SUBCOURSE

MILITARY CRYPTOANALYSIS, PART III

SIMPLE TYPES OF APERIODIC SUBSTITUTION SYSTEM

1938-39

(Introduction and Lesson 1)
30 April 1959

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

Paul S. Willard
Colonel, AGC
Adjutant General
Purpose and Scope:

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

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

Number of Lessons and Approximate Time Required:

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

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

Texts Required:

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

Materials Required:

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

Special Instructions and Information:

Each lesson assignment has a maximum weight of 100. So far as practicable, detailed work sheets which usually form a part of the solution should be submitted with the solutions. They will be returned to the student for file or further study. DO NOT RETURN THE LESSON.
SHEETS UNLESS WORK IS SHOWN THEREON. In all cases show the primary components and keys from which derived.

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

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

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

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

********

LESSON ASSIGNMENT

SUBCOURSE - Military Cryptanalysis, Part III

LESSON - 1

Weight:

15  1a. Solve the following message:

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

5  1b. What is the keyword for the message?

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

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

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

No. 1
S I I S A J C I O L A H F X V Z J G L M L A E A D X T V F A:
L P T I B K T W G T A V T A J Y R Z D E R I T Q D G L W M
M S G U X K Y P R S A R J S U O Z T G U H U Z G A E D I X N
I T L W I Q Z K R M P J C G T Q T A M A Y A C W R A L A H-
A I Z O W E A Z R S N R J M T S Q S E C K D H S G H V F Z V
F M H O Z E K E E V R K D A G S E A E V I X W B Z G N L Z
N R J M E W E S C K D H C C H

No. 2
W G W H P L B Z R S S I B G V S R W N X B F J C G P R X Q A
Q R D L C V H P D G Z V K U T K H Y Z Y I M N R J R M
R K A H I K R B R U C Q X C H J M L X X

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

Weight:

5

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

MSOWS AENQ R KSUBNW NYOY WZEHM BNZRH
AXMDQ DGXXX

Military Cryptanalysis—Part III, 1–p. 4, 1933.
CORRECTION

Problem 3 should read: "The enemy is using the word-length keying system exemplified in Problem 2, but the primary components are differently mixed sequences. The letter Z is employed as word separator. The following message has been intercepted. Solve it, reconstruct the primary component and the key for the message."
REF ID:A60198

ARfY EXTENSION COURSES

LESSON ASSIGNMENT

SUBCOURSE - Military Cryptanalysis, Part III

LESSON - 2

Weight:

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

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

   1 2 3 4 5
A. ANCKG EHWYJ EFVWJ QOVDW PBNFN
B. LUZIU WRPOP IZQVN IVBLI MKQHY
C. WRRKB DJDBL YJJNI ATEJZ DVQZ
D. LXZPU MNAPI MAYJARPOZY BBYKU
E. OVTMGQ DKBUI LYJEJ YQDVVF DGSQS
F. GKGIG DCPBU VGIIJ MUOZC JESOKB
G. QEOMZ OVDVW KKLJN ZAEDPEQOGK
H. UPBUV GIOIR JMNVC MBMGFNKHKLK
J. XMVDW NULCT YXSMEVJDQ DOPQS

Military Cryptanalysis-Part III, 2-p.1,193C.
Weight:

2. Continued:

1 2 3 4 5
K. PB MIF MRRNZ ZBCWM IKA VLD DJQXB
L. SIWTB LYEED GFWZ QZLVUUPPNXA
M. QNLUB IPLMO IZYVT MVGWL JDCWY
N. NBLGK TXYCK EWEKF UQZDFI

3. The enemy is using the word-length keying system exempli-
fied in Problem 2, but the primary components are differently
mixed sequences, the latter Zp being employed for this purpose.
The following message has been intercepted. Solve it, reconstruc-
t the primary component and the key for the message.

1 2 3 4 5 6
A. YRMLT GCYJK HPPFF BBABJJSDDAVKVNU
B. ONNYS FMTLUT ILTFK VDDGZ QUSKA OYPDV
C. XKVWN NPWOT HIYUF WBBAM DWWRG GCBMV
D. CAQPND PZGH GNGOS TKJHG FIVCZ YSAEX
E. XVMHG GXNDL RQTDY JJBKSNUDFP VZDXX

Lay out the working form as follows:

(Material required: Pencil, Paper and Dividers.)

1. On stiff paper, scribe a circle 3 or 4 inches in diameter.
   Divide the circle into 26 equal spaces.
   Letter into these spaces the letters of the alphabet, A to Z,
   pointing the base of the letter toward the center of the circle.
   Inside of the line of letters, number the spaces 1 to 26,
   starting with A.
   Now cut out the circle and lay it aside.

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

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

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

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

   You are now ready to start to encipher.

4. Place cut-out circle on top of circle on sheet, pinning at centers
   so the cut-out will revolve and the respective letters of each circle
   will match up.
   A
   Set the space 1 on the rotating circle opposite A on the stationary
   circle.

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

This brings us to G, from which point we encipher our first word of our sample message, the rotating circle being used for the regular word, and the code word being derived from the stationary or outer circle.

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

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

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

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

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

5. DECIPHERING is simply a reversal of the foregoing.

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

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

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

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

TEST MESSAGE

August 5th, 1930.

A. VFUYO XNEOW XNLDX AQWXV YIPZQ
B. HTBDZ LBZHK PGGVG IPNJF ARXSF
C. KALTN ZGHHS FZVJG EOJUG USOZB
D. JUYXQ JKOV B TWJPI EQPAL SREHM
E. SNHSR YYUMA QKAPX XHLIZ ZCHVM

Military Cryptanalysis-Part III, 2-p.5,1933.
Lesson Assignment Sheet

Subcourse: Military Cryptanalysis, Part III
Lesson: 3

Weight:

8 1a. Solve the following cryptogram:

AXKBY LBLXX LGBJO RXQX KRVGCUCUO
PHQDQ DYUGX KLMAX KJGDD MDFQR YXEJY
ZRDZD DERZY ZVVFMCJUZ YWJPLBNMOK
ZDQ

8 2b. What is the keyword and how does it control the shifting of the primary components?

2 2a. Solve the following cryptogram:

XJHFE USRBB ITLRN FYQRY IJSZG GFJZB
QWVRQ WCQRQ JMUTJ WRDSI WAMPLOL

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

30 3a. Solve the following cryptogram:

ZSIIFQVZORVSSQXUYVLABRAXHXYCR
JECNNFBHCDGRYZAYLMEMYZAUCMYLZB
KLLSZIFQVZORVSSSFCPCMCXHCZCD
GRYIIBDTKZYBOCYLUDHCFBUVYUWVQ
QVQWORKKUFMBVFXMVFBYSXCGSXT
HCRCNBYTLXAUUNLGNWLKOLEMYZAMZ
SQRZRPVRIUBDUNPTDFBBIQTHBDSRU
IDYCHUURRSDHEBDUSIDTMYUDUXRDVZ
RULUBPZYBCGUVSORXSYQXBVCXBQBSI
SD

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

\[
\begin{align*}
C & W I E Q G E R O M V S Q P V M M O X X D U H E D G K E W G \\
U & K F Q Z R V S Q A V G U U V O P C G D S M J H O K J R D O \\
Q & X B S D R O R V S B I C M V I E K Y O E E J B I
\end{align*}
\]

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

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

<table>
<thead>
<tr>
<th>From Station</th>
<th>To Station</th>
<th>Serial No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>B</td>
<td>17</td>
</tr>
<tr>
<td>A</td>
<td>C</td>
<td>15</td>
</tr>
<tr>
<td>B</td>
<td>A</td>
<td>14</td>
</tr>
<tr>
<td>B</td>
<td>C</td>
<td>16</td>
</tr>
<tr>
<td>C</td>
<td>A</td>
<td>21</td>
</tr>
<tr>
<td>C</td>
<td>B</td>
<td>11</td>
</tr>
</tbody>
</table>

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

No. 1

From B to A

\[
\begin{align*}
U & H O K B D Q F Q E H U I A U I O U M U I F S D C O Q G C C \\
O & Y Z F C I P H D B L Z P B I T C A B P B U I J K X G I U O Y
\end{align*}
\]

Weight:

No. 2

From C to A

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

No. 3

From A to C

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

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

LESSON ASSIGNMENT

SUBCOURSE - Military Cryptanalysis, Part III.

LESSON - 4

Weight:

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

1  b. What is the keyword for the messages?

3  c. Indicate the primary components.

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

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

C. O. 95th Infantry

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

Smith, Brigadier General

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

H K D H Z U Z O T Q L E U E G C E Q 4 G E U U C X L J U X Q
A P M P X M V Q H H M L X Q J Z Q U R R R U L L O L D P N M

Military Cryptanalysis, Part III, 4-p.1, 1938.
REF ID:A60198

Weight:
MVXSVUQWOQVEVCHKKBUMOFASSHGXP
WLSDKDBLXOHQH5FJCBUMFDBIKWV
HBPLFESRBSBQWABCPLGHHKTLDGFQXV
NDEVBPGOVQHHMLROURCDSKUWQWNVV
XSVUEUDKRS

LESSON 4 - Problem 1

MESSAGES WORK SHEET.

(1) ZCTPZWZPEPZQX (19) AFEOJTDITT
(2) WTEQMXZSYSPRC (20) KPVFQWPKTEV
(3) TCRWCXTBH (21) ZABGRTXPUQX
(4) EPKCSZRIHa (22) YHEOCUHMDT
(5) YANCtHZNUW (23) CLCPZIKOTH
(6) VZIETIRRGX (24) AFLWZWQMDT
(7) HCQICKGUO (25) ZCWAPMBSAWL
(8) ZCFCLXRKQW (26) HFLMHRZNAPECEI
(9) HWWPTEWCMJS (27) CLZGEMKZTO
(10) EPDOZCLIKcj (28) TPYFKOTIZUH
(11) WTSQZPZIET (29) ZCCPSNEOPHDYL
(12) ZCGGYFCSBG (30) CIGIFTSYTLE
(13) CWZAOOEMHWTP (31) TTSVVDGHPGUZ
(14) CIYGIFBDTVX (32) NOCAIFBJBLGHY
(15) EAQDRDNSRCAPDT (33) XXXPLFEGJL
(16) YFWCQQBZCWC (34) ZCTUMBZJOO
(17) WTEZQSKUHC (35) HCQIWSSBPHCZV
(18) ZCVXQZKZYDWLK

Military Cryptanalysis, Part III, 4-p.3, 1938.
REF ID: A60198

ARMY EXTENSION COURSES
LESSON ASSIGNMENT SHEET

SUBCOURSE - Military Cryptanalysis, Part III
LESSON - 5

Weight:
10 1. Solve the following:

KGGLNGSSAZOKKTA3HwSEDYQZVEALXGNJGFBIMIERFMDPRPIOYVOOBYXXGVHL
GPBWAMTMENUWDPWFYUQE

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

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

1. SCOPAKFBUCGIMJV
2. HHTGMGYHKGQGNIC
3. SRLENTRCTRARBW
4. VLRLEMUTJDQEXO
5. LZVESTEOATGUNVT
6. HYLDAOTEXWWTAX
7. YOQMPDQBQYZUA
8. ZOWKRKIVRWAKCJ
9. CGUQVRBHOSXOXK
10. SRRKMAALWZJAKKMX
11. CAUEJQTEZVJJEU
12. CYUQNCAXXUNRFA

Weight:

13. UOISV ROJHE JBRHI
14. NRIGFWUZPARHZCDT
15. YOKERHNSGZOBACN
16. OYTJRDGCNEJQHNG
17. VBLSQZBDJQIKPZV
18. THNPRBOEFLHXSMK
19. OYUXIRBWBELJIMS
20. SRLMRQFTSVVITQ
21. MHTCYDGYJVWEBZ
22. CMWEXEROMQVVT
23. SRLIKDKQTVWSDXK
24. NOBGXIWIWMIZW
25. YTBUMNIXYWVDHEZ
26. WTTGYCTLMRUNIYWB
27. CWJYIHHJIOATSIGT
28. YOPXIKQAKRWARAH
29. CMWQGHQAJFNZRZF
30. FTWQGRCEBFZEED
31. TOTIFZTHYRSOUJ
32. EZVWNKPVOWKRLCR
33. TZWKDCTKOWTLLKGZ
34. VBLSGNNJUOBUPXB
35. UZBNIKBFUIOZRDM
36. EZKVFWGGEGOUYQK
37. NRLWDEHNPUU LAUHY

Weight:

38. DORFKHKHIFMDHMJ
39. ZAIGRKQOOWOLIAW
40. CSJENVMZDXXMUXT
41. EHWESSEHEMQXWIV
42. OYBEXDOAYXFZWUL
43. YOTKITTTHCPDAHHD
44. ZLPYVCEDSKESSH
45. YHUQIHNPZEWACI

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

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

I.

A. TRSPWGHGXXGJCCXZILKKEVVLX
B. LYLLYDXZZPUAMHZXLNCQJTXYL
C. BPYMVZBQBBFUUVASYSBNVSPPM
D. PXYGWCWJAZJQAUCRNDCCICM
E. HJAUPUNSDLCJAJDKXHGFZCS
F. BAUVGHTFUMKHEMXGEX

II.

G. ZSOPPRRYNP GDUNSHHALIPPQHD
H. WXYLPWPGCBTTGDVABMWDCGYD
J. XDBQUUTQUJUDYPWNGMHQSSF
K. SORMHJOFPWFRRMUEIGJMHYEG
L. JJKSHBHQXEAKKNNYMHBX

REF ID: A60198

Weight:

III.
A. HNFDRERRZTSXXXZPFLJQUEFIJK
B. HJFQXZNTBTEMWSHCYBSKONEOR
C. RNKEDHRYEE

IV.
D. ZJDOHINDKWGYGLCBSKOHJYBE
E. GHGGUULTIPUZKETTZBGAAAPPG
F. FVETJYNSKMHJVPIKPWCWXXX

V.
G. TKKLSGDCWGDOFWAUTWSDSOBGH
H. HCMSEVVSXPVWRGGGLREOWSQ

VI.
J. JUZPCCGHGGALIRGCTNPWJTFIZ
K. CFFZIBLQZDWPUVVVHCBGBBFMS
L. CCBFMMXXX

VII.
M. VVWKLSRLKSERZIFGWEAQXCTSO
N. VIBLYXXX

VIII.
O. SEPBOZRNDYEHHBCRRNKACYFU
P. PRKCIIRKETYIXX

IX.
Q. EIHTXGLRQZSSACBXTTLCRFUVX
R. GLZLRKMWPXTZJFXMQLFUAPEEIE
S. EHNGTTEEDJUSDDKWPVOMMJXX

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

```
NUUBK OCRVS QIFXY MPAIQ GBMRT
SPYCJ VESFC
```
Weight:

1. Solve the following message:

KXIVNLVBSSLNKVVBXETIVQZFNXAMZTZQDLDBLEUDMLSMZFJTVAPNZ;

2. Solve the following message:

123456
A.NCEISGVSKJXCHJIHIBFHKVEDEAIJR
B.LVZGDKVHRMHGYZCNKDJCSLFHIB
C.FHKVCKOAYVDJZVFCFGCFZBFVBSKOA
D.FCJKEKQRMHNWUGJZPBBDJZBJTJBEOZ
E.CGXSULFPXVPFXROFFGFBVBXEBRCE
F.IGTCYGPOLHDCEBUIPHEYGPKQVJBBR
G.XAEWMWYBQFSOCBYCZNEJKFCBFVBBRX
H.EAEBRGPJZJFLVHFCGVCGBPZBRZVTP
I.EHJTMBDJZMHUMEBDSDJLEZGSDHZJK
J.OAPPICEXSGMHQZYHFNDJZMHUTJBJFX
K.CXWWDQQLYFTVDICVNXGCRVLSIKOC
L.AJKLPQREXSENLAKWSIBOFFCTCXSUR
M.HCDEBUFHZNHFQGDJZMSREKZHGCVJ
N.IFHMLHIGRBEQPJEZNEJJKFCBFVBB
O.SKOAYAHEDOHOFHGMISCZNEJUGCZBF

Weight:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.</td>
<td>V</td>
<td>B</td>
<td>B</td>
<td>X</td>
<td>D</td>
<td>J</td>
</tr>
<tr>
<td></td>
<td>V</td>
<td>B</td>
<td>B</td>
<td>X</td>
<td>D</td>
<td>J</td>
</tr>
<tr>
<td>B.</td>
<td>P</td>
<td>D</td>
<td>S</td>
<td>O</td>
<td>A</td>
<td>X</td>
</tr>
</tbody>
</table>

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

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

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

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>BKGWHEZLSIFQPSSGYKXS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>ZOCGEKAABHNMDZPMWVW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>DXYCEJLERHNKGEZIZDK</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>OBISVGMJSIQGMEZCNDWG</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>BKKQCPMTHRHMHEHATKWR</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>ZHVAHPMLZTWNNRAFWGBF</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>OOKXBEKLECQFPSSGYKXO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>BKKWKPQTHERHLTQFWKBG</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>NXIMMPVQBEPIITHCXZDK</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>WHIRXABTWPGAKAHLXTKH</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>AKZBCEIRNFQCXSOGIIWOR</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>AKRAGPFZKPWBBNZLQDKT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>BKGKIVQRBDNGEZLNBSCE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>ZHVQZCFQYAOKRXKNUVOZ</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>BKHACEZCOVTKKNSQTABW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>BKUACNIEGHNRTLKFOSGZ</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>DXIPTRILETOLBCITIABG</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

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

A. QASODPKASHLZEHAYCTQLRQQJX
B. OMEQKFUSBMAKYLPOWYVDJFHTO
C. RKDNBEINPDVWPKOLWAENAEGFA
D. VAMZCFISCXNPBGKWTAOARZBDR
E. EHAHH

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

**MESSAGE NO. 1**

RXOWZ UZULIKTOGDFCJTFMKLR
REAVHJSMAYTIZGAAFGEHNC
ACYAEDGPAIJNQFGTXLKYBE
HJJQSDDPKGHUNRUSQIRKMUPJ
MCTVWOTXSCXCKXCPREXXX

**MESSAGE NO. 2**

IWKWXYOKCFSONSFHSRFVONZKUN
NDYZMZHCACYAC

**MESSAGE NO. 3**

WLWTLOHCHNMQRYONDXJYJGVG
QCSIOOZDVVMBMYDASKYHCQOM
LOTWRCEUNVQNTYQNJHTTZKN
QGMSWRVPWRFWGANCRDCTCJTG
PONQDMBKDZKYNNRCCAHIG
ZPONLOYTDGWRGCOISGQDHOST
IJLFNNRWSIFQIJJZKUDTWREW
PXZUAQJAJSIOCRFKVMBMMIVKB

Weight:

MESSAGE NO. 3 (Continued)

AFXNM JNHIZ SYOZH NFGZZ MYAXT
ZZXYH KCFFT IQGDE GPGM TAoby
FSDPG LIEQA TZXOVDZIPLKICVP
NEIHK BPDKV AMPS PPHZR WKISC
GRFFDFWBUAVMJRILOPDXOXFX

MESSAGE NO. 4

RUJJNIKGOTFEIITHQJPCCGQWZSED
HGWRYTICTVFXJTDARH

MESSAGE NO. 5

BHAEXXHELUOARBZZRBPFWZIAU
SGDxpONBJLCSTJWGNDHGGSGLP
BYUNVZUTGRGCJSYXMNFZNPLIZ
ARUVJVCPOP NQFXTRXSPXGCXC
KXCLV

MESSAGE NO. 6

XQVNMQRYDABHKLYMDGQYOHSYQ
OZSMXCLAIXWAXAVBSHACMSCHTC
WWOXXTKZSYIYQCDPXQVCAORX
PMXESSLKDLOBTYFNFGLAANATN

MESSAGE NO. 7

PGSAWOGTIQGBCUYILPHFHVILG
EDXSWAGIKUDTWTIJJTPKCNKTI
VMVXQUHKZERQTEHTJBXXUFXXX

MESSAGE NO. 8

ZUNXWKZTGC TWFDK KIOL P TZTS
OUXXX

1. The following three cryptograms have been enciphered by a cipher machine employing two primary components which are shifted according to a very long keying sequence. Each message starts at a different point in the keying sequence.

For purposes of simplification, it will be stated that the starting points of Messages No. 2 and 3 are not more than 10 intervals forward or behind the starting point of Message No. 1. Find the proper points of superimposition of these cryptograms and show the actual and expected number of coincidences for the various superimpositions you try, using diagrams such as those given in the text and specifying in each test the messages and superimposition points involved.

No. 1

V Z C Q U H O D C C R P N T X N A D I H M J X K P P X C O T
M B Z V V C A S Y Q S I K Q O P M U X X U N T F F K Y T
N N S C J Z N Z C G C K O R P Z U B S N T Y E Q L N Z E W D
Z P Q Q V X N R B X S J A G A A A U G A Y W B D G C Z F G M
U B H D A W W W K I K F I E B G N F F E 0 0 0 I L Q L X E D
L R J F P V R T M M Q T G Y C B A E H Y C E K T Q V N X O S
D N G F C W J R W C Q C A P C S I E A S S X J L A L L B J J

REF ID: A60198

Weight:

AZPLG ITPIH GSTDO GEGUP WLSMN DYFBY
UKJFH VOZLV GYXNW IVRTF IUQHV XXUCZ
FLXQW GQUVV MCUHP TBVLX CRVMO NXMWO
GBKLY XABFVRHYFZ BUURO

No. 2

BPDIN ITIWL IUOUV HMKHL EZGCUA NHSE
KJASR JPLXS NZIB WNBHP PHXGK GSST
NXJCA HJQEU RUFJV HYEIG DZQCH TBPK
KLVMW WREIV DH. HO LBHUI EBDHK ECDZP
CIHSQ LPYFR PGTZF FAOPF BHZYH TAVMC
DXNNX HFGWI YKHIW WXGOB ECMXF KEXMN
VPWFA XVFTH XTPBVI IOVFKYMY QVTUW
JFVPS AEUOOGARQK MQDDIUATVCSMGG
WTQWING GEPK MEBJZ JOXIC TOGZ CXTGH
SzETJ TZHMA VBFFT WCEOI URTOOKYZGE
MWTBE OZIPO ASKCK OYXGY QHLOWNBDZB
YRSEE TVOIL SHZCP ZHNSR PZLV KMKNR
QYUID ZLGIW XNGXH QNVOYKTAXOTNJFG
NFFKHY HZRSQ QCQCC PFCKZ BPRAX JAUME
HVSVN DJUCT LPHWD XMQQDT UQMDHFMDH
MZNSD QMNTH PIYDV STFRQ JNDFRBTYNV
DUKXP

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

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

(1) 2 1 2 2 1 1 2 2 1 4 1 3 1 9 3
   ABCDEFGHIJKLMNOPQRSTUVWXYZ

(2) 1 2 3 1 2 3 1 3 1 4 1 3 1 4 1 1 1 2
   ABCDEFGHIJKLMNOPQRSTUVWXYZ

(3) 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
   3 1 2 1 2 4 1 3 2 2 4 1 2 3

(4) 1 1 3 1 2 2 2 1 1 3 1 2 1 4 2 2 1 2 3
   ABCDEFGHIJKLMNOPQRSTUVWXYZ

(5) 1 1 1 0 2 1 1 1 2 1 1 3 1 1 2 2 2 2
   ABCDEFGHIJKLMNOPQRSTUVWXYZ

(6) 3 4 1 1 2 4 2 1 4 4 2 2 3 2
   ABCDEFGHIJKLMNOPQRSTUVWXYZ

(7) 2 2 2 4 2 1 2 3 1 3 2 2 4 2 3
   ABCDEFGHIJKLMNOPQRSTUVWXYZ

(8) 2 1 5 1 1 2 1 1 3 3 1 8 3 3
   ABCDEFGHIJKLMNOPQRSTUVWXYZ

(9) 2 1 3 1 2 1 3 1 2 3 2 1 4 2 2 3 1 1
   ABCDEFGHIJKLMNOPQRSTUVWXYZ

(10) 5 2 2 1 2 2 1 1 3 2 4 3 1 4 2
    ABCDEFGHIJKLMNOPQRSTUVWXYZ

### Table: Distribution and Monoalphabeticity

<table>
<thead>
<tr>
<th>Distribution</th>
<th>$\Phi$</th>
<th>Monoalphabetic</th>
<th>Non Monoalphabetic</th>
<th>Decision</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

1. Which distributions are monoalphabetic and which are not?
2. How many different cipher alphabets are there in the distributions classified as monoalphabetic?
3. Allocate the distributions to their respective cipher alphabets.

---

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

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

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

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

**No. 1**

11:45 P.M., 10 June.

(5) AGSUH HPRC S ARA AK OYEB LTYH DRSARK
SITLO XWQHM ADH DWE LUSX UXZ Z MGGVK
NEAGT SFUHG ODHNL DLEOQ UCRX XYL FY
MJWPJ ODF

**No. 2**

4:00 A.M., 11 June.

(5) BBIXJ NYLVG CQVVO UPKCA

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

### Problem 11 - Cryptanalysis III

**Frequency Distribution Table**

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

<table>
<thead>
<tr>
<th>Letters Arranged</th>
</tr>
</thead>
<tbody>
<tr>
<td>According to Frequency</td>
</tr>
</tbody>
</table>

\[
\begin{align*}
34 & \quad D \\
33 & \quad U \\
32 & \quad Q, Z \\
31 & \quad R \\
30 & \quad T \\
29 & \quad A, B, K, L, P \\
28 & \quad O, T \\
27 & \quad E, H \\
26 & \quad V \\
25 & \quad M, S \\
24 & \quad I, N, X, Y \\
23 & \quad I \\
22 & \quad O \\
21 & \quad E \\
20 & \quad J \\
19 & \quad C \\
18 & \quad F, W \\
17 & \quad G
\end{align*}
\]

*Military Cryptanalysis, Part III, 11-p.2a, 1938.*
DETAILS OF SYSTEM

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

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

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

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

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Letter of keyword with which encipherment of message commences</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMASS</td>
<td>1st</td>
</tr>
<tr>
<td>AMITY</td>
<td>2nd</td>
</tr>
<tr>
<td>ARROW</td>
<td>3rd</td>
</tr>
<tr>
<td>ASSAY</td>
<td>4th</td>
</tr>
<tr>
<td>AURAL</td>
<td>5th</td>
</tr>
<tr>
<td>AVAST</td>
<td>6th</td>
</tr>
<tr>
<td>AXIOM</td>
<td>7th</td>
</tr>
<tr>
<td>AZTEC</td>
<td>8th</td>
</tr>
<tr>
<td>BRICK</td>
<td>9th</td>
</tr>
<tr>
<td>BROIL</td>
<td>10th</td>
</tr>
<tr>
<td>BROOD</td>
<td>11th</td>
</tr>
</tbody>
</table>

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

Weight:

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

1) AVAST JEXTWYCKGEEXWXVICNRJGUMSF
2) AXIOMXZJORDVNHNEQPEMIHYIQEGKVI
3) AURALSJECQMYKASEECA NSFSYIXOKJ
4) ASSAYNGLWSWBYAJQO EKFiMRZ FXUEU
5) AZTECWJOKKRREZDWICHYDRRVEJLBMZ
6) AXIOMEBDJKKPQEHUMIVHNRNJEBJHE
7) ASSAYQFNEHGWFRHZJAGGHNCRSXCSSA

8) AURAL GQEBH TBWCC ISXAL MOWNK OKHUE
9) AMASS YRXDK AEYPU YGMJD SJJNX DJEGR
10) AMITY UHNWP YDLIP KUVLE DCJIA KUNJD
11) AMASS YTXQI VBWJT FUHARD EBOXT TNGCC
12) AXIOM EBDKK MBWMU YCJQD KHERES SAJCJ
13) AVAST JEXTO CABCIC TWDDX SJNDQ ESJLB
14) AZTEC VWERU ZIQZX KTKFQ DGNJW EDBER
15) ARROW FTVXL BAWBB CGXCC CJHSS ZNZJO
16) ASSAY HICYK NIFAC HJJQI PIMVS COZIC
17) AVAST JEHDC RRFIW LOVXP ORDRP SOADN
18) AVAST GEBAM ZUNIW SOALP CKEFI PCCCK
19) ASSAY HKFIR PKSVX KXXJR WHSZL BISDC
20) AMASS YTZZ JTLPM YKLFL DQCP I BIGVC
21) AURAL AJELP CRACJ DVLRH NTZTB XUMRD
22) ASSAY HIEMS DIGML REDEU KNPKE RFDSE
23) AURAL GQEKP KRUVE LEXUL CFORW PSQCP
24) AVAST JEHDC YGXX TBMJH NRZLF TOCLE
25) AURAL GQWGD TYCII CTOPX XSWCD RGVMI

2. What is the message keyword for this unit?
3. What are the keywords from which the primary components are derived?

SUBCOURSE - Military Cryptanalysis, Part III

LESSON 1 - Aperiodic keying by word lengths.

Weight:

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

T U E S D A
C O R P S A V I A T I O N R E P O R T S T H A T A T O N L

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

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

5  b. Keyword: T U 2 5 D A Y

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

P L R M A N E
G A S A T T A C K O N A I R D K O M E AT Z E R O E I G H T

N T P L R
F I F T E E N S T O P N O C A S U A L T I E S I N

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

Solutions
The primary components are as follows:

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

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

XYLOPHONE
A B C D E F G I J
K M Q R E T U V
W Z

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

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

No. 1

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

Solutions
3a. Continued:

\[
\begin{align*}
\text{E} & \quad \text{S} & \quad \text{L} & \quad \text{I} & \quad \text{D} & \quad \text{E} & \quad \text{R} \\
\text{TANKS STOP SECTOR OF OUR FIFTY FIFTH} \\
\text{AEDIXNITLMIQZKBMJPJCTQTAMAYACW} \\
\end{align*}
\]

\[
\begin{align*}
\text{U} & \quad \text{L} & \quad \text{E} & \quad \text{S} & \quad \text{L} & \quad \text{I} \\
\text{DIVISION WAS PENETRATED TO ABOUT TWO} \\
\text{RALAHAZMVLMPGDGASEAIGHITLOCKEZHLM} \\
\end{align*}
\]

\[
\begin{align*}
\text{D} & \quad \text{L} & \quad \text{R} & \quad \text{U} & \quad \text{L} \\
\text{HUNDRED YARDS STOP ENEMY ARTILLERY} \\
\text{KCEFSGSFMSHXLCVHPMPBNLBZRSSIBG} \\
\end{align*}
\]

\[
\begin{align*}
\text{E} & \quad \text{S} & \quad \text{L} & \quad \text{I} & \quad \text{D} & \quad \text{E} \\
\text{VERY ACTIVE UNTIL ZERO SEVEN HUNDRED} \\
\text{WGSMSAIZOWEAZSNRRJMTSQSECKDHSGH} \\
\end{align*}
\]

\[
\begin{align*}
\text{R} & \quad \text{U} & \quad \text{L} & \quad \text{S} \\
\text{O'CLOCK STOP OUR COUNTERATTACK BEGINS} \\
\text{VFZVFMHGZEKEBFVRKDAGSEAEEVIXWYZGN} \\
\end{align*}
\]

\[
\begin{align*}
\text{L} & \quad \text{I} & \quad \text{D} & \quad \text{L} \\
\text{AT ZERO NINE HUNDRED} \\
\text{LZNRJMEWESCKDHSGH} \\
\end{align*}
\]

No. 2

\[
\begin{align*}
\text{S} & \quad \text{L} & \quad \text{I} & \quad \text{D} & \quad \text{E} \\
\text{ENEMY ARTILLERY SHELLING OUR POSITION:} \\
\text{WGWHPLBZRSSIBGVSRWWXBJCGPRXQAQRT} \\
\end{align*}
\]

\[
\begin{align*}
\text{R} & \quad \text{U} & \quad \text{L} & \quad \text{S} \\
\text{STOP SECTOR OF FIFTY FIFTH DIVISION} \\
\text{LCVHPDGDZVKUTQTAMYZYIRNRJRMERKA} \\
\end{align*}
\]

\[
\begin{align*}
\text{I} & \quad \text{D} & \quad \text{L} \\
\text{TAKEN BY HIS TANKS} \\
\text{HIKRBRUCQXCRJMLXX} \\
\end{align*}
\]

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

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

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

For No. 1:

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

2
5
6

For No. 2:

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

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

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

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

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

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

Solutions
SOLUTIONS

SUBCOURSE - Military Cryptanalysis, Part III

LESSON 2 - Aperiodic keying by word lengths, continued.

30

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

CHARLES SULZER SHARPE MINORZ
V F U Y O X N E O W X N L D N A Q W X V Y I P Z Q H T B

INVENTORZ T U I S Z CRYPTOGRAPHICZ

SYSTEMZ RECORDEDZ W A R Z OFFICEZ
R G H S F Z V J G E O J U G U S O Z B J U Y Y Q J K C

WASHINGTONZ BANDZ LEADERZ FORTIEZTHZ
V B T W J P I E Q P A L S R E H M S N H S R Y Y U M A Q K A P O

ARTILLERYZ COASTZ ARTILLERYZ CORPSZ
X H L I Z Z C H V M L R I W J Q K F R T G Q F J Z R H T S E B

PRESIDIOZ CALIFORNIAZ MATTHEWSONZ
Y P B Q D A D K G S Q A V E C O F V Q P S D M M Y J B V T L R

COLONELZ FORMERLYZ NATIONALZ GUARDZ
V J O J W X O E T F D A L D X Y N T O X P E T O S D R L M Q B V

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

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

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

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

ANCKGERXKJDFVEVQDWPBNNLZIERWPQIZQNYVBLIMKQHYWRKQBDJDBL
YJJNIATEJPDVQZЛXFTUMPAIMRJARFQZYESKUOTMQQDKBUIL
YJEDYQDVFQGQGKGIGDCPBUVG1HJMUCZCJSOKBQEOJLOVZDVIVKLL
JNZAPDPEQQKUPBUVGI0IRJMVOMBNGFNMLKXMDMJINVL
CTYXSMFVDJQDPOPSBMIFMRRNNZBCWMIKAVLDJQXSINTDBL
YJEDGVNQZLUIUPPNCQNLUBJPLMOIZYVTIVGKLJDCWYNBL
BKTVXCKEWEFKFUQZDFI

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

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

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

d. The keyword for the message is MUSKETRY.

Solutions
The complete text is as follows:

**M U S K E T R Y**

ANCHGEHVTJEFUVIOVQDPOFBPIUZIURVPCIZQVNBILMKQHYWRKQBDJDBL

EIGHT PRISONERS FROM SEVENTY SEVENTH DIVISION INCLUDING ONE

**M U S K E T R Y**

YJJNIAEJDZDVGQLZPUMNAFIJMPYJAROFZEBYKUTMQDKBULL

OFFICER STATE THAT THEIR REGIMENT ATTACHED ON LEFT

**M U S K E T R Y**

YJEDTVFDQOSQGQIGIDQPMUQIGIIJMUQZCJSOKQUBMZOVDWVKKL

OF SIXTEENTH DIVISION STOP FIRST OBJECTIVE WAS HILL

**M U S K E T R Y**

JNZADTEQCOQKUPFLIQIIRJMZVOMBMGFMNLKXMDVWVL

FIVE TWO FIVE STOP THEIR NEXT OBJECTIVE HIGH

**M U S K E T R Y**

CTXSMFVZIJDQDSQSPQIMKMWZCZEMKAVIDQXDOSWTGL

GROUND EAST OF MARSH CREEK STOP FIRST OBJECTIVE

**M U S K E T R Y**

YJEDGTVQZGVLVVUPXAOQLUBPILOVIZYTMOVNLJDCWYNBL

OF OTHER THREE REGIMENTS NORTH AND SOUTH RIDGE

**M U S K E T R Y**

GKTXXGKEWFEKQZDFI

THROUGH ROUND TOPS

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

1 2 3 4 5 6 7 8 9 10

(A - U ON NY SF ML UT)

(B - K V DD GZ Q US KA)

(C - M DW WR LG C BM V)

(D - D Y J JB KS N UF)

Isomorphs

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

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

Solutions

Isomorphs

A&B
MUK
OV
ND
YG
ISZ
TA

Isomorphs

A&C
UMC
OD
NW
YR
SLB
FG
TV

Isomorphs

A&D
LUD
OYB
MNJ
TFSK

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

Isomorphs

A&B, A&C
CMUK
WNDVTA
JRYGFQ
BLSZ

Isomorphs

A&D
AQZ.VGLUDR.CW
TFSKOYBMNJ

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

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

\[
\begin{align*}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 1 & 0 & 11 & 2 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 1 & 1 & 2 & 3 \\
Suppose we superimpose the AQZ ... half-chain over the TFS ... half-chain so as to give values that will correspond to any one of the values given in the partial chains CMUK, WNDOVTA, JRYGFQ, or ELSZ. Thus, selecting W1 in the WNDOVTA chain:

\[
\begin{array}{cccccccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\
\end{array}
\]

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

\[
\begin{array}{cccccccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\
\end{array}
\]

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

\[
\text{WNDOVTAJRYGFQ}
\]

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

\[
\begin{array}{cccccccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\
\end{array}
\]

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

\[
\begin{array}{cccccccccccc}
N & U & O & N & N & Y & J & F & M & L & U & T & G & i & g & s & N & T & \text{ as sequent values for Zp}
\end{array}
\]

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

Solutions

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

\[
\begin{align*}
YRMLT & \quad GCTJH & \quad KPFPE & \quad BBA0E & \quad JSDDA \\
? & \quad ? & \quad ? & \quad ? & \quad ?
\end{align*}
\]

\[
\begin{align*}
VKVNU & \quad ONNYS & \quad FMLUT & \quad I \cdot TFK & \quad VDDGZ ... \\
\end{align*}
\]

Now let us work backward from a known point. It is obvious that immediately preceding the inomorph UONNYSFMLUT there is, in the plain text, a separator letter, $Z_p$. Hence $Z_p$ must be $N_c$. Therefore, the $V$ immediately preceding this $N$ cannot be a separator. The $V$ before the $K$ must be $Z_p$, the separator. If this is correct, then the $A$ immediately in front of that $V$ cannot be a separator; the $A$ in BBA0B must be the separator, $Z_p$. If this is correct, then the last of the two $F$'s in HPFIV must be the separator and not the last, since if the latter were the separator, one would have a 2-letter word with both letters identical (corresponding to BBc), which is impossible in English. By proceeding along those lines, by careful observation and deduction, the entire text can be blocked off into word lengths. Thus:

\[
\begin{align*}
YRMLT & \quad GCTJH & \quad HPF & \quad PFBB & \quad A & \quad OBSDDA & \quad V & \quad KVN \\
UONNYS & \quad FMLUT & \quad ILTF & \quad KVDGZ & \quad QUSKA & \quad OYPDV \\
XKVWN & \quad NPWOT & \quad HIYUF & \quad JBBA & \quad MDWWR & \quad LGCBM & \quad Y \\
CAQPN & \quad DPZGR & \quad NGCOST & \quad KJEFE & \quad IVZSA \\
EXXY & \quad HMGGXN & \quad DLRQT & \quad DJJJBKSNUDF & \quad PVZDA & \quad .
\end{align*}
\]

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

\[
\begin{align*}
D & \quad R & \quad O & \quad N & \quad E \\
YOURZ & \quad PLATCONZ & \quad WILL: & \quad PROCEEDZ & \quad TOZ \\
YRMLT & \quad GCTJH & \quad HPF & \quad PFBB & \quad A & \quad OBSDDA & \quad V & \quad KVN \\
\end{align*}
\]

\[
\begin{align*}
D & \quad R & \quad O & \quad N \\
GETTYSBURGZ & \quad VIAZ & \quad GETTYSBURGZ & \quad PIKEZ \\
UONNYSFMLUT & \quad ILTF & \quad KVDGZ & \quad QUSKA & \quad OYPDV
\end{align*}
\]

Solutions
Military Cryptanalysis-Part III, 2-p.6, 1938.
The primary components are:

Plain ... FEPZHDOLYIBMVLJRSCNXUGQWAKT
Cipher ... GFQXHBLSZICMUEPNDOVTARY

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

<table>
<thead>
<tr>
<th>Plain component</th>
<th>Cipher component</th>
</tr>
</thead>
<tbody>
<tr>
<td>KMNOPQRTVXYZ</td>
<td>JLMOPQRSUWVXYZ</td>
</tr>
</tbody>
</table>

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

\[
\begin{align*}
F & \quad O & \quad G \\
F & \quad I & \quad V & \quad E & \quad H & \quad U & \quad N & \quad D & \quad R & \quad E & \quad N & \quad F & \quad A & \quad N & \quad T & \quad Y & \quad R & \quad E & \quad P & \quad L & \quad A & \quad C & \quad E & \quad M & \quad E \\
A & \quad X & \quad K & \quad B & \quad Y & \quad L & \quad B & \quad L & \quad X & \quad X & \quad L & \quad G & \quad B & \quad J & \quad O & \quad B & \quad V & \quad Y & \quad Q & \quad X & \quad K & \quad R & \quad V & \quad G & \quad E & \quad C & \quad U & \quad C \\
H & \quad N & \quad T & \quad S & \quad A & \quad R & \quad E & \quad R & \quad U & \quad I & \quad Q & \quad E & \quad D & \quad T & \quad O & \quad R & \quad F & \quad I & \quad L & \quad L & \quad C & \quad U & \quad Y & \quad G & \quad X & \quad K & \quad L & \quad V & \quad A & \quad X & \quad J & \quad G & \quad D & \quad D & \quad N \\
R & \quad O & \quad M & \quad B & \quad A & \quad T & \quad U & \quad N & \quad I & \quad T & \quad S & \quad A & \quad S & \quad S & \quad O & \quad O & \quad N & \quad A & \quad S & \quad P & \quad O & \quad S & \quad S & \quad I & \quad P & \quad L & \quad E & \quad O & \quad B & \quad S & \quad S & \quad P & \quad O & \quad L & \quad E & \quad S & \quad T & \quad O & \quad P & \quad R & \quad E & \quad D & \quad Z & \quad D & \quad E & \quad Z & \quad Z & \quad D & \quad D & \quad E & \quad R & \quad Z & \quad Y & \quad Z & \quad V & \quad V & \quad F & \quad M & \quad C & \quad J & \quad V & \quad U & \quad Z & \quad Y & \quad W & \quad J \\
F & \quad O & \quad Q & \quad U & \quad E & \quad S & \quad T & \quad R & \quad E & \quad P & \quad L & \quad E & \quad P & \quad L & \quad N & \quad M & \quad O & \quad K & \quad Z & \quad D & \quad Q & \\
\end{align*}
\]


2

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

\[
\begin{align*}
\text{FOGHORN} \\
6 & \quad 1 & \quad 3 & \quad 7 & \quad 8 & \quad 15 & \quad 14
\end{align*}
\]

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

8

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

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

```
FRIDAY
```

```
POSITIONONWESTSLOPEOFAMBR
```

```
I D A
```

```
OSEHILL
```

```
WAMPLOL
```

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

Thus:

```
FRIDAY
3 5 4 2 1 6
```

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

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

```
<table>
<thead>
<tr>
<th>Line 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Z S I I F Q V Z O R V S Q Q X U T Y V L B R A A K H X Y C R I E C</td>
</tr>
<tr>
<td>COMMUNICATION</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Line 3</td>
</tr>
<tr>
<td>--------</td>
</tr>
<tr>
<td>Z S I I F Q V Z O R V S Q S F C P C N C X H H C Z C D C R I Y I</td>
</tr>
<tr>
<td>COMMUNICATION</td>
</tr>
</tbody>
</table>
```

Solutions

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

ZSIIFQVZORSQ QXUTYVLBRAAXHXY CRIEC COMMUNICATION WITH SECOND DIVISION

ZSIIFQVZORSQ SFCPC MCHHCZC DCRIIYI COMMUNICATION WITH THIRD DIVISION

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

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

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

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

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

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

M(13) O(15)
COMMUNICATION WITH SECOND DIVISION
ZSIIFQVZORSQ QXUTYVLBRAAXHXY

N(14) U(21)
IONWILLBEDISCONTINUEDUNTILJUNETHERE;
CRIECNFBHCDGRYZAYMLEMYZAUCCMYLZBKL

M(13) E(5)
COMMUNICATION WITH THIRD DIVISION UN
ZSIIFQVZORSQ SFCPC MCHHCZCDRIYI

T(20) M(13)
TILFURTHERNOTICESTOPEBGINNINGATZE
BDTENBCYSCBUDHCFBUV YUWVQVQWORKU

Solutions
Weight:

0(15) N(14)
ROZEROFIVEZEROSTRICTRADIOSILE
FBMVFBXHMVFBYSXCXSXTHCRDCNB

U(21) M(13)
NCIWILLBEOBSERVEDUNTILCONTACTWITHTHE
YTLXAUUNLGNLKOLEMYZAMZSQROZRPVRNU

E(5) N(14)
NEMYHASBEENMADESTOP
BDUNPTDFBBIQTHBDSRU

T(20) M(13)
WIRECOMMUNICATIONWILLBERESTRICTED
IDYCHURRZSDHEBDUSIDTMYUDUXRDVZRL

0(15) N(14)
TOABSOLUTEMINIMUMREQUIREMENTS
UBPZYBOGUVSKRXSYQXBVYCBQBISD

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

FAMEF
YOURBATTALIONWILLASSEMBLETABROAD
CWIEQGEROMVSQPVMMOXDUHEDEGWGU

A M EF
JUNCTIONFIVEIGHTSEVENWITH
KFQZRVSQAVGUUVOPCGDMSJHOJKJ

M EFFA
TRANSPORTATIONATFOURTHIRTYPM
RDOQXBDRSBDORSBICMVIEKYOEJBI

5
g. The keyword for Problem 3a is MONUMENT each letter of
which not only determines the secondary alphabet to be employed,

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

In Problem 3b the keyword is FAME, used in exactly the
same manner. 6 1 13 5

Solutions
Military Cryptanalysis-Part III, 3-p.4, 1938.
Weight:
30

a. From the data given it is clear that –
- Message 1 should start with NUMBERFIFTEENX,
- Message 2 should start with NUMBERTWENTYTOX,
- Message 3 should start with NUMBERSTXSEXENX.

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

From B to A

I B E R
NUMBFIFTEENXENMENYMAEHINEGUNNEST
UHOKBDQFQEHUIAUIOUMUIFSDCOQGCGOYZ

I A B E R
APTUREDSPHAVENPRISONERS
CIPHRDZB?BITCAPBUIJKXGIUOY

From C to A

I B E R
NUMBFiftWENTYTOXENEMYAINPLANEHHAVI
UHOKBDPNBFENYPGACOUMIDBRIWICOYSIP

I A B E R
LOCATEDOURCOMMANDPOSTXWILLMOVE
XJGCPBJHIGJOCUIJMEAPBVVUHPO

From A to C

I B E R
NUMBFispersXENXNEZDTWOMORECOPIESOF
UHOKBDZFMZEHUIAIUKZAUHBOFHRDOYHL

I A B E R
IVISIONFIELDCODENUMBERFOUR
FADFZIJUQFRXJGJLBTHOKGFO

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

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

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

Weight:

30

1a. Messages with their plain texts:

(1) REPORT TO CORPS
    zctpzwpcpzqxp

(2) PREPARE MOVIE
    wtoqnxzysprc

(3) NEXT TRAIN WILL
    tcrwctxnh

(4) CHIEF SIGNAL
    efkcszriha

(5) TAKE STEPS TO
    yancihznuw

(6) ORDERS WILL
    vziertirgx

(7) SEND THREE MEN
    hqickguon

(8) REFEREING TO
    zcfclxrkqw

(9) STOP NGRESIST
    hwwptewcimjs

(10) COUNTERATTACK
    epdozclksj

(11) PROMPT ORDER
    wtsqzpriet

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

(12) REGIMENT WILL
    zcggyfcbsbg

(13) ATTACK POSTPONED
    cwaaoemhwp

(14) ADVISE OUR QU
    ciygifbdtvx

(15) CANYOUOVEYOUR
    eaqdrndrsrcaptd

(16) THREEMOREERE
    yfwcqqbscvwc

(17) PREVENT ENEMY
    wtezqskuhc

(18) REQUEST OUTAKE
    zcvqskszydwlk

(19) WHENYOURBRIGADE
    afcojtdtit

(20) GOOD PROGRESS
    kpvfqwpktev

(21) RADIO NUMBER
    zabgrtxpuqx

(22) TWENTYFOUR
    yhooocuhmdt

(23) ACCORDING TO
    clcpzikoth

(24) WHATISYOUR
    aflwwzqmdt

(25) RERADIO MARCH
    scwapmslawl

(26) SHALLWE PROCEED
    hflmhrznapecei

(27) ACTIVITY INCREASING
    clzgemkzto

Solutions
Wight:

(28) NOTHINESEEN tpyfktizuh
(29) RECOMMENDTHAT zccpsnoophdyl
(30) ADVISEATONCE ciygiftyle
(31) TROOPSWILLREMAIN ytsvwdghpguz
(32) INCASEOFFAULURE nocaifbjblghy
(33) RUCHREPLACEMENTS xxxflfegjl
(34) REPLACEMENTS zctmmmbezjoo
(35) SENDINTWOSETS hcqiwysbphczv

1 b. Key for messages: CALAMITY JANE
3 c. Primary components: Plain ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher HYDRAULICBCDEFGHIJKLMNOPQRSTUVWXYZ
1 d. Interrupter: QD.

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

C. O. 95th Infantry

Plain: YOURREGIMENTWILLMOVEUPTOP
Key: MISSMISSISSIPPIIVERMISS
Cipher: JTKFLQJDLPJTJRHRPMTOKWAHCBB

Plain: OSITIONONHILLONENINEONEAN
Key: ISSIPIPERRYMISISSISSIPPIRI
Cipher: TGDHHLSSORPKHITXSDIFLUFRS

Solutions
Military Cryptanalysis, Part III, 4-p.3, 1938.
3. Same primary components as in Problems 1 and 2; each word begins with a new juxtaposition of the primary components, the keyword JAPAN being used for this purpose. The letter X is used as a word separator, and is treated as though it were an ordinary letter. Within each word the cipher component is shifted to the left after the encipherment of each letter, including the X separator. The latter then serves as a signal to shift the cipher component to the next keyletter before beginning to encipher the next word.

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

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

Plain: TRANSFEROFX WOUNDEDXTOKYO
Key: AULICBEFGPQSAULICBEFNONPJK
Cipher: VWLSHKKDDBLXOHHSHSJJCBUMFD

Plain: URXTRUCKXTRAINXFORXTTRANSF
Key: MNOLICBPQSTVWUALINOPQST
Cipher: BIKWVAHPLFESRBSBQWABCPLGH

Plain: ERXTOXHOSPITALXATXSOUTHXN
Key: VWJMKMAULICBEFGPQSAULICBN
Cipher: HKTLDFQXVNDDEVFBGOVQHHMLR

Plain: ANKINGXBLIDGEXSTOXSIMITX
Key: OPQSTVJNMOPQALICPQSTVW
Cipher: OURDCDSKUVQWNVXSVEUDKRS

Solutions
Military Cryptanalysis, Part III, 4-p.5, 1938.
1. The solution of this message requires only the use of two normal sequences, one direct, the other reversed. The usual simple steps having been tried, without success, cipher-text auto-keying is assumed. Since the initial keyletter is unknown, we may disregard the first plain-text letter of the message (which will be found easily enough later, from the context) and start with K as the keyletter. Then the 1st cipher group yields the following:

\[
\begin{align*}
K & \quad G \\
G & \quad G \\
L & \quad N \\
E & \quad A \\
V & \quad Y
\end{align*}
\]

Obviously the word is HEAVY.

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

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

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

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

The plain text of the first 20 messages follows:

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

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

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

The initial keyletters for the messages are as follows:

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

The texts of the messages are as follows:

Solutions
<table>
<thead>
<tr>
<th>Weight:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>A. CGFIRSTDIVISIONSTOPHAVEJU TRSPWGRAXGJG JCBTLK EVVLX</th>
</tr>
</thead>
<tbody>
<tr>
<td>B.</td>
<td>STRETURNSMANDPOSTFRLYLYDXZZPUMAHZKENCJTXYL</td>
</tr>
<tr>
<td>C.</td>
<td>OMHILLFIVENINETWOOCUPIEDBPYMVZBQBBFUVASKSBNVSPPM</td>
</tr>
<tr>
<td>D.</td>
<td>BYFOURTHINFANTRYSTOPENEMYTXYGWCWLJAZJAAUGRNDCCCM</td>
</tr>
<tr>
<td>E.</td>
<td>ONNORTHEISMAKINGAHEAUVYTAAHJAUPUNSDLGLJADXXXHGFZCWS</td>
</tr>
<tr>
<td>F.</td>
<td>CKONHIILSIXZEROSIXBAUVGHPTFUMKKHUXGEXX</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>G. I HAVE SENTAMACHINEGUNSECTIZSOPPRRYNPGDUNSHFLIPPPQHD</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.</td>
<td>ONEFLOMRESERVEDATTALIONFOUXYLBPUWGGETGUVAHMWDCCGID</td>
</tr>
<tr>
<td>J.</td>
<td>RTHINFANTRYTUREINFORCETROXDBQUUQHTJGDVPMWNGMHQSSFSK</td>
</tr>
<tr>
<td>K.</td>
<td>OPSONHILLIVESIXSIXSTOPCGSRMHJOFQWRLKIMWUEIGJMHYEG</td>
</tr>
<tr>
<td>L.</td>
<td>SECONDBEIGADEPERIODJJKSHBEQXEAHKNNYMHBX</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>M. SUBMITRECOMMENDATIONSFORHNHFDERRZTXXZPFLJQUEFIXK</th>
</tr>
</thead>
<tbody>
<tr>
<td>N.</td>
<td>ANDLINGCIVILIANSINYOUCHZONHJFQXZNTBTEMKSHCYSKONEOR</td>
</tr>
<tr>
<td>P.</td>
<td>EOFADVANCERINKEDHRYEE</td>
</tr>
</tbody>
</table>

Solutions
Weight:

IV.

A. CALLMEUPASSGONASYOUCANAND
   ZJDONHNDKWTGYGLCBSKOHJYBE

B. GIVEMEANESTIMATEOFTHEENEM
   GHGGUULIPUZKTETZBG-AAAPPG

C. YSITUATIONONYOURFRONT
   FVETJYNSKMHJVPIKPWDCWXXXX

V.

D. THECGWANTSALISTOFCASUALTI
   TKKLSGDCWGDOFVAUTWSDSOBSH

E. ESATFIVEPMMCNEERENCETODAY
   HCMSEVEVSVXPVWRCGLRREO\$Q

VI.

F. BRIDGEFIVEHUNDREDYARDSOOU
   JUZPCCGIACGALRGCTNPWJTFIZ

G. THEASTOFSCOTTNAEDSSTRENGT
   CFFZIBLQZD\PVUVVHCBGBBFMS

H. HENING
   CTCDFXXXX

VII.

J. SENDCOPYYOURCIRCUITATIONMA
   VVWKSRLLKSERZLPGWEAQXCTSO

K. PATONCE
   VIBLIYXXX

VIII.

L. SUBMITYOURSCHEDULEOFFLIGHT
   SEPBOZRNVDYEHBDERRNACYFW

M. TIMMEDIATELY
   PRKCIIRKETYXXX

Solutions
Weight:

IX.

A. EIGHT INCHES ARE FALLING
   EIGHT FZ GLRQZ SADCXTTL CFUW

B. INVICTAITY ROAD JUNCTION FIV
   GLZLR KMWPX TZJFX MQSFU PEI

C. EBUND REDYARDSEA STOFHERE
   EHTUDEZJUSDDK WPVOM MJXX

X.

D. ENEMY ADVANCE HAS BEEN CHECKED
   LIWQTEAPQEQAO LLYUHXX

E. DSTOPHEISD IGGINGINALONGFRI
   AOZTUNNSDQXEGHJPRVZTOYHQ

F. ONTOFBRIGADE
   JAQYRHHADEEXXX

XI.

G. SUBMIT LIST SHOWING LOCATION
   UBHZLYKNOXCATOYKSBXDiNG

H. OFELEMENTSOFIRSTBGIMADEA
   YHPPPGLYQJXMJXRGRHABEEA

J. PRESENTTIMI
   QLFFVUZKKXX

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

       ..IZNFUQGKTIZRGBSARTNKXSC
       ..ONDITIONWIRELINESNYOURAREA
IZNFUQGKTIZRBSTBXXTOCTILYFCX

The text is seen to begin with

IZNFUQGKTIZRBSEtc.
       ..ONDITIONEtc.

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

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

Solutions
Military Cryptanalysis, Part III, 5-p.6, 1938.
1. This message represents a case of simple plain-text auto-key encipherment with two normal sequences, one direct, the other reversed. The usual simple steps having been tried, without success, plain-text auto-keying is assumed. Since the initial keyletter is unknown, we may assume the first cipher letter of the message to be A, B, C, ... and try to build up text. It happens that the first plain-text letter is A, and yields ADVAN for the cipher group K X I V N.

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

<table>
<thead>
<tr>
<th>Group</th>
<th>No. of Occurrences</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC</td>
<td>9</td>
</tr>
<tr>
<td>KVHQRMH</td>
<td>2</td>
</tr>
<tr>
<td>KOA</td>
<td>4</td>
</tr>
<tr>
<td>DJZ</td>
<td>4</td>
</tr>
<tr>
<td>DJZMH</td>
<td>6</td>
</tr>
<tr>
<td>TJB</td>
<td>2</td>
</tr>
<tr>
<td>GCZ</td>
<td>3</td>
</tr>
<tr>
<td>GCZBFVIG</td>
<td>2</td>
</tr>
<tr>
<td>FCBFVBB</td>
<td>2</td>
</tr>
</tbody>
</table>

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

```
```

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

Suppose we assume:

DIVISION to be enciphered by
JKVHQRMH

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

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

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

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

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

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

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

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

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

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

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

Solutions
Suppose the word ARTILLERY is enciphered by NWUGJZPBB

Setting the Ic under Ap, we have Ip = Jc

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

which is excellent—too good to be wrong. We can also insert Kc and Lc, a very important addition as we can put Lc under Ap and use values of Zc = Ip and Pc = Hp. We have:

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

Pc checks and Zc falls into place.

Now since H and I are in the keyword, Gc might well just precede Jc. If it did, then from encipherment of Ip in ARTILLERY to be Gc, we would have Tc falling in front of Hc, forming a very high frequency digraph.

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

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

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

The plain text is:

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

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

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

The first 15 letters of the running-key text are as follows: SOMETIMESTHE:

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

1 2 3 4 5
CONSIDERTHESTESIEMPLEQUESTI
A. QASODPKASHLZEHYCTQLRQQJX
MOVEFOURBATTALIONSODCKL

A. QASODPKASHLZEHYCTQLRQQJX

B. OMEQKFUSBMAYLPQWYVDJFHTO
ABORERSIMMEDIELYTOUNLOA

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

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

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

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

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

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

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

Each succeeding secondary alphabet is derived by moving the cipher component one place to the right.
The messages and plain text follow:

**MESSAGE NO. 1**

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
INDICATIONS ARE AN EMY ATTACK
RXOW ZUZUL IKTG DFCJT GFMLR

: CKWILL BELMNCHE DEARLY TOMOR
REAHV JVSMA Y TIZG AAFWG ENNC

ROWMORNING STOPIFYOUNEDDADA
CYAEDGPAIJ NQFT GTXLKYBEOHJ

ITTONEALERT ILLERY SUPPORT ORTCOM
QQSDP PKGHUNRSUQ IRKMOUPJMCT

MAADVISEGDASHTHREE
YVWOTXDSCXCKXCPRACT
```

**MESSAGE NO. 2**

```
YOURREGIMEN
IWKWXYOKCF

TWILBERELIEVEDATFOURTOMOR
ONSFHSRFVONZKUNDYAZMZHNCC

ROW
CYA
```

**MESSAGE NO. 3**

```
GDASHFOURCOMMAS ECOND CORPSC
WLWTLQHCNMQRYONDJYJGUVGQ

RFIVEFIVEFOURANDROADJUNCT
CJSTOOZDVVMBMYDASXHCQOMLO

ONTWONINENINEARUNDEERCONST
TWRCUEZNVCNTPYQNJHTTZKQG

ANTIINTERDICTIONBYENEMYSART
SWRVPWRFWGANCRDCTCJTGFPONM

ILLERYSTOPITMAYBENECESSARY
QDEMBVZKYNNRYCCAHHYZPONL

TOROUTEANIMALDRAWNVEHICLE
OYTDGWARGJOISQDHOSTIJLIF
```

Solutions

MESSAGE NO. 3 (Continued)

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

MESSAGE NO. 4

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

MESSAGE NO. 5

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

Solutions
REF ID: A60198

MESSAGE NO. 6

THE COMMANDING GENERAL
X Q V N M Q R Y D A B H K L Y M D G Q Y

THIRD FIELD ARTILLERY Will CON
O H S Y Q O Z S M X C L A I W X A V B S H A C M C S

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

T I N G F I R E FOR OUR ATTACK TOMORROW
O R X P M X E S S L K O D O B T Y F F N F G A A N A

OW
TN

MESSAGE NO. 7

A N E N E MY AIRFIELD HAS BEEN
P G S A W O G T I Q G B C U Y I L P H F H

N R E P O R T E D A T AVEN TO BE ACTING SC H S T O P

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

MESSAGE NO. 8

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

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

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

   (1) KDGIOTPLOSKWAP...
   (2) BPDINIIJWLI...
   (3) CHUVOXBD...

The data for all tests are shown below:

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

Solutions
Weight:

<table>
<thead>
<tr>
<th>Relative Settings Message</th>
<th>No. of Coincidences</th>
<th>Relative Settings Message</th>
<th>No. of Coincidences</th>
</tr>
</thead>
<tbody>
<tr>
<td>#2</td>
<td>#3</td>
<td></td>
<td>#2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>15</td>
<td>475</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>15</td>
<td>474</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>18</td>
<td>473</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>22</td>
<td>472</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
<td>12</td>
<td>471</td>
</tr>
<tr>
<td>1</td>
<td>6</td>
<td>21</td>
<td>470</td>
</tr>
<tr>
<td>1</td>
<td>7</td>
<td>14</td>
<td>469</td>
</tr>
<tr>
<td>1</td>
<td>8</td>
<td>15</td>
<td>468</td>
</tr>
<tr>
<td>1</td>
<td>9</td>
<td>23</td>
<td>467</td>
</tr>
<tr>
<td>1</td>
<td>10</td>
<td>19</td>
<td>466</td>
</tr>
</tbody>
</table>

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

(1) KDGIOJTPLOSKWAPHUCBCJYMCS
REPORTOFAIRRECONNAISSANCE

(2) BPDINIJJWLIUVHMKHEL
ENEMYOBservATIOnPOSTS

(3) CHUVOXBDBOCYMNLUQF
SECONDbATTALIONFOR

Solutions
SUBCOURSE  - Military Cryptanalysis, Part III.

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

Weight:

40 1a. All the distributions have 35 letters each. For plain text, the value of \( E(\phi) \) is \( 0.0667 \times 35 \times 34 = 79 \); for random text \( E(\phi) \) is \( 0.0385 \times 35 \times 34 = 46 \). The midway point between 79 and 46 is 62.5. Consequently we may begin by saying that any distribution which gives a value for \( \phi \) which is 63 or more will tentatively be classified as being monoalphabetic; any distribution which gives a value which is below 63 will tentatively be classified as being not monoalphabetic. Accordingly, the results of this first examination are as follows:

<table>
<thead>
<tr>
<th>Distribution</th>
<th>( \phi )</th>
<th>Monoalphabetic</th>
<th>Non Monoalphabetic</th>
<th>Decision</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Surely</td>
<td>Probably</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>106</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>54</td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>64</td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>4</td>
<td>44</td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>5</td>
<td>108</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>70</td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>7</td>
<td>58</td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>8</td>
<td>104</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>48</td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>10</td>
<td>68</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

60 1b. To answer the questions asked we could begin by testing only the distributions which were classified under a above as being "surely monoalphabetic", and then add to the data thus obtained the results of testing the distributions whose classification

Solutions
is indicated as probably correct and then treating the distributions whose classification is in doubt. But we might as well systematize the work and make all the tests at once. Moreover, it is possible that the $X$-test may corroborate or substantiate the results obtained from the $\Phi$-test; the $X$-test may even cast some doubt upon the accuracy of the results obtained from the $\Phi$-test in certain cases. Hence, we draw up a diagram as follows:

RESULTS OF $X$-TEST

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>52</td>
<td>64</td>
<td>29</td>
<td>46</td>
<td>56</td>
<td>85</td>
<td>119</td>
<td>74</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>38</td>
<td>52</td>
<td>32</td>
<td>47</td>
<td>44</td>
<td>44</td>
<td>38</td>
<td>43</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>40</td>
<td>76</td>
<td>81</td>
<td>64</td>
<td>65</td>
<td>55</td>
<td>78</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>57</td>
<td>48</td>
<td>68</td>
<td>46</td>
<td>36</td>
<td>49</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>82</td>
<td>66</td>
<td>45</td>
<td>34</td>
<td>88</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>51</td>
<td>60</td>
<td>45</td>
<td>81</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>87</td>
<td>86</td>
<td>65</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>77</td>
<td>53</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>48</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Since all the distributions have 35 letters each, the values of $X$ for plain text and for random text are:

$$X_p = 35 \times 35 \times 0.0667 = 81.7075 = 82$$

$$X_r = 35 \times 35 \times 0.0385 = 47.1625 = 47$$

The midway point between the two values is 64.5. Examining the values of $X$ for the various comparisons shown in the diagram above we may set down the following reasoning:

Examining the first line in this diagram, we may say that distributions 1 and 8 are certainly similar and belong to the same monoalphabet ($X=119$); distributions 1 and 7 ($X=85$) most probably belong to the same monoalphabet, too, in which case 1, 7, and 8 are similar and belong together. If this is correct then 7 and 8 when tested against each other should give a high value for $X$. Reference to the table shows that $X$ in this case equals 87, which corroborates the idea that 1, 7, and 8 belong together. Returning to line 1 of the diagram, the values of $X$ for distributions 1-9 and 1-10 are 74 and 50, respectively.

Solutions
The first of these values is considerably above the midpoint value (64.5) and we may feel that there is good evidence for thinking that distribution 9 also belongs to the same monophonic alphabet with 1, 7, and 8. Furthermore, if 9 does belong with 1, 7, and 8, then the X values for 7-9, and 8-9 should be high. They are 66 and 77, respectively. The value 77 for the combination 8-9 is high enough to be considered as substantiating the idea that 9 belongs with 1, 7, and 8, but the value for the combination 7-9 is pretty low and casts some doubt upon the matter. However, let us assume tentatively that 1, 7, 8, and 9 belong together. As for distribution 10, it hardly looks as though it belongs with 1, 7, 8, and 9; moreover the X values for 7-10, 8-10, and 9-10 should be low. They are 65, 53, and 48. Those certainly corroborate the idea that distribution 10 does not belong with 1, 7, 8, and 9.

Still referring to line 1 of the diagram, we may say that distributions 1 and 4, with X = 29, are certainly not alike. But we have already concluded in a above that distribution 4 is "surely not monophonic." Obviously, if distribution 4 is non monophonic it cannot be similar to distribution 1, which is monophonic. Next we consider 1 and 5, with X = 46. Now in the test distribution 5 gave a very high value (108) so that there can be no doubt about its being monophonic. Hence, the low value of X, when 1 and 5 are compared, must be due to a dissimilarity in monophonicity, and we conclude that distributions 1 and 5 belong to different monophonic alphabets.

Likewise, as regards distributions 1 and 6 (X = 56) we conclude that they belong to different monophonic alphabets. Thus we have reached the conclusion that 1 and 5 are different, and that 1 and 6 are different. Now look at the value of X for combination 5-6; it is 82, indicating that distributions 5 and 6 are similar.

We have now disposed of those distributions:

Nos. 1, 7, 8 and 9 belong together
Nos. 5, 6
No. 4 is not monophonic.

There remain distributions 2, 3, and 10 to be classified.

Now 1 and 2 do not go together, since X = 52. But from our work under a above, distribution 2 was classified as "probably not monophonic." Hence, the X test corroborates that conclusion. This is further substantiated by the fact that distribution 2 when tested against all the other distributions (line 2 of the diagram) shows low X values throughout. So we have disposed of distribution 2; it is surely not monophonic and does

Solutions
not belong with either the 1-7-8-9 group or the 5-6 group.

As for distribution 3, it gives a fairly high value for \( X \) when tested against distributions 5 and 6 (76 and 81, respectively). It also gives a fairly high value when tested against distribution 10 (\( X = 78 \)). Do 3, 5, 6, and 10 go together? Note the values:

\[
\begin{align*}
X \text{ for } 3-5 & = 76 & X \text{ for } 5-6 & = 82 \\
" 3-6 & = 81 & " 5-10 & = 88 \\
" 3-10 & = 78 & " 6-10 & = 81
\end{align*}
\]

The foregoing leaves no doubt that 3, 5, 6, and 10 are similar distributions.

All distributions have now been accounted for, with the following conclusions:

1. Distributions 1, 3, 5, 6, 9, and 10 are monalphabetic; 2 and 4 are not.

2. There are but 2 monalphabets represented among the 8 distributions which are monalphabetic.

3. Distributions 1, 7, 8, and 9 belong to one of these monalphabets; distributions 3, 5, 6, and 10 belong to the other.

Solutions
It is clear that the message involves 26 secondary cipher alphabets employed in progression. Transcribing the text in lines of 26 letters, a distribution is made of the cipher letters with reference to the columns in which they appear. This yields the distribution square which has already been furnished.

By using this distribution square it becomes possible to build up the primary cipher component by successively matching pairs of distributions, and applying the X-test. We begin with the D and U distributions, since they have the most data. The expected value of $X$ is: $34 \times 33 \times 0.0667 = 74.8$. None of the juxtapositions of the two distributions gives a cross-product sum that approximates 75; the juxtaposition giving the greatest value for $X$ is as follows:

$$
\begin{array}{cccccccccccc}
D & 1 & 1 & 2 & 3 & 0 & 4 & 1 & 0 & 1 & 1 & 0 & 2 \\
U & 0 & 0 & 1 & 1 & 0 & 4 & 1 & 0 & 2 & 1 & 0 & 0 \\
\end{array}
$$

Other products:

$$
\begin{array}{cccccccccccc}
d & 0 & 2 & 3 & 0 & 1 & 6 & 1 & 0 & 2 & 1 & 0 & 6 \\
\end{array}
$$

Sum of cross-products $(X) = 61$.

But there are several juxtapositions which give values close to this, so that it is inadvisable to assume without further corroboration that this juxtaposition is the correct one.

The next largest distribution is that for Q. This distribution is tested against the D and the U distributions separately and then against the two distributions combined at the various possible juxtapositions. By such procedure it becomes easy to pick out the correct juxtaposition from among several possibilities.

The final result is that the following sequence is constructed:

$$
1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9 \ D \ 11 \ 12 \ 13 \ E \ 15 \ 16 \ 17 \ B \ 19 \ 20 \ 21 \ 22 \ 23 \ 24 \ 25 \ 26
$$

Solutions

The cipher text can now be converted into monoalphabetic terms and solved as a monoalphabetic substitution cipher, whereupon the plain component can be constructed. It is found to be as follows:

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

These two primary components were derived from the following transposition rectangles:

\[
\begin{array}{cccccc}
6 & 5 & 3 & 4 & 2 & 1 \\
Z & Y & M & O & L & E \\
A & B & C & D & F & G \\
H & I & J & K & N & P \\
Q & R & S & T & U & V \\
W & X & & & & \\
\end{array}
\]

\[
\begin{array}{cccccc}
6 & 5 & 3 & 4 & 2 & 1 \\
T & R & O & K & E & Y \\
A & B & C & D & F & G \\
I & J & L & M & N & P \\
U & V & W & X & Z & \\
& & & & & \\
\end{array}
\]

The solution is as follows:

MOVEMENT OF THREE HUNDRED SECO
OB D Z R D RUA J P O D B J R Y Y D R A O X Y X W

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

O NE HUNDRED FIFTY FIVE M H O W I T
R X N E W W T E OU V Z H N K A O A Q F N Q O U S J

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

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

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

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

N C T I O N S I X Z E R O F O U R D A S H D P A R E

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

Solutions
Solutions
MOVEMENT INTO TWELFTH DIVISIONS
OBDZRDREVPLRHTKBKULARMJCKL

2. By "deciphering" the first few letters (that is, setting the reconstructed cipher component against the reconstructed plain component at any point and converting the cipher letters into their plain-component equivalents, sliding the cipher component one space to the left each time), and then completing the plain-component sequence, the first word of the message is found to be RADIO. This gives the correct initial juxtaposition of the two components and the entire message can now be read without further delay. It is as follows:

\[
\begin{align*}
\text{RADIO SILENCE} & \quad \text{UNIT LFLUR THERMS NOTICE} \\
\text{AGSUH} & \quad \text{RPRCS ARAAK OIYEB LTYHD R} \\
\text{STOP} & \quad \text{HENLIFT EDTERIC HANGL HE PRIMA} \\
\text{SITLO XWHNM ADHDW ELUSX UUXZZ MGGVK} \\
\text{RYCOMFONENTSANDUSEUNTILNEWKEYS} & \quad \text{NEAGISFUHGOHDHNL DLEOO QU} \\
\text{REACHYOU} & \quad \text{XRYY} \\
\text{MJWPJODF} & \\
\end{align*}
\]

The text of this message then shows what must be done in order to read No. 2. When the primary components are interchanged and the principle explained above is then applied, the message is found to read as follows:

\[
\begin{align*}
\text{ATTACK} & \quad \text{BEGIN SATF IVEAM} \\
\text{BBI} & \quad \text{IXJNYLVCQVVOUPKCA} \\
\end{align*}
\]

3. Problem 2 illustrates the grave danger of communicating, by radio or any other interceptible agency and especially by means of a current cipher system and cipher key, the key to a future message or set of messages. Current ciphers and keys should never be used for such a purpose; nor should such information be communicated by means susceptible of interception.

Solutions
The first step is, of course, to superimpose the messages properly. This can readily be done by means of the message indicators. Also, since the indicators give the various starting points, the number of different indicators should correspond with the length of the keyword employed by the stations within the net. Only 8 different indicators appear and hence it is safe to assume a key of 8 letters. The superimposition diagram is shown in Fig. 1. Since there are 32 columns we may mark off the varying keying "blocks" (i.e., permuted arrangements of the 8-letter cycles) as shown at the top of Fig. 1.

Frequency distributions are then made for the individual columns of the superimposition diagram, beginning with column 4 and ending with column 29. (Columns 1-3, 30-32 contain so few letters they may be neglected.) The distributions are shown in Fig. 2.

The next step is to apply the X-test to these distributions for the purpose of combining those which belong to the same cipher alphabets in order to facilitate the analysis of the latter. The process is likely to be a laborious one and we prepare a table so as to systematize the work. In this table there are pairs of lines, the upper one of each pair giving the expected values of X, the lower one the actual values for each test. Whenevver we find a case wherein the actual value is high, indicating a possible similarity in the two distributions being tested, we mark it by an asterisk or by underlining it. The result is shown in Table 1, which forms the basis for the analysis of the data from the X-tests.

In order to eliminate possible aberrations in frequency occasioned by the presence of words repeatedly occurring at the beginning of messages, we may start our analysis with column 9, the first column in the second cycle of the key. Immediately we note the high value of X for the matching of columns 9 and 19 (X = 55, whereas the expected value is 42). Also, in this same pair of lines we note the value of X for
combination 9-29 (X = 36, expected value 25). Let us, then, assume that 9, 19, and 29 belong to the same cipher alphabet. If 9, 19 and 29 are really similar, then the X-test for the combination 19-29 should yield a high value. It is 34, whereas the expected value is only 25. Thus we find excellent corroboration for assuming that columns 9, 19 and 29 belong to the same cipher alphabet. We may now look for that column among columns 1 to 8, inclusive, which belongs with 9, 19 and 29. Of course, it may be that column 1, or 2, or 3 belongs in that group but if it does we cannot test the idea because these columns contain so few letters. So we can only start with column 4. The matching of columns 4 and 9 gives a close approximation to the expected value (X = 15, expected value 17) but the values for 4-19 and 4-29 are so low as to make it certain that 4 does not belong with 9-19-29. Columns 5 and 9 certainly do not belong together. But columns 6 and 9 give a high value for X; moreover, the combinations 6-19 and 6-29 give excellent corroboration for the amalgamation of 6-9-19-29. If this is correct we have isolated from among all the 29 columns four which belong in the same cipher alphabet; moreover, we have one representative of this alphabet in each cycle of the key -- which is as it should be.

Now take column 10. There are several candidates for combination with it, so many, indeed, that we are going to have to be very careful. Columns 10-12 give a value of 40; 10-18, a value of 45; 10-22, a value of 36; columns 10-21, a value of 30. None seems to be really outstanding; if we take the combination 10-18 we cannot corroborate its correctness. Let us, therefore, suspend judgment on this column for a few minutes.

Take column 11; certainly it goes with column 24. Now see how good a value the combination 8-11 gives as against 4-11, 5-11, or 7-11 (column 6 can be passed over since it has already been classified with columns 9, 19, 29). Let us assume that 8, 11, and 24 belong together. Then 8-24 should give a high X-value; it is 38, not as high as we would like to have it, but not bad, since it is only 4 points below the expected value. However, notice how much lower the other values are in this same line of data for the combination of column 8 with most of the other columns. For these reasons we may regard it as fairly well established that columns 8, 11, and 24 belong together; moreover, that the alphabet to which they pertain is not represented in the section containing columns 25-29.

Next take column 12. Here is an excellent case presenting no difficulty. It obviously goes with columns 18 and 28. Corroboration is immediately seen in the high value for the matching of 18 and 28 (expected value 33, actual 46). Does column 4, or 5, or 7 belong in this group? Certainly neither 4 nor 7 does; but 5 may,

Solutions
Weight:

for its value, 23, is quite close to the expected value, 25. However, 5 and 14 give a better match, so that we cannot assume 5 belongs with 12, 18, and 28. Let us be content at this point to group only 12, 18, and 28, leaving 5 for further consideration.

Thus far, we have definitely tied together the following columns:

<table>
<thead>
<tr>
<th>Group 1</th>
<th>6-9-19-29</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot; 2:</td>
<td>8-11-24</td>
</tr>
<tr>
<td>&quot; 3:</td>
<td>5-12-18-28</td>
</tr>
</tbody>
</table>

Looking these over we note that we have allocated several columns which are adjacent. Perhaps we can dispense with further X-tests if we have enough data to solve these adjacent columns. Specifically we note that columns 5, 6, 8 and 9 fall within the three groups of columns definitely combined. Therefore, if we can find the group into which column 7 falls we will have 5 adjacent columns, with more than enough data in the respective alphabets to permit of solution of these alphabets. Consequently, let us study column 7 and see what we can do with it.

Certainly column 7 belongs with 17. Columns 15 and 16 with values of 64 and 62 respectively also appear to belong in the same group with 7 and 17. But there are several more candidates: columns 23 (X = 44), 26 (X = 50), 27 (X = 58), and 28 (X = 33). Testing columns 15, 16, 23, 26, 27, 28 against column 17, it becomes clear that only columns 15 and 27 belong with 7 and 17. Thus we have again found a group of 4 columns which go together, with a representative in each keying block.

We have four groups of alphabets with the following columns in each group:

| Group 1 | 5-12-18-28 |
| " 2: | 6-9-19-29 |
| " 3: | 7-15-17-27 |
| " 4: | 8-11-24 |

The respective small distributions are now combined to yield four larger distributions which can be solved by recourse to principles of frequency and indirect symmetry. These distributions are shown below in Fig. 3.

Solution
Obviously in alphabet 3, $E_0 = E_p$. The repeated pentagraph $EBDKK$ in messages 23 and 24, beginning with $E_p$ certainly seems to be $ENEMY$, with $D_0$ in column 9 (alphabet 2) equalling $E_p$, which is corroborated nicely by the frequency of $D_0$ in that alphabet. Also, $B_0$ in alphabet 4 is $N_p$ and the frequency of $B$ is excellent. Once an entering wedge of this kind has been forced into the problem, the rest follows without difficulty.

A reconstruction diagram for the recovery of the cipher component is drawn up and the following sequence is reconstructed:
Cipher comp.: N A J V O B L W S C P X G H U I F T K E R Z M D Q Y

which is seen to be derived from the key NO SMOKING:

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

The plain component is then quickly recovered:

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

which is seen to be derived from the key POSITIVELY:

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

The keyword for the unit whose messages have been solved is CONSIDER.

The letter-for-letter solution of the messages is as follows:

1) REQUIRE TWENTY MINUTE ADVANCE
AVAST J E X T W Y C K G B E B X W X V I C N R J G U M S F
2) THREE MINUTES AFTER RECEIVING
AXIOM X Z J O R D V N H N E Q P E M I H Y I Q E G K V I
3) FRESH TROOPS NEEDED HERE IN OR
AURAL S J E C Q M Y K C A S E E C A N S F S Y I X O K J
4) WOMEN IN CHARGE OF STRAGGLERS
ASSAY N G L W R S W B Y A J Q O E K F I M R Z F X U E U G A
5) ARE YOU READY TO OBSERVE FORTH
AZTEC W J O K K R R E Z D W I C H Y D R R V E J L B M Z
6) ENEMY OBSERVATION PLAN EC RAS
AXIOM E B D K K K P O E H U M I V H N R J E E Y J H E
7) CHIEF SIGNAL OFFICER REQUEST
ASSAY Q F N E H G W F R H Z J A G G H N C R S X C S S A
8) WHEN CAN YOU GET TO GETTYSBURG
AURAL G Q E B H T B W C C I S X A L M O W N K O K H U E

Solution
REF ID:A60198

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

Solution
Military Cryptanalysis, Part III, 12-p.6, 1938.
<table>
<thead>
<tr>
<th>Cycle or &quot;Keying Block&quot;</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Column</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>1.</td>
<td>Y T X Q I V B W J T F U H A R D E O D X T N G C C</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>Q F N E H G W F R H Z J A G G H N C R S X C S S A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td>H I C Y K N I F A C H J J Q I P I M V S C O Z I C</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Solution
Military Cryptanalysis, Part III, 12, p7, 1938
<table>
<thead>
<tr>
<th>Column</th>
<th>N</th>
<th>4 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</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>5 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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6 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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7 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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8 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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9 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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10 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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11 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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12 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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>13 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</td>
</tr>
</tbody>
</table>

**Solutions**

Military Cryptanalysis, Part III, 12, p.8, 1938
Column


17 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 25


20 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 25


22 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 25


Solutions
Military Cryptanalysis, Part III, 12, p.9-1938
<table>
<thead>
<tr>
<th>Column</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>26 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 22</td>
<td></td>
</tr>
<tr>
<td>27 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 21</td>
<td></td>
</tr>
<tr>
<td>29 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 15</td>
<td></td>
</tr>
</tbody>
</table>

Solutions
Military Cryptanalysis, Part III, 12:p.10, 1938
<table>
<thead>
<tr>
<th>Column</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
<th>19</th>
<th>20</th>
<th>21</th>
<th>22</th>
<th>23</th>
<th>24</th>
<th>25</th>
<th>26</th>
<th>27</th>
<th>28</th>
<th>29</th>
</tr>
</thead>
<tbody>
<tr>
<td>Column</td>
<td>N'</td>
<td>15</td>
<td>20</td>
<td>23</td>
<td>25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 N/10</td>
<td>10</td>
<td>13</td>
<td>15</td>
<td>17</td>
<td>17</td>
<td>17</td>
<td>17</td>
<td>17</td>
<td>17</td>
<td>17</td>
<td>17</td>
<td>17</td>
<td>17</td>
<td>17</td>
<td>17</td>
<td>17</td>
<td>17</td>
<td>15</td>
<td>14</td>
<td>13</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6 20</td>
<td>31</td>
<td>33</td>
<td>33</td>
<td>33</td>
<td>33</td>
<td>33</td>
<td>33</td>
<td>33</td>
<td>33</td>
<td>33</td>
<td>33</td>
<td>33</td>
<td>33</td>
<td>33</td>
<td>33</td>
<td>33</td>
<td>29</td>
<td>28</td>
<td>27</td>
<td>20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8 25</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>37</td>
<td>35</td>
<td>33</td>
<td>25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9 25</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>37</td>
<td>35</td>
<td>33</td>
<td>25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 25</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>37</td>
<td>35</td>
<td>33</td>
<td>25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11 25</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>37</td>
<td>35</td>
<td>33</td>
<td>25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12 25</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>37</td>
<td>35</td>
<td>33</td>
<td>25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13 25</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>37</td>
<td>35</td>
<td>33</td>
<td>25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14 25</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>37</td>
<td>35</td>
<td>33</td>
<td>25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15 25</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>37</td>
<td>35</td>
<td>33</td>
<td>25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16 25</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>37</td>
<td>35</td>
<td>33</td>
<td>25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
<td>28</td>
<td>29</td>
<td></td>
</tr>
</tbody>
</table>

Solution
Military Cryptanalysis, Part III, 12.-p.11, 1938
<table>
<thead>
<tr>
<th>Column</th>
<th>N</th>
<th>15</th>
<th>20</th>
<th>23</th>
<th>25</th>
</tr>
</thead>
<tbody>
<tr>
<td>17 25</td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td>18 25</td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td>19 25</td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td>20 25</td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td>21 25</td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td>22 25</td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td>23 25</td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td>24 25</td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td>25 25</td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td>26 22</td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td>27 21</td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td>28 20</td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td></td>
<td>42</td>
<td>42</td>
<td>42</td>
<td>42</td>
</tr>
</tbody>
</table>

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