CLASSICAL CRYPTOGRAPHY COURSE
BY LANAKI

August 22, 1996

LECTURE 16

TRANSPOSITION

SUMMARY

Lecture 16 considers a whole range of Transposition (or displacement) ciphers. We develop our subject using the following references: [BAR2], [FRE4], [KULL], [OP20], [MAST], [COUR], [LEDG], [BOW1], [ELCY].

SIMPLE ROUTE TRANSPOSITIONS (TRAMPS)

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

In their simplest form, TRAMPS may take any of the following routes when employing rectangles or squares for transposing text of a message as illustrated below. The plain-text message is assumed to be merely the normal sequence from A to X, for ease in following the route.

Any geometrical form can be used, but it must be full block; if the letters of a message do not complete the assigned block, nulls (arbitrary letters) must be added.

a) Simple Horizontal:

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

b) Simple Vertical:

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

c) Alternate Horizontal:

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

d) Alternate Vertical:

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

e) Simple Diagonal:

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

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

f) Alternate Diagonal:

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

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

g) Spiral, Clockwise:

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

h) Spiral, Counterclockwise:

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

Example 1 - Let the message be (military text):

At fourteen hundred sighted submarine bearing two three five degrees true. (63)

Suppose we agree to use a completely filled square of eight rows by eight columns, then we must add 1 null to give us a multiple of eight (64). We agree that alternate diagonals will be used for inscription.

```
  1 2 3 4 5 6 7 8
1 A T R T R E M A
2 F U E D D B R O
3 O E N S U I W T
4 N U I S N T H E
5 H G D E G R D G
6 H E B N E E R R
7 T E I E V E T U
8 A R F I E S E N
```

Next the letters are taken off by simple vertical to form the cryptogram:

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

To decipher the cryptogram, the process is reversed. The total number of letters in the cipher text is used to reconstruct the rectangle. Then the cryptogram is inscribed by the agreed upon route and the plain text is taken off by the other agreed upon route.

OTHER GEOMETRICAL FIGURES

We are not limited to the square or rectangle. The routes indicated above work for other geometrical designs with minor modifications.

(a) Trapezoidal design:

```
A T F O U
R T E E N H
U N D R E D S
I G H T E D S U
B M A R I N E M P
```

(b) Triangular design:

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

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

BIURA TTNGM AHDEF OERTR IEENU HDDNE SSUMP

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

AEBCP EURTD MMNSB FSAID NOIRE UUGTH RHNTE E.

SOLUTION HINTS FOR TRAMPS

When but one cryptogram is available, the solution of a tramp is largely trial and error. There are some shortcuts. Use:

a) The beginning and end of the cryptogram will follow the most frequent initials (T A W O B I C S D H) and finals (E T S D N R Y O F L). Words may be assumed which contain these initial or final letters near the beginning or end of the cryptogram.

b) The interval between the letters of expected words, high frequency digraphs, QU and vowel.

c) Long groups of vowels or consonants show up when English is written horizontally and transcribed vertically; these may be assumed to be adjacent.

d) The presence of parts of words are found with certain routes such as spirals and helps to identify the route.

e) Use the total number of letters to suggest the geometric design and fill in the arbitrary figure with the ciphertext to give further clues

NUMERICAL KEYS

A numerical key can be derived from a literal key as we saw in substitution problems:

```
A M E R I C A N
1 6 4 8 5 3 2 7
```

or can be used as a guided for transposing letters like:

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

The letters are take off the above groups and transcribed into standard groups of five letters, all letters marked 1 being taken first, then all those marked 2, etc giving:

NIEOI ROPNO OPNTS ROT

MISCELLANEOUS TRANSPOSITION METHODS

Transposition ciphers come in several simple varieties.

The oldest form may be reversed writing. The reversing process may be applied to regular or irregular groups of plain text letters:

Let the plain text be: Bridge destroyed at eleven pm.

Words Reversed:

E G D I R B D E Y O R T S E D T A N E V E L E M P

Words Reversed and Regrouped into False Lengths:

E G D I R B D E Y O R T S E D T A N E V E L E M P

Text Reversed and Regrouped into Fives:

MPNEV ELETA DEYOR TSEDE GDIRB

Text Reversed and Regrouped into Fives With Nulls every Fifth Position:

TRIMM PNEVP ELETA ADEYR ORTSL EDEGU DIRBM

Columnar by Bigraph:

or

B S	B R
R T	I D
I R	G E
D O	D E
G Y	S T
E E	R O
D D	Y E
E	D

Cipher Text:

B S R T I R D O G Y E E D D E , or
B I G D S R Y D R D E E T O E

or let the new plain be "Prepare to get underway":

Digraphs Reversed :

Plain	PREPA	RETOG	ETUND	ERWAY
Cipher	RPPER	ATEGO	TENUE	DWRYA

RAIL FENCE CIPHER

Just as the name implies, the Rail Fence Cipher resembles an old rail fence found in many parts of New England today; with its zig-zag appearance.

Plain: Prepare to get underway.

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

Ciphertext is taken off horizontally:

PEAEO EUDRA RPRTG TNEWY

It may be composed of any number of rails (or letters in depth) which may be written up or down, coming from a point and then reversing the direction to the end of the message, either filling the final stroke or being short a letter or more.

Any message may be written in with the normal sequence up and down, or visa versa, or it may be written into the points first, and then into successive horizontal rows. It is then taken out by the alternate process.

Table 16-1 shows the total length of a Rail Fence cipher versus the various peaks plus extra letters from 2-10 rails. There is no technical way to solve this cipher, however Table 16-1 can help look at possibilities.

Example:

TAOET NMFOA TNEHM NHWKS POIDI SLFMU HSOBE ALEEW AUFHE ASNES P. (51)

Scanning Table 16-1, for 2 rails there are 26 peaks; 3 rails, 13 peaks plus two extra letters (..); 4 rails, 9 peaks plus two extra letters; 5 rails, 7 peaks plus two extra letters, and so forth. We use the digit which falls directly under the message length; if no digits are shown, take the digit to the left and add for the extra letters the dots.

For a 3-depth, set up a pattern:

```
1       5       9       13
  2   4   6   8   10  12  14
    3       7       11      15
```

The cipher text looks like this:

```
T       T       O
  A   E   N   F   A         ( improbable)
    O       M       T
```

We try to write in the cipher text at the points and follow through to the second row:

```
T       A       O
  H   M   N   H             ( good plain text)
    E       E
```

TABLE 16 - 1

Total Length of Cipher versus Various Peaks plus extra Letters of Rails from 2-10

	3	5	7	9	11	13	15	17	19	21	23	25	27	29
2	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3		2	..	3	..	4	..	5	..	6	..	7	..	8
4			2	..	..	3	..	..	4	..	..	5	..	..
5				2	..	..	..	3	..	..	..	4	..	..
6					2	..	..	..	..	3	..	..	..	..
7						2	..	..	..	..	..	3	..	..
8							2	..	..	..	..	..	..	3
9								2	..	..	..	..	..	..
10									2	..	..	..	..	..

	31	33	35	37	39	41	43	45	47	49	51	53	55
2	16	17	18	19	20	21	22	23	24	25	26	27	28
3	..	9	..	10	..	11	..	12	..	13	..	14	..
4	6	..	..	7	..	..	8	..	..	9	..	..	10
5	..	5	..	..	..	6	..	..	..	7	..	..	..
6	4	..	..	..	..	5	..	..	..	..	6	..	..
7	..	..	..	4	..	..	..	..	..	5	..	..	..
8	..	..	..	..	..	..	4	..	..	..	..	..	..
9	..	3	..	..	..	..	..	..	..	4	..	..	..
10	..	..	..	3	..	..	..	..	..	..	..	..	4

	57	59	61	63	65	67	69	71	73	75	77	79	81
2	29	30	31	32	33	34	35	36	37	38	39	40	41
3	15	..	16	..	17	..	18	..	19	..	20	..	21
4	..	..	11	..	..	12	..	..	13	..	..	14	..
5	8	..	..	..	9	..	..	..	10	..	..	..	11
6	..	..	7	..	..	..	..	8	..	..	..	..	9
7	..	..	6	..	..	..	..	..	7	..	..	..	..
8	5	..	..	..	..	..	..	6	..	..	..	..	..
9	..	..	..	..	5	..	..	..	..	..	..	..	6
10	..	..	..	..	..	..	..	..	5	..	..	..	..

```
   83  85  87  89  91  93  95  97  99  101  103  105
2  42  43  44  45  46  47  48  49  50  51   52   53
3  ..  22  ..  23  ..  24  ..  25  ..  26   ..   27
4  ..  15  ..  ..  16  ..  ..  17  ..  ..   18   ..
5  ..  ..  ..  12  ..  ..  ..  13  ..  ..   ..   14
6  ..  ..  ..  ..  10  ..  ..  ..  ..  11   ..   ..
7  ..   8  ..  ..  ..  ..  ..   9  ..  ..   ..   ..
8  ..   7  ..  ..  ..  ..  ..  ..   8  ..   ..   ..
9  ..  ..  ..  ..  ..  ..  ..   7  ..  ..   ..   ..
10 ..  ..  ..  ..   6  ..  ..  ..  ..  ..   ..   ..

   107  109  111  113  115  117  119
2  54   55   56   57   58   59   60
3  ..   28   ..   29   ..   30   ..
4  ..   19   ..   ..   20   ..   ..
5  ..   ..   ..   15   ..   ..   ..
6  ..   ..   12   ..   ..   ..   ..
7  ..   10   ..   ..   ..   ..   ..
8  ..   ..   ..    9   ..   ..   ..
9  ..   ..   ..    8   ..   ..   ..
10 ..    7   ..   ..   ..   ..   ..
```

REDEFENCE

The railfence cipher may be made more secure when a numerical key is used in addition to the initial transposition. For example:

```
        2  T     L     G     E
        4   H   R Y   D E   H W
        1    E A   B R   T T   O M
        3     E     I     S     R
```

Cipher: EABRT TOMTL GEEIS RHRYD EHW
Key = 2413

Solution is similar to railfence with the help of a tip.

FOUR WINDS CIPHER

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

Taken off clockwise from left to right:

Cryptogram:

RRGNW PEAEO EUDRA PTTEY

HEDGES

```
              R   O   E   P   E   W   R   U   Y

        P   T   D   E   G   R   A   T   A   E   N
```

(Base jumps over two letters) Link P to R to E.

Cryptogram:

ROEPE WRUYP TDEGR ATAEN

DIAMOND

Friedman in [FRE4] describes solution to an unusual diamond design that looks like this:

```
                        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
```

The numbers indicate the method of encipherment. The cipher is taken off vertically by column.

The foregoing examples would indicate that almost any figure can be used for this type of transposition, including stars, polygons and irregulars. It is merely necessary to agree on the figure and the starting points for inscription and transcription processes.

CIVIL WAR MESSAGES

David Kahn gives us an interesting look at Civil War Cryptography. If there was a reason why the North won, it had to be superior cryptography. Anson Stager first superintendent of the Western Union Telegraph Company, was charged by Major General B. McClellan with drawing up a military cipher along the lines that he had devised for Governor Dennison of Ohio. [KAHN]

Stager complied. Soon McClellan was relying on the cipher to protect his communications during his successful campaign in West Virginia. One of the first users was Allan Pinkerton, founder of the agency that bears his name and bodyguard to President Lincoln. The key was very short, it was dependable and was used by the Union forces throughout the Civil War. It was used extensively because the Civil War first employed the telegraph on a large scale. Communications from Washington could take 10 days to their troops depending on weather, health of the telegrapher operators and availability of lines (which sometimes took a circuitous route). During Sherman's march to the sea, the Union had to rely on Southern newspapers for accounts of his slash and burn campaign.

So effective was the Stager cipher that those same Southern newspapers advertised for help from anyone who recognized or could break the Yankee cipher.

Stager's cipher was a word transposition. Stager's telegraphic experience evidently led him to a system in which the ciphertext consisted - as in the new telegraph codes - of ordinary words, which are far less subject to dangerous garbles

than groups of incoherent letters. [There is a funny story how one of the Rebel commanders could not read the cipher message sent to him by one of his forward patrols - prior to Gettysburg no less - so he sent a messenger to the forward post to get a clarification of the cryptogram received. The messenger returned to find his commander under arrest. The message was a warning of a Union trap. The lines were effected by rain that particular day.]

The Stager cipher was appealing because of its simplicity: the plaintext was written out in lines and transcribed by columns, up some and down others in a specified order. His cipher was improved by adding nulls, mazed routes of diagonals and interrupted columns through larger rectangles and per Samuel H. Beckwith, Grants cipher operator, important terms were represented by codewords which were carefully chosen to minimize telegraph error. The cipher expanded from one listed on a single card to that by the end of the war, required 12 pages to list routes and 36 for the 1,608 codewords. This was Cipher 4, the last of a series of 12 that the North employed at various times.

A good example of the system is given by encipherment of the message by President Lincoln on 1 June 1863: For Colonel Ludlow. Richardson and Brown, correspondents of the Tribune , captured at Vicksburg, are detained in Richmond. Please ascertain why they are detained and get them off if you can. The President. Cipher No 9 was in use and provided for the following codeword substitutions: VENUS for colonel, WAYLAND for captured, ODOR for Vicksburg, NEPTUNE for Richmond, ADAM for President of U.S. and NELLY for 4:30 pm time of dispatch. The keyword of GUARD set the size of the rectangle and routes. Nulls were added to the end of each column. The encipherer chose to write out the message in seven lines of five words each with three nulls to complete the rectangle. The plaintext was:

```
For       VENUS           Ludlow   Richardson  and
Brown     correspondents  of       the         Tribune
WAYLAND   at              ODOR     are         detained
at        NEPTUNE         please   ascertain   why
they      are             detained and         get
them      off             if       you         can
ADAM      NELLY           THIS     FILLS       UP
```

Ciphertext: [up the first column,(kissing=null),down second,(turning=null),up fifth,(times=null),down fourth, (belly=null), up third column]

GUARD ADAM THEM THEY AT WAYLAND BROWN FOR KISSING VENUS
CORRESPONDENTS AT NEPTUNE ARE OFF NELLY TURNING UP CAN
GET WHY DETAINED TRIBUNE AND TIMES RICHARDSON THE ARE
ASCERTAIN AND YOU FILLS BELLY THIS IF DETAINED PLEASE
ODOR OF LUDLOW COMMISSIONER.

Confederate cryptography centered around the Vigenere which we have previously studied. The south employed only three keywords: MANCHESTER BLUFF, COMPLETE VICTORY and COME RETRIBUTION. Known also as the Vicksburg cipher the team of Tinker, Chandler and Bates, very early yuppies, were able to read a whopping 90% of the Confederates messages and report them to Lincoln. For example, Grant's troops intercepted a message on eight captured rebels at Vicksburg trying to slip into Vicksburg with 200,000 percussion caps.

The ciphertext message read:

Jackson, May 25, 1863
Lieutenant General Pemberton: My XAFV. USLX WAS VVUFLSJP
by the BRCYAJ. 200000 VEGT. SUAJ. NERP. ZIFM. It will be
GFOECSZOD as they NTYMNX. Bragg MJTPHINZG a QRCMKBSE.
When it DDZGJX. I will YOIG. AS. QHY. NITWM do you YTIAM
the IIKM. VFVEY. How and where is the JSQMLGUGSFTVE.
HBFY is your ROEEL.
J. E. Johnston.

Note the flow of the message and hints along the way. The word separators, the clear text leads you into the next word. The size of the words is known and might be guessed.

The Plaintext based on the Keywords MANCHESTER BLUFF is:

Lieutenant General Pemberton: My last note was captured by the picket. 200000 caps have been sent. It will be increased as they arrive. Bragg is sending a division. When it joins I will come to you. Which do you think the best route? How and where is the enemy encamped? What is your force?

J. E. Johnston.

CRYPTANALYSIS OF THE SINGULAR COLUMNAR TRANSPOSITION CIPHER

Colonel W. Barker has perhaps the best description for cracking the single columnar transposition problem. [BAR3] (a tad better than the master himself.)

Encipherment

Lets start with the plaintext message:

NEED SUPPLIES AT ONCE STOP REQUEST REPLY IMMEDIATELY.

with Literal key: SUMMER TIME

Step 1: Derive the numerical key from literal key.

```
 810 4 5 1 7 9 3 6 2
 S U M M E R T I M E
```

Step 2: Write the plain text beneath the numerical key:

```
 810 4 5 1 7 9 3 6 2
 S U M M E R T I M E
---------------------
| N E E D S U P P L I |
| E S A T O N C E S T |
| O P R E Q U E S T R |
| E P L Y I M M E D I |
| A T E L Y|----------|
 ----------
```

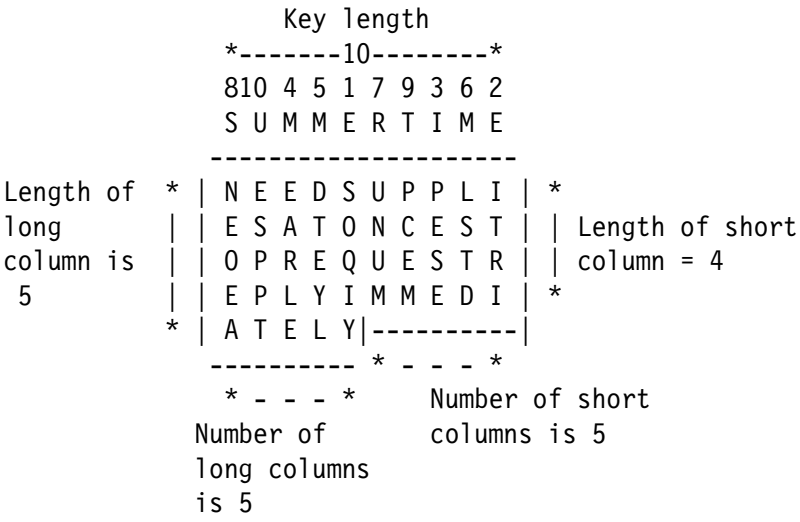
Note we are starting off with the more difficult incomplete rectangle. Technically this is called a matrix and is addressed by its rows and columns. There are two kinds of columnar matrices to be considered, the completely filled matrix and the in-completely filled matrix. The length of the message in a completely filled matrix is a multiple of the key- length which greatly simplifies the solution.

Terminology

The size or dimensions of any matrix depends on two things:

(1) The length of the key.
(2) The length of the message.

Given these two things, we can determine the type of matrix we are dealing with, the number of long and short columns, and the number of letters in each type of column. Graphically we have in our example:



Step 3: Take the columns out in numerical order. Thus the first column out is 1 or S O Q I Y, then I T R I etc.

The cipher text is:

SOQIY ITRIP ESEEA RLEDT EYLLS TDUNU MNEOE APCEM ESPPT

Note that the original plain text has not been changed but merely rearranged or transposed by a numerical key.

Decipherment

Consider the decipherment of the following:

UNCKO MNHTA NSEOT NMIEG OFPER NMAWO OLTGA SFHDO
OLLEN YINRI SIECY COTOR FETNN TSGOR IPTHT NOETX
ISENW ICXMI NREUE T. (96)

With Keyword: APPLE BLOSSOMS

Step 1: Derive the numerical key from the literal.

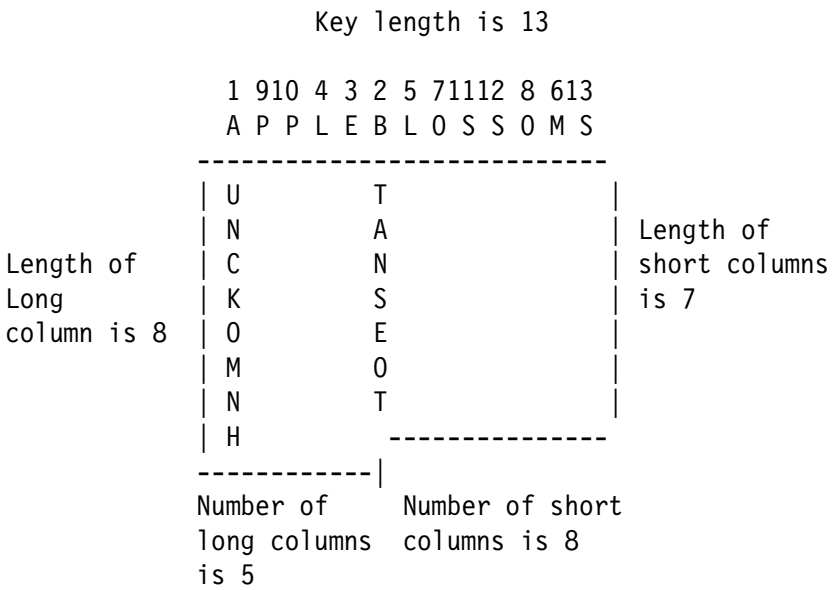
1 910 4 3 2 5 71112 8 613
A P P L E B L O S S O M S

Step 2: Determine the size of the matrix used in encipherment. This step is the most important step in decipherment.

Since the key is 13 and the message length is 96, we divide the key-length into the message length to give:

$$13\overline{)96}\ \ 7\ \text{R}\ 5$$

where 13 is length of key, 96 is length of the message, 7 is the length of the short columns, and 5 is the number of long columns. Since the length of the short column is 7, the length of the long column is 1 more or 8. And, the number long columns is 5, so the number of short columns is the key-length minus the number of long columns (13-5) = 8. Now we have the size of the matrix.



Step 3. Place the columns back into the matrix according to the numerical key. The plain text can now be read horizontally from left to right, top to bottom within the matrix.

```
  1 910 4 3 2 5 71112 8 613
  A P P L E B L O S S O M S
-----------------------------
| U R G E N T L Y N E E D I |
| N F O R M A T I O N C O N |
| C E R N I N G N E W Y O R |
| K T I M E S A R T I C L E |
| O N P A G E S I X C O L U |
| M N T W O O S I X T E E N |
| N T H O F T H I S M O N T |
| H S T O P ----------------
------------|
```

Cipher Text reads:

URGENTLY NEED INFORMATION CONCERNING NEW YORK TIMES
ARTICLE ON PAGE SIX COLUMN TWO OF SIXTEENTH OF THIS
MONTH STOP.

Comparing the steps:

Step	Encipherment	Decipherment
1	Derive numerical key	Derive numerical key
2	Write plain text beneath key	Determine size of matrix from key-length and message length.
3	Take columns out of matrix in numerical order	Put columns into matrix in numerical order

As an introduction to cryptanalysis, we start with special cases and work up to the general solution.

Case 1: Plain Text beginning of a Message Longer than the Key-Length

Given the cipher text message known to be a single columnar transposition:

TTDTI TIIIH NNOBT ERNOO IGSRY SVIAA XNAFN ASMMR IE.

We suspect that the words TRANSMIT INFORMATION is at the beginning of this message.

We begin our solution by writing the ciphertext without group divisions. We then make a biliteral frequency distribution. (The bigram frequency distribution will be 1 less than the total frequency because the last letter does not have a partner.)

```
T T D T I T I I I H N N O B T E R N O O I G S R Y
S V I A A X N A F N A S M M R I E.
```

and,

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

Write out the first few letters of known plain-text beginning horizontally and then horizontally written letters are written the succeeding letters of the given plain text as follows:

```
T R A N S M    HITS
----------
R A N S M I     1
A N S M I T     2
N S M I T I     0
S M I T I N     0
M I T I N F     1
I T I N F O     2
T I N F O R     3
I N F O R M     6
N F O R M A     1
F O R M A T     0
O R M A T I     1
R M A T I O     1
M A T I O N     0
```

We use the biliteral distribution to determine the key length as follows. We start in column 'T' and note that T occurs 5 times in the cipher message with 4 different letters (T, D, I, and E). We specify as a hit (or circle, or mark in someway) any of those letters in the first column. Column 1 has 3 hits - I T I. in column 2 we mark the three letters N, Y, and I as noted from the biliteral frequency distribution. We note the above figure shows the final results. The word inform has 6 hits and is below the word segment TRANSM. For this to have happened the key-length has to be eight (count down the rows) and the beginning within the matrix will look as follows:

```
T R A N S M I T
----------
I N F O R M A T
----------
I O N
```

We now see why the cipher text letter T is followed by I. They are both from the first column to the left in the matrix. Since the ending is I O N falls in the third horizontal row of the matrix; the first column is T I I and that is found in group two of the cipher text.

Since the key is 8, and the number of letters in the message is 42, we can easily determine the size of the matrix used in encipherment. Dividing 8 into 42 gives 40 with 5 as the length of the short, 6 the length of the long and 2 (remainder) being the number of long columns and (8-2) = 6 short columns after them.

We set up the enciphering matrix and write in the known plaintext.

```
  2 4
 -----------------
| T R A N S M I T |
| I N F O R M A T |
| I O N           |
| I O             |
| H I             |
| N G ------------
-----|

      2             4
TTDTI  TIIIH  NNOBT  ERNOO  IGSRY  SVIAA  XNAFN  ASMMR  IE.
```

The TII is a giveaway that this column was the second column (length 6) to be taken out of the matrix during encipherment. The entire column is T I I I H N. We note that R N O O I G is the 4th column (long) with all others being short. The rest of the columns are easily identified and the plain is read horizontally.

```
  2 4 7 3 5 8 6 1
 -----------------
| T R A N S M I T |
| I N F O R M A T |
| I O N B Y R A D |
| I O A T S I X T |
| H I S E V E N I |
| N G ------------
-----|
```

Plain reads:

TRANSMIT INFORMATION BY RADIO AT SIX THIS EVENING.

Note that our solution has yielded the numerical key (which may have been derived as a result of many literal keys). The numerical key is used to read other messages by the same source, collectively called traffic. The trivial issue is that the solution was possible because the known plain was longer than the keyword and hence, set up adjacent vertical letters to identify in the cipher text.

The Analytic Matrix or Hat Diagram

The Analytic matrix (aka Hat Diagram) is a fundamental tool to solve all columnar transposition cipher systems. You only need the keylength and the cipher text itself.

Given the cryptogram:

EIPEI EUFSS ETODE ERTJR OOSCL NTPLH EDGRF TEEEE
SAOIT SNULP VONPT ADAEL YVLT. (64)

with Key length = 10.

Step 1: Determine the size of the enciphering matrix.

Key of 10 into 64 = 6 as the length of the short, 7 as the length of the long columns, 4 as the number of long columns and 10 - 4 = 6 short columns.

or in shorthand 64 = 4 - 7's
6 - 6's

Check: 4 x 7 =28 + 6 x 6 = 36 = 64

Step 2: Divide ciphertext into long and short columns starting with long columns at the head of the message and the short columns at the tail of the message.

EIPEI EU / FSS ETOD / E ERTJR O / OSCL NTP / L
H EDGR / F TEEEE / SAOIT S / NULP VO / NPT ADA / EL
YVLT. (64)

Step 3: Write down vertically from left to right these divided columns, keeping the bottoms of the columns on the same line. Thus:

```
1 2 3 4 5 6 7 8 9 10
E F E O
I S E S L F S N N E
P S R C H T A U P L
E E T L E E O L T Y
I T J N D E I P A V
E O R T G E T V D L
U D O P R E S O A T
*-4-- * * ----6---*
long        short
```

These letters represent the foundation of the hat diagram.

Step 4: Extend the tops of the columns from right to left such that the long columns come at the tail of the message and the short columns at the head of the message.

We begin by drawing a line across the top of the of the present columns:

```
_______
E F E O|_________A
I S E S L F S N N E
P S R C H T A U P L
E E T L E E O L T Y
I T J N D E I P A V
E O R T G E T V D_L
U D O P R E S O A T
```

We start with the short columns on the right, we extend this column and make it long by adding one letter from the column previous to it. We move to the left and make that column long by adding 2 letters from the adjacent column and place on top of the line. We mark the bottom of the letters for the 'borrowed letters' to help us determine the length of the column extended over the top border.

```
_______           V
E F E O|________O_A
I S E S L F S N N E
P S R C H T A U P L
E E T L E E O L T Y
I T J N D E I P_A V
E O R T G E T V D_L
U D O P R E S O A T
```

We extend two more short columns making a total of four extended to long columns.

```
          E
          E I
_______   E T V
E F E O|___E_S_O_A
I S E S L F S N N E
P S R C H T_A U P L
E E T L E E O_L T Y
I T J N D E I P_A V
E O R T G E T V D_L
U D O P R E S O A T
```

At this point, still going from right to left, we extend the balance of the columns as short columns (six in all). Above the line is extend only to the length of the short column.

```
          E E
          D E I
_______   G E T V
E F E O|__R_E_S_O_A
I S E S L F S N N E
P S R C H_T_A U P L
E E T L E E O_L T Y
I T J N D E I P_A V
E O R T G E T V D_L
U D O P R E S O A T
```

The final hat diagram looks like this:

```
1 2 3 4 5 6 7 8 9 10
      J L E E
    O R N D E I
__U_D_O T G E T V
E F E O|P_R_E_S_O_A
I S E S L F S N N E
P S R C_H_T_A U P L
E E T_L E E O_L T Y
I T_J N D E I P_A V
E_O R T G E T V D_L
U D O P R E S O A T
```

Note the lengths of the columns -above the drawn lines at the bottoms of the columns - are from right to left the four long columns and the six short columns.

What does the hat matrix represent?

It represents the columns of the enciphering matrix in numerical order from left to right. Because we do not at this stage know which columns are actually long and short, the hat matrix contains some superfluous letters from the adjacent column. However, regardless of how long and short columns are arranged in the actual enciphering matrix, the columns of the hat matrix will contain all the letters of the columns as found in the actual enciphering matrix.

Case 2: Plain Text Longer than the Key-Length Anywhere in the Message.

Given Cipher Text:

BIEEH VHBSR UAHEE OREBE ECOWV NTETM TAQZT TDRNI
EESNE ELOLO EOERL NINNF R. (61)

Key length unknown.

Step 1: Make a biliteral frequency distribution (from left to right.) [ie. B has 3 contacts I, S, E in that order]

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

Step 2: "Complete the Plain" text for first few letters of known plaintext and apply biliteral frequency distribution. In the columns thus extended, note the 'hits' which follow the top column letter in the biliteral frequency distribution.

```
          Q U E E N     HITS
          ---------
1         U E E N E      2
2         E E N E L      1
3         E N E L I      3
4         N E L I Z      1
5         E L I Z A      0
6         L I Z A B      0
7         I Z A B E      2
8         Z A B E T      5   KEY LENGTH =8
9         A B E T H      2
```

For Z A B E T to have fallen directly under queen, the key-length must be 8, so:

```
          Q U E E N E L I
          Z A B E T H
```

Step 2: Determine size of matrix, columns and construct the hat diagram.

Key of 8 into 61 message length gives 7 as the short length, 8 as the long length, 5 for the number of long columns, and (8-5) 3 short columns. The Hat diagram looks like this:

```
          1 2 3 4 5 6 7 8
                C M
              E O T R
            B O W A N E
        * B S R V Q I L R
          I R E N Z E O L *
long    | E U B T T E L N |
column  8 E A E E T S O I 7  short
= 8     | H H E T D N E N |  column = 7
          V E C M R E O N
          H E O T N E E F
        * B O W A I L R R *
          *---5---* *-3-*
           long     short
```

Step 3: Juxtapose the known plain text with the hat diagram information and rearrange the columns.

```
Start with the Q  found in the 5th column of hat.  The U
               Z                                       A
```

is relatively easy to find in column 2.

```
5 2
M B
T S
A R
Q U E E N E L I
Z A B E T H
T H
T E
D E
R O
N
I
```

In a similar manner the remaining columns are easily identified and added to the juxtaposition:

```
5 2 3 6 4 1 7 8
        C
M B E R O B E R
T S O N W I L L
A R R I V E O N
Q U E E N E L I
Z A B E T H O N
T H E S E V E N
T E E N T H O F
D E C E M B E R
R O O E T   R
N   W L A
I
```

Inspection tells us that the 61 letters lie within the juxtaposition as follows:

```
5 2 3 6 4 1 7 8
        C
M B E*R O B E R
T S O N W I L L
A R R I V E O N
Q U E E N E L I
Z A B E T H O N
T H E S E V E N
T E E N T H O F
D E C E M B E R*
R O O E T   R
N   W L A
I
```

We eliminate the superfluous letters, and shift column 6 to the beginning of the message. The result is the original enciphering matrix and numerical key:

```
5 2 3 6 4 1 7 8

_______________
R O B E R T S O
N W I L L A R R
I V E O N Q U E
E N E L I Z A B
E T H O N T H E
S E V E N T E E
N T H O F_D_E_C
E_M_B_E_R
```

The plain text message is:

ROBERTSON WILL ARRIVE ON QUEEN ELIZABETH ON THE SEVENTEENTH OF DECEMBER.

Proper juxtaposition of columns of the analytic matrix depends not only upon the known plain text portion of the enciphering matrix, but also upon plain text appearing on the horizontal rows. This solution is a little more general as it does not depend on the location of the known plain text.

COMPLETELY COLUMNAR TRANSPOSITION - SOLUTION GIVEN KEY-LENGTH AND A COMPLETELY FILLED MATRIX

The completely filled columnar matrix is a simpler problem because we are dealing with only one column length. There is no problem of determining the long and short columns.

Column Matching:

Given the cipher text:

GLLEF PLUOT HERPI RDEBC NLGEE NNBAR SETHO TEYWP
EHIAO LIRMC SERTS VIIEH EALPO OEAFW TX. (72)

KEY LENGTH = 6

Step 1: Determine size of rectangle.

72 = 6 KEY LENGTH X 12 ROWS

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

This is the hat diagram with just one column length. Solution depends now on merely rearrangement of these six columns into numerical order. There are two ways to do this: 1) Anagraming and 2) column matching.

Anagraming

The cryptanalyst may anagram expected combinations of letters. Finding a Q, we look for a U and a vowel next to it. These could be in the same row. We then juxtaposition the columns or match them for QU_ or combinations like THE or THAT, CK, ING, ION and so forth.

Matching columns based on Validity Weighting

We select a single column at random from the analytic matrix above:

1
G
L
L
E
F
P
L
U
O
T
H
E

Unless by chance that our choice (1/6 chance) is the right hand column, one of the remaining columns will stand to the left of our chosen column. There are 5 juxtapositions:

	VW		VW		VW		VW		VW
12		13		14		15		16	
GR	2	GE	2	GE	2	GM	0	GE	2
LP	0	LN	0	LY	3	LC	0	LA	2
LI	2	LN	0	LW	0	LS	1	LL	2
ER	2	EB	0	EP	1	EE	0	EP	1
FD	0	FA	1	FE	1	FR	1	FO	2
PE	2	PR	2	PH	1	PT	1	PO	2
LB	0	LS	1	LI	2	LS	1	LE	3
UC	1	UE	1	UA	1	UV	0	UA	1
ON	3	OT	2	OO	1	OI	1	OF	3
TL	0	TH	4	TL	0	TI	3	TW	1
HG	0	HO	2	HI	2	HE	4	HT	1
EE	0	ET	0	ER	2	EH	0	EX	3
	---		---		---		---		---
	12		15		16		12		23

where: VW = validity weight for individual bigrams and total column validity weight.

To answer the question, which one of the 5 possibilities is the best fit, we can use Barker's "Letter Contact Weight Chart," Figure 16-2 to match and evaluate the column interactions. [BAR3]

To find the weight of a bigram in Figure 16-2, the first letter of the bigraph is found in the vertical column on the left side of the chart and the second letter is found in the horizontal row of letters along the top of the Figure. The intersection of these two letters is the weight of the bigraph in question. For example QU has a weight of 5, WH has a weight of three. The weights given in Figure 16-3 are of a general nature for English but are roughly dependent upon the expected frequency of occurrence of the bigraphs plus the concept of 'good' bigraphs like QU, LY, CK, TH, etc. Since each of the 5 columns has 12 bigrams to evaluate, we look at the sum of these individual weights as a column validity weight to determine the best column match. The highest column validity weight represents the best fit.

We can speed up the process by using the anagraming approach in addition to the column matching attack. We find the bigram LL in the 16 column combination. LL is usually proceeded by a vowel. Looking at the analytic matrix above at the same row as LL, only column 2 fits the bill. We then place column 2 in front of columns 1 and 6 and check the bigrams, trigrams for impossibilities.

```
2 1 6
R G E
P L A
I L L
R E P
D F O
E P O
B L E
C U A
N O F
L T W
G H T
E E X
```

The last jump to the final juxtaposition is not a big step:

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

The message reads:

EMERGENCY PLANS WILL BE PREPARED FOR THE POSSIBLE EVACUATION OF HILL TWO EIGHT THREE X

As a general rule, the longer the columns the more reliable the use of Figure 16-2 for matching columns. Generally speaking, a random bigram has a validity weight of 1. Thus a mismatched pair of columns of length 10 will have a total validity weight of 10. A validity bigram has a weight of 1.5. So the same example of 10 bigrams will have on average a validity weight of 15.

FIGURE 16-2
LETTER CONTACT WEIGHT CHART

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

IDENTIFICATION OF THE COMPLETELY FILLED MATRIX

There is a valuable test for determining if a complete filled columnar matrix is in play. Table 16-1 is an extensive table of Key Lengths and Column-Lengths of Completely Filled Matrices - Given their Message Length. Table 16-1 covers message lengths from 15 to 300 letters. The key lengths considered are from 3 to 25. In reading the expressions to the right of the various message lengths, the first number is the key length and the second number is the column length. So for 22 X 9 following message length 198, the key length is 22 and the column length is 9. Many message lengths may be the result of several sizes of the completely filled matrices. These various sizes are listed within the limits of the Table 16-1. We use this table to determine whether or not a particular message might have been enciphered with a completely filled matrix. Table 16-1 shows that about 30% of all lengths cannot have resulted from completely filled matrices.

Let's examine the following message:

URIRT PEGRV ATEPI AFZSS ITLFU MAHKI ECOLT CWVAW PEYLO RAESL ERETO M. (56)

Key-Length = unknown

>From Table 16-1, we find at 56 message length four possibilities for a completely filled matrix exist. The key lengths 4, 7, 8 and 14.

We test each of these possibilities without actually reading the message and obtain reliability or validity of each of the particular key-lengths. Normal plain-text contains approximately 40% letters as vowels and that these vowels are evenly

distributed throughout the text. We use the number of vowels in message X 100./number of letters in the message = % of vowels in message. We compute the per row number of vowels, mean difference from normal, expected mean and validity value for the matrix under consideration.

```
                    Number of      Mean
    (7 x 8)         Vowels         Difference
1 2 3 4 5 6 7
U R F U O P S         3             0.2
R V Z M L E L         1             1.8
I A S A T Y E         5             2.2
R T S H C L R         0             2.8
T E I K W O E         4             1.2
P P T I V R T         1             1.8
E I L E A A O         6             3.2
G A F C W E M         2             0.8
                     ---           ----
                     22             14.0 / 8 = 1.80

Expected Mean =22/8 =2.8
```

```
                              Number of   Mean
       (14 X 4)                Vowels     Difference
1 2 3 4 5 6 7 8 9 1011121314
U T R E F I U K O W P O S E      7        1.5
R P V P Z T M I L V E R L T      2        3.5
I E A I S L A E T A Y A E O     11        5.5
R G T A S F H C C W L E R M      2        3.5
                                ---      ----

                                 22       14.0
  Expected Mean = 22/4 = 5.5
  Validity Value= 14/4 = 3.50
```

Four rows, and if this is a valid analytic matrix there should be 24/4 = 5.5 vowels on each row. This is the expected mean for the each row. We tabulate the individual row mean differences and sum them for the matrix. The total of the mean differences is proportional to the number of rows, by dividing this total by the number of rows we obtain the Validity value for this matrix. Table 16-2 shows the interpretation of the validity values. It shows that less than or equal to 0.75 (or closer to it in the indefinite range) the more likely we are dealing with a completely filled matrix with correct ley length. Above 1.10 the more likely it is that the matrix is incorrect.

```
                      Number of    Mean
   (8 X 7)            Vowels       Difference
1 2 3 4 5 6 7 8
U G I T K C Y L         3           .1
R R A L I W L E         3           .1
I V F F E V O R         3           .1
R A Z U C A R E         4           .9
T T S M O W A T         2          1.1
P E S A L P E O         4           .9
E P I H T E S M         3           .1
                       ---         ---
                       22          3.3

Expected Mean = 22/7 =3.1          3.3/7 = 0.47
                                        Validity Value
```

The rows are too short (6 or less) for individual analysis, so we combined them for analysis.

(4 X 14) 1 2 3 4	Number of Vowels	Mean Difference
U I K Y R A I L	5	1.9
I F E O R Z C R	3	.1
T S O A P S L E	3	.1
E I T S G T C L	2	1.1
R L W E V F V R	1	2.1
A U A E T M W T	4	.9
E A P O P H E M	4	.9
	22	7.1

Expected mean = 22/7 combined rows = 3.1
Validity value = 7.1 / 7 = 1.01 (indefinite)

The results indicate that key length = 8 is the correct length.

Key Length	Validity Value of Matrix
14	3.5
8	0.47
7	1.80
4	1.01

Solution proceeds by anagraming and juxtaposition. The CK indicates a possible in the first row. Try the word LUCKY and see how that fits.

```
   (8 X 7)
*       * * * *
1 2 3 4 5 6 7 8
U G I T K C Y L
R R A L I W L E
I V F F E V O R
R A Z U C A R E
T T S M O W A T
P E S A L P E O
E P I H T E S M
```

becomes:

```
* * * * *
8 1 6 5 7 4 3 2
L U C K Y T I G
E R W I L L A R
R I V E O F F V
E R A C R U Z A
T T W O A M S T
O P P L E A S E
M E E T S H I P
```

Key = 81657432

Plaintext: LUCKY TIGER WILL ARRIVE OFF VERA CRUZ AT TWO AM STOP PLEASE MEET SHIP.

TABLE 16-2
VALIDITY VALUES

```
<-------------> 0.75 <----------> 1.10 <------------>

   Valid              Indefinite         Incorrect
   Matrix                                 Matrix
```

TABLE 16-1
Table of Key Lengths and Column Lengths of Completely Filled Matrices - Given The Message Length

15 3 X 5, 5 X 3
16 4 X 4, 8 X 2
17
18 3 X 6, 6 X 3, 9 X 2
19
20 4 X 5, 5 X 4 10 X 2
21 3 X 7, 7 X 3
22 11 X 2
23
24 3 X 8, 4 X 6, 6 X 4, 8 X 3, 12 X 2

25 5 X 5
26 13 X 2
27 3 X 9, 9 X 3
28 4 X 7, 7 X 4, 14 X 2
29
30 3 X 10, 5 X 6, 6 X 5, 10 X 3, 15 X 2
31
32 4 X 8, 8 X 4, 16 X 2
33 3 X 11, 11 X 3
34 17 X 2
35 5 X 7, 7 X 5
36 3 X 12, 4 X 9, 6 X 6, 9 X 4, 12 X 3, 18 X 2
37
38 19 X 2
39 3 X 13, 13 X 3
40 4 X 10, 5 X 8, 8 X 5, 10 X 4, 20 X 2
41
42 3 X 14, 6 X 7, 7 X 6, 14 X 3, 21 X 2
43
44 4 X 11, 11 X 4, 22 X 2
45 3 X 15, 5 X 9, 9 X 5, 15 X 3
46 23 X 2
47
48 3 X 16, 4 X 12, 6 X 8, 8 X 6, 12 X 4, 16 X 3, 24 X 2
49 7 X 7
50 5 X 10, 10 X 5, 25 X 2
51 3 X 17, 17 X 3
52 4 X 13, 13 X 4
53
54 3 X 18, 6 X 9, 9 X 6, 18 X 3
55 5 X 11, 11 X 5
56 4 X 14, 7 X 8, 8 X 7, 14 X 4
57 3 X 19, 19 X 3
58
59
60 3 X 20, 4 X 15, 5 X 12,, 6 X 10, 10 X 6,12 X 5, 15 X 4, 20 X 3
61
62
63 3 X 21, 7 X 9, 9 X 7, 21 X 3
64 4 X 16, 8 X 8, 16 X 4
65 5 X 13, 13 X 5
66 3 X 22, 6 X 11, 11 X 6, 22 X 3
67
68 4 X 17, 17 X 4
69 3 X 23, 23 X 3
70 5 X 14, 7 X 10, 10 X 7, 14 X 5
71
72 3 X 24, 4 X 18, 6 X 12, 8 X 9, 9 X 8,12 X 6, 18 X 4, 24 X 3
73
74
75 3 X 25, 5 X 15, 15 X 5, 25 X 3
76 4 X 19, 19 X 4
77 7 X 11, 11 X 7
78 3 X 26, 6 X 13, 13 X 6
79
80 4 X 20, 5 X 16, 8 X 10, 10 X 8, 16 X 5, 20 X 4
81 3 X 27, 9 X 9
82
83
84 3 X 28, 4 X 21, 6 X 14, 7 X 12, 12 X 7, 14 X 6, 21 X 4
85 5 X 17, 17 X 5

86
87 3 X 29
88 4 X 22, 8 X 11, 11 X 8, 22 X 4
89
90 3 X 30, 5 X 18, 6 X 15, 9 X 10, 10 X 9, 15 X 6, 18 X 5
91 7 X 13, 13 X 7
92 4 X 23, 23 X 4
93 3 X 31
94
95 5 X 19, 19 X 5
96 3 X 32, 4 X 24, 6 X 16, 8 X 12, 12 X 8, 16 X 6, 24 X 4
97
98 7 X 14, 14 X 7
99 3 X 33, 9 X 11, 11 X 9
100 4 X 25, 5 X 20, 10 X 10, 20 X 5, 25 X 4
101
102 3 X 34, 6 X 17, 17 X 6
103
104 4 X 26, 8 X 13, 13 X 8
105 3 X 35, 5 X 21, 7 X 15, 15 X 7, 21 X 5
106
107
108 3 X 36, 4 X 27, 6 X 18, 9 X 12, 12 X 9, 18 X 6
109
110 5 X 22, 10 X 11, 11 X 10, 22 X 5
111 3 X 37
112 4 X 28, 7 X 16, 8 X 14, 14 X 8, 16 X 7
113
114 3 X 38, 6 X 19, 19 X 6
115 5 X 23, 23 X 5
116 4 X 29
117 3 X 39, 9 X 13, 13 X 9
118
119 7 X 17, 17 X 7
120 3 X 40, 4 X 30, 5 X 24, 6 X 20, 8 X 15, 10 X 12, 15 X 8, 20 X 6 , 24 X 5
121 11 X 11
122
123 3 X 41
124 4 X 31
125 5 X 25, 25 X 5,
126 3 X 42, 6 X 21, 7 X 18, 9 X 14, 14 X 9, 18 X 7, 21 X 6
127
128 4 X 32, 8 X 16, 16 X 8
129 3 X 43
130 5 X 26, 10 X 13, 13 X 10
131
132 3 X 44, 4 X 33, 6 X 22, 11 X 12, 12 X 11, 22 X 6
133 7 X 19, 19 X 7
134
135 3 X 45, 5 X 27, 9 X 15, 15 X 9
136 4 X 34, 8 X 17, 17 X 8
137
138 3 X 46, 6 X 23, 23 X 6
139
140 4 X 35, 5 X 28, 7 X 20, 10 X 14, 14 X 10, 20 X 7
141 3 X 47
142
143 11 X 13, 13 X 11
144 3 X 48, 4 X 36, 6 X 24, 8 X 18, 9 X 16, 12 X 12, 16 X 9, 18 X 8, 24 X 6
145 5 X 29
146

147 3 X 49, 7 X 21, 21 X 7
148 4 X 37
149
150 3 X 50, 5 X 30, 6 X 25, 10 X 15, 15 X 10, 25 X 6
151
152 4 X 38, 8 X 19, 19 X 8
153 3 X 51, 9 X 17, 17 X 9
154 7 X 22, 11 X 14, 14 X 11, 22 X 7
155 5 X 31
156 3 X 52, 4 X 39, 6 X 26, 12 X 13, 13 X 12
157
158
159 3 X 53
160 4 X 40, 5 X 32, 8 X 20, 10 X 16, 16 X 10, 20 X 8
161 7 X 23, 23 X 7
162 3 X 54, 6 X 27, 9 X 18, 18 X 9
163
164 4 X 41
165 3 X 55, 5 X 33, 11 X 15, 15 X 11
166
167
168 3 X 56, 4 X 42, 6 X 28, 7 X 24, 8 X 21, 12 X 14, 14 X 12, 21 X 8, 24 X 7
169 13 X 13
170 5 X 34, 10 X 17, 17 X 10
171 3 X 57, 9 X 19, 19 X 9
172 4 X 43
173
174 3 X 58, 6 X 29
175 5 X 35, 7 X 25,25 X 7
176 4 X 44, 8 X 22, 11 X 16, 16 X 11, 22 X 8
177 3 X 59
178
179
180 3 X 60,4 X 45, 5 X 36, 6 X 30, 9 X 20, 10 X 18, 12 X 15, 15 X 12, 18 X 10, 20 X 9
181
182 7 X 26, 13 X 14, 14 X 13
183 3 X 61
184 4 X 46, 8 X 23, 23 X 8
185 5 X 37
186 3 X 62, 6 X 31
187 11 X 17, 17 X 11
188 4 X 47
189 3 X 63, 7 X 27, 9 X 21, 21 X 9
190 5 X 38, 10 X 19, 19 X 10
191
192 3 X 64, 4 X 48, 6 X 32, 8 X 24, 12 X 16, 16 X 12, 24 X 8
193
194
195 3 X 65, 5 X 39, 13 X 15, 15 X 13
196 4 X 49, 7 X 28, 14 X 14
197
198 3 X 66, 6 X 33, 9 X 22, 11 X 18, 18 X 11, 22 X 9
199
200 4 X 50, 5 X 40, 8 X 25, 10 X 20, 20 X 10, 25 X 8
201 3 X 67
202
203 7 X 29
204 3 X 68, 4 X 51, 6 X 34, 12 X 17, 17 X 12
205 5 X 41
206
207 3 X 69, 9 X 23, 23 X 9

208 4 X 52, 8 X 26, 13 X 16, 16 X 13
209 11 X 19, 19 X 11
210 3 X 70, 5 X 42, 6 X 35, 7 X 30, 10 X 21, 14 X 15, 15 X 14, 21 X 10
211
212 4 X 53
213 3 X 71
214
215 5 X 43
216 3 X 72, 4 X 54, 6 X 36, 8 X 27, 9 X 24, 12 X 18, 18 X 12, 24 X 9
217 7 X 31
218
219 3 X 73
220 4 X 55, 5 X 44, 10 X 22, 11 X 20, 20 X 11, 22 X 10
221 13 X 17, 17 X 13
222 3 X 74, 6 X 37
223
224 4 X 56, 7 X 32, 8 X 28, 14 X 16, 16 X 14
225 3 X 75, 5 X 45, 9 X 25, 15 X 15, 25 X 9
226
227
228 3 X 76, 4 X 57, 6 X 38, 12 X 19, 19 X 12
229
230 5 X 46, 10 X 23, 23 X 10
231 3 X 77, 7 X 33, 11 X 21, 21 X 11
232 4 X 58, 8 X 29
233
234 3 X 78, 6 X 39, 9 X 26, 13 X 18, 18 X 13
235 5 X 47
236 4 X 59
237 3 X 79
238 7 X 34, 14 X 17, 17 X 14
239
240 3 X 80, 4 X 60, 5 X 48, 6 X 40, 8 X 30, 10 X 24, 12 X 20, 15 X 16, 16 X 15, 20 X 12, 24 X 10
241
242 11 X 22, 22 X 11
243 3 X 81, 9 X 27
244 4 X 61
245 5 X 49, 7 X 35
246 3 X 82, 6 X 41
247 13 X 19, 19 X 13
248 4 X 62, 8 X 31
249 3 X 83
250 5 X 50, 10 X 25, 25 X 10
251
252 3 X 84, 4 X 63, 6 X 42, 7 X 36, 9 X 28, 12 X 21, 14 X 18, 18 X 14, 21 X 12
253 11 X 23, 23 X 11
254
255 3 X 85, 5 X 51, 15 X 17, 17 X 15
256 4 X 64, 8 X 32, 16 X 16
257
258 3 X 86, 6 X 43
259 7 X 37
260 4 X 65, 5 X 52, 10 X 26, 13 X 20, 20 X 13
261 3 X 87, 9 X 29
262
263
264 3 X 88, 4 X 66, 6 X 44, 8 X 33, 11 X 24, 12 X 22, 22 X 12, 24 X 11
265 5 X 53
266 7 X 38, 14 X 19, 19 X 14
267 3 X 89
268 4 X 67

269
270 3 X 90, 4 X 54, 6 X 45, 9 X 30, 10 X 27, 15 X 18, 18 X 15
271
272 4 X 68, 8 X 34, 16 X 17, 17 X 16
273 3 X 91, 7 X 39, 13 X 21, 21 X 13
274
275 5 X 55, 11 X 25, 25 X 11
276 3 X 92, 4 X 69, 6 X 46, 12 X 23, 23 X 12
277
278
279 3 X 93, 9 X 31
280 4 X 70, 5 X 56, 7 X 40, 8 X 35, 10 X 28, 14 X 20, 20 X 14
281
282 3 X 94, 6 X 47
283
284 4 X 71
285 3 X 95, 5 X 57, 15 X 19, 19 X 15
286 11 X 26, 13 X 22, 22 X 13
287 7 X 41
288 3 X 96, 4 X 72, 6 X 48, 8 X 36, 9 X 32, 12 X 24, 16 X 18, 18 X 16, 24 X 12
289 17 X 17
290 5 X 58, 10 X 29
291 3 X 97
292 4 X 73
293
294 3 X 98, 6 X 49, 7 X 42, 14 X 21, 21 X 14
295 5 X 59
296 4 X 74, 8 X 37
297 3 X 99, 9 X 33, 11 X 27
298
299 13 X 23, 23 X 13
300 3 X 100, 4 X 75, 5 X 60, 6 X 50, 10 X 30, 12 X 25, 15 X 20, 20 X 15, 25 X 12

SOLUTION GIVEN KEY LENGTH PLUS A PROBABLE WORD IN THE TEXT

Given the key-length, we are able to construct the hat diagram; and the analytically juxtapositioning of the matrix columns is facilitated greatly by a probable word.

Given:

RCRKA LPTNA TALMO IDFNV TRTIN FLEFR IONOI WOPIE
CGOAF RDCUH OIAIT ELLPR IRPSN EYRRC IHITI OTWUO
IDSPF SOIEK GMN. (93)

Probable word = NEW YORK Key length = 9

Perform a monoalphabetic frequency distribution.

```
NEW YORK
652 1992
```

The Y is a gimme. Draw up the hat diagram based on key length = 9.

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

>From column 7 with the Y and column 1 with the K:

```
        7     1
        I
        R
        P
        S     R
        N     C
        E     R
  N E W Y O R K
        R     A
        R     L
        C     P
        I     T
        H     N
        I     A
              T
```

We add column 3 with the N, followed by 5 with the R, 6 matches the E, 4 the W, and 8 brings out RICHMOND.

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

O     A T
R N
```

The message is read horizontally:

TRANSPORTATION FACILITIES FROM NEW YORK TO FLORIDA WILL
PRECLUDE PICKUP OF FREIGHT IN RICHMOND, VIRGINIA. STOP.

Barker presents two more special cases leading to the General solution but the basic concepts have been presented in this lecture. [BAR3]

DOUBLE COLUMNAR TRANSPOSITION CIPHER

Courville, Friedman and the Army Extension Course Text No 166 discuss double transposition in copious detail. Cryptanalysis of the double transposition is covered in detail. Essentially the encipherment is polyphase and the decryption hinges on sizing the matrices correctly - especially the first transposition matrix. [COUR], [FRE4], [ARMY]

AMSCO

The AMSCO Cipher is another type of incomplete columnar transposition. Its column-letters are not limed to a column of single letters, but rather alternating single, double, single, double throughout the plain text length. A numerical key is employed. For example:

```
3  1  4  2  5
TH E  WE A  RI
N  GO F  DE C
OR A  TI V  EM
E  DA L  SW A
SC O  MM O  NI
N  EN G  LA N
DD U  RI N  GT
H  ER E  IG N
OF H  EN R  YT
H  EE I  GH T
HX

2-1-2-1-2
1-2-1-2-1
2-1-2-1-2
1-2-1-2-1
2-1-2-1-2
1-2-1-2-1
2-1-2-1-2
1-2-1-2-1
2
    (A)
```

```
2  4  6  1  5  3
T  HE W  EA R  IN
GO F  DE C  OR A
T  IV E  M  ED AL
SW A  SC O  MM O
N  IN E  NG L  AN
DD U  RI N  GT H
E  RE I  GN O  FH
EN R  YT H  EE I
G  HT H

1-2-1-2-1-2
2-1-2-1-2-1
1-2-1-2-1-2
2-1-2-1-2-1
1-2-1-2-1-2
2-1-2-1-2-1
1-2-1-2-1-2
2-1-2-1-2-1
1-2-1

    (B)
```

In matrix (A) the alternating pattern of 2-1-2-1 follows from one end of one line to the next line; but in matrix (B) it is possible to have two 1's or two 2's in the continuation from one line to the next. This is a pecularity of this cipher. Solution is done similarly to the incomplete columnar. Use of a probable word is important for this cipher. Columns are extracted in numerical order.

Example: Tip = PRECIOUS

NTTIN OENOE NTUSD PRTTE RIUUN TOLIV EDSIS ORDEW
LLTIL STSII CRTOL NKOOU XHKIG NALHE ENEOL ESERY
GSPDL SRWIO ANSWI AAENS LEIFS RHPSA FIHRR (115)

Solution:

Divide tip into alternative patterns.

```
    -P RE C IO U S-       PR E CI O US;
```

The ciphertext hits RE = none, IO at 89; PR at 16, CI at 33, US at 13. Accept 2'nd pattern with three hits. Write in the ciphertext on both sides of the known pairs to the extent of 8 - 9 letters.

```
                UN     IN
                T      O
                OL     EN
                I      O
                VE     EN
                D      T
          PR  E CI  O  US
                S      D
                OR     PR
                D      T
                EW     TE
                L      R
                LT     IU
```

We lightly cross out the used letters as we go along. The existence of PR here, shows that the PR of PRECIOUS - appearing just once in the cipher can not be used here so our original assumption is wrong. Therefore the tip is found on two lines.

We test the O's using the alternate pattern 1-2-1-2-1, whenevr an O occurs and see what is plausible. O-54: O LN K OO U XH gives CIOUS SLN*; O-58: O OU X HK gives CIOUS SOUND OXPR*; O-59: O UX H KI gives CIOUS SUX*; O-90: O AN S WI A gives CIOUS SAND; ORSPR DWIT EWATE, which looks good so we write in the column. After EWATE, the rows go bad indicating the bottom of the block. Remember the first letter of the cipher of this type will be found somewhere in the top row of the plaintext. We extend our columns up to the first letter.

The final message is:

```
          O  RI  E  NT  A  LL
          UX U   RY  T  EN T
          H  UN  G  IN  S  IL
          KI T   SP O   L  ES
          G  OL  D  EN  I  TS
          NA I   LS O   FS I
          L  VE  R  EN  R  IC
          HE D   WI T   HP R
       PR E  CI  O  US  S  TO
          NE S   AN D   AF L
          O  OR  S  PR  I  NK
          LE D   WI T   HR O
          S  EW  A  TE  R  --
```

Note the PR was not a bigraph but broken up -P R in the line above.

MYSZKOWSKI

(Named after the famous flying Myszkowski family circus high-wire act) is another incomplete columnar transposition with an erratic method of taking out the ciphertext letters. Keywords with repeated letters are allowed and taken out in left to right order for the repeated letters. In ciphertext 2-, 3- and even 4- decimations are evidenced. A 3-decimation, 3 letters in the keyword are repeated would give rise to every third letter being at issue.

Solution is by period and probable word.

Keying examples:

```
F I C T I O N        P A P I L L A
2 3 1 6 3 5 4        4 1 4 2 3 3 1
A M O O S E I        A M O O S E I
S S O C A L L        S S O C A L L
E D A S T H E        E D A S T H E
W O R D I S S        W O R D I S S
A I D T O M E        A I D T O M E
A N C R O P P        A N C R O P P
E R O R T R I        E R O R T R I
M M E R F R O        M M E R F R O
M T H E A N I        M T H E A N I
M A L S H A B        M A L S H A B
I T O F F E E        I T O F F E E
D I N G O N T        D I N G O N T
R E E B R A N        R E E B R A N
C H E S - - -        C H E S - - -
     (A)                  (B)
```

Cipher (A)

OOARD COEHL ONEEA SEWAA EMMMI DRCMS SADTO IIONO
RTMFT AAHTF IOERH ILESE PIOIB ETNEL HSMPT RNAEN
AOCSD TRRRE SFGBS (95)

Cipher (B)

MISLD EOSIE NPRIM OTIAB TEITE NHOCO DTRRR ESFGB
SSEAL THISO MOPTR FRANH AFEON RAAOS OEAWR ADACE
OMEMH MLIOD NRECE (95)

Compare the keyword mixings for both ciphers and pick up the decimation intervals.

As a partial example of the process:

Given: Keyword = ERMEDICAL, PERIOD = 6

UEIES OCOSH IEIDF AIPLH MLCAU SSRTT OTMUE NRAAN
NROSA XSREF KPNEL OINEN OCMII FOAGZ NADEM CLPRO
SITOM RMCYS NIIAA AKEFT OSINL ATTSQ ESHON YLETD
RTNEF TUESE BEMGA AICRT PONHG OEPAA HOARD RRAFR
NET (163)

Block size is known and may be drawn up as 6 X 27, plus 1.

```
O R I
N T E
N T O
C O M
I T I            Trigraphs off these
F M A            possibilities:
O U G
Z E N               N T E (R)
A N D               (I)NTO
E R M E D I         C O M (M)
C A L               I T I (ION)
P A R               OUG (HT)
O N S               (A or I) - ZEN
I N T               PAR(T)
O R M
R O M
C S Y
```

The final key is: 3 5 4 1 3 2

Non repeated columns are removed exactly previously discussed. Repeated letter columns give rise to the 2- or 3- or 4- decimations, so look at adjacent letters for plain text.

CADENUS

The Cadenus is a double transposition type, employing a keyword, as in columnar transposition, to shift the order of the columns and in addition, to shift the starting point of each column using the same key. The second shift is accomplished by attaching a letter of the alphabet to each row during construction. V and W used together. The block must be complete and 25 letters long in each column.

Example:

```
EASY        AESY
2134        1234
ASEV   A    SYST
EREL   B    RETO
IMIT   C    MTAT
ATIO   D    TLUS
NONT   E    OATL
HEUS   F    EEES
EFUL   G    FIYH
NESS   H    EASD
OFTH   I    FNMS
ECAD   J    CHBH
ENUS   K    NEUV
ISTH   L    SNPM
ATEV   M    TOFA
ERYM   N    RENU
ESSA   O    SEIE
GEMU   P    EIEL
STBE   Q    TARL
AMUL   R    MENT
TIPL   S    IEET
EOFT   T    OGEV
WENT   U    ESIT
YFIV   VW   FAIS
ELET   X    LTNG
TERS   Y    EEUV
LONG   Z    OWUL
```

Cipher:

SYSTR ETOMT ATTLU SOATL etc

Solution procedure:

1. Count the number of letters, divide by 25 = number of columns.

2. Write the cipher into the block by horizontals.

3. Write the probable word and examine the cipher block for correct letters. Anagram.

4. When the entire block has been constructed, find the beginning of the plain text and rewrite the block.
   Place the alphabet at one edge of the block and note the keyword.

AUTO-TRANSPOSITION

The auto transposition cipher is a multiple transposition by groups with a keyword controlling the first cipher group. The letters of each group in turn are converted into a numerical sequence. In some cases, anagraming is an aid, but not always.

To encipher, select a keyword of any length and write in the plaintext under it. Skip a line and repeat the plaintext with the first group under the keyword. Then assign numbers to the keyword's letters in their order of the normal alphabet. Using this resulting numerical sequence apply it to the first group of the plaintext. Continue in this manner through each consecutive group.

key:

```
F R A G I L E*W H E N M E M*B E R S O F A*N O R G A N I
3 7 1 4 5 6 2*7 3 1 6 4 2 5*2 3 6 7 5 4 1*4 6 7 2 1 5 3
```

Plain:
```
W H E N M E M*B E R S O F A*N O R G A N I*Z A T I O N G
```

Cipher:
```
E M W N M E H*A R B F S E O*O R N I A G N*I N G A Z O T
1 5 7 6 4 2 3 1 6 2 4 7 3 5  ...
```

The complete cipher may be written in either groups of five or its true period length. A tip is essential. Placing the tip is an easy exercise and recovering the text after the tip is straightforward but not before it. Anagramming is essential to the solution.

Given: Period = 6, Tip = EIGHTEENEIGHTYSEVE(N)

RHEPTE SCDESE ROOFTO ACYDOS UMREPT WASASS TTTIAS
LIMCAA NICEIH NENEVT BTDOUA GEIHET EGEIHN TEYVSE
RSONUF IENCMO ILNPGI IHUENT TETASD ESECNT GUFSSE
(150)

The tip is found in groups 12, 13 and part of 14.

Cipher
```
     G E I H E T   E G E I H N   T E Y V S E
                   1 5 3 4 6 2   1 6 2 5 3 4
```
Plain
```
     E I G H T E   E N E I G H   T Y S E V E
     1 5 3 4 6 2   1 6 2 5 3 4   4 6 3 1 5 2
```

Cipher text is:

THE PREDESSOR OF TODAYS COMPUTERS WAS A MACHINE INVENTED ABOUT EIGHTEEN EIGHTY SEVEN FOR USE IN COMPILING THE UNITED STATES CENSUS.

Example of the mechanism is:

```
            7 3 1 6 4 2 5
            B E R S O F A    Plain
            1 2 3 4 5 6 7

      =     A R B F S E O    Cipher
```

GRILLE / TURNING GRILLE

Friedman, Masterton, Bowers, LEDGE, Elcy as well as OP-G-20 cover the Grille in detail. [FRE4], [OP20], [MAST], [LEDG], [BOW1], [ELCY].

The grille is an ingenious transposition which the 'stuff that spy used in the field' are made of. Cryptographic grilles are stencils cut with holes for the purpose of uncovering a small part of the paper that the plain text is written on. Generally, both correspondents have identical grilles and know the routes in and out of the grille to inscribe / transcribe the plain /cipher text.

There are eight positions that the grille can be turned, two sides and four 90 degree turns.

Lets illustrate with a 6 X 6 square and the message:

SORTIE WILL COMMENCE AT MIDNIGHT FOUR JUNE

Let open apertures be shown as O and closed be shown by X.

```
    GRILLE                1st Position
  1 2 3 4 5 6               1 2 3 4 5 6
1   O   O                 1   S   O
2 O                       2 R
3       O   O             3       T   I
4         O               4         E
5   O   O                 5   W   I
6           O             6           L

2nd Position              3rd Position
  1 2 3 4 5 6               1 2 3 4 5 6
1         L               1 A
2   C       O             2     T   M
3                         3   I
4   M   M   E             4 D   N
5     N                   5           I
6 C     E                 6     G   H

4th Position              Complete Inscription
  1 2 3 4 5 6               1 2 3 4 5 6
1     T     F             1 A S T O L F
2       O                 2 R C T O M O
3 U   R   J               3 U I R T J I
4                         4 D M N M E E
5 U       N               5 U W N I N I
6   E                     6 C E G E H L
```

Cipher may be taken out by any route.

ASTOL FRCTO MOUIR TJIDM NMEEU WNINI CEGEH L.

To decipher we reverse this process. We may anagram the letters to form another sequence of letters that are intelligible. We assign numbers to the cipher text to facilitate the process. We look for our invariable combinations like QU and CK. These form a good starting point. Grille positions are 180 degrees reciprocals. We can write the grille message out and then reverse the message under it to have reciprocal positions in the square line up vertically.

Problem:
ARUDU CSCIM WETTR NNGOO TMIEL MJENH FOIEI L

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21
A R U D U C S C I M  W  E  T  T  R  N  N  G  O  O  T
L I E I O F H N E J  M  L  E  I  M  T  O  O  G  N  N

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

Each anagram formed with letters on one of these lines corresponds with the reversal of the other plain text formed on the other line. The partial recovery of the plain by anagraming might proceed as follows. (only correct trials are shown)

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

The plain text will break after just nine letters, because the grille used was of that capacity. When one fourth of the total number of letters in the cipher text have been anagrammed without a break in the plain text on either line, the letters which were originally inscribed in reciprocal positions of the grille have been found.

The grille used in this problem may be reconstructed by numbering the cells of the square of 6 x 6 in the normal manner and then cutting out the cells numbered according to the series found 25-8-32-10-22-34-17-6-24.

SWAGMAN / LAZY SWAGMAN TRANSPOSITION

An Australian version of the Tramp, the Swagman uses a keying square composed of somewhat random arrangement of digits between 4 - 8 wide wherein the digits have no repeats within either row or column.

```
3 2 1 4 5
1 5 3 2 4
2 4 5 3 1
5 3 4 1 2
4 1 2 5 3
```

The plain text is written horizontally to form a rectangle commensurate with the width selected - here 5 X 5. If necessary, nulls are added to complete the last letters of the rectangle, which must be a multiple of the width of the square.

Suppose we have a short "message" and a corresponding 4-width box:

```
T H I S   I S A N   E X       2 3 1 4
A M P L   E O F T   H E       3 2 4 1    4 X 10
S W A G   M A N T   R A       4 1 3 2
N S P O   S I T I   O N       1 4 2 3
```

The first column of each box is rearranged according to the first column of the square - thus T is put to the 2nd row (as I and E of the other boxes will be) A is put on the third, S on the fourth, and N on the first. Then H(and S and X) get put on the third row, M on the second, W on the first, and S on the fourth - since the second column of our digital box is 3 2 4 1 . And so on to form the intermediate version:

```
N W I L   S A A T   O A
T M P G   I O T T   E E
A H A O   E S N I   H X
S S P S   M I F N   R N
```

The final cipher is taken off vertically:

NTASW MHSIP APLGO SSIEM AOSIA TNFTT INOEH RAEXN

Lets look at a problem:

POGTC VEEIO AIROR LLDLE NOWGP AIAAN FNGTA THATL
ICTPN HUEAX YGELA DIDAN EUNMB ILANT RRICM EAMIG
LAMPA RTASR POOOA LUPDO BROAS ESELA NSNQL ODUHC
EIAAS CGDSO ORREM BTOWI SOUS.

The crib is Caesar UXPFMP which is TWOELO.

```
POGTC  VEEIO  AIROR  LLDLE  NOWGP  AIAAN  FNGTA  THATL

               o      ee           ll      o
ICTPN  HUEAX  YGELA  DIDAN  EUNMB  ILANT  RRICM  EAMIG


LAMPA  RTASR  POOOA  LUPDO  BROAS  ESELA  NSNQL  ODUHC


EIAAS  CGDSO  ORREM  BTOWI  SOUS.
                     t w    o
```

Since there are only a couple of W's, we look for all the other letters of the crib in ORDER around that area, find them. We come up with a width which puts each letter in consecutive columns. The unique TW and final O narrow things down.

The break is at position 138, or one position removed. 138 is a factor of 6. We find as we put one letter in each several consecutive boxes , we prepare a worksheet of cipher text 6 deep.

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

One row of the key must be 2 1 5 4?? and the key row above it must be ????51.

The message is about an elphant. GARGANTUAN MAMMALIAN
HERBIFORE PACHYDERMATOUS QUADRUPED WITH PLANT I GRADE
LOCOMOTION, A FLEXIBLE PROBOSCIS, TWO LONGATED INCISORS,
ALSO OSCILLATING AURAL APPENDAGES.

```
3 5 1 6 4 2
6 4 3 2 1 5
1 2 6 5 3 4
5 3 4 1 2 6        KEY
4 6 2 3 5 1
2 1 5 4 6 3
```

ZIMMERMAN AND CIPHER 0075

Arthur Zimmermann, the German foreign minister sent a message to Mexico that put the US in a fury. German cryptographers used a cipher known to them as 0075. The message sent was:

C:CTLTZ EMRTH IERSI TNAII WETXC AAMOR OXCEA ATWOA
AONIZ NEETN MXASA LDINF ESZRC ATEIO GZFXA LAEIR
AOMBI OWEWW. (90)

Unfortunately for Zimmermann and the Mexicans, British intelligence cracked 0075 and wired U.S. President Woodrow Wilson the following information (paraphrased here):

CONTENTS OF ZIMMERMANN CABLE FOR YOUR INSPECTION:

P:" CONFIRM THAT MEXICO WILL BE AWARDED TITLE TO ARIZONA
TEXAS NEW MEXICO IF MEXICO ENTER WAR AGAINST USA AZ AZ
AZ"

Encipherment:

The key = 0075 was used in a simple equation to obtain a control key.

```
K=19999 +Key
  ----------   = Control Key
    97

K=19999 +0075
  -----------  = 206.948536
     97
```

All 10 digits are used and the period is ignored.

K= 2069484536

This series of digits is ranked according to the value of each digit and its place in the series. Zero = 10.

```
K = 2 0  6 9 4 8 4 5 3 6       control key
K = 1 10 6 9 3 8 4 5 2 7       ranked control key
```

The plaintext is written below the ranked control key , ten letters to the line, but are written into as opposed to out according to the ranked control key.

```
K = 1 106 9 3 8 4 5 2 7
    C A R H N T F I O M   (C O N F I R M T H A)
    T L C I E W X I M O
    L D A E E D A W B R
    T I T R T A L E I O
    Z N E S N A A T O X
    E F I I M O E X W C
    M E O T X N I C E E
    R S G N A I R A W A
    T Z Z A S Z A A U A
    1 2 3 4 5 6 7 8 910     (RE-RANKED KEY)
```

Next we re-rank below the columns the control key, in this case a straight series 1...10. We take out the columns by this new order and divide into groups of 5.

Ciphertext:

CTLTZ EMRTH IERSI TNAII WETXC AAMOR OXCEA ATWOA
AONIZ NEETN MXASA LDINF ESZRC ATEIO GZFXA LAEIR
AOMBI OWEWW. (90)

We have a double transposition. The primary drawback is that the plain text is out in the open (albeit scrambled). In the above cryptogram, the probable word MEXICO with the X is a good start.

SOLUTIONS FOR LECTURE 15 PROBLEMS - Taken from OP- 20 -G course:

15-1. Naval Text. Recover Keys.

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

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

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

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

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

K F H Q R N J B.

The text appears in lines of 26 letters, which was determined as the key length by factoring. This is an example of a regular progressive cipher. We reconstruct the cipher component from symmetrical sequences. The symmetrical sequences found, with their space relationships in the cipher component are:

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

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

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

The letters in parentheses are assumed to belong to the symmetrical sequences but must be checked.

The reconstruction progresses through stages to give:

```
12345678910111213141516171819202122232425 26  Interval
      O                                    Z     7
 Y    O      C         K       S          Z     5
   H   R     C                                  22
   H                                     X      5
P      R                                        7
-----------------------------------------------
PY H  OR     C         K       S         XZ    (combined)
P                      K          U             5
            B         J L                      (assumed)
           NB       FIJ L   Q         W         22
    A      N              M           W         5
               D           Q                     7
        E      D           Q                    22
-----------------------------------------------
PY(T)HA(G)OREN BCDFIJKLMQSU(V)WXZ               (combined)
```

The cryptogram is then converted to the basis of one cipher alphabet. This conversion process makes use of the known shift between components of the cipher alphabet, reducing each letter to is equivalent value had the components not been shifted during encipherment. The shift is done based on the square table.

Similar to a Viggy:

```
1 PYTHAGORENBCDFIJKLMQSUVWXZ
2 YTHAGORENBCDFIJKLMQSUVWXZP
3 THAGORENBCDFIJKLMQSUVWXZPY
4 HAGORENBCDFIJKLMQSUVWXZPYT   for additional sliding
. .....                              sequences
.
.
.
```

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

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

The primary cipher alphabet for this problem is

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

These sequences are constructed from the words quadricular and pythagorean, both names for the square table used for Viggy and other encipherments.

15-2. Naval Text.

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

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

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

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

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

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

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

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

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

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

D U Q W A T Z O W D C L Z Q M P U K.
D T O T W O T H O U S A N D Y A E T

LECTURE 16 PROBLEMS

1. Complete columnar transposition.

   WKAII GLFGA TEYHN ONSOH LGIRI IAAIR LGAMO
   IMHSF IDFGW NNEYH NEFNH SLNSE THS. (63)

2. Nihilist transposition.

   UCTEO UAMAA LTDMI SUDDS SISNU OLNNH AALTA
   EYELB NEANU NRAPH SNENX ESTAE ASJH.

3. Incomplete columnar

   IENOR RENHR NAITI ETTEC FCOIP TREYA RCHTH
   SPOAL YONCW SNARL TEESN TOYEL ERSOL UAIOE
   VEPOR LNRTS HIMIM E. (relatively)

4. Myszkowski. Battlefield.

   YIITU HSATS OIRLF TSTFD NCUAW WGSUS NYATO
   EBEHR GIPNP OUSOM ELEPO YOONR AYOIO URTES
   UTNAA ILWIR EAEAN RAADP E.

5. Amsco.

   HENTI DAHOS CLOSN PRNSA FENTT TIOAM LROTE
   RTLEI ANCSC RCISO EMGRI YOUIT EMTAC AIAME
   ILIVI SPAEW AMIFA. (propaganda)

6. Tramp.

   CGHES NOONE NAETT SHTIA NEQCB AWRSI LTAOH
   OAUEY OCENA TOMRT HAEFO ROEAU PLNSD STHIG.
   (QCTCLYAPMQQ)

7. Cadenus.

   IRHRC GRETR ESDEE OFOWN ETLNS EOTIG IMNEI
   TSONH LTIID DVLTS NIADS LSRAM TSORU HSCNE
   DNIHU EAGCD IGIRS WSLSH BITNI IHNNH DNICD
   ACGEV NGOEL YBADY OALOS. (circles)

8. Railfence.

   TOEYC SOEFO MSAHH RMOYU LDTAC LATYA LFLME
   EBGOP VIPRV IEEVS ALUDO WTGIG THILL CONT.

9. Redefence. Astronomic improbability.
tip = THE MOON TO

REOEN IOFGS AITWE UMTBA PITNP ACOUH OTICN
SAGFP TRLEE HTREN MROOH LEORN SIVSE ONTAC
SRSEL TUERS HDTRO AGYAH TRAON LE.

10. Turning grille.

TIP = the most serious and; NQEJPGUU

STTAH IRNED GSERL GEOGM AETON ENBIE DOTNH
EAEOS MSTFI LSOCI OEHST SNIER CNTEN SHTEC
SOIOS LHOAU SUSIS EANWA TMNER BOECD OSKRC
MSILT EONMB TLAEA CTNID DIEKD OFNMF AXVEF
ESEU.

11. Swagman. Agreeable toil.

NNWTI HYORS TEKKR IENII VNLSN LOTOO SLAVT
RETSI ROSIM KSCFR SEEAO OMTAC HETTI IWEVO
RHEII N.

REFERENCES AND RESOURCES

(I will append to a future lecture.)