CLASSICAL CRYPTOGRAPHY COURSE
BY LANAKI

20 March 1997
Revision 0

LECTURE 24

SPECIAL TOPICS

COURSE NOTES

Lecture 24 will be devoted to special topics and will present additional cryptograms for solution. I will update and restructure my Volume II references and resources file. Lecture 24 will constitute my final efforts. Updated Volume II references will replace Lecture 25.

Those students interested in course participation certificates please advise me by e-mail, so I have an idea how many to order.

Volume II of our textbook is available through RAGYR and Aegean Park Press. You are encouraged to buy a copy. All of the corrections presented to me by our capable class are included in the book. Those interested in signed copies please advise by private E-mail, and I will maintain a small inventory for that purpose.

SUMMARY

I want to clean up some loose ends in the Transposition area and then shift to a review of some of the more popular ciphers presented in Lectures 1-20. I will present more problems, not so much for a "final exam" as for a chance to improve/enjoy our cryptographic skills. I also want to present some additional legal information regarding Defamation on the Net (an expansion on my Privacy Lecture).

UBCHI

The Ubchi (the U is umlauted) is a double columnar transposition cipher used by the Germans during WWI. It was broken by the French thanks to in part to a radio message sent in unprotected cleartext early in the conflict.

The Ubchi had a keyphrase that was represented by numerals according to the position of its letters. Two identical letters were labeled consecutively if they appeared in the same keyphrase. For example,

```
           5 3 7 8 9 2 6 1 4 10
Keyword:   h e r r s c h a f t
```

For the plaintext: First army X Plan five activated X Cross Marne at set hour.

Ciphertext key block 1:

```
 5 3 7 8 9 2 6 1 4 10
 h e r r s c h a f t
 ------------------
 F I R S T A R M Y X
 P L A N F I V E A C
 T I V A T E D X C R
 O S S M A R N E A T
 S E T H O U R
```

The ciphertext was taken off by columns in numerical order of the keyword columns:

```
              1     2     3    4     5     6     7
Ciphertext:  MEXE AIERU ILISE YACA FPTOS RVDNR RAVST

  8     9    10
SNAMH TFTAO XCRT.
```

(Note the 5 letters groups not observed.)

These groups were then transcribed horizontally into another block beneath the same number sequence:

```
              5 3 7 8 9 2 6 1 4 10
              h e r r s c h a f t
              ------------------
              M E X E A I E R U I
              L I S E Y A C A F P
              T O S R V D N R R A
              V S T S N A M H T F
              T A O X C R T(Z)
```

The next step was to add as many Null letters as there are words in the Keyphrase or Keyword. One null Z was added after the last letter in the last row, T.

The German encipherer once more took these letters from the block by columns in the same numerical sequence and separated into standard groups of five letters each:

```
  1     2    3      4     5    6      7    8     9
RARHZ IADAR EIOSA UFRTM LTVTE CNMTX SSTOE ERSXA YVNCI

10
PAF.
```

To decipher the message, the recipient first had to discern the size of the transposition rectangle in order to learn how long the columns were. This was accomplished by dividing the total number of key numbers into the total number of letters into the message (48 / 10). The quotient was the number of complete rows. The remainder 8 was the number of letters in the incomplete columns. The succeeding steps reversed the corresponding steps in the enciphering process.

Note the similarity with the U.S. Army Double Transposition Cipher System. Barker gives a detailed breakdown of this type of cipher in his book. [BARK] It is not coincidental that the two countries at war had very similar cipher systems in play.

U. S. ARMY DOUBLE TRANSPOSITION CIPHER

One of the more interesting transposition ciphers is the double transposition cipher. One of the guru's in this area is Colonel Wayne Barker. His "Cryptanalysis of the Double Transposition Cipher" is enjoyable reading. I thank him for his liberal permission to excerpt from his reference. [BARK2]

In its most effective form the double transposition cipher is based upon two incompletely filled rectangles with two different length keywords. Nulls must be added before encipherment, not to the end after encipherment. In the deciphering process, we must determine the exact dimensions of the enciphering rectangles R-1 and R-2 by keywords K-1 and K-2, respectively.

The process of encipherment is relatively straight forward. The plain text is read into R-1 by rows, taken out by columns in the order of K-1, transcribed into R-2 in rows and removed from R-2 by columns as dictated by K-2. The ciphertext is then separated into the standard groups of 5 letters for transmission.

The difficulty in decipherment occurs when we must determine the exact dimensions of R-1 and R-2 as well as the sequence and width of K-1 and K-2. Recall that we can use the division of the message length by the key length to give us the number of long columns and length of the short columns. For example, for message length 99 with keylength of 13, we have:

```
                     7     - length of short column
                   ------
     keylength =13  | 99    - message length
                     91
                     --
                      8    - number of long columns
```

The length of the long columns is 1 more than short or 8. The number of short columns is 13 - 8 = 5.

This is Step 1.

To decipher the double transposition cipher, the ciphertext letters are inscribed within R-2, whose dimensions have been determined in Step 1, following the column order of K-2. Thereafter, the horizontal letters within R-2 are inscribed within R-1 following the column order of K-1. The resulting plaintext is read horizontally within R-1. So there we have Steps 2 and 3.

Messages In Depth

Regardless of how complex a transposition system may be, the resulting ciphertext messages may be put in depth, superimposed one above the other, the resulting columns may potentially be matched against one another to produce plaintext. Messages must be the same length. This is not a difficult requirement, especially when nulls are added to get an even number letters in groups of 5.

In essence we construct a giant single columnar transposition cipher of message length L. The problem is reduced to juxtaposing (matching the columns) so that the plaintext is readable.

Given the following six messages at L = 115 letters:

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

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

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

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

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

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

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

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

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

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

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

Message 1:  E O A O I N A N R S R L S T U
Message 2:  U P R O G E W K E E N E N S E
Message 3:  T S A T R A O I A I L N W F F
Message 4:  M E A E R U O R U E S N L F O
Message 5:  I E I E E Y F O T N C T A R E
Message 6:  L R A Y I D O T T S W N R T A
```

We look for letters of low frequency such as Q or QU combinations. We may assume that the messages end in X(s) for nulls. We start with this fact.

```
17  26  37  57  68
 -   -   -   -   -
 R   Y   X   E   I
 X   X   X   X   X
 X   X   X   S   I
 X   X   X   S   I
 O   P   X   T   A
 H   X   X   T   E
```

Column 37 is the last, 26 is before it, and 17 with three X's is the antepenultimate column.

```
17  26  37
 -   -   -
 R   Y   X
 X   X   X
 X   X   X
 X   X   X
 O   P   X
 H   X   X
```

Putting column 57 in the group gives us (QU)ERY and (S)TOP. We might work back from this point with maybe GENERAL SMITH for the last message. We can hook up the QU's for breaks in the middle of the messages.

```
    92 48 57 17  26  37
    -  -  -  -   -   -
    Q  U  E  R   Y   X
    R  Y  X  X   X   X
    O  N  S  X   X   X
    N  T  S  X   X   X
    E  S  T  O   P   X
(S) M  I  T  H   X   X
```

Solve the rest.

Key Recovery After Anagramming

The next step in the process is to recover the keys.

Given 4 messages of L = 85 letters, and their anagramed equivalent:

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

Message 1: M E S S A G E S I X O N E S T O P O U R
Message 2: W E A R E R U N N I N G I N T O H E A V
Message 3: T O C O M M A N D I N G O F F I C E R T
Message 4: O P E R A T I O N S O R D E R S I X T E

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

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

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

Message 1: B Y H E A V Y M O R T A R F I R E S T O
Message 2: E N T L Y N E E D E N G I N E E R P E R
Message 3: E R E P R E S E N T A T I V E Y O U R U
Message 4: U R I E R S T O P A D V I S E B Y R A D

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

Message 1: P W E N E E D C O U N T E R F I R E S T
Message 2: S O N N E L T O R E M O V E M I N E S S
Message 3: N I T H E R E T O M O R R O W F O R M E
Message 4: I O W H E N Y O U H A V E R E C E I V E

           0 8 0 8 2
           5 5 2 2 8

Message 1: O P X X X
Message 2: T O P X X
Message 3: E T I N G
Message 4: D I T X X
```

The C -> P sequence is also known as the anagram key. Given the anagram keys we can recover the keys K-1 and K-2.

The anagram key of the above ciphertext example is:

```
79 76 72 25 63 22 60 69 66 51 57 42 54 39 48 45 19 36 10
33 07 16 13 30 04 84 01 81 27 24 62 78 74 75 71 59 56 41
68 53 65 50 38 35 09 47 21 44 18 06 03 83 15 32 12 29 80
77 73 26 64 23 61 70 67 52 58 43 55 40 49 46 20 37 11 34
08 17 14 31 05 85 02 82 28
```

We can index the anagram key as follows:

```
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19
79 76 72 25 63 22 60 69 66 51 57 42 54 39 48 45 19 36 10


20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38
33 07 16 13 30 04 84 01 81 27 24 62 78 74 75 71 59 56 41

39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57
68 53 65 50 38 35 09 47 21 44 18 06 03 83 15 32 12 29 80

58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76
77 73 26 64 23 61 70 67 52 58 43 55 40 49 46 20 37 11 34

77 78 79 80 81 82 83 84 85
08 17 14 31 05 85 02 82 28
```

The indexed version is known as the P -> C sequence. It is also called the encipher key. Inverting the encipher key index gives us the encipher key derived from the recovered anagram key:

```
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19
27 83 51 25 81 50 21 77 45 19 75 55 23 79 53 22 78 49 17

20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38
73 47 06 62 30 04 60 29 85 56 24 80 54 20 76 44 18 74 43

39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57
14 70 38 12 68 48 16 72 46 15 71 42 10 66 40 13 69 37 11

58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76
67 36 07 63 31 05 61 41 09 65 39 08 64 35 03 59 33 34 02

77 78 79 80 81 82 83 84 85
58 32 01 57 28 84 52 26 82
```

The anagram key is the order of the ciphertext letters to produce plaintext, and the encipher key is the order of the plaintext letters to produce ciphertext.

>From the encipher key we derive the Interval Key. The interval key provides the intervals both positive and negative, between successive terms of the encipher key.:

```
+56 -32 -26 +56 -31 -29 +56 -32 -26 +56 -20 -32 +56 -26
-31 +56 -29 -32 +56 -26 -41 +56 -32 -26 +56 -31 +56 -29
-32 +56 -26 -34 +56 -32 -26 +56 -31 -29 +56 -32 -26 +56
-20 -32 +56 -26 -31 +56 -29 -32 +56 -26 -27 +56 -32 -26
+56 -31 -29 +56 -32 -26 +56 -20 -32 +56 -26 -31 +56 -29
-32 +56 -26 +01 -32 +56 -26 -31 +56 -29 +56 -32 -26 +56
```

We start at identifying K-1 length. There are three lengthy repetitions in the interval key starting with +56 and ending with -26. We look at the terms that give rise to these repetitions.

```
27 83 51 25 81 50 21 77 45 19 75 55 23 79 53 22 78 49 17
20 76 44 18 74 43 14 70 38 12 68 48 16 72 46 15 71 42 10
-------------------------------------------------------
07 07 07 07 07 07 07 07 07 07 07 07 07 07 07 07 07 07 07

20 76 44 18 74 43 14 70 38 12 68 48 16 72 46 15 71 42 10
13 69 37 11 67 36 07 63 31 05 61 41 09 65 39 08 64 35 03
-------------------------------------------------------
07 07 07 07 07 07 07 07 07 07 07 07 07 07 07 07 07 07 07
```

The common difference is the length of K-1.

Setting up R-1:

```
                    -------------------
                    01 02 03 04 05 06 07
                    08 09 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
```

Using the derived encipher key, the first column is

27 83 51 25 81 50 21 77 45 19 75

We start by reconstructing R-2. We know that its horizontal rows come from the vertical columns of R-1 and its vertical columns come from the terms of the encipher key.

```
                       1
                 6 13 20 27 34 41 48 55
                62 69 76 83 02 09 16 23
                30 37 44 51
                   25
                   81
                   50
                   21
```

Knowing the width of R-2 gives the dimensions of R-2.

```
85 = 3 - 10's
     5 - 11's
```

The reconstruction of R-2 continues as we discover the order of columns in R-1 entering R-2. This is done by knowing the vertical terms in R-2, which are successive terms of the encipher key.

The reconstruction of R-1 and R-2 with keys identified are:

```
04 02 06 03 07 01 05  K-1 =7
-------------------
01 02 03 04 05 06 07
08 09 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
```

```
 3  6  4  1  8  7  5  2
 ---------------------
 6 13 20 27 34 41 48 55
62 69 76 83 02 09 16 23
30 37 44 51 58 65 72 79
04 11 18 25 32 39 46 53
60 67 74 81 01 08 15 22
29 36 43 50 57 64 71 78
85 07 14 21 28 35 42 49
56 63 70 77 84 03 10 17
24 31 38 45 52 59 66 73
80 05 12 19 26 33 40 47
54 61 68 75 82
```

Solution where known plaintext occurs at any point within the message.

Barker describes solution of several special "crib" situations. He uses stereotyped beginnings, endings and shows the process of overlaying the crib into R-1 and converting it into R-2. Of more interest is the solution when the plaintext crib is anywhere in the message.

Consider the following problem:

```
DTHIS  ERTRS  OUEST  RRTER  NMNCT  ODANO  TOCFO  ARTPN
OEXOS  VWMUW  ODPOD  ECNEQ  APTIT  AMIIF  CAENA  SWMCC
AILAO  OIMOT  DAJLG  NRFOZ  SPUOO  RTTEO  EBRRO  INNE.
(119)
```

Known plaintext: ROAD JUNCTION QUEBEC FOXTROT TWO FIVE EIGHT ZERO

K-1 = 9

Analysis:

The first step is to number the positions of the letters in the ciphertext and make a bilateral frequency distribution.

```
D-1  T-2  H-3  I-4  S-5  E-6  R-7  T-8  R-9  S-10
O-11 U-12 E-13 S-14 T-15 R-16 R-17 T-18 E-19 R-20
N-21 M-22 N-23 C-24 T-25 O-26 D-27 A-28 N-29 O-30
T-31 O-32 C-33 F-34 O-35 A-36 R-37 T-38 P-39 N-40
O-41 E-42 X-43 O-44 S-45 V-46 W-47 M-48 U-49 W-50
O-51 D-52 P-53 O-54 D-55 E-56 C-57 N-58 E-59 Q-60
A-61 P-62 T-63 I-64 T-65 A-66 M-67 I-68 I-69 F-70
C-71 A-72 E-73 N-74 A-75 S-76 W-77 M-78 C-79 C-80
A-81 I-82 L-83 A-84 O-85 O-86 I-87 M-88 O-89 T-90
D-91 A-92 J-93 L-94 G-95 N-96 R-97 F-98 O-99 Z-100
S-01 P-02 U-03 O-04 O-05 R-06 T-07 T-08 E-09 O-110
E-11 B-12 R-13 R-14 O-15 I-16 N-17 N-18 E- 119
(119)
```

```
A 28 36 61 66 72 75 81 84 92
B 112
C 24 33 57 71 79 80
D 01 27 52 55 91
E 06 13 19 42 56 59 73 109 111 119
F 34 70 98
G 95
H 03
I 04 64 68 69 82 87 116
J 93
K
L 83 94
M 22 48 67 78 88
N 21 23 29 40 58 74 96 117 118
O 11 26 30 32 35 41 44 51 54 85 86 89 99 104 105 110 115
P 39 53 62 102
Q 60
R 07 09 16 17 20 37 97 106 113 114
S 05 10 14 45 76 101
T 02 08 15 18 25 31 38 63 65 90 107 108
U 12 49 103
V 46
W 47 50 77
X 43
Y
Z  100
```

Now on to K-1 at length 9, we write in the known plaintext:

```
1 2 3 4 5 6 7 8 9
-----------------
R O A D J U N C T
I O N Q U E B E C
F O X T R O T T W
O F I V E E I G H
T Z E R O
```

Focus on column 4 with the infrequent letters of Q and V. We can establish this as a row in R-2. We locate two columns that fit the pattern.

```
  P   P
  O   N
  D   O
  E   E
  C   X
  N   O
  E   S
D Q T V R
  A   W
  P   M
  T   U
  I   W
  T   O
  A   D
  M   P
```

The column added to R-2 come directly from the ciphertext. Lets analyze the positional information to reconstruct R-2.

Q and V occur in positions 46 and 60. We can expect the length of of K-2 will be a multiple of 14 because the difference is 14. Letters occurring in the same column of R-1 which occupy the same row of R-2 will be separated in the ciphertext by a multiple of R-2 column lengths. This is a multiple of the key. We might expect that R-2 is 14 for a column length. Two rectangle widths give rise to a column length of 14 for L = 119.

```
              K-2 = 8
1]      119 = 7 - 15's
              1 - 14

              K-2 = 9
2]      119 = 2 - 14's
              7 - 13's
```

Look at letters H and W:

H= 03

W = 47 50 77 --> distances of 44 47 74 which is consistent with column length of 15 and 14 for K-2 =8.

So the width of R-2 is 8. We construct a analytical matrix of width 8:

```
1 2 3 4 5 6 7 8

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

Using the DQTVR as the starting column, we locate columns 5 and 4 of R-1:

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

We mark off the known plaintext and work up and down from the starting row to get the solution with K-1 =9:

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

Wayne's Contribution To Cryptography - Solution that Requires No Known Plaintext Crib.

Colonel Barker found that any double transposition cipher can be expressed as an equivalent single transposition cipher.

Consider the following double transposition encipherment:

```
              3  2  1  5   4    K-1 = 5
              -------------
              1  2  3  4   5
              6  7  8  9  10
              11 12 13 14 15
              16 17 18 19 20
  R-1         21 22 23 24 25
              26 27 28 29 30
              31 32 33 34 35         13 X 5 matrix
              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  -  -

            63 = 3 @ 13 long
                 2 @ 12 short
```

and

```
                3  2  4  1     K-2 =4
                -----------
                03 08 13 18
                23 28 33 38
                43 48 53 58
                63 02 07 12
                17 22 27 32
                37 42 47 52          16 X 4 matrix
                57 62 01 06
 R-2            11 16 21 26
                31 36 41 46          63 = 3 @ 16 long
                51 56 61 05               1 @ 15 short
                10 15 20 25
                30 35 40 45
                50 55 60 04
                09 14 19 24
                29 34 39 44
                49 54 59 -
```

Ciphertext:

```
18 38 58 12 32  52 06 26 46 05  25 45 04 24 44
08 28 48 02 22  42 62 16 36 56  15 35 55 14 34
54 03 23 43 63  17 37 57 11 31  51 10 30 50 09
29 49 13 33 53  07 27 47 01 21  41 61 20 40 60
19 39 59    (63)
```

Note that where the plaintext is a straight numerical sequence, the resulting ciphertext is the encipher key. Exactly the same ciphertext or encipher key will result from the following single columnar transposition cipher:

```
18 07 11 05 04 03 17 06 15 14 13 02 16 10 09 08 12 01 20 19
------------------------------------------------------------
01 02 03 04 05 06 07 08 09 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
```

Ciphertext:

```
18 38 58 12 32  52 06 26 46 05  25 45 04 24 44
08 28 48 02 22  42 62 16 36 56  15 35 55 14 34
54 03 23 43 63  17 37 57 11 31  51 10 30 50 09
29 49 13 33 53  07 27 47 01 21  41 61 20 40 60
19 39 59    (63)
```

matrix = 4 X 20

63 = 3 long @ 4
17 short @ 3

Very simply, the results of using the two double transposition keys 3-2-1- 5-4 and 3-2-4-1 to encipher message L = 63 can be duplicated by using the single transposition key: 18-7-11-5-4-3-17-6-15-14-13-2-16-10-9-8-12-1-20-19. This

result does not surprise the pure mathematicians in the group. The equivalent key, Keqv, reflects K-1, K-2 and the message length.

K-1 (length) X K-2 (length) = Keqv (length of single transposition key)

To successfully attack the Keqv problem, the length of the message, L must be longer than the key.

Plaintext:

```
01 02 03 04 05 06 07 08 09 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
```

Ciphertext:

```
18 38 58 12 32  52 06 26 46 05  25 45 04 24 44
08 28 48 02 22  42 62 16 36 56  15 35 55 14 34
54 03 23 43 63  17 37 57 11 31  51 10 30 50 09
29 49 13 33 53  07 27 47 01 21  41 61 20 40 60
19 39 59    (63)
```

```
K-1: 3-2-1-5-4

K-2: 3-2-4-1
```

Equivalent Single Transposition Key:

```
  Col 1    |  Col 2     | Col 3      | Col 4
    18-7-11-5-4-3-17-6-15-14-13-2-16-10-9-8-12-1-20-19
```

Two points: 1) Given two double transposition keys, there are multiplicity of single columnar transposition keys, each depending upon the length of the plaintext being enciphered, and 2) Given a particular single transposition key, there are only two specific double transposition keys which will give rise to the single transposition key; and both keys K-1 and K-2 may be recovered regardless of the message length L. Keqv can be considered a rotating matrix.

```
                  18 03 13 08     3
                  07 17 02 12     2
                  11 06 16 01     1  K-1
                  05 15 10 20     5
                  04 14 09 19     4

                  3   2  4  1
                     K-2
```

The rotating matrix will be in the form of a complete rectangle and the correct rectangle can be recognized by each of its rows containing a single, different term of K-1. There are several symmetrical relations with respect to this rotating matrix:

1. The row terms of the matrix are equal to each other when considered (MOD n), where n = length K-1.

Modulus five for the above rotating matrix is:

```
                          (mod 5)

18 03 13 08            3 3 3 3
07 17 02 12            2 2 2 2
11 06 16 01            1 1 1 1
05 15 10 20            5 5 5 5
04 14 09 19            4 4 4 4
```

2. There is a difference relationship between row terms.

```
18 -  03  =  +15
03 -  13  =  -10
13 -  08  =  +05
08 -  18  =  -10
```

for the entire matrix, we have:

```
+15 -10 +05 -10
-10 +15 -10 +05
+05 -10 +15 -10
-10 +05 -10 +15
-10 +05 -10 +15
```

The differences are the same, only rotated. If we renumber the values in each row as 'indicators' we have the following row identifications:

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

The row of the matrix containing 1 will not rotate. It will always reflect the value of K-2. The remaining rows will rotate with the rotation depending on the length of the message L. Each row in effect identifies one term of the key K-1. If 2 occurs in a particular row, we know that the position of that row will indicate the position of 2 in K-1. If we can identify a particular letter of the ciphertext as part of a column, we can identify one of the terms in the rotating matrix. The value of that term (mod n), will provide one of the terms of K-1. It is related to all the terms in its row mod n.

The solution of ciphertext problems follows the same lines as discussed previously on a single transposition rectangle. Barker gives three interesting examples. [BARK2] GUNG HO has also addressed the solution of double transposition ciphers. [GUNG]

THE AUGUSTUS CIPHER

The Augustus Cipher is closely related to the Viggy, and is attributed (possibly erroneously) to Emperor Augustus. The rumor is that he used a passage from Homer as the key to encrypt his messages. The key is equal to the length of the plaintext. He used as much keytext as required to meet the message size.

To encrypt the Mth letter of the plaintext, select the Mth letter of the keytext; the position of this letter in the alphabet determines the shift for the plaintext letter. If the Mth plaintext letter is O and the Mth key text letter is C, the shift is three, because C is the 3rd letter in the alphabet, and thus O is replaced by the R, which is 3 places further along in the alphabet. The process is Mod 26. So, the plaintext letter W encrypted by the key letter F (shift = 6) would result in the ciphertext letter C.

Example:

Plain: London calling Moscow with urgent message. Key Phrase: To be or not to be that is the question whether

```
Plain:     L  O  N  D  O  N  C  A  L  L  I  N  G  M
Key Text:  T  O  B  E  O  R  N  O  T  T  O  B  E  T
Shift:    20 15  2  5 15 18 14 15 20 20 15  2  5 20
Cipher:    F  D  P  I  D  F  Q  P  F  F  X  P  L  G

Plain:     O  S  C  O  W  W  I  T  H  U  R  G  E  N  T
Key Text:  H  A  T  I  S  T  H  E  Q  U  E  S  T  I  O
Shift:     8  1 20  9 19 20  8  5 17 21  5 19 20  9 15
Cipher:    W  T  W  X  P  Q  Q  Y  Y  P  W  Z  Y  W  I

Plain:     M  E  S  S  A  G  E
Key Text:  N  W  H  E  T  H  E
Shift:    14 23  8  5 20  8  5
Cipher:    A  B  A  X  U  O  J
```

The Vigenere Tableau can be used to assign letters similar to the standard Viggy. The main difference is the Key text can be long and no repeating. The Augustus cipher can be attacked by dictionary type attacks or by high frequency letters is groups to identify small parts of the text.

SCI.CRYPT CHALLENGE VIGGY

This challenge was issued by Howard Liu of U. C. Davis:

```
FWNGF XSMCK JSVGK WOGWZ FSJJP QIMJR ESIIM GFMIM GOGIU
DSDRX VFVTG GRDRR NOWCI KBOLZ EVVWV ACPLZ FSOVR PGAMX
WFVXZ QBNXY QINEE FGJJK JSHQF XSHIE VCACF WFZCV DFJAJ
OOFIJ GOMXY SIVOV.
```

ACA 's AAHJU (Larry Mayhew) solved this Viggy right away. Try it.

HEADLINE PUZZLE

RIDDLER throws this Headliner from the Wall Street Journal out for us to play with:

```
1. VJZ  UXYMP  LJQMG  EKJR  WMJVIMC'S  JXYM  XZ  WIM
   VKJGGCPPQ?

2. PNRO  UN  SWIODLSWJO  OAYDBZUWNA  OHZNDUM  WM
   CASWGOSB  UN  MOUUSO  VWQTUM  NROD  ZDWRLYB.

3. FKOFMKS  FKSZ  THGUMKS  ULDGU  SLR  NKQQKFMTSZ  KX
   YODEKXF  OHFKHT  JKHU.

4. QPKSYKE=CHKRZE  FYHKG  BKEKSPQ  HEKSPQ  ZU  XYZJUEKJ
    KJB  YPBQFZJP.

5. EUAHBZTLB  EU  ZPEB  NJUS  IEDPZ  JBH  DCEUB  ZT  QJG
    ZPH  QLTTRYGU.
```

Solve the headlines; recover hat, setting and key.

ARISTOCRATS

With the help of FLORDELIS, here are a few Risties to wet the appetite:

1. Naughty Words. K2

NF CH FXUS XE TDSSRHU HT EASSQW UHDS
ADSQXHGE FWNC JWSC N UNC WXFE WXE FWGUP
JXFW N WNUUSD. *UNDEWNOO *OGUERSC.

2. Be Flexible. K1

INPG NV: QCE FNSW, UYWNM, VECM SWNQ GNTSW,
SWNHWF CMWP GC FWNG WOXYG MWCMSW, YOPXW YCSVF
GYWB QOEBSK OP MSNUW.

3. Crackerjack. K?

DXYUV HLOCT LNBFAR MOBQC, ABDUT XBQC TXBS,
QBPUT MLQC HXUA RLNC, SYQCT OBQC, EFYQCOJ
SLQCT TDBQC YA CALSTLQC.

4. How's that again? K?

PTUKAKDKNA NU "QBNALT": RA TGBRAQKJYT
RJQNOBDKNA ZNPEYT QTAQKDKFT DN PKUUTOTADKRY
ZNYTSEYRO DTAQKNAQ.

5. Gone with the wind. K?

KZDFLVYEAT DZBPVJSKX OXSKD FSKDLVYQGW.
KZDBLIYQGF LSGTQF. OZYF GXZBPVL GWSDBLV
OEATVPSYDL. DZBPVYGYQ JXZBPV QDFL.

SIMPLE VARIANTS

Here are a few "change-ups" to consider:

1. The way to get to nowhere.

SRE NR OCYNA MOOTG NI TTUCYLB AB ORP
SISE LCRIC NI DNU ORA GNIOGFLESM IH
SDN IFOH WYDO BYNA.

2. NKWO HWRY PIAV WNNI LKWE SABA ELOT LSEE
FPRO WTNE YTEY RANS NOOE HFSI ENGI BHRO
HSDA SAET ERPO ALEY R.

3. Value System.

```
FIUOY  ACPSN  NEPAD  RECEF  LTSUY  LESSE  FARET
ONINO  ANREP  EFLTC  UYLES  SEAMS  NNYRE  UOVAH
LERAE  ENOHD  TWILO  EV.
```

Solve.

PATRISTOCRATS

Here are three fun Patristocrats for solution and key recovery:

1. Sir Galahad to the Rescue.

```
IYAIS  FWZBU  BJLAX  WVJAX  OBLYB  VNSJN  DJSNY
ISJZP  UUBVQ  WVYBT  IYVAA  ISQAM  BMQPL  YFAJA
IVBIS  JNFWR  AVBMB  QWTAV  JSYNY  FWRAV  ATXPU  UAI.
```

2. Orderly Words.

```
PHKWR  HWMIA  FDAYH  JADUJ  PUGXG  HRXQI  UJDQL
FDTXA  UYDQH  WMXWD  WXDTI  AXSUH  KIDTI  AXJAU
HKIDW  IXJUH  KIDJM  PDYXA  UHKI.
```

3. Oratory.

```
RFKRW  UCQVK  SYRFA  UEKHC  QVYDA  HKIOK  WAYAR
FIRRF  KWKYA  RUUEC  DFVKJ  TRFRU  RFKYW  AHKKD
FKAIJ  XJURK  JUCTF  XKHRF.
```

KEY PHRASE

I don't recall discussing the Key Phrase cipher in much detail. It is a regular cryptogram with a few new twists: 1) a letter may represent itself; 2) a cipher letter may represent more than one plaintext letter; 3) The key word is a 26 letter key phrase rather than a disarranged alphabet.

Edgar Allen Poe like this particular cipher. Example:

```
Plain:    ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher:   FORTITERINRESUAVITERINMODO
```

The Latin Key phrase fortiter in re, suaviter in modo -"strongly in deed, gently in manner."

In Poe's example, the word GAMES would be enciphered EFSIE.

Note that letters may be missing from the cipher key. To solve a key phrase we start with a crib, and work back and forward between the key sentence and the the cryptogram. Remember that one cipher letter may stand for several plaintext, but each plaintext letter has but one substitute.

Try these two Key Phrase ciphers and recover their phrases:

1. Evelyn Wood for drivers?

```
VET  EETTA  SERSEVSRT  SA  DOTTE  ATSETER  TD  VESV
TV  TESWUTD  TSE  VS  ATREAT  SEV  VET  EUSRTAUTSA
DTRED  TE  VTST.
```

2. Handsome salary.

```
ABE  BAAV  AEV  VPEH  EETE  ABE  VPEH  EBEL  EANT
BTEPAEHA  PRREAEAL  EPH  AA  EPTL  ABE  HPEPTE  EAN
OPLLAA  EENE  AL  LAE.
```

ROMANTIC FRENCH KEYPHRASE

Corinne Bure sent me a fun little challenge from France (to her from her boyfriend).

Ciphertext:

```
11 10 02 08 21 23 30 04 06 09 01 07 12 16 21 23 30 21 24
10 02 03 05 21
```

Give it a try then see the answer.

NULL

The only way to attack Null ciphers is to try everything. Here are four. The last in this group is a Doosey.

1. Business advice.

```
We are soon to enlarge night operations.  Temporary
workers all now transferred.  Notify our trainees.
```

2. Daddy was a crypee. He rearranged his son's French lesson:

```
aigle
conversation
printemps
dehors
entendre
tuyau
parler
premier
ouvert
pied
voyager
ferme
vite
casuel
vert
oreille
acheter
apporter
chien
secret
quelque
savant
sale
profond
liste
violon
citron
```

3. It's also Golden.

dashing brainy also Aesop giant fact maestro haggle jail avenue aerie case menace aorta implant bashful aegis brand swat.

4. The Key To Escape.

Sir John Trevanion was imprisoned in Colchester Castle in England during the days of Cromwell. He received this message and deciphered it rather quickly. Sir John was in prison for only a short period before making his dash for freedom. How long would it have taken you?

Worthie Sir John:-Hope, that is ye best comport of ye afflictyd, cannot much, I fear me, help you now. That I wolde saye to you, is this only: if ever I may be able to requite that I do owe you, stand not upon asking of me. 'Tis not much I can do; but what I can do, bee verie sure I wille. I knowe that, if dethe comes, if ordinary men fear it, it frights not you, accounting it for a high honour, to have such a rewarde of your loyalty. Pray yet that you may be spared this soe bitter, cup. I fear not that you will grudge any sufferings; only if it bie submission you can turn them away, 'Tis the part of a wise man. Tell me, an if you can, to do for you any things that you would have done. The general goes back on Wednesday. Restinge your servant to command. R. T.

BACONIAN

Recall the 5 part substitute for each letter of the Baconian Cipher:

A	- AAAAA	N	- ABBAA
B	- AAAAB	O	- ABBAB
C	- AAABA	P	- ABBBA
D	- AAABB	Q	- ABBBB
E	- AABAA	R	- BAAAA
F	- AABAB	S	- BAAAB
G	- AABBA	T	- BAABA
H	- AABBB	U/V	- BAABB
I/J	- ABAAA	W	- BABAA
K	- ABAAB	X	- BABAB
L	- ABABA	Y	- BABBA
M	- ABABB	Z	- BABBB

Any two dissimilar groups can be used to make a Baconian cipher.

Try these two.

1. Carpenters Rule.

```
IXAPR  IOBEE  AEIOU  POOOX  BAYFG  MAYOE  EAGOA
TOAZI  YAFQP  LOAIO  OLEOA  IOACY  EESAA  AOIEZ
OEFAA  EILOG  AHWOK  POOIE  OABEO  AEIRA  VOEZB
DEOPA  FYYSO  OHEOE  EKQEA  OOBME  ATREQ  ENNAO
AEOCY  OAMEA.
```

2. Tried and true.

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

ADFGX CIPHERS

The ADFGX cipher was invented by a skilled German cryptographer during World War I. In the original ADFGX cipher, there were three stages of encipherment, which added to the difficulty. The alphabet square permitted the enciphering alphabet to be inscribed in various ways: vertically, horizontally, circular, etc. Anyway that a Tramp could be defined, the cipher alphabet could be used. A crib was usually necessary to expedite the solution.

Here are three forms of the same cipher:

```
                                        E B O N Y
   a d f g x          S P A C E         B R O W N
   ---------          ---------         ---------
a |A F L Q V      C |A B C D E     W B |A B C D E
d |B G M R W      O |F G H I K     H L |F G H I K
f |C H N S X      M |L M N O P     I A |L M N O P
g |D I O T Y      E |Q R S T U     T C |Q R S T U
x |E K P U Z      T |V W X Y Z     E K |V W X Y Z
```

Try these on for size:

1. Cashless. [WALLET]

```
EO EE PN PO EE NY PM PN SO EE PM EM DE EN PO NN DM
SM DY PN PM DN NN NY DM PO SO DM EM EM DY PO PN NO
NY SO DY PE DY EO EE SM DY DE EE PM PE DN PE DY DE
NO PO DN DM PE DE PN.
```

2. Four-Legged Creatures. [CALLED]

```
EE IE TO TS EH GS TE GE ES IH TE GR GR TO IO EE IE
TO TH TO TR TS TE TE IE EH TS ES TO EE GH IS TO TS
TR TO IH TE RH ES TO EH IR GH EE ES ES EE TS GH EO
TO ES.
```

3. About this cipher.

```
aa ff gf gg fd xa dg ff aa df xa ad gf dg gg fd gd
fg fa gd xf fd xa dg gd fg gg fd xa fa fd xa fa xd
xa dg da gf aa dg ga.
```

COLUMNAR TRANSPOSITIONS

These complete columnar transpositions should be easy:

1. Political Logic?

```
WSCCC  SRTTE  TIWTR  EACFK  HHTHH  YDROT  OPAAU  USGOR
CEILO  RYORW  MONIN  IOELE  ELSMT  NHTOC  OOIOE  ITDNH
```

2. They spit in your face too.

```
LEARM  ENOAC  AWMSG  STYUH  OESHL  RVIUA  UUMAR  IAYEO
SNSGE  METSY  ETXHL  FDSAO  AYAYA  IATET  LHAHR  IETAO
RLMNV  HUDNU  HSSYR  PETCN  IGTEA  EEMRE  TAMNL  HRHLU.
```

NIHILIST TRANSPOSITIONS

I have always enjoyed the Nihilist ciphers. Basically it is a square columnar which is written in by rows, and removed by columns. We rearrange the rows and columns by the same numerical (keyworded) sequence. For example: 1. Imported.

```
ISRSE  EULCL  SGRVT  TESIU  AOAEN  HITHR  YHEHN
FINOE  DHANE  TAUCS  NYTPS  NPRET  MEHSI  OEUER
AINIF CTCYI  R.
```

2. Open 10 to 5.

```
IOINS  YSKIL  FSTAT  DEIEO  UATIF  OAEOE  OTSRT
AFSMS  RTHSI  NLCFH  GNOTL  WOEER  NEMOU  ORMHU
FTDIA  ASCDN  IIETC  NPOTO  CBFPK  SIDCY.
```

DEFAMATION ON THE NET

Law on the net is way behind the technology. There is a particular danger and risk in the area of Defamation and Privacy. Assume that every thing you write on the net can be read and disseminated to millions of readers, without delay. This is particularly true if the material is "juicy." This week the Supreme Court must take up the questions of indecency and pornography on the net. Do they hold that their jurisdiction is world wide? Do they permit anyone to say anything - no matter how bad - no matter how true - in favor of the First Amendment Freedom of Speech provisions?

The cards are stacked the wrong way. A person defames another when he or she makes a false statement about that person that injures his or her reputation. This includes both libel and slander.

It is possible for a person to go to a national provider, like AOL, Free, upload 1,000,000 bytes of pure trash about you or your family, their medical, sexual, financial behavior - all being fiction! - to a common bulletin board, and then drop the service, leaving behind material that is perused by 1000's of people a day using "search engines". In the real world, reputation can be injured in public discussion, loss of job opportunity, or professional contact. This is especially true if one's circle of business and friends is well connected to the cyber world. Defamation suits involve big money - about $100,000 up front and $150/hour against time spent.

Why? A statement only defames if it is untrue. If a reasonable jury would say "so what if he called you.. how were you hurt?," then your case is not strong. Even when your case is strong, system operators have strong protection from liability. A major defense is the public figure exception. Online services qualify for this exception as both publishers and distributors of information. The private figure is given more protection. For practical purposes, a plaintiff can look forward to many depositions to harass before he will get his case before the jury. Amicus curiae briefs from all sorts of groups will surface to stop any restriction on the ability to defame your neighbor.

Even accusations detailing instances of dishonesty, disloyalty, distasteful sexual practices, and other reputation - staining events that never happened give rise to defamation claims. Even if an online service prints a retraction, how do you know that EVERY person who saw the lies will get the retraction? in Europe? In Africa? etc. The real problem created by defamations is the set of unpleasant associations created by the false accusations. Even when retracted, the negative image is carried in the mind for years. "Mere opinion" is protected speech as well as satirical and political commentary. Look at the attacks on the President.

A violation of Privacy may arise from publishing messages on an online service about a person's private affairs that a "reasonable person" would find highly offensive, and that are not part of the publics legitimate concern. As a practical matter the disclosure must be major and cause great pain and embarrassment to lead to legal justification for substantial money damages.

Privacy claims don't apply to events that occur in public, are a matter of public record, or can be claimed as newsworthy.

There is a variation on the standard right of privacy called "false light" privacy. A false light claim arises when someone reports something about someone else in a misleading context that injures that person. The false light claim needs to be offensive to the average reader or viewer.

Another privacy-related right is that of publicity. It prevents people from exploiting your name or image for profit without consent through licensing arrangements with the owner of the right.

The Daniel v Dow Jones, (520NYS2d 334) case relieved the online provider from giving out erroneous information that may injure another. The court stated, " The First Amendment precludes the imposition of liability for nondefamatory, negligently untruthful news." The only exception to this is when a "special relationship" existed with the systems operator.

Lance Rose has written an authoritative book on your online rights called: "Netlaw," The Guidebook to the Changing Legal Frontier, Osborne Mcgraw-Hill, NY, 1995. [ROSL]

I feel that cryptography is our way of limiting the damage - At least our E-mail can be safe from prying eyes. We may not be able to stop the loose cannons, but most of us have integrity and can protect our privacy with the appropriate use of cryptographic tools.

ANSWERS TO LECTURE 24 PROBLEMS ****

Liu's Challenge Viggy:

Key = COVER.

Discovery: The actual side of your face never revealed being trapped in a Labyrinth. I chase you. Hide transfigurations - thousands of them. Movement of your eyebrows make earthquake.

RIDDLER'S Headliner:

1. Can video games play teacher's aid in the classroom?

2. Move to liberalize encryption exports is unlikely to settle fights over privacy.

3. Circuit City lawsuit shows the difficulty in proving racial bias.

4. Seagram=Viacom trial damages images of Bronfman and Redstone.

5. Investors in this fund might use gains to buy the Brooklyn Bridge.

Key -- MEGAZORD
Setting -- MORPH
Hat -- RANGERS

```
5 1 4 3 2 6 7
R A N G E R S

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

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

Aristocrats

1. At no time is freedom of speech more precious than when a man hits his thumb with a hammer. Marshall Lumsden.

2. Want ad: for sale, cheap, drop leaf table, leaves open to seat eight people, hinge holds them firmly in place.

3. Thief walks around block, notes lock shop, comes back when dark, picks lock quickly, packs stock in knapsack.

4. Definition of Sponge: an expansible absorption module sensitive to differential molecular tensions.

5. Windstruck nightfowl blown downstream. windspread soked. Bird alights amongst buckthorns, nightmare flight ends.

Simple Variants

1. Backwards. Anybody who finds himself going in circles is probably cutting too many corners.

2. Reverse each pair of letters. Know why Rip Van Winkle was able to sleep for tenty years? None of his neighbors had a stereo player.

3. Reverse the first two letters,then the next three in sequence. If you can spend a perfectly useless afternoon in a perfectly useless manner you have learned to live.

Patristocrats

1. The tip of a lance borne by a charging knight in full armor had three times as much penetrating power as a modern high-powered bullet.

2. Four words that contain five vowels in alphabetical order are abstemious, abstentious, arsenious and facetious.

3. The trouble with some public speakers is that there is too much length to their speeches and not enough depth.

Key Phrase Ciphers

1. Sweet are the uses of adversity. The chief advantage of speed reading is that it enables you to figure out the cloverleaf signs in time.

2. Proverb. Better late than never. The good old days were the days when your greatest ambition was to earn the salary you cannot live on now.

Romantic French Keyphrase:

Use the French Phrase " L' essentiel est invisible pour les yeux."

Invert the order and number sequentially.

```
L  E  S  S  E  N  T  I  E  L  E  S  T  I  N  V  I  S  I
33 32 31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16 15

B  L  E  P  O  U  R  L  E  S  Y  E  U  X
14 13 12 11 10 09 08 07 06 05 04 03 02 01
```

The Plaintext converts to:

POUR TES YEUX L'EST EST L'OUEST" = For your eyes the East is the West.

Nulls

1. Ist letters. Waste not want not.

2. Up the third column. To solve ciphers try everything.

3. After the letter A. Silence is golden.

4. Third letter after each punctuation mark. Panel at east end of chapel slides.

Baconian

1. Vowels = A; consonants = B. Measure thrice before cutting once.

2. Numbers represent how many times a letter is repeated before it changes. Old friends are best.

ADFGX

1. SPEND; MONEY. Alt. Horizontals. Most of us wouldn't have such fat wallets if we removed our credit cards.

2. TIGER; HORSE. Straight horizontals. The Romans called the zebra a horse-tiger because of its stripes.

3. Straight verticals. Another name for this cipher is the checkerboard.

Columnar Transpositions

1. 8 x 10. How come those politicians who claim the country is ruined try so hard to get control of the wreck?

2. 10 x 12. Llamas are very shy, yet have great curiosity and must examine anything unusual. Although of the same order as camels they are smaller with no hump.

Nihilist Transpositions

1. 321867594. A group of Russian Nihilists in the late nineteenth century may have used this cipher for secrecy.

2. 35976428110. The most difficult task of the medical profession nowadays is to train patients to become sick during office hours only.

ON A PERSONAL NOTE

our course is complete. Together, we have made a special contribution to the science of cryptography. We have brought a new group of interested souls to the ACA. We have revitalized the very outlook of the ACA. As we move into the Millennium, we have accomplished our professional goals and improved our skills.

It has meant a lot to me to be your class facilitator. Please remember me when you write my VALE. Explain to Y-ME that the two years that we have been in cipherspace together was worth her patience.

Lastly, Classical Cryptography Course Volumes I and II represent our best efforts to leave a lasting reference in the study of the science of cryptography. Please buy them, put them in your cryptographic library and help us preserve a great legacy. Send me your comments, solutions and questions, as you complete the various lectures. So that I can order the correct amount, I need to know how many of you want me to send you a class participation certificate. It is not necessary to have completed all the problems to be eligible. If you enjoyed the effort and learned something along the way, then I am happy to include your NOM.

If you have enjoyed my course in classical cryptography, then Tell the EB, or write MICROPOD, FIZZY, QUIPOGAM, SCRYER or PHOENIX. They will appreciate your comments. I also would like to have your comments and evaluations so that I can improve the material should I attempt a rerun of this course at a later date.

My best to you and your families. Again, I am deeply honored to have been your teacher / facilitator for this course.

LANAKI
20 March 1997