Op-20-GR

RESTRICTED

NAVY DEPARTMENT
Office of Chief of Naval Operations
WASHINGTON.

ELEMENTARY COURSE IN CRYPTANALYSIS

ASSIGNMENT No. 9

GRILLE TRANSPOSITION CIPHERS

1. Cryptographic grilles resemble ordinary stencils in that they are sheets of a thin material in which perforations have been cut for the purpose of uncovering desired parts of the object upon which they have been superimposed. Cross-section paper is the most convenient material of which to make a model grille and for use as the under sheet, because when cells are cut from the paper grille the perforations will disclose like cells of the under sheet, and letters of the message may be inscribed through these apertures.

2. In the simplest type of grille, the apertures are cut in prearranged locations, the grille is superimposed upon the cross-section paper in a prearranged position, and the letters of the message are inscribed by following a prearranged route. The cipher text is then transcribed; the letters being taken by following any agreed-upon route which is perpendicular to the route of inscription. There are eight positions in which a rectangular grille may be used; obverse or reverse surface up, and with one of four sides placed at the top for each of these surfaces.

3. Another type called a revolving grille may be prepared by perforating a square sheet of cross-section paper in an apparently irregular fashion, but the apertures are so distributed that when the grille is turned four times successively about its center in 90 degree steps, all the cells of the under sheet will have been exposed for inscription. (See illustration No. 1, page 3).

4. To decipher a cryptogram in a grille system the enciphering process is reversed. Obviously, the decipherer must possess an identically constructed grille, must have a prearranged knowledge of the successive positions of the grille, and must know the routes of inscription and transcription for the letters of the message.

5. When the total number of letters in the message is greater or less than the capacity of the grille, various methods may be arranged for striking out certain cells of the under sheet, or for combining the positions of the grille to form a larger figure before transcription from the under sheet. A revolving square grille may have an odd number of cells per side, in which case the center cell is not perforated. Also, the procedure in inscribing and transcribing may be reversed so that enciphering by one method is the same as deciphering by the other.

SOLUTION OF A GRILLE CIPHER

6. It will be assumed that the conclusion has been reached that the following message may have been enciphered by means of a revolving square grille:

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

7. A study of the grille positions shown in paragraph 2 will show that after 180 degrees of turning, the apertures of the grille will be occupying positions which are reciprocals of their former positions. Therefore, if the cryptogram be written on one line, and below it the same cryptogram is written in the reversed order of letters, then letters occupying reciprocal positions in the square will be lined up vertically. The above problem written in this manner, with numbers assigned, appears as follows:

ASSIGNMENT No. 9

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
A	R	U	D	U	C	S	C	I	M	W	E	T	T	R	N	N	G
L	I	E	I	O	F	H	N	E	J	M	L	E	I	M	T	O	O

19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
O	O	T	M	I	E	L	M	J	E	N	H	F	O	I	E	I	L
G	N	N	R	T	T	E	W	M	I	C	S	C	U	D	U	R	A

Each anagram formed with letters on one of these lines corresponds with the reversal of other plain text formed on the other line. The range of building plain text is very limited and many trials may be necessary before a correct one is found. Due to the structure of a revolving grille, the letters of a good word will occur in the cipher text in a uniform direction, fairly close together. This is a characteristic indication of this type of cipher when confirmed by words showing up in the reverse direction underneath.

8. The partial recovery of the plain text by anagramming might proceed as follows: (only correct trials are shown)

34	17		22	34	17		22	34	17	6		25	8	32	10	22	34	17	6	24
E	N		M	E	N		M	E	N	C		L	C	O	M	M	E	N	C	E
U	O		R	U	O		R	U	O	F		E	N	U	J	R	U	O	F	T

As each column is used for the anagramming process it should be checked to prevent using it again. The plain text of this problem will break on one of the lines, after nine letters have been placed, because the grille used was of that capacity.

9. When one fourth of the total number of letters in the cipher text have been anagrammed without a break in the plain text on either line, the letters which were originally inscribed in reciprocal positions of the grille have been found. The grille used in this problem may be reconstructed by numbering the cells of a square of cross-section paper (6 by 6) in the normal manner of writing and then cutting out the cells numbered according to the series found - 28-8-32-10-22-34-17-6-24.

REMARKS ON TRANSPOSITION CIPHERS

10. The transposition methods which have been described in their applications to single letters may be used for pairs of letters, sets of three or more letters, or as secondary steps after a substitution process has been completed. Since the solution of most transposition ciphers is accomplished by some form of the anagramming process, less space is devoted to transposition methods in this Course, than the more varied solutions to substitution processes. The cryptanalyst must depend on a wide technical experience to succeed with anagrams, and must use his own ingenuity to reconstruct a transposition system.

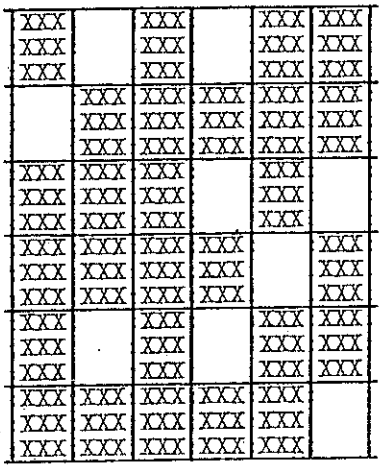
11. Transposition methods vary greatly in cryptographic security; some have practically no security, while others have a very high degree. As a general rule, transposition systems have advantages of speed and simplicity over substitution systems, however, transposition ciphers have several serious disadvantages in practical usage. First, they do not allow sufficient latitude for the occurrence of errors in handling. Many transposition messages would be completely unintelligible to the average cryptographic clerk if a single letter were omitted. Also, two or more cryptograms in the same key which contain exactly the same number of letters may be solved, the key recovered, and all other messages in that key deciphered. Finally, when the degree of security depends on a double process, a poorly trained or careless cryptographic clerk may fail to perform both steps correctly.

ASSIGNMENT No. 9

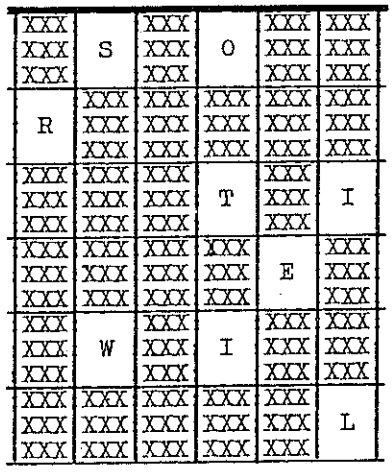
Illustration No.1

Message: SORTIE WILL COMMENCE AT MIDNIGHT FOUR JUNE.

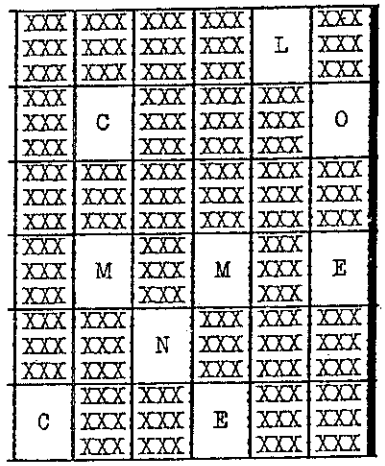
Grille:



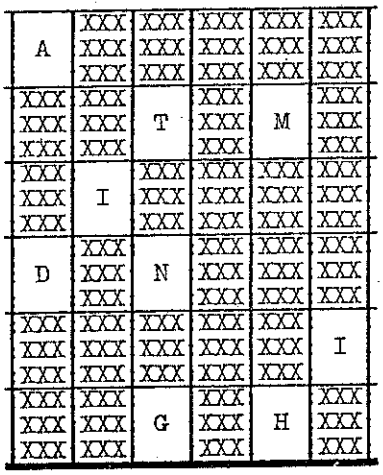
1st Position:



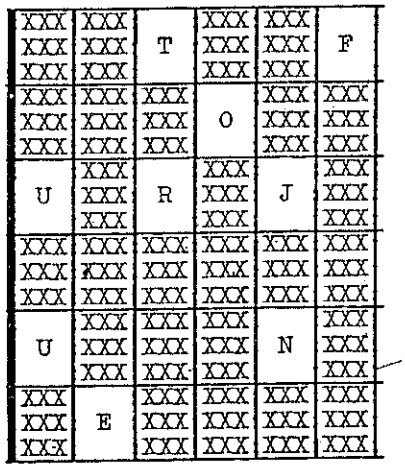
2nd Position:



3rd Position:



4th Position:



Complete Inscription:

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

The letters may now be transcribed by any of the simple routes to form the cryptogram. For example: ASTOL FRCTO MOUIR TJIDM NMEEU WNINI CEGEH L.

...

Problem No. 1 Serial No. 1 Naval Text

SDYUH ENRIT AOENR MELRA OPIED NANTD GRAIT RFIOH ELNFS WIIEN

NHGCA CURLO FOTR

Problem No. 1 Serial No. 2 Naval Text

ATMUF HEEAS VUTNL DLEEI SRNDF GESOR EPFOL OMFRS ITITI NHCSE

RPREO ECROO TQMF

ASSIGNMENT No. 9

Problem No. 2 — Naval Text

GOAUR UIDRT ELEEI EIGFO UOGHN HARTT SEENV CEREN HUUNE ASDIT

SENER RTRUU ESLFY EBDRS COIEO AMURG HTFRE LDISE EENGX FTTXH

Problem No. 3 Serial No. 1 — Naval Text

MBAAT ETNNH GRAET EIOTG LSEUE SNDBE FSMHI AIVID PREES ODIDE

NTPEE SSCLC TRIRO NEYOT EOYNE ENNCO RNNOE USSSF ERODR EISSE

Problem No. 3 Serial No. 2 — Naval Text

EOENO AEPIN PGAEG OHRCR RTUZE IGNEE HTRSY OLPEY RSOOS NIPTG

EDHEW DOETT OWTNE AEDCC HIOEN UNTPY RFDOD SUSTE YIOIN XVTEI

Problem No. 4 — Non-Naval Text

PTIIN CDIFN UERFE OSRDS PUOMS EPCRE TALTA CTIOO TRNLE IMRSE

TSBEA WCAAR ESINV PDSAE YDRRO SETYC OEBEO PUDAE TIRWE AONTG

CMOHE WXZFN IDCTO CERPS OHLEE TCOID TSUFY JATTO HUSS

Problem No. 5 Serial No. 1

From: AB (Force Comdr.) 0018-0615
To: CD (CinC)

UIORE EECHR TILGE ESCNE HUEVP SGCRA OTROZ ERRET PYARN DOIFO

GOSON

Problem No. 5 Serial No. 2

From: AB (Force Comdr.) 0018-0625
To: CD (CinC)

UNCRE EEDUR RILAS ESAGE DOOVP ROCRC OTHTZ WRREE PYAUT DOFFO

EOSOH

Problem No. 5 Serial No. 3

From: AB (Force Comdr.) 0018-0642
To: CD (CinC)

EFBEK SSEOC SNGRI TIOAV NEZIU RRAMS AAEGE OMTRN AHNAW ITEIB

CNTGU

Double columnar transposition. Fleets are in contact.

It is important that the Student's full name and present address appear on all work sheets and correspondence. Course material will be returned only in the penalty envelopes provided for that purpose.

B L A N K

NAVY DEPARTMENT
Office of Chief of Naval Operations
WASHINGTON.

ELEMENTARY COURSE IN CRYPTANALYSIS

ASSIGNMENT No. 10

POLYGRAPHIC SUBSTITUTION

1. In all the methods of substitution previously described in this Course, single letters of the plain text were treated to a certain enciphering process. These are called monographic substitution methods, and include the systems employing more than one letter or figure as the cipher value for a single plain text letter. In polygraphic substitution, however, combinations of plain text letters, considered as indivisible units, are used as the basis for determining the cipher equivalents of these units.

2. In true polygraphic substitution, all the letters of the plain text unit must enter into the determination of each of the characters used in its cipher group equivalent. For example, in a certain digraphic system ER plain may be enciphered as KS, and ED plain as CN cipher; a difference in the identity of but one of the plain text letters producing a difference in the identity of both letters of the cipher pair. Some cipher systems are polygraphic in nature, that is, the plain text is divided into definite units before the enciphering process is applied, yet these systems may be reduced to combinations of monoalphabetic and polyalphabetic substitution. For example, in a certain false digraphic system ON plain may be enciphered as EB, and IN plain as QB cipher; a difference in the identity of one of the plain text letters producing a difference in the identity of but one letter of the cipher pair.

3. The purpose of polygraphic substitution systems is the suppression or elimination of the frequency characteristics of the individual plain language letters. Theoretically, the larger the unit of plain text used as the basis for encipherment, the greater will be the security of the polygraphic system. Practical considerations prohibit the handling of units greater than three letters when speed and ease of operation are desired.

DIGRAPHIC SUBSTITUTION SYSTEMS

4. A simple method of effecting digraphic substitution is illustrated by the table below. It is employed on the coordinate system, the first letter of the plain text pair being found in the left hand column, and the second letter of the plain text pair in the top row. The cipher pair is then found at the intersection of the row and column thus indicated. Only a part of the table is shown:

	A	B	C	D	E	F	G	H	I	J	etc.
A :	DS	LL	FN	WH	MD	IM	JY	LI	RK	MF	
B :	KO	RF	YM	SS	CA	UP	HP	SM	DN	TW	
C :	HK	HA	DT	FQ	GM	YR	KK	GH	NY	ZZ	
D :	EW	GV	QM	EH	JB	QS	UN	WW	XV	FA	
E :	ZT	WT	OP	CN	DA	OA	SR	LG	MJ	CO	

To encipher the word CABBAGE by the system shown, the word is first separated into digraphs (a null is added at the end of a message when necessary to complete the last plain text unit); CA BB AG EJ. The cipher equivalent for these digraphs are HK RF JY CO.

5. The cipher equivalents in the table above are placed at random. Such polygraphic substitution systems are relatively secure against solution, but require that both an enciphering and a deciphering table be constructed in advance. A random selection of cipher equivalents can be employed in a single table by

making it reciprocal in nature; that is, in a certain system ND plain may be enciphered as CY and CY plain as ND cipher. The latter system would be less secure than the purely random type.

6. A still less secure system which produces a false polygraphic substitution, may be constructed by means of keyword sequences. The advantage of this type is the ease with which changes can be made in the key. A false digraphic substitution system may use the conventional type of square table with additional sequences placed as shown below:

1st Letter		2nd Letter	
Plain	Cipher	A B C D E F G H I J etc - Plain	
A	U	R E G U L A T I O N . .	
B	N	E G U L A T I O N B . . .	
C	I	G U L A T I O N B C . . .	Cipher
D	F	U L A T I O N B C D . . .	
E	O	L A T I O N B C D F . .	
F	R	A T I O N B C D F H .	
G	M	T I O N B C D F H .	
H	A	I O N B C D F H .	
I	B	O N B C D F H	etc.
etc	etc		

The message BEACH DEAD AHEAD would be enciphered thus:

BE AC HD EA DA HE AD
NA UG AB OL FU AC UU

7. The results of encipherment by means of square tables of the Vigenere type may always be duplicated by the use of sliding strips. To correspond with the system illustrated in paragraph 6, the sliding strips would be lined up as follows in enciphering the digraphs BE and AC:

Plain letters--(1st) A B C D E F G H I J etc. Fixed
(2nd) A B C D E F G H I J K L M N etc. Movable
Cipher letters-(1st) U N I F O R M A B C etc. Fixed
(2nd) R E G U L A T I O N B C D F etc. Movable

Plain letters--(1st) A B C D E F G H I J K L etc. Fixed
(2nd) A B C D E F G H I J K L M N etc. Movable
Cipher letters-(1st) U N I F O R M A B C D E etc. Fixed
(2nd) R E G U L A T I O N B C D F etc. Movable

Both movable strips are fastened to the same slide, which is placed so that the second letter of the plain digraph to be enciphered falls under "A" of the first plain sequence. This automatically lines up the second letter of the cipher pair, which pair is found below the first letter of the plain text digraph.

SOLUTION OF DIGRAPHIC SUBSTITUTION CIPHERS

8. The solution of digraphic substitution ciphers does not depend upon the frequency characteristics of single letters, but rests chiefly upon the possibility of analysis on the basis of the frequencies of pairs of plain text letters. Digraphic frequencies are difficult to use because of the indefinite or varying significance of the data available. In the first place, there are 676 different units to be considered (the permutations of the 26 letters taken two at a time) instead of merely the 26 letters. Also, data corresponding with the classification of vowels and consonants can not be employed.

9. There is an even chance that, after encipherment, repeated plain text digraphs will result in the same different cipher digraphs. Therefore, the normal frequency of a plain text digraph is about twice its normal expectancy for

for repetition in a digraphic substitution cipher, and may be considerably more at variance from the normal in short amounts of text. When "known words" may be assumed in solving a certain message, such words as SEVENTEEN, CONDITION, AS SOON AS, and JOIN MAIN BODY, may be placed by locating repeated digraphs.

10. False digraphic substitution systems are usually recognized after a study of the frequency tables for each of the letters of the cipher pairs, and the principles employed in solving monoalphabetic and polyalphabetic substitution used in their solution.

Problem No. 1 Serial No. 1

FROM: GR (CINC BLACK) 0017-1645
TO : OK (FORCE COMMANDER BLACK) April 17, 1940

TO MZ LJ CC HR SG LZ QJ HX KD UQ LO QD BD HA QD SW IH FD WZ

FD BH CC HR YS LV IE QD GY SJ XD IC EZ LW

Problem No. 1 Serial No. 2

FROM: LM (FORCE COMMANDER BLACK) 0017-1640
TO : GR (CINC BLACK) April 17, 1940

LJ IV YJ XD AU IU KS LJ LC OF DR US IV UD JD WV LY DX PE CC

LS JX IB MH MO ZC KD OA RR MZ IH BV XV LQ KC YJ IV MD SE MD

RT MH IJ HG SW IH HG JX IB MH MO EG BJ HX IC CJ BJ QR AX KD

LX ZZ SE XA AC RR ND QJ BX TC OC FD DX AC KC DX EC

Problem No. 1 Serial No. 3

FROM: LM (FORCE COMMANDER BLACK) 0017-1635
TO : GR (CINC BLACK) April 17, 1940
INFO: XH, PV (SHIPS)

DC UD WZ DD MD FE WW WD FJ EZ VV OJ BL NE IH FD PV FG HX WG

LD UV KR EZ VV OJ UX SV LY HC QD KC SE GY UG LD DR JL

Problem No. 1 Serial No. 4

FROM: LM (FORCE COMMANDER BLACK) 0017-1630
TO : AY, TW (SHIPS) April 17, 1940
INFO: GR (CINC BLACK)

EZ RQ XD ZV RR LO KH DD EJ NS LJ ZV PQ MD BV BH DX QX MH OC

MH JX BS LJ TC NW GY SJ OV IE QD KH JO UV SO MZ HX ER EQ LJ

ZZ RX EJ MH YD AG ZC QD AG EZ VQ BV VC OW QJ DJ KC OF RU WV

LY DX IC RR LJ LC OF IU TX FG NB JD

Problem No. 1 Serial No. 5

FROM: GR (CINC BLACK) 0017-2110
TO : AB (COLLECTIVE CALL) April 17, 1940

OC MH JX BS LC GD DO XD HJ JV FJ XD VO HV EJ IV UD LJ TD WX

JM ME DH PZ DR OV IE QD KH JO UV SO MZ HX PZ QD QJ NE IH FD

ASSIGNMENT No. 10

RX ZZ HD DX TD WX SE MD TN MZ GC AN MZ EG WL SE UZ KS LD UV

KR ZC LY JD VD OJ BB LV UE IH BV OA IT KZ MH LO LJ WX ZC HR

YS LV IE LC RR OC MH LC FQ IV IE QD NG MH MD TR MH HG DO MZ

HX TC UZ XI PC PZ BH EX LD KC QD LJ ZV PQ MD BV BH GD LO MH

BK SG PC MQ BH LC MJ

Problem No. 1 Collateral Information

Messages are in the "work sheet" form and the student is given the benefit of the preliminary analysis. The numerous long repetitions, all occurring on the "even beat", indicate that some sort of digraphic substitution cipher has been employed. Reconstruct the cipher.

Fleet maneuvers in the Caribbean Sea. Scouting operations are still in progress. A few isolated contacts have been made. Probable composition of Enemy Fleet:

Battleships	Cruisers	Destroyers	Air Force
WEST VIRGINIA (Flagship)	TRENTON	LITCHFIELD	SARATOGA
	MARBLEHEAD	PREBLE	LANGLEY
	RICHMOND	PRUITT	GANNET
MARYLAND	MEMPHIS	NOA	
TENNESSEE		DECATUR	Submarine Force
NEW MEXICO		SICARD	
MISSISSIPPI		HULBERT	ARGONNE (Tender
CALIFORNIA		WM B. PRESTON	V-1, V-2, & V-3

Digrapnic Frequency Table:

	(2nd letter)																									
	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	Total
A	-	-	2	-	-	-	2	-	-	-	-	-	-	1	-	-	-	-	-	-	1	-	-	1	-	-	7
B	-	1	-	1	-	-	-	5	-	2	1	1	-	-	-	-	-	-	2	-	-	5	-	1	-	-	19
C	-	-	3	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	4
D	-	-	1	2	-	-	-	1	-	2	-	-	-	-	2	-	-	3	-	-	-	-	-	6	-	-	17
E	-	-	1	-	-	-	2	-	-	3	-	-	-	-	-	-	1	1	-	-	-	-	-	1	-	5	14
F	-	-	-	4	1	-	2	-	-	2	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	10
G	-	-	1	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	3	-	6
H	1	-	1	1	-	-	3	-	-	1	-	-	-	-	-	-	-	3	-	-	-	1	-	6	-	-	17
I	-	2	3	-	5	-	-	6	-	1	-	-	-	-	-	-	-	-	-	1	2	5	-	-	-	-	25
J	-	-	-	2	-	-	-	-	-	-	-	1	1	-	2	-	-	-	-	-	-	1	-	4	-	-	11
K	-	-	5	3	-	-	-	3	-	-	-	-	-	-	-	-	-	2	2	-	-	-	-	-	-	1	16
L	-	-	6	4	-	-	-	-	-	11	-	-	-	-	4	-	1	-	1	-	-	3	1	1	4	1	37
M	-	-	-	7	1	-	-	12	-	1	-	-	-	-	2	-	1	-	-	-	-	-	-	-	-	7	31
N	-	1	-	1	2	-	1	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	1	-	-	-	7
O	2	-	4	-	-	3	-	-	-	3	-	-	-	-	-	-	-	-	1	-	-	1	1	-	-	-	15
P	-	-	2	-	1	-	-	-	-	-	-	-	-	-	-	-	2	-	-	-	-	1	-	-	-	3	9
Q	-	-	-	10	-	-	-	-	-	4	-	-	-	-	-	-	-	1	-	-	-	-	-	1	-	-	16
R	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	5	-	1	1	-	-	2	-	-	10
S	-	-	-	-	5	-	2	-	-	2	-	-	-	-	1	-	-	-	-	-	-	1	2	-	-	-	13
T	-	-	3	2	-	-	-	-	-	-	-	-	-	1	1	-	-	1	-	-	-	-	-	1	-	-	9
U	-	-	-	3	1	-	1	-	-	-	-	-	-	-	-	-	1	-	1	-	-	4	-	1	-	2	14
V	-	-	-	1	1	-	-	-	-	-	-	-	-	-	2	-	1	-	-	-	-	2	-	-	-	-	7
W	-	-	-	1	-	-	1	-	-	-	-	1	-	-	-	-	-	-	-	-	-	2	1	3	-	2	11
X	1	-	-	5	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	8
Y	-	-	-	1	-	-	-	-	-	2	-	-	-	-	-	-	-	-	2	-	-	-	-	-	-	-	5
Z	-	-	4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	3	-	-	3	-	10
Total	4	4	36	50	17	3	14	27	1	35	1	3	1	2	14	0	9	16	10	2	4	30	6	28	7	24	348

ASSIGNMENT No. 10

Problem No. 2 Serial No. 1

FROM: SF (SHIP) 0016-1110
TO : RX (CINC BLACK) April 16, 1940

240 709 311 845 724 137 395 824 381 720 677 354 384 844 375 355 508 240 785 702

720 375 240 710 605 815 244 375 373 229 221 335 700 814 711 240 712 822 704

Problem No. 2 Serial No. 2

FROM: HA (SHIP) 0016-1115
TO : RX (CINC BLACK) April 16, 1940

240 719 724 654 600 372 725 351 148 580 351 441 190 711 200 605 801 833 790 711

208 240 785 702 720 375 240 710 605 815 244 375 715 774 379 221 335 706 724 240

840 706 724 224

Problem No. 2 Serial No. 3

FROM: PK (SHIP) 0016-1120
TO : LG (FORCE COMMANDER BLACK) April 16, 1940

240 709 311 845 724 137 395 824 381 720 677 354 745 730 532 221 328 240 785 702

720 375 240 710 605 815 244 375 373 229 221 335 700 481 715 774 382 822 704

Problem No. 2 Serial No. 4

FROM: LG (FORCE COMMANDER BLACK) 0016-1200
TO : PK, SF, HA (SHIPS) April 16, 1940

580 751 424 381 720 791 200 321 695 824 381 720 602 325 142 244 185 661 400 840

778 840 708 707 325 203 240 720 840 706 724 232 331 162 829 700 814 711 840 271

355 385 240 281 589 125 595 144 542 245 661 400 840 770 845 377 199 700 471 190

539 838 725 244 681 322 331 180 244 384 445 651 384 321 702 829 721 201 445 651

373 242 724 841 695 261 710 718 702 720 661 424 351 373 231 833 790 561 331

Problem No. 2 Serial No. 5

FROM: LG (FORCE COMMANDER BLACK) 0016-1220
TO : RX (CINC BLACK) April 16, 1940

720 719 529 311 845 724 274 702 841 425 135 321 271 310 710 845 592 325 720 674

ASSIGNMENT No. 10

Problem No. 2 Collateral Information

Messages are in the form of work sheets with the text spaced into tri-numeral groups. The repetitions, all occurring on the same "beat", indicate that a tri-numeral system has been employed. The long repetitions from several origins indicate that a given word or phrase on a given "beat" can be enciphered in only one way, that is, the system appears to have no "varients". There are 113 different tri-numeral groups out of a total of 241. The numbers run from 125 to 845, a known range of 720 and a possible range of 800.

Solve the messages and reconstruct the system used.

Fleet maneuvers in the Caribbean Sea. Scouting operations are still in progress. A few isolated contacts have been made. Probable composition of Enemy Fleet:

Battleships	Cruisers	Destroyers	Air Force
WEST VIRGINIA (Flagship)	TRENTON	LITCHFIELD	SARATOGA
	MARBLEHEAD	PREBLE	LANGLEY
MARYLAND	RICHMOND	PRUITT	
TENNESSEE	MEMPHIS	NOA	
NEW MEXICO		DECATUR	Submarine Force
MISSISSIPPI		SICARD	
CALIFORNIA		HULBERT	ARGONNE (Tender)
		WM B. PRESTON	V-1, V-2, & V-3

Trigraphic Frequency Table

125-1	221-4	311-3	379-1	529-1	661-3	712-1	785-3
135-1	224-1	321-3	381-4	532-1	674-1	715-2	790-2
137-2	229-2	322-1	382-1	539-1	677-2	718-1	791-1
142-1	231-1	325-3	384-3	542-1	681-1	719-2	801-1
144-1	232-1	328-1	385-1	561-1	695-2	720-11	814-2
148-1	240-13	331-3	395-2	580-2	700-4	721-1	815-3
162-1	242-1	335-3	400-2	589-1	702-6	724-8	822-2
180-1	244-6	351-3	424-2	592-1	704-2	725-2	824-3
185-1	245-1	354-2	425-1	595-1	706-3	730-1	829-2
190-2	261-1	355-2	441-1	600-1	707-1	745-1	833-2
199-1	271-2	372-1	445-2	602-1	708-1	751-1	838-1
200-2	274-1	373-4	471-1	605-4	709-2	770-1	840-6
201-1	281-1	375-7	481-1	651-2	710-5	774-2	841-2
203-1	310-1	377-1	508-1	654-1	711-4	778-1	844-1
208-1							845-5

Problem No. 3 Serial No. 1

FROM: DH (FORCE COMMANDER BLACK) '0017-0030
TO : QA, LB (SHIPS)

AM VZ FY FT ZV OJ AZ ZV VG VZ OA CQ YO ZY CM QO CC PW QO SL
NI CA CM AO ZO MO MS VS

Problem No. 3 Serial No. 2

FROM: QA (SHIP)
TO : JZ (CINC BLACK) 0017-0525

VA OQ AA AZ RP IU QA JC HH ZF QO ZV QO GC DF CN OI OZ YY VA
QI ZF QO NU AP ZC GC DF TM QO NU SV SA OO CA YX AQ OT OZ CZ
AM GR QA AN OX QZ ZV GW WY HH

ASSIGNMENT No. 10

Problem No. 3 Serial No. 3

FROM: QA (SHIP) 0017-0550
TO : JZ (CINC BLACK)

VE GW VE OM SG OX IQ MT MV CN AM MO AP ZC CZ CA VE OM VQ LZ
JN

Problem No. 3 Serial No. 4

FROM: QA (SHIP) 0017-0615
TO : JZ (CINC BLACK)

TM QU SD AU EK FQ SV YX JC ZV SD AU OZ OM OA AU RP SO FH MC
CT AO SV SA SO KV CA LZ OA FK ZA NU CN SA VZ CZ SV VA OZ SD
AU MW CC

Problem No. 3 Serial No. 5

FROM: RP (SHIP) 0017-0715
TO : JZ (CINC BLACK)

TM IV MC IR GE OS AZ JC ZV SD AU OZ AE QA EE QA QU VA QI ZF
QO NU AP ZC MW CC MW CC VZ ZC SV VA GR QA SQ OE GO

Problem No. 3 Serial No. 6

FROM: JZ (CINC BLACK) 0017-1125
TO : DH (FORCE COMMANDER BLACK)

QV MZ AA EX MG ND HE OM QA HX RM MW CC TM SQ CA PG CC HV AN
ZZ MS YY MO KE WR ZV QO CT AO SV SA SO KV OE JO ZA NU MO GV
ZF QO CN OI OZ AV

Problem No. 3 Serial No. 7

FROM: TG (SHIP) 0017-0905
TO : JZ (CINC BLACK)

MO MW CC KE WR RL QB NU QV MZ AA EX EO QO MC JH OZ DH ND JC
AO CV JV ZF QO NU CZ AM QZ ZK AM AZ

Problem No. 3 Collateral Information

Messages are in the form of work sheets with the text spaced into two-letter groups. The repetitions, all occurring on the same "beat", indicate that a digraphic system has been employed. The long repetitions from several origins indicate that a given word or phrase on a given "beat" can be enciphered in only one way, that is, the system appears to have no "varients". There are 116 different digraphs out of a possible total of 676.

Solve the messages, and reconstruct the system if possible.

The date is April 17, 1930. The general conditions are Fleet maneuvers in the Caribbean Sea. Scouting operations are still in progress. Contacts between scouts have been made, but the main bodies have not yet been located. Probable composition of Enemy Fleet:

ASSIGNMENT No. 10

Battleships	Cruisers	Destroyers	Air Force
WEST VIRGINIA (Flagship)	TRENTON	LITCHFIELD	SARATOGA
	MARBLEHEAD	PREBLE	LANGLEY
	RICHMOND	PRUITT	GANNET
MARYLAND	MEMPHIS	NOA	
TENNESSEE		DECATUR	Submarine Force
NEW MEXICO		SICARD	
MISSISSIPPI		HULBERT	ARGONNE (Tender)
CALIFORNIA		WM B. PRESTON	V-1, V-2 & V-3

Digraphic Frequency Table

	(2nd letter)																									
	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	Total
A	3	-	-	-	1	-	-	-	-	-	-	-	5	2	4	3	1	-	-	-	-	-	-	-	-	-	29
B	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0
C	5	-	7	-	1	-	-	-	-	-	-	-	2	4	1	1	-	-	-	2	-	1	-	-	-	3	27
D	-	-	-	-	-	2	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	3
E	-	-	-	-	1	-	-	-	-	-	1	-	-	-	1	-	-	-	-	-	-	-	-	2	-	-	5
F	-	-	-	-	-	-	-	1	-	-	1	-	-	-	-	-	1	-	-	1	-	-	-	-	1	-	5
G	-	-	2	-	1	1	-	-	-	-	-	-	-	-	1	-	-	2	-	-	-	1	2	-	-	-	10
H	-	-	-	-	1	-	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	1	-	-	5
I	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	1	-	-	1	1	-	-	-	-	4
J	-	-	4	-	-	-	-	1	-	-	-	-	-	1	1	-	-	-	-	-	-	1	-	-	-	-	8
K	-	-	-	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2	-	-	-	-	4
L	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2	2
M	-	-	2	-	-	-	1	-	-	-	-	-	-	-	5	-	-	-	2	1	-	1	5	-	-	2	19
N	-	-	-	2	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	7	-	-	-	-	-	10
O	3	-	-	-	1	-	-	-	2	1	-	-	4	-	1	-	1	-	1	1	-	-	-	2	-	7	24
P	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	2
Q	6	1	-	-	-	-	-	-	2	-	-	-	-	-	10	-	-	-	-	-	2	2	-	-	-	2	25
R	-	-	-	-	-	-	-	-	-	-	-	1	1	-	-	2	-	-	-	-	-	-	-	-	-	-	4
S	4	-	-	4	-	-	1	-	-	-	-	1	-	-	3	-	2	-	-	-	-	6	-	-	-	-	21
T	-	-	-	-	-	-	-	-	-	-	-	-	4	-	-	-	-	-	-	-	-	-	-	-	-	-	4
U	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0
V	5	-	-	-	3	-	-	1	-	-	-	-	-	-	-	-	1	-	1	-	-	-	-	-	-	3	14
W	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2	-	-	-	-	-	-	1	1	4
X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0
Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	2	2	-	5
Z	2	-	5	-	-	5	-	-	-	-	1	-	-	-	1	-	-	-	-	-	-	7	-	-	1	1	23
	28	1	20	6	11	8	3	6	5	1	3	2	16	7	28	6	8	5	4	5	15	23	8	7	6	25	-Total- 257

It is important that the Student's full name, rank, rate or title, and present address appear on all work sheets and correspondence. Course material will be returned only in the penalty envelopes provided for that purpose.

B L A N K

Op-20-GR

RESTRICTED

NAVY DEPARTMENT
Office of Chief of Naval Operations
WASHINGTON.

ELEMENTARY COURSE IN CRYPTANALYSIS

ASSIGNMENT No. 11

DIAGONAL DIGRAPHIC SUBSTITUTION

1. An advantage of diagonal digraphic substitution over the systems described in the preceding assignment is that such systems may be constructed with much smaller figures. The basic method of encipherment is the use of an imaginary rectangle whose diagonally opposite corners are formed by the plain-letter pair and their equivalent cipher pair. This method is illustrated in the example below, which is constructed with four rectangular sections, each containing a complete alphabet sequence.

	A	F	L	Q	V	R	E	C	T	A
	B	G	M	R	W	N	G	L	B	D
Plain (1)	C	H	N	S	X	F	H	I	K	M
	D	I	O	T	Y	O	P	Q	S	U
	E	K	P	U	Z	V	W	X	Y	Z
	D	I	A	G	O	A	B	C	D	E
	N	L	B	C	E	F	G	H	I	K
Cipher (2)	F	H	K	M	P	L	M	N	O	P
	Q	R	S	T	U	Q	R	S	T	U
	V	W	X	Y	Z	V	W	X	Y	Z

Cipher (1)

Plain (2)

To encipher a digraph by this system, the first and second letters are located in the sections marked Plain (1) and Plain (2), respectively, and the cipher pair is found in the sections marked Cipher (1) and Cipher (2), at the corners of an imaginary rectangle whose diagonal is indicated by the plain-letter pair. An enciphered message would appear as follows:

Plain - AB AN DO NS HI PQ
Cipher - ED CF SF IS KL VS

2. If it is desired to employ a smaller diagonal digraphic system, a rectangle of but two sections may be constructed. For example:

	A	B	C	D	E	R	E	C	T	A
Plain (1)	F	G	H	I	K	N	G	L	B	D
	L	M	N	O	P	F	H	I	K	M
Cipher (2)	Q	R	S	T	U	O	P	Q	S	U
	V	W	X	Y	Z	V	W	X	Y	Z

Plain (2)

Cipher (1)

A36462

When the letters of the plain digraph form opposite corners of an imaginary rectangle, the basic method of encipherment is the same as in the four section rectangle. When both letters of the plain pair occur in the same row, the imaginary rectangle becomes a single line, and according to the basic diagonal method, the cipher digraph is formed as the reciprocal of the plain digraph. Thus, AN plain is enciphered by RF, RE plain becomes PB cipher, AT plain becomes TA cipher, and ER plain becomes RE cipher.

3. The size of the figure employed may be still further reduced by employing a rectangle composed of a single alphabet sequence. In this case, there are several conventional modifications necessary to the basic method in order to find certain cipher equivalents. The system described below constitutes what is generally called the "Playfair" system.

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

The following cases illustrate the various methods of finding cipher equivalents:

(a) When the imaginary rectangle can be formed, the basic method of encipherment is used; RD plain becomes AN cipher, NE plain becomes GR cipher, etc.

(b) When both letters of the plain pair occur in the same row, the letters immediately to the right of the first and second plain letters form the first and second letters, respectively, of the cipher pair. For this purpose the letters of the left hand column are considered to be projected to the right of the figure. RE plain becomes EC cipher, RT plain becomes EA cipher, EA plain becomes CR cipher. AE plain becomes RC cipher, etc.

(c) When both letters of the plain pair occur in the same column, the letters immediately below the first and second plain letters form the first and second letters, respectively, of the cipher pair. For this purpose the letters of the top row are considered to be projected to the bottom of the figure. RN plain becomes NF cipher, EW plain becomes GE cipher, WE plain becomes EG cipher, OR plain becomes VN cipher, etc.

(d) When the plain-text message is being separated into digraphs in preparation for encipherment, any identical letters which fall within the same pair must have a null inserted between them because it is impossible to encipher doubled letters otherwise by this system.

The message BATTLESHIPS COMMENCE FIRING would appear as follows when enciphered by the system shown:

BA TK TL ES HI PS CO MX ME NC EF IR IN GP
DT BS CB TP IK QU RQ IZ HA LR RH FC FL HW

4. The "Playfair" system has been widely used where it was desired to have a simply constructed digraphic system whose key could be readily changed in the field of operation. Cryptograms enciphered with this system can be recognized by the absence of doubled letters in the cipher digraphs. Other weaknesses in the "Playfair" system will be pointed out in the next section as an example of the analysis of a known cryptographic system which should be made prior to the solution of cryptograms enciphered by the known system.

5. It is not essential that diagonal digraphic systems be in the shape of perfect squares, such as those shown above; other rectangular designs will

serve equally well with little or no modification in method.

ANALYSIS OF THE "PLAYFAIR" CIPHER SYSTEM

6. According to the way cipher pairs are formed by the "Playfair" system, a plain letter can be replaced by only five other letters, which are the other four in the same row and the one just below it in the same column:

X E X X X
X

Hence, a frequent plain letter, such as E, will cause letters in the position marked X to occur frequently in the cipher text.

7. If a given cipher digraph represents a certain plain digraph, any other cipher digraph containing one of the same cipher values may also represent a plain digraph containing one of the same plain letters similarly placed in the plain digraph. For instance, there is a probability of one in five that if EK. cipher is the equivalent of TH plain, any cipher pair beginning with E will represent T plain, or any cipher pair ending in K will represent H plain.

8. A cipher digraph and its plain equivalent can never contain the same letter in the same position in each digraph. That is, NE cipher can never represent N plain, or E plain.

9. If the same letter occurs in different positions in both the cipher and plain digraphs, the three letters involved are in adjacent positions in the same row or column of the figure used. Thus, if EC cipher represents RE plain, the sequence REC appears in a row or column of the original figure.

10. Since all reversed cipher digraphs represent reversed plain digraphs, the relative frequencies of reversed cipher digraphs give indications of their plain equivalents. That is, if the cipher digraphs EC and CE are both high frequency digraphs in a certain text, their plain equivalents may be RE and ER respectively.

11. Reconstruction of the figure used is of great assistance during the solution of a "Playfair" cipher. The original figure may not be reconstructed at first because of the manner in which end rows and columns are considered to be projected to their opposite positions. However, when a systematically-mixed sequence was used, the original figure is recognized by discovery of the key.

Problem No. 1 — Non-Naval Text

ONE OF THEIR DATES T
NMBIG UFCIT EAQBR SBEWP ECQBR NHEOM LTMHE CRGNM QCASR IRWZD THCLD

CEPRS NMDVE PMKCE HQNML ARIMB GHTSB QHBCL ACPGQ BMHTT GRBUB AGHUH

ELMPW OKKHB DQTXG NSGLR HIRGR GLOMK BADZC PRMHE NMGKA GNCBF MSFCL

ODQGM CGOWE VDQPI MXPGG HUXHB RMRIC QECOC EARRR LATQB BRNGH RQSQO

RIQCB UUBAH UCMCS GEFCE RRKCI RFCFE ABUDP KORAC SNEVD QKCEB MHLHM

KOHPG GHQNP ENSLA RIMBE VCLHI RNTNE PPEPD RRDQC UYTGR HMGTN GHRWI

FEFCZ DSCNM RHRSC LUGOR FCRMA EFCRT KCRGI WCUSL MKFAC PPGGK ACRTO

WRIQB MIMKU BRYLC XTRMC PWMLC

ASSIGNMENT No. 11

Problem No. 2 Serial No. 1

FROM: RN (FORCE COMMANDER)
TO : OK (COLLECTIVE CALL)
INFO: GL (FORCE COMMANDER)

0016-2225
April 16, 1940

FP TZ FV PR ZF PZ BF EI YX ON XM GU DF UA DF LR LP BF DV LP

FH IX FA XY IN XM GU NI XY YZ PD GF ZR EG TB BF XV YM FS YF

ZF HY VZ EQ IB PT LP IA FU XV ID LA NQ EQ BF RF TQ KH ZP IX

RT YX RY FR FV MS HG DS LP HE KS FV QZ FH NX KH UF DV SD FH

ZD RZ GY ZF YE KN AL NX KH XF RY TX PR RY TX PR LE RF PH ZL

AF GY ZF YE XM CO YZ VN LE RF PH SB VG FS FR SQ

Problem No. 2 Serial No. 2

FROM: GL (FORCE COMMANDER)
TO : DY (SHIP)
INFO: ZB (CINC)

0016-2220
April 16, 1940

FR XM SC SM FU RF LG CR EW PF QL WE GF EW BU HV HF ZT ZF YR

ZF PZ BF AZ RF SK SA XY RZ AF UV BT XP DF UH PY QT PY VN KH

XF RY TX PR RY TX PR LE RF PH ZL AF GY LA TZ ZL BF WS FR XP

FY XP ND UF MS SM MS HY YM BC XY OQ

Problem No. 2 Serial No. 3

FROM: GL (FORCE COMMANDER)
TO : DY, HV, ST (SHIPS)
INFO: ZB (CINC)

0016-2250
April 16, 1940

EG GY LA TZ VG FS FR SN ZT ZF YR ZF PZ BF EI YX ON XM GU DF

UA DF LR LP BF DV EL XY ND CP RF YS AY ZM NB RY TX PR LP HE

KS FV TA YX TA NX KH UF DV SD FH ZD RZ GY ZF YE HX PR AF GY

LA TZ XM TB FP UV FR RY TX PR LE RF PX RF SK SW QF RF TF MY

YA FH AQ QF UN RZ UV FR ZT NB RY OM UN RZ MS LZ RF SK NG NB

RY TX PR RF ZR MS SM FU RF LG CR EW PF ZF XY GU ZF ZY FH EG

SK SC

Problem No. 2 Serial No. 4

FROM: WX (?)
TO : ZB (CINC)

0016-2250
April 16, 1940

EG FP TZ FV PR ZF VG FS FR NW RY AL BS DV HY VN MS XM QF ZF

FG TX PR AF PF YF MK RF ND SF PH FU SK FN LD PU OE MO UB BU

ZW ZL BF WS ZF WQ TA FG TP AL BS DV HY DM US AL HO AY PD FR

XM TZ BF DV ZA ZD PF ZL BF WS PK FH XM FV ZQ GE XK GU LF HV

ASSIGNMENT No. 11

YR ZF SY FY ET NU LF SZ PH FU SK FN LD

Problem No. 2 Collateral Information

Messages are in the "work sheet" form and the student is given the benefit of the preliminary analysis. From the lengths of the numerous long repetitions, and the intervals between them, it should be obvious that some sort of digraphic substitution cipher has been employed. Solve the messages, reconstruct the cipher used and other details of the system.

Fleet maneuvers in the Caribbean Sea. Scouting operations are still in progress.
Probable composition of Enemy Fleet:

Battleships	Cruisers	Destroyers	Air Force
WEST VIRGINIA (Flagship)	TRENTON (Flagship)	LITCHFIELD (Flagship)	SARATOGA (Flagship)
MARYLAND	MARBLEHEAD	PREBLE	LANGLEY
TENNESSEE	RICHMOND	PRUITT	GANNET
NEW MEXICO	MEMPHIS	NOA	
MISSISSIPPI		DECATUR	**Submarine Force**
CALIFORNIA		SICARD	
		HULBERT	ARGONNE (Flagship & Tender)
		WM. B. PRESTON	
			V-1, V-2, & V-3

Digraphic Frequency Table:

	(2nd letter) 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	Total
A	--	-	-	--	--	5	-	-	-	-	-	4	-	-	-	-	1	-	-	-	-	-	-	-	2	1	13
B	-	-	1	-	-	11	-	-	1	-	-	-	-	-	-	-	-	-	2	1	2	-	-	-	-	-	18
C	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	1	-	1	-	-	-	-	-	-	-	-	3
D	-	-	-	-	-	5	-	-	-	-	-	-	1	-	-	-	-	1	1	-	-	7	-	-	-	-	15
E	-	-	-	-	-	-	4	-	2	-	-	1	-	-	-	-	2	-	-	-	-	-	3	-	-	-	13
F	1	-	-	-	-	-	2	7	-	-	-	-	-	2	-	3	-	9	4	-	6	6	-	-	2	-	42
G	-	-	-	-	1	2	-	-	-	-	-	-	-	-	-	-	-	-	-	5	-	-	-	-	6	-	14
H	-	-	-	-	2	1	1	-	-	-	-	-	-	-	1	-	-	-	-	-	2	-	2	4	-	13
I	1	1	-	1	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	1	-	-	5
J	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0
K	-	-	-	-	-	-	-	5	-	-	-	-	-	1	-	-	-	-	2	-	-	-	-	-	-	-	8
L	4	-	-	2	4	2	2	-	-	-	-	-	-	-	-	6	-	2	-	-	-	-	1	-	-	1	24
M	-	-	-	-	-	-	-	-	-	-	1	-	-	-	1	-	-	-	3	-	-	-	-	-	1	-	9
N	-	3	-	2	-	-	1	-	1	-	-	-	-	-	-	-	1	-	-	-	1	-	1	3	-	-	13
O	-	-	-	-	1	-	-	-	-	-	-	-	1	1	-	-	1	-	-	-	-	-	-	-	-	-	4
P	-	-	-	2	-	4	-	5	-	-	1	-	-	-	-	-	-	10	-	2	1	-	-	-	2	3	30
Q	-	-	-	-	-	3	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	1	5
R	-	-	-	-	-	15	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	10	5	31
S	1	1	2	2	-	1	-	-	-	-	6	-	3	2	-	-	1	-	-	-	-	-	1	-	1	1	22
T	3	2	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	8	-	6	20
U	1	-	-	-	-	3	-	-	-	-	-	-	2	2	-	-	-	-	-	3	2	-	-	-	-	-	13
V	-	-	-	-	-	3	2	-	1	-	-	-	-	3	-	-	-	-	-	-	-	-	-	-	-	1	10
W	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	1	-	3	-	-	-	-	-	-	-	5
X	-	-	-	-	-	2	-	-	-	-	1	-	9	-	-	3	-	-	-	-	-	2	-	-	7	-	24
Y	1	-	-	-	3	2	-	-	-	-	-	-	2	-	-	-	-	3	1	-	-	-	-	5	-	2	19
Z	-	-	-	4	-	14	-	-	-	-	-	5	-	-	-	1	1	2	-	3	-	-	1	-	-	-	32
Total	13	7	3	13	12	74	12	17	5	0	9	11	18	12	3	14	8	28	19	8	18	19	7	19	35	21	405

ASSIGNMENT No. 11

Problem No. 3 Serial No. 1

FROM: XY (UNIT COMMANDER) 0012-1225
TO : CD (FORCE COMMANDER)

QF AF BM EU IG PD EW EU OY UU GI PX IT AN BM EU OZ WC IE OF

SP IU JA EW SQ HG MQ PC YH PN GM FK IX OW ED II SE WW FG IX

WW HG YF IU EV TH SE BS DJ TZ EA RD EJ RW IO HA HM RA HL PU

TP JO HL AK GF QJ RK FK QF AF IU OC TH SE WA FG IB EF SX IM

KQ PZ JM WI FV LL HG EU UY ST SC BS DC HL BQ SQ LE HA TT QD

PN YS PB EU VH LC HU SM QF AF BM EU IR

Problem No. 3 Serial No. 2

FROM: XY (UNIT COMMANDER) 0013-1218
TO : AB (FORCE COMMANDER)

TG QD PN YS PN PR IU IT ST KG JL IO TH OG EU QD QF AF BM EU

IU IQ JN SX TI YD TW YE PA

Problem No. 3 Serial No. 3

FROM: AB (FORCE COMMANDER) 0013-1730
TO : AM, AN (SHIPS)

SQ DJ BI QW OG IT QD BQ EV IN BQ TH YB EJ RW ST GW PO JC GW

HL BY KQ PZ JM AN KG IQ BM IT ST FL UT LB SK JH FD HM QX JN

SQ LU EC BD QR JO SA HQ BQ OF HI EW IF

Problem No. 3 Serial No. 4

FROM: XY (UNIT COMMANDER) 0010-1825
TO : AB (FORCE COMMANDER)

IM IL YL UU GE PZ HM ST QG UF RH BM TM ML IO SZ US TT TD QD

BF LG SK IM SM MF VZ GR FK QT IU EV TC BU IV IM SC FD HM QI

JJ SF BS DX

Problem No. 3 Collateral Information

Digraphic Frequency Table

ASSIGNMENT No. 11

	(2nd letter)																										Total
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
A	-	-	-	-	-	4	-	-	-	-	1	-	-	2	-	-	-	-	-	-	-	-	-	-	-	-	7
B	-	-	-	1	-	1	-	-	-	-	-	-	5	-	-	1	4	-	3	-	1	-	-	-	1	-	17
C	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0
D	-	-	1	-	-	-	-	-	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	4
E	1	-	1	1	-	1	-	-	-	2	-	-	-	-	-	-	-	-	-	-	8	2	3	-	-	-	19
F	-	-	-	3	-	-	2	-	-	-	3	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	9
G	-	-	-	-	1	1	-	-	-	-	-	1	1	-	-	-	-	1	-	-	-	-	2	-	-	-	7
H	2	-	-	-	-	-	3	-	1	-	-	4	4	1	-	-	1	-	-	-	1	-	-	-	-	-	17
I	-	1	-	-	1	1	1	-	1	-	-	1	4	-	4	-	2	1	-	3	6	1	1	2	-	-	30
J	-	-	1	-	-	-	-	1	-	1	-	1	4	2	2	-	-	-	-	-	-	-	-	-	-	-	12
K	-	-	-	-	-	-	2	-	-	-	-	-	-	-	-	-	3	-	-	-	-	-	-	-	-	-	5
L	-	2	-	-	1	-	1	-	-	-	-	1	-	-	-	-	-	-	-	-	1	-	-	-	-	-	5
M	-	-	-	-	-	1	-	-	-	-	-	1	-	-	-	-	1	-	-	-	-	-	-	-	-	-	3
N	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0
O	-	-	1	-	-	1	1	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	1	-	1	1	7
P	1	1	-	1	-	-	-	-	-	-	-	-	4	1	-	-	-	1	-	-	1	-	-	1	-	4	15
Q	-	-	-	6	-	5	1	-	-	1	-	-	-	-	-	-	-	1	-	1	-	-	1	1	-	-	17
R	1	-	1	-	-	-	-	1	-	-	1	-	-	-	-	-	-	-	-	-	-	-	2	-	-	-	6
S	1	-	2	-	4	-	-	-	-	-	2	2	-	1	1	-	4	-	-	5	-	-	-	2	-	1	25
T	-	-	1	1	-	-	2	4	1	-	-	1	-	-	-	-	-	-	-	1	-	-	-	-	-	1	13
U	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	1	-	3	-	-	-	1	-	6
V	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	2
W	3	-	1	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	5
X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0
Y	-	-	1	1	1	1	-	1	-	-	-	-	-	-	-	-	-	-	2	-	-	-	-	-	-	-	8
Z	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0
Total	-	9	2	11	15	8	17	13	8	4	6	7	10	21	9	8	3	16	4	6	10	21	5	9	7	3	8	240

It is important that the Student's full name and present address appear on all work sheets and correspondence. Course material will be returned only in the penalty envelopes provided for that purpose.

B L A N K

Op-20-GR

RESTRICTED

NAVY DEPARTMENT
Office of Chief of Naval Operations
. WASHINGTON.

ELEMENTARY COURSE IN CRYPTANALYSIS

ASSIGNMENT No. 12

OPEN CODE

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, of course, 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.

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.

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 ETMSI NNNWQ

Serial 2 - ATALC NIMDE OTNIE LEGIG OEMRI GFIHE NHISO UKONP

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 regulation size. We are now out of quarintine 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 dont want you and John feeling downhearted.

Write a line to Lieut. R.A. Root of H.M.S. Colossus telling him I received his letter of May twelfth but cannot reply till after a weeks time. Inform Dorothy you have received this and to write me a line or two.

Love to all

Herbert.

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 pad:

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

PROBLEM No. 5

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

BUILD NEW NO LEARN 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

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 Elois do to her As always, Jerry.

Before you mail the solutions to this assignment please include your full name, rate, rank, or title, and latest address. Use only the official envelopes provided for mailing your work sheets.

B L A N K