

EXTENSION COURSE of the ARMY SECURITY AGENCY

SUBCOURSE 20-6

MILITARY CRYPTANALYSIS, PART 1
MONOALPHABETIC SUBSTITUTION SYSTEMS

~~RESTRICTED~~ Dissemination of restricted matter.--No person is entitled solely by virtue of his grade or position to knowledge or possession of classified matter. Such matter is entrusted only to those individuals whose official duties require such knowledge or possession. (See also paragraph 23b, AR 380-5, 6 March 1946.)

HEADQUARTERS, ARMY SECURITY AGENCY

JUNE 1947

~~RESTRICTED~~

**EXTENSION COURSE OF THE ARMY SECURITY AGENCY
SUBCOURSE 20-6, MILITARY CRYPTANALYSIS, PART I
MONOALPHABETIC SUBSTITUTION SYSTEMS**

Security Considerations.

This course and the accompanying text have been ~~classified RESTRICTED~~ to facilitate their dissemination to extension students of the Army Security Reserve. Nevertheless, this material is to be safeguarded in the same manner as ~~CONFIDENTIAL~~ matter, and every precaution will be taken to prevent disclosure to unauthorized personnel.

Introduction.

This is the first of a series of subcourses on the science of military cryptanalytics. The purpose of this subcourse is to teach the student the methods of analysis of systems which form a basis for the more simple military cipher systems. An understanding of these principles is necessary to grasp the advanced cryptanalytic techniques employed in the attack on the complex systems which comprise present-day military cryptography.

The scope of this subcourse is: fundamental principles; uniliteral substitution; polyliteral substitution; polygraphic substitution; and miscellaneous monoalphabetic substitution systems. It consists of nine lessons and an examination as follows:

- Lesson 1, Fundamental principles; frequency distributions.
- Lesson 2, Uniliteral substitution with standard cipher alphabets.
- Lesson 3, Uniliteral substitution with mixed cipher alphabets.
- Lesson 4, Polyliteral substitution with mono-equivalent cipher alphabets.
- Lesson 5, Polyliteral substitution with poly-equivalent cipher alphabets.
- Lesson 6, Polygraphic substitution: 4-square and 2-square matrices.
- Lesson 7, Polygraphic substitution: Playfair systems.
- Lesson 8, Polygraphic substitution: quadricular tables.
- Lesson 9, Miscellaneous monoalphabetic substitution systems.

Examination.

30 credits are allowed for the subcourse. You will not be limited as to the number of hours you may spend in the solution of the subcourse, any lesson, or the examination. For statistical purposes you are required to enter the number of hours spent on solution in the answer sheet.

Texts and materials furnished:

- Military Cryptanalysis, Part I (1942).
- *Appendix 2 (November 1946).
- *TM 11-484, Elementary Military Cryptography, March 1945.
- *TM 11-485, Advanced Military Cryptography, 8 June 1944.
- *Strip device (ASA Training Aid No. 1).

~~RESTRICTED~~

~~RESTRICTED~~

*Printed and blank alphabet strips (Training Aid No. 2).
Cross-section paper.

*This material may be retained upon completion of the subcourse. No other materials are required.

This course was prepared under the direction of the Chief, Army Security Agency.

Special Instructions.

So far as practicable, detailed work sheets which usually form a part of the solution should be submitted with the solutions. In all the lessons of this subcourse, it is required that the student recover all the cipher and plain text alphabets used. He will also be required to state the method of operation of each system and give the keys upon which each component is based. The specific keys and any cipher table employed must be recovered.

~~RESTRICTED~~

~~RESTRICTED~~

**EXTENSION COURSE OF THE ARMY SECURITY AGENCY
LESSON ASSIGNMENT SHEET**

SUBCOURSE 20-6	Military Cryptanalysis, Part I
LESSON 1	Fundamental principles; frequency distributions
CREDIT	3
TEXT ASSIGNMENT	Text, Sections I to IV, inclusive; attached memoranda
MATERIALS REQUIRED	Cross-section paper of ¼ inch squares
SUGGESTIONS	None
EXERCISES	
Weight	

- 4 1. What four fundamental operations are involved in the solution of practically every cryptogram?
- 2 2. In the solution of cryptograms involving a form of substitution to what simple terms is it necessary to reduce them in order to reach a solution?
- 2 3. Is it always necessary to determine the specific key in order to reconstruct the plain text?
- 10 4. Using cross-section paper prepare a uniliteral frequency bar distribution of the letters of the following paragraph:

"The shortest and surest way to live with honor in the world is to be in reality what we would appear to be; all human virtues increase and strengthen themselves by the practice and experience of them."
- 2 5. *a.* What percent (in round numbers) of the letters in English telegraphic text are *E*'s?
- 2 *b.* What are the four most frequent consonants in English telegraphic text?
- 2 *c.* What are the four most frequent digraphs in English telegraphic text?
- 2 *d.* Account for the discrepancies between frequencies of letters in English literary text and English telegraphic text.
- 4 6. What four facts can be determined from a study of the uniliteral frequency distribution of a cryptogram?

~~RESTRICTED~~

~~RESTRICTED~~

5 c. GXYVL ZXMXS LOZGR WEJLX PWTkZ
 GMXLW QIVZW QBRXK KTDVL MXAEX
 VHMXA LOTLY TKDWX GBQKQ LWZXG
 RTYYZ KTOXG AWXLQ LOZGR XVWGQ

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

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

5 a. ANVOR LOUNQ RLEZW ZHNEZ WZBOR
 ZKYLFAOZSO ONORF PJZPP LDZDN
 LRZLB LABWZ HNAPO WQHOO RZIZU

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

5 b. ESPAP LVDLY OECZF RSDTY ESTDO
 TDECT MFETZ YBFTN VWJTO PYETQ
 JTELD OTCPN EDELY OLCON TASPc

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

5 c. PYHYL XOLWY JJVYX OILYR YQYPJ
 KNYLK YHYLC PAYAC LYXIR QYJVO
 ZKoxC PCREK UKUPJ IUJUO PRIAS

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

~~RESTRICTED~~

~~RESTRICTED~~

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

I. Time intercepted 1612 by HS WFF V LDC

GR 35 BT
 NR 17 DYBIE DUFTO AMEJA KIBON
 SGC OY FOBAK DODLA LUFYD KAWAL
 APAYN CODAP KEDUR JOPID JENOX
 MEHAZ LOGIS KUTEG EVAUK IPBEM
 KEHZA HOBWE AVDUZ FOFA _ EMCOZ
 EGBLO DOFYO ENC _ _ MAWEN _ _ _ _ _
 _ _ _ _ _

II. Time intercepted 1610 by MR MFF V LDC

GR 35 BT
 NRI _ DYBIE BUFTO AMEJA KIBON
 IPKO _ F _ BAK DODLA LUFYL KAWAL
 APAYN _ _ _ _ _ DUA _ _ PID JENOX
 NEHAZ LOGIS KUTEG EVAUC IRBW
 KEHZA SOBWE VADUZ FOFET EMCOZ
 EGBLO DOFYO AECDA MAWEN _ _ _ OM
 EMCOZ ACFAH LOFIR 0935

III. Time intercepted 1612 by YG WFF V LDK

GR _ _ BT
 NR 17 DYBIE DUFTO AMEJA KSBON
 IPCOY _ _ _ A _ DO _ _ _ LUFYL KAWAL
 APETYN CODAP KEDUR WOPID JENOX
 MEHAZ LOGHKUTEG EVAUK IPBEM
 KEHZA HOBWE AVDUZ FOFET EMCOZ
 EGBLO DOFYO ENCOA MAWEN MAWEN
 EXFOM EMCOZ ACFAH LOFIR 0935

~~RESTRICTED~~

~~RESTRICTED~~**MEMORANDUM ON TRAFFIC INTERCEPTS**

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

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

3. In all intercept activities where operators are used for copying the traffic, one of the most likely errors to be found is caused by the human error in reception. For this reason cryptanalysts and their assistants should be familiar with the Morse telegraph alphabets and the most common errors of wire and radio transmission methods so as to be able to correct garbled groups when they occur. In this work reference is made to the table given on page 82 of TM 11-484 (Elementary Military Cryptography).

~~RESTRICTED~~

~~RESTRICTED~~

EXTENSION COURSE OF THE ARMY SECURITY AGENCY
LESSON ASSIGNMENT SHEET

SUBCOURSE 20-6
LESSON 2

Military Cryptanalysis, Part I
Unilateral substitution with standard
cipher alphabets

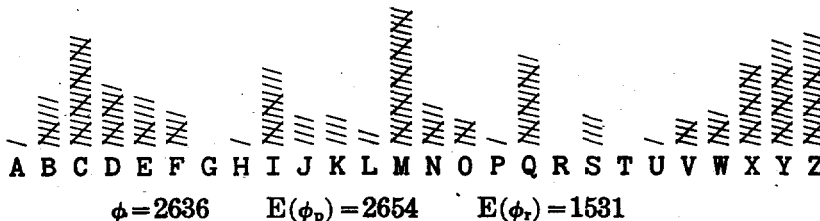
CREDIT
TEXT ASSIGNMENT
MATERIALS REQUIRED
SUGGESTIONS
EXERCISES

3
Text, Section V; attached memorandum
None
None

Weight

40 1. a. Solve the following cryptogram:

	5	10	15	20	25
A	J M Q V S	Q Z X I F	F M Z S L	I Z M L Z	C E M E B
B	F Q O M E	M D X Y Q	O Z C Y Y	X J M Z I	V M Z I Y
C	O Q W Y I	D K Y M V	M Z M N Q	E Q K M X	C C W Z B
D	C Y I X I	C D Y Y X	C B Z Q I	F Z C Q N	H W D O X
E	I C D J Q	Y P M M D	Y M V M Z	M F S N Q	E Q K M N
F	Q D N E W	O J M A W	I B E M D	X N M Y X	Z C S M N
G	Y X C B U	M Q Z M E	C V I D K	C W Z X Z	C C B Y X
H	C Z M Q Z	B C Y I X	I C D Y Y	X C B Z Q	F Y X C D



~~RESTRICTED~~

~~RESTRICTED~~

- 5 b. What is the specific key?
- 5 c. Name two methods of solving ciphers of this type.
2. Solve the following cryptograms:
- 10 a. Q H H Y L Y D W Q J J M E F C
- 10 b. Y X S E D Y F S X U H W X U S
- 5 c. What are the specific keys?
- 10 3. a. In the solution of a substitution cipher by completing the plain component sequence involving reversed standard alphabets, what are the successive steps?
- 5 b. What is the first step one should take in attempting to solve an unknown cryptogram that is obviously a substitution cipher?
- 5 c. If this step is unsuccessful and the cryptogram is obviously monoalphabetic in character, what type of cipher alphabet may be assumed to have been used?
- 5 d. Why do monoalphabetic cryptograms involving standard cipher alphabets yield such a low degree of cryptographic security?

~~RESTRICTED~~

MEMORANDUM ON CRYPTANALYTIC PROCEDURE

The following suggestions will promote systematization of procedure and logic in analysis. Experience has shown that time and labor can be saved by careful attention to these instructions.

1. Most of the problems in this course are already laid out in worksheet form, to spare the student the clerical labor of copying out the text. However in those cases where worksheets must be prepared, the cipher text should be copied in ink on cross-section paper, one letter per cell. There should be a single space between letters or digraphs in monoalphabetic systems, and a single space between period lengths in polyalphabetic systems. In aperiodic systems groupings may be in five letters, unless the system lends a better alternative. At least three spaces between successive lines of cipher text is recommended in order to leave room for multiple assumptions. Line and column indicators are to be made for each cryptogram, to facilitate reference in the step-by-step commentary. Margins should be left on all sides for notes, etc. *All* worksheets and notes should be submitted together upon the completion of a lesson.

2. Enciphering alphabets, enciphering diagrams, etc., as well as all keywords and specific keys should be included in a solution. Keyword derivation from transposed sequences will also be shown. Whereas there should be a letter-for-letter decryptment *under* the cipher text, the final plaintext version in word-lengths should correct any errors or garbles in the text. Nulls or indicators showing sentence separation, change of key, etc., may be enclosed in parentheses.

3. If completing the plain component sequence yields no solution, then uniliteral frequency distributions (or digraphic distributions, if a digraphic system) should be made. Triliteral frequency distributions will enable the separation of vowels and consonants and furnish much additional valuable data. In a difficult case trilaterals may give the only clues to solution: this is especially true in foreign language cryptograms. If the problem entails the selection of proper generatrices in polyalphabetic ciphers, the use of alphabet strips will save much time. In polypartite systems, reduce the cryptogram to monoliteral terms wherever possible.

4. Repetitions should be underscored in a manner facilitating their location and interpretation: colored pencils will be found useful. It is recommended that the frequencies of letters comprising the repetitions be inscribed over their respective letters. Likewise, the frequencies of the first 10 and last 10 letters should also be inscribed, as in many cases these positions lend themselves readily to attack. If the problem proves difficult, then it is best to inscribe the frequencies over all the cipher letters of the text, in order better to visualize *frequency-patterns* of words.

5. Step-by-step analyses should accompany all problems: they should be brief and concise, yet at the same time specific. The steps should be jotted down *as they are made*, and at the end they should be combined into a complete resume of the analysis. It is not necessary to be verbose, but *all* the steps which were taken to achieve solution should be specified, so that at any future date the solution may be reconstructed following the exact manner in which it was first accomplished. Assumptions of words, etc., should be referred

~~RESTRICTED~~

~~RESTRICTED~~

to with line and column indicators and couched in the proper cryptologic language or symbols. All keywords and specific keys, as well as the mechanics of the general system, should be stated at the end of the commentary.

6. Violations of cryptographic security observed in the problem studied may be included at the close of the commentary. These violations may be stereotypic phraseology (especially in beginnings or endings of messages), related keywords, keywords of military nature, unnecessary punctuation, general wordiness, or any other practices dangerous to cryptographic security which may be seized upon by the cryptanalyst as entering wedges in solution.

~~RESTRICTED~~

~~RESTRICTED~~

**EXTENSION COURSE OF THE ARMY SECURITY AGENCY
LESSON ASSIGNMENT SHEET**

SUBCOURSE 20-6

LESSON 3

Military Cryptanalysis, Part I

Unilateral substitution with mixed cipher alphabets

CREDIT

3

TEXT ASSIGNMENT

Text, Section VI; attached memorandum

MATERIALS REQUIRED

Cross-section paper of ¼ inch squares

SUGGESTIONS

None

EXERCISES

Weight

- 20 1. a. Construct a trilateral frequency distribution showing one prefix and one suffix of the cryptogram below. On the worksheet below indicate by under-scoring in black all repetitions of three or more letters. Other significant details may be marked in different colors.
- 6 b. Prepare a condensed table of repetitions of digraphs and trigraphs appearing more than twice, and include all repetitions of longer polygraphs.
- 20 2. a. Using the data obtained in a and b above, complete the solution of the cryptogram.

5

10

15

20

25

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

~~RESTRICTED~~

~~RESTRICTED~~

5

b.

RGRQRU T D S P Y U R D P Z F T A V D R C A Y C F O
 J O D R Z Y U U F S P P F U Z R T F A D Y G P

7. In solving several unrelated monoalphabetic cryptograms the following cipher alphabets were reconstructed. Recover all keywords in each case. To expedite solution, significant segments have been underlined.

2

a.

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

2

b.

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

2

c.

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

2

d.

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

2

e.

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

~~RESTRICTED~~

~~RESTRICTED~~

**MEMORANDUM ON ALPHABET RECONSTRUCTION
AND KEYWORD DERIVATION**

1. Concurrent with the solution of a cryptogram, there should be a simultaneous effort in the reconstruction of the general system and recovery of the specific keys. Much labor can thus be saved as recovery of the keys early in the stages of solution transforms the process of decrypting into one of decryptographing.

2. A cipher alphabet consists of two sequences, e.g.,
- a. the plain component is a standard alphabet, cipher component mixed;
 - b. the cipher component is a standard alphabet, plain component mixed;
 - c. both components are the same mixed sequence;
 - d. both components are the same mixed sequence, running in reverse; or
 - e. the components are differently mixed sequences.

3. Let us examine several types of mixed sequences, using the keyword HYDRAULIC as an example:

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

The ordinary keyword-mixed sequence derived from the above will be:

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

The two principal transposition-mixed types will read:

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

Other types may arise from route transpositions as follows:

- d. H B P Q E Y D F S T G R A J V W K U L M X Z N I C O
e. H Y B P E D R F Q S G A U J T V K L I M W X N C O Z
f. P B Q H E S Y F T D G V R J W A K X U M Z L N I O C
g. H Y D R A U L I C O N M K J G F E B P Q S T V W X Z
h. O C I L U A R D Y H B P Q S T V W X Z N M K J G F E
i. H Y E B P Q S T G F D R A U K J V W X Z N M L I C O
j. C P I O Q B L N S E H U M Z T F Y A K X V G D R J W etc.

Any transposition system may be employed to produce a systematically-mixed sequence: practicability of method is the only determining factor. It must be remembered that the greatest amount of systematic mixing will produce a sequence inherently no more secure than a random alphabet.

~~RESTRICTED~~

~~RESTRICTED~~

4. The student would do well to construct both enciphering and deciphering versions of cipher alphabets recovered. For example, in the following case

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

no semblance of a key is apparent; but in the inverse form

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

the key-phrase "NOW IS THE TIME FOR ALL GOOD MEN TO COME TO THE AID OF THEIR PARTY" is quite clear. In other types of mixed sequences, first the one form is attacked, and then if negative results are obtained the inverse form is treated.

5. Let us consider the following cipher alphabet:

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

The section V W X seems to be superimposed parts of the non-keyword portions of mixed
J K L

sequences. Adding Y Z to the plain component, we get V W X Y Z which is certainly con-
J K L N P

sistent as far as alphabetical progression goes, and indicates that the letters M and O are present in the keyword of the cipher component. Continuing in this vein, the section M N O Q S T V W X Y Z is rapidly established by correlating both sequences. It is obvious
B E F G H I J K L N P

that the plain component keyword begins right after the Z, and that the cipher component keyword probably just precedes the B. Going to the right, Z R H suggests keywords like
P Q R

RHOMBOID, RHEUMATISM, etc. These trials are quickly repudiated; therefore we go on to Z R E which is acceptable. Z R E K is found wanting, but Z R E P is very sat-
P Q S P Q S T P Q S U

isfactory, and this is soon expanded to Z R E P U B L I C, and in a moment or two we
P Q S U V W X Y Z

recover the complete cipher alphabet:

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

6. In the example below the student will observe that the alphabets are reciprocal: this is an indication of identical sequences at a shift of 13, or that a mixed sequence running against itself in reverse has been employed. In this case the W X Y Z points to the latter hypothesis.
Z Y X W

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

Starting with the V W X Y Z R cluster, we see that the keyword begins with the letter R;
R Z Y X W V

therefore the next letter should be a vowel. Z R A is not acceptable, but Z R E is fine, show-
W V H W V T

~~RESTRICTED~~

~~RESTRICTED~~

ing that the letter U appears in the keyword. Continuing the same line of reasoning as in the preceding example, and with a little further experimentation, the final alphabet is discovered to be

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

7. In the next example, all efforts to derive keywords on the basis of keyword-mixed sequences are fruitless: the conclusion is therefore drawn that this is a case of a transposition.

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

Considering the mechanics of the cryptography involved, and assuming for the time being that Z is at the bottom of the matrix and not in the keyword, we start with the letters to the left, or if this fails, to the right of Z in the cipher component, obtaining the column N

K
Z

which is not incompatible if N is in the keyword on the top row. If we place Y to the left of Z and build up its column, we get E N which is certainly excellent. This is expanded

J K

Y Z

into I M E N which quickly becomes 7 1 8 4 3 5 2 6 9. This last example was very

G H J K
W X Y Z

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

easy because none of the letters V W X Y Z appeared in the keyword; but other cases should hardly prove more difficult.

8. Two additional methods that have been encountered for deriving mixed sequences may be mentioned. One is a slight modification of the preceding paragraph, when the keyword contains repeated letters, viz:

1 8 7 3 4 9 5 2 6

C O M . I T . E .

A B D F G H J K L

N P Q R S U V W X

Y Z

which produces the mixed sequence

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

The other method is the interrupted-key columnar transposition system, viz:

2 1 3 5 4 6

J A N U R Y

B C)

D)

E F G)

H I K L M)

O P Q S)

T V W X Z -)

which produces the mixed sequence

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

~~RESTRICTED~~

~~RESTRICTED~~

The first example will succumb to the treatment outlined in paragraph 7, whereas the second method is vulnerable owing to the presence of the fragments E H O T, F I P V and G K Q W in the sequence which may be anagrammed. Note the fragment B D E H O T, composed of an ascending sequence of letters: this is an outward indication of the interrupted-key columnar method.

9. There are still other methods used for the production of mixed sequences, but space does not permit giving further examples. However the student should by this time be able to devise methods of attack for any special cases that may present themselves, based upon the weaknesses or peculiarities inherent in the system of cryptography involved.

~~RESTRICTED~~

~~RESTRICTED~~

**EXTENSION COURSE OF THE ARMY SECURITY AGENCY
LESSON ASSIGNMENT SHEET**

SUBCOURSE 20-6

LESSON 4

CREDIT

TEXT ASSIGNMENT

MATERIALS REQUIRED

SUGGESTIONS

EXERCISES

Weight

20

1. Solve and recover all keys:

Military Cryptanalysis, Part I

Polyliteral substitution with mono-equivalent cipher alphabets

3

Text, Section VII; attached memorandum

Cross-section paper of ¼ inch squares

None

	5					10					15				
A	DT	LR	WE	OE	OE	WH	RR	WR	LA	WH	WA	DE	DA	WR	LE
B	LE	OR	RE	WT	OR	WA	OH	WH	OR	LE	LR	WA	RR	RR	WH
C	WA	WH	OE	OR	LE	LE	WR	WA	WH	OH	LR	LE	LR	WA	OH
D	OE	LR	OA	OA	OE	LR	OR	RE	OA	OA	WH	WT	WH	WA	WA
E	WR	WA	WH	DE	RT	OE	WH	WH	RE	OR	OA	RT	OE	LR	OR
F	RE	WR	WE	WA	OH	DE	WR	LR	WA	WA	WR	WA	WH	DE	DA
G	LR	LR	WA	WH	OA	DE	LR	LT	LT	LR	OA	WR	DE	WR	LR
H	WA	OA	LR	RA	RA	LR	WE	OE	DE	RT	OE	WH	RR	WR	LA
J	WH	WA	DE	DA	WR	LE	LE	OT	WH	OE	WH	WH	WA	RA	LR
K	OE	OH	WH	RE	OT	DT	OR	RE	RE	WR	DE	WR	LR	WA	OR
L	LE	OR	OE	DE	WR	LE	LE	WH	OE	DT	OA	WE	LT	LT	LR
M	OE	DE	OA	DE	LR	LT	OH	LR	LE	LR	WA	WH	LE	OT	WH
N	WA	WA	WR	WA	RR										

~~RESTRICTED~~

~~RESTRICTED~~

	A	E	H	R	T
D	3	12	-	-	3
L	2	13	-	21	5
O	10	14	6	10	3
R	3	7	-	5	3
W	22	4	22	13	2

$\phi = 2288$ $E(\phi_r) = 1362$ $E(\phi_p) = 2270$
 (25-element alphabet)

20. 2. This message was sent by the Fifteenth Infantry. Solve it and recover all keys:

	5					10					15				
A	CY	AO	NX	CN	NO	CN	AO	AO	OG	ON	NG	BY	OX	OX	RO
B	CG	NY	RO	AN	RE	AG	RO	OX	AO	AN	AX	AX	AG	AN	AG
C	CN	RO	OX	OX	BY	AN	AG	CN	BE	CX	BN	BX	CG	RO	ON
D	CO	RE	CN	AY	BG	CE	ON	NO	AO	OG	RO	NO	NO	RO	RE
E	OO	NG	BY	OX	OX	RY	AG	AX	BY	AN	OG	CN	AO	OY	OG
F	NO	OX	CY	NX	OG	AO	AN	CN	AG	RE	AG	BY	OG	NO	AO
G	BO	AO	CN	CG	AG	CN	ON	BO	CN	AO	OY	CO	OE	ON	NO
H	AO	OG	RO	NO	NG	RO	NO	AG	CN	RE	AO	OX	RX	AE	BY
J	AN	BO													

	E	G	N	O	X	Y
A	1	9	7	12	3	1
B	1	1	1	3	1	6
C	1	3	11	2	1	2
N	-	3	-	9	2	1
O	1	7	5	1	9	2
R	5	-	-	9	1	1

$\phi = 716$ $E(\phi_r) = 410$ $E(\phi_p) = 960$ (approx.)
 (36-element alphabet)

~~RESTRICTED~~

~~RESTRICTED~~

20

3. Solve and recover all keys:

5

10

15

A	<u>RG</u>	GP	<u>EE</u>	<u>GR</u>	RG	GP	<u>ES</u>	GR	RG	PP	<u>GE</u>	PR	GE	RG	GS
B	AS	GR	RR	GS	AE	PP	GP	GA	PP	RA	<u>EA</u>	ES	GR	RG	PP
C	<u>GE</u>	RA	PR	GS	RE	GP	AR	GP	GS	PP	GP	RG	RA	EA	PP
D	PS	PG	<u>AR</u>	<u>PE</u>	<u>GA</u>	<u>RR</u>	<u>RG</u>	<u>GP</u>	<u>RR</u>	RE	PG	PP	RA	EA	RS
E	PG	PE	RG	<u>AR</u>	<u>PE</u>	<u>GA</u>	<u>RR</u>	<u>RG</u>	<u>GP</u>	<u>RR</u>	RP	AE	GS	GA	AP
F	GP	PP	RA	EP	ES	GP	RA	GP	RA	PE	PR	PR	AE	GR	GP
G	RA	GA	GP	GP	RR	GP	RR	GR	AS	AS	GP	RR	GR	GS	PP
H	GP	AE	GE	RS	PG	RG	GS	RE	PP	GR	GG	GS	<u>PP</u>	<u>GR</u>	<u>PG</u>
J	<u>GA</u>	PG	RS	RE	PG	AS	PR	GS	GA	GE	RR	<u>EA</u>	<u>ES</u>	<u>GR</u>	<u>RG</u>
K	RR	RP	GS	PP	PP	GS	AE	<u>GR</u>	<u>PG</u>	<u>GA</u>	EP	<u>RG</u>	<u>GP</u>	<u>EE</u>	<u>GR</u>
L	RA	GR	<u>PP</u>	<u>GR</u>	<u>PG</u>	<u>GA</u>	AR	GS	RA	RP	GP	GP	GA	GS	PE
M	ES	PG	RG	GR	ER	GP	RR	RP	GE	RG	GP	AG	GR	AS	GP
N	GA	PP	GS	AE	AR	PA	EP	RG	GP	PR	AE	GE	<u>RG</u>	<u>GP</u>	<u>EE</u>
P	GP	RA	PP	GP	RR										

	A	E	G	P	R	S
A	-	7	1	1	5	5
E	4	3	-	3	1	5
G	11	7	1	27	16	14
P	1	5	10	16	6	1
R	11	4	16	4	12	3

$\phi = 2294$

$E(\phi_r) = 1164$

$E(\phi_p) = 2260$ (approx.)

(30-element alphabet)

~~RESTRICTED~~

~~RESTRICTED~~

20

4. Solve and recover all keys:

5

10

A	AAC	ACA	AAA	ACA	AAC	ACA	ACC	BAC	ACA	CCA
B	CAA	ACB	AAC	BCC	ACA	ABA	ABA	BAA	BBB	ACA
C	ACC	ACB	BCC	BAB	ACA	AAC	AAA	AAB	CBA	ACA
D	AAA	CAA	ACB	AAC	ABB	BBC	AAC	ACA	BBB	AAB
E	BCC	ACA	ACC	ABB	CBB	AAB	ABC	ABC	BAA	BBA
F	CBA	BAA	ACC	BAC	ACA	ABB	CAA	ACC	ACA	CBB
G	CAB	CAA	ABA	AAB	ABB	AAB	CAA	ACC	ABA	ACC
H	CAA	AAC	ABB	BBC	CAA	AAA	AAC	BCA	ABA	AAB
J	CBC	CAA	ACC	ACA	AAA	AAB	CBA	ACA		

	A	A	A	B	B	B	C	C	C
	A	B	C	A	B	C	A	B	C
A	5	7	8	5	5	2	14	3	8
B	3	1	2	1	2	2	1	-	3
C	8	1	-	3	2	1	1	-	-

$\phi = 486$

$E(\phi_r) = 284$

$E(\phi_p) = 505$ (approx.)

(27-element alphabet)

~~RESTRICTED~~

~~RESTRICTED~~

5. The following is a text in the Baudot teletype code enciphered by a simple machine employing five two-position switches which operate polarized relays. Each switch has the function of changing the polarity of its respective baud (a single "mark" or "space" impulse), if the switch is in the 'active' position. If the switch is in the 'inactive' position, the polarity of the baud is unaffected. The switch settings remain constant for each message. As an example, if switches 1 and 4 are active (*), and 2, 3 and 5 are inactive (-), then the word ENEMY is enciphered thus:

Key: *—*— *—*— *—*— *—*— *—*—
 Plain: MSSSS SSMMS MSSSS SSMMM MSMSM
 Cipher: SSSMS MSMSS SSSMS MSMSM SSMMM

It is suspected that the same signature is in the text as was present in Problem 2. Solve the message and recover the switch settings.

	1	2	3	4	5	6	7	8	9	10
A	MSMSS	MSMMS	MSSSM	MMSM	MMMS	MSSSM	SMMS	SMSSS	SSSSS	SMSMS
B	MSMSS	MSSSS	MSSSM	SSMMM	MMSSM	MSMS	MSMM	MMMSM	MMMSM	SSMMM
C	MMSSM	MMMM	SSMSM	MMSM	MSMSS	MSSSM	SMMSM	MMMM	MSMSS	MMSSM
D	MMSS	MMSS	SSMSM	MMMM	SSSSS	MSSSM	SSSM	MMSSM	MMMM	SSMSM
E	MSSSM	MSMMS	MSSMM	MSSSM	MSSMM	SSMSM	SMSS	MSMSS	MSMMS	MSSMM
F	MSSSM	SMMS	SMSM	MMSSM	SMMSS	MMSSS	SMMSM	SMSSM	MSMMS	SSSSS
G	MMSS	MSSMS	SMSMS	MMMSM	MMMSM	MSSSM	MSSSM	SMMSM	MSMSS	SMMSS
H	SMMSM	MSMSS	SSMSM	MMMM	MSSSM	MSMM	MSMMS	MMSS	MSSSM	SMMMS
J	SMSSS	MSMSS	SMSMS	MSSSM	MMSSM	MSSMM	SSSM			

M M M M S S S S
 M M S S M M S S
 M S M S M S M S

MM	5	1	4	4	3	1	6	1
MS	1	5	-	8	4	1	13	1
SM	-	3	4	3	1	3	1	2
SS	2	-	5	-	2	-	-	3

$\phi = 386$

$E(\phi_r) = 234$

$E(\phi_p) = 480$ (approx.)

(32-element alphabet)

~~RESTRICTED~~

~~RESTRICTED~~

**EXTENSION COURSE OF THE ARMY SECURITY AGENCY
LESSON ASSIGNMENT SHEET**

SUBCOURSE 20-6

LESSON 5

Military Cryptanalysis, Part I

Polyliteral substitution with poly-equivalent cipher alphabets

CREDIT

3

TEXT ASSIGNMENT

Text, Section VIII; attached memorandum

MATERIALS REQUIRED

Cross-section paper of ¼ inch squares

SUGGESTIONS

None

EXERCISES

Weight

- 5 1. a. What is the purpose of providing variants in a cipher system?
5 b. From the cryptanalytic point of view, how does simple monoalphabetic substitution differ from monoalphabetic substitution with variants?
- 20 2. Solve and recover all keys:

5

10

15

A	RA DE KE PE VE TI BO LA GO DU JO BE KI BI JO
B	BU JA VA ME LA BE KI RE FE DO VI JO SA DO JE
C	KI BA MO SA CU GE GE PI BO KI JU CE CI MI NE
D	PO JU CE RE NA BU BE KO RA DE KE TE SE TI JO
E	FA GO DU DO JE KI DI JO BU JA CE BO FO BA BU
F	DA LE JO NI DO NA BO BE PI GI ME TE CO JO TI
G	SA BO TI DU MO FA BU NA DU DE TO GI BE SE BU
H	GE CO PA TA KE CE NA VA MO LO ME NA DU DE CE
J	BO FO DA DU DA LE BO SI JO VA DO DE TI NI DO
K	CO FI DE VE CI BU DA LE BO VI DO NA JO BE KI
L	VA DU DE KO GO RE MO PE SA RA JE KA DO PI RI

~~RESTRICTED~~

~~RESTRICTED~~

20

3. Solve and recover all keys:

5

10

15

A	DR	DD	SY	DA	RA	RR	SB	YA	BT	TY	AR	HI	DB	TB	AD
B	YY	YB	SA	AA	HI	DA	TD	HR	YB	TD	RB	RI	AI	HH	BT
C	DD	IA	AI	BB	HA	YD	TH	YA	HI	BA	YT	YD	YY	BD	YH
D	SD	DI	SB	AA	ST	YD	RH	SD	SR	YR	DT	SR	RA	RR	YB
E	SA	BT	TY	HR	AI	DB	IB	AD	DY	YB	SA	HA	HI	DA	TD
F	TS	DB	SH	YH	DI	SD	TT	TT	YY	HH	ST	YI	SB	AA	ST
G	DD	AH	DH	YT	RH	HI	ID	AR	SB	BA	RI	HB	AI	HI	RH
H	DB	SH	HA	RI	DA	AI	IB	YB	DI	SI	DD	YA	BB	YT	HH
J	II	YH	TY	BS	DD	YR	SR	RI	HH	TD	DT	TA	AI	RY	ST
K	SH	DH	AB	AI	TI	YT	AH	HY	AR	AI	RH	DI	YD	DD	YA
L	TB	DT	HH	SB	AA	DT	DD	RH	YD	DR	YB	DH	SH	SR	DD
M	DA	SI	RI	ID	ST	BD	SI	SD	TT	BH	SH	RI	AA	HI	BB
N	IS	BI	HI	RH	AY	DB	BA	AI	DH	SH					

~~RESTRICTED~~

~~RESTRICTED~~

25

4. Solve and recover all keys:

	5					10					15				
A	99	18	57	82	12	28	78	90	25	04	15	30	04	06	14
B	57	34	64	20	72	15	30	02	57	44	84	52	66	11	81
C	87	58	35	78	31	14	70	90	68	47	30	13	15	21	86
D	92	43	10	30	35	20	31	32	64	18	57	26	84	12	06
E	34	25	69	72	90	78	07	90	31	29	57	50	82	19	53
F	31	72	51	36	10	86	36	47	18	67	26	04	92	82	30
G	08	31	58	90	88	87	91	10	20	82	31	14	56	57	31
H	88	04	31	30	66	47	30	36	18	99	20	06	97	31	21
J	55	99	18	20	10	28	74	68	90	41	69	82	90	78	31
K	86	88	15	91	26	92	72	87	14	43	20	53	28	64	92
L	47	02	58	35	10	96	05	34	37	85	06	26	80	50	92
M	68	10	70	81	92	18	02	86	49	47	07	82	94	06	69
N	15	21	90	56	10	40	01	68	90	15	35	57	52	32	60
P	47	64	36	71	06	55	00	68	78	45	52	12	69	43	

~~RESTRICTED~~

~~RESTRICTED~~

25 5. This message is suspected of having an ending similar to Problem 4. Solve it and recover all keys:

	5					10					15				
A	22	08	71	29	19	83	05	34	76	58	05	56	62	26	22
B	35	48	75	13	78	58	34	65	02	07	71	51	87	35	96
C	10	32	69	45	47	81	46	11	01	14	67	37	75	79	35
D	30	53	29	37	46	60	19	30	94	66	49	68	88	57	98
E	84	93	30	86	28	90	51	04	53	03	84	76	58	31	57
F	42	12	86	49	36	79	54	28	09	38	24	41	86	63	79
G	08	28	67	68	66	94	22	63	71	66	83	56	05	07	58
H	95	60	19	62	26	48	23	59	40	38	15	67	43	92	42
J	62	77	43	79	54	69	38	65	16	82	10	96	67	97	57
K	48	93	24	13	53	29	46	37	32	65	12	94	84	95	68
L	83	93	98	37	75	79	45	12	97	84	53	03	75	76	95
M	31	29	32	21	49	17	25	73	00	69	86	36	79	45	19
N	77	98	38	95	97	93	94	98	72	42	59	00	08	50	44
P	27	26	62	57	06	91	23								

~~RESTRICTED~~

FREQUENCY DISTRIBUTIONS

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

Problem 2

	A	B	D	H	I	R	S	T	Y
A	5	1	2	2	9	3	-	-	1
B	3	3	2	1	1	-	1	3	-
D	5	5	8	4	4	2	-	4	1
H	3	1	-	5	8	2	-	-	1
I	1	3	1	-	1	-	1	-	-
R	2	1	-	6	6	2	-	-	1
S	3	5	4	6	3	4	-	5	1
T	1	2	4	1	1	-	1	3	3
Y	4	6	5	3	1	2	-	4	3

Problem 3

	0	1	2	3	4	5	6	7	8	9
0	1	1	3	-	4	1	6	2	1	-
1	7	1	3	1	4	6	-	-	6	1
2	6	3	-	-	2	4	-	3	1	
3	7	1	0	2	-	3	4	4	1	-
4	1	1	-	3	1	1	-	6	-	1
5	2	1	3	2	-	2	2	7	3	-
6	1	-	-	4	-	2	1	5	4	
7	2	1	4	-	1	-	-	5	-	
8	1	2	6	-	2	1	4	3	3	-
9	9	2	6	-	1	-	1	1	-	3

Problem 4

	0	1	2	3	4	5	6	7	8	9
0	2	1	1	2	1	3	1	2	3	1
1	2	1	3	2	1	1	1	1	-	4
2	-	1	3	2	2	1	3	1	3	4
3	3	2	3	-	2	3	2	4	4	-
4	1	1	3	2	1	3	3	1	3	3
5	1	2	-	4	2	-	2	4	4	2
6	2	-	4	2	-	3	3	4	3	3
7	-	3	1	1	-	4	3	2	1	6
8	-	1	1	3	4	-	4	1	1	-
9	1	1	1	4	4	4	2	3	4	-

Problem 5

~~RESTRICTED~~

~~RESTRICTED~~**MEMORANDUM ON STEREOTYPIC BEGINNINGS AND ENDINGS**

Within the confines of the comparatively limited scope of military messages, stereotyping of phraseology is inevitable. Particularly in the beginnings of messages is this limitation apparent: thus these positions lend themselves most readily to attack by the cryptanalyst. The following list of stereotypes have a high frequency of positional occurrence, and therefore are to be shunned by the cryptographer as conscientiously as they are looked for by the cryptanalyst. It is to be noted that a stereotypic initial word often may suggest a whole opening phrase. For example, if a message begins with the word HEAVY, then it is not too unlikely that the opening phrase is "HEAVY ARTILLERY (FIRE, BARRAGE) (FALLING, INTERDICTING) . . .," which might be expanded into "HEAVY ARTILLERY FIRE FALLING ON OUR POSITIONS (NORTH, EAST, SOUTH, WEST) OF. . ."

BEGINNINGS

ACKNOWLEDGE	LOCATION (OF)
ADVANCE	NUMBERS (1, 1st, 2, 2nd, etc.)
ADVISE	ORDERS
ARRIVE	OUR
ATTACK	PARAPHRASE
ATTENTION	PLEASE
CANCEL	POSITION
CITE	PREPARE
COMMANDING (GENERAL)	PROCEED
COMMUNICATION (OFFICER)	RECEIPT
CONCENTRATE	RECEIVE
CONFIRM	RECOMMEND
CONTINUE	REFER (-RING) (TO) (YOUR)
DEPART (-URE)	REFERENCE (YOUR) (MESSAGE, RADIO-
DISCONTINUE	GRAM, TELEGRAM) (NUMBER)
ENEMY	REPEAT
EQUIPMENT	REPORT
EXPEDITE	REQUEST
FOLLOWING	REQUIRE
FOR	RERAD
FROM	REURAD
HEAVY	SEND
HOSTILE	SUPPLY
INFORM (-ATION)	VERIFY
IN REPLY (TO) (YOUR)	YOUR (S)

ENDINGS

ACKNOWLEDGE	PERIOD
ADVISE (IMMEDIATELY)	REPLY
CONFIRM	REFERENCE
END	REQUESTED
END OF MESSAGE	SIGNED (NAME)
IMMEDIATELY	STOP
NUMBERS (1, 1st, 2, 2nd, etc.)	TITLES (MAJ, COL, ETC.)

~~RESTRICTED~~

~~RESTRICTED~~

**EXTENSION COURSE OF THE ARMY SECURITY AGENCY
LESSON ASSIGNMENT SHEET**

SUBCOURSE 20-6
LESSON 6

Military Cryptanalysis, Part I
Polygraphic substitution systems: 4-
square and 2-square matrices

CREDIT
TEXT ASSIGNMENT

3
Text, pars. 41-44, Section IX; attached
memoranda

MATERIALS REQUIRED
SUGGESTIONS

Cross-section paper of ¼ inch squares
Review Section VIII, TM 11-485

EXERCISES

Weight

- 4 1. a. What is polyliteral substitution? What is polygraphic substitution?
4 b. In true digraphic substitution, if RE_p yields QN_c , is it possible for RN_p
to yield AZ_c ?
2 c. What is the fundamental purpose of polygraphic substitution?
10 2. a. Construct a digraphic frequency distribution of the cryptogram below.
20 b. The following cryptogram is suspected to contain the word INFANTRY.
Solve it and recover all keys:

	5	10	15
A	AF SM DH FG <u>SP OS AB</u> TU ZF OG TR UH IF PQ <u>SO</u> →		
B	← RO MA CS KN SM KH TT UF HF UE QM OC NU DC EA		
C	AM QM AF VD LK BT QU FC NI TT CG MT <u>SA HH</u> PU		
D	ZR <u>KU IW RH DS IM SW</u> AC <u>MT SP OS AB</u> GN KP TD		
E	TT TU IM II SN <u>SA HH</u> QM SH II PQ <u>RH DS IM SW</u>		
F	YO CC UF QI TR <u>MT SP OS</u> AI KU <u>KU IW</u> <u>SO RO MA</u> →		
G	← CS KN YO QA FC CS VS DH LS KS AC QT OQ		

~~RESTRICTED~~

~~RESTRICTED~~

20 3. The enemy is suspected of using a 4-square matrix wherein the plain components are mixed sequences and the cipher components are standard alphabets (I=J) inscribed in straight horizontals. Solve the following cryptogram and reconstruct the original matrix:

	5					10					15				
A	DO	GV	XX	HA	<u>TP PN</u>	DF	OW	FS	YN	<u>DP YK</u>	<u>DP YK</u>	WH			
B	WL	IA	NF	OB	<u>DE GV</u>	HX	VC	OP	RY	<u>OP DQ</u>	RY	WT	<u>DP</u>		
C	YK	DP	YK	QZ	<u>FS IX</u>	GW	DB	AF	HW	NE	VO	YA	LZ	CW	
D	TY	DQ	GN	WN	NS	IH	CA	VI	HH	OF	WZ	YN	WM	WH	OG
E	EV	YN	NL	NK	XI	<u>WH WL</u>	IA	NF	OB	DE	GV	FS	OF	WH	
F	NF	<u>OP DQ</u>	XO	FA	WN	LQ	<u>DP YK</u>	BP	IE	<u>DP YK</u>	SD	NQ			
G	<u>DP YK</u>	<u>TP PN</u>	VT	TF	BL	MW	CW	IE	TE	FS	CY	OK	YD		
H	OM	XE	VT	<u>FS IX</u>	HB	IH	MP	YN	LZ	YN	NW	GR			

20 4. Solve the following cryptogram and reconstruct the enciphering matrix. It is suspected that this message probably has a stereotypic ending.

	5					10					15				
A	NK	KZ	FQ	KG	QD	RR	RO	NK	MV	TR	KE	HQ	FZ	QR	PE
B	NK	RD	FW	IV	<u>EF FF</u>	<u>XT</u>	NB	LZ	NV	EU	RO	PQ	DA	<u>ML</u>	
C	<u>EU</u>	KV	FF	LL	FM	CF	QP	EI	<u>RC</u>	<u>SO</u>	<u>RS</u>	BC	<u>SD</u>	<u>LN</u>	<u>CD</u>
D	<u>IE</u>	<u>HG</u>	<u>TM</u>	<u>VE</u>	<u>FP</u>	<u>QP</u>	<u>SI</u>	KZ	FW	FP	NB	QR	IZ	IW	<u>EF</u>
E	<u>FF</u>	<u>XT</u>	LW	NX	PD	KK	KV	RD	FP	QR	MX	AR	PZ	FW	<u>ML</u>
F	<u>EU</u>	IN	FF	LW	NC	<u>LN</u>	<u>CD</u>	<u>QP</u>	<u>SI</u>	KE	FR	HP	ON	IM	HC
G	SM	KZ	IL	FN	FP	LV	LQ	PD	<u>AS</u>	FK					

~~RESTRICTED~~

~~RESTRICTED~~

- 20 5. The following two messages were intercepted on the same circuit half an hour apart, message "B" being in answer to a request for a repeat. Solve the texts, and determine the cause of the cryptographic error involved:

MESSAGE "A"

	5	10	15
A	DS ZM <u>CM GI QM AB VG ED</u> SU XI TO <u>SQ OR NR SB</u> →		
B	← <u>PN QO HN TB LL QN QS SI CR YU TQ CC KG AT FN</u>		
C	YF <u>VG ED CG NU MO LL NP SO SB NP</u> <u>SQ OR NR SB</u> →		
D	← <u>PN CM MB RP OG LL YX <u>CM GI QM AB</u> SO NQ LZ LC</u>		
E	FD YR VI OR SB		

MESSAGE "B"

	5	10	15
A	OY RU <u>PU KV TU WO IW LL</u> NR EV VD <u>NB BZ YZ NO</u> →		
B	← <u>AS TD HS VO DE TS TY NV PZ SR VB PM FW WQ XS</u>		
C	SK <u>IW LL PW YR CD DE YC ND NO YC</u> <u>NB BZ YZ NO</u> →		
D	← <u>AS PU CO UC BW DE SF <u>PU KV TU WO</u> ND YB DI DM</u>		
E	XL SZ IV BZ NO		

~~RESTRICTED~~

~~RESTRICTED~~

MEMORANDUM ON THE SOLUTION OF 2-SQUARE MATRICES

1. If the student reviews paragraph 34 of TM 11-485, he will refresh his memory on the enciphering and deciphering processes of the two types of 2-square matrices. In the horizontal 2-square matrix illustrated in Fig. 36, the first member of the plaintext digraph comes from the same square as the second member of the cipher-text digraph, whereas the θ^2_p comes from the same square as the θ^1_c . Thus in the digram, $TH_p = SD_c$; $AN_p = UO_c$; $RE_p = ER_c$; $MO_p = OM_c$. However, the cryptography of the vertical 2-square matrix is analogous to that of the 4-square system, in that the θ^1_p and the θ^1_c come from the upper component, whereas the θ^2_p and θ^2_c are found in the lower component. Thus in Fig. 38, $CO_p = IA_c$; $RE_p = IL_c$; $CA_p = CA_c$; $WI_p = WI_c$.

2. The cryptographic idiosyncracies of 2-square matrices may be exploited by the analyst in attacking such systems. In the vertical 2-square, 20% of the possible 625 plaintext digraphs will be self-enciphered, such as $CA_p = CA_c$ in the example. In the horizontal 2-square, 20% of the 625 digraphs will be enciphered by themselves in reversed form, as in the example $RE_p = ER_c$. Therefore if an examination of the cryptogram at hand discloses a goodly proportion of cipher digraphs which could well be plaintext digraphs, then one may assume that a vertical 2-square has been used. On the other hand, if a large number of cipher digraphs could be good plaintext digraphs if the positions of the letters were reversed, then the assumption would arise that the cryptogram was produced by a horizontal 2-square matrix. Sometimes skeletons of words or even whole phrases are self-evident in the text, affording an easy entering wedge into the problem.

3. During the reconstruction of the squares of the matrix, the student should keep clear on his worksheets which letters are in the same row, and which are in the same column. It will be found expeditious to draw a dividing line (either horizontal or vertical, depending on the type of 2-square involved) on the page to keep the elements of the two squares independent, recording the values which are in the same row or column, writing down the letters as they are assumed until enough values have been established to facilitate reconstruction of the matrix. In the early stages of this process the student must exercise care in recording the letters so that no false relationships are formed; in other words, the values should be written down so that they are not in the same row or column with any other letters than those with which they are known to be related. This will entail spreading the work rather widely over the page.

~~RESTRICTED~~

~~RESTRICTED~~

DIGRAPHIC IDIOMORPHS: GENERAL

<u>AB AB</u>			
-G	EN ER	AL AL	AR M-
	NE	ED ED	
-P	RO CE	ED ED	
-S	UC CE	ED ED	
-D	ET RA	IN IN	G-
	-L	IN IN	G-
	-M	IN IN	G-
	OB TA	IN IN	G-
	QU	IN IN	E-
	RA	IN IN	G-
	RE MA	IN IN	G-
	SH	IN IN	G-
-T	RA	IN IN	G-
	CR	IS IS	
PO	SI TI	ON ON	
	-A	RE RE	EN FO RC ED
	-A	SU SU	AL
	BO	TH TH	E-
	WI	TH TH	E-
-P	AR	TI TI	ON
RE	PE	TI TI	ON
	VI	VI	D-

<u>AB — AB</u>			
-M	AI NT	AI	N-
RE	AR GU	AR	D-
	CH	UR CH	
	DE	CI DE	
	DE	CO DE	
	DI	VI DI	NG
SP	EA RH	EA	D-
-R	ED	UC ED	
-S	CH	ED UL	ED
-B	EE NN	EE	DE D-
	EM	BL EM	
AM	EN DM	EN	T-
CO	NT	EN TM	EN T-
-S	EV	EN TE	EN
-S	EV	EN TE	EN TH
	EN	TR EN	CH
	ER	AS ER	

<u>AB — AB</u>			
	TH	ER EF	ER EN CE
	TH	ER ES	ER VE
	WH	ER EV	ER
-C	AR EL	ES SN	ES S-
		GE OR	GE
	SC	HO OL	HO US E-
-I	LL UM	IN AT	IN G-
		IN CL	IN E-
	-F	IR	IN GL IN E-
	MA	IN TA	IN
-I	NF AL	LI BI	LI TY
	-A	ME ND	ME NT
	SO	ME TI	ME
	-O	NE NI	NE
		NO TK	NO WN
		NO WK	NO WN
-A	PP OI	NT ME	NT
-C	ON TE	NT ME	NT
	-C	OM PR	OM IS E-
	-P	ON TO	ON
-T	HR	OU GH	OU T-
	-N	OW KN	OW N-
		PH OS	PH OR US
		PO ST	PO NE
TR	OO	PS HI	PS
	PA	RA PH	RA SE
	-P	RE FE	RE NC E-
		RE FE	RE NC E-
-T	HE	RE FO	RE
	-P	RE PA	RE
		RE TI	RE
		RE VE	RE NT
	-C	RO SS	RO AD S-
CA	RE LE	SS NE	SS
	AT	TE MP	TE D-
		TH AT	TH E-
	-F	OR	TH WI TH
-I	NV ES	TI GA	TI ON
		ES TI	MA TI ON
-D	ES	TI NA	TI ON
	AC	TI VI	TI ES
	-H	UM DR	UM

~~RESTRICTED~~

~~RESTRICTED~~AB — — AB

-P AN AM AC AN AL
 AR BI TR AR Y-
 AS SO ON AS
 AC CE PT AN CE
 EM PL AC EM EN T-
 -Q UA RT ER MA ST ER
 -I NT ER PR ET ER
 -A CC ES SO RI ES
 IN CL UD IN G-
 -D IR EC TF IR E-
 TO MO RR OW MO RN IN G-
 PA NA MA CA NA L-
 -I NT ER ME NT
 -I NT ER VE NT IO N-
 CO NT IN GE NT
 -C ON DI TI ON
 -T OM OR RO WM OR NI NG
 RA DI OG RA M-
 RE AS SU RE
 -P RE MA TU RE
 -D EF EN SI VE PO SI TI ON
 IN TE RD IC TE D-
 QU AR TE RM AS TE R-
 IN TE RP RE TE R-
 IN TE RR UP TE D-
 -F OR TI FI CA TI ON

AB — — — AB

AR MO RE DC AR
 EN FO RC EM EN T-
 RE EN FO RC EM EN TS
 IN DE TE RM IN AT E-
 IN TE RE ST IN G-
 IN TE RF ER IN G-
 IN TE RV EN IN G-
 -I NC OM PE TE NC E-
 -C ON GR ES SI ON AL
 -D EM ON ST RA TI ON
 -C ON SU MP TI ON
 PH OT OG RA PH
 TH IR TE EN TH

AB — — — — AB

-I NS TA LL AT IO NS
 -C ON CE NT RA TI ON
 -C ON FL AG RA TI ON
 -C ON SI DE RA TI ON

AB — AB AB

MA IN CL IN IN G-
 IN TA IN IN G-

~~RESTRICTED~~

~~RESTRICTED~~

EXTENSION COURSE OF THE ARMY SECURITY AGENCY
LESSON ASSIGNMENT SHEET

SUBCOURSE 20-6
LESSON 7

Military Cryptanalysis, Part I
Polygraphic substitution systems: Playfair cipher systems

CREDIT
TEXT ASSIGNMENT

3
Text, pars. 45-46, Section IX; attached memoranda

MATERIALS REQUIRED
SUGGESTIONS

Cross-section paper of 1/4 inch squares
Review Section VIII, TM 11-485

EXERCISES

Weight

- 35 1. What are the characteristics of the normal Playfair cipher which make it recognizable?
- 20 2. Solve the following and recover the keyword:

	5					10					15				
A	QO	AP	QO	CM	PQ	BQ	HO	<u>WE</u>	<u>OB</u>	DQ	WE	LC	FT	OF	TE
B	OC	AO	OC	CK	BX	CM	BV	LF	LX	<u>EX</u>	<u>TW</u>	<u>SD</u>	<u>ND</u>	VL	VR
C	FR	XV	AR	<u>VD</u>	<u>LZ</u>	<u>SB</u>	<u>XV</u>	FW	QV	DL	BK	CM	<u>SB</u>	<u>XV</u>	<u>WS</u> →
D	<u>QO</u>	<u>PA</u>	BQ	TE	OC	FR	BV	VQ	QV	TL	VQ	CX	LY	FW	<u>WS</u> →
E	<u>QO</u>	<u>PA</u>	BZ	RF	PV	IV	VD	SZ	<u>TW</u>	<u>XE</u>	<u>WE</u>	OB	IR	DC	PV
F	VZ	<u>SD</u>	<u>ND</u>	MD	FV	ZD	MH	ZD	VP	BG	MH	DC	VB	RO	CK
G	PA	AP	MS	AO	<u>TW</u>	<u>XE</u>	<u>VD</u>	<u>LZ</u>	VL	ZR	RZ	LY	OQ	RZ	QR
H	CS	AR	DC	MA	YM	MS	BX	LP	TK	TK	DW				

~~RESTRICTED~~

~~RESTRICTED~~

- 20 3. The following cryptogram is suspected to contain the word DIVISION. Solve it and recover the original enciphering square.

	5	10	15
A	MP <u>QK KA</u> SZ <u>QK KA</u> HX <u>EH LK</u> YS ND <u>TP CQ</u> OL NP		
B	RC AH <u>LM SK</u> ND YG QK <u>DU RF</u> QK <u>EH LK</u> YS ND TP		
C	SA OE SY FR QP FE YS MO FD AF RJ RS <u>DU RF</u> RN		
D	<u>TP CQ</u> UL <u>LM SK</u> ND UD FM JE HR VN QK UD EC LF		
E	AK BH IY QV SM FO SY DY		

- 20 4. a. Solve the following cryptogram and recover the original enciphering square. It is suspected that this message is signed "WINTHROP COL INF."

	5	10	15
A	4L 65 4L C3 <u>1V</u> PV 7W XV ZX <u>B1</u> DS 07 L4 CW 4K		
B	OF RT <u>4L 79</u> OL HR YN MR RM DQ QV 9R 6M CX 4K		
C	QF 4N <u>4L 79</u> OL HR OP E4 NR QB 4M XS WN \emptyset E NU		
D	GC QX 4K \emptyset D <u>51</u> NP Z5 4R L4 VQ PF HN <u>4L 79</u> OL		
E	<u>HR</u> EM 8X <u>41</u> ND AP <u>Z1</u> 4N XC M4 RT P6 4M 5H FZ		
F	C3 R9 Q4 CI 2H XZ 48 <u>10</u> L4 YN PQ LM HR T4 PQ		
G	BQ RM D3		

- 2 b. What is the principal disadvantage of such a system for military purposes?

~~RESTRICTED~~

~~RESTRICTED~~

- 20 5. The following message was intercepted and solved by the cryptanalytic section at GHQ. The plaintext was found to read: "DIVISION RESERVES HAVE REACHED CROSSROADS EIGHT NINE THREE DASH B." Reconstruct the general system and show the specific key:

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

6. From the solution of three Playfair ciphers, the following squares were derived. Reconstruct the original squares and show the keywords.

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

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

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

~~RESTRICTED~~

~~RESTRICTED~~

DIGRAPHIC FREQUENCY DISTRIBUTIONS

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

4 5 7 10 7 2 2 2 5 4 4 8 4 6 9 5 1 11 6 5 2 7

Problem 2

~~RESTRICTED~~

~~RESTRICTED~~

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

Problem 3

~~RESTRICTED~~

~~RESTRICTED~~**MEMORANDUM ON PLAYFAIR KEYWORD DERIVATION**

1. Reconstruction of the square in Playfair ciphers takes place concurrently with the evolution of the plaintext, once a few correct assumptions are made. However, the square that is derived may not necessarily be the original enciphering square: more than likely it will be one of the 24 possible cyclic permutations of the original square. If the Playfair consisted of a keyword-mixed sequence, a permutation of the square will cause no difficulty in recovering the original matrix and hence the keyword. For example, if the derived square is Q T L N O then the square P Y R A M

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

is easily constructed because of the tell-tale letters U V W X Z occurring in a row of the derivative square. But when the Playfair square consists of a transposition-mixed sequence, then a different procedure must be adopted.

2. As an example, let us take the transposition matrix

5 8 6 1 4 3 2 7 from which A F T D K is the original square. Using the methods illustrated in a previous memorandum ("Alphabet reconstruction and keyword derivation"), the columns I D S will afford rapid recovery of the keyword. But if instead of the original

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

square we had one of its permutations such as Q S Z R E , then the columns F V O are

H K L	
V W X	

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

without significance; therefore the procedure above is inapplicable without a slight modification.

3. Since it will be noted that a permutation of the rows will not affect the procedure of keyword recovery, then we construct a 9 x 5 rectangle Q S Z R E Q S Z R which contains

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

the five squares of the successive permutations of the columns. A 5 x 5 cut-out square will be found convenient in testing each permutation in turn. Affirmative results will be obtained when the correct permutation is reached, which in this case is the third square in the rectangle, namely

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

~~RESTRICTED~~

~~RESTRICTED~~

DIGRAPHIC IDIOMORPHS: PLAYFAIR

AB BA

SC	AB BA	RD	SH	EL LE	D-
	AF FA	BL E-	-H	EM ME	DI N-
	AF FA	IR	ST	EM ME	D-
-B	AG GA	GE	ST	EP PE	D-
-H AW	AI IA	N-	AV	ER RE	D-
	AL LA	RE AS	CO	NF ER	RE D-
-B	AL LA	ST	-I	NT ER	RE D-
-F	AL LA	CY	-R	EF ER	RE D-
IN ST	AL LA	TI ON S-		ES SE	NC E-
-P AR	AL LA	X-		ES SE	NT IA L-
	AP PA	RA TU S-	AD	DR ES	SE S-
	AP PA	RE L-	-C	OM PR	ES SE D-
	AP PA	RE NT	CO	NF ES	SE D-
	AP PA	RE NT LY	IM	PR ES	SE D-
	AR RA	NG E-	-L	ES SE	N-
	AR RA	Y-	-M	ES SE	NG ER
-B	AR RA	CK S-	PR	ES SE	D-
-B	AR RA	GE	PR	OF ES	SE D-
-E MB	AR RA	SX SE D-	-P	RO GR	ES SE D-
-N	AR RA	TI ON	-S	TR ES	SE D-
	AS SA	IL AN T-	-S	TR ES	SE S-
	AS SA	UL T-	-V	ES SE	L-
-A MB	AS SA	DO R-	WI	TN ES	SE S-
-I MP	AS SA	BL E-		AB ET	TE D-
-M	AS SA	CR E-	-C	IG AR	ET TE S-
-P	AS SA	GE	-B	ET TE	R-
	AT TA	CH	-L	ET TE	R-
	AT TA	CK	-E	IG HT	TH RE E-
	AT TA	IN	-R	IB BI	NG
-B	AT TA	LI ON	FO	RB ID	DI NG
-R	AT TA	N-	-D	IF FI	CU LT
	BO OB	YT RA P-	-B	IL LI	ON
IN	DE ED		-F	IL LI	NG
-W	EB BE	D-	-K	IL LI	NG
	EF FE	CT	-M	IL LI	ME TE R-
	EF FE	CT IV E-	-M	IL LI	NG
CO MP	EL LE	D-	-M	IL LI	ON
-E XC	EL LE	NC E-	SH	IL LI	NG
-E XC	EL LE	NT	SP	IL LI	NG
-E XP	EL LE	D-	-T	IL LI	NG
-I MP	EL LE	D-	-W	IL LI	AM
-P	EL LE	T-	-W	IL LI	NG
PR OP	EL LE	D-		IM MI	GR AN T-
-R EP	EL LE	D-		IM MI	GR AT IO N-

~~RESTRICTED~~

~~RESTRICTED~~

AB BA			AB — BA		
	IM MI	NE NT	PR AC	TI CA	BL E-
SW	IM MI	NG	PR AC	TI CA	L-
-B EG	IN NI	NG	-T AC	TI CA	L-
SP	IN NI	NG	-D IV	EB OM	BE R-
-W	IN NI	NG		EN GI	NE ER
CL	IP PI	NG	-G	EN UI	NE
SH	IP PI	NG	-I NT	ER FE	RE
-S TR	IP PI	NG	-I NT	ER FE	RE NC E-
	IR RI	GA TI ON	-P EN	ET RA	TE
-M	IS SI	NG	-R	EV OL	VE R-
-M	IS SI	ON		IN FI	NI TE
-A DM	IS SI	ON	-D	IS PO	SI TI ON
EM	IS SI	ON	-S	IT UA	TI ON
-H	IS SI	NG	CA	NA DI	AN
PE RM	IS SI	ON	VE TE	RI NA	RI AN
TR AN SM	IS SI	ON		NI NE	TE EN
EM	IT TI	NG		NI NE	TE EN TH
-F	IT TI	NG		PE RC	EP TI ON
-S PL	IT TI	NG	-P	RE MI	ER
PE RM	IT TI	NG	-S UR	RE ND	ER
-A FT ER	NO ON		-O UR	SE LV	ES
FO RE	NO ON		TH EM	SE LV	ES
	NO ON	TI ME	DE	SE RV	ES
-F	OL LO	W-	RE	SE RV	ES
-H	OL LO	W-		SE RV	ES
-C	OM MO	N-			
-C	OM MO	TI ON			
PO SI TI	ON NO	RT HO F-			
-R EC	ON NO	IT ER			
	OP PO	RT UN E-			
	OP PO	RT UN IT Y-			
	OP PO	SE			
	OP PO	SI TE			
	OP PO	SI TI ON			
-C	OR RO	BO RA TE			
-C	OR RO	DE			
-T OM	OR RO	W-			
-B	OT TO	M-			
-C	OT TO	N-			
CA	RE ER				
-S	UC CU	MB ED			

~~RESTRICTED~~

~~RESTRICTED~~

AB — — BA

DE BA RK ED
DE CL AR ED
DE FE ND ED
DE MA ND ED
DE PA RT ED
DE PL OY ED
DE PO RT ED
DE SE RT ED
DE TA CH ED

PR

EC ED EN CE

EM PL OY ME NT

EN TR AI NE D-

ME AS UR EM EN T-

NE GL IG EN CE

NO TA TI ON

PA RA GR AP H-

RE CE IV ER

RE CO RD ER

RE GI ST ER

RE PE AT ER

RE PO RT ER

RE VO LV ER

-P

RO JE CT OR

AS

SE MB LI ES

AB — — — BA

DE SE CR AT ED

DE SI GN AT ED

DE SP AT CH ED

EN EM YP LA NE S-

-D ET ER IO RA TE

-S EV EN TY FI VE

IR RE GU LA RI TY

NO MI NA TI ON

SU SP IC IO US

AB — — — — BA

DE MO NS TR AT ED

NO TI FI CA TI ON

~~RESTRICTED~~

~~RESTRICTED~~

**EXTENSION COURSE OF THE ARMY SECURITY AGENCY
LESSON ASSIGNMENT SHEET**

SUBCOURSE 20-6

LESSON 8

CREDIT

TEXT ASSIGNMENT

MATERIALS REQUIRED

SUGGESTIONS

EXERCISES

Weight

Military Cryptanalysis, Part I

Polygraphic substitution: quadricular
tables

3

Text, Section IX

Cross-section paper of ¼ inch squares

Review Section VII, TM 11-485

30

1. The following cryptogram is suspected to contain the word RECON-
NAISSANCE. Solve the text, and reconstruct the enciphering diagram:

5

10

15

A	SA	<u>CJ</u>	<u>JY</u>	RO	HT	KP	LP	DO	CV	PS	LN	PE	GN	RP	SP
B	FP	LU	<u>QT</u>	<u>LW</u>	PR	CJ	KL	RN	QE	RO	CV	MF	SE	LZ	QZ
C	RR	AO	TH	SQ	PG	TL	GL	NR	QS	UZ	KK	<u>KK</u>	<u>JE</u>	MV	NL
D	LU	AR	QE	SA	MW	KK	LP	SL	AP	PZ	QV	KK	PB	<u>CJ</u>	<u>JY</u>
E	RL	CJ	HA	CO	AR	BH	LL	JH	QT	RP	AS	SL	RP	SL	NL
F	<u>QJ</u>	<u>QT</u>	<u>AJ</u>	NL	IG	NR	WX	AI	HI	YD	<u>KK</u>	<u>JE</u>	CP	YO	SP
G	KO	FB	QT	QP	YP	NZ	SO	AM	DZ	KR	FP	SX	PK	FJ	PR
H	OE	AK	CE	AS	LP	DO	PB	SI	AX	SX	PB	LP	HT	WX	RF
J	GZ	<u>QT</u>	<u>LW</u>	PR	<u>CJ</u>	<u>JY</u>	AK	HT	JY	AA	NN	SX	CB	RO	WE
K	SA	RD	LL	ML	AX	AF	YU	NC	PK	MS	NE	<u>QJ</u>	<u>QT</u>	<u>AJ</u>	

~~RESTRICTED~~

~~RESTRICTED~~

35 2. This cryptogram is suspected of having a beginning similar to that of Problem 1. Solve the text, and reconstruct the enciphering diagram:

	1	2	3	4	5	6	7	8	9	10
A	003	<u>315</u>	097	114	347	261	067	217	314	241
B	195	062	350	115	006	451	062	<u>141</u>	<u>072</u>	472
C	189	192	018	400	189	067	<u>315</u>	<u>097</u>	530	403
D	<u>115</u>	<u>393</u>	262	609	192	356	115	186	122	467
E	212	071	074	237	235	114	416	<u>115</u>	<u>393</u>	271
F	055	293	186	552	009	062	471	141	150	193
G	186	516	184	266	274	470	002	238	053	186
H	<u>141</u>	<u>072</u>	236	516	189	004	195	191	479	067
J	008	397	080	137	105	189	391	262	343	408
K	133	273	071	084	274	400	367	223	403	186
L	211	524	008	292	011	122	393	284		

~~RESTRICTED~~

~~RESTRICTED~~

85

3. This cryptogram is suspected to begin with the stereotype "REFERRING TO YOUR MESSAGE" or "REFERENCE YOUR MESSAGE." Solve the text, and reconstruct the enciphering diagram:

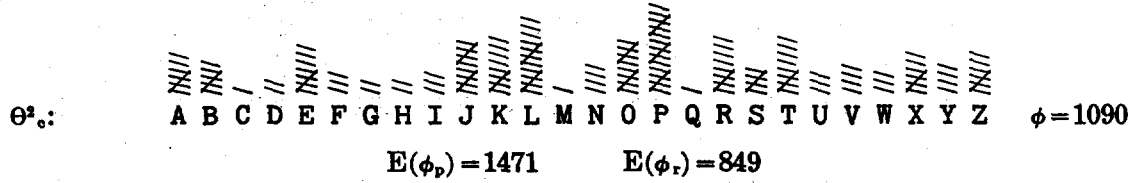
	1	2	3	4	5	6	7	8	9	10
A	MRA	DMT	<u>GCI</u>	YIY	MFG	NNL	SRK	QFB	<u>DMD</u>	WII
B	DSZ	GNM	IJA	GOO	<u>LGI</u>	DEV	LTD	<u>GCI</u>	IYD	LCI
C	MMT	JIU	PNM	VZP	<u>LGI</u>	DMY	ITI	<u>POV</u>	GIP	TGO
D	PLM	MCH	JPB	MRC	<u>DGK</u>	FWJ	IHC	EEF	MDO	DSZ
E	TEN	<u>DGK</u>	<u>FWI</u>	NNM	LEV	EZF	TAS	DIP	HMT	TDL
F	GTR	QMD	MZU	R0D	NPC	JNJ	<u>GCI</u>	<u>IQM</u>	UZK	LIY
G	NJN	CWQ	MZF	VOD	NWG	PRG	NLC	URP	MIA	DGI
H	VRG	NRF	URV	PIF	DUJ	TDL	POJ	VRT	DAZ	MRI
J	IFX	DGG	DHV	<u>VZP</u>	<u>IQM</u>	<u>EMF</u>	JPC	SMK	JLM	MND
K	PQW	YZB	OZN	IJY	IPJ	DMD	YJP	NIP	<u>EMF</u>	JPC
L	<u>SMK</u>	<u>JLF</u>	ENG	NPW	FNV	FJJ	IWI	GTT	MOT	EOW
M	CRV	WLF	ELE	TSZ	TNM	VRS	MTR	TEQ	VRV	QJQ
N	MRV	<u>NOV</u>	<u>GIP</u>	RMT	KQX	GCJ	ELC	MZH	PRT	LMN
P	LCR	IYR	CZY	GPW	XPA					

~~RESTRICTED~~

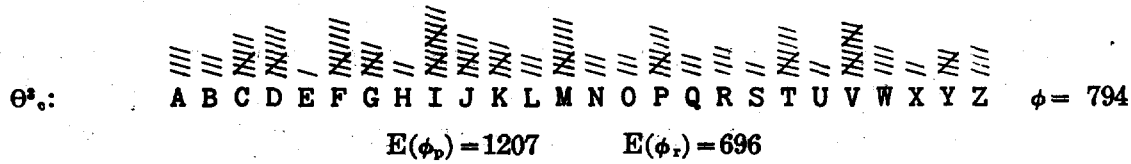
~~RESTRICTED~~

FREQUENCY DISTRIBUTIONS

Problem 1



Problem 3

~~RESTRICTED~~

~~RESTRICTED~~

**EXTENSION COURSE OF THE ARMY SECURITY AGENCY
LESSON ASSIGNMENT SHEET**

SUBCOURSE 20-6

LESSON 9

CREDIT

TEXT ASSIGNMENT

MATERIALS REQUIRED

SUGGESTIONS

EXERCISES

Weight

Military Cryptanalysis, Part I

Miscellaneous monoalphabetic substitution systems

3

Text, Section X

Cross-section paper of ¼ inch squares

Read appended Partial Analysis Sheets

- 2 1. *a.* What characters are most used in practical cryptography today?
- 2 *b.* What is the usual preliminary procedure in solving cryptograms involving symbols?
- 4 *c.* In monoalphabetic substitution with variants, what characters are most commonly used? Why?
- 2 2. What is the primary purpose of an analytical key?
- 25 3. Solve the following cryptogram, and recover all keys:
- 5 10 15 20 25

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

~~RESTRICTED~~

~~RESTRICTED~~

- 20 4. Below is an intercepted message which is suspected to begin with the words "FIFTH DIVISION." Solve it and recover all keys:

6 7 2 6 7 8 6 5 5 5 7 2 8 7 2 8 5 2 3 7 7 2 8 5 7

6 3 8 7 2 7 7 6 8 4 7 8 2 7 7 8 6 3 7 8 3 8 5 2 8

6 2 3 7 7 8 5 8 6 3 7 8 0 5 8 8 6 2 5 9 5 9 1 5 8

5 6 6 6 0 5 8 5 8 0 6 8 1 6 7 0 5 9 5 9 2 7 7 6 8

5 9 3 8 8

- 20 5. This message below is suspected to contain the same plain text as Problem 4. Reconstruct the general system and recover all keys:

3 5 5 9 1 5 9 2 2 8 8 6 6 0 0 2 4 6 3 5 7 8 8 8 1

7 7 7 7 7 8 4 3 3 0 1 0 4 3 5 5 5 3 9 9 6 6 6 1 1

2 9 8 7 2 5 8 7 0 0 2 9 3 8 8 7 5 0 0 8 0 7 1 0 6

9 7 6 4 0 0 2 3 0 0 3 1 8 5 8 0 6 9 5 8 9 7 4 4 2

0 2 2 3 2 7 6 8 4 9 9 1 3 0 0 1 4 0 9 0 6 8 6 7 8

7 4 9 2 3 0 0 1 0 2 4 4 0 9 2 9 1 1 0 0 5 5 7 2 0

4 9 7 6 6 8 3 3 3 0 7 7 5 1 2 2 4 7 8 0 1 1 1 1 0

3 0 6 6 3 3 0 4 4 4 6 0 1 2 2 1 1 8 9 8

~~RESTRICTED~~

~~RESTRICTED~~

25

6. The enemy is using a system incorporating a 10 x 10 bipartite square consisting of letters, digits and syllables. The row and column coordinates are invariable, but a different internal chart is used each day. The chart for 16 December was reconstructed and found to be based on the keyword PYRAMIDS as follows:

	0	1	2	3	4	5	6	7	8	9
0	P	Y	R	RA	RE	RED	RES	RI	RO	A
1	<u>1</u>	AL	AN	AND	AR	ARE	AS	AT	ATE	ATI
2	M	ME	I	9	IN	ING	ION	IS	IT	IVE
3	D	4	DA	DE	S	SE	SH	ST	STO	B
4	2	BE	C	3	CA	CE	CO	COM	E	5
5	EA	ED	EN	ENT	ER	ERE	ERS	ES	EST	F
6	6	G	7	H	8	HAS	HE	J	Ø	K
7	L	LA	LE	N	ND	NE	NT	O	OF	ON
8	OR	OU	Q	T	TE	TED	TER	TH	THE	THI
9	THR	TI	TO	U	V	VE	W	WE	X	Z

The next day the following cryptogram, suspected to contain the word CROSSROADS, was intercepted. Solve the text, reconstruct the chart for the day, and determine the specific key:

			5			10			15						
A	20	88	<u>50</u>	<u>58</u>	<u>95</u>	63	62	30	69	69	94	15	58	<u>92</u>	<u>07</u>
B	84	73	60	35	77	95	61	38	<u>78</u>	<u>30</u>	<u>50</u>	66	94	15	44
C	84	62	12	12	20	38	31	42	67	67	93	52	01	83	10
D	32	02	79	10	36	84	72	94	44	68	79	54	78	69	<u>50</u>
E	58	95	58	79	62	14	30	<u>50</u>	71	<u>94</u>	<u>35</u>	87	79	<u>97</u>	<u>58</u>
F	<u>02</u>	<u>02</u>	10	78	47	22	97	58	88	09	84	53	03	01	93
G	44	78	79	79	<u>78</u>	<u>30</u>	<u>50</u>	79	57	55	59	54	08	54	94
H	72	89	72	60	82	72	94	44	<u>92</u>	<u>07</u>	79	82	05	10	79
J	94	10	10	02	58	28	<u>97</u>	<u>58</u>	<u>02</u>	<u>02</u>	43	69	05	96	50
K	93	<u>50</u>	<u>58</u>	<u>95</u>	63	58	07	11	21	<u>50</u>	<u>71</u>	<u>94</u>	<u>35</u>	84	27
L	30	54	87	50	35	68									

~~RESTRICTED~~

~~RESTRICTED~~

PARTIAL ANALYSIS SHEETS
LESSON 9, MILITARY CRYPTANALYSIS, PART I

Problem 3

In taking a uniliteral frequency distribution of this cryptogram, it was observed that the positions of the peaks and troughs of the distribution seemed to change during the compilation. The over-all distribution is

8	7	9	6	6	12	10	20	19	11	18	9	5	6	9	21	4	22	10	24	5	19	8	21	3	N=300	
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	
$\phi = 4136$						$E(\phi_p) = 5983$						$E(\phi_r) = 3363$														

If the cryptogram is divided into two 150-letter sections, then the distributions are as follows:

	5	4	5	2	1	7	5	8	10	9	12	5	6	1	4	2	10	-	10	2	14	2	9	3	13	1		
1.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z		
	$\phi = 1144$																											
	3	3	4	4	5	5	5	12	9	2	5	4	3	4	2	7	11	4	12	8	10	3	10	5	8	2		
2.	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		
	$E(\phi_p) = 1520$														$E(\phi_r) = 868$													

When the message is divided into three 100-letter sections, then

	5	2	2	2	1	6	5	5	8	4	6	3	5	1	3	-	9	-	6	1	11	1	6	1	6	1		
1.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z		
	$\phi = 498$																											
	2	3	5	-	4	1	3	4	6	6	7	3	2	2	2	8	5	3	5	1	5	2	6	2	13	-		
2.	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		
	$\phi = 484$																											
	1	2	2	4	1	5	2	11	5	1	4	3	2	2	1	1	7	1	11	8	8	2	7	5	2	2		
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		
	$E(\phi_p) = 660$														$E(\phi_r) = 381$													

When divided into four 75-letter sections, the distributions are

	4	1	2	1	1	5	4	4	5	3	4	3	5	1	1	-	6	-	4	1	11	1	4	-	3	1		
1.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z		
	$\phi = 293$																											
	1	3	3	1	-	2	1	4	5	6	8	2	1	-	3	2	4	-	6	1	3	1	5	3	10	-		
2.	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		
	$\phi = 306$																											
	2	2	2	1	5	2	3	2	4	1	2	2	2	2	1	6	5	4	5	4	2	3	3	3	7	-		
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		
	$\phi = 212$																											
	1	1	2	3	-	3	2	10	5	1	3	2	1	2	1	1	6	-	7	4	8	-	7	2	1	2		
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		
	$E(\phi_p) = 370$														$E(\phi_r) = 212$													

~~RESTRICTED~~

~~RESTRICTED~~

Upon dividing the text into five 60-letter sections, the distributions are

1.	4 1 - 1 1 3 3 4 5 3 2 3 5 1 1 - 4 - 3 1 8 1 3 - 2 1	$\phi = 180$
	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z	
2.	1 1 4 1 - 3 2 2 3 4 5 2 1 - 2 - 5 - 7 - 3 1 4 1 8 -	$\phi = 200$
	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.	- 3 2 - 2 1 - 2 6 3 5 - 1 2 2 6 3 2 1 1 4 1 4 2 7 -	$\phi = 178$
	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	
4.	2 1 2 3 3 4 4 3 - - 2 2 1 - - 2 4 2 5 7 2 2 1 4 4 -	$\phi = 156$
	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	
5.	1 1 1 1 - 1 1 9 5 1 3 2 1 2 1 1 5 - 6 1 7 - 7 1 - 2	$\phi = 238$
	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	
	$E(\phi_p) = 236$ $E(\phi_r) = 136$	

Finally, upon dividing the cryptogram into six 50-letter sections, the distributions are

1.	≡ - - - ≡ ≡ ≡ ≡ ≡ - - ≡ - - ≡ ≡ ≡ ≡ ≡ - - ≡ ≡ ≡ - -	$\phi = 123$
	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z	
2.	- - ≡ - - ≡ ≡ ≡ ≡ ≡ - ≡ ≡ ≡ ≡ ≡ ≡ ≡ ≡ ≡ ≡ ≡ - - ≡	$\phi = 142$
	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.	≡ ≡ ≡ - - ≡ ≡ ≡ ≡ ≡ - - - - ≡ ≡ ≡ ≡ ≡ ≡ ≡ ≡ ≡ ≡ ≡	$\phi = 138$
	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	
4.	≡ - - ≡ ≡ ≡ ≡ ≡ - - - - - - ≡ ≡ ≡ ≡ ≡ ≡ ≡ ≡ ≡ ≡ ≡	$\phi = 122$
	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	
5.	≡ ≡ ≡ ≡ ≡ ≡ ≡ - - - - - - ≡ ≡ ≡ ≡ ≡ ≡ ≡ ≡ ≡ ≡ ≡	$\phi = 148$
	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	
6.	- - - - ≡ ≡ ≡ - - ≡ ≡ - - - - ≡ ≡ ≡ ≡ ≡ ≡ ≡ ≡ ≡ ≡	$\phi = 192$
	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	
	$E(\phi_p) = 163$ $E(\phi_r) = 94$	

This last set of distributions gives the most satisfactory results, both as regards the ϕ -test and also the expected number of blanks (cf. chart on page 25 of Text). From these several sets of distributions we were trying to determine the first two or three sections of the text that were monoalphabetically enciphered. The division not only seems to be approximately 50 letters, but it also appears that practically all the sections are of equal length.

~~RESTRICTED~~

~~RESTRICTED~~

**EXTENSION COURSE OF THE ARMY SECURITY AGENCY
LESSON ASSIGNMENT SHEET**

SUBCOURSE 20-6	Military Cryptanalysis, Part I
EXAMINATION	
CREDIT	3
TEXT ASSIGNMENT	None
MATERIALS REQUIRED	Cross-section paper of ¼ inch squares
SUGGESTIONS	None
EXERCISES	
Weight	

Until now the problems of each lesson have followed very closely the order of subject matter in the text, so that the student knew fairly well what types of systems were involved. This examination is designed to test the student's power of observation and logic in determining the general cryptographic system. All that is required in the five problems below is the determination of the general system, together with the reasons for the particular classification. Solution of the message texts is not mandatory, but strongly recommended: recovery of the plaintexts and specific keys certainly would furnish the student with irrefutable proof of the validity of his hypotheses.

20 1. L W H P C X B V L W H V K Z J P B P G R B X H S L
 Q K R H V F R L X B T C S B P K S B Z K R C N B P
 F W H P D W H V G T B P D S B N D Q K W F T B V F
 Q F R H R D Z D S H P D Q K Z B X G V H N L R F X
 H Q C Z K S B V J Q M R H X B S L Q B R F W J S B
 T K Z H W M S B N L S B Q B X K S D T H T M N H P
 C T B P H V D S J V D W H V H N L Q H P C Q C R B
 R L W K R H V F X F R B N C S B P J P H V D Z F Z
 B V L W C W B Z F S B W B P L X X X X X

~~RESTRICTED~~

~~RESTRICTED~~

20 2. EMURB WPZLS ERMWU ROBOP UWBWB
 Q T I O N I Y B H Y V M I W B E G O P S C D V C C
 O D C X S O U D I Y M C Y X D Y H S O U S M O N B
 Q T I O N O B O P Z D N O I L L B E R O R T R E M
 D T E N R T B N T A K B C O O B O B E Z S K Z Z S
 M E G E B D F G N S H R L I X S E S V R L E S U U
 S K S P E W L D E G B W D M T Z T I O N S I V M E
 R E T A K P H T I M B H H O H I Z U D M O E K H P

20 3. GHUIP GJHNI MBSPR IUSNS SHPGB
 R Q S A J O O Q R S S I P Q S M H V J I P Q I V V
 J F K I H G S A N Y P T K K D Y J K Q X Z V N P R
 O Q N J S N U Y E F E N P Z V N P R O Q Q T K L N
 F F H O N Q U P O Q H U Q T V O T N D O J T K L P
 O W O J T E J W N Q E K J A E I O U T I Q Q G T B
 A N N K Z X V U K R E M M Q R R T E I I K V P X V
 U K R R E M W K I K V P X V U D A E I P R S Q I I
 G W Q L Q U X V V X V U A T G W Q Q V P

~~RESTRICTED~~

~~RESTRICTED~~

- 20 4. These two messages were intercepted on the same circuit during a morning offensive.

Message "A"

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

Message "B"

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

- 20 5.

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

~~RESTRICTED~~

~~RESTRICTED~~

~~RESTRICTED~~