLY IN AFTERNOON STRONG CAVALRY ATTACK ESTIMATED THREE  
REGIMENTS ON FRONT TWENTYTHIRD CAV DIVISION RESULTED IN  
FORCING BACK THAT UNIT PERIOD AT NINETEEN HOUR CAVALRY CORPS  
HELD GENERAL LINE SOUTH OF RIGHTER RANCH TO DAVENPORT  
HOSTILE ATTACK APPARENTLY STOPPED NEAR

## ARMY EXTENSION COURSES

## SOLUTIONS

SUBCOURSE - Military Cryptanalysis, Part II  
 LESSON 2 -Repeating-key systems with mixed cipher alphabets.

Weight:

- 60 1. Polyalphabetic substitution with four mixed cipher alphabets,  
 based on the word BALTIMORE.  
 Cipher alphabets:

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

Keyword: CITY

Plain text:

CORPS SUMMARY OF OPERATIONS G DASH THREE PROVISIONAL  
 CAV CORPS AT ZERO FIVE ZERO ZERO CAV CORPS HELD GENERAL  
 LINE CHRISTINE DASH COMPBELLTON WITH DIVISIONS ABREAST  
 AND WITH CORPS RESERVE OF TWO CAV BRIGS AND ONE MECHANIZED  
 REGIMENT PERIOD DURING FORENOON LEFT DIVISION FORCED BACK  
 BY STRONG BLACK INFANTRY ATTACK ESTIMATED TWO DIVISIONS  
 RIGHT DIVISION IN CONTACT WITH COVERING FORCES ONLY PERIOD  
 EARLY IN AFTERNOON STRONG CAVALRY ATTACK ESTIMATED THREE  
 REGIMENTS ON FRONT TWENTYTHIRD CAV DIVISION RESULTED IN  
 FORCING BACK THAT UNIT PERIOD AT NINETEEN HOUR CAVALRY CORPS  
 HELD GENERAL LINE SOUTH OF RIGHTER RANCH TO DAVENPORT  
 HOSTILE ATTACK APPARENTLY STOPPED LEAR

## ARMY EXTENSION COURSES

## SOLUTIONS

SUBCOURSE

- Military Cryptanalysis, Part II

LESSON 3

- Repeating-key systems, mixed plain component.

Weight:

- 2 1. Direct symmetry can be used only when the plain component is known.
- 2 2. The cipher component.
- 6 3. The first and fifth letters of the keyword are the same letter.
- 90 4. Polyalphabetic substitution with mixed plain component based on the word COPYRIGHTED, using seven cipher alphabets of plain normal sequence.

Cipher alphabets:

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

Keyword: KEYWORD

Plain text:

TO: CG THIRD ARMY  
FROM: IV CORPS DEWEES RANCH, TEXAS.

TO COMMANDING GENERAL THIRD ARMY STOP DURING NIGHT TROOPS  
WERE REORGANIZED TO ATTACK AT ZERO FIVE ONE ZERO STOP AT  
TWO TWO FIVE ZERO BOTH DIVISIONS REPORTED PART OF THEIR  
LINES WERE FORCED TO FALL BACK DUE TO CONCENTRATIONS OF  
MUSTARD GAS IN THEIR SECTORS LATER IT WAS DISCOVERED THE  
GAS USED WAS TEAR AND LINES WERE REORGANIZED STOP ATTACK

Solutions

Military Cryptanalysis, Part II, 3-p 1  
1937.

Weight:

LAUNCHED AT ZERO FIVE ZERO ZERO AND MET WITH LITTLE  
RESISTANCE INITIALLY STOP RESISTANCE STIFFENED IN FRONT  
OF FOURTH DIVISION AS TORDILLA HILL WAS APPROACHED COMMA  
BUT THIS POSITION WAS TAKEN BY ONE FIVE ZERO ZERO STOP  
AT ONE ONE ONE FIVE THE FOURTH AND ONE HUNDRED SIXTH TANK  
COMPANIES WERE DETACHED FROM THE FOURTH CORPS BY ARMY  
ORDER AND REPORTED TO THE EIGHTH CORPS STOP AS THE ATTACK  
APPROACHED THE BLACK DEFENSIVE POSITION COMMA IT WAS SLOWED  
UP BY ARTILLERY FIRE AND LITTLE PROGRESS WAS MADE AFTER  
ONE SEVEN ZERO ZERO END OF MESSAGE BLAKE LOCK ASST G DASH  
THREE

## ARMY EXTENSION COURSES

## SOLUTIONS

SUBCOURSE - Military Cryptanalysis, Part II

LESSON IV - Indirect Symmetry; secondary alphabets.

Weight:

- 5 1. a JANUARY
- 5 b GOVERNMENT
- 5 c CHINESE PORT
- 5 d CRYPTANALYSIS
- 5 2. 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25.
- 30 3. W A S H I N G T O B C D E F J K L M P Q R U V W X Y Z
- 10 4. 1st 10 or -16 ; 2d 19 or -7; 3d 20 or -6 ;  
4th 4 or -22 ; 5th 14 or -12.
- 5 5. Plain : WASHINGTONBCDEFJKLMPQRUVXYZ  
Cipher: WASHINGTONBCDEFJKLMPQRUVXYZWASHINGTONBCDEFJKLMPQRUVXYZ
- 10 6. Plain text:  
WE ARE EXPECTING A MOVE TO BORTON SCHOOLHOUSE TONIGHT  
SOON AFTER ONE AM TO DEFEND THE LINES EAST OF BORTON  
SCHOOLHOUSE BE PREPARED AT THAT TIME TO MOVE OUT PROMPTLY  
STOP OUR ADV. . . etc.
- 5 7. Plain W A S H I N G T O B C D E F J K L M P Q R U V X Y Z  
Cipher 1 C D E F J K L M P Q R U V X Y Z W A S H I N G T O B  
Cipher 2 Q R U V X Y Z W A S H I N G T O B C D E F J K L M P  
Cipher 3 R U V X Y Z W A S H I N G T O B C D E F J K L M P Q  
Cipher 4 I N G T O B C D E F J K L M P Q R U V X Y Z W A S H  
Cipher 5 J K L M P Q R U V X Y Z W A S H I N G T O B C D E F  
Keyword: DRUNK
- 15 8. It was plain text.

Solutions

Military Cryptanalysis, Part II, 4-p 1  
1937.



## ARMY EXTENSION COURSES

## SOLUTIONS

SUBCOURSE - Military Cryptanalysis, Part II,  
 LESSON V - Mixed components; indirect symmetry.

Weight:

95

## 1. Plain text:

RED CAVALRY FORCES HAVE CONCENTRATED EAST OF CROSS  
 ROADS SIX NINE FOUR DASH B STOP RED INFANTRY IS MOVING  
 TOWARD PASS AT THE NORTH END OF THE WILDWOODS STOP IT  
 WAS REPORTED AT NINE AM AS BEING WITHOUT ARTILLERY  
 ALTHOUGH THIS HAS NOT BEEN VERIFIED BY OUR CAVALRY  
 STOP AT NOON TODAY NO OTHER RED TROOPS WERE REPORTED  
 TO HAVE ARTILLERY WEST OF E SMITH STOP WITH THESE  
 EXCEPTIONS COMMA ONE MORE SMALL FORCE AT GREENE COMMA  
 AND THE AIR FIELD AT NEW BOSTON COMMA WE CAN EXPECT  
 THESE TO BE THE ONLY ENEMY FORCES IN THE THEATRE OF  
 OPERATIONS BEFORE THE FIFTEENTH OF JUNE STOP ALL THREE  
 DIVISIONS OF THIS CORPS WILL BE PREPARED TO MOVE EARLY  
 ON THE NIGHT OF MAY FIFTEENTH TO THE LINE FIVE ONE  
 ONE DASH FIVE SEVEN THREE POINT ONE AND SIX ONE SIX  
 POINT SEVEN.

Plain and cipher alphabets: JUGOSLAVIBCDEFHMKMNPQRTWXYZ,  
 based on keyword: JUGOSLAVIA

Weight:

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

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

Solution by guessing from study of repeats and frequencies  
 the following:

Line 3 KHBS . . . . . STOP  
 Line 4 HRY . . . . . THE  
 Line 4 BDX . . . . . THE  
 Line 6 CLHHNVMOU . . . . ARTILLERY  
 Line 11 WRLZB . . . . . COMMA  
 Line 20 YKCTS . . . . . POINT

With those words as a start, the whole last line can be filled in and the words EAST OF in Line 2 and WEST OF in Line 10 can be guessed.

These values are sufficient to complete the chain of a secondary alphabet, which can be decimated to give the primary alphabet.

- 3        2. That the two corresponding letters of the keyword are the same.
- 1        3. BRONZE PICK
- 1        4. No, it may be under any letter.

## ARMY EXTENSION COURSES

## SOLUTIONS

SUBCOURSE - Military Cryptanalysis, Part II,  
 LESSON VI - Indirect symmetry.

Weight:

60. 1. Message A and Message B have the same plain text:  
 AN ENEMY FORCE ESTIMATED AT TWO BRIGADES HAS REACHED  
 RJ SIX ZERO DASH A STOP OUR COMPANY WILL STOP ALL  
 TRAFFIC EAST OF RJ SEVEN ZERO FIVE AND TAKE UP A  
 POSITION FOR DEFENSE OF HILL ONE SIX ZERO ONE STOP  
 MAKE ALL ARRANGEMENTS REQUIRED QUICKLY REED

Plain and cipher alphabets are the same, based upon the key-  
 word QUICKSILVER:

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

## "Box" for Message A

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

Keyword: MOTORS under plain letter A.

## "Box" for Message B

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

Keyword: UNITED under plain letter A.

Weight:

40

2. Message C best solved by factoring to get four alphabets, and then completing the plain (mixed) component and picking the high-frequency generatrices.

"Box" for Message C

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

Keyword: BEDS under plain letter A.

## Plain text:

THIS DIVISION IS TO TAKE OVER THE SECOND DIVISIONS AREA  
AT NINE THIS DATE.

## ARMY EXTENSION COURSES

## SOLUTIONS

SUBCOURSE - Military Cryptanalysis, Part II  
 LESSON VII - Indirect symmetry.

Weight:

100

- Both messages have the same plain text:

OUR ADVANCE HAS BEEN STOPPED AT RJ SIX ZERO

FIVE YOUR REGIMENT WILL CONTINUE ATTACK ADVISE.

The plain component and the cipher components are the same sequence, based upon the keyword SATURDAY:

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

## "Box" for Message A

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

Keyword: CURT under plain letter Z.

## "Box" for Message B

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

Keyword: CANTON under plain letter E.



## ARMY EXTENSION COURSES

## SOLUTIONS

SUBCOURSE Military Cryptanalysis, Part II

LESSON VIII Indirect symmetry.

Weight:

100 1. Both messages have the same plain text:

ENEMY ARTILLERY FIRE IS INTERDICTING CROSSROADS ONE  
SEVEN EIGHT DASH I ALSO ONE EIGHT SEVEN ONE.

The plain and cipher alphabets are the same, based  
on the words: KEYWORD MIXED.

KEYWORD MIX ABCFGHJLN PQSTUVZ

"Box" for Message No. 1

Plain	KEYWORD MIX ABCFGHJLN PQSTUVZ
Cipher 1	CFGHJLN PQSTUVZKEYWORD MIX AB
Cipher 2	RD MIX ABCFGHJLN PQSTUVZKEYWO
Cipher 3	VZKEYWORD MIX ABCFGHJLN PQSTU
Cipher 4	STUVZKEYWORD MIX ABCFGHJLN PQ
Cipher 5	TUVZKEYWORD MIX ABCFGHJLN PQS

Keyword: THIRD under plain letter A.

"Box" for Message No. 2

Plain	KEYWORD MIX ABCFGHJLN PQSTUVZ
Cipher 1	TUVZKEYWORD MIX ABCFGHJLN PQS
Cipher 2	LN PQSTUVZKEYWORD MIX ABCFGHJ
Cipher 3	X ABCFGHJLN PQSTUVZKEYWORD MI
Cipher 4	MIX ABCFGHJLN PQSTUVZKEYWORD
Cipher 5	QSTUVZKEYWORD MIX ABCFGHJLN P
Cipher 6	NPQSTUVZKEYWORD MIX ABCFGHJL

Keyword: DEPLOY under plain letter A.

The number of alphabets in each message can be determined  
in several ways, the easiest of which is:

Weight:

Since the twenty-fifth and fifty-fifth letters of both messages are the same letter (E and N, resp.), an interval of thirty, this number must be a common multiple of the number of letters in each keyword and one of the alphabets in one message must be the same as some one of the alphabets in the other. Keywords of 5 and 6 letters are thus practically determined. In Message No. 2, at the end there is a trigraph, VAU, repeated at an interval of 12. This fixes the keyword length of Message No. 2 at 6 and that of Message No. 1 at 5.

The messages can now be laid off into alphabets. It is best to set down the numbers of the alphabets of each pair of letters:

1234512345123451234512345123451234512345123451234512345123451234512345123451234  
FUZYVTAQWFWDWUXQAZWLQJQTENFALOOPAINMKWZDNKIFUMDTTGFP CANNHPACTTPZKODDXBIKZPUOXJT  
UXAGTYEFLVBPEPTHZPOCLZJPEULPJKGRSOVFLTFLKPKXAYSJUXAHIMNUPYKXKDIORVAUZUTJFUHAZVAC  
1234561234561234561234561234561234561234561234561234561234561234561234561234561234561

If the messages have the same plain text, the following pairs of values can be obtained:

<u>1-1</u>	<u>2-2</u>	<u>3-3</u>	<u>4-4</u>	<u>5-5</u>	<u>1-6</u>	<u>2-1</u>	<u>3-2</u>	<u>4-3</u>	<u>5-4</u>	<u>1-5</u>	<u>2-6</u>	<u>3-1</u>	<u>4-2</u>	<u>5-3</u>
FU	UX	ZA	YG	VT	TY	AE	QF	WL	FV	WB	DF	WE	UP	XT
OG	PR	AS	KC	KV	MF	KL	WT	ZF	DL	NK	KF	YK	FX	UA
TD	TI	PO	ZB	KV	OA	DU	DZ	XU	BT	IJ	KF	ZU	PH	UA
(HZ)2-4														
<u>1-4</u>	<u>2-5</u>	<u>3-6</u>	<u>4-1</u>	<u>5-2</u>	<u>1-3</u>	<u>2-4</u>	<u>3-5</u>	<u>4-6</u>	<u>5-1</u>	<u>1-2</u>	<u>2-3</u>	<u>3-4</u>	<u>4-5</u>	<u>5-6</u>
QH	AZ	ZP	WO	LC	QL	UZ	QJ	TP	EE	NU	FL	AP	LJ	OK
MY	DS	TJ	TU	GX	FA	FH	CI	AM	NN	NU	HP	PY	AX	OK
OZ	XV	JA	TU											

In 3-3 we have Z A S.  
From 2-5, Z S :: A D, which gives Z A S D.  
From 3-2, where D Z occurs, we get T . . W and F . . Q  
  
From 1-3, F Q :: A L, which gives Z A S D L  
From 4-5, A L :: X J, which gives X . . J  
From 2-4, F U :: H Z, which permits addition of H Z to 1-1.  
Then from 1-1, Z D :: H T, giving H . . T . . W  
From 5-4, D L :: F V :: B T, which gives F V . Q and permits H . B T . . W  
From 1-5, B W :: K N :: J I, giving K . . . N and X . . J . . I  
From 3-5, J I :: Q C, which gives Q . . . C



From 2-2, X I :: U T, giving U . . . . T since we  
 had X . . J . . . I  
 From 2-5, S D :: V X, giving F V X Q

We now have the following chains, all in the same interval:

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

From 4-2, F X :: U P, giving U . P O H . B T . . W

From 4-6, P T :: M A, giving M . . . Z A S D L

From 1-6, O T :: A Y, giving Z A S D L Y

From 3-1, Y Z :: K U, giving U . . . . K which gives  
 U . P O H K B T . . W

We now have the following : M . . . Z A S D L Y  
 U . P O H K B T . . W  
 F V X Q . J . C . I

From the relation A P Y in 3-4, the interval of which compared to the chains we already have, can only be 15, or -11, we have :

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

which can readily be completely filled in. Decimation at an interval or seven to the left (determined by the letters A B C F G H J etc.) gives the primary component :

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

All of the alphabets in both boxes can be placed with respect to each other by the process explained in solution to Lesson VII. As one of the keys is 5 letters long and the other, 6, which two numbers have no factors and no common multiple less than their product, all of the alphabets can be placed relative to each other, determining the keys in the "boxes".

NOTE: It is suggested the student go over this point thoroughly.

Correctly guessing only one letter and any one letter of the plain text then immediately produces complete solution.

Solutions.

Military Cryptanalysis, Part II, 8- p3  
 1937.

## ARMY EXTENSION COURSES

## SOLUTIONS

SUBCOURSE - Military Cryptanalysis, Part II.

LESSON IX - Indirect Symmetry.

Weight

100 1. Different mixed sequences slid against each other:

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

The plain text of the message is:

A SQUADRON OF BOMBING PLANES FLYING SOUTH DROPPED EIGHT LARGE BOMBS ON THE RAILROAD BRIDGE AT EAST RIVER WHICH DESTROYED THE APPROACH ON THIS SIDE BUT DID NOT SERIOUSLY DAMAGE THE MAIN SPAN STOP AS THIS DAMAGE WILL REQUIRE AT LEAST EIGHT DAYS TO REPAIR IT WILL BE NECESSARY TO ROUTE ALL TRAFFIC ACROSS THE RIVER VIA FIRST STREET BRIDGE IN NEW VENICE STOP THE FIRST ENGINEERS WILL REPAIR THE APPROACH WITH ALL POSSIBLE SPEED AND ADVISE THE DIVISION ENGINEER AS TO THE TIME THAT WE CAN EXPECT TO RESUME TRAFFIC OVER EAST RIVER BRIDGE STOP WHERE ARTILLERY AMMUNITION MUST BE TRANSPORTED OVER THE RIVER THIS WILL BE DONE BY TRUCK VIA THE FERRY AT ZIMMERS FALLS

STOP IF AMMUNITION IS NEEDED BY THE ARTILLERY NORTH  
 OF WILSONS SCHOOL IT WILL BE FURNISHED THEM FROM  
 AMMUNITION NOW AT WILSONS SCHOOL STOP ALL AMBULANCES  
 WILL BE ROUTED VIA FERRY AT SIMS EXCEPT AMBULANCES  
 FROM THAT DIVISION ARTILLERY NORTH OF THE BRIDGE AT  
 CY JONES SCHOOL.

From repeats and frequency considerations, W Q N G  
 4 5 6 7  
 guessed to be STOP; then W S X W Q to be FIRST.  
 1 2 3 4 5  
 Several THE's, AMBULANCES, ARTILLERY and DIVISION  
 follow.

Indirect symmetry, while applicable is usually of  
 little value where two different mixed sequences are  
 used as by the time enough values can be inserted in  
 the "box" to produce results, the plain text can be read  
 directly from frequency considerations and skeletons of  
 words. However, the principle is extremely valuable  
 in solving more complicated systems.

## ARMY EXTENSION COURSES

## SOLUTIONS

SUBCOURSE - Military Cryptanalysis, Part II.

LESSON X - Indirect Symmetry.

Weight:

100. 1. The plain text is as follows, the repeat being underlined:

ARTILLERY FIRE IS INTERDICTING THE ROAD FROM R J SIX

EIGHT EIGHT DASH A TO A POINT EIGHT HUNDRED YARDS

SOUTHWEST OF CROSS-ROADS SEVEN EIGHT SEVEN STOP

MUSTARD GAS HAS BEEN SPRAYED ON ROAD FROM R J SIX EIGHT

EIGHT DASH A TO A POINT EIGHT HUNDRED YARDS SOUTHWEST

OF CROSS-ROADS SEVEN EIGHT SEVEN X B.

Repeat patterns or ideomorphisms indicate the exact beginning and end of the repeat of the same plain text. These are superimposed and the five sets of pairs taken out, it having been determined that there are five alphabets involved:

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

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

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

Pairs are taken out:

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

From 4-3, we get

M E	and from 5-1, C W L I
Y S	Y K H
L D H W P K	G P D X J
Z U N	O A U
B I X	

Most fortuitously, the letters L and W occur in chains in both sets of values. D and P also occur in the same relationship. If we spread out the 5-1 column so that C and W are at an interval of three, we can combine the two sets of relationships by reversing all the chains from 4-3:

5-1	4-3
C . . W . . L . . I	E M
Y . . K . . H	S Y
G . . P . . D . . X . . J	K P W H D L
O . . A . . U	N U Z
	X I B

Combining the two (as they are now at the same interval):

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

which combine to give:

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

Solutions.

Military Cryptanalysis, Part II, 10-p 2

1937.

From 2-1, B O :: Y C and L X :: U T , which give:

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

Which can readily be completed to give:

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

This happens to be the primary sequence. If some other interval was used as the basic interval to build up the chain, the secondary derived must be decimated at different odd intervals until by trial this sequence is obtained. The primary sequence is recognized by the relationships of such letters as (in this case) JOV, KPW, LQX, etc. When this is noted, the transposition key can be built up to get the key-word:

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

Now since  $S_1 = A_5$ , we can start the "box" (although we do not know what the plain-text equivalent of  $S_1$  and  $A_5$  are):

Plain	O	
		_____
1	S	(T)
2		(L)
Cipher	3	
	4	
	5	A

from which alphabets 1 and 5 can be completely filled in.

Now since  $T_1 = L_2$ , we can add  $L_2$  under  $T_1$ , and fill in alphabet 2. Similarly, the rest of the "box" may be completed and the key-word LUCKY noted.

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

Solutions.

Military Cryptanalysis, Part II, 10-p 3.  
1937.

The whole message can now be reduced to a monoalphabet and solved, whereupon the plain component, based upon the words HAND SIDE becomes evident.

The plain component is:

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

Solutions.

Military Cryptanalysis, Part II, 10-p 4.

1937