Op-20-GR

RESTRICTED

NAVY DEPARTMENT
Office of Chief of Naval Operations
WASHINGTON.

ELEMENTARY COURSE IN CRYPTANALYSIS

ASSIGNMENT No. 5

EQUIVALENT CIPHER ALPHABETS

1. Any sequence containing 26 letters may be rearranged so that all the letters which are originally separated by equal intervals will also be spaced at equal intervals in the new related sequences. Including the original sequence, a total of six related sequences may be constructed.

Example:

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

In this example, a normal alphabet sequence has been re-spaced to form the other five related sequences. In constructing them, the original sequence is regarded as a circle and the letters are counted off in equal intervals, then written in adjacent positions to form each related sequence.

2. Only the odd intervals from 3 to 11 can be used in re-spacing a 26 letter sequence to form different related sequences. It is obvious that the even intervals will produce 13 letter sequences, and that the interval 13 can not be used. The odd intervals from 15 to 25 will produce identical sequences with those from 1 to 11, but reversed in direction.

3. Cipher alphabets may be re-spaced to form equivalent cipher alphabets by the same process as that applied to construct related sequences.

Example:

Original Cipher Alpnabet

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

Equivalent Cipher Alphabet

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

4. An equivalent cipher alphabet can not be distinguished from the original cipher alphabet unless a systematic construction or some outside information is available to identify the original one. The secondary alphabets generated by shifting the points of coincidence of the plain and cipher components are the same alphabets regardless of which equivalent cipher alphabet has been shifted.

Example:

Secondary Cipher Alphabet

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

Equivalent Secondary Cipher Alphabet

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

The secondary cipher alphabet of this example has been derived by shifting the cipher component of the original cipher alphabet of paragraph 3, and the equivalent secondary cipher alphabet by shifting the cipher component of the equivalent alphabet of paragraph 3.

The number of spaces each cipher component has been shifted is not the same in each case, yet the plain and cipher values correspond exactly in each case after re-spacing.

REMARKS ON KEY RECOVERY

5. An equivalent or related sequence is a sequence in which there are spaced at equal intervals letters which were at equal intervals in the original sequence. Including the original sequence, there are six such equivalent sequences, corresponding to absolute spacings of 1, 3, 5, 7, 9, and 11. Suppose the following has been recovered in the solution of a cryptogram:

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

There is definite evidence of system here, including a fragmentary keyword. Construct the other five equivalent sequences by respacing the above by intervals 3, 5, 7, 9, and 11.

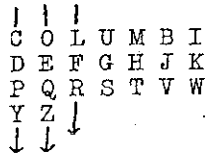
	Spacing																							
1.	1	X	P	E	L	U	M	B	I	A	C	Y	Q	F	G	H	J	K	N	D	O	Z	R	S	T	V	W
2.	3	X	L	B	C	F	J	D	R	V	P	U	I	Y	G	K	O	S	W	E	M	A	Q	H	N	Z	T
3.	5	X	M	Y	J	Z	W	U	C	H	O	V	L	A	G	D	T	E	I	G	N	S	P	B	Q	K	R
4.	7	X	I	H	R	E	C	K	T	U	Q	D	W	B	G	Z	P	A	J	S	L	Y	N	V	M	F	O
5.	9	X	C	D	P	Y	O	E	Q	Z	L	F	R	U	G	S	M	H	T	B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

The equivalent sequences were developed by the process of decimating. Only five equivalent sequences need be retained due to the fact that decimating by 13 gives 13 pairs of letters, and by any odd number higher than 13 results in the same sequence as already obtained running backward. Decimating by even numbers will result in two 13-letter sequences (26 letters in the alphabet).

One of these five is the sequence used by the encipherer. Careful inspection shows that the sequence obtained from spacing 9 has a regular and systematic pattern, exhibiting all the characteristics of a transposed keyword sequence:

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

The generating figure built up from this sequence turns out to be:



This is the only one of the six sequences which will yield this figure.

6. Inspection of the foregoing equivalent sequences shows that letters which were adjacent in the original sequence are now separated as follows:

Seq. No.	Int.	Interval between originally adjacent letters in (1)	
1	1	1	0 + 1
2	3	9	3 x 9 = 27 = 26 + 1
3	5	21	5 x 21 = 105 = 4.26 + 1
4	7	15	7 x 15 = 105 = 4.26 + 1
5	9	3	3 x 9 = 27 = 26 + 1
6	11	19	11 x 19 = 209 = 8.26 + 1

From these figures the following rules may be deducted:

"To obtain an equivalent sequence in which letters adjacent in the original sequence are spaced any desired odd number of letters apart, respace the original sequence by that number which, when multiplied by the desired letter spacing, will give a product which is one greater than the nearest even multiple of 26." For example, the final spacing of 3 in sequence No. 5, multiplied by the respacing interval of 9 for this sequence, gives 27, a result 1 greater than 26. Respacing intervals of 23, 21, 19, 17, and 15 will give the reverse of the above five sequences, in which originally adjacent letters are separated by 17, 5, 11, 23, and 7 letters respectively. This rule is useful when it is desired to expand a sequence to some other letter spacing.

RECONSTRUCTION OF MULTIPLE ALPHABET SYSTEMS

7. When the same sequence has been used for each of the cipher components of a multiple alphabet system, there are definite relationships between the individual cipher values which may be utilized in recovering other cipher values after a few have been identified through analysis.

(a) When the plain component is originally a normal sequence, the cipher sequences will be recovered in their original order and new values may be placed in the various cipher components as soon as their relative positions have been established.

(b) When the plain and cipher components are originally the same mixed sequence, the plain component enters into the reconstruction in the same manner as another cipher component.

(c) The reconstruction of a multiple alphabet system in which the plain component is a different mixed sequence from that used in the cipher components, requires a relatively large number of values identified by analysis.

8. The principles used in the reconstruction of multiple alphabet systems are explained by the following case in which the plain and cipher components are different mixed sequences.

(p) - D I P L O M A C Y B E F G H J K N Q R S T U V W X Z
(c1) - Q P Q V W X Z T H U R S D A Y B C E F G I J K L M N
(c2) - N O P Q V W X Z T H U R S D A Y B C E F G I J K L M
(c3) - E F G I J K L M N O P Q V W X Z T H U R S D A Y B C

The interval between letters of two cipher components, letters which occur in the same vertical column, is equal to the amount of displacement of one component from the other.

O (c1) to N (c2) is an interval of one, the amount of shift between the cipher components (1) and (2).

E (c3) to O (c1) is the same interval as O (c3) to U (c1), and is the same interval as U (c3) to F (c1), etc.

Thus, a chain of letters, E, O, U, F, etc., with correct relative spacings, could be made from the vertical relationships alone, when the order of the plain component sequence is unknown. A set of equivalent alphabets might be the result of construction by this means, but the original in this case would be recognized when the proper spacing is found.

If the vertical relationship is used between components which are originally displaced an even number of letters, such as (c2) and (c3), a chain of only 13 letters will result, and if the components were originally displaced 13 letters, they would show only reciprocal relationships.

9. The application of the principles explained in paragraph 6 will be demonstrated by a practical problem. Suppose the Enciphering Table obtained during the solution of a cryptogram appeared as follows:

(p) -	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
(c1) -	Z	U	T		R		D	A	P			V		C	W				G	I						H
(c2) -	X	H	Z	N	U			D	O				W	B	V			E	F	G						T
(c3) -	L			E	P			W	F			I	K	T	J			U	R	S						

Since the linear interval between R and P (c1) is the same as that between P and F (c3) i.e., R...P and P...F we may arbitrarily assume this interval to be one (by placing the two columns in which the identically spaced pairs occur together) and build a cipher sequence accordingly.

Component will be included as:

Illustration No. 1

(p) -	E	I
(c1) -	R	P
(c2) -	U	O
(c3) -	P	F

R preceeds P in the first cipher alphabet: F follows P in the third cipher alphabet. If the sequences are identical, there should be an R preceeding P in the third cipher alphabet and P in the first should be followed by an F. F cipher has not been recovered in the first alphabet. R cipher in the third alphabet occurs beneath S (p).

Illustration No. 2

(p) -	S	I	E
(c1) -	G	R	P
(c2) -	F	U	O
(c3) -	R	P	F

Illustration No. 3

(p) -			S	E	I			
(c1) -			G	R	P	F	U	O
(c2) -	G	R	P	F	U	O		
(c3) -		G	R	P	F	U	O	

G preceeds R in the first, so it should form part of the sequence in the third.

The process of adding new values to the plain and cipher sequences progresses through the following stages.

Illustration No. 4

(p) -								T			S	E	I	R	B				Y						
(c1) -								I	S		G	R	P	F	U	O	E	H			T				
(c2) -				I	S			G	R	P	F	U	O	E	H			T							
(c3) -					I	S		G	R	P	F	U	O	E	H			T							

Illustration No. 5

(p) -							O			L	T			S	E	I	R	B			Y		N	C						
(c1) -							W	J		V	I	S		G	R	P	F	U	O	E	H		C	T		B	Z		
(c2) -			W	J			V	I	S		G	R	P	F	U	O	E	H			C	T		B	Z				
(c3) -				W	J		V	I	S		G	R	P	F	U	O	E	H			C	T		B	Z				

ASSIGNMENT No. 5

Illustration No. 6

```
(p)  -    M   H O   G L T     S E I R B     Y   N C     A
(c1) -L   X K A W J D V I S   G R P F U O E H   C T   B Z
(c2) -K A W J D V I S   G R P F U O E H   C T   B Z L   X
(c3) -  X K A W J D V I S   G R P F U O E H   C T   B Z L
```

The intervals between E, F, and G, and between V, W, and X, in the cipher sequence obtained above, indicate that equivalent alphabets have been recovered which should be re-spaced by counting off every third letter in the reverse direction.

Illustration No. 7

```
(p)  -   I   L O M A C Y B E   G H     N   R S T
(c1) - O P   V W X Z T H U R S D A   B C E F G I J K L
(c2) -   O P   V W X Z T H U R S D A   B C E F G I J K L
(c3) - E F G I J K L     O P   V W X Z T H U R S D A   B C
```

The keyword sequences used are now visible and the missing values can be entered.

CONTINUATION OF SOLUTION FROM ASSIGNMENT No. 4

10. A few more values are necessary in Table IV of Assignment No. 4, in order to completely reconstruct the system used. Let us obtain these from the following parts of the cryptogram (Assignment No. 4, page No. 10):

Line 1

Alph -	1	2	3	4	5	6	7	8
(c) -	K	P	T	X	S	L	I	C
(p) -	C	O		M	E	N		E
New -			M				C	

Line 6

1	2	3	4	5	6	7	8	9	Ø
K	F	M	P	S	L	G	X	A	H
C		T		E	N	T	Y		I
			W						

Lines 1 and 2

Alph -	1	2	3	4	5	6	7	8	9	Ø
(c) -	M	J	K	A	Q	J	B	F	Z	A
(p) -	N	H	U	N	D	R	E	D		O
New -									F	

1	2	3	4	5	6	7	8	9	Ø	1
J	G	M	B	S	L	N	P	H	H	E
		T	E	E	N	A		R	I	
U	R						P			L

11. Adding the new values just obtained to those in Table IV of Assignment No. 4, gives the following table for use in reconstructing the system:

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

The reciprocal relationship between the plain and each cipher component will be ignored.

On account of the L and B being found in two vertical columns, a good starting point is to assume the L and B to be adjacent in the cipher component. Then the following will also appear in the cipher component: GN, KI, MA, FQ, CS, PG, and WE.

ASSIGNMENT No. 5

Using the PGN sequence in the first three cipher components, partial reconstruction can be made:

Plain --	W T A	O R	P L
: (c)			
: 1 -	P G N		W E
: 2 -	V	P G N	
:3-6-8 -	M A	H J	P G N
: 4-7 -	P G N	D	
: 5 -			P G N
: 9 -	C S	H J	
: 10 -		M A	

Plain --	H E W T A	S O R	Z N P L U
: (c)			
: 1 -	L B P G N		O C S M A W E H J
: 2 -	H J V	L B P G N	
:3-6-8 -	O C S M A	W E H J V	L B P G N K
: 4-7 -	L B P G N	K I D	O C S M A
: 5 -	O C S M A	W E H J V	L B P G N
: 9 -	O C S M A	W E H J V	
: 10 -	Z	O C S M A	

The three partial reconstructions may now be combined:

Plain --	H E W T A	S O R	Z N P L U
: (c)			
: 1 -	L B P G N		O C S M A W E H J
: 2 -	H J V L B P G N		
:3-6-8 -	O C S M A W E H J	V L B P G N	K I D
: 4-7 -	L B P G N K I D	O C S M A	
: 5 -	O C S M A W E H J	V L B P G N	
: 9 -	O C S M A W E H J	V	
: 10 -	Z O C S M A		

It has been shown that most of the cipher sequence could be obtained without considering the fact that the plain component is the same sequence reversed. The important point is that the complete system may be reconstructed from a relatively few values obtained through analysis of the cryptogram.

The sequence used in this problem is random mixed, therefore, the original one cannot be distinguished from a related one which may be reconstructed. The ten cipher components are set with the keyword GUANTANAMO under A (p).

REMARKS ON POLYALPHABETIC SUBSTITUTION

12. The same method used in determining which cipher values probably represent vowels or consonants may be applied to polyalphabet substitution ciphers as that described in Assignment No. 1, for monoalphabetic substitution. However, the values in each alphabet must be considered with their respective prefixes and suffixes in adjacent alphabets in studying the frequencies of their combinations.

13. After the original sequences of a polyalphabet substitution system have been recovered, subsequent messages using these sequences may be solved by a modification of the method of completing the plain component described in Assignment No. 2. The plain component sequence must be completed beneath the letters of each individual alphabet in order to select the proper generatrix which corresponds with each alphabet. The proper generatrix will show more and a better assortment of high frequency letters than any of the other generatrices.

ASSIGNMENT No. 5

14. In some cases there will be insufficient recoveries to permit the mechanical reconstruction illustrated in paragraph 9. Another method which is useful in this case will be illustrated, using the same data given in paragraph 9, in order to compare the two different techniques.

It can be noted that the cipher letters E, F, and G in the second alphabet are under the plain letters R, S, and T. This indicates that they are also lined up that way in the original table so we start our building-up from there:

Illustration No. 1

(p) - R S T
(c1) - G I
(c2) - E F G
(c3) - U R S

This expands immediately to:

Illustration No. 2

(p) - R S T
(c1) - E F G I
(c2) - E F G I
(c3) - U R S

There being no E in (c1) and no I in (c2) we shift to another section for attack: In (c2) and (c3), W(c2) is over K(c3) and V(c2) is over J(c3). These low frequency letters are likely to be adjacent in a keyword sequence:

Illustration No. 3

(p) - O M
(c1) - W
(c2) - V W
(c3) - J K

This expands to:

Illustration No. 4

(p) - L O M
(c1) - V W
(c2) - V W
(c3) - I J K

The I in (c3) connects the second group to the first and expands it to:

Illustration No. 5

(p) - D I L O M
(c1) - P V W
(c2) - N O
(c3) - E F G I J K

X(c2) and L(c3) under A(p) indicates that it follows after M(p) and that the keyword is DIPLOMAT or DIPLOMATIC, etc., in the plain component. Further building-up gives:

Illustration No. 6

(p) -	D	I	P	L	O	M	A	C	Y	B	E	F	G	H	J	K	N	Q	R	S	T	U	V	W	X	Z
(c1) -	O	P		V	W	X	Z	T	H	U	R		D	A				E	F	G	I					
(c2) -	N	O	P		V	W	X	Z	T	H	U	R		D				E	F	G	I	J	K			
(c3) -	E	F	G	I	J	K				P		V	W	X	Z	T	H	U	R	S						

The plain keyword is revealed as DIPLOMACY and the cipher keyword as THURSDAY.

ASSIGNMENT No. 5

Problem No. 1

From: JZ (CinC BLACK). ØØ16-1615
To : OK (COLLECTIVE CALL). 16 April 193Ø

DGHKT WFYFJ NVHKC JEAXH ZIJMF RXPQB HXNIO VPVIH IEGJB UZUUC VWHUA

BEDQC EEGIT WWVFB WXHFQ SIFRP XZHLS ZEGAW VAHFC CDVZB OZYVY SFGHJ

YHQQH ZXGOB NCULT YCIIP MSJLP MSJLB UCRKP ZDYKQ VKVGP HXOJC EEGXW

EWTVH SWJMX VVHOB NLVFB YCDKB OJPOJ BXUUC EEGGW VAHFC VXGUF NFPGC

DGDXX TCUQS VDYKZ VZUUZ FMPXB TCVFX DVIGC DGDJJ GZVFD SWCGC NFXQS

MDYKZ VIEMO WZYDT NVTXT UZOFT TEDOJ BKYFZ VWJKT WXOFQ NXJQA VMHRJ

NXCUA FCGTF NXRUA VZYYF EWWUP UMYTL SZCUL ZFTPC VFTPC VXGUF NFPNM

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
(1) -		3	1	4	5	2	1	2	1	1			3	10	2			1	5	3	4	15	5	1	3	5
(2) -	2		7	4	8	7	3	1	3	1	2	1	3			1			2			4	7	12		9
(3) -	1		3	5	1	1	10	9	2	6				1	3	5	1	2		4	5	7	1	1	9	
(4) -	1			1		11	5	1	4	3	8	4	3	1	4	2	6	2		2	10	2		5	1	1
(5) -	4	10	12	1		4		4		7		2	1		2	6	3		3	7			3	3	1	4

Problem No. 2

From: CRUISER DIVISION COMMANDER. Ø5Ø515 MARCH
To : CRUISER DIVISION (HOUSTON, AUGUSTA, CHICAGO).

PIDHI YACSQ TQKVK IXFVW YQJMB AHQBA QZSAJ BKGRA ROGHF NQMGA QPNMB

EIARD LZOAS BQCCK IHEMM NXNHK LOGDK PJCCO YQMBF BXCEK IKEZA LTMZQ

NJNYM NCMXX BWKZY BQNYP BCMCW PNMCD AOGZA AIBHX YJNBF RGZHH YYXLF

IWBXM EWPPK QIEAF MSIAF JHGKN PZMFQ NTIKD EWZBI RLFXB RKFCQ YBBRV

ROKLV PIDHI YQCCK FBGGI BUJMB AHQBU JHSCH FLWLF BAGCJ QWIVH FQFVE

FOORA RQCCK RWMCJ PARZQ NJNYN LICRP BCMCE BWGMN LUBHJ PIKLI HJMOD

NQJMB AHQBL

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
(1) -	5	10			3	4		1	4	2		6	1	7		7	3	7		1					7	
(2) -	3	2	3				1	6	6	5	3	1		1	5	1	10		1	3	2		7	3	2	3
(3) -	2	4	7	2	2	4	7		3	3	6		10	6	3	1		3	1	2			1	1		2
(4) -	4	5	11	2	1		2	7			2	4	6		1	1		5	1			4		4	3	5
(5) -	6	5		5	2	6		3	6	4	8	1	3	3	1	3	5		1		1	2	2	2	1	

ASSIGNMENT No. 5

Problem No. 3 Serial No. 1

From: AB.
To : CD (COLLECTIVE CALL).

PYAVG GRLIV KDMFT VFSXV ONOWB SBNOW PAHHA ZWTVI TXOTO OYGDB OUYJR

LIVFL TYCPT SNSHS NVXDW UFADL WUSUP AZHNA WDTRH CUTJV AXXNZ ONFMN

NOOCP AHWAC NIAVG GRLIV HGWYE CLPXW ONLGU GOPSS DNGAD GMYVT YXDSS

VNLUQ VKTLT VMIZM SDLRI QXAKV

Problem No. 3 Serial No. 2

From: EF (UNIT CALL).
To : AB.

XAOLR MNGFN NUDOM DKCXF DVNSN AKMAW RLIVE WWSHH OCPAZ STIGL GVOXO

TOOSL XYUMH AQTVA YADZH VYFXA ZZHAQ TLWAB WTHTS DWOOV OCNQV STCAG

OVKDM FTVFT XGMMF DMNDA TGOTN CLSXF BVIGH DGMZB YWONL GUNSL NAMYV

HAAMJ FMZSY TVUFX OTOOU

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
(a)	1	1		6			1	1					7	5	4	5	2	4	1		2	4		6	11	2
(1)	8	1		4		4	4		1	1		6		5	2		2		4	10			2	2		6	1
(2)	2	2	1	2	1	2	3	6	4	1	2	2	3	2	11				2		3	1	7	2		4
(3)	3		2	1				4	2		1	2	5	5	5	2		2	3		2	4	16	2		1
(4)	6			1	1	4	2	4	2		4	4		7	6	1		1	4		6	1			5	3
(5)	7	2	7	4			2	9			1		5	2				1	1		6		1	2	1	4	5	1
(6)																										

Problem No. 4 Serial No. 1

From: COMMANDER BATTLE FORCE. ØØ611ØØ MARCH
To : COMSUBRON ONE. COMSUBDIV SIX.

KBYSA DORSD RPOHZ KTUEC QKPDK BRRPO RBPML LKRRN YOHWS HATOR SDRPJ

PMDAN LXIOV YUBRU ADLXH SUKUP UKAUA BDSCO TMFHA LEHGU CFKWT

Problem No. 4 Serial No. 2

From: COMSUBDIV SIX. ØØ614ØØ MARCH
To : SEALION. SEAWOLF. SAURY.
Info: COMSUBRON ONE.

OBUCR GEOPD BDHNQ CWNLQ UKCHV HQKBU CGEGQ JLAMH VNHZR HEGTM YRFJF

PFVWY VWUCO FLXRP TKKOV WBDHN QCWBN OBMOJ DBBZB ZVHBR JTOBU CRGEN

HZVHV OAMRE HULZN

ASSIGNMENT No. 5

Problem No. 5

Peshawar, India, August 13, 1930. Peshawar is a British Indian Army Post guarding the Khyber (Khaiber) pass, the gateway between Northwest India and Afghanistan. It is fortified against periodic attacks by Afridi Tribes.

RLWFN PPQQA JUVMZ DMIUK YKUZO SEMUE GXQCF SUEBI ZPUSI CUEDU SZSQH

FUTJV MNIYK AUNAT IPQWB APWDZ ITEPZ HIBBQ LEOQS WNRHH ZYNAX BKUIP

XKUCA HIHMU EUPAL CUTRV DXKEQ RIKYP FHFWE VWAEA XQXKU ICICZ WKTWJ

BHUSH IBBQL ZDEGB WAEQR KUVBG EGTBR DCTOF DXKUH OPZVD VKCIW ZEKSN

IMZHR LWQAK JBAZC TLRYH LANAR YKOKI XYFUF SWRDE CQSWN RHHZN PEAYX

OXYPL ELABM DJBGT CKZWC XWFMV FXKRC XXKEA QSWNR HHZVW MFCXF EKYJY

HIBBQ LJUIV WGJPU WGYYF XHIBI ZRWBO JNMGU BWXAX DUPNW WZHAI IAYHD

VHREB TFCKR IUVBB TQSWN RHHZO UVCUB VEMKJ YKFZQ ZNCTW JMNRR GCSGH

FSZCV GNAZL WICHU STWTY AHUTA FMNJM HISOE YRDIA YSKSJ WPVEP ZZAFN

KCYKX XBGUU

Problem No. 6

From: COMMANDER CRUISER DIVISION SIX. 24Ø93Ø APRIL
To : CRUISER DIVISION SIX.

ZXALK WTHMG PPEUG DQVIG HUUPM WBUZQ BTOYF PJYZF LXAOS XPEUG ZFQUA

AKWLV KCLJI TBESX HZNZL JJUGD SGRGZ XXXMW ZHQVA AMGHN QUAAK WLVKZ

BRKPA ZJAWP OYCFO OXPHC LJITB ESXHG HVNWR AJXHS LUZAM ZRUZS NUXNQ

VAAMG HLSSB JAUAP AVUVF QYVOR GPLVY YJLZJ RAWZH EYYVP FTQXL

(Collateral Information: It is believed that the cruisers Marblehead, Raleigh, Concord, Cincinnati and Trenton are in Division Six.)

It is necessary 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. 6

SLIDING STRIPS, CIPHER DISKS, AND SQUARE TABLES

1. It has been noted that secondary cipher alphabets may be derived from an original or primary cipher alphabet by shifting its cipher component relative to the plain component. Also, that components of cipher alphabets consisted of either normal or identical mixed sequences written in the same or in opposite directions, or their components consisted of different mixed sequences.

2. In a polyalphabet substitution system the components of the original cipher alphabet may be placed on sliding strips for convenience in shifting them to the desired points of coincidence as designated by the key in effect at the time. Cipher wheels or disks will accomplish the same result in a somewhat more convenient form, since the sequences are written in a circle and therefore coincide continuously throughout their length. Cipher disks consist of a rotating disk, the circumference of which is divided into 26 equal segments carrying one of the sequences, and a stationary disk, similar but slightly larger carrying the other sequence, upon which the rotating disk turns concentrically.

3. A square table contains all the cipher alphabets which result from the sliding of strips or rotating of disks carrying the components of the alphabet. Square tables are often called "Vigenere Tables" after the French cryptanalyst who first advocated their use. The conventional form of square table is constructed as follows, using the keyword PYTHAGOREAN:

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

ASSIGNMENT No. 6

This square table represents the cipher alphabets resulting from the shifting of identical sequences, written in the same direction. The top line contains one component while the other 25 lines contain the various relative positions which the sequence occupies in forming the secondary cipher alphabets.

A square table representing the results of sliding different sequences, or identical ones written in opposite directions, must have a line added at the top to contain the other component.

4. When sliding strips, cipher disks, or square tables are employed in multiple alphabet or non-periodic cipher systems, the cipher value which coincides with the initial letter of the plain component is usually the "key" to the particular cipher alphabet designated for use. Thus, the left hand column of a square table contains the key values.

REGULAR PROGRESSIVE-ALPHABET CIPHERS

5. When the 26 cipher alphabets of a square table are used in regular order to encipher successive plain-text letters, (the same effect as sliding strips or rotating disks one letter at a time) the system is called a regular progressive-alphabet cipher system. Although regular shifts in amounts greater than one step at a time are also regular progressive cipher systems, the components of the cipher alphabet could be respaced to reduce the shift to one letter, between the encipherments of successive plain letters.

6. The encipherment of a message by a regular progressive alphabet cipher system, using the square table of paragraph 3, would appear as follows:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
M	Y	P	O	S	I	T	I	O	N	L	A	T	I	T	U	D	E	T	W	E	N	T	Y	T	H
M	T	T	N	X	Q	E	U	I	M	Y	J	I	Y	K	B	T	Z	S	K	T	A	X	X	P	T

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

N	T	Y	T	H	R	E	E	D	A	S	H	T	H	I	R	T	E	E	N	A	T	S	E	V	E

N	H	H	G	R	D	I	J	S	F	A	L	I	K	T	V	M	Z	P	T	X	W	K	G	S	R

N	T	E	E	N	H	U	N	D	R	E	D
N	H	B	C	F	E	Y	K	S	K	M	W

The numbers at the top of each column designate the line of the square table which was used as the cipher component for enciphering the plain letters of that column.

Note that repetitions in the plain text do not produce repetitions in the cipher text unless they occur at an interval which is a multiple of 26.

SYMMETRICAL SEQUENCES

7. If the same plain-text letter is enciphered by the successive lines of a square table, the resulting cipher values are those of the cipher component in its original order. Therefore, the corresponding cipher values of a plain-text repetition will be found separated by the same interval in the cipher component as in the text of the message. These series of cipher values which have a direct space-relationship in the cryptogram and the cipher component are called symmetrical sequences. The space-relationship between the corresponding letters of symmetrical sequences becomes the interval between the columns into which they fall, when the cryptogram is written in lines of 26 letters

Symmetrical sequence:	X	X	P	T	R	N	B	J	E	Z	N	N
	H	H	G	R	D	I	J	S	F	A	I	I

The corresponding letters of these symmetrical sequences (taken from the cryptogram of paragraph 6) are at intervals of five columns, and they will be found at intervals of five in the cipher component. This may be verified by reference to the square table of paragraph 3. The use of this space-relationship in reconstructing the cipher component will be demonstrated later.

8. Symmetrical sequences can not be readily recognized in an unsolved cryptogram unless some of the cipher values are repeated, such as those underlined in the example of paragraph 7. The symmetry of the other cipher values resulting from plain text repetitions becomes evident only after the cipher component has been partially reconstructed. Chance may cause a few values in a cryptogram to have the outward appearance of a symmetrical sequence, yet these may not be the results of plain-text repetitions. Symmetrical sequences are also found in cryptograms enciphered by other types of cipher systems and are valuable aids in their solution.

SOLUTION OF A REGULAR PROGRESSIVE CIPHER

9. The problem:

J Z S S W B P D Z Z L F O M E K Q P D J H C K U M C

A B C O O X M Y S I I G B S G G Y V D S W A J O Q E

K U P W K N J K C C H W O Z Q Q B P Y N V J J O Q E

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

D H U V N K V K C Y Y A L R Q O O Q D N Z C G L R E

K F H Q R N J B

The text of the problem appears in lines of 26 letters, which was determined as the key length by the process of factoring.

10. If standard cipher alphabets had been used in this problem, the solution could be obtained by the method of completing the plain component. In applying this method to regular progressive ciphers, the plain text appears on a diagonal line due to the shifting of the cipher component, instead of the horizontal line in the case of monoalphabet ciphers. Also, if sufficient text had been given, this problem could be solved as a 26 multiple alphabet cipher. However, the special method for solving regular progressive ciphers, by the reconstruction of the cipher component from symmetrical sequences, will be demonstrated.

11. The symmetrical sequences found, with their space-relationships in the cipher component, are as follows:

(K U) M C A B C O O X M Y S I I -- 5
(U P) W K N J K C C H W O Z Q Q

C D S L R W C (F Q I) -- 22
R E K F H Q R (N J B)

S S W B P D Z Z -- 7
Y Y A L R Q O O

The letters in parentheses may be assumed to belong to the symmetrical sequences, but their positions in the cipher component must be checked with other good values.

12. The reconstruction of the cipher component progresses through the following steps:

ASSIGNMENT No. 6

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	Interval
						O																			Z	7
	Y					O					C					K				S					Z	5
			H				R				C															22
			H																					X		5
P							R																			7
P	Y		H			O	R				C					K				S				X	Z	Combined
P																K				S	U			X	Z	5
										B					J		L									Assumed
								N		B			F	I	J		L		Q.				W			22
			A					N										M					W			5
												D							Q							7
							E					D														22
P	Y	(T)	H	A	(G)	O	R	E	N	B	C	D	F	I	J	K	L	M	Q	S	U	(V)	W	X	Z	Combined

This complete reconstruction of the cipher component was aided by the fact that it is a keyword sequence, but partial reconstructions could also be used to advantage.

13. Now that the cipher component is recovered, the cryptogram can be "converted" to the basis of one cipher alphabet. This conversion process makes use of the known shift between the components of the cipher alphabet, thus reducing each letter of the cryptogram to its equivalent value had the components not been shifted during the encipherment of the message.

14. In order to make use of the known step-by-step progression, the cipher component must be shifted as in a square table. The square table for this problem is that given under paragraph 3. The cryptogram could be converted to the basis of the cipher sequence itself in the position it occupied during the encipherment of the first letter of the message. Thus, the first letter remains as "J", the second becomes "X", which is the letter of the first line of the square table above "Z" of the second line, etc. The first two lines of the problem with the converted values and plain equivalents found by solving of the monalphabet substitution are as follows:

Line 1 ----- J Z S S W B P D Z Z L F O M E K Q P D J H C K U M C
Converted -- J X M L Q G S G L K R T S G S Y H N S V N K S X S D
Plain ------ M Y P O S I T I O N L A T I T U D E T W E N T Y T H

Line 2 ----- A B C O O X M Y S I I G B S G G Y V D S W A J O Q E
Converted -- A N N H T Q D S D G A S X R L K C G S Y H N Q N U N
Plain ------ R E E D A S H T H I R T Y L O N G I T U D E S E V E

15. It should be necessary to convert only a few lines of any problem to have sufficient text to solve the monoalphabetic substitution. The plain sequence can then be written as an extra line above the square table and the message deciphered by taking the plain values off directly instead of the values in the top line of the square table. The primary cipher alphabet for this problem is:

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

These sequences are constructed from the words QUADRICULAR and PYTHAGOREAN, which are two other names for a square table.

ASSIGNMENT No. 6

Problem No. 1 Naval Text

A U V Z I S Z F B F Y E I R B I O W A O Y J L B L D

D G K U I T T Z B D B E Q I O C J R F W X D Y H G M

S P P I S W Y P F V S Y G G S H Q K L A L Z A Q F N

U T C Q H D G Y L B Z P D V C S J N W G N T P T M S

H J T W C K O C M X Z P Z R R U Y I W H H M E Z F L

O O F I S W L P D N W T Z H H T I R L Y I P N Q F N

U T C Q H D G Y L B Z P D V C S J N W G N T P T M E

O S V B W J B L V X Z P Z R R U Y I W H H P L P F T

R B P G X B U L V N W J P R G I H F Q X L N B L P S

H J T W I J T T Q W E E Q F O I I Z P M B J Q P Y M

D U Q W A T Z O W D C L Z Q M P H U K

Problem No. 2 Naval Text

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

E H V X G A B L U J B K Q P Z P Z U R T Q I E M P D

R Z V Z S G K B B Q J F U U R I V R F F Y H R I N R

A U Q L F J S K P Q J E A P X A J X W J Y E X P L O

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

E P B A G K J R H G B N J W Q X Z U U O Y W E E B K

I B W W A C J R Y G Q U F V X O U D U G U J X Z Q I

A B I J S V W K H P B V M U V N Z U W T S R W H E D

C D C S F I E P M O D K F C R P M B J V B R I P P D

S N V T A G K L M Q X K J Z R P M B M I Z M R Y Q A

D H S S O G S B J

Problem No. 3 Naval Text

A W H V Q J R H I A L C Q K D O C W O G V X H T X B

G V F A V D G A G G X R B K N A J I Z A G L K P V C

E E G P B C E W J Z O D M K M K S J X H H R C Q B H

T H G F W F M L G O U T N M B O G T P L O S M R X T

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

T M D O Q Q Y M Z O Q F A K L P N T N T B A H R R S

O G Z R V R Y E F E N

ASSIGNMENT No. 6

Problem No. 4 Naval Text

14 April 1930 -- Fleet Tactical Exercises. Forces not in contact.

FROM: AB (FORCE COMDR IN BLACK FLEET)
TO : CD, EF, GH, IJ (CALLS NOT IDENTIFIED)
INFO: YZ (COMDR BLACK FLEET) Time groups: 0014-1600

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

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. 7

SIMPLE ROUTE TRANSPOSITIONS

1. Transposition ciphers have been defined as that type in which the elements or units of the plain text, whether one is dealing with individual letters or groups of letters, retain their original identities but merely undergo some change in their relative positions or sequences so that the message becomes unintelligible. The majority of transposition methods involve the use of a design or geometric figure, such as a square, rectangle, triangle, etc., in which the letters of the plain text are first inscribed or written according to a previously agreed upon direction of writing and then transcribed or taken off according to another and different previously agreed-upon direction, to form the text of the cryptogram.

2. The simple routes employing rectangles for transposing the text of a message are illustrated below. The plain text message is assumed to be merely the normal sequence from a to x, for ease in following the route.

(a) Simple Horizontal:

ABCDEF	FEDCBA	STUVWX	XWVUTS
GHIJKL	LKJIHG	MNOPQR	RQPONM
MNOPQR	RQPONM	GHIJKL	LKJIHG
STUVWX	XWVUTS	ABCDEF	FEDCBA

(b) Simple Vertical:

AEIMQU	DHLPTX	UQMIEA	XTPLHD
BFJNRV	CGKOSW	VRNJFB	WSOKGC
CGKOSW	BFJNRV	WSOKGC	VRNJFB
DHLPTX	AEIMQU	XTPLHD	UQMIEA

(c) Alternate Horizontal:

ABCDEF	FEDCBA	XWVUTS	STUVWX
LKJIHG	GHIJKL	MNOPQR	RQPONM
MNOPQR	RQPONM	LKJIHG	GHIJKL
XWVUTS	STUVWX	ABCDEF	FEDCBA

(d) Alternate Vertical:

AHIPQX	DELMTU	XQPIHA	UTMLED
BGJORW	CFKNSV	WROJGB	VSNKFC
CFKNSV	BGJORW	VSNKFC	WROJGB
DELMTU	AHIPQX	UTMLED	XQPIHA

(e) Simple Diagonal:

ABDGKO	GKOSVX	OKGDBA	XVSOKG
CEHLPS	DHLPTW	SPLHEC	WTPLHD
FIMQTV	BEIMQU	VTQMIF	UQMIEB
JNRUWX	ACFJNR	XWURNJ	RNJFCA
ACFJNR	JNRUWX	RNJFCA	XWURNJ
BEIMQU	FIMQTV	UQMIEB	VTQMIF
DHLPTW	CEHLPS	WTPLHD	SPLHEC
GKOSVX	ABDGKO	XVSOKG	OKGDBA

(f) Alternate diagonal:

ABFGNO	GNOUVX	ONGFBA	XVUONG
CEHMPU	FHMPTW	UPMHEC	WTPMHF
DILQTV	BEILQS	VTQLID	SQLIEB
JKRSWX	ACDJKR	XWSRKJ	RKJDCA
ACDJKR	JKRSWX	RKJDCA	XWSRKJ
BEILQS	DILQTV	SQLIEB	VTQLID
FHMPTW	CEHMPU	WTPMHF	UPMHEC
GNOUVX	ABFGNO	XVUONG	ONGFBA

(g) Spiral Clockwise:

ABCDEF	LMNOPA	IJKLMN	DEFGHI
PQRSTG	KVWXQB	HUVWXO	CRSTUJ
OXWVUH	JUTSRC	GTSRQP	BQXWVK
NMLKJI	IHGFED	FEDCBA	APONML

(h) Spiral Counter-Clockwise:

APONML	NMLKJI	IHGFED	FEDCBA
BQXWVK	OXWVUH	JUTSRC	GTSRQP
CRSTUJ	PQRSTG	KVWXQB	HUVWXO
DEFGHI	ABCDEF	LMNOPA	IJKLMN

3. The letters of the plain text may be inscribed within the cells of a rectangle according to one route and taken off by another route to form the cipher text. If the rectangle is not completely filled by the plain text, "nulls", that is, dummy letters having no significance, are usually inserted in the vacant cells.

ASSIGNMENT No. 7

Example -- Let the message be:

AT FOURTEEN HUNDRED SIGHTED SUBMARINE BEARING TWO THREE FIVE DEGREES TRUE.

Suppose it has been agreed to use a completely filled rectangle of eight columns, then it is necessary to add one null to make the total number of letters in the message a multiple of eight (64 letters). A rectangle of 64 cells, 8 x 8, is prepared, and the plain text inscribed according to an agreed-upon route, in this case alternate diagonal:

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

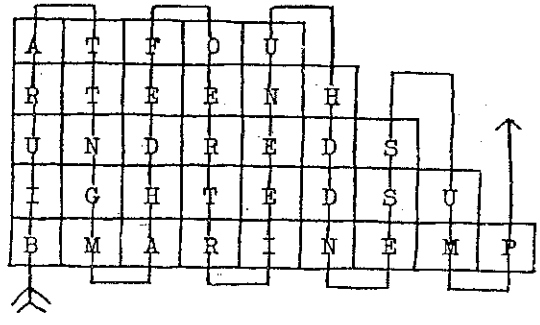
Next, the letters are taken off by an agreed upon route, in this case simple vertical, to form the cryptogram:

AFONH HTATU EUGEE RRENI DBIFT DSSEN EIRDU
NGEVE EBITR EESMR WHDRT EAOTE GRUN

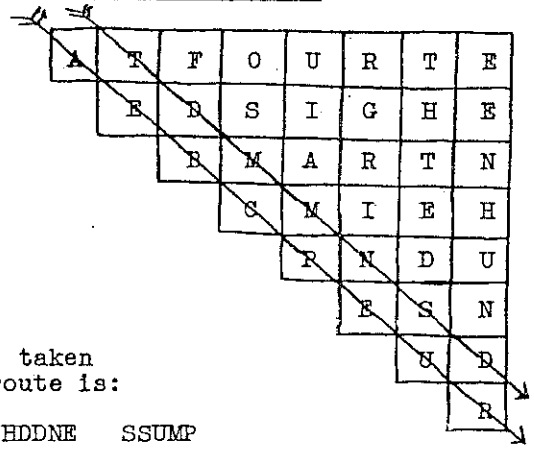
To decipher such a cryptogram the process is reversed. First, the total number of letters in the cipher text must be found, and the rectangle constructed accordingly. Then the cryptogram is inscribed by the agreed-upon route and the plain text taken off by the other agreed-upon route.

4. The routes illustrated for transposing messages by inscribing them within rectangles may also be applied to other geometrical figures, with minor modifications in some cases. Two practicable types of figures are illustrated below:

(a) Trapezoidal Design:



(b) Triangular Design:



The cryptogram resulting from figure (a) taken off according to an alternate vertical route is:

BIURA TTNGM AHDEF OERTR IEENU HDDNE SSUMP

That resulting from figure (b) taken off according to a diagonal route is:

AEBCP EURTD MMNSD FSAID NOIRE UUGTH RHNTE E

ASSIGNMENT No. 7

KEYWORDS AND NUMERICAL KEYS

5. It is often necessary, in performing certain cryptographic operations, to employ a numerical key, which may consist of a relatively long sequence of numbers difficult or impossible for the average cipher clerk to memorize. A literal key, consisting of either a single letter, a single word, a phrase, a sentence, or more, may be converted into a numerical key by numbering the letters of the literal key in alphabetical order. If there are two A's, 1 is assigned to the first A and 2 to the other, and if there are no A's, 1 is assigned to the letter next in alphabetical order, etc.

Example -- Literal key ------- A M E R I C A N
Numerical key ----- 1 6 4 8 5 3 2 7

6. The cryptanalyst may be unaware of the fact that a literal key has been employed as the basis for deriving a numerical key. The recovery of a literal key is a comparatively simple matter once the method of its employment is known. Letters near the beginning of the alphabet are assumed for the low numbers in accordance with their alphabetical order. Often more than one literal key may be found to fit a given numerical key, but the cryptanalyst is not usually concerned as to which key was used originally. For this reason, literal keys are not required in the solution of assignments in this course.

7. A numerical key may be employed as follows in transposing the letters of a message:

7-2-4-5-3-6-1	7-2-4-5-3-6-1	7-2-4-5
R E P O R T N	O O N P O S I	T I O N

The letters are taken from the above groups and transcribed in groups of five, all letters marked 1 being taken first, then all those marked 2, etc.

Cryptogram: NIEOI ROPNO OPNTS ROT

The above type is more properly discussed under Columnar Transpositions, which are covered in the next assignment.

MISCELLANEOUS TRANSPOSITION METHODS

8. The oldest and simplest transposition method is reversed writing. The reversing process may be applied either to regular or to irregular groups of plain text letters.

Example: Plain ---------- PREPARE TO GET UNDERWAY
Cryptogram ----- (digraphs reversed):
RPPER ATEGO TENUE DWRYA

9. Another simple type of transposition is called "rail-fence" writing because it is produced by writing the message in this form:

P E A E O E U D R A
R P R T G T N E W Y

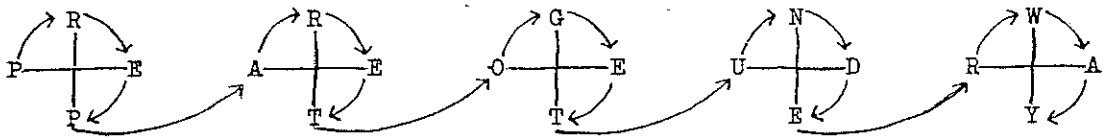
The cipher text is taken from the horizontal lines to yield this cryptogram:

PEAEO EUDRA RPRTG TNEWY

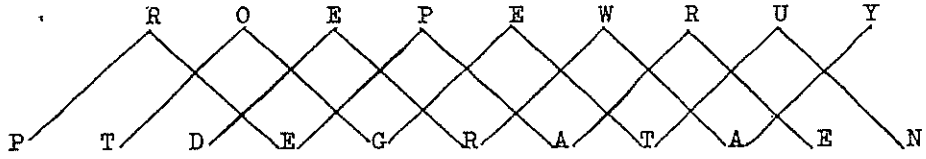
Both reversed and rail-fence writing are in reality special cases of the simple route transposition previously described.

10. In order to demonstrate the use of miscellaneous designs for performing transpositions, two methods are illustrated below:

ASSIGNMENT No. 7



Cryptogram: RRGNW PEAEO EUDRA PITEY .



Cryptogram: ROEPE WRUYP TDEGR ATAEN

11. From the foregoing examples, it is obvious that many other figures may be used for effecting transpositions of this kind, such as stars of varying numbers of points, polygons of various symmetrical shapes, etc. It is merely necessary to agree upon the figures, the number of figures per line, and the starting points of the inscription and transcription processes.

SOLUTION OF ROUTE TRANSPOSITION CIPHERS

12. When but one cryptogram is available, the solution of a route transposition cipher is largely a trial and error method. A study of the cryptogram will often show which routes are the most likely ones for experimentation. Some of the points to be noted in this preliminary study are:

(a) The beginning and end of the cryptogram. The most frequent initial letters in English are T A W O B I C S D H in the order named, and the most common endings of words are E T S D N R Y O F L in the order given. Words may be assumed which contain the letters found near the beginning or end of the cryptogram and evidence discovered as to the transposition system used.

(b) The intervals between the letters of expected words, high frequency digraphs, etc. Counting the intervals between letters which could form expected words or high frequency combinations will often give an indication of the system used. Q in English is always followed by U which in turn is followed by another vowel.

(c) Long groups of vowels or consonants. When English is written horizontally and transcribed vertically there are often long groups of vowels and consonants which appear in the cipher text, and which may be assumed to be adjacent in solving cryptograms of this type. Nearly 62% of the digraphs in English text are either vowel-consonant or consonant-vowel arrangements.

(d) The presence of parts of words. Certain routes, such as spirals, may leave parts of the plain text either in its original or reversed order, and thus aid the cryptanalysts materially in his determination of the type of transposition used.

13. If the preliminary study fails to indicate the proper procedure, the solution of a simple route transposition cipher can be achieved by writing the cryptogram in various ways within figures whose dimensions are suggested by the total number of letters in the message. It is unnecessary to try all the routes given under paragraph 2, because the same result is obtained by inspection

of one trial figure of each type for portions of words reading horizontally, diagonally, vertically, spirally, etc. In some cases employing diagonal routes no experiment is necessary with regard to the dimensions of the figure, since the letters at one end of the cryptogram will serve to build up a corner of the figure. The methods of solution described above are sufficient for the simpler routes, and when they fail, a more complicated route is indicated which may require two or more messages of equal length for a method of solution to be described later.

PROBLEMS FOR ASSIGNMENT No. 7

Problem No. 1 Naval Text

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

Problem No. 2 Naval Text

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

Problem No. 3 Naval Text

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

Problem No. 4 Naval Text

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

Problem No. 5 Naval Text

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

Problem No. 6 Non-Naval Text

D I A G T O E H T Y E A O P S O P S N A R T I H L N I O T E

ASSIGNMENT No. 7

X L H I N S C H A N G E T R I Y C T T E T H H V I C N O I T

E V G D F E P T O E N G E M E N R R L I N F L I T C N I S R

E E E T R L S N I A L A O N M I O E T N O N I N H S A E O R

Problem No. 7 Non-Naval Text

M E O H S B T T S E F D K F Y O I S O L S E F A R A T O N F

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

E T H C Y E C O E O T E R C E R R C N P R O R S C I I R E I

R W H P S O H N G H C H T C P G N B I E X E I A I Y O R E S

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

A H P

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. 8

ANAGRAMMING

1. The most powerful method which can be used in the solution of transposition ciphers is "anagramming." There are many minor variations included by the term anagramming. Basically, however, anagramming is the process of rearranging a group of letters to form another sequence of letters which are intelligible. For example, the words EDDIE CANTOR may be anagrammed with this result -- ACTOR INDEED. As applied to transposition ciphers, anagramming of the cipher text letters to form plain text may be possible with a single message, but there may also be nothing to indicate that the assumed plain text is correct unless the system used is very simple.

KNOWN WORD METHOD

2. Suppose, however, there are available two cipher messages of the same length in the same transposition pattern. Lining up two such cipher messages under each other, we can say that the letters of a plain text word in the upper message will have plain text under them in the lower message, and vice versa.

For example:

Cipher Posn.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Msg. #1 --	M	O	K	E	T	A	D	E	D	E	I	Y	S	F	E	N	T	P	I	N	B	A	E	F	L
Msg. #2 --	A	N	O	R	O	T	T	H	E	C	T	Y	U	D	E	W	T	N	P	E	E	W	D	R	D

Let us now assume a word in the upper message and see what can be anagrammed underneath it.

Assume in Msg. #1	S	P	E	E	D
Position numbers of such	13	18	4	4	7
letters in Msg. #1			8	8	9
			10	10	
			15	15	
			23	23	
Corresponding letters	U	N	R	R	T
in Msg. #2			H	H	E
			C	C	
			E	E	
			D	D	

ASSIGNMENT No. 8

25
8 13 18 23 4 9 14
(H) U N D R E (D) then becomes evident. The student should complete the solution of this pair of messages by extending the anagramming process both forwards and backwards from HUNDRED. Think over, for future use, the significance of the additive "5" which is apparent 8-13-18-23-4-9-14 series.

IDENTICAL WORD, IDENTICAL LOCATION

3. Take two other messages of identical lengths and systems:

Cipher Posn.-	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Msg. #1 --	V	I	L	N	C	I	L	O	D	E	S	I	W	F	S	I	T	W	O	I	B	Y	I	R	X
Msg. #2 --	V	I	U	I	O	I	L	N	T	W	S	I	L	E	I	I	T	I	D	N	B	Y	M	N	D

Note in this case the excessive number of coincident letters between the two messages. Compare this with the previous example. Pure chance would give one coincidence in a message of this length, and over four or five would give a strong suspicion that the same word or words had been used at the same plain location in both messages.

Here the coincident letters are V I I L S I I T B Y, which can be anagrammed into V I S I B I L I T Y.

The student should complete the solution of the above, and also anagram in a similar fashion for practice -- A M D I Y O N B, R D E E Y S O T R and R N T E D O H Z R D A E U.

4. Note the regularity, also, of the underscored coincidences in the two equal length cipher messages above. Even in unequal length messages of the single columnar type, repetitions rather than coincidences between two messages in the same key are common. When present and underlined they form a diagonal pattern which is quite characteristic of that type of cipher and useful for assuming possible key lengths. They are caused by the same key cutting through identical words or phrases in both messages.

COLUMNAR ANAGRAMMING

5. Another variety of anagramming is columnar anagramming. For instance, assume a message contains one Q and two U's. The Q undoubtedly goes with one of the U's, unless it is a null, garble or part of a code word. Let us line up the letters following the Q with the letters following the two U's to see which makes the better looking set of digraphs.

Qu - 3	Qu - 3
St - 23	Sr - 1
De - 15	Dt - 6
Hr - 7	Hp - 1
Pl - 5	Px - 0
Er - 43	Eo - 6
At - 31	Aa - 1
127	18

The left hand column is undoubtedly the best looking. To make this clearer let us put the normal digraph frequencies beside the various digraphs and total, as above. The comparison of 127 with 18 is quite conclusive.

ASSIGNMENT No. 8

6. To obtain a start on this type of anagramming the more invariable combinations are the best with which to experiment. The digraph QU is the best English combination to try because Q and U are of low individual frequency. High frequency digraphs, such as TH, are good although there may be so many T's and H's that the exact letters which go together are not so easily determined. Combinations which form part of expected words in the kind of text involved are excellent naturally as the basis of the anagramming process. TW, JO, CK, CH, WO, WE, IX, ZE, TY are useful digraphs for this purpose in English.

COLUMNAR TRANSPOSITION METHODS

7. Columnar Transposition is a variation of the simple vertical or horizontal route transpositions discussed in Assignment #7, the variation being in the taking off of the columns or rows in an irregular order instead of in regular succession. The simplest type of columnar transposition uses a completely filled rectangle; a more complicated type uses an incompletely filled rectangle; and the so-called double transpositions are still more complicated with the use of columnar methods twice in succession, perhaps with different keys or different rectangles.

8. A literal or numerical key may be used to designate the irregular order desired for taking off the columns to perform a columnar transposition. While in practical work a complete analysis to discover the literal key as well as the numerical key would be desired, the deciphering numerical key will be considered sufficient for the problems in this course.

9. Columnar transposition methods are susceptible of considerable variation. The key may be changed automatically with the time of origin of the message, or it is possible to prepare a long list of suitable keys and to designate the key used by an "indicator" which is inserted in the cipher text in a prearranged position. Another variation is possible by changing the direction of the inscription or the transcription processes, using any of the routes indicated in Assignment No. 7.

COMPLETELY FILLED RECTANGLES

10. When a transposition system requires that the rectangle be completely filled, sufficient nulls would ordinarily be added at the end of a message to do this. From a communication security standpoint it should be mentioned that XXX are undesirable as nulls; preferable would be random-chosen nulls in accordance with the normal frequency table of English.

As an example of a columnar transposition, completely filled rectangle, consider the following:

Plain - FORM SCOUTING LINE ON COURSE NINE ZERO.
Key - 6 1 5 8 7 3 4 2

F	O	R	M	S	C	O	U
T	I	N	G	L	I	N	E
O	N	C	O	U	R	S	E
N	I	N	E	Z	E	R	O

Cipher - OINI UEEO CIRE ONSR RNCN FTON SLUZ MGOE

ASSIGNMENT No. 8

11. To decipher the cipher of the preceding paragraph, the first step is to prepare a rectangle with the proper number of cells. The number of letters in the cipher, in this case 32, is divided by the key length 8, resulting in the dimensions 8 by 4.

Cipher - OINIU EEOCI REONS RRNCH FTONS LUZMG OE

Key -	6	1	5	8	7	3	4	2
	O				C			U
	I				I			E
	N				R			E
	I				E			O

The letters of only the first three columns have been inscribed above. The complete message will reappear after the process has been completed.

INCOMPLETELY FILLED RECTANGLES

12. The difficulty of solution of columnar transposition is much increased if the rectangle in which the message is inscribed is not completely filled. The difficulties placed in the way of the solution are more than would be suspected as a result of so simple a change in method as that which merely involves leaving one or more cells vacant in the last row of cells in the rectangle.

An example of this method follows:

Plain - NO ENEMY CONTACTS MADE TODAY

Key -	4	6	1	3	7	2	5
	N	O	E	N	E	M	Y
	C	O	N	T	A	C	T
	S	M	A	D	E	T	O
	D	A	Y	T			

Cipher- ENAYM CTNTD TNGSD YTOOO MAEAE

This example also illustrates a procedure which ensures that the final five letter group of the cipher will be a complete group. The letters of the message must be counted and if their total is not an exact multiple of five, it must be made so by the addition of nulls, before the transposition process is applied.

In deciphering the number of letters in the above cipher (25) divided by the known key length, (7) determines the shape of the figure in which the text is to be inscribed, that is, three complete lines with a remainder of four letters on the last line as follows:

Key - 4	6	1	3	7	2	5
	E				M	
	N				C	

ASSIGNMENT No. 8

A T

Y

SOLUTION OF COLUMNAR TRANSPOSITION CIPHER

COMPLETELY FILLED RECTANGLES

13. Let us assume that we have a problem with the following cipher text:

REOUN ATLER RANSM LLNGR EUFWE BETAN OEFIY LSCAC GIBBI OEBEA
ULSIU NSOET EFXIF PRNRH

With 70 letters, our first assumptions are that a completely filled rectangle was used in enciphering our plain text. A 7-x-10, 10-x-7, 5-x-14, 14-x-5 etc., might have been used. To illustrate, a 10-x-7 rectangle is laid out.

1	2	3	4	5	6	7	8	9	10
R	L	M	H	A	L	B	A	S	I
E	E	L	F	N	S	B	U	O	F
O	R	L	W	O	C	I	L	E	P
U	R	N	E	E	A	O	S	T	R
N	A	G	B	F	C	E	I	E	N
A	N	R	E	I	G	B	U	F	R
T	S	E	T	Y	I	E	N	X	H

On the left side of the figure we write the line numbers in a vertical column. On the right side we put the vowel count for each line. Even with so few letters as 10 per line, our vowel percentage is pretty accurate. Thus with 10 letters per line we should have 40% or 4 vowels to the line. If we consistently have either too many vowels or too many consonants we can easily see that the assumed figure is incorrect. Our figure now looks like this:

Line No.	1	2	3	4	5	6	7	8	9	10	Vowel Count
1	R	L	M	U	A	L	B	A	S	I	4 = 40%
2	E	E	L	F	N	S	B	U	O	F	4 = 40%
3	O	R	L	W	O	C	I	L	E	P	4 = 40%
4	U	R	N	E	E	A	O	S	T	R	5 = 50%
5	N	A	G	B	F	C	E	I	E	N	4 = 40%
6	A	N	R	E	I	G	B	U	F	R	4 = 40%
7	T	S	E	T	Y	I	E	N	X	H	3 = 30%

The information on vowel count and the general appearance seems good, so we next try to line up to make plain text (anagramming). After several attempts we finally find our plain text and the deciphering key: ALL SUBMARINES OF BLUE FORCE WILL OPERATE ON SURFACE BEGINNING FEBRUARY SIXTEENTH and 5-2-6-9-4-7-3-8-1-10.

Other ideas for solutions will develop from the discussion of incompletely filled rectangles in the following paragraphs.

INCOMPLETELY FILLED RECTANGLES

14. Let us suppose that we have the following cipher:

ASSIGNMENT No. 8

A T

Y

SOLUTION OF COLUMNAR TRANSPOSITION CIPHER

COMPLETELY FILLED RECTANGLES

13. Let us assume that we have a problem with the following cipher text:

REOUN ATLER RANSM LLNGR EUFWE BETAN OEFIY LSCAC GIBBI OEBEA
ULSIU NSOET EFXIF PRNRH

With 70 letters, our first assumptions are that a completely filled rectangle was used in enciphering our plain text. A 7-x-10, 10-x-7, 5-x-14, 14-x-5 etc., might have been used. To illustrate, a 10-x-7 rectangle is laid out.

1	2	3	4	5	6	7	8	9	10
R	L	M	H	A	L	B	A	S	I
E	E	L	F	N	S	B	U	O	F
O	R	L	W	O	C	I	L	E	P
U	R	N	E	E	A	O	S	T	R
N	A	G	B	F	C	E	I	E	N
A	N	R	E	I	G	B	U	F	R
T	S	E	T	Y	I	E	N	X	H

On the left side of the figure we write the line numbers in a vertical column. On the right side we put the vowel count for each line. Even with so few letters as 10 per line, our vowel percentage is pretty accurate. Thus with 10 letters per line we should have 40% or 4 vowels to the line. If we consistently have either too many vowels or too many consonants we can easily see that the assumed figure is incorrect. Our figure now looks like this:

	1	2	3	4	5	6	7	8	9	10	Vowel Count
Line No. 1	R	L	M	U	A	L	B	A	S	I	4 = 40%
2	E	E	L	F	N	S	B	U	O	F	4 = 40%
3	O	R	L	W	O	C	I	L	E	P	4 = 40%
4	U	R	N	E	E	A	O	S	T	R	5 = 50%
5	N	A	G	B	F	C	E	I	E	N	4 = 40%
6	A	N	R	E	I	G	B	U	F	R	4 = 40%
7	T	S	E	T	Y	I	E	N	X	H	3 = 30%

The information on vowel count and the general appearance seems good, so we next try to line up to make plain text (anagramming). After several attempts we finally find our plain text and the deciphering key: ALL SUBMARINES OF BLUE FORCE WILL OPERATE ON SURFACE BEGINNING FEBRUARY SIXTEENTH and 5-2-6-9-4-7-3-8-1-10.

Other ideas for solutions will develop from the discussion of incompletely filled rectangles in the following paragraphs.

INCOMPLETELY FILLED RECTANGLES

14. Let us suppose that we have the following cipher:

ASSIGNMENT No. 8

16. The terminations of the first and last columns will aid in determining the correct size of the rectangle when they are used to line up adjacent letters. An example of a perfect break would be to find a "Q" and "J" in the first column, then, in searching for a "U" and an "O" the same distance apart, to find them in the last column. This would then determine both the top and bottom limits of the rectangle and from that the key length.

17. Note the string of consonants on strip number (4), and the string of vowels on strip number (6). These indicate that strips (4) and (6) might be adjacent in the original figure. To begin the rearrangement of the strips assume that the T of strip number (6) and the H of strip number (4) are on the same horizontal line as shown below. (All the logical trials are not shown, but the combinations which lead to the correct arrangement of the columns are underlined).

(6)	(4)
I	
E	
E	
G	
S	
B	M
F	B
E	W
A	T
A	C
I	N
R	Y
T	H
A	S
I	S
E	R
L	E
	R

(6)	(4)	(5)
		N
		U
	S	E
B	M	A
F	B	L
E	W	I
A	T	E
A	C	E
I	N	G
R	Y	S
T	H	B
A	S	F
I	S	E
E	R	
L	E	
	R	

(1)	(6)	(4)	(5)
			N
			U
	S		E
U	B	M	A
O	F	B	L
C	E	W	I
R	A	T	E
F	A	C	E
N	I	N	G
A	R	Y	S
N	T	H	B
L	A	S	F
E	I	S	E
O	E	R	
P	L	E	
U		R	

The remainder of the solution is quite simple. It is merely necessary to add columns which contain letters that build up words already begun. The completed solution is as follows:

Strip Number -	(7)	(8)	(2)	(4)	(1)	(6)	(4)	(5)	(3)
	A	L	L	S	U	B	M	A	R
	I	N	E	S	O	F	B	L	U
	E	F	O	R	C	E	W	I	L
	L	O	P	E	R	A	T	E	O
	N	S	U	R	F	A	C	E	B
	E	G	I	N	N	I	N	G	F
	E	B	R	U	A	R	Y	S	I
	X	T	E	E	N	T	H		

Numerical Key - 8 -- 9 -- 2 -- 5 -- 1 -- 7 -- 4 -- 6 -- 3

The previous method described for solving incomplete columnar transpositions suggested assuming a rectangle, writing the letters of the cipher on the strips of paper, and inscribing additional letters at the top and bottom of assumed columns to allow for various columns being short or long.

In using this method there is one deduction to be made. If during the decrypting it is found that by radically shifting one or more columns vertically plain text is found on one or two lines horizontally, but on no more than this, the deduction to be drawn is that the shape of figure is almost but not quite correct.

ASSIGNMENT No. 8

18. Another method of attacking this type of cipher may be used, a slight modification of the previous method. Let us, for example, take the same message as given in paragraph 13. We assume, with 70 letters of cipher text, that an 8-x-9 rectangle was used. We write the problem in columns as follows:

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

The form the problem is in at present is obviously incorrect. With 70 letters of cipher text and 72 spaces in the figure there must be two columns one letter short, and any two of the eight columns can be these short ones.

If the first column is one of the short ones, then the "L" at the bottom belongs at the top of column two. If column two is a short one, then the "U" at the bottom of it belongs at the top of column three, and if both columns one and two are short, then the last two letters at the bottom of column two, "R" and "U" belong at the top of the third column. Also, if the first two columns are short, or if one and three are short, then the last two letters of column three belong at the top of column four etc. With these deductions in mind, we add letters to the tops of the last 7 columns as follows:

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

With our figure made up for our assumed 8-x-9 rectangle in this manner we have allowed for all the possible shifts we may have and still have an 8-x-9 figure. If we cannot find plain text in a figure made up in this manner we know definitely that our assumption is incorrect. If we do find plain text, we know our assumption is correct as to size of figure, and if we find plain text after a radical shift of more than allowable distance, we know that our correct figure is close to the assumed size which we are investigating.

Having our figure, as given above, with the "caps" on it we proceed to decipher the message following a procedure similar to that given in paragraph 15, with the added assumption that all of the letters of the top line of the plain text can be found in the top line of the assumed rectangle or in the cap above and similarly the other lines of plain text may be displaced vertically not more than the distance permitted by the cap.

This same method can be applied to any size figure assumed to be correct. The number of letters used to "cap" our columns depends on the number of short columns in the assumed rectangle.

19. The "known word" method of anagramming, modified, can be applied to a solution of columnar transposition ciphers. The assumed known word may be used to build up adjacent columns especially where there are low frequency

letters in the word.

When the first word or phrase is known or suspected, the size of the rectangle and the subsequent solution of the problem may be obtained in this manner. In the example previously given assume that the word "SUBMARINE" is in the first line of the message. This assumption is aided by "U" being the first letter. Assume a key length of eight. This gives a figure containing six columns of nine letters and two of eight letters in depth. Therefore, the assumed word must be in the letters underlined below:

UOCRF NANLE OPUIR ERULO BFIMB WTCNY HSSRE ENUEA LIEEG SBSFE
AIRTA IELNE EXLNF OSGBT

There is no "B" underlined, therefore, the two assumptions do not coincide. Assume a key length of nine. This gives seven columns of eight and two of seven letters:

(1) (2) (3) (4) (5) (6) (7) (8) (9) (10)
UOCRF NANLE OPUIR ERULO BFIMB WTCNY HSSRE RNUEA LIEEG SBSFE

(11) (12) (13) (14)
AIRTA IELNE EXLNF OSGBT

In group (5) there is a "B" to line up with the "U" in group (1). The interval between them is 24 and the letters in the intervening groups must be (2): "L", (4): "R". Continuing, the next can be one of two "S's". Then, "A" or "L". Then, "S" or "F". Then, "I" or "E" and "L" or "N". These cannot anagram into "SUBMARINE" or any word and the beginning of "SUBMARINE". Therefore, follow the same steps using the "B" in group (10). This permits the use of "M" in group (5) and the line "ALL SUBMAR" comes out proving the key length assumption. This method may be combined with the capping method of laying out the problem.

Similarly the letters of any long word known or assumed to be in the body of the text will be found at intervals which are exact multiples of the height of the original rectangle in the case of a completely filled rectangle and approximate multiples in the case of an incompletely filled rectangle.

DOUBLE TRANSPOSITION CIPHERS

20. Double transpositions may be made in a number of ways. For instance, the message may be put through a rectangle once by a columnar, then through the same rectangle by a row transposition. It may be put through the same columnar process twice using the same or different keys for each phase. Different rectangles could also be used for each phase.

21. All transpositions, however, have one great weakness which simplifies their solution, no matter how complicated the transposition system may be. If two messages can be found of the same length in the same key, solution is possible by anagramming. This is further the only direct method of attack on double transposition ciphers.

22. In the first section of this assignment the anagramming of two messages of identical lengths in the same key is discussed. This process is of course equally applicable to intergral multiples of the rectangle size. For instance, assume the rectangle is 10 x 10, or 100 letters long, and that these rectangles are used in succession with the same key for messages over 100 letters in length. Then the first 100 letters of two long messages in the same key would anagram with each other. In a similar manner, the first 100 letters would anagram with the second 100 letters in a single message over 200 letters

ASSIGNMENT No. 8

long, etc.

23. It might be possible to anagram identical key messages of approximately the same length, i. e. - a single letter or at the most a few letters difference. This would require considerable skill, however, to maintain the proper offset in the anagramming.

24. Pamphlet No. 40, forwarded with this assignment, describes in detail a process for recovering the numerical keys of a double transposition cipher after the plain text has been solved.

PROBLEMS

KEY RECOVERY DESIRABLE BUT NOT COMPULSORY

Assignment No. 8

Problem No. 1

FROM: AB (FORCE COMDR).
TO : XY (UNIDENTIFIED).

EOSNA ENXOE SORZI STNVN RCENG THNHR OAUUN EOEAE EFXER ARYEU TREVV

HHIED AODGA NREZO YMRSG RNDTD RRGIO ATOSE GVVED NEIRN DYIDR DOTSH

AEAND LOGAZ RDTOI ZLNNR NNCRN IESEO

Problem No. 2

FROM: MN (FORCE COMDR).
TO : PQ (AIRCRAFT UNIT COMDR).

UHTSH SMSEJ IDEAH ROOAT EFERM IMEPC AIEVC GGELI QRNDA EXOIL DCHTC

EADSV IESDG HEPIO KDBBL CNANH RNNMO TSUNI GUAAB CNOME AGRTO ECGAU

IANTR TETIS BBZEN SMYEE GNNTR OBFP

Problem No. 3 Serial No. 1

FROM: FG (SCOUTING FORCE COMDR). MARCH 7.
TO : SD (DETACHED UNIT COMDR).

CVYRN ETATA HNHEE ITINB GNWRW EHOIN RTEYR HNATC EETUN AOTGT SOETC

BFOCR DAFIS GFANE ITHMD TETAG FTEIY LHFUR IEF

Problem No. 3 Serial No. 2

FROM: SD (DETACHED UNIT COMDR). MARCH 8.
TO : FG (SCOUTING FORCE COMDR).

NSORO AGEMP WSIPA TISDN RRRDH AEAEB SLABE TEFOT IFMNC UDOMU FEENA

HRNYC TRBNO VHEBR EWUVO UOATN VASED ESESI AOS

Problem No. 3 Serial No. 3

FROM: SD (DETACHED UNIT COMDR). MARCH 9.
TO : FG (SCOUTING FORCE COMDR).

VEASY NNIET FSAUN ESTOO IRRNT IEHAU GBHSE RRUWG OROAE OIHRH TYDBE

ASSIGNMENT No. 8

EKAFT EEPSR ERISC MODKS AOOSC TSCRU RFHLA EFC

Problem No. 4 Serial No. 1

FROM: DR (UNIDENTIFIED). 0015-1315
TO : CN (FORCE COMDR-BLACK).

OFIIU RCDLH EENFT NEYRO SIOBO DRBVA LANIA MTEYA FPENV GTTUI VNRES

RTRLR HTOSR TEDAE ENUYB OULAI NFFAU RTEEP VIANT IREEG TNBAR EVOFD

FROAK EATWT

Problem No. 4 Serial No. 2

FROM: CN (FORCE COMDR-BLACK). 0015-1710
TO : JX (UNIDENTIFIED).

OTIZA UATOR TPSOD EKEAA YOSBL UERNR DFPVL WCSSN NFTOR FGLSP GETRR

ODMCR ARTOA RTBHT UBTIE ZCUEE EIIAY NRIAO AREEI IEEHR TTKPT AROLE

SGDOD MIOHL

Collateral Information:

Fleet tactical exercises in Caribbean Sea; Black Fleet vs Blue Fleet. Both messages are in the same key. Solve the messages, work out the system and recover the key.

Problem No. 5

FROM: CN (FORCE COMDR-BLACK).. 0017-2130
TO : AB (COLLECTIVE CALL).

TRPAB PSEES ERETL EOINO ASOEA TYOWA ANNHL GUHUR UDNNO ESOAR LNOAI

HTVIE TOEHG OAEMI TROEF ZOURT UAILN TIRZD ARTNE ACMFU SMRSE LNTVN

SNAAT AIOSO UTNEO HFSRN EYACP NTOEF DNHVG DVCNS BNFTE TUINV DTZTL

LYUER SHNET OIEEH SCYCO IEHST DAPA

Problem No. 6 Naval Text.

RDLRD CSIIP DTFGI SOOAI EHXED RTNYN INNSN IPUSN HSNII XTUSP RSSTN

ETXEF IASOT OSSIT YIEVD DIUOE SEAOE EGUSO YMOEO OOOTO SXCNF RENFT

CEAAN NSVJW TSLCX VEONY TEASA NOOAI RELEO TEECG PNRPL RFVLH DITOI

MANUR GWRIT

B L A N K