~~CONFIDENTIAL~~
~~Modified Handling Authorized~~

NATIONAL SECURITY AGENCY

PROBLEM BOOK

COURSE, MILITARY CRYPTANALYTICS, PART I

(Short title: MC–I Problems)

NOTICE: This material contains information affecting the national defense of the United States within the meaning of the espionage laws, Title 18, U.S.C., Sections 793 and 794, the transmission or the revelation of which in any manner to an unauthorized person is prohibited by law.

National Security Agency
Washington 25, D. C.

May 1954

~~CONFIDENTIAL~~
~~Modified Handling Authorized~~

NATIONAL SECURITY AGENCY

PROBLEM BOOK

COURSE, MILITARY CRYPTANALYTICS, PART I

(Short title: MC–I Problems)

National Security Agency
Washington 25, D. C.

May 1954

(BLANK)

COURSE IN MILITARY CRYPTANALYTICS, PART I

Monoalphabetic Substitution Systems

Introduction

This is the first of a series of six basic courses in the science of military cryptanalytics. The purpose of this course is to impart to the student the methods and techniques which form the basis for the cryptanalysis of simple types of military cipher systems. An understanding of these principles is necessary to grasp the more advanced cryptanalytic techniques employed in the attack on the complex cryptosystems which constitute present-day military cryptography.

The scope of this course is: fundamental principles; uniliteral substitution; multiliteral substitution; polygraphic substitution; and miscellaneous monoalphabetic substitution systems. It consists of 10 lessons as follows:

Lesson 1, Fundamental principles

Lesson 2, Uniliteral substitution with standard and mixed cipher alphabets

Lesson 3, Multiliteral substitution: miscellaneous matrices; Baconian and Trithemian systems; elementary Baudot-systems

Lesson 4, Multiliteral substitution with variants

Lesson 5, Polygraphic substitution: four-square and two-square matrices

Lesson 6, Polygraphic substitution: Playfair cipher systems

Lesson 7, Polygraphic substitution: large tables

Lesson 8, Monoalphabetic substitution with irregular-length cipher units: monome-dinome systems and others

Lesson 9, Syllabary squares and code charts

Lesson 10, Miscellaneous monoalphabetic substitution systems; concealment systems

The text reference for this course is the National Security Agency publication "Military Cryptanalytics, Part I" by W. F. Friedman and L. D. Callimahos. The portion of the text which should be read by the student prior to doing each lesson is indicated in the lesson heading as the TEXT ASSIGNMENT. There are certain text *appendices* from which the student will derive considerable assistance in almost every lesson of this course, namely, Appendices 2, 3, and 4; no further restatement concerning these appendices will appear in the TEXT ASSIGNMENT of any lesson because of their universal applicability, but the student should become familiar with these appendices early in the course and should refer to them as often as necessary when working on each lesson.

This course has been designed as a self-study or extension-type course. The cryptograms contained herein have for the most part been arranged in proper worksheet form, obviating the necessity of recopying; and frequency distributions have been given to reduce the amount of time spent on the purely clerical labor incidental to the solution. The underlying texts of the cryptograms comprise hypothetical ground, naval, air, and general administrative messages. Where necessary for solution, the specific nature of the text of any particular cryptogram is indicated. Otherwise, the text of a message may be assumed to be general administrative or ground text.

The only materials required are cross-section paper of ¼-inch squares, and a set of printed and blank alphabet strips. An eraser is of the utmost importance.

Special Instructions

So far as is practicable, detailed work sheets which usually form a part of the solution should be submitted with the solutions. In all the lessons of this course, it is required that the student recover all cipher alphabets, cipher tables, and specific keys used. He will also be required to state the method of operation of each cryptosystem and give the key words upon which each component is based.

NATIONAL SECURITY AGENCY
Washington 25, D. C.

COURSE	Military Cryptanalytics, Part I
LESSON 1	Fundamental principles
TEXT ASSIGNMENT	Chapters I–IV, inclusive

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

   b. What six additional elements are also highly desirable?

2. *a.* Define the terms "cryptology", "cryptography", "cryptanalytics", and "cryptanalysis."

   b. What are the essential differences between substitution and transposition?

   c. Differentiate between a code and a cipher system.

   d. Explain the difference between the terms "general system" and "specific key."

   e. Distinguish between monoalphabetic and polyalphabetic substitution.

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

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

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

6. Indicate the language in which you would expect the plain text of the encrypted portion of the following message to be written. Give reasons for your answer.

From: João Fialho, Rio de Janeiro.
To: Gualterio Costa, Lisbon.

Com referência ao seu telegrama. NSM NRJPN INJ PMVCOCEN VNPSN PMBMPCEN QMT JBCVCJ IJUM DTGAJ LTMCPN KPJUCEMIVCNP PMHMQQN UMIVCHMISJQ SMPVMCPJ SPCHMQSPM.

7. *a.* The letter *E* represents what percentage (to the nearest *whole* percent) of the letters in English telegraphic text?

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

   c. What are the five letters of lowest frequency in English telegraphic text?

   d. What are the four most frequent digraphs in English telegraphic text?

   e. Account for the discrepancies between frequencies of letters in English literary text and English telegraphic text.

8. What three facts can be determined from a study of the uniliteral frequency distribution?

9. In the following extract from a speech given during World War II, each dash indicates the omission of a letter. Complete the text by writing the necessary letters over each dash to form appropriate words.

"Washington's Birthday is a most a p _ _ _ _ _ _ _ _ _ _ occasion for us to talk with each _ _ _ _ _ about things as they are _ _ _ _ _ and things as we _ _ _ _ they shall be in the _ _ _ _ _ _.

"For _ _ _ _ t years, General Washington and his _ _ _ _ _ _ _ _ _- _ _ _ Army were faced c o _ _ _ _ _ _ _ _ _ _ with formidable _ _ _ _ and recurring _ _ _ _ _ _ _. _ _ _ _ _ _ _ _ and equipment were lacking. In a _ _ _ _ _, every winter was a Valley Forge. Throughout the _ _ _ _ _ _ _ _ _ states there existed selfish men, jealous men, _ _ _ _ _ u l men, who _ _ _ _ _ _ _ _ _ _ _ that Washington's _ _ _ _ _ was hopeless, that he should ask for a n _ _ _ _ _ _ _ _ _ peace.

"Washington's _ _ _ _ _ _ _ in those hard _ _ _ _ _ has provided the _ _ _ _ _ for all Americans ever since--a model of moral _ _ _- _ _ _ a. He held to his _ _ _ _ _ _, as it had been charted in the Declaration of Independence. He and the _ _ _ _ _ men who _ _ _ _ _ _ with him knew that no man's life or _ _ _ _ _ _ _ was secure, without freedom and free i _ _ _ _ _ _ _ _ _ n s.

"The present _ _ _ _ _ struggle has _ _ _ _ _ _ us increasingly that _ _ _ _ _ o m of person and _ _ _ _ _ _ _ y of property anywhere in the _ _ _ _ _ depend upon the security of the rights and obligations of liberty and _ _ _ _ _ _ _ everywhere in the world.

"This war is a new _ _ _ _ of war. It is _ _ _ _ _ _ _ _ _ _ from all other wars of the _ _ _ _, not only in its methods and _ _ _ _ _ _ _ but also in its geography. It is warfare in terms of every c o n _ _ _ _ _ _, every _ _ _ _ n d, every sea, and every a _ _-_ _ n e in the world. The _ _ _ _ _ oceans which have been h e r _ _ _ _ _ in the past as our _ _ _ _ _ _ _ _ _ _ _ from attack have become _ _ _ _ _ s s battlefields on which we are _ _ _- _ _ _ _ _ _ being challenged by our enemies."

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

(1) AT NOTHING REPORT THIS TIME TO

(2) ARTILLERY SECTOR BARRAGE NORTHWEST HEAVY IN

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

(1) Eight SESTYODRER have DTPADERE to join SAKT REOFC

(2) ABELNU to contact ATTAINBLO on my right AFKLN

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

(1) OLANG RIDGE TANK GIMNOV EHOTISL EAST NOMLCU

(2) DOWN MEYEN OFANERTON SIX THIS OTHS SNEALP

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

(1) ADELY AACKTT CDDEEHLSU OT CCEEMMNO AT EGHIT HIST GIMNNOR

(2) ADEEIILMMTY NOPU CEEIPRT ADHIRTWW OT AADEEGNPRRR IINOOPST

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

(1) ORSUU ABIMR AEHNS ENSUV ADKOR ADEGM EEINN EMNVY EELSS S

(2) AEIRR ACNNO AINSS CEEPR AORST ILLRT EEMRY ACELP EMNST DERST

DEOY

11. 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."

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

a. O R A N A T H P N O S K T C D M E E E S C E R A E

R N U S A E T L G D A Y E C A

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

b. D H J J K Q O A H R X K S O F H P Q G A P P H L A

D I A D E H J R O A M A H Q A

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

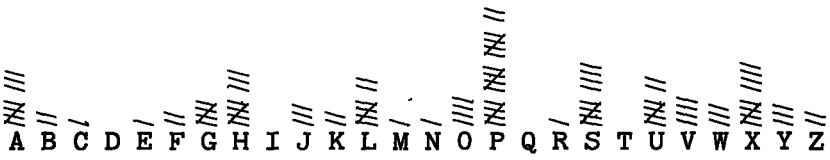
~~CONFIDENTIAL~~

c. R O L E H K B W F Z C Q C P Z N V J W Z M I V E Q
E P C I N O J S J U Y M W Q B

13. Which of the following substitution ciphers are monoalphabetic?

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

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



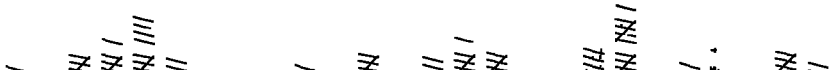
c. G X Y V L Z X M X S L O Z G R W E J L X P W T K Z
G M X L W Q I V Z W Q B R X K K T D V L M X A E X
V H M X A L O T L Y T K D W X G B Q K Q L W Z X G
R T Y Y Z K T O X G A W X L Q L O Z G R X V W G Q

14. 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.

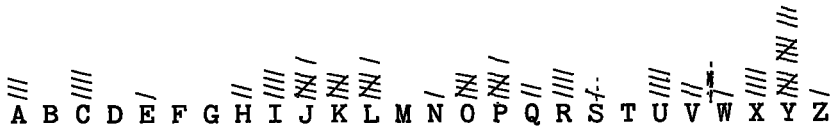
a. A N V O R L O U N Q R L E Z W Z H N E Z W Z B O R
Z K Y L F A O Z S O O N O R F P J Z P P L D Z D N
L R Z L B L A B W Z H N A P O W Q H O O R Z I Z U

~~CONFIDENTIAL~~

b. E S P A P L V D L Y O E C Z F R S D T Y E S T D O
T D E C T M F E T Z Y B F T N V W J T O P Y E T Q
J T E L D O T C P N E D E L Y O L C O N T A S P C



c. P Y H Y L X O L W Y J J V Y X O I L Y R Y Q Y P J
K N Y L K Y H Y L C P A Y A C L Y X I R Q Y J V O
Z K O X C P C R E K U K U P J I U J U O P R I A S



15. Derive the ϕ_p, ϕ_r, ϕ_o, Λ_p, Λ_r, and Λ_o for each of the following distributions, and evaluate the [monoalphabetic] goodness of ϕ_o and Λ_o of each in terms of "good", "fair", or "poor", entering these data in the attached diagram. On the basis of the foregoing, decide which distributions are most probably monoalphabetic and which are most probably non-monoalphabetic, indicating your decision by a check ($\surd$) in the diagram; in the case of those not clearly belonging in either of these categories, check "decision suspended".

a. 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

b. 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 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

d. 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. 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

f. 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. 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

h. 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

	N	ϕ_p	ϕ_r	ϕ_o	Λ_p	Λ_r	Λ_o	Goodness of ϕ_o G	Goodness of ϕ_o F	Goodness of ϕ_o P	Goodness of Λ_o G	Goodness of Λ_o F	Goodness of Λ_o P	Decision mono.	Decision non-mono.	Decision susp.
a.																
b.																
c.																
d.																
e.																
f.																
g.																
h.																

16. From the intercepted traffic of three intercept stations operating in the same sector of the front, the following code 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 code text sent by the enemy station.

I. Time intercepted 1612 by HS W F F DE L D C

GR 35 $\overline{\text{BT}}$

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

II. Time intercepted 161Ø by MR M F F DE L D C

GR 35 $\overline{\text{BT}}$

NR Ø_ D Y B I E B U F T O A M E J A K I B O N
I P K O _ F _ B A K D O D L A L U F Y L K A W A L
A P A Y N _ _ _ _ _ _ _ D U A _ _ P I D J E N O X
N E H A Z L O G I S K U T E G E V A U C I R B W
K E H Z A S O B W E V A D U Z F O F E T E M C O Z
E G B L O D O F Y O A E C D A M A W E N _ _ _ O M
E M C O Z A C F A H L O F I R Ø 9 3 5

~~CONFIDENTIAL~~

III. Time intercepted 1612 by YG W F F DE L D K

GR _ _ $\overline{\text{BT}}$

NR 17 D Y B I E D U F T O A M E J A K S B O N

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

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

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

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

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

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

(BLANK)

NATIONAL SECURITY AGENCY
Washington 25, D. C.

COURSE	Military Cryptanalytics, Part I
LESSON 2	Uniliteral substitution with standard and mixed cipher alphabets
TEXT ASSIGNMENT	Chapters V and VI

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

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

2. *a.* Name two methods of solving monoalphabetic substitution ciphers involving standard cipher alphabets.

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

c. Why do monoalphabetic cryptograms involving standard cipher alphabets yield such a low degree of cryptosecurity?

3. What are four characteristics of vowels which permit their classification as such in monoalphabetic substitution ciphers involving mixed cipher alphabets?

4. *a.* What two places in every message lend themselves more readily to successful attack by the assumption of words than do any other places? Explain.

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

5. *a.* What is meant by the word pattern "A B C B A D B"?

b. For each pattern given below, indicate one good English word that contains the pattern:

(1) A B C B A D B

(2) A A B A

(3) A B C D A

6. Give two reasons why the enciphered text of a military message is generally divided into groups of five characters, prior to transmission.

7. Solve the following cryptogram and indicate the specific key ($A_p = \theta_c$):

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

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

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

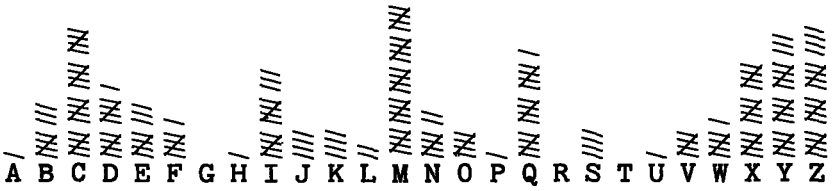
C Y I X I C D Y Y X C B Z Q I F Z C Q N H W D O X

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

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

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

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



$\phi_p = 2655$ $\phi_r = 1531$ $\phi_o = 2636$

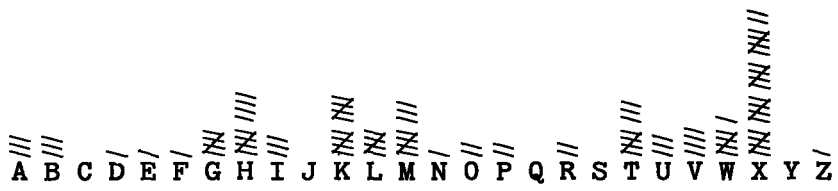
8. Solve the following cryptogram, and indicate the specific key:

W X L M K H R X K L A T O X U X X G H K W X K X W

M H I K H V X X W T M H G V X M H T K X T P A X K

X L N U F T K B G X T V M B O B M R A T L U X X G

K X I H K M X W L M H I T V D G H P E X W Z X X X



$\phi_p = 660$ $\phi_r = 381$ $\phi_o = 848$

9. Solve the following cryptograms, and indicate the specific keys:

a. Q H H Y L Y D W Q J J M E F C

b. Y X S E D Y F S X U H W X U S

10. The following badly garbled cryptogram was intercepted. Reconstruct the original plaintext message, resolving the errors and omissions, and indicate the specific key:

H U V S H U D S U - E K H C U I E Q W U D K - R U

H O X H U U U Y M X J I U - U D T Q J U T E D U A

Y N T U S - - - - - I J E F Y D I J K H S J Y E -

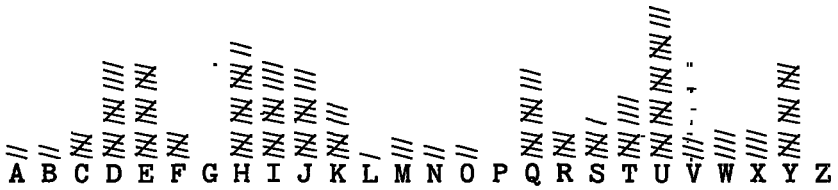
I O Q L U R U U N Y I I K U - J E Q B D I K R H E

T Y D Q J - S E C C Q - T I J E Y D Y W Y Q J U K

D Y J J H Q Y D C D W F H E W H Q K I K D T U H J

X A F H E R Y I Y E D I E V F Q H Q M H Q U X J -

E E V - F - S Y Q B T H T U H I D M C R U H I Y T



$\phi_p = 2270$ $\phi_r = 1311$ $\phi_o = 2136$

11. *a.* Construct a triliteral frequency distribution showing one prefix and one suffix of the letters of the cryptogram below. On the work sheet below, indicate by underscoring in black all repetitions of three or more letters. Other significant details may be marked in different colors.

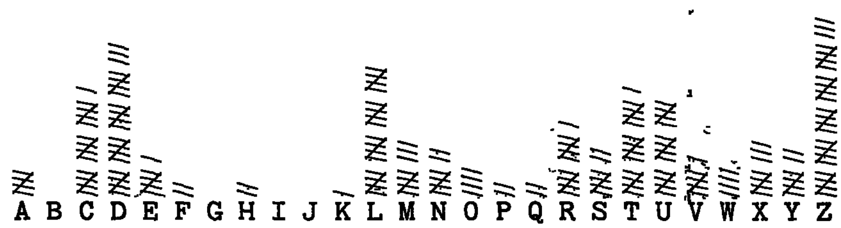
b. Prepare a condensed table of repetitions of digraphs and trigraphs appearing more than twice, and include all repetitions of longer polygraphs.

c. Using the data obtained in *a* and *b* above, complete the solution of the cryptogram, and recover all keys.

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

12. Solve the cryptogram below, suspected to contain the probable word "BLOCKADE"; recover all keys.

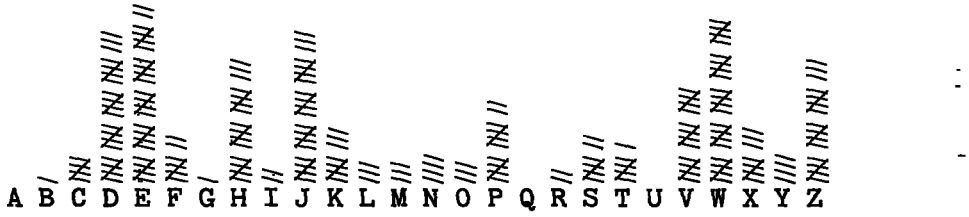
	5	10	15	20	25
A	L C T C E	L U Z O D	U C R E A	W Z U S N	F Z X D Y
B	D R T L D	S D R Z S	D E U C M	U Z Z K Z	U D C D V
C	T Q T X D	A O Y Z C	Z W Y D X	P T V Z D	S C M Z Z
D	R Z A Q L	L D E C M	Z U R X D	T L C M T	L W Z Z R
E	Z S S Z X	C Z V L C	D O U D X	P Z C W T	U U T H Z
F	S U D A D	E U F Z L	L Z Y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



$\phi_p = 2655$ $\phi_r = 1532$ $\phi_o = 2770$

13. Solve the following cryptogram, and recover all keys:

```
          5         10        15        20        25
A | J Z D F V  W H E D Z  V H W D S  Y K T W D  O E D Z D
B | E D S E C  C W H H W  E D Z T E  X X W S Z  V N Z V Z
C | S P F J K  V Z T Y P  H J D W O  L J W D P  V P W T I
D | R E D Z E  X E K V F  P J V E Y  H H J E F  E D Z F V →
E | W H E D Z  V H J P J  Z H J L P  J X E K V  J L T W M
F | W H W E D  W H W D M  W S W D W  J R E X I  Y K Z C E
G | K D J P W  D C E M W  D O N Z H  J J E P J  J P S B E →
H | K V F E H  W J W E D  H N Z H J  E X X P W  V J E N D
J | H J E F S  E D X W V  C P J W E  D V Z G K  Z H J Z T
```



$\phi_p = 3362$ $\phi_r = 1940$ $\phi_o = 3560$

14. Using the sequences recovered in Problem 13, solve the following cryptograms and indicate the specific keys:

a. U R J J R X Q U Q X K S A R B B E T O I

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

$\phi_p = 25$ $\phi_r = 15$ $\phi_o = 16$

b. F D L D Y X Z U M U E U F P N D V O F E A L Y R W

U M L J X A F D Y E X E K Q P D O Y C V R E U A X

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

$\phi_p = 163$ $\phi_r = 94$ $\phi_o = 118$

15. The following cryptograms, enciphered with random cipher alphabets, are in bona fide word lengths. Solve them.

a. H Y A R V J Z G H A R O T V K C G K M M G K H Z M L K U G

L K U G O R O E H O Z E M V H F S R M J R O T

J E H Z P U H G V E G M R O M C J K K S J K U M E

b. R G R Q R U 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

c. C D G W D S A L C A U M M D C R B U C D Y V D V D J R

I Y S U A U Y V S L Z C Y S S C U T D C

16. In solving several unrelated monoalphabetic cryptograms, the following cipher alphabets were reconstructed. Recover the key words from any five of these alphabets. To facilitate solution, significant segments have been underlined.

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

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

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

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

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

f.

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

g.

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

h.

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

NATIONAL SECURITY AGENCY
Washington 25, D. C.

COURSE	Military Cryptanalytics, Part I
LESSON 3	Multiliteral substitution with single-equivalent cipher alphabets
TEXT ASSIGNMENT	Chapter VII

1. Solve the following cryptogram, and recover all keys:

					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										

(For distribution, see next page)

	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	15	2

$\phi_p = 2270$ $\phi_r = 1362$ $\phi_o = 2362$

(25-element alphabet)

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

$\phi_p = 960$ (approx.) $\phi_r = 410$ $\phi_o = 716$

(36-element alphabet)

3. Solve the following cryptogram, and recover all keys:

	5							10						15
A	RG	GP	EE	GR	RG	GP	ES	GR	RG	PP	GE	PR	GE	RG	GS
B	AS	GR	RR	GS	AE	PP	GP	GA	PP	RA	EA	ES	GR	RG	PP
C	GE	RA	PR	GS	RE	GP	AR	GP	GS	PP	GP	RG	RA	EA	PP
D	PS	PG	AR	PE	GA	RR	RG	GP	RR	RE	PG	PP	RA	EA	RS
E	PG	PE	RG	AR	PE	GA	RR	RG	GP	RR	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	PP	GR	PG
J	GA	PG	RS	RE	PG	AS	PR	GS	GA	GE	RR	EA	ES	GR	RG
K	RR	RP	GS	PP	PP	GS	AE	GR	PG	GA	EP	RG	GP	EE	GR
L	RA	GR	PP	GR	PG	GA	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	RG	GP	EE
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

$\phi_p = 2260$ (approx.) $\phi_r = 1164$ $\phi_o = 2294$

(30-element alphabet)

4. Solve the following cryptogram, and recover all keys:

					5					10
A	AAC	AAB	BBA	AAB	AAC	AAB	ABB	ACC	AAB	CCA
B	ABA	ABC	AAC	CAA	AAB	BAA	BAA	AAA	BBB	AAB
C	ABB	ABC	CAA	BAB	AAB	AAC	BBA	ACB	CBA	AAB
D	BBA	BCC	ACB	BBB	BBC	ACA	BBA	ABA	ABC	AAC
E	ACA	BBC	AAC	AAB	AAB	BBC	AAA	BAA	BAB	AAB
F	AAB	ABB	ACC	AAA	ABB	ACC	AAB	BCC	BCC	AAB
G	BAC	CCC	ABB	AAB	CBC	ACA	ACA	AAC	ACB	CAB
H	AAA	ACA	CCB	AAB	AAC	ABA	BAA	ACB	CBC	CCB
J	AAB	AAC	ABA	CCB	AAB	AAC	ABA			

		2:	A	A	A	B	B	B	C	C	C
		3:	A	B	C	A	B	C	A	B	C
1:	A		4	18	10	5	5	3	5	4	3
	B		4	2	1	4	2	3	-	-	3
	C		2	1	-	1	-	2	1	3	1

$\phi_p = 499$ $\phi_r = 277$ $\phi_o = 542$

(27-element alphabet)

5. Solve the following naval message, and recover all keys:

1 1 1 0 1 1 0 3 3 3 1 2 2 3 1 0 3 0 2 3 3 3 1 2 2 3 1 0 0 0

0 6 0 0 2 6 0 6 1 0 1 5 2 3 1 4 0 4 2 4 2 4 0 5 2 3 3 2 0 6

0 3 0 4 2 6 1 1 2 2 3 3 2 6 3 1 2 3 3 4 1 1 0 5 2 3 3 0 1 1

0 0 0 0 1 1 2 2 0 0 2 0 0 1 0 0 2 6 0 0 0 6 1 5 1 6 2 6 1 1

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

3 0 5 1 1 2 4 2 3 0 5 2 6 0 4 2 2 2 2 1 2 1 6 0 4 1 0 1 5 1

1 0 0 2 3 1 4 1 2 2 3 0 1 0 5 0 0 1 1 3 5 0 0 2 4 1 1 1 1 1

3 3 5 0 4 1 0 1 3 1 4 2 3 0 5 0 3 0 4 2 6 0 6 2 3 1 0 3 6 0

6. Solve the following cryptogram, and recover all keys:

45264	56282	02523	29276	16145	23820
63216	52729	27212	60652	16729	47694
56529	02146	04161	25424	90692	12143
65026	45672	92325	61272	84543	04182
04221	67262	94523	41252	92945	23820
46272	34506	52921	63023	45646	74565
29082	21670	23456	12582	02947	27650
29210	23472	12543	65000		

7. Solve the following cryptogram, and recover all keys:

05105	23804	91161	38349	22702	74491
16138	33834	92274	27505	31612	74492
16127	14914	92274	38216	12724	91161
27138	10523	84274	05405	23801	61491
16105	22713	80271	05227	44910	51052
05327	14921	60491	05227	10502	74163
38016	11653	85492	27405	20531	61494
49238	42713	82492	27427	20522	71380
49127	02714	91270	49149	12702	72273
05505	30522	74272	16127	13814	93052
49449	24910	52380	05149	23834	91492
27449	23823	82384	38105	23844	91050

8. The following is a text in the Baudot teleprinter 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 (x), and 2, 3, and 5 are inactive (o), then the word REPORT is enciphered thus:

Key:	xooxo	xooxo	xooxo	xooxo	xooxo	xooxo
Plain:	−+−+−	+−−−−	−+++−	−−−++	−+−+−	−−−−+
Cipher:	++−−−	−−−+−	+++++	+−−−+	++−−−	+−−++

Solve the message and recover the switch settings:

	1	2	3	4	5	6	7	8	9	10
A	+−+−−	+−++−	+−−−+	++−++	++++−	+−−−+	−+++−	−+−−−	−−−−−	−+−+−
B	+−+−−	+−−−−	+−−−+	−−+++	++−−+	++−+−	+−+++	+++−+	+++−+	−−+++
C	++−−+	+++++	−−+−+	++−++	+−+−−	+−−−+	−++−+	+++++	+−+−−	++−−+
D	+++−−	+++−−	−−+−+	+++++	−−−−−	+−−−+	−−−++	++−−+	+++++	−−+−+
E	+−−−+	+−++−	+−−++	+−−−+	+−−++	−−+−+	−++−−	+−+−−	+−++−	+−−++
F	+−−−+	−+++−	−+−++	++−−+	−++−−	++−−−	−++−+	−+−−+	+−++−	−−−−−
G	+++−−	+−−+−	−+−+−	+++−+	+++−+	+−−−+	+−−−+	−++−+	+−+−−	−++−−
H	−++−+	+−+−−	−−+−+	+++++	+−−−+	++−++	+−++−	+++−−	+−−−+	−+++−
J	−+−−−	+−+−−	−+−+−	+−−−+	++−−+	+−−++	−−−++			

3:	+	+	+	+	−	−	−	−
4:	+	+	−	−	+	+	−	−
5:	+	−	+	−	+	−	+	−

	++	5	1	4	4	3	1	6	1
	+−	1	5	−	8	4	1	13	1
1,2:	−+	−	3	4	3	1	3	1	2
	−−	2	−	5	−	2	−	−	3

$\phi_p = 480$ (approx.) $\phi_r = 234$ $\phi_o = 386$

(32-element alphabet)

(BLANK)

(BLANK)

NATIONAL SECURITY AGENCY
Washington 25, D. C.

COURSE	Military Cryptanalytics, Part I
LESSON 4	Multiliteral substitution with variants
TEXT ASSIGNMENT	Chapter VIII

1. Solve the following cryptogram, 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

(For distribution, see page 5)

2. Solve the following cryptogram, 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					

(For distribution, see page 5)

3. Solve the following cryptogram, 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
O	47	64	36	71	06	55	00	68	78	45	52	12	69	43	

(For distribution, see page 5)

4. This message is suspected of having an ending similar to Problem 3. 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
O	27	26	62	57	06	91	23								

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 1

	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 2

	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	10	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 3

	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 4

5. Solve the following cryptogram, and recover all keys:

80713 06941 35696 80213 28061 37695
69680 91394 78800 25513 28096 91134
47713 68026 97695 13913 72502 56475
80280 88091 35802 25247 31341 39696
25525 12508 09132 47825 81314 74256
69525 51301 36477 13169 46966 90699
80247 46951 30801 80525 11378 04470
69213 11308 03477

6. Solve the following cryptogram, and recover all keys:

18905 52131 89011 04414 52131 34022
05518 92022 35156 19005 52240 55145
19020 21561 67189 08815 60110 44190
08801 11900 22055 05514 54044 15460
35832 53583 14303 41532 53474 15459
46035 83813 14280 27946 04603 14448
51628 03143 58404 33637 04044 15291
37031 43036 73730 72971 87296 73684
70757 26957 30572 71872 97075 72550
57261 76847 29729 60661 77186 51572
71871 85385 94572

7. Solve the following cryptogram, and recover all keys:

72109	19015	41776	04657	89925	96235
70368	62717	67091	83938	99294	88596
52368	62170	37091	22620	80735	96695
04627	17032	53136	77644	22537	12262
47907	38026	22703	88434	30196	04118
66826	27034	15596	84825	35230	46569
16375	84979	74893	10920	85780	73541
97477	67212	08479	35210	91365	78947
39865	97030	28334	15432	54516	59910
04639	82992	26541	09142	43430	28208
75852	33987	03712	25322	67217	58569

8. The following cryptograms are suspected to be isologs. Solve them, and recover all keys:

Message "A"

09728 23144 33987 73514 27769 10677
94418 99479 41948 66432 24374 48499
56758 47636 35546 81176 12242 30777
76194 15272 62644 85211 21361 71687
28759 72459 47047 20204 22145 53570
21377 58467 36166 13037 05358 25876
64403 33524 36847 98975 76679 83637
79946 05777 46243 95667 15086 47920
54391 27284 32060 43178 94367 66414
32190 15429 62648 60975 47915 66679
14422 70281 93894 71368 35325 27686
21707 79439 22000

Message "B"

87560 77444 35211 41109 33772 89084
55415 78586 41056 35506 15844 48995
20110 23777 58199 19437 57052 62714
37174 88756 25154 11724 98779 72367
61813 38507 47890 68719 65521 08875
68548 81270 37609 17554 83811 72477
85433 50805 37598 60718 37306 17704
06159 62714 46551 69370 50945 58696
19561 70682 86600 23474 55377 71502
16576 41295 65052 00751 47289 33956
59497 38764 66574 72261 08560 73763
68350 48516 25000

9. The following naval messages are suspected to be isologs, containing the probable word "TASK FORCE" Solve them, and recover all keys.

Message "A"

43022 83524 26060 98448 56175 57368
05544 54713 25748 18995 73211 78809
78230 46746 55566 38971 52835 54310
66179 30225 49705 63605 75310 83452
92351 03132 27998 93539 26288 11095
80473 12200 63369 42108 52097 11477
11306 68721 98883 68453 95650 15184
59749 92076 67000

Message "B"

77639 32338 96687 32583 16771 36033
25195 21007 61936 37147 94702 74323
91551 84030 23211 74696 15784 34746
34170 59391 35584 17645 65752 24915
07432 64598 99104 17307 66639 31127
90402 53353 77760 84479 75139 10388
02285 42214 80132 62568 27529 42875
07934 45455 20000

10. The following cryptogram is suspected to begin with the opening stereotype "REFERENCE YOUR MESSAGE....". Solve it, and recover all keys.

40162	42385	52104	83121	44422	37211
99099	42127	37912	77785	80116	44444
13378	77640	12255	50022	48883	78850
22287	84629	99920	06648	91253	20729
01331	81222	90051	99523	19391	41936
61045	48376	88311	15454	00022	05509
60615	57129	18859	20396	66603	14945
35079	88552	82411	08663	05032	28600
07722	55212	00080	00774	72883	40000

(BLANK)

(BLANK)

NATIONAL SECURITY AGENCY
Washington 25, D. C.

COURSE	Military Cryptanalytics, Part I
LESSON 5	Polygraphic substitution: four-square and two-square matrices
TEXT ASSIGNMENT	Pars. 64–70, inclusive; par. 73

1. Construct a digraphic distribution for the cryptogram below. Solve the cryptogram, and recover all keys.

	5					10							15
A	MH	EA	XP	SO	ZP	LM	HT	XN	PR	QU	EH	HG	RH	GR	LC
B	HU	ZW	VA	BD	MD	WO	HU	ZB	XR	DD	DU	RH	GR	CG	HO
C	SO	ZB	XN	WS	ZO	RG	BL	PC	SO	ZP	ZC	OC	BL	BT	QL
D	CP	GR	CC	LU	SD	WS	PR	PX	MD	YG	AM	DF	MH	IL	QH
E	CQ	YO	IQ	PF	GF	ND	BI	PF	CC	VA	LF	CC	CQ	YO	OZ
F	RT	OQ	VH	CG	IQ	KP	DL	IY	AO	HA	CG	HO	PF	GF	TD
G	CP	AO	HA	CV	LF	CC	CQ	YO	QU	OD	CN	OG	CN	WA	QC
H	HT	MH	KQ	ZG	LC	HU	PB	GT	ID	WQ	OF	WG	ZO	LG	KG
J	DL	ZW	VA	ZB	XR	AU	VA	DH	PF	MH	PF	ZB	OH	WL	CG
K	HO	LZ	SO	ZB	XN	WS	ZO	IU	TA	AO	GA	HA	EU	MH	YO
L	LT	EU	MH	HU	LV	WQ	MZ	YT	ZT	ZO	YG	SO	LZ	CP	EU
M	ON	MU	WG	RT	CG	HO	MH	MS	PR	OT	MF	LF	CP	KS	RO
N	WZ	MN	QU	CP	AO	HA	CV	CO	MH	DT	DU	PF	GF	NQ	YG
O	QD	IB	WS	ZO	YG	BB	YO	ZN	XR	LW	HU	IQ	WS	QD	DC
P	ZB	IB	RM	SO	EN	IA	RU	DW	GR	CG	HO	MH	MS	PR	QD
Q	DC	LZ	TN	WL	KN	PF	XD	UT	WA	ZO					

2. The following cryptogram is suspected to contain the probable word "REQUISITIONS". Solve it and recover all keys.

					5						10				15
A	DI	AF	IQ	GY	II	KG	IT	GC	QC	OV	DE	KU	DM	RI	RN
B	RO	NK	UN	KP	DH	CU	RH	PA	QQ	PL	OD	CM	YB	HE	MR
C	QQ	EG	LP	QC	IP	OP	LN	SN	DT	DP	UT	RS	EM	RN	OA
D	QL	OD	DA	QC	DZ	EM	WK	NK	DC	XP	RK	HT	HE	QR	QU
E	BP	LP	LK	NQ	LE	SR	HF	SQ	SO	QR	CM	QL	HL	AC	TX
F	GK	KF	CM	TT	OB	RP	IT	BK	MP	HL	BC	IU	MT	ZF	RW
G	ZR	CK	CM	DC	VC	OA	UA	QP	RR	IV	RQ	PK	TP	CE	QH
H	KP	UC	RO	NK	HO	QQ	PL	OD	CM	YB	HE	MR	DI	AF	IQ
J	IT	IW	SO	EM	DM	QT	RQ	BK	LG	TB	CE	AY	IU	LK	NX

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

$_2\phi_p = 125$ $_2\phi_r = 27$ $_2\phi_o = 106$

3. The following cryptogram was enciphered by means of an inverse four-square matrix, wherein the cipher sections are normal alphabets (I = J) inscribed in straight horizontals. Solve it and recover all keys.

				5					10					15
A	QU	KF	FT	TO	IP	KI	GB	AD	ES	FQ	HD	GL	AG	KI	EE
B	TO	RD	GH	SO	RH	FO	FV	KI	GO	RH	HD	GU	UU	IP	WF
C	ON	MD	RI	HB	ME	SO	BU	MO	FF	UK	GI	GL	AG	OO	MI
D	GH	PQ	GI	FG	ER	GI	IO	NL	QD	FQ	QK	HD	WG	FG	FG
E	NU	TO	MH	LP	OK	GG	QX	AH	GQ	PY	KT	PZ	KT	LP	FV
F	KY	KT	NE	RT	UQ	IT	RK	FG	DN	US	ID	LU	PD	HA	KB
G	OD	GT	FZ	IA	FQ	FF	ZD	PI	GH	RI	QC	FQ	AH	GQ	MT
H	FU	AH	GQ	PD	DP	TY	LP	EQ	AN	SD	RT	TL	LC	KI	KA
J	RI	DC	TO	LU	FA	RF	UC	TO	WF						

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

$_2\phi_p = 114$ $_2\phi_r = 25$ $_2\phi_o = 126$

4. Solve the following cryptogram and recover all keys:

	5						10						15	
A	WB	IT	HS	SE	SS	NA	EC	PA	RT	RG	DO	CP	RO	TT	GA
B	TC	EN	LZ	RT	OO	OA	DP	EH	PV	NI	FN	EO	TS	OO	WC
C	AD	WB	SP	EN	QC	OV	AS	BS	VD	DR	NS	RO	QC	CA	WO →
D	← OG	EN	ZP	QS	WO	PO	PA	RT	RG	SN	IS	CE	OT	NR	RO →
E	← QC	ZE	WO	OG	EN	ZP	QS	WB	OP	WQ	RP	IA	HA	EC	OG
F	HA	EH	ZT	SQ	PO	IT	CN	HA	RT	WP	SU	HS	CA	AB	SQ →
G	← SS	SQ	DA	SG	AZ	IA	CW	HA	IE	KN	RD	SA	LE	NH	BP
H	NA	AC	SQ	SS	SQ	DA	SS	NZ	IE	KN	OD	CW	HA	WO	PO
J	AE	KR	TS	MC	AL	HW									

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

$_2\phi_p = 109$ $_2\phi_r = 24$ $_2\phi_o = 152$

5. The following two messages were intercepted on the same radio link half an hour apart, Message "B" being in answer to a request for a service. Solve the texts, recover all keys, and determine the cause of the cryptographic error involved.

Message "A"

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

Message "B"

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

6. The following cryptogram, suspected to begin with the words "AIR RECONNAISSANCE REPORTS", was enciphered by means of a four-square matrix with four different keyword-mixed sections. Solve it and recover all keys.

	5								10						15
A	IC	RO	IK	HC	AA	OU	TC	IH	BO	NR	RD	TT	CD	FI	LP
B	MS	TD	XA	LB	EA	OY	TI	PC	PF	HC	QC	RD	TM	XB	US
C	CD	MO	EB	IV	HE	GG	LB	XA	ND	US	KC	SF	EA	OY	KC
D	PL	HC	US	LO	BT	NK	NL	IG	PF	HC	ND	GC	IX	YF	RR
E	HE	GG	OW	IR	QI	IL	IR	NB	TT	HG	TM	OU	SC	BT	RD
F	US	HS	LB	SO	AR	UF	CS	CA	EH	CF	TS	OE	AQ	HC	TM
G	AR	NR	OS	RU	OE	AQ	LA	DB	XA	IA	CT	NK	OG	SF	UI
H	OE	CB	TY	US	HS	AS	TD	HC	AS	CF	TS	OE	AQ	BD	IK
J	CS	QI	BR	NK	LB	SO	AR	PN	QE	ME	NR	RD	UF	AR	NB
K	UT	RS	GC	SC	GC	NL	SO	BD	SF	OR	US	HS	KG	IH	AS
L	SF	CK	HD	BD	TY										

(See distribution on following page)

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

$_2\phi_p = 165$ $_2\phi_r = 36$ $_2\phi_o = 228$

(BLANK)

~~CONFIDENTIAL~~
~~Modified Handling Authorized~~

NATIONAL SECURITY AGENCY
Washington 25, D. C.

COURSE	Military Cryptanalytics, Part I
LESSON 6	Polygraphic substitution: Playfair cipher systems
TEXT ASSIGNMENT	Pars. 71 and 73.

1. Solve the following cryptogram and recover all keys:

	5					10							15
A	UA	SK	UA	SP	KM	MR	IO	OR	IX	YR	OR	OS	MS SD UA →
B	← RH LV	BR	SA	AK	SW	AX	SA	BG	CW	PN	CW	XS AU	BS →
C	← NA	NM	SM	VU	YN	AR	OR	HG	RA	RL	SA	YN	UK SA OR
D	MY	IA	AU	BF	MS	SD	UN	WC	AS	EN	CA	HN	DR FB NL
E	AS	BU	RF	VU	RO	MW	BE	RP	NY	IA	CU	GR	WO SR XS →
F	← AU	BU	LB	UG	DM	KS	MR	GN	HQ	DM	DU	HU	SB WC AS
G	UB	EO	AS	AD	WB	NO	DK	AD	FB	RH	SP	RW	HO UC AD
H	FT	NO	SB	AU	RD	OT	MS	SD	UN	XB	VL	UA	KS HQ KS →
J	← MR	UA	RH	LV	CU	CW	FB	NL	QO	AR	OR	HG	RA LV AL
K	UB	UA	CE	RB	AD	EQ	YX	OE	XH	UM	SW	PR	FS ON UK
L	GN	DR	UP	UR	XW	RW	QH	FR	SD	AS	NO	AD	UA WB NO
M	WS	IG	FS	LR	UB	CA	UO	RP	AS	SB	NW	BH	NP BS NA
N	UA	OE	RB	RB	RZ	RO	KR	OR	VR	NU	US	DR	SR SP RW
O	FR	DA											

(For distribution, see page 2)

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

$_2\phi_p = 266$ $_2\phi_r = 58$ $_2\phi_o = 316$

2. The following cryptogram is suspected to contain the word "DIVISION". Solve it and recover all keys.

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

3. Solve the following cryptogram and recover all keys. It is suspected that this message is signed "WINTHROP COL INF".

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

4. The following cryptogram is suspected to contain the signature "CLINTON COURTNEY COL INF." Solve it and recover all keys.

L H Q E F I P X O E O P Y Q E N C O P C M A G Z H E F Q E L

M C O B Y F M E B O D K D Y S Y F Q E L E F D F H E F Q E T

O L I E G G Y H L O S L M L Q L B P J Z S P T F A O F Q R L

D Q E L N H Q E F F M I B T Z O F G W J F O S L M D P Y F Q

E L B L Y B Y F Q E L Y F Q E L L M S X L E B I F E F D M Q

E C F Z N L Q E M F X S L M T O L I D Y O A D S F E O S Q E

M L E F Q R Q I L U B P S T L M F H L M F I K Q E F F Y F Q

E L T O L L G D Y D T L Q L B P K F A O F Q R O T P C Q E M

O S Q E M L M B L Y B G C G Z F Q R W O O L S A P S K L L M

E S Z Q R L K M O E S P S R N

5. The following cryptogram is suspected to contain the probable beginning "PART ONE OF THREE PARTS." Solve it and recover all keys.

N B B V C Q K V H I E B M M N B B V I I B D L B K L S F X V

R K C B V M K R Y F Q T B V R H V I Y P Y B V H B O D B F T

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

I B L H Z V G Y U U Y C A V E G H I R W U V H P K R B D D I

S Y E A I Z N T I Q N Y M W P Y F Y I K K T S Y U E Q V X P

U V P T F M R W I P Y C V D D R F Y G B S M Y C A V E G H I

K G N Y N L T B I V K R H F G L F L F G A B Y D P T I Q N Y

Y F Q T B V I K N Y C M V H P B P T L P I Z Y U K I E G U U

T Q F Y B C Y D P B N R V Y V A Y G O Z

NATIONAL SECURITY AGENCY
Washington 25, D. C.

COURSE	Military Cryptanalytics, Part I
LESSON 7	Polygraphic substitution: large tables
TEXT ASSIGNMENT	Pars. 72 and 73

1. The following cryptogram is suspected to contain the probable word "RECONNAISSANCE" Solve it and recover all keys.

					5					10					15
A	SA	CJ	JY	RO	HT	KP	LP	DO	CV	PS	LN	PE	GN	RP	SP
B	FP	LU	QT	LW	PR	CJ	KL	RN	QE	RO	CV	MF	SE	LZ	QZ
C	RR	AO	TH	SQ	PG	TL	GL	NR	QS	UZ	KK	KK	JE	MV	NL
D	LU	AR	QE	SA	MW	KK	LP	SL	AP	PZ	QV	KK	PB	CJ	JY
E	RL	CJ	HA	CO	AR	BH	LL	JH	QT	RP	AS	SL	RP	SL	NL
F	QJ	QT	AJ	NL	IG	NR	WX	AI	HI	YD	KK	JE	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	QT	LW	PR	CJ	JY	AK	HT	JY	AA	NN	SX	CB	RO	WE
K	SA	RD	LL	ML	AX	AF	YU	NC	PK	MS	NE	QJ	QT	AJ	

(For distribution, see next page)

(Frequency distribution for Problem 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	
A	1	-	-	-	-	1	-	-	1	2	2	-	1	-	1	1	-	2	2	-	-	-	-	2	-	-	16
B	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1
C	-	1	-	-	1	-	-	-	-	5	-	-	-	-	1	1	-	-	-	-	-	2	-	-	-	-	11
D	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2	-	-	-	-	-	-	-	-	-	-	1	3
E	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
F	-	1	-	-	-	-	-	-	-	1	-	-	-	-	-	2	-	-	-	-	-	-	-	-	-	-	4
G	-	-	-	-	-	-	-	-	-	-	-	1	-	1	-	-	-	-	-	-	-	-	-	-	-	1	3
H	1	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	3	-	-	-	-	-	-	5
I	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1
J	-	-	-	-	2	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	4	-	7
K	-	-	-	-	-	-	-	-	-	-	5	1	-	-	1	1	-	1	-	-	-	-	-	-	-	-	9
L	-	-	-	-	-	-	-	-	-	-	-	2	-	1	-	4	-	-	-	-	2	-	2	-	-	1	12
M	-	-	-	-	-	1	-	-	-	-	-	1	-	-	-	-	-	-	1	-	-	1	1	-	-	-	5
N	-	-	1	-	1	-	-	-	-	-	-	3	-	1	-	-	-	2	-	-	-	-	-	-	-	1	9
O	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1
P	-	3	-	-	1	-	1	-	-	-	2	-	-	-	-	-	-	3	1	-	-	-	-	-	-	1	12
Q	-	-	-	-	2	-	-	-	-	2	-	-	-	-	-	1	-	-	1	6	-	1	-	-	-	1	14
R	-	-	-	1	-	1	-	-	-	-	-	1	-	1	3	3	-	1	-	-	-	-	-	-	-	-	11
S	3	-	-	-	1	-	-	-	1	-	-	3	-	-	1	2	1	-	-	-	-	-	-	3	-	-	15
T	-	-	-	-	-	-	-	1	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2
U	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	1
V	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
W	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2	-	-	3
X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Y	-	-	-	1	-	-	-	-	-	-	-	-	-	-	1	1	-	-	-	-	1	-	-	-	-	-	4
Z	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	5	5	1	2	10	3	2	3	3	10	9	13	1	4	10	16	1	9	5	9	3	4	3	7	4	7	

Digraphic phi data

$_2\phi_p = 152$ $_2\phi_r = 33$ $_2\phi_o = 184$

Monographic phi data

$\phi_p = 1471$ $\phi_r = 849$

Initial ltrs: $\phi_o = 1386$ Final ltrs: $\phi_o = 1096$

2. The following cryptogram is suspected to begin with the opening words "WEATHER FORECAST FOR WEDNESDAY ONE THREE SEPTEMBER". Solve it and recover all keys.

					5						10				15
A	OL	TS	HM	XD	AW	AU	ST	ZF	AW	OL	QJ	WD	EM	KB	SA
B	OD	WE	WD	TG	YG	KC	VE	JY	DY	QG	HX	FE	KK	FP	OR
C	IF	OD	RD	MU	OB	MH	HG	SK	VQ	VQ	OD	QL	AW	WR	US
D	KK	DO	CA	US	VQ	OD	DO	YD	VE	MY	MH	JY	DY	MY	HX
E	HM	ST	YG	EI	VU	VQ	VC	TS	KX	XD	MX	DO	CK	SK	LX
F	US	MH	BZ	LU	CF	XW	BQ	VJ	OU	JD	IW	QF	UO	US	NO
G	LH	EC	WD	XJ	JM	VQ	AI	YD	VE	MY	MH	VR	VE	AP	VQ
H	ZE	HT	KW	CK	XW	BQ	HZ	BR	HP	CJ	FS	TW	OG	ZX	IZ
J	AM	AG	JD	YG	FE	MH	ER	VE	OU	TW	WD	JY	DY	RK	RG
K	WF	TG	AW	QW	DO	OD	VE	JY	TS	WP	OZ	NT	IW	HX	YJ
L	BZ	KW	CK	DQ	AM										

3. The following two messages, intercepted on links known to be passing traffic enciphered by means of random digraphic tables, are believed to be isologs containing the probable signature "MAJ GEN CARTER WORTHINGTON" Solve the texts and reconstruct the fragmentary table.

Message "A"

	5						10						15	
A	CX	JI	GO	NB	XJ	LV	OP	LD	XG	OI	UT	LI	ZV	DM	DE
B	AY	AM	CX	BD	DZ	JX	VK	DQ	IY	IG	JO	KW	DE	IG	JX
C	BR	OU	LN	SR	SC	DE	UW	QK	VN	LN	ZH	YM	IQ	DW	KS
D	ER	AV	ZH	LD	RD	DE	IQ	OF	QQ	HT	OF	VB	DE	PC	JI
E	GS	XJ	NZ	NN	IG	OF	NB	SR	ZH	JU	TI	AA	GP	DZ	GP
F	XF	DE	KW	FH	WX	ML	PY	RN	AY	AM	ER	AJ	UI	SX	OW
G	UW	QK	VN	LN	ZH	YM	AV	HW	OW	SC	JX	OF	QQ	MO	SR
H	AY	NR	DZ	CO	IS	SR	ZH	HT	VF	IQ	VN	FH	TQ	UT	HT
J	EX	EV	XG	IY	IG	OF	YR	JL	OF	OF	IA	IG	BT	MO	SR
K	AY	NR	HF	WX	GD	PX	OL	CO	EN	SG	SL	MG	CX	ID	VM
L	OP	IH	LN	ZH	TM	SL	SC	OF	GL	IG					

Message "B"

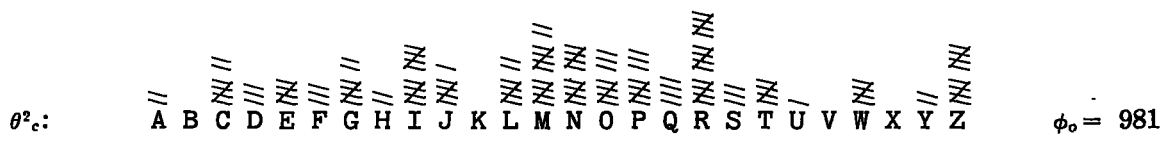
	5						10						15	
A	CX	JI	GO	NB	XJ	LV	OP	LD	XG	OI	UI	SC	XJ	NZ	NN
B	IG	ER	AJ	OF	ZH	WC	PM	SR	AY	NR	KQ	RI	BR	LD	YM
C	JO	ED	XG	TI	CO	VU	QF	UO	KM	LI	JX	EN	MX	QF	NE
D	SC	SR	WX	LH	HK	EN	FW	DT	SL	DR	LV	CO	WG	ZT	IG
E	NU	DM	DE	AY	PS	XQ	XQ	TI	LH	YO	CX	VF	OF	JL	OF
F	CO	HI	IQ	PC	DZ	CH	NN	IY	IG	WG	CX	BD	KC	UT	FJ
G	QF	UO	KM	LI	JX	VU	IN	XS	LI	UW	RI	DT	SL	VF	IY
H	IG	IG	SC	DE	VF	TI	JX	FL	LN	KJ	RT	ER	SX	OW	JI
J	AJ	JX	SR	AY	PS	NR	QV	GP	PS	LV	JI	DT	EE	VF	IY
K	IG	SL	DJ	PS	KS	JO	SC	DE	IQ	CH	LI	ER	AJ	VF	TF
L	WX	ZZ	LI	JX	FG	LI	CO	LV	CX	CC					

4. Solve the following cryptogram and recover all keys:

	1	2	3	4	5	6	7	8	9	10
A	003	315	097	114	347	261	067	217	314	241
B	195	062	350	115	006	451	062	141	072	472
C	189	192	018	400	189	067	315	097	530	403
D	115	393	262	609	192	356	115	186	122	467
E	212	071	074	237	235	114	416	115	393	271
F	055	293	186	552	009	062	471	141	150	193
G	186	516	184	266	274	470	002	238	053	186
H	141	072	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		

5. The cryptogram below is suspected to begin with the stereotype "REFERRING TO YOUR MESSAGE" OR "REFERENCE YOUR MESSAGE". Solve the text and recover all keys.

	1	2	3	4	5	6	7	8	9	10
A	MRA	DMT	GCI	YIY	MFG	NNL	SRK	QFB	DMD	WII
B	DSZ	GNM	IJA	GOO	LGI	DEV	LTD	GCI	IYD	LCI
C	MMT	JIU	PNM	VZP	LGI	DMY	ITI	POV	GIP	TGO
D	PLM	MCH	JPB	MRC	DGK	FWJ	IHC	EEF	MDO	DSZ
E	TEN	DGK	FWI	NNM	LEV	EZF	TAS	DIP	HMT	TDL
F	GTR	QMD	MZU	ROD	NPC	JNJ	GCI	IQM	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	VZP	IQM	EMF	JPC	SMK	JLM	MND
K	PQW	YZB	OZN	IJY	IPJ	DMD	YJP	NIP	EMF	JPC
L	SMK	JLF	ENG	NPW	FNV	FJJ	IWI	GTT	MOT	EOW
M	CRV	WLF	ELE	TSZ	TNM	VRS	MTR	TEQ	VRV	QJQ
N	MRV	NOV	GIP	RMT	KQX	GCJ	ELC	MZH	PRT	LNM
O	LCR	IYR	CZY	GPW	XPA					



$\phi_p = 1207$ $\phi_r = 696$

6. The following cryptogram is suspected to contain the probable word "AIRCRAFT". The encipherment is believed to involve a tetranome trigraphic system employing a matrix similar to that illustrated in Fig. 59 of the text, the ciphertext sections being composed of the dinomes 00–99 inscribed in the normal manner of writing, but the plaintext sections consisting of keyword-mixed sequences which differ from those in the text example. Solve the cryptogram and recover all keys.

	1	2	3	4	5	6	7	8	9	10
A	0601	7849	4912	2533	1747	6031	4270	8240	1877	6111
B	0240	1245	4827	1236	5681	6831	4214	9945	1875	8917
C	3309	4143	8843	5342	7719	1517	2774	3249	4507	4872
D	6011	1266	4145	7327	6760	5345	7619	5945	7349	3043
E	7709	2819	4322	0129	3875	2713	3046	9040	0775	6561
F	2911	2507	3576	1505	4214	9875	3570	0208	6583	6161
G	3247	2107	1777	3918	2533	1747	0264	1956	1242	4707
H	7772	3296	3491	0576	0779	5514	1145	3143	8569	2871

(BLANK)

NATIONAL SECURITY AGENCY
Washington 25, D. C.

COURSE	Military Cryptanalytics, Part I
LESSON 8	Monoalphabetic substitution with irregular-length cipher units: monome-dinome systems and others
TEXT ASSIGNMENT	Chapter X

1. Solve the following monome-dinome cryptogram and recover the original matrix:

78131 76784 31174 50078 76343 47807
41346 53334 01331 01799 78318 76441
31917 92478 74179 10834 76033 55723
40178 31347 46554 65323 41305 86131
34767 30345 77787 48763 77689 76072
76747 88123 11278 31788 76503 47753
17807 67921 07276 07310 17997 88878
74703 05323 15777 71034 76371 33764
47117 37607 88390 00666 33300 03985
79531 31533 78342 47800 17230 75560
34850 74547 83189

2. The following monome-dinome cryptogram is believed to contain the probable word "DIVISION". Solve the text and recover the original matrix:

17832 00066 16927 80635 28420 04596

95220 01900 21500 40563 26746 12576

80705 88123 53921 31118 13281 29159

46465 61576 52844 90033 94526 59400

25284 30032 00457 80758 80707 00526

73941 20854 56640 59352 91625 97612

46977 89125 05945 22008 41401 51129

31702 91067 53763 59062 38071 67003

84670 04267 78579 20084 17919 60266

43595 65697 00036 12004 97616 87202

60045 70787 05971 26122 81200 19003

00841 76912 09599 72673

3. The following cryptogram was intercepted on a link which has been known to be passing traffic in two different monome-dinome systems, one involving a matrix of the type shown in Fig. 75 of the text, the other involving a matrix of the type in Fig. 77. Solve the text of the message and recover the original matrix.

47631 82870 14628 31274 12741 16263

16054 63152 84662 60736 97728 46198

46972 13808 46287 46364 83788 72846

60846 28738 27578 87073 18279 62736

97462 83107 36977 45636 26962 73168

62763 12138 08462 87316 06379 82647

28467

4. The following messages, intercepted on a link known to be passing monome-dinome traffic, are believed to be isologs. Solve the texts and recover the original matrices.

Message "A"

94872	33935	61227	89316	23405	09079
43810	57678	93386	41999	83809	08334
94194	76279	99496	30576	79199	54343
57683	04186	07981	43349	83529	09638

Message "B"

94378	11935	62887	39326	81405	09079
41320	57673	93136	41999	81309	03114
94194	76879	99496	10576	79199	54343
57631	04136	07982	43149	31589	09613

5. The following messages are believed to be isologous monome-dinome ciphers. Solve the texts and recover the original matrices:

Message "A"

73507 09885 01652 37531 09804 39858
14983 12316 52371 12890 93312 42689
30741 59012 54398 50563 98460 77297
30415 65075 43098 13500 74379 06814
51983 12316 52371 13559 33124 39842
16361 80772 97056 29092 58145 15465
07901 10121 98617 56398 94163 84731
35039 04398

Message "B"

36713 45807 18921 63867 55406 58179
56296 89216 37798 07485 62909 18085
43072 74292 56571 84650 14339 73640
72171 32564 58871 43063 74180 79875
62968 92163 77676 85629 06509 89612
34339 73484 97424 81798 72517 13747
74292 78017 08465 26896 80036 88716
74065

6. Solve the following monome-dinome-trinome cryptogram and recover the original matrix:

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

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

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

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

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

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

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

7. Solve the following uniliteral-biliteral cryptogram, and recover all keys:

P V O Y A C K R T E A U O O D K N W O I B K E I A U B T A P

W O I D G O B K N T A E N X B T A E B G Y A E U I E N L C T

E O B Z F H O O B L Y I E B G U U O N T B X P X R M I B K A

C W O I E P K C G P V A Y E F T E I N M P K S G E Y A O D K

U E D L R Z E Y A N G C W U Y A U P K P M E O I A C V P W Y

R W O Y C W A P W O I Y A O R W S V C H E I R V C K Y Y P K

O I C K Y N W O D H R K D G E A E B X U E R X D M E Y A B T

E U C W N G R T D W P H O A O P G U N G R K C V Y O N Z B G

U E N T X

8. The following cryptogram, enciphered in a Playfair-type digraphic-monographic system, is suspected to begin with the probable stereotype "MORNING REPORT FOR MONDAY NOVEMBER TWENTY FIRST". Solve the text and recover all keys.

A Q T I N J F Q H Q P T L G P T A Q S K I V A T X C J E H Q

P Z K M R Z G H Y N P N P P Q Q T D M K M L R G P T B W R Z

P Z P R G L V T P G G A H H Q M P G A Y Q M H M F K R R K Q

H Q M K M R J N P H E J C M D K Z Y S R K Q B C A K Q R Y Q

M C Q G G A H H Q N P R Y Q M Q X G L V Q H J T N M Q K P D

A H C T M K Q V G G A H H Q T A K Q V P K M R J N P H E J C

M D K Z Y S R K L V L O C M X C X K T P

9. The following cryptogram was enciphered in a dinome-trinome digraphic system employing matrices similar to those in Figs. 90*a* and *b*, except that the internal numerical sequences have been changed. The message is suspected to end with the signature "VINCENT ANDERSEN COL INF". Solve the text and reconstruct the matrices involved.

71665 73330 13492 25221 39225 86765

01802 60940 44263 12514 47303 60733

96104 70273 72027 53072 85735 39518

42301 07824 22132 71923 51903 51663

92569 09402 78709 40353 01078 21946

95755 85962 42213 27197 65187 26752

74097 55734 86919 61182 81051 02719

85196 57392 20085 32536 75171 92577

63494 35234 45067 19349 22522 04714

41045 22216 57508 77537 16223 93144

24586 34944 82506

10. The following cryptogram, based on a Morse code system, is suspected to begin with a spelled-out number. Solve it and recover all keys:

71430 62809 18592 35607 61572 04953

79012 87548 65983 04037 95327 30751

34904 56564 20813 01258 16408 97156

64597 60410 83159 34702 68032 95357

25173 02589 41582 60360 91754

(BLANK)

~~CONFIDENTIAL~~
~~Modified Handling Authorized~~

NATIONAL SECURITY AGENCY
Washington 25, D. C.

COURSE	Military Cryptanalytics, Part I
LESSON 9	Syllabary squares and code charts
TEXT ASSIGNMENT	Par. 80

1. The following cryptogram is suspected to begin with the words "REFERENCE YOUR MESSAGE NUMBER THREE FIVE FOUR DATED ONE SEVEN SEPTEMBER". Solve the text, and reconstruct the cryptosystem employed.

C R D S C R J S I S K S J T Y C L S K R C Q E R B Y J Q I R

K P K O J R C R S D T F S D J T Y C D P F R D X B R C S F S

J S C S J U F R J Q I R K P K U P D D O F O X B P L C R R B

D U K P I S L S J S K O K R G O J N L P K P C O F S P F J P

C R R B F T J N L R A Y J S H T F O X B Q C K R H T E S D Y

L R H Q K U P C F O J N L R C N L U F T J S E O J S F X C U

Y F E S K P J S H X B R P F B X X B F Y S C D P K S K U C R

J W O C S L R B K O K R F X J U L P B R Q C K S K V B Q C P

J P C P J U J R C S O E J R F P J S H U B O B R K W P C R I

H V O B J P K R F Y D O R D D U K P D T B P L P H T F O X B

2. The enemy is using a system incorporating a 10 x 10 bipartite square within which there are inscribed 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 key word "PYRAMIDS" as follows:

	Ø	1	2	3	4	5	6	7	8	9
Ø	P	Y	R	RA	RE	RED	RES	RI	RO	A
1	1	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	0	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 internal key word:

20 88 50 58 95 63 62 30 69 69 94 15 58 92 07

84 73 60 35 77 95 61 38 78 30 50 66 94 15 44

84 62 12 12 20 38 31 42 67 67 93 52 01 83 10

32 02 79 10 36 84 72 94 44 68 79 54 78 69 50

58 95 58 79 62 14 30 50 71 94 35 87 79 97 58

02 02 10 78 47 22 97 58 88 09 84 53 03 01 93

44 78 79 79 78 30 50 79 57 55 59 54 08 54 94

72 89 72 60 82 72 94 44 92 07 79 82 05 10 79

94 10 10 02 58 28 97 58 02 02 43 69 05 96 50

93 50 58 95 63 58 07 11 21 50 71 94 35 84 27

30 54 87 50 35 68

3. The following two messages were encrypted by means of the Aggressor code chart illustrated in Fig. 100 of the text, but with a different set of coordinates. It is suspected that both messages end with the signature "ENRIQUE VALENZUELA". Reconstruct the plain texts and recover the coordinates of the chart.

Message "A"

AT FH XL MK ZU AL CO TG QT KQ RD KN KL EL DR

JP XT RO GY RJ UA SG BW AT HX OD DV IX SR BD

LI CE XL JA VL TA ET UY NV QL KH WD AL YG PT

DI LG YR LU EF NY ZR QQ LX SY UV

Message "B"

AL LQ QT MB VU EL UA TX XL PQ RJ WG IM GG XC

AT DR NP QT JB WD KZ EQ LA UG WJ AL YX PL OZ

SR LZ AG YG XH FG YY UP

4. The following message was encrypted by means of the Aggressor code chart illustrated in Fig. 100 of the text, but with a set of *non-variant* coordinates. Reconstruct the plain text and recover the sequences for the row and column coordinates.

EO BO JO BO EO IO AY IT JO DO EO AZ JO IQ AU

KU EO FQ AQ JO JZ JQ JY EO JS JO JT JS EO AX

AN AQ LX JO BO FU DU IP EO HQ BQ GQ JP AS IR

CZ AT JO BW EO JS JO HZ JP IZ HX KV EO FV JO

LR EO FV DT DS LS ET LT JS KS BW JX ET MW JX

5. The following 30 messages, intercepted on low-level ground nets, have been selected for study because of homogeneous characteristics. Solve the texts and reconstruct the cryptosystem employed. (A condensed table of the repetitions contained in these messages is included on pages 10–12.)

No. 1 INL DE ETN 1630 08 Aug 53

77 05 19 39 45 39 89 19 59 25 49 32 35 22 35
90 00 45 95 60 81 55 05 90 32 62 00 92 08 78
95 50 36 05 79 60 92 58 90 95 42 93 05 27 88
65 00 21

No. 2 INL DE ETN 1633 08 Aug 53

77 05 19 19 45 39 89 69 09 25 49 32 35 22 35
97 45 95 60 37 62 05 10 50 11 00 61 78 95 07
05 88 31 95 13 05 29 19 89 45 95 20 49 43

No. 3 INL DE ETN 1636 08 Aug 53

77 05 19 69 45 39 89 69 09 25 49 32 35 22 35
97 45 73 32 15 55 95 74 05 82 92 46 21 95 50
70 65 05 45 95 28 05 62 41 07 11 10 45 88 61
95 49 05 90

No. 4 SIA DE BYE 0805 10 Aug 53

77 05 09 89 45 09 49 09 09 25 39 09 32 35 22
35 97 45 95 99 00 88 05 60 68 90 95 34 05 78
32 35 04 23 92 85 61 95 46 05 90

No. 5 LQS DE QEI 1836 11 Aug 53

77 05 79 29 45 39 49 69 09 25 39 39 32 35 22
35 90 00 45 95 87 05 56 73 32 15 55 95 37 05
82 92 46 78 95 91 05 27 06 28 66 00 91 80 53
24

No. 6 ALU DE YUT 1644 12 Aug 53

77 05 69 19 45 39 89 79 09 25 39 19 32 35 22
35 97 45 95 22 05 80 46 96 24 95 76 05 27 95
08 67 39 82 05 45 95 50 75 05 71 26 00 18 34
22 61

No. 7 QEI DE INL 1256 20 Aug 53

77 05 19 19 45 39 19 59 09 25 19 09 32 35 22
35 97 45 95 20 68 05 46 22 31 72 56 72 57 80
50 90 51 54 37 95 46 05 27 95 60 97 05 90 88
31 55 50 35

No. 8 USO DE SIA 0917 21 Aug 53

77 05 39 39 45 09 99 39 59 25 19 39 32 35 22
35 97 45 95 25 05 60 23 52 95 68 05 21 95 10
05 92 52 90 78 38 48 35 10 00 95 97 05 90

No. 9 OAY DE NBQ 2357 27 Sep 53

77 05 99 69 45 19 69 59 09 25 19 29 96 80 93
60 17 40 45 95 98 05 57 80 40 74 63 00 95 76
05 27 95 08 15 05 46 80 10 55 95 39 82

No. 10 NBQ DE OAY 0010 28 Sep 53

77 05 09 39 45 09 09 09 59 25 19 49 96 80 93
60 17 40 45 95 50 15 52 05 10 50 11 98 59 09
09 95 01 78 19 05 27 95 21 69 05 49 49 89 64
94 14 30 76

No. 11 OAY DE ALU 1008 29 Sep 53

77 05 39 79 45 39 09 09 09 25 19 99 96 80 00
52 60 17 40 45 95 99 05 62 34 55 50 35 95 23
05 20 35 31 06 60 38 06 95 41 05 92 74 01 79
04 95 83

No. 12 USO DE TOB 2219 29 Sep 53

77 05 69 99 45 19 19 39 59 25 19 99 96 80 00
52 60 12 76 45 95 60 63 31 05 56 21 95 50 24
65 05 45 95 04 05 56 01 95 80 38 93 05 27 22
46 63 95 27

No. 13 ETN DE SIA 2347 30 Sep 53

77 05 19 39 45 19 69 79 09 25 69 09 96 80 93
60 12 76 45 95 71 08 14 05 50 35 00 27 95 85
05 37 17 95 86 66 11 05 45 95 88 05 87 24 90
17 56 96 24

No. 14 TOB DE BYE 2142 30 Sep 53

77 05 49 99 45 19 39 69 59 25 69 09 90 52 80
93 60 17 40 45 95 53 05 01 95 11 60 57 05 36
21 22 95 45 05 25 37 04 63 17 95 86 05 01 62
43 90 90 95 45

No. 15 BYE DE YUT 1818 10 Oct 53

77 05 89 09 45 39 49 39 09 25 39 09 50 62 01
17 40 45 95 61 05 79 19 59 95 12 05 72 45 95
10 05 92 74 95 29 05 45 95 82 05 78 97 40 35
62 00 54 90

~~CONFIDENTIAL~~

No. 16 SIA DE USO 1629 17 Oct 53

77 05 79 59 45 39 89 19 59 25 39 29 50 62 01
12 76 45 95 44 60 66 05 13 90 95 32 05 56 36
22 22 93 75 13 05 79 59 49 64 94 95 21 69 05
59 99 19

No. 17 ALU DE LQS 2001 19 Oct 53

77 05 69 29 45 39 99 59 59 25 39 99 50 62 00
50 17 40 45 95 02 05 33 95 41 05 67 80 50 00
90 10 50 11 98 78 95 50 09 05 45 88 61 95 35
05 14 72 10 55

No. 18 LQS DE YUT 0905 12 Nov 53

77 05 39 89 45 09 99 09 09 25 39 19 26 08 60
17 40 45 95 18 26 05 90 95 71 05 56 01 90 92
75 66 40 88 40 90 16 95 69 05 27 19 03 32 62
30 95 80

No. 19 SIA DE ETN 1314 14 Nov 53

77 05 39 89 45 39 69 39 09 25 39 79 70 50 08
60 12 76 45 95 26 35 05 52 75 42 32 35 90 98
45 95 33 48 05 61 45 95 88 05 60 68 90 92 60
80 76 16 92 08

No. 20 INL DE SIA 1116 25 Nov 53

77 05 19 79 45 39 39 39 09 25 19 59 26 15 52
60 17 40 45 73 32 15 55 95 30 31 03 06 72 10
05 92 74 45 95 16 05 72 57 40 35 80 98 95 06
84 97 05 90

No. 21 YUT DE BYE 1348 04 Dec 53

77 05 59 89 45 39 69 79 59 25 79 67 13 60 17
40 45 95 31 47 05 45 95 32 05 56 01 91 30 52
95 61 05 49 69 09 45 95 16 06 05 19 83 95 33
05 47 01 44

No. 22 OAY DE INL 1956 06 Dec 53

77 05 79 09 45 39 99 59 09 25 89 72 52 13 60
12 76 45 95 60 81 40 12 05 72 96 08 40 36 95
58 05 90 78 95 90 05 90 28 92 72 45 95 28 05
26 40 60 36

No. 23 QEI DE YUT 1710 07 Dec 53

77 05 69 19 45 39 29 09 59 25 29 67 62 52 60
17 40 45 95 51 32 05 37 95 59 05 01 95 46 05
63 95 08 57 05 45 95 60 28 05 71 26 00 18 34
22 61

No. 24 EIB DE BQT 1207 05 Jan 54

77 05 69 09 45 39 19 09 09 25 59 02 34 35 31
55 45 95 72 60 05 03 50 50 80 95 17 05 54 97
92 10 10 95 89 05 56 78 95 19 05 76 70 96 62
01 40

No. 25 NLE DE IAQ 1519 11 Jan 54

77 05 79 29 45 39 59 39 09 25 39 39 02 32 70
35 31 55 45 95 92 41 54 00 89 05 50 80 63 35
24 92 10 95 96 05 26 21 95 66 05 86 60 92 98
35 96

No. 26 QSN DE TNY 1034 12 Jan 54

77 05 19 69 45 39 09 69 09 25 39 19 02 34 35
32 40 55 45 95 50 81 56 12 05 72 49 95 58 05
90 95 90 05 16 09 89 09 09 88 31 81 00 54 36
80 31 30

No. 27 YEO DE UTA 0932 23 Feb 54

77 05 39 89 45 09 99 19 59 25 19 69 82 52 12
40 35 31 55 45 95 60 37 73 05 72 95 39 05 66
35 24 76 14 00 00 76 55 82 92 46 95 64 50 57
05 90

No. 28 SOL DE AYS 1440 13 Mar 54

77 05 19 39 45 39 79 69 59 25 39 69 60 31 18
45 95 92 57 05 90 80 53 90 93 44 95 39 30 05
12 50 60 12 56 52 31 10 55 95 92 05 60 23 70
56

No. 29 LUI DE OBU 1846 30 Mar 54

77 05 69 09 45 39 49 79 09 25 69 09 60 31 62
42 45 95 08 83 00 71 94 05 01 95 53 27 05 62
43 90 90 56 37 77 32 12 10 92 94 95 38 05 73
32 72

No. 30 BQT DE UTA 0503 31 Mar 54

77 05 09 39 45 09 59 09 09 25 69 39 84 40 62
42 45 95 79 05 01 95 22

CONDENSED TABLE OF REPETITIONS
FOR PROBLEM 5

The first column designates the particular dinome; the second column shows the frequency of the particular dinome; and the third column indicates the messages (with occurrences of more than one shown in parentheses) in which the particular dinome is found.

00	22	1(3), 2, 4, 5(2), 6, 8, 9, 11, 12, 13, 15, 17(2), 23, 25, 26, 27(2), 29
01	14	10, 11, 12, 14(2), 15, 16, 18, 21(2), 23, 24, 29, 30
02	4	17, 24, 25, 26
03	3	18, 20, 24
04	4	4, 11, 12, 14
05	134	1(4), 2(4), 3(5), 4(4), 5(4), 6(5), 7(4), 8(5), 9(4), 10(4), 11(4), 12(5), 13(5), 14(5), 15(6), 16(5), 17(5), 18(4), 19(4), 20(4), 21(6), 22(5), 23(6), 24(5), 25(4), 26(4), 27(4), 28(4), 29(4), 30(2)
06	6	5, 11(2), 20(2), 21
07	2	2, 3
08	10	1, 6, 9, 13, 18, 19(2), 22, 23, 29
09	55	2, 3, 4(5), 5, 6, 7(2), 8, 9, 10(6), 11(3), 13(2), 14, 15(3), 17, 18(3), 19, 20, 21, 22(2), 23, 24(3), 25, 26(5), 27, 29(3), 30(4)
10	15	2, 3, 8(2), 9, 10, 15, 17(2), 20, 24(2), 25, 28, 29
11	6	2, 3, 10, 13, 14, 17
12	12	12, 13, 15, 16, 19, 22(2), 26, 27, 28(2), 29
13	5	2, 16(2), 21, 22
14	4	10, 13, 17, 27
15	6	3, 5, 9, 10, 20(2)
16	5	18, 19, 20, 21, 26
17	14	9, 10, 11, 13(2), 14(2), 15, 17, 18, 20, 21, 23, 24
18	4	6, 18, 23, 28
19	40	1(2), 2(3), 3, 6(2), 7(4), 8, 9(2), 10(2), 11, 12(3), 13(2), 14, 15, 16(2), 18(2), 20(2), 21, 23, 24(2), 26(2), 27(2), 28
20	3	2, 7, 11
21	9	1, 3, 8, 10, 12, 14, 16(2), 25
22	16	1, 2, 3, 4, 5, 6(3), 7(2), 8, 12, 14, 16, 23, 30
23	4	4, 8, 11, 28
24	7	5, 6, 12, 13(2), 25, 27
25	32	1, 2, 3, 4, 5, 6, 7, 8(2), 9, 10, 11, 12, 13, 14(2), 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30
26	8	6, 18(2), 19, 20, 22, 23, 25
27	11	1, 5, 6, 7, 9, 10, 12(2), 13, 18, 29
28	5	3, 5, 22(2), 23
29	9	2, 5, 9, 15, 16, 17, 23(2), 25
30	6	10, 18, 20, 21, 26, 28
31	15	2, 7(2), 11, 12, 20, 21, 24, 25, 26(2), 27, 28(2), 29
32	22	1(2), 2, 3(2), 4(2), 5(2), 6, 7, 8, 16, 18, 19, 20, 21, 23, 25, 26, 29(2)
33	3	17, 19, 21
34	6	4, 6, 11, 23, 24, 26

35	34	1(2), 2(2), 3(2), 4(3), 5(2), 6(2), 7(3), 8(3), 11(2), 13, 15, 17, 19(2), 20, 24, 25(3), 26, 27(2)
36	6	1, 14, 16, 22(2), 26
37	8	2, 5, 7, 13, 14, 23, 27, 29
38	4	8, 11, 12, 29
39	58	1(2), 2, 3, 4, 5(3), 6(3), 7, 8(4), 9, 10, 11(2), 12, 13, 14, 15(3), 16(2), 17(2), 18(2), 19(4), 20(3), 21, 22, 23, 24, 25(4), 26(2), 27(2), 28(4), 29, 30(2)
40	22	9(2), 10, 11, 14, 15(2), 17, 18(3), 20(2), 21, 22(3), 23, 24, 26, 27, 30
41	4	3, 11, 17, 25
42	4	1, 19, 29, 30
43	3	2, 14, 29
44	3	16, 21, 28
45	78	1(2), 2(3), 3(4), 4(2), 5(2), 6(3), 7(2), 8(2), 9(2), 10(2), 11(2), 12(3), 13(3), 14(4), 15(4), 16(2), 17(3), 18(2), 19(4), 20(3), 21(4), 22(3), 23(3), 24(2), 25(2), 26(2), 27(2), 28(2), 29(2), 30(2)
46	10	3, 4, 5, 6, 7(2), 9, 12, 23, 27
47	2	21(2)
48	2	8, 19
49	16	1, 2(2), 3(2), 4, 5, 10(3), 14, 15, 16, 21, 26, 29
50	25	1, 2, 3, 6, 7(2), 10(2), 11, 12, 13, 15, 16, 17(5), 19, 24(2), 25, 26, 27, 28
51	2	7, 23
52	13	8(2), 10, 11, 12, 14, 19, 20, 21, 22, 23, 27, 28
53	4	5, 14, 28, 29
54	5	7, 15, 24, 25, 26
55	14	1, 3, 5, 7, 9, 11, 17, 20, 24, 25, 26, 27(2), 28
56	13	5, 7, 12(2), 13, 16, 18, 21, 24, 26, 28(2), 29
57	7	7, 9, 14, 20, 23, 27, 28
58	3	1, 22, 26
59	26	1, 7, 8, 9, 10(2), 12, 14, 15, 16(4), 17(2), 20, 21(2), 22, 23(2), 24, 25, 27, 28, 30
60	34	1(2), 2, 4, 7, 8, 9, 10, 11(2), 12(2), 13, 14(2), 16, 18, 19(3), 20, 21, 22(3), 23(2), 24, 25, 27, 28(3), 29
61	9	2, 3, 4, 6, 15, 17, 19, 21, 23
62	15	1, 2, 3, 11, 14, 15(2), 16, 17, 18, 23, 24, 29(2), 30
63	6	9, 12(2), 14, 23, 25
64	3	10, 16, 27
65	3	1, 3, 12
66	6	5, 13, 16, 18, 25, 27
67	4	6, 17, 21, 23
68	4	4, 7, 8, 19
69	29	2, 3(2), 5, 6, 9(2), 10, 12, 13(2), 14(2), 16, 17, 18, 19, 21(2), 23, 24, 26(2), 27, 28(2), 29(2), 30
70	5	3, 19, 24, 25, 28
71	5	6, 13, 18, 23, 29
72	13	7(2), 15, 17, 20(2), 22(3), 24, 26, 27, 29
73	5	3, 5, 20, 27, 29
74	5	3, 9, 11, 15, 20
75	4	6, 16, 18, 19
76	12	6, 9, 10, 12, 13, 16, 19(2), 22, 24, 27(2)

77	31	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, 27, 28, 29(2), 30
78	10	1, 2, 4, 5, 8, 10, 15, 17, 22, 24
79	18	1, 5, 6, 11(2), 13, 15, 16(2), 19, 20, 21(2), 22, 25, 28, 29, 30
80	20	5, 6, 7, 9(3), 10, 11, 12(2), 13, 14, 17, 18, 19, 20, 24, 25, 26, 28
81	4	1, 22, 26(2)
82	7	3, 5, 6, 9, 15, 27(2)
83	3	11, 21, 29
84	2	20, 30
85	2	4, 13
86	3	13, 14, 25
87	2	5, 13
88	10	1, 2, 3, 4, 7, 13, 17, 18, 19, 26
89	17	1, 2(2), 3, 4, 6, 10, 15, 16, 18, 19, 21, 22, 24, 25, 26, 27
90	34	1(3), 3, 4(2), 5, 7(2), 8(2), 13, 14(3), 15, 16, 17, 18(3), 19(2), 20, 22(3), 26(2), 27, 28(2), 29(2)
91	3	5(2), 21
92	21	1(2), 3, 4, 5, 8, 11, 15, 18, 19(2), 20, 22, 24, 25(3), 27, 28(2), 29
93	7	1, 9, 10, 12, 13, 14, 28
94	4	10, 16, 29(2)
95	111	1(3), 2(4), 3(4), 4(3), 5(3), 6(4), 7(3), 8(4), 9(4), 10(3), 11(4), 12(5), 13(4), 14(5), 15(5), 16(4), 17(4), 18(4), 19(3), 20(3), 21(5), 22(4), 23(5), 24(4), 25(3), 26(3), 27(3), 28(3), 29(3), 30(2)
96	11	6, 9, 10, 11, 12, 13(2), 22, 24, 25(2)
97	11	2, 3, 4, 6, 7(2), 8(2), 15, 20, 24
98	6	9, 10, 17, 19, 20, 25
99	14	4, 8, 9, 11(2), 12(2), 14, 16, 17(2), 18, 22, 27
	1400	

NATIONAL SECURITY AGENCY
Washington 25, D. C.

COURSE	Military Cryptanalytics, Part I
LESSON 10	Miscellaneous monalphabetic substitution systems; concealment systems
TEXT ASSIGNMENT	Pars. 81–84

1. The following two messages were intercepted on the same net during a morning offensive Solve them and recover all keys.

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

2. Solve the following cryptogram and recover all keys.

G H U I P G J H N I M B S P R I U S N S S H P G B 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

3. The following cryptogram is suspected to contain the word "REGIMENT". Solve it and recover all keys.

B U F W W H E A G H M I T A J J S K L S M N H I U 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 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 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 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 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

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 P M I O P

U Q A R H K Y Q C G W P G E P G A E P L V G F H J F B B L Z

U S S X S R M Y F Q X T S H D T T D Y C F X F Q H H L P K T

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

J H K I U S W W A L H S I U M H H A E Z I I Z W H H P H W U

4. The following cryptogram is suspected to contain the word "BATTALION". Solve it and recover all keys.

R D I T J O G D P F Q U M T D I K R U I U L H K I M A S K I

J M H Q D B B U G I A U Y B U I L Q U M P D T T D F K Q U D

B B U G I K F B K V U Q U I K Z K Q U H K T D H T E C M K I

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

T E R D I C D I D R L U J Q U M J M V U I R K E T I K H Q A

5. The following two messages are suspected to be isologs. Recover the plain text and reconstruct the cipher alphabet involved.

Message "A"

Q M S L G P W J R N N P H R E E N Q O H M A B G R P L N W J

R N N V H M A Y T R G S L A P H M H X R E F R G B I L N P H

Message "B"

E T O S R D M O T A D P C O N N O R X D T A R S U T W G A S

U A S A S N Y E X L I A H R I P L N S A O F G S B E O E L T

6. Solve any five of the ten innocent-text messages given below.

a. TO COVER AND HIDE YOUR FINANCES, I MAINTAIN STAFF TO BARTER FRANC EXCHANGE.

b. BEARER IS A FRIEND. I CANNOT WRITE MUCH. WILL YOU BE READY TO MEET A TRUSTED INTERMEDIARY SO YOU CAN GIVE ALL NECESSARY DOCUMENTS TO HIM NEXT WEEK? I HAVE NOTHING MORE TO SAY.

c. The following is an actual radiogram which was held up by a censor:

ES100 81 RADIO-WASHINGTON DC 210P JULY 1 1941

ROBERT C JOHNSTON III
CARE HELVETIA PALACE HOTEL LUGANO (SWITZERLAND)

MATERIALS ADEQUATE. CONTRACTS YOUR ASSISTANT RETURNED TO ME WERE OKAY AT CONSULATE. INSURANCE EXPEDITED QUOTATIONS ON CARGO RATES ALSO AS OF TOTAL POOLED SHIPMENTS. BECAUSE PRESENT HOLDING OF SHARES IS LINKED TO UNDECLARED ASSETS ATTENTION IS DIRECTED TO PROGRAM OF DENUNCIATION BY AGGRESSIVE MINORITY CHALLENGING DIVIDENDS. REALTY VALUES PREDICT SUSTAINED EXCEPTIONAL PROFITS HEREAFTER WITH DISCLOSURES AT MEETING ON SEVENTEENTH BREAKING UP RENEWED OPPOSITION.

REMSEN

d. The following message, poorly spelled, is shown just as it was written by the originator.

DISATISFIED WITH IMMIDIATE RESULTS OF YOUR AMALYSIS STOP ADITIONAL RENUNERATION TO ALL PERSENNEL WHO INDENTIFY COMPONANT PARTS OF THE ALLOIS OTHER THAN NICKEL OR COPPER

e. CATALOG VALUES CANCELED UNLESS OFFER STRENGTHENED. COMPLEX SELECTION EFFECTIVELY STALEMATED. PSYCHOLOGICAL FOUNDATION UNWARRANTED

f. REQUEST CONSIDERATION OF ONLY THE MOST USUAL PLACEMENTS OF ORDERS FOR BALANCED BUSINESS TRANSACTION. LET NOTICE BE GIVEN FOR A SUBSTITUTION AS SOME ARTICLES NOT EASILY CHANGED. PARTNER AGREEMENT IS EXTRA HELPFUL WHEN MAXIMUM.

g. The secret text in the following message was solved by Sherlock Holmes in one of Sir Arthur Conan Doyle's stories.

"The supply of game for London is going steadily up. Head-keeper Hudson, we believe, has been now told to receive all orders for fly-paper and for preservation of your hen-pheasant's life."

h. In April 1941, the French (Nazi-controlled) newspaper *Paris-Soir* printed the following poem by an anonymous contributor apparently extolling Adolph Hitler. A fairly literal translation is given beneath the original.

Aimons et admirons le Chancelier Hitler
L'éternelle Angleterre est indigne de vivre
Maudissons et écrasons le peuple d'outre-mer
Le Nazi sur la terre sera seul à survivre.
Soyons donc le soutien du Führer allemand
Des boys navigateurs finira l'odyssée
A eux seuls appartient un juste châtiment
La Palme du vainqueur attend la Croix gammée.

(Let us love and admire Chancellor Hitler
Eternal England is not worthy to live
Curse and eliminate the people across the sea
Nazidom on earth will be the sole survivor.
Let us therefore support the German Führer
The seafaring boys will finish the odyssey
To them alone a fitting punishment
The palm of victory awaits the swastika.)

i. The following telegrams were filed by the same originator to the same addressee on successive days.

Message No. 1

MONEY SENT TO NEW HAVEN IN BANK ON ARTS ACCOUNT. HE MAY HAVE DRAWN ALL AND GONE HOME BEING SO BORED. AS ALWAYS HE NEEDS A LOT OF CASH, YET IS NOT ABLE TO DO MUCH WITH THE MONEY SENT TO PAY HIS LAB SCHOOL BILLS.

Message No. 2.

SENT FORTY DOLLARS BY CHECK TO HENRY AND ALICE AFTER THEY PAYED ALL ARTS OLD DEBTS STOP. I REALLY WANT AGREEMENT WITH THEM AND WE MUST MAKE ART STOP CHARGES AND BILLS ABOUT TOWN. SEND NO MORE CHECKS TO HIM OR CASH TO WASTE ALWAYS FOR HE SPENDS IT.

Message No. 3

MOTHER SENDS LOVE AND WAITS EACH LETTER AS SHE ALWAYS DOES, SO WRITE AS MANY AS TOM AND ELOIS DO TO HER AS ALWAYS, JERRY.

j. The following innocent-text message is suspected to contain information on ships sailing from Boston.

AT NINE ELEVEN THIS MORNING FOLLOWING CONVERSATION SURPRISED REPORTERS: "RUSSIA, FRANCE AND ENGLAND ASSURED PREPARATIONS WERE NOW RAPIDLY ATTAINING SATISFACTORY ALLOCATIONS. HOWEVER, THEIR ALLOTMENTS VARIED SLIGHTLY, AND IN AGREEING PROBABLY WERE NOT SURE OF THE OUTCOME. UNLESS TERMS ARE QUICKLY DETERMINED, MANY SPECIFIC AGREEMENTS WITH EACH OTHER WILL HAVE TO BE MADE."

~~CONFIDENTIAL~~