SRH- 171

NAVY DEPARTMENT
Office of the Chief of Naval Operations
WASHINGTON

SECONDARY COURSE IN CRYPTANALYSIS

Op-20-GR

~~RESTRICTED~~

NAVY DEPARTMENT
Office of Chief of Naval Operations
WASHINGTON.

SECONDARY COURSE IN CRYPTANALYSIS

ASSIGNMENT No. 1

INTRODUCTION

1. The attention of all students is invited to the RESTRICTED classification of the subject of Cryptanalysis, which prohibits revealing any information concerning this course, or the fact that such a course exists, to any person not in the U.S. Navy or Naval Reserve.

2. This course of instruction is designed as a means of continuing the training, in most cases by correspondence, of the students who have successfully completed the Elementary Course in Cryptanalysis. In general, this course will be conducted along the same lines as the Elementary Course, i.e., the course will be divided into assignments, and the students will complete each assignment in turn before being issued the succeeding assignment. Prefacing each assignment will be what is considered sufficient instructional information for the average student at that stage of training to complete the problems given.

3. The Secondary Course contains some problems of the types already studied in the Elementary Course, and in some cases the problems will be no more difficult. In general, however, the problems are more difficult and require the student to exercise the ingenuity which his previous training in cipher solution has fostered. The collateral information furnished will be found to diminish constantly and the student will find himself thrown more and more on his own resources.

4. As in the Elementary Course, if the student becomes hopelessly bogged down in his attack on any problem, he is instructed to forward his work sheets to the Chief of Naval Operations (Communication Security Section) for inspection, and assistance will be furnished and the work sheets returned. Upon completion of an assignment, the student should forward the solution with any pertinent remarks on his method of attack, but should retain his work sheets for future reference.

5. The synoptic table (page 2) shows diagrammatically the various types of ciphers which were treated in the Elementary Course in Cryptanalysis. It is designed to summarize the relationships between these elementary systems, and to indicate the points at which the more advanced types branch off. It will be noticed that the type called mono-alphabet substitution in the text of this Course is listed in the table under the sub-heading mono-graphic, because, unless the distinction between mono-graphic and poly-graphic types is desired, the term mono-alphabet substitution is generally taken to refer to the mono-graphic type.

6. The extent of the Elementary Course was to explain the elementary methods of solving the simpler cryptographic systems. More advanced methods may be necessary to solve special cases or variations in these basic systems. Mono-alphabet substitution has been covered, except for the complicated poly-graphic methods which are seldom used. Under periodic poly-alphabet substitution the multiple alphabet and the regular progressive-alphabet types have been discussed. Under single transposition the simple routes, columnar, and grille systems were mentioned.

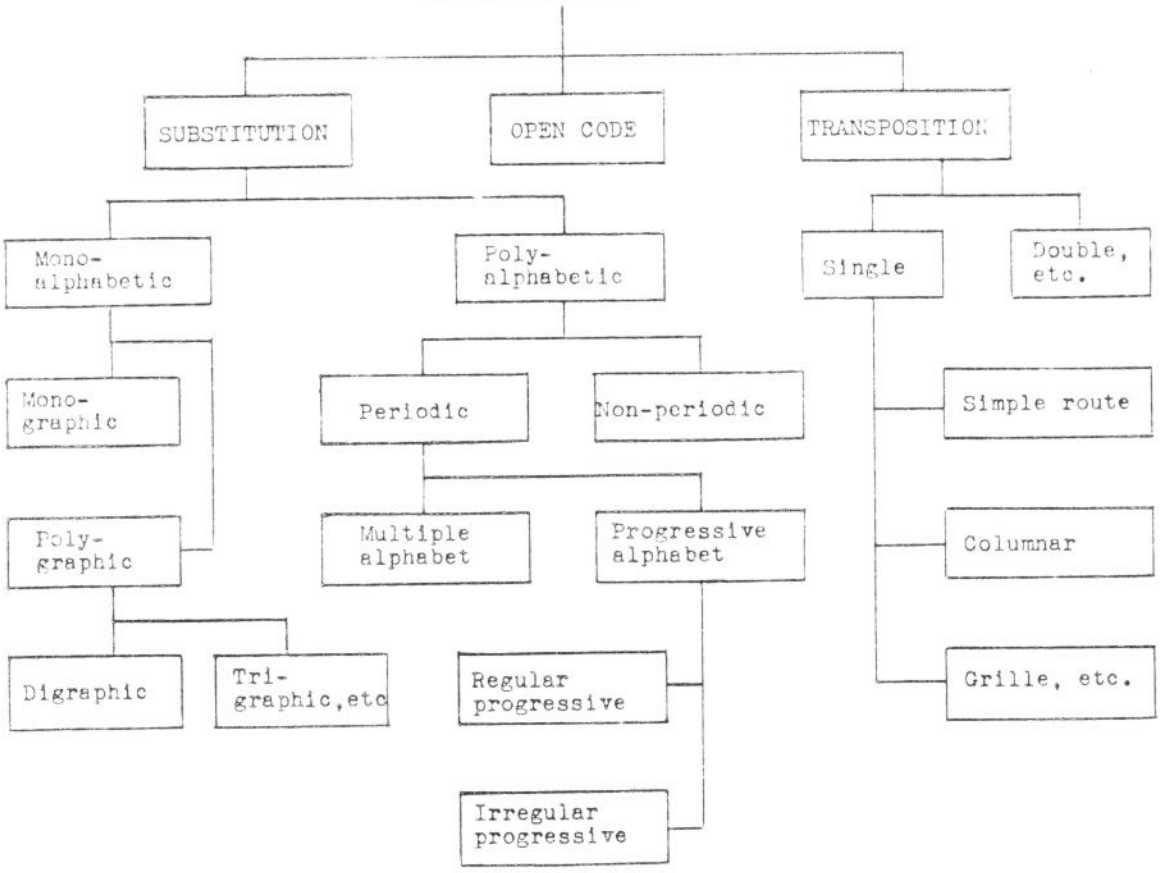
7. Some of the cryptographic methods remaining to be explained further are:

(a) Irregular progressive ciphers, (b) Non-periodic methods (continuous key and multiple sliding alphabet systems), (c) Double transpositions, and (d) Superimposition of cipher systems.

ASSIGNMENT No. 1

SYNOPTIC TABLE FOR CIPHER ANALYSIS

CRYPTOGRAPHIC METHODS



GENERAL REMARKS ON CRYPTANALYTIC METHODS

8. The method of exposition in the Elementary Course was to give a working knowledge of each type of system from the standpoint of cryptography, then to outline briefly a method of solving the system, and finally to give a few problems in order that the student might discover for himself the steps necessary for a complete analysis and solution. The student should guard against establishing in his mind a definite method of attack for each cryptographic problem. A study of the mental processes of a successful cryptanalyst reveals that the method of reasoning must be inductive rather than deductive. In other words, he must proceed from the limited specific facts available in a given cryptogram, to the general system, and not from the general system to the specific fact. While the two processes of logic are never entirely separated in practice, research has shown that the more purely inductive the process becomes, the more successful will be the result.

9. There are some cryptanalysts who advocate learning the subject of cryptanalysis through the actual solution of cryptograms alone, in order that the purely inductive processes of reasoning may be developed from the start. However, it is believed that experience in solving the various types of elementary cipher systems will save considerable time and effort on the part of the student,

002

who would otherwise be duplicating the work of the pioneers in cryptanalytical research. If some of the explanations have been found rather brief, it is probably the result of an effort to leave the rest to the imagination of the student.

10. The basic methods of solving many of the elementary cryptographic systems may also be applied to the solution of the more advanced systems, with correspondingly increased complications added. For instance, the general method of attack used for regular progressive ciphers will aid in the solution of irregular progressive ciphers.

11. For the student who has arrived at the present point in his cryptanalytical training, very little exercise has been given in one of the most difficult tasks of analysis, which is the determination of the basic type of system involved in the encipherment of a particular problem. Unfortunately, there are no absolutely definite tests that can be applied to cipher text which will disclose the system used. The only method of determining the system is often by the long and laborious process of elimination. The only knowledge that the cryptanalyst can bring to his aid in this most difficult step is that gained by long experience and practice in the analysis of many different types of systems.

Problem No. 1

A B A/B A I F A/C C A/B Y C C/A A C/ O U A A A/B C C C/B C B/A N B C/A B A/ S I

A C C/A B D E C/A A B/B R B C/A B C/ L E C B C/A B/ X I A/B C B/B N A B/C A C/ G T

B C C/B C O N B/C A C/B T C C/A B C/ O E A C A/A B S B/C A C/C T B B/A C A/ W A

A A B/A C R D C/A B B/A S A C/B A B/ U C B A B/A B G E C/A B B/ S C A C/A A B/ T R

A B C/C B E V A/A B C/A E A B/A B B/ R S A C A/B B A L C/B C C/B O A A/A A A/ F C

B C C/A A O U C/A A B/A R B B/A B C/ S E B A A/B C F O C/A A B/C R A C/C B B/ T W

B C C/B A O I H C/B C C/A O A C/A A B/ U R A B B/A B S S B/A C A/A A A B/A C A/ R A

C A C/B C T O C/B A B/A G C A/C A C/ A T B C C/A A O R B/A B C/C E A C/A B A/ T I

A A B/A B R E C/C A C/B T C C/C B B/ O W A C A/A A A R B/A C C/B D C A/A C A/ M A

A B A/B C I N B/A C B/B 3 C C/A C C/ O D C C A/ Y

Problem No. 2

G I U L A T R E T E T O I T H T U D I I M L F V E I R O S P

O O C H S X R D R E A F R O E N O N F A D R T O O I O E W E

I A O S F R R L S T O S T A E L P I T T N D L M T M I Y S R

S S P O B N D W A H A O R T A E A E Y L I D S O E Y O C N O

Problem No. 3 Serial No. 1

FROM: XY (CINC)
TO : AB (COLLECTIVE CALL)

0017-2315 APRIL 1930

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

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

ASSIGNMENT No. 1

Problem No. 3 Serial No. 1 (Continued)

Y W T V K U E G D T C L K H C O K O N Q R E P L W L H Z M Q L Q U O J

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

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

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

M U K J U V D M L

Problem No. 3 Serial No. 2 0018-0015

FROM: CY (CINC)
TO : CD (FORCE COMMANDER)

C U F N D H P D V T F G X Y U V Y F G K J X U X F N C D Y M A H K O J

X U I J D H J T W W U O L Y U T W E N Q H C N F Q Q Q J A L G P O Q Z

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

G U E R L V P T U U H V K J S H N S M D K Y F

Frequency table:

Cipher ------	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alphabet #1 -	5	1		1	4	1	5		1				5	1		2			4	2			2	5	6	
Alphabet #2 -	1		1		1	2	1					3	7	4	1	3	2			2	10	4	4			
Alphabet #3 -	2		2	2	1	4	5	1	5	2	2	3		4				2		7	1		3	2	1	
Alphabet #4 -	3		5		1	4	1	3		6	1			2	2	2	6	2	6		1	2	1	1		
Alphabet #5 -			1	2			2		5		2	6	2	7	4	2	2	4		1	3	3			1	2
Alphabet #6 -		3	1	1				4			8	4			6		6				7	3	3	3		
Alphabet #7 -	2		1	5	2		2	2		11	2	2				4		5	1	1			1		5	3

Problem No. 4 Serial No. 1

FROM: COMMANDER BLACK FLEET
TO : COMMANDER SUBMARINE FORCE, BLACK FLEET

WCYQA UBBUL LSADS OVSWY DNSWS XHDSY ATMHX LUWCO KQRKW EFWYY

ECNVH PHYSH TOQAD JOBAK ZDHKQ PDMZZ RABQQ LLYTX HBJEY OLYNX

IHORQ EBXQR YCYYQ KRADE LQXHM SXRDB JQTDW LKAGU NVZJO YQODE

DOIGR OCBQS IOCQD UDXIC OXSBH YOPDX ROBIM RNFEL IIDXV YWLTM

CXGNQ BBPDH OBFQR PDYEL IGRKJ HBJEY NOXNL KFEXR DNMFM SNSWS

NLAAO PLLYU LUBAH KHLKI RKLJL RVNOY EJHIR AOTQP LUWRI ZKLIC

LULJO HMLQY XXDTD XFWYY ZWBAM LNSFT

Problem No. 4 Serial No. 2

FROM: COMMANDER BLACK FLEET 0014-1200
TO : COMMANDER SUBMARINE FORCE, BLACK FLEET

JRBSW ZWBAM LNSAH NAYFY JRGXL SWDPQ PBFTS YWNCQ CHYTX HBJEY

OLYNX IHORQ EBXQR YCYYQ KRADE LQXHM SXRDB JQTDO PNNYA POCAB

OLWAH AALGZ NVZJO YQODD RCYQA UBBUL EHKDE NWZJG OTRDH PCCDV

ULPWD ADAUV XGLIH NTMHX LUWCO KQRKW DLMFM RNSWS KHLKB CUQFY A

004

ASSIGNMENT NO. 2 NOT AVAILABLE FOR REVIEW

RESTRICTED
(Revised Sept. 1939)

ASSIGNMENT NO. 3 - SECONDARY COURSE IN CRYPTANALYSIS

ANALYTICAL SOLUTION OF UNKNOWN CIPHER SYSTEM

Introduction

1. Heretofore the assignment has taken the name of the cipher system involved. The introductory remarks have defined the cipher system, described some of its properties, and have shown an example of enciphering and deciphering.

2. In this assignment we will reverse the former procedure. The cipher system will be unnamed and unknown. All you will learn about the cipher system is what will come out in the process of solution and in the "post-mortem", which appears after the last problem. The problems will be in variant forms of the basic system, or in closely related systems. Our interest is in the technique of cipher solution and in certain tests which can be applied to unknown ciphers. These tests are furnished the student gratis in so far as the formulation of the test and the clerical operations are concerned.

3. The interpretation of the tests we are leaving up to the student, as the purpose of the course is to teach him to think inductively - that is, from effect back to cause.

4. We are not giving all the tests which could be applied to unknown systems, because this might be misleading at this stage of the game and would be too lengthy a process. We are limiting you to the tests which should give indications of significance for the type of cipher in question. These tests could be profitably applied to any unknown cipher system even though the results would be negative in a large percentage of cases. Also, we are not carrying these tests as far as we could, or as far as might be necessary with a system which was unknown in fact rather than by supposition. We carry the tests far enough to cover the range in which a significant response can be expected and have dropped them shortly after this point in order to save ourselves unnecessary labor in preparing the assignment and paper for printing it.

5.

6. Students should realize that the cipher systems with which we are dealing are not important from a practical viewpoint but excellent for instructional purposes. Their security depends almost entirely upon the system itself being unknown; once the system is known the security vanishes. Our interest is in the tests of significance and technique of solution. The

cipher system is just a guinea pig. The biologist is not interested in the guinea pig but in the guinea pig's reaction to a specific treatment. The biologist performs an experiment on a guinea pig with the idea of applying it at a later date to animals of a higher order.

PAGE 3 NOT RELEASABLE

ERRATA -

ASSIGNMENT No. 3 - SECONDARY COURSE (Revised)

Correct as follows:

Page 5, line 2, change to read;

J J A R Z D U X F A I A I W J O C W N H U X B S O

Page 5, line 11 - 11th letter - Change Z to A

Page 6, line 18 - 21st letter - Change Q to W

Page 19, line 12 - 4th letter - Change X to Y

Page 19, line 20 - last letter -Change E to L

Page 30, line 24 - 11th letter - Change T to R

Page 30, line 21 - 22nd letter - Change U to T

Page 32, line 2 - 17th letter - Change H to J

PAGE 4 NOT RELEASABLE

ASSIGNMENT No. 3 - SECONDARY COURSE (REVISED)

PROBLEM No. 1

Serial No. 1

0030-0200 (June)

From: AB (Force Comdr. Blue)
To: XY (Collective call)
Info: IM (C-in-C,Blue), FG, HR, NZ (Type Comdrs.)

1 D O W C J C E V P X P T K N V Q Y Q Y M Z R R E H

2 J J A R Z D I X F A O A O W K P C W M J I X B S P

3 O M L P G U M U R Y S F I Z D G V Z Q Y M P P U N

4 R I K V Z Z Q Y L R Y Y P Q E V O O Y C E V P X P

5 X K Q V J A M M F N B O R F L D S W A D W S W J C

6 A S A X Z N H Y Q U M A U N U U N M Q H V A I D H

7 O I V Y P T W K X B K E P N J Q U H P C N N G O H

8 B E I B I Q H A Y M Z D W A N A O F Y F Q E R X F

9 Y S V Z R V Q U H A Y M Z D W S W J C A W A S L N

10 B V M E I E M X I J N P W W J P T W P D R E I A I

11 F X F C C V I Q D H Z E I V C W J N D H K Y L P Y

12 S D B M U A H A C T N V N R I L T O W O W K X K S

13 F J F N Y J K O R Z Q U W P T W L C Q S W A D L Y

14 B F U Y L O S F Y J H A O Q Q H Y W K E X J R J B

15 J X K K C U C I V Z C K X M N D D J A A P W P W N

16 R V X X P I W B P E I Z Z S A O B P G J N E X B O

PROBLEM No. 1

Serial No. 2

From: NZ (Type Comdr.)
To : QP (Unit Comdr.)
Info: ST (Unit Comdr.)

0001-0900 (July)

17 A C T N Q Y T Y M G X Q Q A E W P P I Q E R Z M R

18 F W I I B J X K X L H V X Z T I Q U X Y Q Y P J M

19 U P C K X B X E I V O V V O R Z U C U C Q D S J X

20 Z D H K C K X A E T X K N R E X I G G Z M U H L E

21 I M Z G A N Q H L O

Serial No. 3

From: AB (Force Comdr.)
To : ST (Unit Comdr.)
Info: NZ (Type Comdr.)

0001-1845

22 A A T G O B F Y C G T A U H K B F I X O C E I M P

23 X K N R G K X A E R K V T T G J L L C T R F Z S E

24 M E W E S F F X P X D Q U X F S H H Y Y E V V K R

25 K R I M Q S S K D R W K Z D U U N V J W K B E I Z

26 S W J I H

Collateral Information

Red and Blue maneuvers. No contacts have been made. Direction finder bearings taken on Serial No. 1 indicated that the transmitting vessel was in the vicinity of Hampton Roads. It is known that Blue has a force in this area, but it is not known whether or not this force has sailed. The principal theater of operations is the Caribbean - West Indies area. Direction finder bearings on Serial No. 3 showed the transmitting ship well to the southward of her earlier position.

Problem No. 1 - Overall frequency table:

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
32		23		27		12		30		27		24		20		26		20		24		31		26	
	17		20		20		21		25		14		23		27		24		15		25		34		23

Repetitions

Lines	Repetition	Interval	Factors
1,4	C E V P X P	89	Prime
5,13	S W A D	203	7.29
8,9	H A Y M Z D W	27	3.3.3
20,23	K X A E	50	2.5.5

013

PAGES 8 THROUGH 18 NOT RELEASABLE

ASSIGNMENT NO. 3 - SECONDARY COURSE (Revised)

PROBLEM No. 2

Serial No. 1

From: LM (Comdr Scouting Force). 0006-1000
To : PQ (Comdr Aircraft, Scouting Force).

1 A M Z T E C U A J O P J U B X O Z Y O Z I A R U T

2 G S M L Z W D R H E B O O L A K H Z D N D E K D S

3 F O X F E S J F O N J W P D V H Z R F Z V X R Q N

4 A H N K H P A H P I A C G Z V G A F J D X C N P Z

5 T D Z G A Z I P R E C B Z C T R I C D I A M T X H

6 T F C U J L Z D K P Z F Y Z J C F L L W T L W Y T

7 R L W R L Y B L C Q H K L D J X D G A K J A K H Q

8 B Y L S Y P R L S U I G I P J Y W P I W W O S F A

9 S F I T J T J D M P J M B J L B H F D X P H T P M

10 C I P Q P L N M L Q J Z B Y F Z C E L M U L R O L

11 X O K I J U Y V Y V F M Y E M K C Y I C K Y M W M

12 H W V X Q Q T I Q B N V J U V Z F U S W U W H L C

13 Y F V C S A V R A Z U Q L Z B G G B Z D B J N L L

14 Q F R Q W Q H U N M Q N H H X P H S C M S W S V V

15 V D Q P Y G L I L K E L H S F T Q W N K W Q F C U

16 O U C F F J E F J N E Z T R K V Z U A F R Z W G Z

17 F A N F I O N H E A H S Y K O R B W B K H R H M G

18 F V R Y S Q R S S W O K C W D V V R A R Q A Z E C

19 R S K G I U G P S R W V E W Q U F Z A A G P I G W

20 I G V O N U H Q U E

013

PROBLEM NO. 2 (Continued)

Serial No. 2

From: LM
To : PQ

0006-1200

21 B N A X C B X J Z Q J A S W A X C Q A Y U U L Y M

22 L C I I M E G M D K S E P J E B S R B J B S U H B

23 I D L I J X N K X Q H S Q D Q E K G R D Q R X E B

24 M A T P T G B C Z H T N O S P K J P Y D A J X I S

25 H Z D A V T T U H T R A U U V G I R A O R X E Q F

26 R Q I U O I O I H E T H S H N J D Q A A Q Z P S S

27 S Q X X B X S I S S M V X S U D X Z L X A K X T P

28 I T L T Y K N L B S F S S J R T S H C G C P S J L

29 S U T S R B K M B G

Collateral Information: Fleet maneuvers in the Caribbean - Scouting operations are still in progress.

Overall Frequency Table

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
34	26	20	23	29	24	21	19	31	41	27	31	22													
	26	23	28	32	23	33	21	26	31	26	22	24	32												

016

PAGES 21 THROUGH 31 NOT RELEASABLE

PROBLEM NO. 3 - SECONDARY COURSE - (Revised)

Serial No. 1

From: AB (Unit Comdr.)
To : CD (CinC)

1 X B S T G A M V E E J Q S A J R I R F U R J N V P

2 S J G N F T R U C D Z T I V G C H M E Q V M U V S

3 E E I Y F S K B M F G L Z N W V S U Q N K P Q W R

4 S Q J Z X V B C I L P P L X Q H I D V C I S P P J

5 T P N X W H

Serial No. 2

From: EF (Unit Comdr.)
To : CD (CinC)

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

7 R L B O D Q G M M V O E Q W R S M V O S T P I S G

8 G W M S O U Q G K M O G W N Z C B H Y C I M O D Q

9 M

Serial No. 3

From: XY (Force Comdr.)
To : GH, IJ

10 X B U J F W O U Q V R Q U A O Y P D R F N J Z O P

11 O F P R E N C H R A H G V Q U K J H W G I C H S F

12 T L Q W B T D D F G Q J O M H R R I R S D G X X O

13 N X T H A P R X C A Z G G P W X C A Z S B N W O M

14 G X W N H Z B E R F S G Y Z M C T N U G S N M F X

15 W N R O Y T D D M G N Z E Y C C Z N C O D W F R H

16 M P Q R Z X W V N V B Y Y D L K Q

Collateral Information: Fleet maneuvers in the Caribbean Area. Fleets in contact. Scouting operations still in progress.

Repetitions

X B S T G	Line 1			
X B S T G	" 6	0	0	
T D D	Line 12			
T D D	" 15	131	Prime	

Overall frequency table

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
8	15		9	20		11		7		19		15		17		14		10		16		10			
	11		13		12		12		11		6		17		15		20		13		15		14		13

PAGES 34 THROUGH 44 NOT RELEASABLE

[redacted]

Op-20-GR

NAVY DEPARTMENT
OFFICE OF CHIEF OF NAVAL OPERATIONS
WASHINGTON

ASSIGNMENT No.4 - (Revised)

- SECONDARY COURSE -

INTRODUCTION

The problems in this Assignment continue the instruction commenced in Assignment No.3. The same general type of system with modifications is being investigated.

On completion of this assignment a "post mortem" will be sent discussing and analyzing the problems covered in Assignments 3 and 4.

021

ASSIGNMENT No.4 - SECONDARY COURSE (Revised)

PROBLEM No. 1
Serial No.1

0030-0205

From: XY (Force Comdr.)
To : AB (Type Comdr.)

W T I Q C W L I C N O H Y R U N U Y C A O F O X C E B O E L

W N L I N D R Q I O T Z A I H F C Y X M Z K Y Q Y C F C G F

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

E N F Z U X C J V E O Z G Z T E D Z L U K Z C G Y N E A B O

E H W A U Z S O S U X R B B T Y A J O B S L G I Y E K Y S Q

I N S J Q

Collateral Information

Fleet maneuvers Caribbean. These messages intercepted by attacking Red forces. Contact not yet made, fleets not in striking or observing distance. Probable words: SUBMARINE, DIVISION, OPERATION, ORDER, BERMUDA, GUANTANAMO, CUBA, HAITI, SAMANA BAY, PORT AU PRINCE.

Serial No. 2

From: AB
To : CD (Div.Comdr.)
EF
GH

0030-0500

S C G P K W X F I D P I S L B S U V P Z O E V U X P O R A C

G Y N F U L E E O Q Y M P U M O R P K E D Z L U O Y O L C B

E N F Z U X C J V E O S C G Y N E U Z L K E O S Y O L B O A

Y E K Y S Q I N X C G Y N E A W K A E R R A F N F

Serial No. 3

From: AB
To : CO, EF, GH

0030-0530

Z O T K C W I T B E P P O R T S P H W A U Z S A R O K S U I

H T K K Y H T E M W S Z T U B P S O X W

OL2

PROBLEM No.1

Repetitions		Interval	
C G P K W X F P	Line 3		
C G P K W X F P	Line 7	56	2 x 2 x 2 x 7
Y M P U M	Line 3		
Y M P U M	Line 8	31	Prime
T M D Z L U	Line 3		
T M D Z L U	Line 4	28	2 x 2 x 7

		Interval	
Y O L C B E N F Z U X C J V E O	Line 3		
Y O L C B E N F Z U X C J V E O	Line 8	30	2 x 3 x 5
C G Y N E	Line 4		
C G Y N E	Line 7	83	Prime
C G Y N E	Line 9	70	2 x 5 x 7
H W A U Z S	Line 5		
H W A U Z S	Line 11	104	2 x 2 x 2 x 13
Y E K Y S Q I N	Line 5		
Y E K Y S Q I N	Line 10	54	2 x 3 x 3 x 3
L K E O	Line 8		
L K E O	Line 9	44	2 x 2 x 11
E D Z L U	Line 3		
E D Z L U	Line 8	28	2 x 2 x 7
E D Z L U	Line 4	56	2 x 2 x 2 x 7

Problem No. 1 - Overall frequency table:

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
12	11	17	5	23	8	9	6	12	4	14	13	6	15	20	14	10	9	17	11	19	6	11	10	21	17

PAGES 4 THROUGH 14 NOT RELEASABLE

ASSIGNMENT No.4 - SECONDARY COURSE (Revised)

PROBLEM No.2

Serial No.1 0003-1430 (Blue)

Scouting operations still in progress in Caribbean between Red and Blue.

1 F X I F J J D C F D W C P Z K X Z S F H D D U X H G X H E H F D U

2 U F J W H F I H C V N T V S E Z H D L J Z T S R C F P I F K J A M

3 T B U Y Q R C P V V R H T J A M T B U Y C R I I T O Q L P G X G I

4 H H U L F R C U E R A U M

Serial No.2 0003-1010 (Blue)

5 K T J D C F F Q D X L D D U X H C X H E J F H V A S D U E F J W H

6 F I H C V M T V S E Z H K L W Z C L D F K J A M I B O Y Y D C I H

7 U Y Q R C P V V R H T J A M T B U Y C R I J Z T N B G O Y G K I W

8 T W L E G J A Q W M Z S F

Serial No.3 0003-1600 (Blue)

9 O B H U C F I F K D C U T X E H F D U L F J W H F M Z Z S F D A Q

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

11 Y V H J X O B U Y C N I N T G A C W X X M S K U X E Y P T I N U V

12 J N

025

ASSIGNMENT NO.4 - SECONDARY COURSE (Revised)

PROBLEM No. 2

REPETITIONS		INTERVAL	FACTORS
J D C F P	Line 1		
J D C F P	Line 5	3	3
D U X H G X H E	Line 1		
D U X H G X H E	Line 5	9	3 x 3
E H F D U U F J W H P	Line 1		
E H F D U U F J W H P	Line 9	14	2 x 7
D F K J A M	Line 2		
D F K J A M	Line 6	9	3 x 3
D F K J A M	Line 10	16	2 x 2 x 4
V R H T J A M	Line 3		
V R H T J A M	Line 7	2	2
V R H T J A M	Line 10	17	Prime

OVERALL FREQUENCY TABLE

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
11	8	16	20	10	21	10	23	13	18	9	8	9	5	7	11	7	11	9	17	21	12	10	13	10	12

PAGES 17 THROUGH 27 NOT RELEASABLE

ASSIGNMENT No. 4 - SECONDARY COURSE (Revised)

PROBLEM No. 3

Tactical maneuvers between Red and Blue in Caribbean.
No contacts have been made.

From: EF (Force Comdr).
To : LL (Collective Call)

NAVAL COMMUNICE	COMMUNICE	NCE				
FQVLO	KVJBF	OEHCF	INCDP	XTKPD	MUZKE	TNKQQ
HSYOF	XFFZW	WEALX	CIDWH	EBFYH	VUKKU	CSKIW
ZRTPI	BCQLY	ZRGMJ	JHWED	XWEZS	LSYTL	TODZS
OBRKC	YXFDT	CRDUR	BXYMA	YRINO	MEDSC	BRLJC
PCFLC	DJTEN	GGSYC	SZJTF	PAEAT	DSZXI	TVXTR
SLSYT	LTODZ	SOBRS	KDOYE	DSCBR	LPQLC	QHTKL
CSNHP	CYBVE	KRKWU	WOIHJ	QMJIK	CFIJR	RYHPC
UBTXV	CFLRN	IYHCC	MHZFY	DIAFT	HXIXU	JSZPA
EACZS	GGODV	WGASO	TYOKR	TTNGC	LJDYR	QXYOC
XEILR	DTCBE	ZVHXG	WPATG	GBEDS	CBRRT	XIHDB
RGGSS	RIPUV	PQACN	PSSXB	SRECX	KSYOF	XFTRH
FHPCJ	DWHER	FYHVU	SFYPE	UJVSC	PHDIL	GQYGZ
KFTYP	IHJJH	WEZLY	LHWJV	JGLKJ	LZJCU	ZRXBG
ISVTU	PJGXR	HXNGQ	RZRRM	JEUBF	UFGVS	OBYAV
UJYAX	ZZAGP	NHVPS	EFUVX	XEQJN	FUICM	JCUVS
VCVXT	IAFZH	PFNXM	BIHFZ	SNWDK	SUIBP	LNWLC
SXXUH	PAEAX	BCVWN	XVIOT	HFVJK	XKHNH	PFMFF
FIQHZ	GGJFT	QRXWG	ISIFI	WKFES	PYYXS	EODDP

FREQUENCY TABLE

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
18	22	36	24	25	36	23	31	28	24	21	21	10	16	16	26	16	29	37	27	20	23	18

X	Y	Z
33	27	23

028

ASSIGNMENT No.4 - SECONDARY COURSE (Revised)

PROBLEM No.3 (Continued)

REPETITIONS		INTERVAL	FACTORS
D W H E B F Y H V U	Line 2		
D W H E B F Y H V U	Line 12	338	2 x 13 x 13
S L S Y T L T O D Z S O B R	Line 3		
S L S Y T L T O D Z S O B R	Line 6	81	3 x 3 x 3 x 3
E D S C B R L	Line 6		
E D S C B R L	Line 4	63	3 x 3 x 7
E D S C B R	Line 6		
E D S C B R	Line 10	143	11 x 13
S Y Q F X F F	Line 2		
S Y Q F X F F	Line 11	340	2 x 2 x 5 x 17
J J H W E	Line 3		
J J H W E	Line 13	343	7 x 7 x 7

PAGES 30 THROUGH 40 NOT RELEASABLE

ASSIGNMENT No.4 - SECONDARY COURSE (Revised)

PROBLEM No.4

Serial No.1

From: AB (Force Comdr).
To : CD (Type Comdr). 0029 - 0300

B I O I Q U N L L S K G F Z S D K D B F L M U X B S R J N S D R

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

R F U O K K Y D A P W S J C U Y Q F C H H U D C E C E H Y G N K

E Q B R R S O E F I U D Q F G V X U A L I S E L V W O V O U N L

I V F L O N L W V K C R H X S A R S K F C C Z Z

Serial No.2

From: CD
To : EF, GH, XY 0029 - 0500

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

Q I K E F T A F K H R C S F E I G Q S Z K F F D V K R C E H Y G

N K E C B R R J E I V K I S N E J M Y H M J H C T P N K I K H J

G Z T C M T C O G Z Q F R C C C Z Z

Serial No.3

From: CD
To : EF, GH, XY 0029 - 0600

F O U I R S A F B T H T K A G G X K U V J U N B K X T P G X K Y

B E Q K G F S L K V I Y G N F

OVERALL FREQUENCY TABLE

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
9	12	13	7	14	20	15	16	13	13	23	11	5	13	8	6	16	16	18	10	12	12	4	5	8	11

ASSIGNMENT No.4 - SECONDARY COURSE (Revised)

PROBLEM No.4 (Continued)

REPETITIONS		INTERVAL	FACTOR
G B J R	Line 2		
G B J R	Line 6	56	2 x 2 x 2 x 7
C E H Y G N K E Q B R R	Line 3		
C E H Y G N K E Q B R R	Line 7	30	2 x 3 x 5
C C Z Z	Line 5		
C C Z Z	Line 9	38	2 x 19
Q F	Line 3		
Q F	Line 4	28	2 x 2 x 7
U N	Line 4		
U N	Line 10	104	2 x 2 x 2 x 13
I K	Line 7		
I K	Line 8	59	Prime

COLLATERAL INFORMATION

Fleet maneuvers. Contact not yet made.

032

PAGES 43 THROUGH 53 NOT RELEASABLE

PUBLICATION
Op-20-GR

NAVY DEPARTMENT
OFFICE OF CHIEF OF NAVAL OPERATIONS
WASHINGTON

Original
Dec 1939

- SECONDARY COURSE -

- ASSIGNMENT No. 5 -

- INTRODUCTION -

In assignments No. 3 and 4 (revised) of the Secondary Course in Cryptanalysis, certain new methods of attacking cipher problems were introduced.

In this assignment various types of ciphers are presented wherein the student is given an opportunity to apply these tests. In each problem, all messages are in the same system.

One problem cannot be solved with the amount of text given. Each student is requested to make his analysis as far as he is able. The statement that one problem cannot be solved is made so that no student will spend 25 or 30 hours on a problem he cannot solve. On the other hand, the student must distinguish between the unsolvable problem and one he may spend an hour on, and consider it unworkable, when actually 3 or 4 hours work would lead to a solution.

As in the other revised assignments, clerical work has been provided up to statistical counts. It is evident by this time that inferences to be drawn by various statistics must be paralleled by overall frequency counts, repetitions, etc. In order to save paper and condense the assignments, only the summary sheet of tally counts for each problem is provided. If the student considers certain tally counts necessary, these sheets will be forwarded on request. The student is urged to make preliminary analysis of all problems before requesting any tally counts (if necessary) in order that he may ask for such tallies at one time while working in the remaining problems.

One new test has been introduced -- the coincidence test applied to the different messages of any one problem, reference Pamphlet No. 6, page No. 6.

034

ASSIGNMENT No. 5 -- SECONDARY COURSE

Problem No. 1

Serial No. 1

FROM: LN. 0012-0700 MAY.
TO : LK.

BARINGEIGHTZERO TRUE RANGETWENT
GTUARO BTRBYEKTA IEADTAU OBTEMTOE
YNINETHOUSANDFROMLATITUDEFIFTY
HORO TEYIDNUOSPAIWCUERE DSTPRPEH
TWOFORTYFOWRLONGHUNDRDSIXTYNN
ELIPIAEHPIDACIOBYDOSATSNRVEHIOO
FTHRTYESTIMATEDSPEDSIXPLUSTE
TEYRAEHTNERWUETSNETTSNRVFCDNETT
NCOURSENORTHLIGHTFORCSMOVINGT
OLIDANTOIAEYCRBYEPIALTNWIARUBE
OSTARBOARDBOWOFHEAYYCRUISSRSXC
INEUAGIUASGIMIPYTUXHLADRNTANVL
ARRILRSNCTINSIGHTNOW
UAARTANOIERONRBYEOIM

Serial No. 2

FROM: LK. 0012-1300 MAY.
TO : JD.

BEPRPAREDTOATTACKDCISIVLYTM
GTFATFUATSEIUEEULZSTLRNRLTCHEY
ROUGHOPENINGBETWEENTWORED
AIDBYIFTOROBGTEMTTOHMLATSGUEEC
CSNPGROUPSUSINGSMOREOVERMYIN
TNYRFBAIDFNDNROBNWIZTLIATAMHRU
TENTIONTODRAWSINGLEREDBBTOSOUT
ETOERIOEISAULNRCBCTATSGGEINIDE
HWARDOFMAINBODY
YMUASIPWUROGISH

Overall frequency table (Total letters 335)

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
28	11	7	12	35	7	9	9	31	0	2	7	8	20	24	8	0	24	14	36	16	3	6	4	12	2

335

PAGE 3 NOT RELEASABLE

ASSIGNMENT No. 5 -- SECONDARY COURSE

Problem No. 2.

Serial No. 1

FROM: XY 0007-0600 MARCH.
TO : AB

B O W T F O G N N I L N I S D D E B E V I T A L I T S I S N

O O N E E R C S S B E L I M O W T E Y D O B N I A M E R D A

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

P S E V I F L O C N I S D D L I M Y T H I H R U O C Y O V N

K Y T N E W T D T T S I D Y T N R U O F S T O N E B L E R N

K U Y T H G I E E S I D Y T F I F S B B Y M E N E M I M E N

I N T S O R F G N I R A S E L

Serial No. 2

FROM: CD. 0007-0900 MARCH.
TO : AB.

F O G N I T S I I S D D E E R H V I T A L E R D S N O C G N

I W R C S B B E N O E N O E N I L N D E H C A T E D A E H A

E L I M G N I R A E B E T Y B D E N E E Y T N E W T T S R U

O O Y O V N Y T N E W T D E I D E V I F D E L I M E E H H T

U O F E N O E S R H T E E R H T L P S E V I F R S T O N H O

W T O O M O R F S E

Overall frequency table (Total letters 355)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
11	12	10	18	53	13	7	9	31	0	2	11	11	31	26	2	0	21	24	29	6	7	8

X	Y	Z
0	13	0

037

PAGE 5 NOT RELEASABLE

ASSIGNMENT No. 5 -- SECONDARY COURSE

Problem No. 3

Serial No. 1

FROM: AB. 0001-1300
TO : CD.

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

Serial No. 2

FROM: CD. 0001-1400
TO : AB.

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

Serial No. 3

FROM: CD. 0002-0800
TO : AB.

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

039

ASSIGNMENT No. 5 -- SECONDARY COURSE

Problem No. 3 (Continued)

Collateral information

These messages were intercepted during fleet maneuvers in the Pacific. The messages themselves were not fixed in any way but are potentially actual messages.

Overall frequency table (Total letters 385)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
14	12	15	14	13	4	9	15	10	17	17	20	12	10	15	22	18	13	25	7	14

V	W	X	Y	Z
12	14	16	18	13

ASSIGNMENT No. 5 -- SECONDARY COURSE

Problem No. 4

Serial No. 1

FROM: GH (Force Comdr). 0006-0800 JULY.
TO : PD (Task Force Comdr).
INFO: AN (CinC), HN (Force Comdr), ZA (Task Group Comdr),
BS (Com-15).

P G N I L H R M D I A T N L M U C M C G G J A Y N I K E V V

X A Q I S J X G C O J L D M F B J G W B O G D R M J M R D K

O G O N X Z R Q I S G R K Q I A H P R T Q L B R T C D O S F

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

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

D Y N F T Y R J K O S B H J K M B W A H R Y J Y R U B L W B

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

Z H W R Y J Y R U G H K H N Z Y J M V C L H R M N X Q Z N G

R T P Y Z E O F C Q I Y P T G E P G C C P N A P G K L A K D

B T P S E F T G M J O B J G J O Y R C S E X Y O Y Y N F V W

F M G A J B T C W I A O G E U B L M U O X G E P G C Y N R T

G A O Y N F T Q W D Y J G J A O V C M P E Q U B A C J W F W

R A O S Y O C M J N Z A V M J N M H A K W B L X L A H R M G

V M E Z U C U W Q E D C B U U O F Y Q P N I B M P R C B F V

Q L G D P E E F A M P G E S E V I C Y L C S H B O B G A W B

D M P N X A I C A T D C B W I S G M L H R U J W A R D T I S

B X G Q C E V V X A V M G T B S

041

ASSIGNMENT No. 5 -- SECONDARY COURSE

Problem No. 4 (Continued)

Serial No. 2

FROM: GH (Force Comdr). 0006-1630 JULY.
TO : BS (Shore Activity).
INFO: AB (CinC), HN (Force Comdr).

SPER

Z J O S H B P Q N L C W I A P R J B O X G E Y P G A F B L H

I K X O Y M F B T I I B R T W B D I N H T V B R T G G C Q N

X K T H W B R Y J R U Z D I T N L H R U J A R D T I S J X

G C E V V X A V M G T B S P R J O S A O S Z X R Q C P Q R

O F K W C K K Q A O M R T G G I N Q Y N I U I E E N Z I U M

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

P L X R U E W D Y L P V C U B L C U W P L B R A H Q H B M

E A K K H T E N K K I U U O F Y Q W I A P R J A O O F K T H

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

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

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

W H K N R

Collateral information

Red and Blue Fleet Tactical Exercises in the Caribbean.

Overall frequency table (Total letters 831)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
41	47	39	24	30	23	44	31	37	32	26	26	42	30	37	35	26	44	25	33

U	V	W	X	Y	Z
26	26	33	31	30	13

042

PAGE 10 NOT RELEASABLE

Op-20-GR

RESTRICTED

NAVY DEPARTMENT
Office of Chief of Naval Operations
WASHINGTON

SECONDARY COURSE IN CRYPTANALYSIS

ASSIGNMENT No. 6

REMARKS

1. In this assignment as in assignment No. 5, various types of ciphers are presented in order that the student may continue the application of the tests introduced in Pamphlet No. 6.

2. One problem cannot be solved. The same remarks in regard to this problem as were made in the preceding assignment are again brought to the students' attention.

3. Clerical assistance on the various problems has been provided as far as was deemed necessary without giving away the system.

Problem No. 1

FROM: VD (FORCE COMDR). TO: WK (SHIPS). 132100 SEPTEMBER

1.	ZRBKB	YGSYU	JXGNI	KBGGP	XBDON	YQMXH	JZUUD	GWKMF	SKDRX	KGLTO
2.	JZHHB	PKTXT	HOWHW	DKXKP	WEDSY	RELGN	YBEAM	HVXMF	RUZQJ	KHBYJ
3.	POCHX	KRKNX	OMDTV	OBKPK	WBQIR	QQGTG	TISNJ	UWMPH	FUFHV	HTOGD
4.	QHCJD	BJVLW	XBKWJ	KLFAP	JDXHS	TFQFP	TYVJM	FWMDF	ZAGZB	NWBQB
5.	NMBZJ	FMAUW	OHOYK	EQLGF	ZJWOF	WZRGF	ZXHXX	YYQAP	DVPFX	DQXHZ
6.	KDOAK	EIVHZ	QBQJD	QKMJU	OATCZ	AFPFP	TYVIJ	DGVEM	EUQLO	DQVHX
7.	EHGXJ	MFUVH	JSGHB	LGZHP	IOFGV	GFUGK	XXONQ	PPSMF	WWKQX	KRIBO
8.	KMJJE	DKCNG	HXOEH	OFVEK	ZSGGA	UESGA	NIFED	GYCFV	QSYLY	CRHWC
9.	JFEYD	VSJZT	VJVBF	JHBFM	BZHBF	UQMDU	QBHXF	VUYQP	WVEHO	LOCGJ
10.	YQXJE	DMTHW	CHHWJ	ICLEJ	BJWCX	VLLYE	HROSE	MNGJZ	PTKBH	DDECJ
11.	DAHOB	NNVDW	ODXHK	ELEIG	EBKWQ	URBEM	HIQOH	AYQXK	DRJHF	BGOZJ
12.	BEUBF	DCPTU	WBQWJ	VOEGN	HBKWQ	URBEM	HIQWJ	RXJMR	VADTR	FWZHY
13.	DUBXL	EHCVH	HVTBO	EBPUP	DBDWP	SKSGS	OCEAO	DAWHH	QF	

Collateral Information:

Fleet maneuvers off the California Coast. The opposing fleets have not yet made contact; scouting operations are still in progress.

Ships present: TENNESSEE, COLORADO, TEXAS, WEST VIRGINIA, MARYLAND, NEW YORK, MISSISSIPPI, and CALIFORNIA.

61517

044

PAGE 2 NOT RELEASABLE

ASSIGNMENT No. 6

Collateral Information (Continued):

Prior information leads us to believe that this message deals with communication operating procedure; i.e., perhaps a radio frequency plan.

Problem No. 2 Serial No. 1

FROM: XY (SHIPS). TO: AB (CINC). 151000.

AVXLB FOPBQ PKCSA AVLBC SCLBK POFOX BBJOY DFBQL BBBOR EOM

Problem No. 2 Serial No. 2

FROM: AB (CINC). TO: CD (FORCE COMDR). 151030.

QQOKQ FOAHF YLVBL TPKBB XELOX QLBJI QEBLP KYPKX QXLSB QMQ

Problem No. 2 Serial No. 3

FROM: XY (SHIPS). TO: AB (CINC). 151100.

EDEDO EWOQT OEZQF LZKDK RLBLB AKZAB KOXFF XLLKC ABLQB PBBFX QFBBF

OSPBB PBKQJ ULCSA BBFBW OBELE BUOBB XBWCI QESKA DFZRZ KOULQ DOBXV

KKBBU YKKRK JAFLP WLKLF LFL

Collateral Information:

Overall Frequency Table:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
9	40	6	6	9	16	-	1	2	4	20	25	2	-	18	10	17	4	6	2	4	4	4	11	4	5

ASSIGNMENT No. 6

Collateral Information (Continued):

Fleet Maneuvers. Fleets in contact.

Problem No. 3 Serial No. 1

FROM: AB (CINC). TO: CD (FORCE COMDR).

0012 EJSTX RDRDC GYMHQ OCYGP TVBGP PGBDG IVTPA ZFXHF YGZAO EPBXX
IWDPH OMNAR YICHZ TJPIN FTFGZ ADZAV RJNVO UJSZJ ROSTB DPYDU JHAFF
WCLDC ZRKCA GGYDV FMLDH HZUNI GTOIN XWVZA MDFQJ EUTNH RQNJC HAUMD
ABIHA ZMFGN HGOOQ YEOOP MCGQG VOPNO FRCOJ AJESS TPBRQ WNATK LCWFB
WWXGY MMUQM DHDLI MMAUH UZSCM 0730

Problem No. 3 Serial No. 2

FROM: AB (CINC). TO: GH (FORCE COMDR).

0012 IHUBC ZAHJJ QBPXP WMCPR UGSNL WJWVI OKJMM JSTXB KWNGN VHHBH
DXAKE BKUDF FAMJC XLXLT YWLYL BCLML ZPQTR CMOBA LJBAD THAWI VKHNY

ASSIGNMENT No. 6

Problem No. 3 Serial No. 2 (Continued)

DNFKI XOAMT EHZZU YUEPS QAGLW CCITJ PIRNT PQJKH DGARS XVSTS JYKBH

RFAXL MIIPM MELWB DYARD SLEAD INGXX THREE LASEI KNKVN DFNEX VZLQJ

QVWOI SUOZN YUPUV KWKBX DAKWP 0830

Problem No. 3 Serial No. 3

FROM: AB (CINC). TO: EF (FORCE COMDR).

0012 GLMYS XYCKI IFSJN IFZOQ FEFYG NHKEM VBBBC XJKJE SHPPM DSKLA

FSHIK EQDKA HNSZK WXWRR MAESV CBQNX XXUZP ZUENL YJAGF USWPW UMPFA

GZMQL DXZQM NVNHX HBBKD ZDDQR ANJEL WAQKS VTTMN UPVMM SPUBH WJDXB

MSZJT ARJOT LPIPO MDBAY DHAOX AXSIH QBDCG XUBMD LXFOT CDKGT MIRAT

LIAXK NEXXB HQOTX UGOWZ CNAHO 0700

Collateral Information:

Fleet maneuvers in the Pacific. Contact has been made.

Overall Frequency Table: Total of 720 letters.

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
43	30	24	35	23	23	28	35	26	29	26	25	36	33	26	31	22	21	28	27	24	20	26	33	20	26

048

ASSIGNMENT No. 6

Problem No. 4

FROM: AB (TASK COMDR). TO: CD (COLLECTIVE CALL). 170200

HFIGT UCKCT CSUYI HTWYX YSCJR UKTLL IBVJP NBAMV BGRRC UWWOO DKLJW

GEGVV SYCOT UTOQD GKOZA DZRDS UYIHD BAGHW DKBFS WIHUY WBUGG XKHFK

VAUGG PYHMU VJTXY XYSCJ RUKTL LIBVJ PNMFO PIFEG HGOKS UIRIJ IZVDZ

GUTFF FVTAC KXJON BRCJR UKTLF OPDFP PFZIK EJPMD RABRP UWMUR PIKYC

DSFZE HKKDG MLIGU TGPYH MUIXS LMPOM IGWSX JSSYB UTGPV JZGTS YBGPA

TTHYH VJVYO OFVGK WSXJX XTXPM LKQYH YTUBK HDCSB RDSOL HHMPP O1BTS

NZQJO SVJBU LJPOT GLTTQ ZGRUZ GAFCJ PMDRU PYHOM GKDMC OYCVY TXCJP

MOMYE TXTBD ATXVJ YN

Collateral Information:

Fleet maneuvers. Fleets not in contact.

Overall Frequency Table Total of 402 letters.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
9	16	15	16	5	14	25	18	16	20	19	12	16	5	19	21	4	14	17	26	23	16	10	15	22	9

ASSIGNMENT No. 6

Problem No. 5 Serial No. 1

FROM: XY (SHIP). TO: AB (FORCE COMDR). 011000 JULY.

HEUUN TFOCG UBHPT HVOAF UTHGL JNCDU

Problem No. 5 Serial No. 2

FROM: XY (SHIP). TO: AB (FORCE COMDR). 021000 JULY.

PPPJE GFOQN FTHCM UCITN RAGXE HGDNI WHACG RCKOQ

Problem No. 5 Serial No. 3

FROM: AB (FORCE COMDR). TO: OP (CINC). 021400 JULY

JQRFM PEUWO GUAYE UBCPE HOOED UJBTY WWOFR UPPVO WTHPF UPDAI CJPGP PYHGT WBUFP

WGWES UOHQD JVLFG LCAGO ARWCF BZHTE NCOOP JTWQN GGBUP PCKHY TNPTE JTKAR TPHBG

QAWCI MECGE GVWFA WTWAA PEWNK

Problem No. 5 Serial No. 4

FROM: AB (FORCE COMDR). TO: OP (CINC). 021600 JULY.

KCFWE HVWAM ICONN PGDXE GVEEG PSGFM AFUJC GOLFU KJPSS QUEVH QXDLU FSMHZ

Collateral Information:
Fleet maneuvers in the Eastern Pacific. A scouting force has been sent to observe the movements of merchant ships off the East Indian Islands. Locality of operations Latitude 7 North Longitude 114 East.

Overall Frequency Table: Total of 285 letters. Overall IC = 1.24

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
14	7	18	7	18	16	22	17	5	9	6	5	6	11	14	23	9	6	5	15	19	7	17	3	4	2

050

ASSIGNMENTS 7 AND 8 NOT AVAILABLE FOR REVIEW

ASSIGNMENT 9 NOT RELEASABLE

ASSIGNMENT 10 NOT AVAILABLE FOR REVIEW

ASSIGNMENT 11 NOT RELEASABLE

Op-20-GR
October 1940.

NAVY DEPARTMENT
Office of Chief of Naval Operations
WASHINGTON

RESTRICTED

****

SECONDARY COURSE IN CRYPTANALYSIS

ASSIGNMENT No. 12

****

00000
000
0

- SECONDARY COURSE IN CRYPTANALYSIS -

1. The type of problem dealt with in this assignment is called "Open Code", which is defined as a code or cipher that either appears to be innocent and harmless or else appears to be extremely vague and ambiguous. There are nearly as many systems of this nature as there are individuals using them. Open code has no place as a regular system in a military communication organization and is suitable only for use between individuals. Various types have long been favorites with those engaged in espionage and those trying to send information in censored mail. For such purposes, the more innocent appearing the cipher is, the better. Open Code is given in this assignment to familiarize the student with some of the more common types of cipher in this category. In many cases, problems can more accurately be considered puzzles rather than cryptograms.

2. A very common system is one in which frequently used words are substituted for other words which are closely associated with the subject matter that the correspondents expect to discuss. For example, "I have" might mean "New York", "I had" = "San Pedro", "of course" = "submarine". When cleverly used it is practically impossible to distinguish such a code message from other straight-forward communications which discuss the doings of genuine people in a natural way. Even if suspected, the system is hard to break and much more text is needed than is usually available. The futility of most "Open Codes" should be evident from the fact that paraphrasing by the censor completely destroys the hidden message.

3. Other common types are given with a brief word of explanation concerning them. One of the most common systems is one in which normal and innocent language is used and the hidden message is revealed by reading every N th letter or every N th word, or the first and last letters of words. The variations that have been employed are practically limitless. Another method is one in which the hidden letters or words are thickened slightly, as though the writer were having difficulties with a poor pen. Sometimes the hidden text is indicated by small dashes, misplaced commas, false punctuation, or breaks in a word. False punctuation may be employed to disguise short hand. The use of a grille is an old favorite, employing words instead of letters. In this type, the text doesn't make sense, and, ofcourse, would not pass any censorship. Numeral ciphers are often employed disguised as legitimate business accounts or a jumble of figures on what had seemingly been used as a scratch pad.

4. The types mentioned are the most common of a large number of such systems. The problems given herein should offer no real difficulty to the student at this stage of training. In all cases, there is believed to be sufficient text and collateral information to permit solution.

056

5. There is one classic open code system invented by Sir Francis Bacon. By the various combinations of upper and lower case letters, taken by groups of five, he was able to disguise a hidden meaning to certain of his writings beneath what appeared to be poor typesetting. Still another system is one in which a few letters of the alphabet are used to encipher the hidden message and all other letters of the alphabet are used as nulls. The message is first enciphered using the effective cipher letters and the nulls are inserted where they fit to produce words and sentences. As in other types, paraphrasing obliterates the hidden text.

RESTRICTED

- ASSIGNMENT No. 1 -

PROBLEM No. 1

The following letter might have escaped detection had not the addressee been under suspicion:

Dear John:

Yesterday I shot two ducks among a thousand I saw feeding. Tons of birds, plenty of time, lots of ammunition, but no luck!

I'm leaving here Sunday for New York. Please meet me at the Carleton about midnight that night or Monday morning at ten.

Sincerely,

PROBLEM No.2

The following two messages were intercepted simultaneously on two different frequencies. The calls, headings, etc., were heard just previously on a third frequency:

Serial 1 -

PRILY OFRER PRETR FETON TSAON

NOEGT ETISI NNNWQ

Serial 2 -

ATALC NIIDE OTIIE LEGIG OEMRI

GFIHE NHISO UKONP

053

PROBLEM No. 3

The following letter from a prisoner of war caught the censor's eye:

2 July 1917

My dear Sally

Last week's letters may not go through as they exceeded regulations. We are now out of quarantine and two other officers have joined us in the same house, making a party of five including Yeats-Brown and Stone - both old residents of the camp and very good fellows. We are busy making ourselves as comfortable as possible. Anything except very primitive furniture is out of the question. Have met only a few of the other prisoners whose story of capture are most interesting and thrilling.

About that other matter we discussed you may think I have broken my word but if you read my letter right I am sure you will see it from this point of view. I don't want you and John feeling downhearted.

059

PROBLEM No. 3 - (Cont'd)

Write a Line to Frank R. H. Root of H.M.S. Colossus telling him I received his letter of May 4th & that I cannot reply this after a week's time. Inform Dorothy you have received This and to write me a Line in turn -

Love to all

H -

PROBLEM No. 4

The following mass of figures appeared in a letter which otherwise seemed innocent. The numerals, however, did not seem to have any bearing on the rest of the letter, and were written carelessly on the back of one sheet, as though the sheet had been used previously as a scratch pat:

35	12	25	23	28
25	35	16	15	15
31	47	41	34	26
91			19	25
	31	20	13	28
11	24	31	25	30
28	19	29	129	152
15	30	30		
54	15	19	30	30
	14	13	18	25
31	133	15	15	55
24		157	24	
14	29		13	23
15	30	26	15	19
28	11	28	115	22
112	30	25		22
	15	13	12	15
25	29	15	31	28
12	144	15	15	129
29		14	24	
15	14	136	25	
28	15		29	
32	26	30	136	
11	11	25		
30	28	55	11	
19	30		19	
25	23		28	
24	15		15	
250	24		29	
	30		102	
	216			

060

RESTRICTED

PROBLEM No. 5

The following letter was found among the effects of a person suspected of being engaged in espionage:

BUILD NEW NO LEAKS STOP UNABLE

SYSTEM DEFINITE WHICH NEWS WILL EXPLAIN

PRESENT PLANS USUAL REQUIRE FAILURE ABOUT

STOP SOURCES THINK AND TWO NO

LONGER NEW NEED CONTACTS FUNDS MUST

ABLE TO MONTHS TO BE MADE

PROBLEM No. 6

The following is one of the so-called Scotch telegrams (Scotch-o-grams) which appeared in Judge:

THOMAS INJURED ERASED AFFORD ERECTED

ANALYSIS HURT TOO INFECTIOUS DEAD

RESTRICTED

- PROBLEM No. 7 -

Dearest Mother:

Have you heard whether you will be allowed to travel this summer or have you made up your mind to wait until after the war? I hope that you have. It may be hot at home but at least there you aren't running the risk of being torpedoed some dark night.

Speaking of heat, I am getting very tired of sitting at a desk in the office and I am very anxious to get a job at sea again. By the way, I saw Jack North last Sunday. He is home on leave looking very fit and refreshingly optimistic.

I'll let you know by Sunday when I can be home again for a few days. XX

With love,
Harry.

- PROBLEM No. 8 -

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

SERIAL 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.

SERIAL 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.

SERIAL No. 3

Mother sends love and waits each letter as she always does so write as many as Tom and Eloise do to her As always, Jerry.

TRAINING PAMPHLET NO. 7 NOT RELEASABLE