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-factorng; 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.

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

[Signature]

Paul S. Willard
Colonel, AGC
Adjutant General
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 trigraphs 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:

UCGZD FRCAJ GTZVF WFZVU KHZVH
DREUE WAZFRU QOBNQ QCOJL DZGBY
WHICR KWNVR FGIAV GINUP GIHGD
ABNBP CFLBZ UCGZD UGCGO WHCAJ
ECPRE QHYAS EGNBS JSXSR JQYFH
KHCZD LSXNW SFYVQ XCLPH VRCIL
KWIAD JSGBY ARABQ YSNGB KPOEJ
VOMUK SBIIH JFINQ KHICW ZWMQL
NWMBR FKCYJ UCHGL FIYGR YUEG
LVYFL YVNSO SBEBI GILPR JDMFW

Military Cryptanalysis-Part II, 1-p 2
1937.
Weight:
GDUZP MBCGL GBQVO DQIAW ABORW
GPYSX JBCFK WRCAD FMUZR MBNFG
WGCEH VPIGK XCLFH NSHGB XWPRV
SBXSR JZUEJ WFAHQ KGNBS YOMBO
ABYSR JHLNF LCLFZ AZFOH GPNNL
FOVYH SHZBX JQIEQ WFMNW SBSGL
ESUSW WFYVJ ZHUKP LCGBU JCQFW
GDWTV WQIAG VWPVV ACH

3. Solve the following and recover the keyword:
VKS WD EXFCK CZKEK FTYZD IFNWA
EUJTA XRPCI MAXHG GRLNA VNQJY
MWD WD GAVZW DGIUS PVKWJ YYHYT
LSNZZ EFVTK UHJTB ZDIFN WAEHZ
NXKAS HZL
Note: The enemy has been using reversed standard alphabets.

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

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

To: CG Provisional Cavalry Corps
KOWYZ NMXHG HLNXB LGHAN RFOPD
QYPNE QWMEE PEFIG EEULJ LIQGA
MRHVL RAWGZ BNFXI UOMQX TETL

Military Cryptanalysis-Part II, l-p 3
1937.
REF ID:A4146451

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:

FQUHA WXDIV IUXCP HHVTP PQVNNK
RTNNX DKHEQ KXZFN PQNYU OTSPQ
UHAIW XHVPT PZRKH VPXHV PBCZM
GBSVM HKOIH PRKCK JOWEM MBGVP
PPRAC WDBXN QZHJK PXPZO LFOOI
GVQXP VYDVR YAXTF GBFPN OPKYW
ULAEU SHQEP MQMYI MUOKW TFGQN
LVEEM CPFXH RULKG KLWXQ LBGPA
GYUOW DECBE NGXJP LJXOO IGVNX
PEGBO RADIM EDLVP SQNID KTBSC

Military Cryptanalysis, Part II, 2-p 1
1937.
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.

JUAAC HAXFR KKTUK YMSMU ZHUDE
SFLUO TCKQR RRRUSW CEXZG NAKBU
GEMHN IKQRP IYKYG NTGRQ QBEEL
WAKQH BSSJY ZJWAK QHZYK PLUZC
GB

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

ADCNO GZRT FUSOS WITZI UXFOR
BZBMY BUZCD XODCX PGJDY PAFDB

Military Cryptanalysis, Part II, 2-p 2
1937.
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:

1. Direct symmetry can be used only when the plain component is known. (Line out incorrect one.)

2. Which component must be known in order to make possible the matching of distributions of cipher alphabets?

3. If the first and fifth cipher alphabets show similar frequency distributions, what can be deduced as to the nature of the keyword?

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 U 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 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

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

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 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
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
P M H S L I B K W X P F Q H I Z E 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 W 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
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 P C N T P L E X V E
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

Military Cryptanalysis, Part III, 3-p 2
1937.
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. NGSUHTIRIVYKWBLXCMZDJOEPAFQ
   5
   b. OMDFKUGNCJSZRBIQYEAHPXVTFLLW
   5
   c. JRFUPZMBEKTVGLQDCQSDLANW
   5
   d. ZYASDGKQWCPNIEHMUXRTLBFPJOV

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:

Military Cryptanalysis, Part II, 4-p 1
1937.
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: 0 Ø p r etc. . . . . . . . . . . . .
mixed sequence 26 letters long

Cipher: 0 Ø p r etc. . . . . . . . . . . . . 0 Ø p r etc.
same mixed sequence repeated - 52 letters long

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

MESSAGE "B".

<table>
<thead>
<tr>
<th>C N U Y W</th>
<th>V L E Y</th>
<th>M X Z C K</th>
<th>A A L L U</th>
<th>P S S Y U</th>
</tr>
</thead>
<tbody>
<tr>
<td>X W G Y V</td>
<td>K N U U U</td>
<td>P I G M W</td>
<td>K I A T W</td>
<td>W X Z L L</td>
</tr>
<tr>
<td>S F G V K</td>
<td>I N N N U</td>
<td>M V U D U</td>
<td>J C G D V</td>
<td>A A L L V</td>
</tr>
<tr>
<td>N W E Y V</td>
<td>A D A R E</td>
<td>E W S V V</td>
<td>N F U K C</td>
<td>etc.</td>
</tr>
</tbody>
</table>

Military Cryptanalysis, Part II, 4-p 2 1937.
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".

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?

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.
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"?

Military Cryptanalysis, Part II, 5-p 1
1937.
LESSON FIVE

MESSAGE

XJITZ FPVYV MNTNL CJIDT FNTHTL XWZT
HJOKH BZEYE VPNHZ NMAEA RWHXA RFWKK
VGAKH BSWMR DLNCN UAJEF QNSUC IVLJK
XZKNX CPXZX KLJLH RYQKE MBDKK HNFJE
AZUKH BSCZL RPNXD BAXMR BBHQC PPCF
EJLGT GRXPE SBOLH HNM0D ORGAV BFSPS
NWUZZ COLZP KJHPJ JRKET HTXTH JWDK
IIKTH BSIZJ ANHAW NPJTE ABDXX JYFZO
ANKKK PAHYT TNNAL NVLPK CJOLH HNM0
UCBKIH BZHIK DBDKH BSYES MBDFX PYZHT
TRLHC CWLRZ BNHXR BAHIZ BQGYW JWHCS
LIBXG PWLRZ BRHWH KYIEO MBMS EVQML
ENUAW XWLRZ BCEZT XYZWT FBZPL CYXVP
KBDXW XNJMJ KSTYW JWHIN RBDXH RYIZO
KNCHD PAIZN ALURL QKWHS MJCQA UYHTS
NNCDR XYAZE TRGMH RAHR DTLKU BOAVW
YGLKU BAHIL DQGRL YAHWK XJIAW WKBMT
BIGBW XVMMJ DMDAW QGIGW DUXL XVMZE
YGBMU XYKEM KNHXX XYFCF NULPL CYBMM
YGNXL YKCTS ALBNC NHCUJ RJUQM YKCTS
VJSXC

Military Cryptanalysis, Part II, 5-p 2
1937.
Military Cryptanalysis, Part II, 5-p 2
1937.
Military Cryptanalysis, Part II, 5-p 2
1937.
ARMS 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

Message A

DNC to DBA 2:15 pm.

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

Message B

DNC to DBB 2:30 pm.

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

Military Cryptanalysis, Part II, 6-p 1
1937.
2. Solve the following message and determine the keyword.

Message C

DNC to DBC 4:00 pm.
WFKQF QRXLQ TFCXG GWECL PSAKW
FAQRU TFFAK ICKG OCDKR EDJOQ
PCWFK QFEXC

Worksheet for Problem 1

Military Cryptanalysis, Part II, 6. p 2
1937.
Message A
MUOUV DSWKNCICHLBJSIMXOPJCINWNUR
MTOGGSONDIAHTPZXXKEONNVMG QOKJ
ACKAYQQSO MCBBMHKJQCTHSJJOYWUY
HOJNEJZJMLCZEONNERJOOMVIOHMQH
MCKGJRICWNKOMHYMMTIYUYFICHHX
KEONNGZMJKNYOHMRUOPHRFTMMMJ
DNOROXMJXXRQXAFMVECHT

Message B
UWWCOLOHTBPUAZFFFHDDJKTOXFUCPQJ
UPQJFDHMOTUMZPUUCKGVOPGMUFTCX
AILDVDSAZDTJWFAYMXA1MHXXQNSYQS
ZNXLHMYXOSARVQPMOHQOTJGWNWUZW
UIBJQXOUAYSBCJSOJVZUSQEXUAUCK
GVQPMTRJXLMWENWOEEXNUPEPSJRUX
WMBZKQJKBZKPOYRVAZP

Military Cryptanalysis, Part II, 6-p 3
1937.
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

Military Cryptanalysis, Part II, 7-p-l
1937.
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 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

Military Cryptanalysis, Part II, 8-p 1
1937.
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.

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

Military Cryptanalysis, Part II, 9-p 2
1937.
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.
Military Cryptanalysis, Part II, 10-p 2.
1937.
REF ID: A4146451

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 CONTINUE 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(M)M TOMORROW STOP CG SECOND DIVISION


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.

Solutions

Military Cryptanalysis, Part II, 1-p 1

1937.
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.
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
HELDER GENERAL LINE SOUTH OF RIGHTER RANCH TO DAVENTPORT
HOSTILE ATTACK APPARENTLY STOPPED YEA
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 T
       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 AS 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
HELDT GENERAL LINE SOUTH OF RIGHTER RANCH TO DAVENPORT
HOSTILE ATTACK APPARENTLY STOPPED LEAR
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: COPYRIGHTEDABFJKLMQSUWVXZ

Cipher: KLMNOPQRSTUWXYZABCD

Y Z ABCDEFGHIJKLMNOPQRSTUVWXYZ

WXZABCD EFGHIJKLMNOPQRSTUVWXYZ

OQRSTUWXYZABCD EFGHIJKLMNOPQRSTUVWXYZ

RSTUWXYZABCD EFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABCD

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
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
REF ID: A4146451

ARMY EXTENSION COURSES

SOLUTIONS

SUBCOURSE - Military Cryptanalysis, Part II

LESSON IV - Indirect Symmetry; secondary alphabets.

Weight:

5 1. a JANUARY
   b GOVERNMENT
   c CHINESE PORT
   d CRYPTOANLYSIS

5 2. 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25.


10 4. 1st \(\text{or -16};\) 2d \(\text{or -7};\) 3d \(\text{or -6};\)

   4th \(\text{or -22};\) 5th \(\text{or -12}.

5 5. Plain: WASHINGTOBCEFJKLMPRUVXYZ

   Cipher: WASHINGTOBCEFJKLMPRUVXYZWASHINGTOBCEFJKLMPRUVXYZ

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.
Solutions
Military Cryptanalysis, Part II, 5p 1
1937.
Weight:

Plain: JUGOSLAVIBCDEFHKNPQRSTWXYZ

Cipher 1: OSLAVIBCDEFGKMNPTWZJUG
Cipher 2: HKMNPTWZJUGOSLAVIBCD
Cipher 3: XYZJUGOSLAVIBCD
Cipher 4: DPQRTWXZJUGOSLAVIBCD
Cipher 5: QRTWXZJUGOSLAVIBCD
Cipher 6: AVIBCDEFGKMNPTWZJUGOSL
Cipher 7: EFHKNPQRSTUVWXYZJUGOSLAVIBCD
Cipher 8: GOSLAVIBCD
Cipher 9: SLAVICDEFGKMNPTWZJUGOSL
Cipher 10: BCDEFGKMNPTWZJUGOSLAVI

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

Line 3 KHBS . . . . . STOP
Line 4 HRY . . . . . THE
Line 5 BDX . . . . . THE
Line 6 GHLHNVMOU . . 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.

Solutions
Military Cryptanalysis, Part II, 5-p 2
1937.
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:

<table>
<thead>
<tr>
<th>Plain</th>
<th>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</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cipher 1</td>
<td>V E R A B C F G H J M N O P T W X Y Z Q U I C K S L</td>
</tr>
<tr>
<td>Cipher 3</td>
<td>B D F G H J M N O P T W X Y Z Q U I C K S L V E A</td>
</tr>
<tr>
<td>Cipher 5</td>
<td>Z 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</td>
</tr>
</tbody>
</table>

Keyword: MOTORS under plain letter A.

"Box" for Message B

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

Keyword: UNITED under plain letter A.

Solutions
Military Cryptanalysis, Part II, 6-p 1
1937.
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    QUICKSILVERABDFGHJMNOPTWXYZ
Cipher 1 UICKSILVERABDFGHJMNOPTWXYZQ
Cipher 2 YZQUICKSILVERABDFGHJMNOPTWX
Cipher 3 ICKSLIVERABDFGHJMNOPTWXYZQU
Cipher 4 TWXYZQUICKSILVERABDFGHJMNOP

Keyword: BEDS under plain letter A.

Plain text:

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

Solutions
Military Cryptanalysis, Part II, 6-p 2
1937.
1. 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:

SATURDAYBCEFHIGJKLMNOPQVWXZ

"Box" for Message A

Plain SATURDAYBCEFHIGJKLMNOPQVWXZ
Cipher 1 EFGHIJKLMNOPQVWXZSATURDAYBC
Cipher 2 RDYBCEFHIGJKLMNOPQVWXZSATU
Cipher 3 DBCEFHIGJKLMNOPQVWXZSATUR
Cipher 4 URDBCEFGHIJKLMNOPQVWXZSAT

Keyword: CURT under plain letter Z.

"Box" for Message B

Plain SATURDAYBCEFHIGJKLMNOPQVWXZ
Cipher 1 ZSATURDAYBCEFHIGJKLMNOPQVWX
Cipher 2 NOPQVWXZSATURDAYBCEFHIGJKLM
Cipher 3 EFGHIJKLMNOPQVWXZSATURDAYBC
Cipher 4 OPQVWXZSATURDAYBCEFHIGJKLMN
Cipher 5 FGHJKLMNOPQVWXZSATURDAYBC
Cipher 6 EFGHIJKLMNOPQVWXZSATURDAYBC

Keyword: CANTON under plain letter E.

Solutions
Military Cryptanalysis, Part II, 7-p 1
1937.
**Weight:**

Solution of Problem

<table>
<thead>
<tr>
<th>1-1</th>
<th>2-2</th>
<th>3-3</th>
<th>4-4</th>
<th>1-5</th>
<th>2-6</th>
<th>4-2</th>
<th>1-3</th>
<th>2-4</th>
<th>3-5</th>
<th>4-6</th>
</tr>
</thead>
<tbody>
<tr>
<td>TN</td>
<td>BQ</td>
<td>EI</td>
<td>RP</td>
<td>JK</td>
<td>SD</td>
<td>YS</td>
<td>QF</td>
<td>MM</td>
<td>IT</td>
<td>MV</td>
</tr>
<tr>
<td>EZ</td>
<td>GZ</td>
<td>JN</td>
<td>HT</td>
<td>AT</td>
<td>MV</td>
<td>BA</td>
<td>VG</td>
<td>UU</td>
<td>XI</td>
<td>JO</td>
</tr>
<tr>
<td>FS</td>
<td>YP</td>
<td>BG</td>
<td>MB</td>
<td>EF</td>
<td>KE</td>
<td>UW</td>
<td>TM</td>
<td>NN</td>
<td>CW</td>
<td>XU</td>
</tr>
<tr>
<td>VH</td>
<td>SJ</td>
<td>EZ</td>
<td>TU</td>
<td>BH</td>
<td>BU</td>
<td>BV</td>
<td>TT</td>
<td>KR</td>
<td>NW</td>
<td>PS</td>
</tr>
<tr>
<td>NC</td>
<td>VF</td>
<td>SL</td>
<td>VW</td>
<td>PZ</td>
<td>QK</td>
<td>GS</td>
<td>XX</td>
<td>VG</td>
<td>BI</td>
<td>LV</td>
</tr>
<tr>
<td>AM</td>
<td>RN</td>
<td>GH</td>
<td>YG</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note that the 2-6 and the 3-5 columns are the same interval and can be combined; likewise, columns 4-2 and 2-4.

From 4-2 and 2-4, get immediately: BVGS and XIT.

From 3-3, since B and G are at interval of 2 in the 4-2 chain, we have also: B.G, E.I, and J.N.

From 2-2, we have BG and QZ in the same interval. This gives QFZ.

Also from 2-2, FJ and VS. Since we have V.S, this gives QFZJ.N.

From 1-5, VG :: WH and from 3-5, WH :: NB. Since we have VG already adjacent, we can add NB to the chain. This enables us to say:

QFZJNBVS

From this point, the chain is rapidly completed to:

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

Noting that J, K and L are in order at interval of 7, decimation at this interval produces the primary alphabet:

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

Since T and N in the two first alphabets represent the same (the first) letter, the two first alphabets can be entered in their boxes in their proper relation.

Then since J and K represent the same letter in 1 and 5, alphabet 5 can be entered in the box in its proper relation, etc. All the odd numbered columns can be placed with proper relation to each other. Likewise, all the even numbered columns can be placed with respect to each other, but not in their relation to the odd columns. The two sets of alphabets can be placed in proper relation either by sliding the two sets of alphabets along each other until the keyword appears or by making frequency tables of the two sets of alphabets and matching the two frequency distributions.

**Solutions**

Military Cryptanalysis, Part II, 7-p 2
1937.
Solutions
Military Cryptanalysis, Part II, 8-p 1
1937.
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, VAY, 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:

<table>
<thead>
<tr>
<th>1-1</th>
<th>2-2</th>
<th>3-3</th>
<th>4-4</th>
<th>5-5</th>
<th>1-6</th>
<th>2-1</th>
<th>3-2</th>
<th>4-3</th>
<th>5-4</th>
<th>1-5</th>
<th>2-6</th>
<th>3-1</th>
<th>4-2</th>
<th>5-3</th>
</tr>
</thead>
<tbody>
<tr>
<td>FU</td>
<td>UX</td>
<td>ZA</td>
<td>YG</td>
<td>VT</td>
<td>TY</td>
<td>AE</td>
<td>QF</td>
<td>WL</td>
<td>FV</td>
<td>WB</td>
<td>DP</td>
<td>WE</td>
<td>UP</td>
<td>XT</td>
</tr>
<tr>
<td>OG</td>
<td>PR</td>
<td>AS</td>
<td>KC</td>
<td>KV</td>
<td>MF</td>
<td>KL</td>
<td>WT</td>
<td>ZF</td>
<td>DL</td>
<td>NK</td>
<td>KY</td>
<td>FX</td>
<td>UA</td>
<td></td>
</tr>
<tr>
<td>TD</td>
<td>TI</td>
<td>PO</td>
<td>ZB</td>
<td>KV</td>
<td>OA</td>
<td>DU</td>
<td>DZ</td>
<td>XU</td>
<td>BT</td>
<td>IJ</td>
<td>KM</td>
<td>ZU</td>
<td>PH</td>
<td>UA</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>1-1</th>
<th>2-4</th>
<th>3-6</th>
<th>4-1</th>
<th>5-2</th>
<th>1-3</th>
<th>2-4</th>
<th>3-5</th>
<th>4-6</th>
<th>5-1</th>
<th>1-2</th>
<th>2-3</th>
<th>3-4</th>
<th>4-5</th>
<th>5-6</th>
</tr>
</thead>
<tbody>
<tr>
<td>QH</td>
<td>AZ</td>
<td>ZP</td>
<td>WO</td>
<td>LC</td>
<td>OL</td>
<td>UZ</td>
<td>QJ</td>
<td>TP</td>
<td>EE</td>
<td>NU</td>
<td>FL</td>
<td>AP</td>
<td>LJ</td>
<td>OK</td>
</tr>
<tr>
<td>MY</td>
<td>DS</td>
<td>TJ</td>
<td>TU</td>
<td>GX</td>
<td>FA</td>
<td>PH</td>
<td>CI</td>
<td>AM</td>
<td>NN</td>
<td>NU</td>
<td>HP</td>
<td>FY</td>
<td>AX</td>
<td>OK</td>
</tr>
</tbody>
</table>

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.

Solutions

Military Cryptanalysis, Part II, 8-p 2
1937.
From 2-2, X I :: UT, giving U ... T since we had X ... I.
From 2-5, S D :: VX, giving F VX Q.

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

Z ASD L
F VX Q, J C I
P Q
K ... N
U ... H BT ... W

From 4-2, FX :: UP, giving U P O H B T ... W.

From 4-6, PT :: MA, giving M ... Z ASD L.
From 1-6, OT :: AY, giving Z ASD L Y.
From 3-1, YZ :: KU, giving U ... K which gives
U P O H K B T ... W.

We now have the following:
M ... Z ASD L Y
U P O H K B T ... W
F VX 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 ASD L Y F VX 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:

ABC F G H J L N P Q S T U V Z KEYWORD 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.
SOLUTIONS

SUBCOURSE - Military Cryptanalysis, Part II.

LESSON IX - Indirect Symmetry.

Weight

100

1. Different mixed sequences slid against each other:

Plain

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>C</td>
<td>U</td>
</tr>
<tr>
<td>M</td>
<td>D</td>
<td>V</td>
</tr>
<tr>
<td>N</td>
<td>E</td>
<td>W</td>
</tr>
<tr>
<td>O</td>
<td>F</td>
<td>X</td>
</tr>
<tr>
<td>P</td>
<td>G</td>
<td>Y</td>
</tr>
<tr>
<td>Q</td>
<td>H</td>
<td>Z</td>
</tr>
</tbody>
</table>

Cipher

<table>
<thead>
<tr>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>W</td>
<td>M</td>
<td>Y</td>
<td>F</td>
</tr>
<tr>
<td>X</td>
<td>N</td>
<td>Z</td>
<td>J</td>
</tr>
<tr>
<td>Y</td>
<td>Q</td>
<td>I</td>
<td>E</td>
</tr>
<tr>
<td>Z</td>
<td>P</td>
<td>K</td>
<td>H</td>
</tr>
<tr>
<td>R</td>
<td>S</td>
<td>T</td>
<td>G</td>
</tr>
<tr>
<td>I</td>
<td>U</td>
<td>V</td>
<td>C</td>
</tr>
</tbody>
</table>

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

Solutions.

Military Cryptanalysis, Part II, 9- pl 1937.
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 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.
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
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
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 S T W H O G B G M W
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
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
K Y L X X A T E W U C 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
```

Solutions.
Military Cryptanalysis, Part II, 10-p 1.
1937.
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
E 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
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
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:

YGCKPWHDLXIBJOVRAFNUZTEM

Which can readily be completed to give:

YGCKPWHDLQXIBJOVRAFNUZTEM

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, KTPW, LQX, etc. When this is noted, the transposition key can be built up to get the key-word:

4 3 1 2 5
RIGHT
ABCD
FJKLM
NOPQRS
UVWXYZ
Z

Now since S1 = A5, we can start the "box" (although we do not know what the plain-text equivalent of S1 and A5 are):

Plain 0

1 S (T)
2
Ciphertext 3

4
5 A

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

Now since T1 = L2, we can add L2 under T1, and fill in alphabet 2. Similarly, the rest of the "box" may be completed and the key-word LUCKY noted.

1 SYGCKPWHDLQXIBJOVRAFNUZTEM
2 IBJOVRAFNUZTEMYSYGCKPWHDLQX
3 NUZTEMYSYGCKPWHDLQXIBJOVRAF
4 UZTEMYSYGCKPWHDLQXIBJOVRAFN
5 AFNUZTEMYSYGCKPWHDLQXIBJOVR

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:

```
HANDSIEBCFGJKLMNPQRSTUWXYZ
```