Assignment No. 1

Prob. 1

THIS SHORT CRYPTOGRAM IS GIVEN AS AN EXERCISE IN THE SOLUTION OF A CIPHER BY INSPECTION

Prob. 2

WHEN ASKED ABOUT HIS PLAN OF CAMPAIGN GENERAL STONEWALL JACKSON REPLIED TO AN INQUISITIVE CHAPLAIN CAN YOU KEEP A SECRET YES THE EAGER CLERIC ANSWERED WELL SO CAN I SAID THE GENERAL

Prob. 3

DEVELOPMENT OF MEANS FOR RAPID COMMUNICATION HAS DONE CONSIDERABLE TOWARD CREATING A BETTER INTERNATIONAL UNDERSTANDING

Prob. 4

IN THE GOOD OLD DAYS WORDS WERE CAREFULLY SPACED IN CRYPTOGRAMS LIKE THIS BUT TODAY WORDS ARE RUN TOGETHER AND THE TEXT IS DIVIDED INTO GROUPS OF FIVE LETTERS TO INSURE ACCURACY IN TELEGRAPHIC TRANSMISSION

Prob. 5

PREPARE TO GET UNDERWAY AT ZERO EIGHT HUNDRED PLUS FIVE TIME FOURTEEN APRIL PERIOD BE PREPARED FOR MAXIMUM SPEED TWENTY KNOTS

Prob. 6

A RECIPROCAL ALPHABET IS ONE IN WHICH ALL THE VALUES IN THE ALPHABET ARE RECIPROCAL IN PAIRS

Prob. 7

AT ZERO FIVE HUNDRED DESTROYER DIVISION SEVENTEEN CHANGE COURSE TO THREE FIVE FOUR

Assignment No. 2

Prob. 1
VISUAL CONTACT NOT YET MADE WITH DESTROYER DETACHMENT PERIOD ARGONNE DIRECTED REMAIN VICINITY RENDEZVOUS TO MAKE CONTACT AND DELIVER COPIES ALL SECRET AND PUBLICATIONS

Sys.- Untransposed keyword mixed sequence
Key.- WESTERN UNION TELEGRAPH COMPANY

Prob. 2
ROME INVENTED THE FIRST SUBSTITUTION SYSTEM KNOWN JULIUS CAESAR USED AN ALPHABET IN WHICH D WAS SUBSTITUTED FOR A COMMA E FOR B COMMA F FOR C ETC IN HIS CORRESPONDENCE

Sys.- Reversed keyword sequence.
Key.- JANUARY FEBRUARY MARCH where Q(p) is A(c)

Prob. 3
PEARY ARRIVED NAKIN G FIFTEEN HUNDRED THIS DATE FOREIGN MEN OF WAR PRESENT TWO BRITISH GUNBOATS ONE JAPANESE DESTROYER AT PRESENT NO APPREHENSION AMONG FOREIGNERS CITY QUIET

Sys.- Vertical Sequence
Key.- BLACK

Prob. 4
IN THE STUDY OF CRYPTANALYSIS THE INDUCTIVE APPROACH IS PREFERRED BY THIS METHOD THE STUDENT LEARNS TO MAKE HIS OWN ANALYSIS AND IS NOT DEPENDENT ON RULES LEARNED FROM TEXT BOOKS

Sys.- Vert. Sequence
Key.- Cryptograph

Prob. 5
DECIPHERING IS BOTH A SCIENCE AND AN ART IT IS A SCIENCE BECAUSE CERTAIN DEFINITE LAWS AND PRINCIPLES HAVE BEEN ESTABLISHED WHICH PERTAIN TO IT IT IS ALSO AN ART BECAUSE OF THE LARGE PART PLAYED IN IT BY IMAGINATION SKILL AND EXPERIENCE

Ordinary sequence of alphabet, taken off vertically in columns 71362548

Prob. 6

CIPHER WORK WILL HAVE LITTLE PERMANENT ATTRACTION FOR ONE WHO EXPECTS RESULTS AT ONCE WITHOUT LABOR FOR THERE IS A VAST AMOUNT OF PURELY ROUTINE LABOR IN THE PREPARATION OF FREQUENCY TABLES AND OTHER THINGS BEFORE THE MESSAGE BEGINS TO APPEAR

Sys. Transposed keyword sequence, Alternate Diagonal starting upper left hand corner
Key. OPERATIONS

Assignment No. 3

Prob. 1

RECONNOITER AUXCAYES BAY AT DAYLIGHT SEVENTEEN APRIL AND THEN PROCEED THRU POINT GEORGE ON COURSE THREE THREE ZERO SPEED TWELVE PERIOD REPORT NOON POSITION TOMORROW

Plain alphabet arranged after keyword NEW YORK and all letters numbered from one to twentysix beginning with N=1

Prob. 2

WEATHER FORECAST THURSDAY PARTLY CLOUDY WITH SCATTERED SHOWERS EASTERLY WINDS AT SURFACE AVERAGING TWENTYFIVE KNOTS VISIBILITY LESS THAN AVERAGE UNDESIRABLE FLYING CONDITIONS PERIOD HEIGHT OF LOWER CLOUDS AT PRESENT ABOUT ONE THOUSAND FEET

Keyword MONDAY written in 5x5 square, horizontal and vertical columns numbered from 1 to 5 ~~xndxkwex~~

Prob. 3

AT FIFTEEN FIFTY ATTACKED BY FIVE LEXINGTON HEAVY BOMBING PLANES UNDER ANTIAIRCRAFT FIRE THREE MINUTES PLANES BOMBING POSITION ALTITUDE ONE FOUR THOUSAND FEET NO DAMAGE TO SARATOGA

Keyword USNAVY inscribed in 5x5 square, columns and lines letterred with vowels.

Prob. 4

SIGHTED SUBMARINE LATITUDE THIRTY DEGREES TWENTYONE MINUTES LONGITUDE ONE HUNDRED FORTY TWO DEGREES SIXTEEN MINUTES AT NINETEEN FORTY FOURTEEN MARCH PERIOD POSSIBLE THIS IS BASE COVERING GREAT CIRCLE ROUTE TO SANFRANCISCO

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

Diagraphs used interchangeably

Prob. 5

DESTROYERS OF OFFENSIVE SCREEN WILL FUEL TOMORROW SUNDAY BEGINNING AT DAYLIGHT PERIOD OILERS TAKE STATION AS SOON AS PRACTICABLE AND COMPLETE ALL NECESSARY ARRANGEMENTS

ABCDEFGHIJKLMNOPQRSTUVWXYZ
ETOANIRSHMETOANIRSHMETOANIRSHM
LUCMPFYWLUCMPFYWLUCMPFYWLU

Digraphs used interchangeably

Assignment No. 4

Prob. 1

SUBMARINE BOMBED ON SURFACE BY NINE FIGHTERS AND TWO SCOUTS WITH TWENTY TWO BOMBS XX ONE HUNDRED SIXTEEN POUNDS EACH AT THIRTEEN FORTY THREE ON BEARING TWO SEVEN FIVE DISTANCE FORTYFIVE MILES FROM FLEET GUIDE PERIOD SUBMARINE SUBMERGED FOR FIVE MINUTES AFTER ATTACK PERIOD ON RETURN TO SURFACE PLANES CONTINUED ATTACK WITH MACHINE GUNS

System: Two alphabets in normal sequence arranged so that A (p) equals US (c)

Prob. 2

AT DAYLIGHT TOMORROW THURSDAY BRANT AND TERN SWEEP NORTHWEST SIDE OF BUOYED CHANNEL FROM NORTHERN BUOYS TO POINT AFIRM PERIOD QUAIL AND TANAGER TAKE STATION AT ENTRANCE BUOY POINT AFIRM PERIOD KINGFISHER REMAIN AT ANCHOR AND DETACHED FROM MINE SWEEPING DETACHMENT TO REPORT TO COMMANDER AIRCRAFT PERIOD WHIPPOORWILL REPORT TO COMMANDER TENDER DETACHMENT UPON COMPLETION OF PATROL

System: Five alphabets in normal sequence
Key: MARCH

Prob. 3

OFFENSIVE SCREEN MADE CONTACT ENEMY SCOUTING LINE YESTERDAY MONDAY AND SARATOGA LEXINGTON BOMBED EACH OTHER PERIOD SARATOGA DAMAGED TWENTYFIVE PERCENT LEXINGTON THIRTYEIGHT PERCENT PERIOD UP TO PRESENT BOMBED ONE HEAVY AND ONE LIGHT CRUISER DECATUR FIRED SIX TORPEDOES AT LIGHT CRUISER TORPEDO PLANES ATTACKED ONE HEAVY CRUISER PENNSYLVANIA FIRED ON ONE LIGHT CRUISER TWENTY MINUTES PERIOD OFFENSIVE SCREEN NOW OPERATION VICINITY ENEMY CRUISER CONCENTRATION COMMA LEXINGTON NOT SIGHTED TODAY PERIOD ONE ENEMY CRUISER REPORTED NINETY MILES TO EASTWARD OF OUR NOON POSITION

System: Ten alphabets in normal sequence
Key: DEPARTMENT

Prob. 4

NO TRACE OF ENEMY MAIN BODY IN SEARCH TO LATITUDE ONE NINE THREE ZERO ON SIXTY MILE FRONT FROM NAVASSA TOWARD GUANTANAMO PERIOD BELIEVE WRIGHT SEAPLANE BASE LOCATED AT GUANTANAMO PERIOD WILL RETIRE ON COURSE TWO ONE THREE DURING DARKNESS RESUMING SEARCH AT DAYLIGHT PERIOD ENEMY RADIO TRANSMISSION HEARD ON FORTYONE HUNDRED KILOCYCLES AT SEVENTEEN HUNDRED NO BEARING OBTAINED

System: Two alphabets. Systematically mixed sequence using keyword NEWMEXICO.
Alphabets set so that A (p) equals NO (ϕ)

Prob. 5

ENEMY BATTLESHIP BEARING ZERO EIGHT FIVE TRUE PERIOD
BE PREPARED TO LAUNCH PLANES IN ACCORDANCE OPERATION
ORDER NUMBER SIX PERIOD DESTROYERS TAKE STATION TO
LAUNCH TORPEDO ATTACK ON ENEMY MAIN BODY DURING DARKNESS

System: Five systematically mixed alphabets using the keyword PRUDENTIAL attanged so that A(p) equals TUNIS (c)

:EVE BLUE WILL CONCENTRATE NEAR
I LONG SEVENTYFIVE STOP MAIN BODY
APRIL FOR DECISIVE ACTION USING
'ERATIONS SEVENTEEN APRIL STOP
)DY STOP SCOUTING AND STRIKING
? CONCENTRATE AND RETIRE BEFORE
(AT DAYLIGHT EIGHTEEN APRIL

e same sequence. Transposed
FLORIDA KEYS. Vert Trans.

;O AS GUIDE IN LAT ONE NINE DASH
N ON BEARING ONE ONE FIVE DISTANCE
NO CONTACT REPORT ON TYPE COM-
E CHICAGO REPORT POSITION HOURLY
) LAUNCH PLANES AND SEARCH NORTH
SEVENTEEN HUNDRED AT DARK REJOIN

eyword ARIZONA
?ENNSYLVANIA

3E AND INCREASE SPEED TO TWENTY-
)F ANTIAIRCRAFT DEFENSE AT DAWN
VE PERIOD REPORT ALL CONTACTS TO

E FIVE ZERO DISTANT TEN MILES
YFIVE HUNDRED COURSE ESTIMATE
FIRE DUE LOW CLOUDS PERIOD AM

eyword NAVAL RESERVE
BUREAU NAVIGATION

HMENT AT DUTCH HARBOR SUBDIV
RIVE WITHIN FORTNIGHT

SIX HUNDRED MONDAY TO JOIN SAURY
AD TORPEDOES FRIDAY SEALION WHEN

r
Keyword Rendezvous

Prob. 5

THE SIX SQUADRONS OF ARMY AIRPLANES ON DUTY IN THE SECTOR ARE CREDITED WITH BREAKING UP PLANS FOR A MASS ATTACK ON PESHAWAR IN ONE DAY THE MACHINES DROPPED SIX THOUSAND SMALL BOMBS AND THEN HAVE MADE DAILY ATTACKS ON VARIOUS GROUPS OF AFRIDIS THE AIRFORCE HAS EVACUATED THE WOMEN FROM PARACHINAR EIGHTY MILES FROM PESHAWAR BY AIRLINE KOHAT TWENTYONE MILES TO THE SOUTH OF PESHAWAR IS STILL UNDER ATTACK IT IS BELIEVED THAT THE AFRIDIS WERE NOT REPULSED BY THEIR CASUALTIES AROUND PESHAWAR PROPER BUT MERELY DECIDED THAT THE CITY WHICH IS HEAVILY DEFENDED AS THE GATEWAY TO THE KHYBER PASS WAS IMPREGNABLE

Plain component in normal order
Cipher component derived from Keyword COBENHAVEN set up in 3x5 rectangle and taken off in alternate diagonal manner beginning in upper left hand corner

A (pl) set against KHYBER
KHAIBER (c)

Prob. 6

LANDING FORCE WILL COMPRISE ONE BLUEJACKET COMPANY EACH FROM CINCINNATI MARBLEHEAD AND ARTILLERY PLATOON OO CONCORD CINCINNATI DESIGNATE BEACHMASTER MARBLEHEAD PROVIDE PORTABLE RADIO UNIT CONCORE DETERMINE MOST SUITABLE POINT FOR DEBARKING

Plain component derived from Keyword SUBSTITUTION
Cipher component from Keyword ALPHABET
S (pl) set against FOUR (c)

ASSIGNMENT No. 6

Prob. 1

AT TWENTYTWO TWENTYFIVE OPENED FIRE ON STURTEVANT AND DICKINSON FOR SIX MINUTES AT THREE THOUSAND YARDS PERIOD TWENTYTWO THIRTY FIVE OPENED FIRE ON RICHMOND FOR FIVE MINUTES AT FOUR THOUSAND YARDS PERIOD TWENTYTWO FORTYSEVEN OPENED FIRE ON UPSHUR AND TWO ENEMY DESTROYERS FOR THIRTEEN MINUTES AT SIX THOUSAND TO TWO THOUSAND YARDS

Sys: Plain and Cipher components both normal alphabets
Vigenere Table.

Prob. 2

DESTROYERS DICKERSON AND LAMBERT UNDER FIRE SECONDARY BATTERY TWO AND ONE HALF MINUTES EACH AT MEAN RANGE TWENTYSEVEN HUNDRED YARDS COMMA LEARY UNDER FIRE MAIN BATTERY ONE AND ONE HALF MINUTES AT MEAN RANGE FOUR THOUSAND COMMA TARBELL UNDER FIRE SECONDARY BATTERY FOR TWO MINUTES AT MEAN RANGE OF FORTY FIVE HUNDRED YARDS

Sys: Plain and Cipher components both derived from Keyword RHODEISLAND
Vigenere Table

Prob. 3

AT TWENTYONE TWENTYSIX SARATOGA ATTACKED BY HERBERT SIX TORPEDOES RANGE FIVE HUNDRED COMMA TWO HITS PERIOD AT TWENTYONE TWENTYSEVEN DICKERSON FIRED SIX TORPEDOES RANGE FIKE HUNDRED COMMA TWO HITS

Sys: Plain and Cipher components same sequence. Systematically mixed keyword sequences from Keyword OPERATING written in 3x9 rectangle and taken off vertically starting at lower right hand corner.
Vigenere Table

Prob. 4

AT ZERO SIX HUNDRED FIFTEEN APRIL FORM SCOUTING LINE BEARING ZERO FIVE ZERO DEGREES TRENTON GUIDE IN EAST ANSWERING FIRST REPEATER SCOUTING DISTANCE TWENTY MILES ORDER OF SHIPS FROM EASTWARD DECATUR MEMPHIS TRENTON RICHMOND MARBLEHEAD LITCHFIELD PERIOD HULBERT AND PRESTON JOIN COMAIRRONS SARATOGA IN VICINITY MAIN BODY AS LINKING VESSELS AND DISTANT PLANE GUARDS PERIOD AIRONS OPERATE AT DISCRETION UNDER PROTECTION OF SCOUTING LINE TO LOCATE AND ATTACK LEXINGTON PERIOD COMMENCE SCOUTING AT ZERO SIX HUNDRED SPEED TWENTY COURSE THREE TWO ZERO PARAGRAPH LOCATE AND DESTROY LEXINGTON PERIOD COMAIRRONS AND COMDR BLACK FLEET PLEASE DELIVER TO DESTROYERS

Sys: Plain and Cipher components different sequences of random selection Pl - AGUOQJMEWNBISZHXDKYLVRTFPC
C - ALGXRJWSCOTVIDNYUFPMBKHQZE

Vigenere Table

ELEMENTARY COURSE IN CRYPTANALYSIS

Assignment No. 7

Problem No. 1

CONTACTED THREE ENEMY DESTROYERS BUT UNABLE TO ENGAGE DUE TO THEIR JOINING UP WITH MAIN BODY

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

Problem No. 2

WHEN IN ALL RESPECTS READY FOR SEA PEARY PROCEED SHANGHAI AND REPORT TO SENIOR OFFICER PRESENT AFLOAT FOR DUTY AS STATION SHIP SHANGHAI

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

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

T T O S I S A G A T
S A I N H P H N H I
```

Problem No. 3

BATTLESHIP DIVISION TWO PROCEED ON SERVICE ASSIGNED

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

Assignment No. 7

Problem No. 4

PROCEED IN ACCORDANCE WITH OPERATION ORDER NUMBER ONE PERIOD ON COMPLETION OF ASSIGNED DUTY RETURN TO BASE AND AWAIT FURTHER INSTRUCTIONS

P O E D N C O D N E I H P R T O O D R U B R N
R C E I A C R A C W T O E A I N R E N M E O E

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

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

Problem No. 5

UPON THE REPORTING OF HIS RELIEF LIEUTENANT JOHN H DOLAN U S NAVY DETACHED TENNESSEE PROCEED AND REPORT TO ROPER FOR DUTY AS EXECUTIVE OFFICER

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

Problem No. 6

TRANSPOSITION CIPHERS INVOLVE NO CHANGE IN THE IDENTITY OF THE LETTERS OF THE PLAIN TEXT SEMI-COLON ONLY THE ORIGINAL ARRANGEMENT IS CHANGED

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

Assignment No. 7

Problem No. 7

ONE OF THE MOST DIFFICULT TASKS BEFORE THE CRYPT-ANALYST IS THE CORRECTION OF ERRORS WHICH CREEP INTO CIPHER TEXTS IN THE PROCESS OF ENCIPHERING AND TRANSMITTING BY TELEGRAPH OR RADIO

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

E. J. Rowett
33-H Ridge Rd.
Greenbelt, Md.

ASSIGNMENT 8

Problem 1

ARRANGE DESTROYER CONVOY FOR DAMAGED CV SIX RETURNING RENDEZVOUS DOG AND ARRIVING LAT NINE DASH ZERO THREE NORTH LONG ONE SIXTY NINE DASH ZERO SEVEN AT ZERO ONE HUNDRED

KEY:- 12 9 3 7 14 10 1 11 5 2 6 13 4 8

Completely filled Rectangle 14 X 10. Text written in form in columns according to key and removed in normal English order.

Problem 2

DURING DAYLIGHT MARCH EIGHTEENTH REQUEST PHOTOGRAPHIC RECONNAISSANCE AND BOMBING ATTACKS BE MADE RENDEZVOUS FOX OBJECTIVE BOMBINGS AIR FIELDS GUN EMPLACEMENTS

KEY:- 6 1 10 3 7 9 5 2 11 4 8

Incompletely filled rectangle.(5 nulls at end of last line) Rectangle is 11 X 13. Text inscribed according to key and removed in normal English order.

Problem 3

Serial 1

BEGINNING MARCH EIGHT CHANGE ARC OF SEARCH TO THAT BETWEEN LATITUDES THIRTY FIFTEEN AND TWENTY FOUR FORTY FIVE

Serial 2

HAVE OBSERVED TWO ENEMY SUBMARINES OPERATING UPON SURFACE TO EAST OF LINE NORTHWARD FROM HIS ADVANCED SUB BASE

Serial 3

ENEMY STRIKING FORCE OF FOUR HEAVY CRUISERS AND TWO CARRIERS HAS LEFT BASE BAKER ON COURSE TO SOUTH AT HIGH SPEED

KEY:- 7 3 6 1 4 8 5 2

Double Columnar transposition in incompletely filled rectangle, 8 X 12. Same key used for both transpositions.

E. J. Rowett
33-H Ridge Rd.
Greenbelt, Md.

ASSIGNMENT 8

Problem 4

Serial 1

AT TWELVE FORTY FIVE OBTAINED RADIO BEARINGS ON APPARENTLY NAVAL TRANSMITTER ON ABOUT FOUR HUNDRED FIFTY FIVE KCS BEARING THREE FIVE FOUR TRUE

Serial 2

LIGHT CRUISERS SIGHTED FROM TOP BEARING ZERO ZERO FOUR TRUE PERIOD THEY WILL PROBABLY CLOSE AT SUNSET PERIOD AT DARK LEAVE FORMATION AND ATTACK

KEY:- Columnar Key - 3 8 4 10 1 5 9 6 7 2
Linear Key - 8 9 2 4 12 5 10 3 6 11 1 7

Two way transposition in completely filled rectangle 10 X 12. Text is inscribed in form according to columnar key and removed by linear key.

Problem 5

AT ZERO FIVE THIRTY LAUNCH ALL PLANES ON SIGNAL COMMA SCOUT BY PAIRS BY SHIP UNITS ON COURSE THREE FOUR ZERO TO LATITUDE SEVENTEEN DASH FIFTY THEN RENDEZVOUS ON TRENTON WITH ONE THOUSAND FEET OVER NAVASS ALIGHT AND PROCEED GUANTANAMO-

KEY:- 6 1 11 9 4 5 7 2 10 12 8 3

12 X 17 incompletely filled rectangle. Text inscribed according to key and removed in normal English order.

Problem 6

CRUDIVS FIVE AND SIX JOIN DESFLOT TWO AND CARRY OUT ASSIGNED MISSION UPON COMPLETION OF SEARCH OPERATIONS XX SUSPICIOUS VESSEL REPORTED IN AREA DOG NORTH OF LAT TWENTY SEVEN FORTY NINE LONG SIXTY EIGHT SIXTEEN

KEY:- 8 1 7 12 4 9 2 5 3 6 11 10

Incompletely filled rectangle 12 x 15. Text inscribed according to key and removed in normal English order.

E. J. Rowett
33-H Ridge Rd.
Greenbelt, Md.

ASSIGNMENT 9

Problem 1

Serial 1

SHORE PARROLS ENCOUNTERED DIFFICULTY IN MAINTAINING ORDER ALONG THE WHARF

Serial 2

A FULL REPORT IS REQUESTED FROM THE COMMANDING OFFICER OF THE VESSELS IN PORT

XXXXX

Grill used 8 x 8 - numbered in normal English order, the following cells are open 1-5-12-15-17-22-27-32-36-39-42-45-49-51-56-62. Rotated counterclockwise.

Problem 2

AT EIGHTEEN HUNDRED SIGHTED FOUR LIGHT CRUISERS BEARING THREE FOUR SEVEN TRUE FROM FLEET GUIDE ON AN EASTEULY COURSE XX

Grill used is 10 x 10 with following cells open: 3-10-11-15-18-24-29-32-37-40-41-43-44-48-56-66-68-70-73-80-81-82-85-87-96. Rotated clockwise.

Problem 3

Serial 1

BATTLESHIPS DEPLOY ON COURSE THREE ONE FIVE DESTROYERS FORM ANTISUBMARINE SCREEN ON DISENGAGED SIDE OTC IN TENNESSEE

Serial 2

ONE CRUISER SIGHTED IN POSITION GEORGE HYPO TWO ON COURSE ONE EIGHT ZERO SPEED TWENTYFIVE APPARENTLY ON DETACHED DUTY X

Grill which is used is 10 x 10 with the following cells open: 2-4-7-19-21-23-26-34-39-41-45-47-50-53-59-65-68-72-77-79-84-86-92-98-100. Rotated counterclockwise.

Problem 4

INFORMATION RECEIVED YOU ARE ON DEPT OF JUSTICE SUSPECT LIST AND ARE BEING WATCHED STOP IF US DECLARES WAR PROCEED TO MEXICO CITY AND REPORT TO EMBASSY STOP WATCH FOR SLEUTHS

Grill used is 12 x 12 with the following cells open: 8-10-14-16-18-24-32-34-38-40-43-48-54-57-61-63-67-70-72-79-85-87-89-93-95-103-110-112-117-119-126-128-134-136-142-144

E. J. Rowett
33-H Ridge Rd.
Greenbelt, Md.

ASSIGNMENT 9

Problem 5

Serial 1
FORCES PREVIOUSLY REPORTED ARE CHANGING COURSE TO ONE EIGHT ZERO

Serial 2
FORCES PREVIOUSLY REPORTED AHEAD CHANGED COURSE TO TWO FOUR ZERO

Serial 3
I AM ATTACKING EIGHT SUBMARINES ON SURFACE BEARING TWO ZERO SEVEN

KEY:- 9 2 5 6 3 7 1 10 11 8 4

Double columnar transposition in completely filled rectangle 11 x 5. Same key used for both transpositions.

E. J. Rowett
33-H Ridge Rd.
Greenbelt, Md.

ASSIGNMENT 10

PROBLEM 1

Serial 1

OPERATE AT DISCRETION EXCEPT EXECUTE PLAN GEORGE ONE AT DAYLIGHT EIGHTEEN APRIL

Serial 2

AT FIFTEEN FIFTY ATTACKED BY FIVE LEXINGTON HEAVY BOMBING PLANES UNDER ANTIAIRCRAFT FIRE THREE MINUTES PLANES BOMBING POSITION ALTITUDE ONE FOUR THOUSAND FEET NO DAMAGE TO SARATOGA

Serial 3

HAVE ORDERED HULBERT PRUITT EXCHANGE MISSIONS PERIOD PRUIT LOSING WATER AT HIGH SPEED SX

Serial 4

PROCEED INDEPENDENTLY AT DISCRETION TO JOIN MAIN BODY AT DAYLIGHT EIGHTEEN APRIL PERIOD DECATUR CONTINUE AS LATE AS PRACTICABLE TO TRACK LEXINGTON AND ATTACK IF POSSIBLE

Serial 5

MAIN BODY TAKE SPEED THIRTEEN POINT FIVE AT ZERO TWO HUNDRED EIGHTEEN APRIL PERIOD FLEET CHANGE COURSE TO ZERO THREE ZERO AT ZERO SIX THIRTY PERIOD LANGLEY ESTABLISH ANTISUBMARINE PATROL AT DAYLIGHT AND MAINTAIN FIGHTERS IN READINESS PERIOD AIR SQUADRONS OPERATE AT DISCRETION KEEPING VISUAL CONTACT

SYSTEM: False digraphic, with first character of each digraph variable and determined from a square table and with second character of digraph having a constant value.

Keyword for cipher component of 1st letter of digraph: STENOGRAPHY - vertical mixed sequence with plain component a normal alphabet.

Keyword for cipher component of 2nd letter of digraph: CRYPTOGRAMS - vertical mixed sequence with plain component a normal alphabet.

E. J. Rowett
33-H Ridge Rd.
Greenbelt, Md.

ASSIGNMENT 10

PROBLEM 2

Serial 1

ONE CRUISER LAT SIXTEEN DASH THIRTYSIX LONG SEVENTYONE DASH FORTYTWO COURSE THREE ONE FIVE X

Serial 2

ONE MERCHANT VESSEL LAT SEVENTEEN DASH EIGHTEEN LONG SEVENTYONE DASH FORTYEIGHT COURSE ZERO NINE ZERO X

Serial 3

ONE CRUISER LAT SIXTEEN DASH FIFTY FOUR LONG SEVENTYONE DASH FORTYTWO COURSE TWO EIGHT FIVE X

Serial 4

AT FOURTEEN HUNDRED SIXTEEN APRIL FORM SCOUTING LINE BEARING ONE NINE ZERO FROM VICE THREE IN POSITION QUACK SAIL HYPO SCOUTING DISTANCE TWENTY MILES ORDER FROM NORTH VICE THREE VICE ONE VICE TWO PERIOD SPEED ELEVEN COURSE TWO EIGHT ZERO

Serial 5

ENEMY CRUISER PREVIOUSLY REPORTED IS A FRIEND X

SYSTEM:

1st letter	TUVWXYZABC	DEFGHIJKLM	NOPQRS
K	1001234567891	101234567891	2012345
L	130	140	150
M	160	170	180
N	190	200	210
O	220	230	240
P	250	260	270
Q	280	290	300
R	310	320	330
S	340	350	360
T	370	380	390
U	400	410	420
V	430	440	450
W	460	470	480
X	490	500	510
Y	520	530	540
Z	550	560	570
A	580	590	600
B	610	620	630
C	640	650	660
D	670	680	690
E	700	710	720
F	730	740	750
G	760	770	780
H	790	800	810
I	820	830	840
J	850	860	870

E. J. Rowett
33-H Ridge Rd.
Greenbelt, Md.

ASSIGNMENT 10

PROBLEM 3

Serial 1

RECONNOITER WESTERN COAST OF HAITI ENROUTE NEW SCOUTING STATIONS

Serial 2

ONE MINESWEEPER LAT SEVENTEEN DASH FIFTEEN LONG SEVENTYFOUR DASH TWENTYSEVEN COURSE THREE THREE ZERO SPEED TEN KNOTS

Serial 3

SANK SANDPIPER BY GUNFIRE AT FOUR THOUSAND YARDS X

Serial 4

TWO LIGHT CRUISERS LAT EIGHTEEN DASH TWENTYONE LONG SEVENTYFOUR DASH FIFTYFIVE COURSE ONE EIGHT ZERO

Serial 5

TWO ENEMY PLANES LAT EIGHTEEN ZERO ZERO LONG SEVENTYFOUR ZERO ZERO COURSE ONE ZERO FIVE X

Serial 6

BEARING OF COMMANDER BLUE ZERO TWO FOUR FROM POSITION LAT EIGHTEEN LONG SEVENTY FIVE FIFTY AT ELEVEN FIFTEEN X

Serial 7

AT ZERO EIGHT FORTY BEARING OF TENNESSEE FROM LANGLEY SEVENTYTHREE DEGREES

SYSTEM: True digraphic

Note: With the relatively small percentage of digraphs recovered I was unable to reconstruct a definite system, however a check of true values of high frequency letters in first and second positions gives some indication that a system may have been employed in making up the cipher component of the table.

E. J. Rowett
33-H Ridge Rd.
Greenbelt, Md.

ASSIGNMENT 11

PROBLEM 1

ONE OF THE GREATEST ADVOCATES OF COMMUNICATION SECURITY WAS GENERAL STONEWALL JACKSON PERIOD HIS RETICENCE OFTEN IRRITATED HIS FELLOW OFFICERS WHO THOUGHT IT IMPLIED A WANT OF CONFIDENCE IN THEM PERIOD HOWEVER MANY OF HIS VICTORIES CAN BE ATTRIBUTED TO HIS SURPRISE ATTACKS AND THE FACT THAT THE FEDERAL FORCES NEVER HAD AN INKLING OF HIS PLANS PERIOD THEN IN SO SMALL A MATTER AS WRITING TO HIS WIFE HE WAS CONSISTENT FOR HE TOLD HER THAT IT WAS UNLIKE AN OFFICER TO WRITE MILITARY NEWS TO ANY ONE

SYSTEM: Diagonal Digraphic Substitution using this table:

	ABCDE|EDCBA	
	FGHIK|KIHGF	
1st plain	LMNOP|PONML	1st cipher
	QRSTU|UTSRQ	
	VWXYZ|ZYXWV	
	EDCBA|ABCDE	
	KIHGF|FGHIK	
2nd cipher	PONML|LMNOP	2nd plain
	UTSRQ|QRSTU	
	ZYXWV|VWXYZ	

PROBLEM 2

Serial 1

SEVENTEEN APRIL FORM SCOUTING LINE BEARING EAST ORDER OF SCOUTS FROM EAST DECATUR RICHMOND TRENTON MARBLEHEAD LITCHFIELD CARRIER GROUP AS BEFORE TRENTON GUIDE AT POINT CAST SCOUTING DISTANCE TWENTY MILES COURSE THREE THREE ZERO SPEED TWENTY COMMENCE ZERO SIX HUNDRED X

Serial 2

RECONNOITER AUXCAYES BAY AT DAYLIGHT SEVENTEEN APRIL PERIOD PROCEED THRU POINT GEORGE ON COURSE THREE THREE ZERO SPEED TWENTY PERIOD REPORT POSITION NOON TOMORROW X

Serial 3

AT TWELVE HUNDRED SEVENTEEN APRIL FORM SCOUTING LINE BEARING ZERO SIX ZERO FROM VICE THREE AT POINT GEORGE SCOUTING DISTANCE TWENTY SPEED TWELVE COURSE THREE THREE ZERO PERIOD ORDER FROM WESTWARD VICE THREE VICE TWO VICE ONE PERIOD VICE THREE RECONNOITER AUXCAYES ENROUTE NEW STATION X

Serial 4

AT SEVENTEEN HUNDRED MET LEXINGTON CONCORD AND THREE DESTROYERS IN POSITION SAIL HYPO WILLIAM PERIOD ENGAGED THE LEXINGTON WHILE SHE WAS RECOVERING PLANES PERIOD LOST CONTACT ABOUT EIGHTEEN FORTY FIVE IN POSITION SAI

SYSTEM: "Playfair" digraphic substitution. Square formed from Keyword LEXINGTON

LAPZE	LEXINGTO
BQXGR	ABCDFHKM
IDSNF	PQRSUVWY
UGHVT	Z
KWOMY	

E. J. Rowett
33-H Ridge Rd.
Greenbelt, Md.

ASSIGNMENT 11

PROBLEM 3

Serial 1

SUBMARINE CRUISING SUBMERGED BEARING TWO EIGHT ZERO DISTANT FORTY FROM FLEET GUIDE AT TWELVE TWENTY PERIOD ATTACKED WITH EIGHTEEN ONE HUNDRED POUND BOMBS WHILE SUBMERGED AT TWELVE SIXTEEN PERIOD WILL CONTINUE TO TRACK AND ATTACK NO DESTROYERS IN VICINITY SUBMARINE Q

Serial 2

DESTROYER ORDERED TO PROCEED AGAINST SUBMARINE REPORTED BY NEW YORK

Serial 3

TAKE ASSIGNED STATIONS AT DAYLIGHT TOMORROW MONDAY PERIOD BE PREPARED TO LAUNCH TWO PLANES FOR TACTICAL SCOUTING AT SUNRISE J

Serial 4

ENEMY SUBMARINE TO SOUTHWARD O(F) FLEET GUIDE DISTANCE TWENTYFIVE MILES PERIOD HAVE SENT PLANES TO ATTACK.

SYSTEM: False digraphic substitution with the first letter of each digraph being taken from a straight keyword cipher component against a normal alphabet plain component. Keyword used for first sequence is BALTIMORE.

The second letter of the digraph is obtained from a viginere table the cipher component of which is derived from a straight keyword sequence using the keyword WASHINGTON. The successive lines of the table are offset one step to the left progressing downward.

The plain component of the second letter is a plain alphabet in normal order.

E. J. Rowett
33-H Ridge Rd.
Greenbelt, Md.

ASSIGNMENT No. 12

Problem 1

TWO THOUSAND TONS OF AMMUNITION LEAVING NEW YORK AT MIDNIGHT MONDAY

SYSTEM: Read every 4th word.

Problem 2

PARTIALLY CONFIRMED REPORT ENTIRE FLEET GOING TO SEA MORNING OF EIGHTEENTH MISSION UNKNOWN QP

SYSTEM: Simple rail fence transposition.

Problem 3

IN FUTURE TAKE CENTRE WORD THEN FIRST AND LAST OF EACH LINE

SYSTEM: Formed by taking first letter after each break in word of text.

Problem 4

YOU ARE UNDER OBSERVATION BY UNITED STATES DEPARTMENT OF JUSTICE PROCEED TO MEXICO THENCE BUENOS AIRES REPORT TO MILLER

SYSTEM: Simple substitution cipher formed by converting the letters of the alphabet into their normal numerical equivalent (order of position in alphabet) and adding to each number.

Problem 5

NO DEFINITE NEWS USUAL SOURCES NO LONGER ABLE TO LEARN PLANS STOP THINK NEW CONTACTS MUST BE MADE STOP UNABLE EXPLAIN PRESENT FAILURE AND NEED FUNDS TO BUILD NEW SYSTEM WHICH REQUIRE ABOUT TWO MONTHS

SYSTEM: Grill used 6 X 6 with following cells open: 3 - 8 - 10 - 15 - 20- 24 - 25 - 30 - 31 Rotated counterclockwise.

Problem 6

TOM IS INJURED HE RACED A FORD HE WRECKED IT AND ALICE IS HURT TOO IN FACT SHE IS DEAD

ASSIGNMENT 12

Problem 7

URGENT BRITISH TROOPS WILL ATTEMPT LANDING SOUTHERN GALLIPOLI PENNINSULA ABOUT MIDDLE OF NEXT MONTH

SYSTEM: Text divided into groups of five, underlined characters combinning with others in each group to form a pattern similar to a dot and dash code:

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

Problem 8

ONE LARGE TRANSPORT SAILING MONDAY NINE DESTROYERS LEFT AT DAWN ON PATROL ONE DESTROYER IN PORT

SYSTEM: Simple substitution. Text based on order of vowels in message. vowels combined consecutively in pairs and deciphered by means of table. Insufficient text to complete table:

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

Op-20-GR

RESTRICTED

NAVY DEPARTMENT
Office of Chief of Naval Operations
WASHINGTON.

ELEMENTARY COURSE IN CRYPTANALYSIS

TRAINING PAMPHLET No. 1

RECONSTRUCTION OF SIMPLE CIPHER SYSTEMS

1. In cipher solution, it is not sufficient that the cryptanalyst solve a particular cryptogram and stop there. He should reconstruct the cipher system in its entirety, if possible, and recover the key, if one was used. Before setting the problem aside as finished business, he should know all the details of the system used and be as familiar with it as the person who constructed it. In other words, he should train himself to extract every possible scrap of information from the cipher text available.

2. The type of key used depends upon the characteristics of the cipher system. Only the commonest types will be discussed in this pamphlet, that is, systems employing sequences based upon keywords or based upon numerical keys which were derived from keywords. The advantage of using a keyword from which to derive alphabet sequences is that the correspondents need carry no alphabet sequences in writing and must merely memorize a previously designated keyword and the method to be used in converting the word into the alphabet sequence in order to encipher or decipher the system.

UNTRANSPOSED KEY WORD SEQUENCES

3. The simplest type of keyword sequence is that in which the keyword is written first (omitting any letter on its second and subsequent appearances in the key), followed by the remaining letters of the alphabet. For example, if the keyword is WASHINGTON, D.C., the straight or untransposed keyword sequence is W A S H I N G T O D C B E F J K L M P Q R U V X Y Z.

4. In the simplest types of monoalphabet substitution, such a keyword sequence could be used as the cipher alphabet or component and the plain alphabet or component would be a normal alphabet, as follows:

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

This is an ENCIPHERING table and the word NAVY would be enciphered FWUY. In the solution of a cryptogram in this system, the keyword WASHINGTON, D.C., is immediately apparent if the cryptanalyst reconstructs an ENCIPHERING table, as shown above. However, if he reconstructs the DECIPHERING table during his solution, he obtains the following:

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

There is evidence of system, as opposed to random substitution, in the underlined portions of the sequence but no keyword is apparent. The student has merely to convert his DECIPHERING table to an ENCIPHERING table to get the key. Usually it is better to reconstruct the ENCIPHERING table because it is most often the one in which the keyword was originally inserted, but to be certain of not overlooking any evidence of system, the student should reconstruct both the

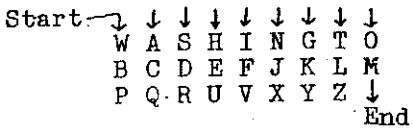
ENCIPHERING and DECIPHERING tables simultaneously.

TRANSPOSED KEYWORD SEQUENCES

5. The most common method of developing a transposed keyword sequence is to write out the keyword on one line and the remaining letters of the alphabet under the key, thus:

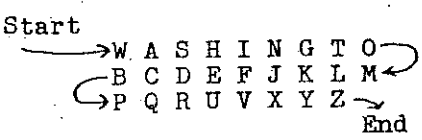
W A S H I N G T O
B C D E F H K L M
P Q R U V X Y Z

The transposition may be made in a large number of ways, the most common of which are route transpositions, such as: vertical, alternate vertical, alternate horizontal, diagonal, alternate diagonal, spiral, either clockwise or counter-clockwise, and labyrinth, following a previously agreed upon pattern. In any of the above methods, the start may be made at any one of the four corners of the rectangle. Examples of these routes are as follows:

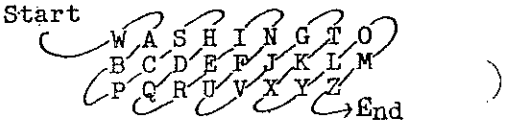


Vertical sequence:
W B P A C Q S D R etc.

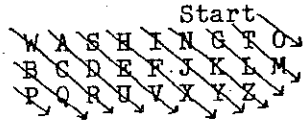
Alternate vertical sequence:
W B P Q C A S D R etc.



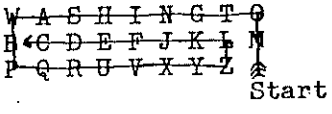
Alternate horizontal sequence:
W A S H I N G T O M L K J etc.



Alternate diagonal sequence:
W A B P C S H D Q etc.



Diagonal, starting at upper right corner sequence:
O T M G L N K Z etc.



Spiral, counter-clockwise sequence:
M O T G N I H S etc.

COLUMNAR TRANSPOSITION SEQUENCES

6. In addition to route transposition, another very common type is columnar transposition. Vertical columns are transposed irregularly in accordance with a numerical key, which may or may not have been derived from a literal key. (Recovery of literal keys will be illustrated later in this pamphlet).

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

Sequence:
H E U G K Y I F V W B P etc.

RECOVERY OF UNTRANSPOSED KEYWORD SEQUENCES

7. Recovery of non-transposed keyword sequences is very simple and involves a mere glance at the recovered sequence to discover the key.

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

The letters Z Y X W V U are significant and reveal the system. The key is TICONDEROGA (reversed) by inspection, where O plain = T cipher.

RECOVERY OF TRANSPOSED KEYWORD SEQUENCES

8. Recovery of transposed keyword sequences is also simple once the student is trained to recognize evidences of system. In the following recovered sequence:

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

Note the regularity of spacing between, M, O, P, Q, S, T and also F, G, H, J, K. Since low freguency letters have less chance of being in the keyword than high freguency letters, it is usually more satisfactory to look for regularity of spacing between them than between high freguency letters to make a start. The two sequences listed above (M O P Q S T and F G H J K) are spotted because the spacing between P and Q in one was noticed to be the same as that between J and K in the other. This regularity of spacing indicated that the letters M O P Q S T (also F G H J I C) were on the same horizontal line in the transposition rectangle and that the method of transposition was regular rather than alternate. Write one sequence, M O P Q S T on a horizontal line and fill in the intervening letters in the cipher alphabet above and below in a column:

A R
F G
M O P Q S T
V W X

The F G on the line above and the V W X on the line below look good. Complete the figure.

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

Key - CARIBBEAN. Method - Vertical transposition.
Start - Upper left corner

9. Another keyword is recovered as follows from the cipher component:

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

Here again the spacing between J-K and P-Q is the same. Extending each sequence yields no results using the same spacing.

Try varying the spacing:
2 3 5 3 5 2

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

The sequences B C D F J K M and N O P Q S T can be built up by varying the spacing from 1 to 5 in a regularly irregular manner. Such variation is characteristic of alternate transposition of some kind.

Try alternate vertical first, writing one sequence B C D F J K M on a horizontal line, and filling in on the alternate vertical:

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

The keyword comes out but the rectangle is somewhat offside. If alternate diagonal transposition is tried, the results are:

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

Thus, once it was decided that alternate transposition is involved, even an incorrect vertical method gave the key, after a fashion. If the student understands the above illustrated route transposed key recoveries, he should be able to recover keys transposed by all other route methods.

RECOVERY OF KEYS OF COLUMNAR TRANSPOSITION SEQUENCES

10. The first step in recovery of keywords transposed by the columnar method is similar to recovery of other transpositions, that is, the discovery of regularities and peculiarities of spacing and the correct interpretation of these characteristics. Suppose the recovered cipher component is:

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

In the underlined groups of letters, note that the first letter of each group is near the beginning of a standard alphabet, the second letter of each group comes later in a standard alphabet than any of the first letters of the groups, etc. From the number of groups, the key length is learned to be 7, and the lengths of the columns are 3 and 4 letters. Write the groups in vertical columns, after numbering them consecutively:

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

Rearrange to form a standard alphabet:

(3)	(7)	(2)	(4)	(6)	(1)	(5)
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		

The numerical key for the columnar transposition:

3--7--2--4--6--1--5

KEY RECOVERY WHEN BOTH PLAIN AND CIPHER COMPONENTS ARE UNKNOWN (BUT IDENTICAL SEQUENCES)

11. In the cases discussed up to this point, the plain component has been a standard alphabet, and it was only necessary to work with the cipher sequence to reconvert to the original keyword.

When the plain component is not a standard alphabet, but is a straight or transposed keyword sequence (either the same sequence as the cipher component or a different sequence), recovery of the key(s) is difficult in monoalphabet substitution because there is only one plain and one cipher sequence with which to work. The process is one of rearrangement of the two sequences. In polyalphabet substitution, where there are two or more cipher alphabets, the principles involved are identical with those in monoalphabet systems, but the work is easier because there are two or more cipher alphabets with which to work.

12. Before illustrating the recovery of the key when both plain and cipher components are unknown (identical) sequences, it is necessary that the student understand "equivalent sequences". Any sequence of 26 letters may be decimated or respaced so that all letters (such as A-B-C, etc.) which were originally spaced at equal intervals will also be respaced at equal intervals (but the interval is different from the original interval) in the new related or equivalent sequence. As an illustration, a standard alphabet is used and is respaced at intervals of 3, 5, 7, 9, 11, and 15, etc., spaces to produce equivalent sequences. Only the odd intervals can be used in respacing a 26 letter sequence to form related or equivalent sequences. It should be obvious that even intervals will produce 13 letter sequences. The interval 13 can not be used, either, because it produces a sequence of 2 letters only, and repeats.

EQUIVALENT SEQUENCES

Sequence No.	Interval	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
		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	1	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
2	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
3	5	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
4	7	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
5	9	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
6	11	A	P	E	T	I	X	M	B	Q	F	U	J	Y	N	C	R	G	V	K	Z	O	D	S	H	W	L
7	15																										

Note that sequence No. 7 is the same as sequence No. 6 reversed. Likewise, sequences with intervals of 17, 19, 21, 23, and 25 are the reverse of sequences with intervals of 9, 7, 5, 3, and 1 respectively.

Thus, in any alphabet of 26 letters, there are a total of 6 different equivalent sequences, each of which has an equivalent reverse sequence.

13. In systems in which the plain and cipher components are unknown (identical) sequences, the cipher alphabets recovered during solution will not appear to be the same sequences in either the ENCIPHERING or DECIPHERING table. For example, a recovered ENCIPHERING TABLE is as follows:

ENCIPHERING TABLE

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

The five cipher sequences are all different. Cipher alphabet No. 4 is a standard alphabet, or the same as the plain component. This is sufficient evidence to assume that the five alphabets are associated alphabets and the plain component sequence is the same as the cipher component sequence. We know that in the original form O (plain) was set against TION (cipher).

14. The first step is to build up an arbitrary sequence such that the sequence of the plain component and all five cipher alphabets will be the same. A start can be made with any letter of the cipher component, such as A, with its cipher equivalents. The next letter of the sequence which we are building is also selected at random. In building up our sequence in this manner, on our first attempt we have a 12 to 25 chance of building one of the equivalent sequences, a 12 to 25 chance of hitting a sequence of 13 and repeat, and a 1 to 25 chance of selecting the 13 interval sequence of 2 letters. If we do happen to build up one of the equivalent sequences, there is only one chance in 12 that it will be the sequence originally used. Start with A (plain) and as the next letter of the sequence, select a letter at random, such as Y (plain).

Plain ----	A	Y
Cipher (1)	M	H
Cipher (2)	Z	U
Cipher (3)	E	A
Cipher (4)	A	Y
Cipher (5)	U	Q

From this point on, the sequences build themselves up, i.e., in cipher alphabet 5 we have the sequence U Q. In alphabet No. 2, the sequence Z U. If all sequences are to be the same, the Z U of No. 2 must be followed by Q. In the table find Q in cipher alphabet No. 2. It appears under T (plain). Add these values.

Plain ----	A	Y	T
Cipher (1)	M	H	C
Cipher (2)	Z	U	Q D
Cipher (3)	E	A	Y
Cipher (4)	A	Y	T
Cipher (5)	U	Q	D

Continue building in this manner:

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

The sequence builds up to 13 letters and then starts to repeat. This means that in arbitrarily selecting Y (plain) as following A, we happened to hit upon an even numbered interval. That is, in the original component, A and Y were an even number of spaces apart. We must try again, using a letter other than Y as the second of the sequence. Try Q and build as follows:

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

This sequence builds to 26 and all 6 sequences are the same. This recovered sequence may be the original used or it may be one of its eleven equivalent sequences. (The table above will decipher all messages in the same key). First, examine the sequence for evidences of "system":

5 5 5 5 5

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

1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2

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

The letters F G H J K L in reversed order are spaced at intervals of 5. Write the sequence on a horizontal line and try to complete the figure:

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

The attempt is unsuccessful but there is so much evidence of transposition in the spacing of F G H J K L that we are certain there is a keyword hidden in the sequence. Obviously, our sequence is not the original, but is one of the equivalents. Decimate the sequence to get the other five equivalents, one of which must be the original or its reverse:

```
                    7           7           7
Int. 3 -    A F Y K T Z N U G Q L D P M W H R C V S X B J I E O

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

                3   3   3     2   3   5     3   3
Int. 7 -    A D J U V K W O L B N C Y M E Q X Z R F P I G S T H

Int. 9 -    A K N Q P H V B E F T U L M R S J O Y Z G D W C X I

Int.11 -    A B R D N F J C P U Y I V M G K E S W Q T O X H L Z
```

Scrutinize all equivalent sequences for evidences of system. In Int. 3, the sequence F G H J K L is all spaced at 7 but yields nothing. In Int. 5, the spacing of this alphabet does not look promising. In the Int. 7 sequence, the series B C E F G H J K L N with spacing 2-3-5-3-3-3-3-3-is characteristic of alternate transposition. Write these letters on a horizontal line and fill in the intervening letters of the sequence on either the vertical or diagonal in alternate directions:

```
  L Y M
B C E F G H J K L N
N Q R
X Z
```

This looks good-- complete the figure:

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

Therefore, the keyword is OLYMPIAD transposed by alternate diagonal transposition, and O (plain) is set against PTION (cipher).

15. In the illustration given above, the enciphering table given in paragraph 13 was filled in solid. Very often upon completion of solution of a problem this table will contain many blanks because the cipher text of the problem was insufficient to recover all values. When blanks are numerous it is often necessary to exercise ingenuity in building up the sequences illustrated in paragraph 14. Once the sequences are completed and the key is recovered, the blanks in the ENCIPHERING TABLE can then be filled in.

KEY RECOVERY WHEN BOTH PLAIN AND CIPHER COMPONENTS ARE UNKNOWN (AND DIFFERENT) SEQUENCES

16. In the Enciphering Table given in paragraph 13, cipher alphabet No. 4 was a standard alphabet, the same as the plain component in the table. This was sufficient evidence to believe that the cipher alphabets were associated alphabets and the plain and cipher component were identical sequences. Had cipher alphabet No. 4 not been the same as the plain component, there would have been no way of learning at the start whether the plain and cipher components were identical or different sequences. However, the method of attack is much the same in either case. Not knowing whether the plain and cipher components are identical, it is assumed that they are not. An arbitrary sequence is built up as in paragraph 14, using only the cipher alphabets in building cipher sequences which are the same. The plain text values are recorded, as in paragraph 14, and the plain sequence thus built up will quickly show whether it is identical with or different from the cipher component.

17. As an illustration, the following ENCIPHERING TABLE is recovered:

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

At first glance the cipher alphabets may seem entirely dissimilar. Closer inspection will reveal the presence of reciprocal values. For example, in the 2 cipher alphabets, note the pairs U_1 P_2 and P_1 U_2 B_1 R_2 and R_1 B_2. Compare plain text values with each cipher alphabet in turn: $D_p=L_1$, $L_p=D_1$ etc; $F_p=J_2$, $J_p=F_2$. Therefore, the plain and cipher components are the reverse sequence of each other, and all the values are reciprocals. Knowing this, it is easy to construct an arbitrary sequence such that the cipher alphabets are both the same and the plain alphabet is the reverse of the cipher alphabets. Note in the Enciphering Table the values:

Plain ----	V	W	X	Y	Z
Cipher (1)	N	K	J	H	G
Cipher (2)	L	O	C	Z	Y

In Cipher (1), the sequence N K J H G or, reversed, is in natural order. In Cipher (2), Z Y is in natural reverse order, and the letters L, O, C, I, M must be in the keyword. To obtain more values, record the values corresponding to G H J K N appearing in the plain component and N K J H G in Cipher alphabet (2).

Plain ----	G	H	J	K	N
Cipher (1)	Z	Y	X	W	V
Cipher (2)	H	G	F	E	D

Plain ----	D	E	F	G	H	J	K	N
Cipher (1)	L	O	C	Z	Y	X	W	V
Cipher (2)	N	K	J	H	G	F	E	D

We have now picked up D E F (or F E D) to add to our sequence D E F G H J K N. At this point the two sequences D E F G H J K N and V W X Y Z C O L have been recovered and it is known that letters C I L M O are in the keyword. To extend our recovered sequences, let us assume for the purposes of trial that the low frequency letters P and Q are not in the keyword and can be added to our D E F . . . N sequence:

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

If this is correct, U is in the keyword and we may prefix I A to the D E F . . . sequence.

Plain ----	I	A	D	E	F
Cipher (1)	M	U	L	O	C
Cipher (2)	Q	P	N	K	J

Check.

We now know that the keyword starts COLUM, and ends in I or A, and we have recovered sequences I A D E F G H J K N P Q and S T V W X Y Z C O L U M leaving only letters B and R to place. The key is obviously COLUMBIA. The plain component and the cipher component are reversed, producing reciprocals. In reciprocal systems, it is usually possible to complete key recovery with fewer recovered values (i.e., with more blanks in the Enciphering Table than other systems of this general class. In systems where the plain and cipher components are different and independent (non-reciprocal), it is necessary to recover a few more values in the tables to reconstruct the sequences than is the case with reciprocal systems or with the plain component a standard alphabet.

18. Another illustration is given of this type in which both the plain and cipher components are unknown (and different) sequences. The recovered enciphering table is:

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

The 2 cipher alphabets appear different and there is no evidence as to whether the plain component is the same or a different sequence from the cipher component. Lacking information, it will be assumed that the 2 components are different sequences and a sequence will be constructed which will be the same for cipher alphabets No. 1 and 2. If the plain component is the same as the cipher

component, the plain sequence will turn out to be the same as the cipher. Constructing the sequence by the method illustrated in paragraph 14:

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

It is now seen that the plain component is different from the cipher component. Neglect the plain component for the moment and recover the key from the cipher sequence:

		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
Equi -	(1)	A	V	Y	Q	O	I	N	F	K	T	W	Z	R	D	S	B	G	M	U	X	L	H	E	P	C	J
val-	(2)	A	Q	N	T	R	B	U	H	C	V	O	F	W	D	G	X	E	J	Y	I	K	Z	S	M	L	P
ent	(3)	A	I	W	B	etc.																					
Se-	(4)	A	F	S	H	etc.																					
quen-	(5)	A	T	U	V	etc.																					
ce	(6)	A	Z	E	F	etc.																					

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

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

Keyword for cipher component is RHODE ISLAND transposed by vertical route transposition.

To obtain the key for the plain component, rearrange the values to correspond to the correct arrangement of the cipher component:

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

The arrangement of the plain component is the original and it is necessary to write out the equivalent sequences. The spacing indicates alternate transposition.

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

Plain component keyword is NEWPORT transposed by alternate vertical transposition. N (plain) sets against A (1) - V (2) cipher.

RECOVERY OF A LITERAL KEY FROM A NUMERICAL KEY

19. Before illustrating the method of recovering a keyword from the numerical key found by solution of a cryptogram, the reverse process will be explained, that is, how a numerical key is obtained from the keyword. Suppose the keyword to be used is GUANTANAMO. Starting at the beginning of the English alphabet (A) and over it write a 1, i.e.,

1
GUANTANAMO. Over the second and third A's write a 2 and 3 respectively:

1 2 3
GUANTANAMO. Search for B's, C's, D's, etc. There are none and the next letter in order of appearance in a standard alphabet is G, which is marked 4, followed M(5), N(6), N(7), o(8), T(9), U(10):

				1					
4	0	1	6	9	2	7	3	5	8
G	U	A	N	T	A	N	A	M	O

Similarly, the numeral keys for the word COMMUNICATIONS is:

2 10 6 7 14 8 4 3 1 13 5 11 9 12
C O M M U N I C A T I O N S.

20. Having a numerical key, to find the literal key or keyword is more or less a trial and error process. Suppose the key is 2-3-7-1-8-9-5-4-6-10. The digit 1 marks the position of the lowest letter of the English alphabet appearing in the keyword. It may be "A", or it may be B, C, D, E, F. The chances are that it is one of these six. Write these possibilities under digit 1:

2-3-7-1-8-9-5-4-6-10
A
B
C
D
E

The letter "A" cannot possibly be in the position of digit 2. The letters, B, C, D, E, F, G, H, I, J, K are possibilities. In the position of digit 3 and 4, the letters may also be B, but since B is low frequency letter it is unlikely. Continue this process for each digit.

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

The possibilities are recorded as shown. In this particular problem the numerals are in such an arrangement that there are a huge number of possible combinations. This is due chiefly to the fact that 2-3-4, 5-6, and 7-8-9-10 appear in series from left to right. The process from now on, in this and other problems of this type, is one of trial and error.

Let us suppose that the first letter of the keyword is a consonant, either B, C, or D. If that is true, the second letter is probably a vowel, E or I. Also, the fourth letter under digit 1 is probably A. Mark the assumptions in the table:

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

If the second letter is E, the 8th letter of the keyword under 4 might also be E, a high frequency letter which often occurs twice in 10-letter words. Mark it tentatively.

If the first letter is a consonant (B, C, D) the second a vowel (E, I) and the fourth a vowel (A), the third must be a consonant, probably between F and R. The digit series 7-8-9-10 may represent one letter, or as many as four different letters, but probably not more than three.

The chances are that at least one of the letters involved in this series is a high frequency letter and appears twice or more. All four of the series should be between J and U, and at least one of the letters is an R, an S, or a T. Block off these probabilities.

The letter in position 8 should be a consonant. If 4 is an E or I, 10 is probably a consonant or it may be Y.

With this further blocking off completed, an attempt is made to fit a word. The keyword may be anything, but knowledge of the most common combinations is still valuable. Taking the first two letters, DE is more common than BE or CE as a

word beginning. On this assumption we have De-A. Various combinations are tried with the consonants in position 3. When P is tried, DEPA immediately suggests DEPART. We find that R and T fit in with our previous analysis of the letters which could appear in position 8 and 9. The rest of the word ment suggests itself and is found to check.

21. In recovery of the keyword from a numerical key there are no thumb rules that can be furnished the student. A knowledge of letter combinations is helpful and reasoning can be applied in a small measure as illustrated in paragraph 17. In general the longer the numerical key is, the less chances there is of the possibility of more than one word fulfilling the conditions. Very often short numerical keys will yield several literal keys and for all practical purposes one keyword recovered from a numerical key is as good as another. However, there is a certain amount of satisfaction in recovering the word actually used and the student almost invariably knows when he has recovered the correct word.

22. In this pamphlet the common types of keys and keywords have been covered. There are variations of the methods illustrated which may be encountered from time to time and which should offer no difficulty if this pamphlet is understood. After all, we must of necessity leave a great deal to the ingenuity of the student. Our method is to point out the right general direction but to let him find the path for himself.

23. Key recovery is very important because it is used constantly in the practical applications of cryptanalysis. Cryptographic systems are not changed often in modern communications, but key are changed frequently. Complete reconstruction of a system discloses every bit of information concerning it with the result that when a key is changed but the basic system remains the same, reduction of the new key is simple and rapid.

RECOVERY OF LITERAL KEY-SETTING OF ALPHABETS PRIOR TO SOLUTION OF PROBLEM

24. In the general subject of key recovery there is a short cut method of determining, even before actual solution commences, the actual cipher letters of each alphabet in a periodic cipher which are set against one of the letters of the plain component, if such a setting has been made in accordance with a literal key-setting word. Just as keyword alphabets are employed in order that correspondents may remember them without recording the, the key-setting, or point of coincidence between a designated letter of the plain component and each cipher alphabet, is usually an easily remembered word. The most common letter of the plain component against which the cipher alphabets are set is A, regardless of A's position in the plain component sequence. For example, in the following:

Plain ----	A	B	C	D	E	F	G	H	.	.	.	.	.
Cipher (1)	N	V	Q	R	D	P	O	M	.	.	.	.	.
Cipher (2)	A	X	T	N	V	Q	R	D	.	.	.	.	.
Cipher (3)	V	Q	R	D	P	O	M	S	L	.	.	.	.
Cipher (4)	Y	L	J	H	C	U	A	X	.	.	.	.	.

The cipher alphabets were set against A (plain) in accordance with the key-setting word NAVY (cipher).

25. After the determination of the number of cipher alphabets has been made, the frequency table is constructed. Since A (plain) is the 4th highest frequency letter, the cipher letters which represent A in each alphabet should be the fourth highest cipher letters in their respective alphabets. If the letter distribution in each alphabet is in accordance with the theoretical average appearing in the Standard Frequency Tables, the 4th highest cipher letters will immediately spell out the key-setting. Although the letter distribution in cryptograms of practical length is not in exact accordance with the average distribution, it is often possible to extract the key setting by listing the cipher

letters of each alphabet in accordance with their frequency of occurrence and tracing out the key-setting word. For example, the following table was obtain from actual cryptogram:

Cipher

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
(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	3	8	7	3	1	3	1	2	1	4	-	-	1	-	-	2	-	-	4	7	12	-	9
(3)	1	-	3	4	1	1	9	10	2	5	-	-	-	1	6	5	1	2	-	4	4	7	1	1	9	-
(4)	1	-	-	1	-	11	5	1	4	3	10	4	3	1	4	2	6	2	-	2	9	2	-	4	1	1
(5)	5	10	12	1	-	4	-	4	-	7	-	2	1	-	2	6	3	-	3	7	-	-	3	3	1	4

Alphabets

Listing the letters of each alphabet in their order of frequencies, it is not difficult to trace the word SCOUT, which is correct. A knowledge of the type of key formerly used in SIMILAR systems from the same source is helpful. Also from the length of the keyword being sought, the maximum and minimum number of vowels to be expected should be estimated as an aid in tracing the word.

1	2	3	4	5
V	X	H	F	C
N	Z	G	K	B
E	E	Y	U	J
S	C	V	Q	T
W	F	O	G	P
Z	W	J		A
		P		

26. An alternate method of using keywords is to set the key letters of the cipher component against the first letter of the keyword of the plain component (i.e., problem No. 2, assignment No. 5 of the Elementary Course in Cryptanalysis). Since the letter in question will probably be a high frequency letter, it is often possible to trace out the keyword setting. The process will be just like that described herein except that the cipher values for A (plain) will not be obtained.

27. This short cut will not always work because of insufficient text or letter distribution so irregular that it is impossible to find the key. Some of the key letters may not appear in the first dozen highest frequency letters. However, a trial of this short cut method takes very little time - the frequency table must be made anyway - and when it is successful the gain is great. First, the value for one important vowel is found in each alphabet and even more important, the spacial relationship between the cipher alphabets is indicated which will be of great assistance in reconstructing the cipher sequence as soon as a correct plain text assumption is made.

B L A N K

Op-20-GR

RESTRICTED

NAVY DEPARTMENT
Office of Chief of Naval Operations
WASHINGTON.

ELEMENTARY COURSE IN CRYPTANALYSIS

TRAINING PAMPHLET No. 2

GENERAL PRINCIPLES OF COMMUNICATION SECURITY

1. Communication security, as a subject, is at least 2,000 years old, for we find in the writings of the ancient Greeks and Romans, references to the ciphers used by them in their military campaigns. Throughout the ages, greater or lesser attention has been paid to the subject by virtually every nation which has engaged in warfare or diplomatic intrigue. But not until the Great War did it become a subject of sufficient importance to warrant more than a cursory interest on the part of any except those engaged in the inner circles of the work.

2. As a matter of fact, those experts who were most vitally concerned did everything within their power to keep the subject away from the glare of publicity. They felt, and justly so, that the smaller the group of persons who were cognizant of the security measures taken and the results of counter-espionage work, the less chance there would be of drying up the sources of information which careless enemies left open. Such a policy did very well as long as the number of messages which had to be enciphered remained small and within the capabilities of small groups of people. With the Great War, however, with its operations on an unprecedented scale and with the development of radio with its illimitable possibilities for the passing of information and orders, the handling of secret communications became absolutely impossible for the small, well-trained groups of people which had formerly been entrusted with it.

3. This was the time when the fallacy of the "ostrich policy" became not only apparent but disastrous. Poorly trained troops were rushed into the field with codes and ciphers which they did not understand and which they could not have been expected to handle properly. The result was an avalanche of misguided effort which enemy cryptanalysts were quick to seize upon and convert to valuable information.

4. With the ending of the war there was a marked change in policy with regard to communication security by all of the nations which had participated. Each one said in essence, "By keeping our methods of communication security so away from enemy eyes, we failed to let our own people in on the secrets. Thus, when called upon to function in the heat of battle they failed, and nothing else could have been expected. That will never happen again."

5. It may happen again, but the chances are very much against it. Since the war there have been innumerable books written in whole or in part concerning the role which communication security, and lack of it, had to play. Much of the literature has been for popular consumption and has proved extremely welcome. Much of it has been technical in nature, for the lessons of the war, and the developments of communications in general have both pointed to an even greater part for this element of military effort in any war to come, and the development of experts capable of dealing with it is essential. Some of it has been general and some of it has been most detailed in nature. But regardless of the general tenor, all of the literature and all of the experience gained points to the fact that only by education and indoctrination of all concerned, may communication security be successfully maintained.

6. The purpose of this pamphlet is merely to present in as readable form as possible, some of the lessons which have been learned and some of the measures that must be taken if we are to keep our vital secrets away from prying enemy ears.

7. "Communication Security" embraces the principles governing the safeguarding of information, conveyed by any means, (publications, letters, radio,

visual, cable or landline telegraph, mail, messenger, and word of mouth) from falling into the hands of unauthorized persons, no matter how remote they may be from connection with potential enemy services. The conclusions reached herein pertain primarily to information transmitted by radio, but apply as well to other forms of communication. These conclusions are in no way based on hypothetical supposition, but, on the contrary, have been developed through actual experience, our own and that of other nations. Examples and authentic anecdotes are given in support of many of the ideas presented, but, in some cases, these are vague and lacking in detail for reasons which, it is thought, will be obvious.

8. Some of the means by which secret information may reach unauthorized persons are:

(1) Careless conversation.
(2) Careless handling of translations of encrypted despatches.
(3) Careless censorship of material released to newspapers and periodicals.
(4) Careless handling and safeguarding of secret publications.
(5) Improper classification of matter and improper selection of systems of cryptography.
(6) Careless radio operation.
(7) Cryptanalytic solution of code and cipher systems.
(8) Improper selection of communication facilities.
(9) Espionage.

9. The order of tabulation does not indicate order of importance. Such indication would be impossible because it is dependent upon time, place, and existing conditions. Forgetfulness of any one weakness may bring about calamity.

CARELESS CONVERSATION

A wise old owl lived in an oak;
The more he heard, the less he spoke;
The less he spoke, the more he heard--
Why can't we be like that wise old bird?

10. Admiral Bacon, R. N., has said, "So long as plans are locked up in the minds of the admiral and his one or two chief assistants, secrecy is possible. As soon as parts have to be let out, secrecy is apt to vanish. Mind you, when a person has guessed a secret, he usually feels himself quite at liberty to talk about it even if it be against the interests of his country, simply because it has not been divulged to him under the bond of secrecy. It is gratifying to some to let others know how clever they have been in guessing a plausible solution." It is typical of the American character to dislike ostentatious secrecy and to abhor secrativeness in any form. Admirable as this trait may be, it is a dangerous one in officers who must, by reason of their profession, keep in their heads information, the disclosure of which would be inimical to the interests of the country. The officer who, in the midst of a conversation on professional topics, finds it necessary to say, "I would rather not talk any further on that", feels uncomfortably, and, perhaps justly, like a character in a melodramatic novel. There are other ways, and, after all, sudden silence after unrestrained volubility can be as revealing as the most open statement of fact. The officer in frequent contact with outsiders can adopt one of three poses with regard to talking shop; he may assume consistent silence, he may resort to consistent and mendacious garrulity, or he may consistently plead ignorance. The first and last are undoubtedly the safest. The second is a method for experts: the old fashioned sailor who regaled visitors to his ship with "tall tales" about the vessel and its gear may not have been a model Christian, but he had his points.

11. In discussing professional subjects with persons in whom one has the utmost confidence--close friends or members of one's family--it is well to consider that, although they would never knowingly reveal information given them, still they may, in ignorance of its importance, inadvertently pass on some detail to a third person in casual conversation. Confidential information can be actually embarrassing to one who has no need of it, and is therefore much better kept locked behind the lips of those for whom it is of professional interest and who

are capable of realizing all of its possibilities. Some of those who served out of San Diego in the autumn of 1929, just prior to the commencement of the decommissioning of certain destroyers, may remember that, although the question of decommissioning was given a confidential character by Commander Destroyer Squadrons, and personnel were warned not to discuss it outside of the service, yet all the developments as they appeared were common knowledge throughout the vicinity of the fleet base. As a remoter, although far more serious "horrible example", witness the embarrassment of high British officials after Jutland when they found that the "rocking-chair brigade" around the tea-tables of London was chatting freely about the secret (so carefully guarded at the Admiralty) that the loss of British ships in the engagement was due to improper design of ammunition supply from magazines! In this connection, it is not the purpose of this pamphlet to enter into a digression into the relative merits of the two sexes in the exercise of discretion, so that the following unauthenticated anecdote will have to stand without further discussion.

12. History tells of the strange report that went the rounds during the early part of the war to the effect that 250,000 Russian troops had landed on the French Channel coast via Scotland and England, for service on the Western Front. The report caused a certain amount of consternation in Berlin and was believed by many in Paris. It exercised such control over the imagination of one German agent in Scotland that he actually reported having seen them--"huge, bearded men with snow still clinging to their boots". It is said that this fantastic tale was started on its way by British Intelligence officers who carefully imparted it as a deadly secret to ladies of their acquaintance!

CARELESS HANDLING OF TRANSLATIONS OF ENCRYPTED DESPATCHES

13. If the unguarded tongue is a menace to security in general, then the wastebasket is a double menace to communication security. For translations of encrypted despatches which are carelessly tossed in innocent-looking wastebaskets are not only available to an alert enemy for the information which they themselves divulge, but are of inestimable help to enemy cryptanalysts in the solving and reconstruction of the cryptographic systems utilized.

14. It simply stands to reason that if an expert cryptanalyst can obtain a copy of the cipher text of the message (a comparatively easy procedure) and then obtain an exact translation of it (as from a wastebasket), then by a simple process of working backwards, the values can be deduced, the general method worked out and subsequent messages in the same system read with ease. It is just one such "break" that cryptanalysts dream and hope for.

15. A paraphrase of the exact translation is of but slightly less value to the cryptanalyst. In many cases all he needs to know in order to be able to break into a message is the general subject--whether it concerns "submarines" or "battleships" or whether or not a date mentioned is "November 21" or "December 31". This means that although translations should always be paraphrased for distribution, the paraphrased copies should be as zealously guarded as the exact translations--and more particularly, that nothing connected with encrypted messages should ever be consigned to the ordinary wastebasket.

16. It is a fact that during the Peace Conference in Paris after the World War, the paper from the wastebaskets of the delegates became an almost openly marketable commodity. Scarcely a piece of writing on the subject of international espionage is published without some mention of the services of charwomen in this respect. Whether such writings can be trusted or not is beside the point. They at least reveal the possibilities in this direction.

17. The moral is: All notes, work sheets, carbon paper, and other materials used in coding work must be destroyed by burning as soon as possible, and, all translations, exact and paraphrased, must be kept in carefully guarded places until their usefulness is at an end, when they too must be destroyed by burning.

TRAINING PAMPHLET No. 2

CARELESS CENSORSHIP OF MATERIAL RELEASED TO NEWSPAPERS

AND OTHER PERIODICALS

18. Closely allied with the revelations made in indiscreet conversations are those made as a result of careless censorship in releasing material to the press. It must always be remembered that the press of a nation may, in general, be considered as extremely loyal and as anxious to help win a particular war as any other body of the citizenry. On the other hand, it must likewise be remembered that the business of the press is to obtain and publish news. It is going to publish anything it can lay its hands on, unless it realizes the inherent dangers to the security of the country in the publishing of such news. This means that all news concerning a nation's military operations (and therefore coming under the cognizance of military censors), which it is desired to keep secret, must (1) be kept from the press, or (2) be given to the press with a frank statement as to its danger.

19. The second method is invariably the best, for the ability of "newshawks" to ferret out news, despite efforts to keep it hidden, is axiomatic. It is the newshawk's only reason for being. Some of the nations in the Great War realized this fact and made most of it.

20. For instance, when the British Admiralty, early in 1918, planned to block the Zeebrugge submarine base entrance with concrete-filled block ships, it was decided to commandeer two Mersey River ferries for the purpose. As these craft were sure to be missed by the people of Liverpool and vicinity, and undesirable publicity threatened, the entire press of Britain was taken into the secret and their cooperation requested. Never a sign or trace of the news leaked out, and the press loyally carried out the wishes of the Admiralty.

21. It is significant that this instance of taking the press into the confidence of the nation came after 3 long years of war. Some earlier experiences with the press had not been quite so satisfactory. Admiral Jellicoe, for instance, had been most zealous in keeping news of the fleet away from the press and had thereby incurred its violent dislike. This dislike showed itself after the Battle of Jutland when the press, with presumably the best of intentions, flayed the administration and the naval command at sea. Whether or not this attitude hurt the British and Allied cause in the long run is doubtful, but there can be no question but that it hurt the British morale at a time when the best of morale was needed.

22. Another point to be constantly borne in mind in dealings with the press is that even the most innocuous-looking items of news may carry information of vital importance. The relation of every piece of information to the broad general picture must always be allowed for.

23. Early in 1918, it was known that the Germans were preparing a great spring offensive on the Western Front. Where they would strike was not known. In Switzerland, an intelligence agent of the Allies, in glancing through a small Baden journal came across a letter to the editor from the proud mother of a young German aviator who had lost his life while flying over the area of the Fifth British Army. She quoted a letter of condolence and sympathy from the German Army Commander in that area. It was signed "Von Hutier." The provincial editor had evidently seen no harm in printing it.

24. Never before had Von Hutier, organizer of the victorious campaign at Riga and elsewhere on the Russian front, been located on the Western Front. His taking over part of the line was a secret, carefully guarded by the Germans. The learning of this secret was the entering wedge by which the British Intelligence, through further research, of course, determined where, when, and how the expected offensive would break. Von Hutier's character, his past record, his location, all pointed to the crossing of the River Oise as the opening move in an attack with Amiens as objective. The British line was ready at the proper time--and Von Hutier did not accomplish his mission. This incident is especially interesting in showing from what small acorns of information the complete oaks of connected intelligence may grow.

TRAINING PAMPHLET No. 2

CARELESS HANDLING OF REGISTERED PUBLICATIONS

25. The business of modern navies has become so complex and technical that each navy strives to keep from the others those bits of information which it has laboriously arrived at and which it thinks will give it an advantage over others, if and when they should clash in another Jutland or another Coronel.

26. These bits of information are multitudinous in number and can only be recorded in sets of books which go to make up the confidential libraries of each navy. Among such books are the codes and ciphers, the instructions and all the other paraphernalia connected with cryptographic systems. "Security" in general, is interested in the safeguarding of the entire library. "Communication Security" is interested in preserving our cryptographic paraphernalia from prying enemy eyes.

27. At the outbreak of the World War the British Navy set up a gigantic cryptanalytical organization in the Admiralty which later became the famous "Chamber 40." Little is known concerning the success or failure of this organization at strictly cryptanalytical work, but it is known that German code books recovered from the German cruiser MAGDEBERG, which ran aground and was wrecked off the coast of Russia, found their way to "Chamber 40", and it is fact that "Chamber 40" produced invaluable intelligence on which were based many of the British operations. It can be no secret that at least some of this intelligence came out of the code books recovered from the MAGDEBERG, and yet, as far as is known, these books were not superseded for 2 years.

28. The first undoubted and absolute principle of communication security is preservation of the physical security of codes and ciphers and all that pertain to them.

29. It is not enough that such material be preserved permanently, or until they are superseded or placed out of effect. It must be kept constantly under proper supervision and in carefully guarded places. The reason for this is that an enemy agent, intent upon obtaining the information contained in a code book, will seize and keep the book for a length of time only sufficient to have it photographed and then return it, hoping that its absence from its authorized place has not been noticed. It has been estimated that a reasonably large-sized code book may be photographed in 2 hours. Codes or ciphers left on wardroom transoms are a menace, not only to the officer who is "signed up" for them but to the entire naval service.

30. Furthermore, it is vital that proper precautions be taken to insure that unauthorized persons are not allowed access to secret files or spaces containing secret files, or knowledge of the contents of such files. Even within the service there is no reason why officers unconcerned with secret matters or communications should have any access whatever to secret stowage until it becomes necessary in the normal conduct of their duties. As in a previous paragraph, it is appropriate to remark that unnecessary secret information is a burden to him who holds it.

CARELESS RADIO OPERATION

31. The historically outstanding examples of good and poor radio discipline may be found in any account of the conduct of British and German naval operations during the World War. The German commander in chief made a practice of sending out numerous operation orders by radio before a sortie, with the result that the radio direction finders of the British enabled them to know in every case when the enemy fleet had left Wilhelmshaven for the outer anchorage in the Jade. On the other hand, the German attempts at radio direction finding never succeeded in obtaining information of value.

32. The World War and our own fleet problems and exercises of past years are rich in examples of the proper and the improper use of radio. The lessons learned show that attention must be given to many items--maintenance of radio silence, adherence to correct procedure, careful sending to reduce number of

repetitions, elimination of unnecessary and unauthorized transmissions, use of correct call signs, and so on.

33. But more important than blind attention to detailed and explicit orders in the preservation of radio security is an active and vivid imagination which pries into the question of what the enemy might be able to deduce from some particular transmission. The most innocuous-looking messages are sometimes loaded with military dynamite. For instance, one could not possibly have objected to the broadcasting of weather reports from the shore station at Scapa Flow. There was no information in them alone which could have been of any possible value to the Germans. However, instead of sending them out every day, the British sent them out only when important units of the Grand Fleet were at sea. A German operator at Neuminster noted this and for some time was able to advise his Admiralty as to when the enemy was at sea. No amount of radio discipline within the Grand Fleet could offset the damaging effect of those apparently innocent weather reports.

34. Nor was there anything particularly revealing in the fact that a "bier-abend" arranged for a group of destroyer officers at one of the German bases had been postponed. The British were supposedly not interested in how or when the Germans had their evenings of beer drinking. A radio message was therefore sent out to all the officers affected and likewise, to all intentional purposes, to the British Admiralty. But the British were interested in just such facts, particularly when linked up with other facts of a similar nature. In this specific case that message concerning the "bier-abend" served to justify completely the assumption that the Germans had a sortie on for that night--as indeed they did have. It resulted in the Battle of Dogger Bank.

35. Mighty events may well be outlined in tiny strings of innocent words.

CRYPTANALYTIC SOLUTION OF CODE AND CIPHER SYSTEMS

36. The failure of the great German offensive on the Western Front in 1918 may to a considerable extent be attributed to the work of one man, Captain Painvin of the French Intelligence Service. This officer, through decryption of German radio messages, was able to obtain vital information of the attack, prior to and during its progress. His "break" came as the result of an improper use of cipher on the part of perhaps no more than two German communication officers. Two days after the new German cipher had been put in effect (March 11, 1918), a German station transmitted in the old cipher a request for repetition of a message which had been sent out in the new. The originator obliged with the original message in the old cipher. The French now had the same message in the old, previously decrypted cipher, and in the new cipher upon which the Germans were depending for security of their plans. As a result the French were soon reading all German operation orders in the new system before the Germans themselves were quite accustomed to its use. This particular cryptographic error was enormously costly to the Germans.

37. That is an illustration of but one of the many coding errors which smooth the way for cryptanalysts. The instructions issued with each individual code or cipher must be followed carefully in order that the benefits of past experience may not be wasted through lack of knowledge. Experience is the best teacher, but the other man's experience is much less costly than one's own.

IMPROPER SELECTION OF COMMUNICATION FACILITIES

38. Undue radio activity in an area might serve to betray the location and movements of a fleet. It is also true that cessation of all radio signals will tend to indicate the imposing of radio silence and the probable imminence of a major operation. The German commander's great mistake at Wilhelmshaven lay in his use of radio where visual or mail boat would have served equally well with far greater security. Radio must never be used when telegraph, cable, courier service, guard mail, or visual can be made to serve the purpose.

39. In time of war an officer courier service is usually established between important points. Secret communications are not normally transmitted through the mails, but are forwarded through this courier service. Secret matter will be carried on the person of the messenger or kept in his immediate vicinity. On prolonged voyages in merchant vessels under the registry of the nation involved, such matter is usually kept in the safes of the masters or pursers in sealed containers. Sometimes an armed naval guard is assigned to accompany the messenger.

40. Diplomatic officers in various parts of the world use diplomatic pouches for transmission of correspondence to and from their capitals. These pouches may usually be used for certain naval correspondence. Their inviolability is guaranteed by international agreement. But, so was the neutrality of Belgium.

IMPROPER CLASSIFICATION OF MATTER AND IMPROPER SELECTION OF SYSTEMS OF CRYPTOGRAPHY

41. Information once transmitted in a secret system must remain secret forever. The contents of a secret message must not be revealed to unauthorized persons in any way. Conversely, information which cannot be kept secret or is not actually secret must not be put into a secret code or cipher. It has happened on more than one occasion that a ship of the Navy has been ordered to undertake a certain movement, the instructions for the operation being encoded in a secret system. Such operations always become public, and it is obviously fatal to transmit in secret code anything whatsoever concerning them.

42. The considerations of (1) selection of communication facilities and (2) classification of matter are closely allied in their effects upon cryptographic security. Cryptographic security is maintained by the proper employment and use of code and cipher systems. The degree of security attained will depend directly upon (1) the purposes for which codes and ciphers are employed, (2) the technical perfection attained by the personnel connected with code and cipher work, and (3) the length of time codes and ciphers are continued in effect. The length of time a system is continued in effect depends upon (1) the amount of improper employment and use to which the system has been subjected and (2) the amount of proper employment and use to which the system has been subjected. The effective periods of cryptographic systems are determined and prescribed by high authority.

43. It is obvious that, in order that cryptographic systems may be continued effective for reasonable lengths of time, a careful supervision must be maintained over the employment and use of these systems. This supervision is carried on through the function of message censorship which is the immediate responsibility of the communication officer under the commanding officer. In time of war, certain major activities will establish a continuous watch of "message censors", who will function under the communication officer and, in some cases, directly under an "assistant to the communication officer for cryptographic security." The duties of these "message censors" is indicated in detail in confidential instructions. In commands where the limited officer complement does not permit of establishment of a continuous watch of "message censors", the function of message censorship devolves directly upon the communication officer and his assistants, in peace as well as in war.

ESPIONAGE

44. The most accurate and valuable information concerning important matters is to be found in secret documents. The principal governments of the world maintain extensive intelligence services whose missions are to obtain such secret information of other governments. The forms of espionage which have been used in the past and which are being used to obtain information are extremely effective. It has been quite possible for an agent to gain information through the confidence of an unsuspecting individual or to gain access to a secret document, photograph it and return it without the knowledge of the custodian.

B L A N K

Op-20-GR

RESTRICTED

NAVY DEPARTMENT
Office of Chief of Naval Operations
WASHINGTON.

ELEMENTARY COURSE IN CRYPTANALYSIS

TRAINING PAMPHLET No. 40

A NUMERICAL METHOD FOR THE SOLUTION OF DOUBLE TRANSPOSITION CIPHERS

1. In any cipher problem, the student has been advised to attempt, whenever possible, key recovery simultaneously with recovery of plain text. Since, in transposition ciphers the plain text values are known at the start, such procedure is equally advantageous in solving this type of cipher.

2. If the complete plain text of a double transposition cipher has been recovered, key reconstruction is comparatively simple by means of various numerical processes. In addition, however, it is possible, provided a sufficiently extensive sequence of plain text has been recovered, to reconstruct by similar numerical means the transposition keys simultaneously with the recovery of the remainder of the plain text. Generally speaking, the longer the recovered plain text sequence, the easier this process is. If the transposition blocks are completely filled rectangles, the process is also considerably easier.

NUMERICAL EXAMINATION OF DOUBLE TRANSPOSITION PROCESS

3. Consider the nature of the typical double transposition process from a numerical standpoint. Each character in a line of normal plain text is separated by a numerical interval of 1. If the plain text is considered as a normal numerical sequence, it would read: 1-2-3-4-5-6-7-8-9-10-11-12.....etc.

4. Let us take as an example a plain text of 117 letters, with two transposition blocks 15 and 11 columns wide. In the first transposition block, with a key length of 15, each character in a column of the plain text is separated by a vertical numerical interval equal to the key length, i.e., in Fig. 1, column 13, 1-16, 16-31, 31-46, etc., each separated by a numerical interval of 15.

Figure 1 Plain Text Sequence in First Transposition Block

1st key -	13	7	5	4	10	1	8	15	6	12	2	11	3	9	14
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
	91	92	93	94	95	96	97	98	99	100	101	102	103	104	105
	106	107	108	109	110	111	112	113	114	115	116	117			

5. These columns of the first transposition block become lines in the second unit, with the characters now separated by a horizontal numerical constant, which is the length of the first key -- 15, as in Fig. 2.

ransposition Block

2	6	5	1
111/	11	26	41
43	58	73	88
94	109/	3	18
24	39	54	69
62	77	92	107/
112/	14	29	44
50	65	80	95
102	117/	10	25
16	31	46	61
75	90	105/	8

/

ɔe of 15, which is constant
. Notice also that there are
ıracters in the same second
ımns occur. For example,
ɔe of 51 occurs until the end
), and 63-114; then, a con-

LAIN TEXT SEQUENCE

ɥuence of plain text, for ex-
ı enciphered in this trans-

ı Block

12	2	11	3	9	14
10	11	12	13	14	15
25	26	27	28	29	30
40	41	42	43	44	45
55	56	57	58	59	60
70	71	72	73	74	75
85	86	87	88	89	90
100	101	102	103	104	105
115	116	117			

Figure 4 Plain Text Sequence in Second Transposition Block

2nd key -	11	3	7	4	10	8	9	2	6	5	1
	6	21	36	51	66	81	96	111/	11	26	41
	56	71	86	101	116/	13	28	43	58	73	88
	103/	4	19	34	49	64	79	94	109/	3	18
	33	48	63	78	93	108/	9	24	39	54	69
	84	99	114/	2	17	32	47	62	77	92	107/
	7	22	37	52	67	82	97	112/	14	29	44
	59	74	89	104/	5	20	35	50	65	80	95
	110/	12	27	42	57	72	87	102	117/	10	25
	40	55	70	85	100	115/	1	16	31	46	61
	76	91	106/	15	30	45	60	75	90	105/	8
	23	38	53	68	83	98	113/				

8. In Fig. 4, note the diagonal distribution pattern of this plain text sequence in the second transposition block. Such a pattern is quite characteristic of columnar transpositions. Note also that in block No. 2, a horizontal constant of 15 ordinarily separates plain text letters as mentioned previously. Skipping a plain text letter raises this constant to 30 naturally; skipping two plain text letters the constant becomes 45, etc.

9. The columns of the second transposition block are taken off in accordance with the second key to form the cipher text. Notice where the given plain text sequence values appear in this numerical cipher text.

Figure 5

41 88 18 69 107 44 95 25 61 8 111 43 94 24 62 112 50 102

16 75 21 71 4 48.....etc.

10. In this final numerical sequence in Fig. 5, we have a kind of spread-out numerical skeleton of the second transposition block. If the process used to construct this final sequence were reversed, we should be able to reconstruct the transposition keys by means of the mathematical relationships of these cipher sequence numerical values with each other.

EXAMPLE OF NUMERICAL SOLUTION

11. Given: The following two messages, each 117 letters in length, enciphered in the same double transposition system. Solve the message, work out the system, and recover the key.

Serial No. 1

ARPAD MEEDI CLNYS HODIS TNIIB RHTHI EOEPA GRLZT WGIHO HELDR

UIMDZ	TOEOV	NNNET	AIASI	IOCET	ANUDN	ERBEM	ADEIT	PTDGT	AIDUT
RKDSE	IRRMA	ETTAT	EE						

Serial No. 2

TOAEM	CSNDM	EUSES	SESAY	HTPAN	DCSCO	ENUTA	EERSD	DBRIN	NKTUB
DHAEE	IISAF	HTRIK	AIKTB	IAELE	AOIGR	RTNTO	RRVTD	DPTAI	NTIBT
RXDOU	CEVCD	EHLTR	HE						

12. Also given: The following plain text sequences from each message have been recovered by means of the anagramming process.(explained in Assignment No. 8).

Serial No. 1 -- P E R I O D A T Z E R O E I G H T H U N D R E D

Serial No. 2 -- D U R I N G T H E S E A T T A C K S B O M B E R

PROVISIONAL NUMBERING OF PLAIN TEXT SEQUENCES

13. Since the absolute numerical positions of these plain text letters in the original plain text 1-117 are not known, we provisionally assign them any numerical sequence, such as 60-83. It should be noted that adding or subtracting a constant from all the tabulated values does not alter the mathematical relationships mentioned before.

14. We then enter these provisional numbers on the respective letters in the cipher texts. Plot them in sequence, entering numbers, where available, in successive squares of a strip (2 rows wide 117 squares long). Duplicate the numbers in a second strip as in Fig. 6.

Figure 6

Cipher text (1) -	A	R	P	A	D	M	E	E	D	I	C	L	N	Y	S	H	-	-	-	-	-
Numbers (1) -					80		69									77	-	-	-	-	-
Numbers (2) -					80		69									77	-	-	-	-	-
Cipher text (2) -	T	O	A	E	M	C	S	N	D	M	E	U	S	E	S	S	-	-	-	-	-

In Fig. 6, cut the rows apart on the dotted line, forming two separate strips.

Note: Certain of these provisional numbers may be found to have more than one possible location on the cipher texts. That is, in the case of this particular pair plain text sequences, there are two possible locations in the cipher texts for each of the plain text pairs EU, ES, RE, OA, IT, HC, and three possible locations for the pair EE. Such a situation is likely to occur by chance whenever only two messages of similar underlying text are anagrammed. When three or more messages are anagrammed, the probability of such repetitions occuring is sharply reduced; for practical anagramming purposes, three or more messages would be used. For the sake of simplicity here, only the two messages given herewith will be used as an example of the process and the proper cipher text location for each number will be assumed to be established.

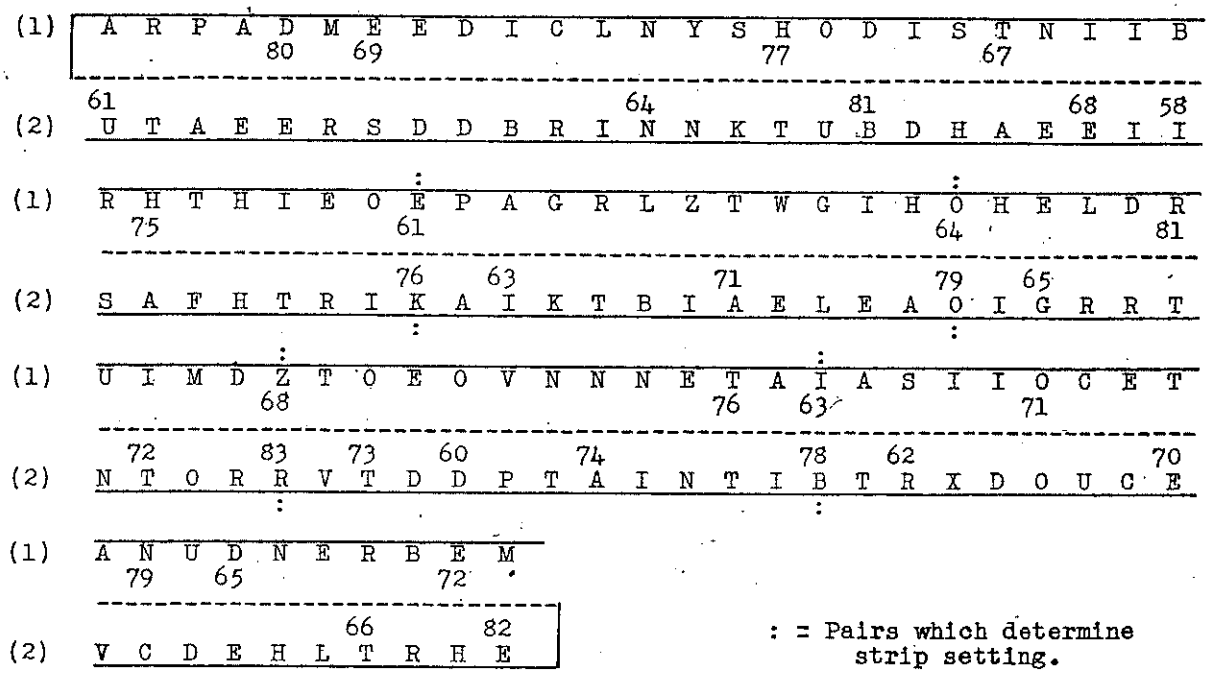
DETERMINATION OF FIRST KEY LENGTH

15. The next step is to discover the numerical constant which is the key

length of the first transposition block. By sliding one strip against the other, we can match various segments of the numerical cipher sequence and duplicate at some setting of the strips conditions within the second transposition block. When a constant numerical difference of reasonable recurrence is found, this difference will be the first key length or an integral multiple of that key length.

16. We slide the strips position by position looking for a constant difference and meet with no success, until the strips are set with (1) 61 over (2) 76, (1) 64 over (2) 79, (1) 68 over (2) 83, and (1) 63 over (2) 78, all checking at plus 15 as in Fig. 7. These four additives establish the first key length as 15. One further check on the additive 15 is found in the strip setting (1) 60 over (2) 75 when (1) 66 is over (2) 81.

Figure 7



: = Pairs which determine strip setting.

PREDICTION OF NEW VALUES

17. With the strips now set to give these differences of 15 as in Fig. 7, we can predict values in either strip for the unmatched numbers corresponding to the recovered plain text in the other strip, adding or subtracting 15, as the case may require. Some entries will be incorrect because the sequences end; but the correct picture will emerge as the new values are checked with the cipher text. That is, every numerical value recovered will also recover a new letter value in the plain text sequence, which should be built up simultaneously as a check on these numerical values. It pays to be bold in these first assumptions, because erroneous values will show up easily.

18. Using this procedure, let us build up values within the sequence shown in Fig. 7. Fig. 8 shows the results of the assumptions as follows: Starting with (1) 61 over (2) 76, we find the next space is blank; in the third space we assume a 48 to match the 63 by subtracting 15, and at the same time fill in Cipher A for position 48 in the plain text sequence in Fig. 9. Over (2) 71 we place (1) 56 which recovers (p-1) T. For (2) 65, (1) 50 is assumed, giving (p-1) E. (1) 81 gives (2) 96 and (p-2) T, (2) 72 gives (1) 57 and (p-1) I, (2) 73 gives (1) 58 and (p-1) O. The new plain text sequence TIO now looks promising. An N for position 59 in the plain text sequence should turn up. (2) 60

gives (1) 45 and (p-1) O, (2) 74 gives (1) 59 and the expected (p-1) N, completing the sequence TION. (1) 76 gives (2) 91 and (p-2) T.

Figure 8 Sliding Cipher Strips

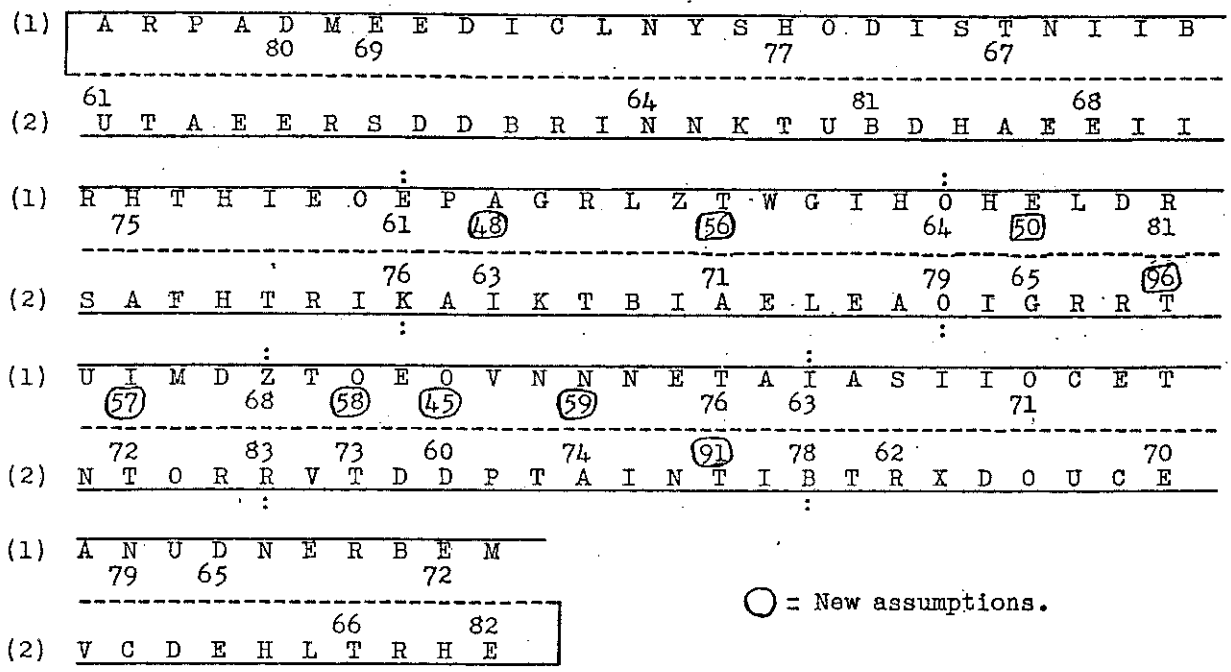
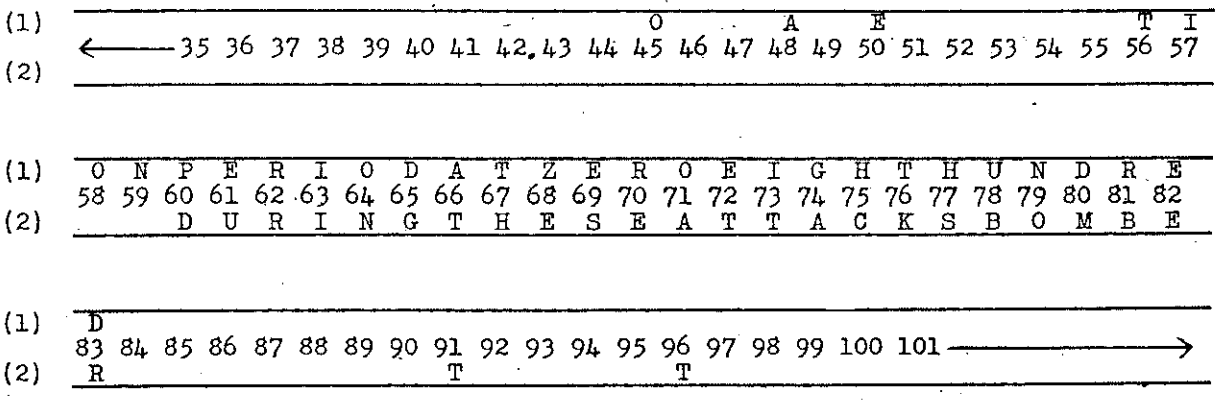
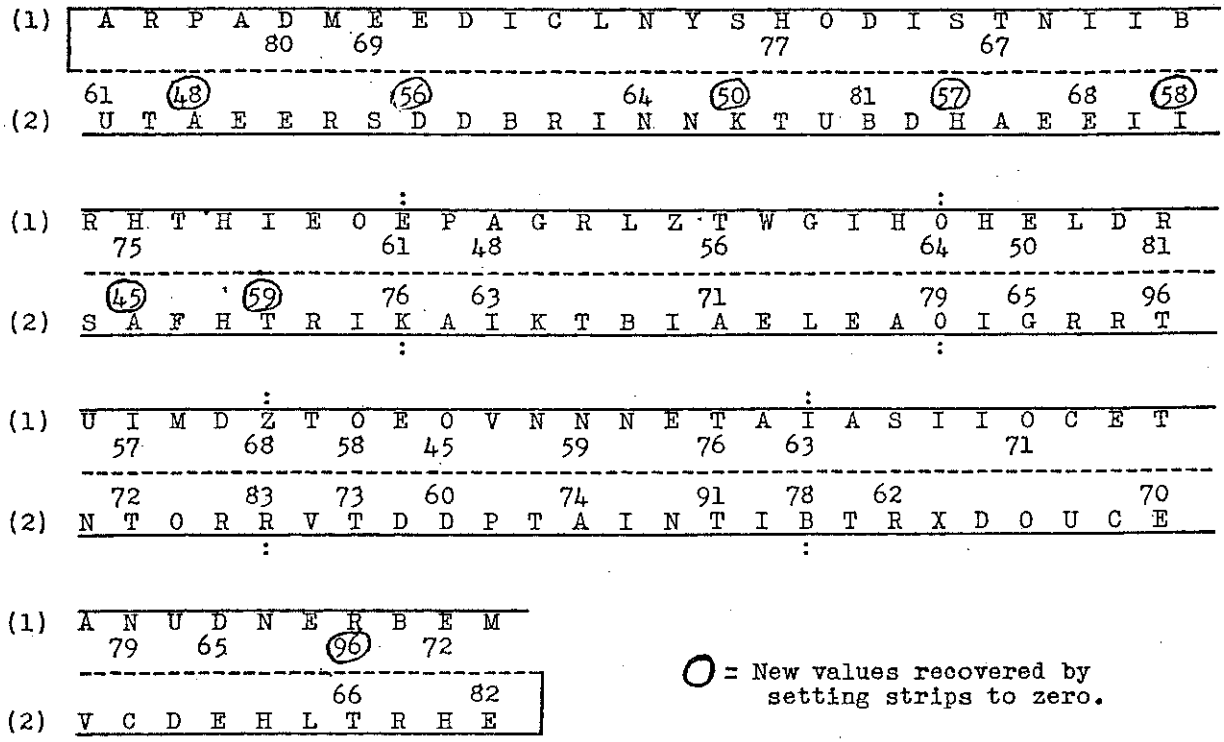


Figure 9 Plain Text Sequence



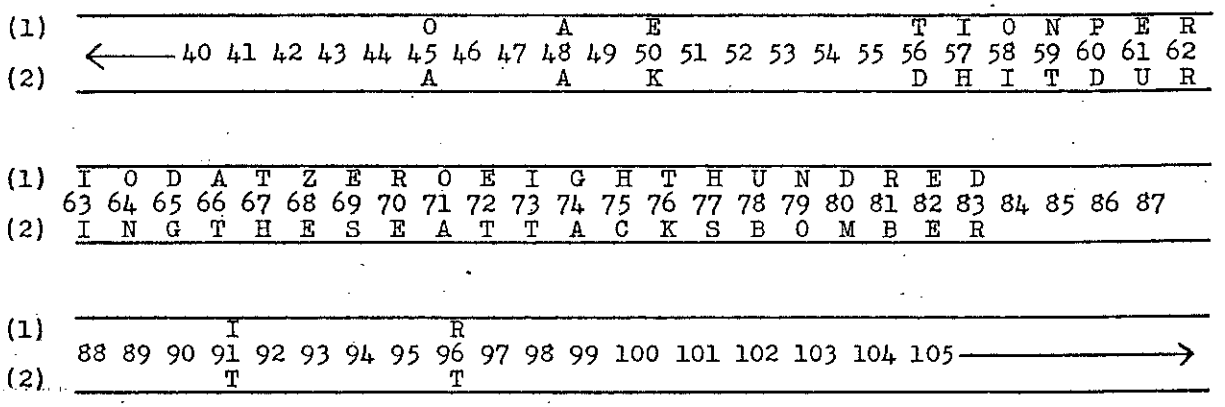
19. Now reset the strips to zero and enter the newly recovered values on both strips, as the case may be (Fig. 10). Additional plain text is now recovered. The sequence A - - K - K looks likely for A T T A C K (Fig. 11).

Figure 10 Sliding Cipher Strips



○ = New values recovered by setting strips to zero.

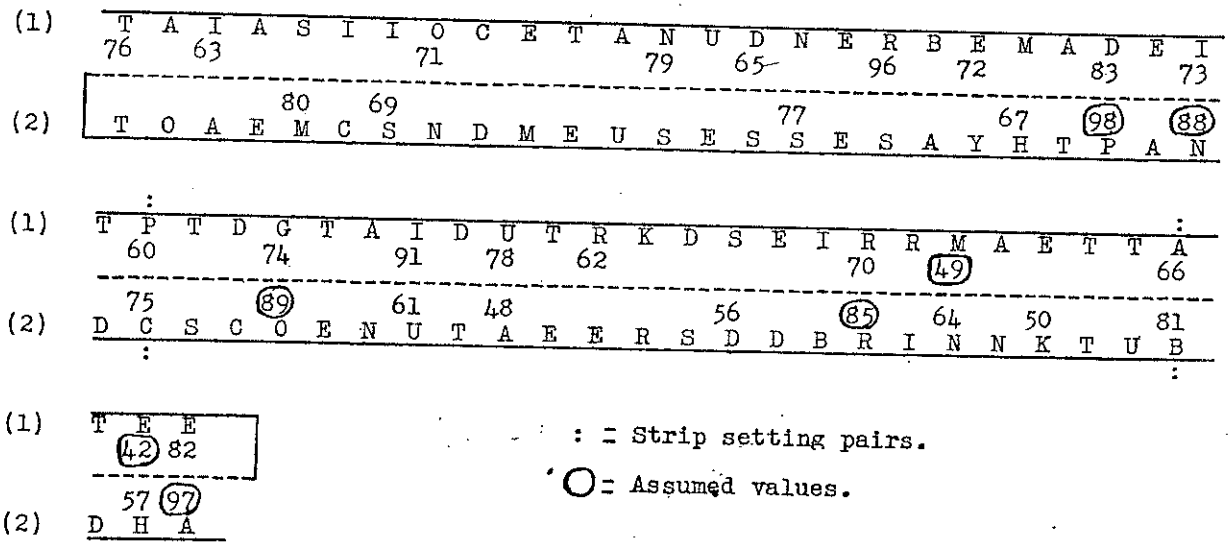
Figure 11 Plain Text Sequence



20. In Fig. 10, notice also that (1) 75 now appears over (2) 45, and (1) 96 over (2) 66, a constant difference of 30. This is what we might expect, an integral multiple of 15. Sequences containing these pairs build up as before, but with the constant difference of 30 instead of 15.

21. Return now to the (1) 60 over (2) 75 and (1) 66 over (2) 81 strip setting which was mentioned in paragraph 16. In Fig. 12, starting from (1) 60 over (2) 75, we find (2) 89 beneath (1) 74, recovering (p-2) 0. In Fig. 13, the general process continues as before; the strips are reset to zero after new values have been assumed. Additional sequences with differences of 30 or 34 will appear. These differences operate in precisely similar fashion as the constant 15, and may be filled in accordingly. The words ATTACK, FROM, and VISIBILITY soon become apparent. The remaining plain text will be gradually recovered as the strips are tried in new settings on the basis of the newly recovered numerical values.

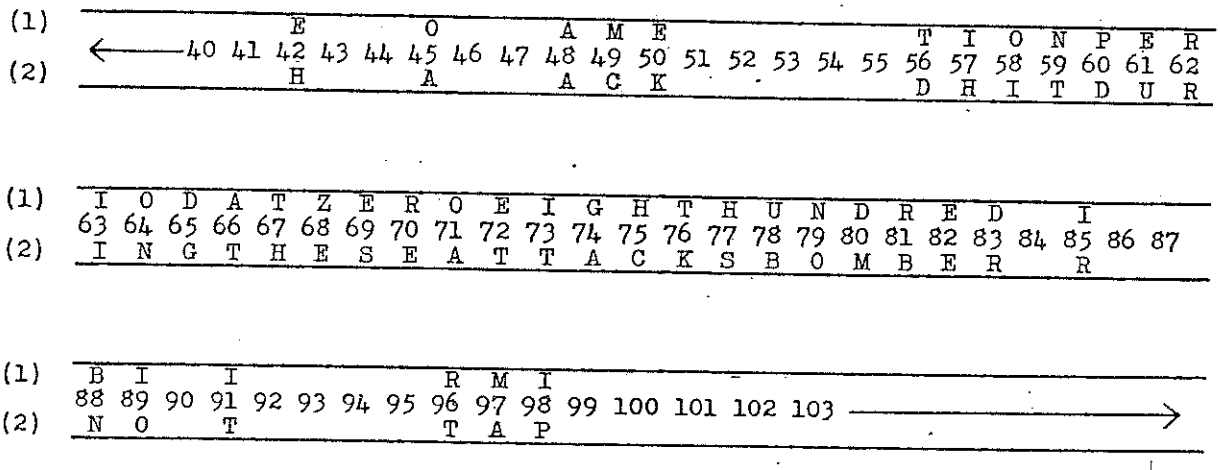
Figure 12 Sliding Cipher Strips



: = Strip setting pairs.

O = Assumed values.

Figure 13 Plain Text Sequence

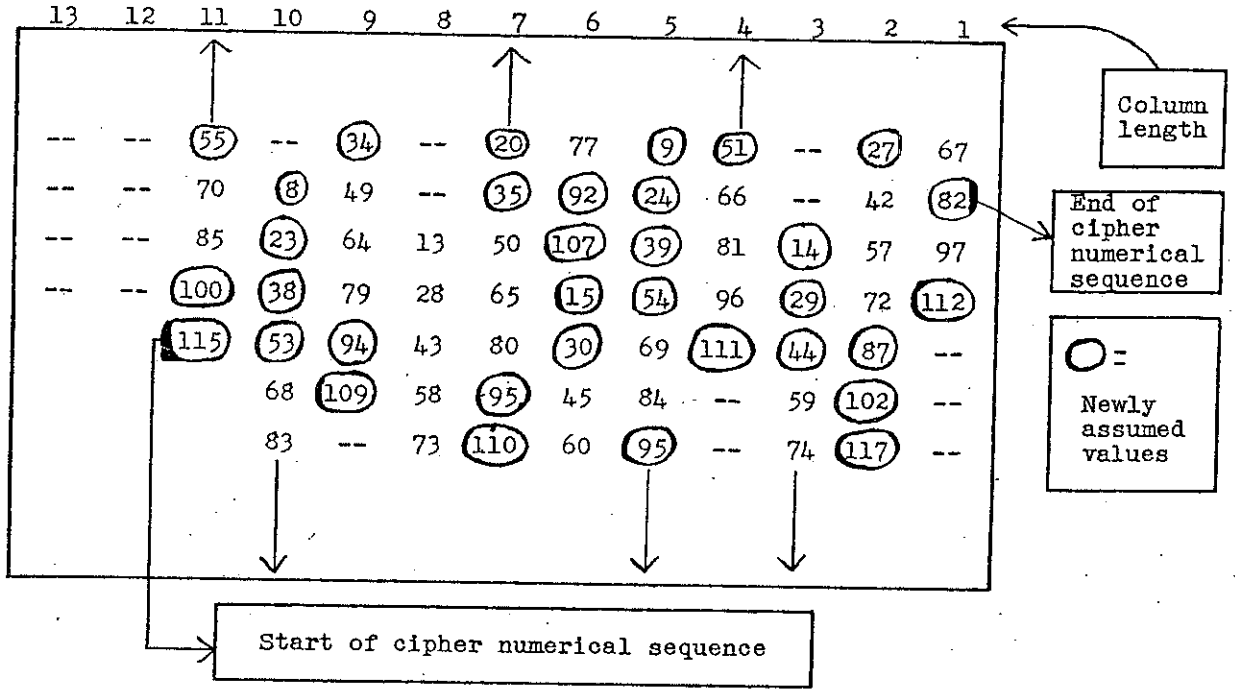


KEY RECONSTRUCTION

22. After the first few values have thus been recovered, it is time-saving and helpful in the further solution of the problem to begin construction of the second transposition block. The beginnings and ends of the cipher sequences are the most convenient places at which to start, since at these points the sequences each have one established terminus.

23. A sequence is chosen of a length which approximates a likely column length for transposition block No. 2. Assume, for example, the length 13, which would indicate a key length of 9 for block No. 2. Using the sliding strips as before, look for a matching sequence on the basis of the additive or subtractive 15. As each sequence is placed into position, new values are assumed on the plus 15 basis to fill the blank spaces. The partial result is as follows (Figure 14):

Figure 14



24. The student will notice that when the sequence 115-53-94-43-80-30-69-111-44-87 is placed in position, the column length 13 does not hold true, since this sequence extends no further than 115. We continue on the basis of a column length of 11, which has held thus far. This length will result in an incompletely filled rectangle for the second block with the shorter columns of length 10 and the key length 11. It should be remembered that in building up the second transposition block in this manner, the block is on its side -- that is, the lines in Fig. 10 are actually the columns of the second block.

25. Quite often, by means of numerical relationships, the second key length may be discovered before reconstruction of the second transposition block is started. For example, in this problem when the sliding strips are set with (1) 61 over (2) 76, (1) 64 over (2) 79, (1) 68 over (2) 83, and (1) 63 over (2) 78, these four number pairs are separated from each other in the cipher text by

intervals of 11, 10, and 11 respectively. The mechanics of the second transposition block causes constant differences between the sliding strips to appear only when the characters are originally separated by equal vertical columnar intervals within the second block. Since the total text length is 117, a good guess at the length of the second block columns would be 11 with the shorter columns 10.

26. The new values assumed in this key reconstruction are entered on the sliding strips as before. It will now be possible to divide off the cipher sequence into the proper segments of 10 and 11. To complete the problem, it is necessary only to continue all three processes, sliding strips, recovery of plain text, and reconstruction of the second transposition block.

27. Reconstruction of the first transposition block proceeds by taking off the sequences from the completed second block and rearranging them in their proper order.

28. It is suggested that the student complete this problem as training in this method of solution.

GENERAL REMARKS

29. This same general method may be used when two or more sequences of plain text have been recovered. In such cases, a subtractive or additive constant will be discovered, but will not necessarily be the equivalent of the first key length, unless by chance suitable provisional numbers happen to have been assigned to the recovered plain text sequences.

30. In all cases, integral multiples of the first key length may serve to connect known numerical values and thus help provide a sufficient skeleton to start the reconstruction of the second transposition block.

31. When, however, the complete plain text of a message has been recovered by means of anagramming, it is possible to eliminate the strip sliding method and proceed directly with key recovery by arithmetical means. In such cases, each plain text character is given a numerical value indicating its position in the plain text sequence. These values are substituted for their corresponding values in the cipher text. That is, the original cipher text is numbered according to the final plain text sequence. A numerical constant is then added to a sizable portion of this numerical sequence, and when the correct constant equal to the key length of the first transposition block has been thus added, the resulting new sequence will be found duplicated elsewhere in the numerical sequence. Reconstruction of the second transposition block on the basis of this additive constant can then proceed as described in paragraphs 15 and 16. The strip sliding method is ordinarily quicker, however, since it may be started with only partial plain text recoveries.

32. This general method can also be applied to the solution of a single message where a probable word or word-sequence is available.

B L A N K