CAUTION: THESE RECORDS WILL BE USED FOR OFFICIAL PURPOSES ONLY, DO NOT REMOVE PAPERS NOR REVEAL CONTENTS TO UNAUTHORIZED PERSON(S)

# RECORDS CHARGE-OUT

REF ID:A64639

10212

| | | | |
|---|---|---|---|
| DATE OF REQUEST | 25 Jan 61 | SUSPENSE DATE | 10 Feb 61 |

| | | | | |
|---|---|---|---|---|
| FILE OR SERIAL NUMBER AND SUBJECT | From File of Special Consultant (Friedman)<br>Course in Military Cryptanalysis, Part I Lessons 1, 2, 3 & 4 | | | |
| TO | NAME AND EXTENSION OF PERSON REQUESTING FILE<br>Mr. William Friedman LI6-8520 | ORGANIZATION, BUILDING, AND ROOM NUMBER<br>310 2nd Str, SE, Wash, D.C. | | |
| RETURN TO | Mrs. Christian, AG-24, NSA, Ft. Geo, G. Meade, Md. | DATE RET'ND. | INITIAL HERE | |
| INSTRUCTIONS | WHEN TRANSFERRING FILE TO ANOTHER PERSON, COMPLETE SELF-ADDRESSED TRANSFER COUPON BELOW, DETACH, STITCH TO BLANK LETTER-SIZE PAPER AND PLACE IN OUT-GOING MAIL SERVICE. | | | |

10212

## 2ND TRANSFER COUPON

TO:

FILE (serial number and subject)

TRANSFERRED TO: (name and extension)

ORGANIZATION, BUILDING, AND ROOM NUMBER

DATE (sig) (ext.)

~~RESTRICTED~~

~~Security Information~~

NATIONAL SECURITY AGENCY

# COURSE

# IN

# MILITARY CRYPTANALYSIS, PART I

NOTICE: This document contains information affecting the national defense of the United States within the meaning of the Espionage Laws, Title 18, U.S.C., Sections 793, 794 and Title 50, U.S.C., Sections 46, 46a and 46b. Its transmission or the revelation of its contents in any manner to an unauthorized person is prohibited by law.

National Security Agency
Washington 25, D. C.

December 1952

record taken from
WFF's home

~~RESTRICTED~~

(BLANK)

# COURSE IN MILITARY CRYPTANALYSIS, PART I

## Monoalphabetic Substitution Systems

### Introduction

This is the first of a series of six basic courses in the art of military cryptanalysis. The purpose of this course is to impart to the student the methods and techniques which form the basis for the cryptanalysis of the 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; unilitcral substitution; multiliteral substitution; polygraphic substitution; and miscellaneous monoalphabetic substitution systems. It consists of ten lessons and an examination as follows:

Lesson 1, Fundamental principles

Lesson 2, Unilitcral substitution with standard and mixed cipher alphabets

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

Lesson 4, Multiliteral substitution with variants

Lesson 5, Polygraphic substitution: small matrices

Lesson 6, Polygraphic substitution: quadricular tables

Lesson 7, Polygraphic substitution: miscellaneous systems

Lesson 8, Miscellaneous monoalphabetic substitution systems; concealment systems

Lesson 9, Monoalphabetic substitution with irregular-length cipher units: monome-dinome systems; miscellaneous systems

Lesson 10, Syllabary squares and code charts

Examination

The text reference for this course is the National Security Agency publication, "Military Cryptanalysis, Part I" (December 1952).

This course has been designed as a self-study or extension-type course; therefore, there is no limit placed on the number of hours that may be spent in the completion of the course, any lesson, or the examination. However, for statistical purposes it is requested that the student indicate the number of hours spent in the completion of each lesson and the examination.

The cryptograms in this course 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 $\frac{1}{4}$-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 Cryptanalysis, Part I |
| LESSON 1 | Fundamental principles |
| TEXT ASSIGNMENT | Sections 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", 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, São Paulo, Brasil.
To: Gualterio Costa, New York City.

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 (in round numbers) 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 e 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 ACEPT ELORR OPRST AILRT EELRY ACIMP EEMNT

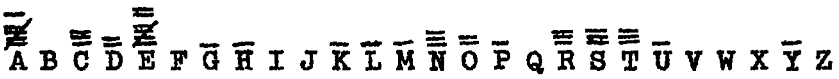
DESST DEORY

11. Using cross-section paper prepare a uniliteral frequency bar distribution of the letters of the following paragraph:

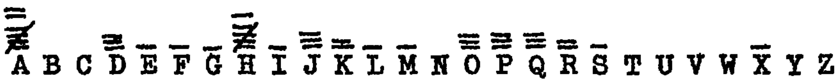
> "The shortest and surest way to live with honor in the
> world is to be in reality what we would appear to be;
> all human virtues increase and strengthen themselves by
> the practice and experience of them."

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

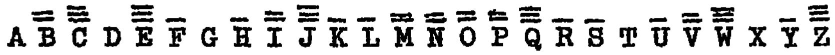
a. ORANA THPNO SKTCD MEEES CERAE
RNUSA ETLGD AYECA



b. DHJJK QOAHR XKSOF HPQGA PPHLA
DIADE HJROA MAHQA

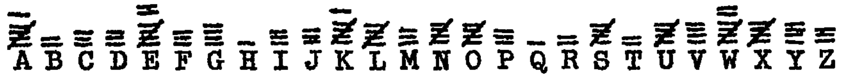


c. ROLEH KBWFZ CQCPZ NVJWZ MIVEQ
EPCIN OJSJU YMWQB

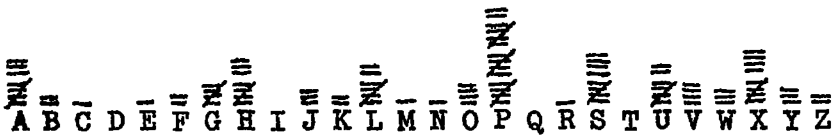


13. Which of the following substitution ciphers are monoalphabetic?

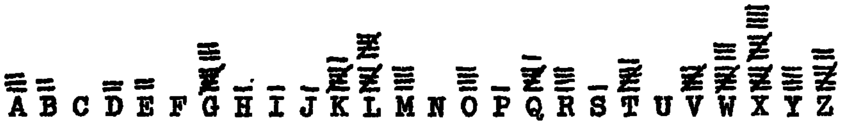
a. UJKLW EUVKL FSPAQ PHTKR DZNGL
SELYN XYXBX JDATU WEUZG WFVXM
MNZAY AOSGU DCLGI OEWJE IFOKM
KNWAP KOIEV AROEV WSCWN SBCYX



b. HUPYP XXAEP AFGZP VGLHA SLXHU
SXXAY PWKAS LHPRH ALOBA XPLVS
WUPJP OBSHU HUPGF XGKPH PVSWU
PJOPZ SVPYS MPOAX ULSLP CGNJX

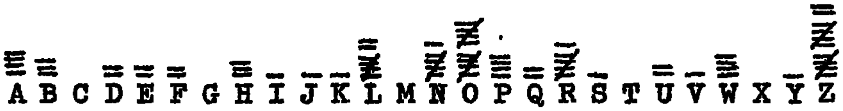


c. GXYVL ZXMXS LOZGR WEJLX PWTKZ
GMXLW QIVZW QBRXK KTDVL MXAEX
VHMXA LOTLY TKDWX GBQKQ LWZXG
RTYYZ KTOXG AWXLQ LOZGR XVWGQ

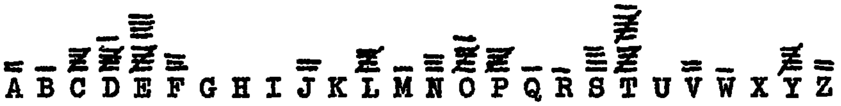


14. The following messages were enciphered monoalphabetically. Determine in each case whether the cipher alphabet used was a standard or mixed alphabet and if standard, whether direct or reversed.

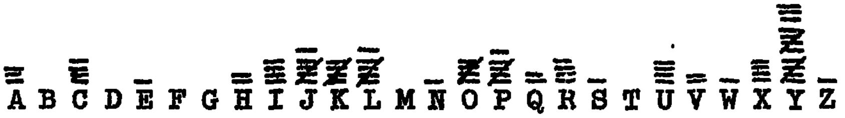
a. ANVOR LOUNQ RLEZW ZHNEZ WZBOR
ZKYLF AOZSO ONORF PJZPP LDZDN
LRZLB LABWZ HNAPO WQHOO RZIZU



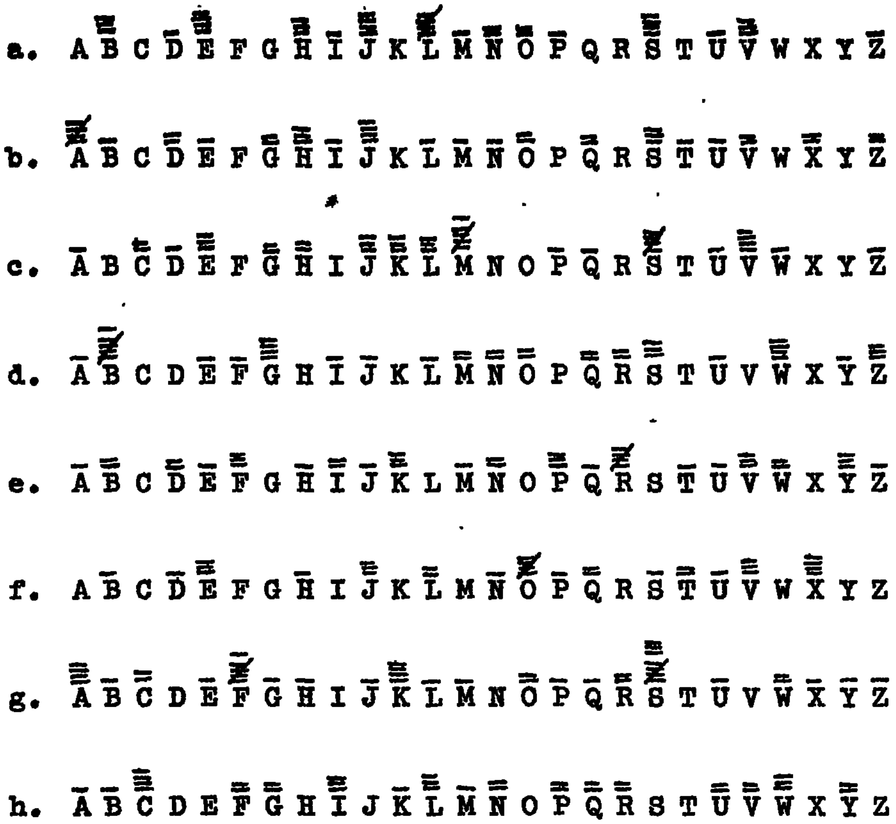
b. ESPAP LVDLY OECZF RSDTY ESTDO
TDECT MFETZ YBFTN VWJTO PYETQ
JTELD OTCPN EDELY OLCON TASPC



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



15. Derive the $\phi_p$, $\phi_r$, $\phi_o$, $\Lambda_p$, $\Lambda_r$, and $\Lambda_o$ for each of the following distributions, and evaluate the [monoalphabetic] goodness of $\phi_o$ and $\Lambda_o$ 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 (✓) in the diagram; in the case of those not clearly belonging in either of these categories, check "decision suspended".



| | | | | | | | | Goodness of $\phi_o$ | | | Goodness of $\Lambda_o$ | | | Decision | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | N | $\phi_p$ | $\phi_r$ | $\phi_o$ | $\Lambda_p$ | $\Lambda_r$ | $\Lambda_o$ | G | F | P | G | F | P | mono. | non-mono. | 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   V   L D C

GR  35   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 1610 by MR       M F F   V   L D C

GR  35   BT

   NR I_   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   0 9 3 5

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

GR  _ _   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   0 9 3 5
```

(BLANK)

~~RESTRICTED~~ ~~Security Information~~

NATIONAL SECURITY AGENCY
Washington 25, D. C.

| | |
|---|---|
| COURSE | Military Cryptanalysis, Part I |
| LESSON 2 | Unililteral substitution with standard and mixed cipher alphabets |
| TEXT ASSIGNMENT | Sections 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 monoalphsbetic 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:

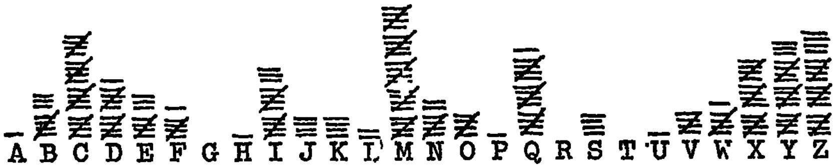
(1) A B C B A D B

(2) A A B A

(3) A B C D A

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

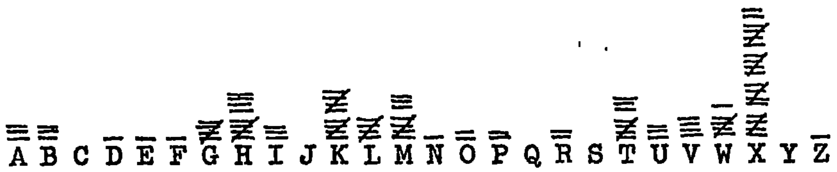
```
JMQVS  QZXIF  FMZSL  IZMLZ  CEMEB
FQOME  MDXYQ  OZCYY  XJMZI  VMZIY
OQWYI  DKYMV  MZMNQ  EQKMX  CCWZB
CYIXI  CDYYX  CBZQI  FZCQN  HWDOX
ICDJQ  YPMMD  YMVMZ  MFSNQ  EQKMN
QDNEW  OJMAW  IBEMD  XNMYX  ZCSMN
YXCBU  MQZME  CVIDK  CWZXZ  CCBYX
CZMQZ  BCYIX  ICDYY  XCBZQ  FYXCD
```



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

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

```
WXLMK  HRXKL  ATOXU  XXGHK  WXKXW
MHIKH  VXXWT  MHGVX  MHTKX  TPAXK
XLNUF  TKBGX  TVMBO  BMRAT  LUXXG
KXIHK  MXWLM  HITVD  GHPEX  WZXXX
```



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

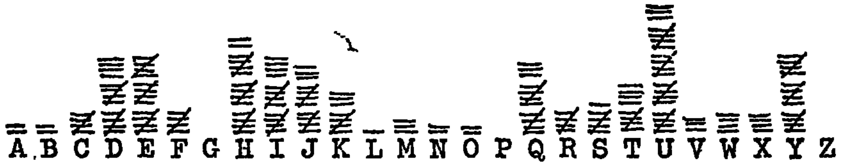
8. Solve the following cryptograms, and indicate the specific keys:

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

9. 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

10. 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.

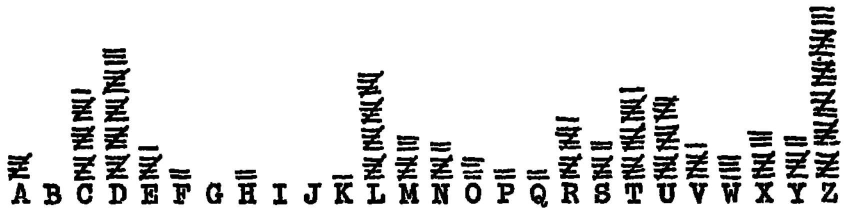
b. Prepare a condensed table of repetitions of digraphs and trigraphs appearing more than twice, and include all repetitions of longer polygraphs.

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 |

11. 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
```

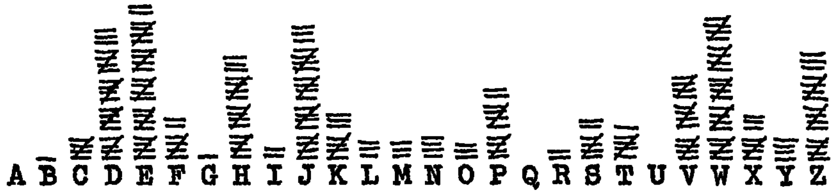


$\phi_p = 2655$ $\phi_r = 1532$ $\phi_o = 2770$

~~RESTRICTED~~

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

```
        5    10    15    20    25
A  JZDFV WHEDZ VHWDS YKTWD OEDZD
B  EDSEC CWHHW EDZTE XXWSZ VNZVZ
C  SPFJK VZTYP HJDWO LJWDP VPWTI
D  REDZE XEKVF PJVEY HHJEF EDZFV
E  WHEDZ VHJPJ ZHJLP JXEKV JLTWM
F  WHWED WHWDM WSWDW JREXI YKZCE
G  KDJPW DCEMW DONZH JJEPJ JPSBE
H  KVFEH WJWED HNZHJ EXXPW VJEND
J  HJEFS EDXWV CPJWE DVZGK ZHJZT
```

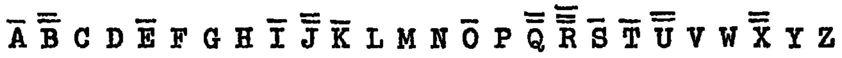


$\phi_p=3362$ $\phi_r=1940$ $\phi_o=3560$

~~RESTRICTED~~

13. Using the sequences recovered in Problem 12, solve the following cryptograms and indicate the specific keys:

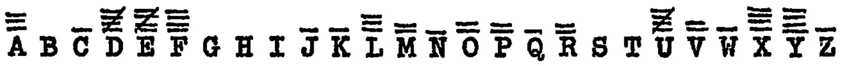
a. U R J J R  X Q U Q X  K S A R B  B E T O I



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

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



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

14. 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

15. In solving several unrelated monoalphabetic cryptograms, the following cipher alphabets were reconstructed. Recover all key words in each case. 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: 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

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

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: 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

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 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

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 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

~~RESTRICTED~~

~~Security Information~~

NATIONAL SECURITY AGENCY
Washington 25, D. C.

COURSE — Military Cryptanalysis, Part I

LESSON 3 — Multiliteral substitution with single-equivalent cipher alphabets

TEXT ASSIGNMENT — Section 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)

~~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 |

$\phi_p$=2270 $\phi_r$=1362 $\phi_o$=2288

(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:

```
11101   10333   12231   03023   33122   31000
06002   60610   15231   40424   24052   33206
03042   61122   33263   12334   11052   33011
00001   12200   20010   02600   06151   62611
13367   89310   62222   26050   41221   04101
30511   24230   52604   22221   21604   10151
10023   14122   30105   00113   50024   11111
33504   10131   42305   03042   60623   10360
```

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 ENEMY is enciphered thus:

| | | | | | |
|---|---|---|---|---|---|
| Key: | 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: | + | - | + | - | + | - | + | - |
| 1,2: | ++ | 5 | 1 | 4 | 4 | 3 | 1 | 6 | 1 |
| | +- | 1 | 5 | - | 8 | 4 | 1 | 13 | 1 |
| | -+ | - | 3 | 4 | 3 | 1 | 3 | 1 | 2 |
| | -- | 2 | - | 5 | - | 2 | - | - | 3 |

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

(32-element alphabet)

~~RESTRICTED~~

~~Security Information~~

NATIONAL SECURITY AGENCY
Washington 25, D. C.

| | |
|---|---|
| COURSE | Military Cryptanalysis, Part I |
| LESSON 4 | Multiliteral substitution with variants |
| TEXT ASSIGNMENT | Section 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)

~~RESTRICTED~~

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)

~~RESTRICTED~~

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 |
| P | 47 | 64 | 36 | 71 | 06 | 55 | 00 | 68 | 78 | 45 | 52 | 12 | 69 | 43 | |

(For distribution, see page 5)

~~RESTRICTED~~

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 | 26 | 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 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

~~RESTRICTED~~

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   58578
```

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  33609  17554  83811  72477
85433  50805  37598  60718  37306  17704
06159  62714  46551  69370  50945  58696
19561  70681  86600  83474  55377  71502
16576  41295  65052  00751  47289  33956
59497  38764  66574  72261  08560  73763
68350  48516  25000
```

9. Tho following naval messages are suspected to bc 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
```