PRACTICAL CRYPTANALYSIS

VOLUME IV

"CRYPTOGRAPHIC ABC'S"

by

WILLIAM G. BRYAN

VOLUME I

Substitution and Transposition Ciphers

THE AMERICAN CRYPTOGRAM ASSOCIATION

1967

PRACTICAL CRYPTANALYSIS

VOLUME IV

"CRYPTOGRAPHIC ABC'S"

by

WILLIAM G. BRYAN

VOLUME I

Substitution and Transposition Ciphers

THE AMERICAN CRYPTOGRAM ASSOCIATION

1967

VOLUME I

CONTENTS

CHAPTER I. THE NULL CIPHER

In many ciphers "nulls" (useless letters) are used to complete the final five-letter group; or are inserted within a cipher to upset frequencies, or for some other hidden purpose. This is not true with The Null Cipher.

In the Null Cipher, the majority of ciphertext letters are "nulls"; and only ones, depending on their position in words, either with a systematic pattern, as initial, final; 1-2-1-2 front and back; 1-2-3-2-1; 1-2-3-4-1-2-3-4; or some prearranged sequence 1-6-8-9-1-6-8-9, etc. may be used to give legitimate plaintext. A variation of the numerical arrangement, however, might be that the plaintext letters occur after certain other letters (nulls) and only after these specific letters; that is, a "T" after a doubled vowel is chosen for the plaintext; but a "T" after an "H" is ignored. There seems to be no limit to the Null Cipher from the constructor's viewpoint, and so it is difficult to explain all angles. The best advice is to try everything.

Problem 1.
Getting out orders depends momentarily on routine necessary in negotiations. Gauge time or you overwork uselessly.

Problem 2.
TUBER SPENT USHER START AMPLE VAPOR CRYPT ITCHY ROOST TEMPT CLEAR TOWEL ASHEN PRAWN AFTER HUMOR BRACE TRYST

Problem 3.
Perhaps facing the statistics efficiently from natural assumed operation offer the reaction; now that each plan pursued aids neither association or club viewed within normal agenda.

CHAPTER II. THE BACONIAN CIPHER

Like the Null Cipher, the Baconian Cipher has endless possibilities, but unlike the Null Cipher, there is a more systematic approach to solution. The Baconian is based on groups of five units, either A-units or B-units, to produce such combinations as AAAAA or ABABA, etc. A special Baconian alphabet is necessary as the first requirement:

A-aaaaa	IJ-abaaa	R-baaaa
B-aaaab	K-abaab	S-baaab
C-aaaba	L-ababa	T-baaba
D-aaabb	M-ababb	UV-baabb
E-aabaa	N-abbaa	W-babaa
F-aabab	O-abbab	X-babab
G-aabba	P-abbba	Y-babba
H-aabbb	Q-abbbb	Z-babbb

Notice that no group begins with a double B; a peculiarity of this cipher; and a fact which aids solution, since it is known that such an occurrence cannot exist.

The number "5" enters strongly into the picture. The length of the cipher must be divisible by five; words used in the cipher itself must be five-letters long; or a series may be composed of five digits, etc. This is because the above alphabet is made up of five units, part A- and part B- or all A.

A-units and B-units are devised from various schemes.

Either, for example, may be represented by consonants, by vowels (but not both); by the letters A-M or N-Z; they may be shown by those letters which have an upright stroke above or below the line of a typewritten character as against those which do not: b d p h versus c e n o; there may be verbs and adjectives; nouns and adjectives; common and proper nouns; BUT whatever arrangement is chosen it must be broken up into paired series, so that one can be A's and the other B's.

Take for example: SUCCESS

```
  S     U     C     C     E     S     S
baaab baabb aaaba aaaba aabaa baaab baaab
```

Since the Baconian ciphertext does not have to read sensibly, though many of them do, and these mean more preparation, suppose a series of numbers is to be used to portray the above example, using the odd digits for the A's and the even digits for the B's. The resultant cipher would be:

29774 93186 75761 11749 79453 41114 63972, or if the letters A-M are to be B's and the letters N-Z are to be A's, the cipher might commence:

```
COME OUT PLENTY TO EVERY FROM YOUR SOONER AT LENGTH etc.
A    N   N      N  A     A    N    N      A  A
M    Z   Z      Z  M     M    Z    Z      M  M
```

Problem 4.

ANKLE DRAFT JUROR FREAK BEACH VALVE AISLE FILLY DROLL YOKEL ASTER SPOIL CABIN TEETH BLUNT BERRY YACHT MEDAL FRESH BORNE FELON MOUND KODAK NEVER ANGRY BEARD LOYAL STOVE DREAM CADET ANTIC ROSIN OCCUR EVERY SHADY ATLAS BLACK ROGUE BASIC SLOOP DOZEN JUMPY MAYOR KNOCK WEARY ELVES CRUSH FENCE HANDY LURCH IRONY FUNNY HYENA SEVEN MOGUL KAYAK PYGMY OFTEN MYRRH ULTRA FRAUD SQUAW WOMAN GIVEN IVORY IRATE GLEAM NINNY FLOUR SHACK HEAVY QUILT ROUTE CABIN REALM ZEBRA ACORN BLEAT FIEND EXIST CAIRN MACAW GYPSY FLOOR LEMON LUCKY SINGE KNELT TABLE INLET MOUND YODEL GAUDY WIDTH BREAD

Problem 5.

RAISE FLOSS GULCH SHEEP ASTER MOULD BATIK CUBED THEIR CENTS MAGIC WIELD JEANS GENIE PLAID

Problem 6.

Some people are always afraid to take a chance when it comes their way. Frequently they refuse emphatically to gamble a minor, paltry sum on a winning number or horse preferring an outright gain instead of doubtful or unsure profit. But others are rewarded and admit they have earned awards.

CHAPTER III. THE KEY-PHRASE CIPHER

The Key-Phrase Cipher is a glorified Aristocrat with the same as well as different plaintext equivalents for the ciphertext. The message is written out in normal word divisions, and the substitutions taken from a 26-letter phrase (a complete thought). In this manner, E-plain might be represented by itself, and also for I, R, and S in the cipher, so that frequently ciphertext words resemble such odd combinations as RFFFFW, and each F stands for a different plaintext substitute.

Take for example the following message:

DOMESTIC NOTE: AN OBSTRUCTION TO TOGETHERNESS IS STEAK THAT RUNS TO LEATHERNESS; and the enciphering alphabet is:

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

The cipher then becomes:

```
DOMESTIC NOTE: AN OBSTRUCTION TO TOGETHERNESS IS STEAK THAT RUNS
IATSMEGL HAES: AH ALMEONLEGAH EA EAOSETSOHSMM GM MESAL ETAE ONHM

TO LEATHERNESS.
EA DSAETSOGSMM.
```

This is almost like an Aristocrat, except that A-cipher can be A, O and X plain; L may be B, C, K; N is F or U; O is H, J, or R; and T is H, M, or F. Note, however, that if H plain is T in one spot, it must be T everywhere it appears. In other words, every plaintext letter has but one substitute, but one ciphertext letter may have more than one equivalent in the plain.

Supposing the following cipher is at hand, with the tip: MISTLETOE:

```
WOILLULYU OI YAU NUMO ONORN OI FLLMOOELUT LY NFSOAE SYOUM LY REMU
FLL TOIUFIUI ONUA FAT ILUUSUT NYNWOAE LOSEOT OFLW.
```

There is only one place for a 9-letter word, the tip, and that is the first word. Write in:

```
WOILLULYU   and set up the normal alphabet, showing beneath it the
mistletoe   known substitutes:
```

```
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
        U       O     L W   Y       I L
```

Then, under each ciphertext letter (lower row) show in light notation, the plaintext equivalent, until a legitimate word appears from the resulting combinations; underline them, and disregard them for the future. After step one, the message reads:

```
WOILLULYU OI YAU NUMO ONORN OI FLLMOOELUT LY NFSOAE SYOUM LY REMU
mistletoe is o e  e i i i   is  ll ii le  lo    i    oie  io    e
                                tt    t   t               t
```

```
FLL TOIUFIUI ONUA RMEINUT FAT ILUUSUT NYMWOAE LOSEOT OFLW
 ll  ise ses i e     s e      slee e   o mi   li  i  i lm
 tt                            t              t        t
```

1. YAU suggests ONE, with N-plain and A-cipher.
2. FAT, now -N- suggests AND with A-plain and F-cipher; and D-plain for T-cipher. This proves TOIUFIUI as DISEASES and FLL as ALL.
3. Two words ending in -IN(E), suggest -ING, so G is E.
4. NFSOAE, shwoing -A-ING may be tried for various words: HAVING, SAVING, TAKING, SAYING, etc. If it is HAVING, in ONORN, the form would be IHI-H, which looks well for WHICH. So, N is H, S is V, O is W, and R is C.
5. There are some odd-looking words now:

```
HE-I ATT-IIGTED VOIE- CG-E C-GSHED STEEVED HO-MING TIVGID IATM
   w  ll ww l       w                  l              lw     w l
```

None of these help much by themselves, but in the sense of the message:

MISTLETOE IS ONE .... WHICH IS .... TO HAVING .... TO .... ALL DISEASES ....

The gap between TO and ALL must be CURE, so E may also be U, and M is R. This sets up CRUSHED.

6. HER- suggests HERB, so O besides being I and W can also be B. This proves OFLW as BALM.
7. Not much time is now lost in filling out the other words of the cipher, and the resulting "keyphrase" turns out to be:

```
FORTUNEN--ALWAYSSMILESO---     which can be forced as
        ot             nus
```

Problem 7. BETWEEN
NHGE POI WEGRIP GN RIIIEIEEWHE PWWT HIPBIII IWPUOIE WIN PHWNIHE UI *WNHUEW OWE EGEI GRH BGHN "HWWOIH".

Problem 8. BUILDINGS
CTD *MNEEIEDE SDND MINNEDE EEC IICDN *MTNEECEISE EEIIDNDE ISE CTDEN EIMNDE MEEEEESAE EDEDMNICDE MR CTD ESIEEDEE.

Problem 9. INTRODUCED
UEUEVEVI OALA TVVLECEUAC TV *NLELTCY OA UAYVUA OAAV Y NELATEV TAIIAL LYCAV OTVA VAA NLETV OYI OLAUOAC ENN VAA UEYIV.

CHAPTER IV. THE TRI-DIGITAL CIPHER

The Tri-Digital Cipher uses a numerical key of ten digits as its base, which may or may not be derived from a literal key. It also uses a keyword alphabet written into a block 10x3, utilizing the full 26 letters. The final column, however, contains no letters, but nulls (blanks); as well as the cell directly to the left in the bottom of the third row. This final column of nulls is used as a word separator, thus:

```
N O V E L C R A F T (optional)
6 7 0 3 5 2 8 1 4 9 (numerical key)
S A F E B L O W I - )
N G C D H J K M P - )keyword alphabet
Q R T U V X Y Z - - )with blanks
```

Plaintext is prepared as with an Aristocrat, with word spaces. Then, each plaintext letter receives that digit for its substitution which is taken from the enciphering block (this, of course, varies with each problem); and in this case, (9) is written as a word separator, thus:

```
C H A R L E S - D I C K E N S - F I R S T - V I S I T E D -
0 5 7 7 2 3 6 9 3 4 0 8 3 6 6 9 0 4 7 6 0 9 5 4 6 4 0 3 3 9
```

In solving a cipher of this type, the opening wedge is its weakness: a double-digit cannot be the word separator digit, and so, after careful scrutiny, the "impossibles" may be eliminated. Of the remaining digits, scan the ciphertext, and by common sense, discard all but one. This is done, by watching to see where, 1, let's say, appears in the cipher; if there is a skip of fifteen letters or more between 1's, it cannot be the separator, etc.

Here is a Tri-Digital cipher to be solved with the tip: ORIGINALLY.

Write out the cipher on the worksheet and scan it for the double-digits:

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

Check these off against the series 1-0 as being impossible for a word separator: 8 6 5 2 are all doubled. That leaves 1 3 4 7 9 0. Now, re-scan the text for 1; it appears good for the separator, and is so noted, but the others must be checked as well. 3: it starts the cipher, so may be discarded. 4: the first span is 14 letters between two 4's. 7: spans are 13, 17, 15, 2, 8. 26, so 7 may be tossed out. 9: spans are 6, 15. 1, 9, 5, 11, 22 and this may be added to the impossibilities. 0: 1, 28, and this is out also, so that "1" is the word separator. Either encircle this digit or underline it, to show its separating power.

There is now, only one ten-letter word at 4-2-0-8-0-7-4-8-8-5, for the tip, so it is placed here. Set up a blank block; assign the last column to 1, the separator; and write in the various letters from the cipher with their proper digital equivalents taken from the tip, and throughout the cipher. These are not sure values but one-third values, for, remember, there are three letters for each column, although they may bear the same digit; and two in the last column.

```
- - - - - - - - - - 1
                    -
                    -
                  - -
```

From here on, this cipher works like a Key-Phrase cipher, but by using digits instead of letters. As fast as legitimate words are found, underline them.

The ciphertext now reads:

```
3 0 4 2 6 2 9 - 2 6 2 6 - 7 4 6 - 4 8 2 4 5 9 - 9 2 4 3 3 8 0 7 8
  i o r   r     r   r     n o     o   r o y       r o     g i n g
    a                       a     a     a           a     l

- 9 8 4 6 0 6 9 - 5 4 2 - 0 7 5 4 7 6 9 - 4 2 0 8 0 7 4 8 8 5 - 6
    g o   i       y o r   i n y o n       O R I G I N A L L Y
    l a             a           a

0 6 5 - 2 6 2 6 - 9 0 8 3 - 2 4 6 6 6 2 7 9 - 4 5 - 4 - 8 6 4 6 6
i   y   r   r       i g     r o       r n     o y   o   g   o
                      l       a               a     A   l   a

6 2 0 9 4 8 - 3 6 9 0 8 7 - 4 5 - 8 4 2 0 4 5 9 - 5 0 8 5 2 6 9 -
  r i   o g         i g n   o y   g o r i o         i g y r
        a l           l     a     l a     a           l

0 7 6 2 0 9 4 6 6 8 5 - 2 4 8 6 7 - 4 7 8 5 - 0 8 - 2 6 9 6 7 6 -
i n   r     o     g y   r o g   n   o n g y   i g   r       n
            a     l       a l           l       l

5 6 4 2 9 - 0 4 9 - 0 6 9 - 6 4 2 6 - 9 4 6 6 4 7 - 5 5 7 9 6 0 4
y   o r     i o     i         o         o     o n   y y       i o
    a         a               a         a     a                 a

7 - 9 6 6 7 - 4 2 2 8 0 6 3
n         n   o     g i
              a     l
```

From here out, it is a case of trial and error, assuming words, and entering these assumptions lightly in pencil to see if they prove themselves elsewhere in the cipher. As they are proven, write them under their proper digits in the block, but remember, that no more than three letters can bear the same digit. Suggestions are:

```
542;   8420459;   55796047;   86466620948;  etc.
yor    gorious       tion          rical
f      a             s
```

Recovery of the keyword block is the most complex part of this system, and it isn't easy! Given this recovered block:

```
4 1 3 8 0 5 6 7 2 9
F O N B L D K R I -
X H P U C T A Y E -
G M     S V     W -
```

The three lines have to be juggled so that a keyword results with the rest of the alphabet following. The opening wedge here looks like leaving the V-W in the third row and bringing down the X-Y from the second, with perhaps using U, too, from the second row.

Draw up a blank block and assign 9 to the separator; and underneath it write in the possibilities:

```
- - 8 5 2 4 7 - - 9
                  -
                  -
    U V W X Y z - -
    B D I F R
      T E G
```

The DEF looks good for the second row of the finished block, with TIG falling in the keyword:

```
- - 8 5 2 4 7 - - 9
      T I G       -
    B D E F       -
    U V W X Y Z - -
            R
```

H cannot follow the F in row two, for there are three letters for this column; nor can I as it is already placed. K could, in the column with Y, and so only one letter may be added here; or K could be in the same column as Z throwing J above the Y. If the latter is true, the partly recovered block would be:

```
- - 8 5 2 4 7 6 - 9
      T I G R A   -
    B D E F J K   -
    U V W X Y Z - -
```

L cannot follow K; nor can M, but N can, throwing P into the keyword. The combination TIGRAP, offers excellent possibilities to finish the keyword block. There is one wrong assumption in the BU column, but this is to be expected, in this type of recovery.

problem 10. DESTROYED

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

Problem 11. ASSUMED

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

CHAPTER V. THE 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.

It may be composed of any number of rails (or letters in depth) which may be written up or down, coming to 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 vice versa, or it may be written into the points first, and then into the successive horizontal rows. It is then taken out by the alternate process.

For decipherment, a table has been found of value, which accompanies this article. For example, here is a cipher of 51 letters. Scanning the table, using the total number of letters in the top line, and varying lengths of rails: 2 rails, there are 26 peaks; 3 rails, 13 peaks plus two extra letters (..); 4 rails, 9 peaks plus 2 extra letters; 5 rails, 7 peaks plus 2 extra letters; 6 rails, 6 peaks with no extra letters; 7 rails, 5 peaks plus 2 extra letters; 8 rails,4 peaks plus 8 extra letters; 9 rails, 4 peaks plus 2 extra letters; and 10 rails, 3 peaks plus 14 extra letters. In other words, use that digit which falls directly under the message length; and if no digits are shown, take the digit to the left and add for the extra letters the dots.

Given this cipher of 51 letters:

TAOET NMFOA TNEHM NHWKS POIDI SLFMU HSOBE ALEEW AUFHE ASNES P

There is no technical way of solving this cipher; it becomes a case of trial and error, testing various depths and various numbers of rails.

For a 3-depth, set up a pattern:

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

to complete 51 letters, and write in the ciphertext in this way:

```
T   T   O
 A E N F A
  O   M   T
```

which certainly does not look like good plaintext.

Next, knowing the diagram for three rails and 51 letters, write in the ciphertext first at the points, and then follow through in the second horizontal row, thus:

```
T   A   O
 H M N H
  E   E
```

which looks perfect and makes solution sure.

Problem 12. Four rails.
ICATA SOOGL OWDTA HTHRU REITF YUDOA LFFAN OORWC UYOER DNGTR LLBSF MLPNE OYPEE OFOYM (70)

Problem 13. Three rails.
TSNUH POTEO TFMIB NADEH NIEMW SNEHL AFOFS AWMLO AUESK HEAES P (51)

Problem 14. (?) rails.
AIRAE FLEDP RAESC NMMRI PAPHE HETNP OONEB ONECE FKIRD SIANH OREND HEHPR SAESW TRTWA C (71)

RAIL FENCE TABLE (Top line shows total length of cipher); column indicate various peaks plus extra letters of rails from 2-10.

	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43
2	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
3		2	..	3	..	4	..	5	..	6	..	7	..	8	..	9	..	10	..	11	..
4			2	..	..	3	..	..	4	..	..	5	..	..	6	..	..	7	..	..	8
5				2	..	..	..	3	..	..	..	4	..	..	..	5	..	..	..	6	..
6					2	..	..	..	..	3	..	..	..	..	4	..	..	..	..	5	..
7						2	..	..	..	..	..	3	..	..	..	..	..	4	..	..	..
8							2	..	..	..	..	..	..	3	..	..	..	..	..	..	4
9								2	..	..	..	..	..	..	..	3	..	..	..	..	..
10									2	..	..	..	..	..	..	..	..	3	..	..	..

	45	47	49	51	53	55	57	59	61	63	65	67	69	71	73	75	77	79	81	83	85
2	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43
3	12	..	13	..	14	..	15	..	16	..	17	..	18	..	19	..	20	..	21	..	22
4	..	..	9	..	..	10	..	..	11	..	..	12	..	..	13	..	..	14	..	..	15
5	..	..	7	..	..	..	8	..	..	..	9	..	..	..	10	..	..	..	11	..	..
6	..	..	..	6	..	..	..	..	7	..	..	..	..	8	..	..	..	..	9	..	..
7	..	..	5	..	..	..	..	..	6	..	..	..	..	..	7	..	..	..	..	..	8
8	..	..	..	..	..	..	5	..	..	..	..	..	..	6	..	..	..	..	..	..	7
9	..	..	4	..	..	..	..	..	..	..	5	..	..	..	..	..	..	..	6	..	..
10	..	..	..	..	..	4	..	..	..	..	..	..	..	..	5	..	..	..	..	..	..

	87	89	91	93	95	97	99	101	103	105	107	109	111	113	115	117	119
2	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
3	..	23	..	24	..	25	..	26	..	27	..	28	..	29	..	30	..
4	..	..	16	..	..	17	..	..	18	..	..	19	..	..	20	..	..
5	..	12	..	..	..	13	..	..	..	14	..	..	..	15	..	..	..
6	..	..	10	..	..	..	..	11	..	..	..	..	12	..	..	..	..
7	..	..	..	..	..	9	..	..	..	..	..	10	..	..	..	..	..
8	..	..	..	..	..	..	8	..	..	..	..	..	..	9	..	..	..
9	..	..	..	..	..	7	..	..	..	..	..	..	..	8	..	..	..
10	..	..	6	..	..	..	..	..	..	..	..	7	..	..	..	..	..

CHAPTER VI. THE ROUTE TRANSPOSITION CIPHER

A Transposition Cipher means that there is no encipherment, that is, a substitution of letters of a message; but that the actual letters are rearranged according to some plan to disrupt their normal succession.

The simplest form of the "tramp" is the Route method. A block of either a square or oblong is used, but it must be a full block; if the letters of a message do not complete the assigned block, nulls (arbitrary letters are added).

There are eight basic routes in this cipher, which may commence at any one of the four corners of the block, making 32 possible routes all told. These are, with their diagrams, using the message with a block of 36 letters: HOISTING ROPE NOW OF IRON USED TO BE OF FIBRE.

1. Horizontals
```
H O I S T I
N G R O P E
N O W O F I
R O N U S E
D T O B E O
F F I B R E
```

2. Alternate horizontals
```
H O I S T I
E P O R G N
N O W O F I
E S U N O R
D T O B E O
E R B I F F
```

3. Verticals
```
H N N R D F
O G O O T F
I R W N O I
S O O U B B
T P F S E R
I E I E O W
```

4. Alternate Verticals
```
H E N E D E
O P O S T R
I O W U O B
S R O N B I
T G F O E F
I N I R O F
```

5. Diagonals
```
H O S N P O
I T G E F U
I R N I S O
O O R E B F
W O D E F B
N T O I R E
```

6. Alternate diagonals
```
H O I N W O
I T G O F T
S R N I D O
O E R E B I
P O S E F B
N U O F R E
```

7. Clockwise
```
H O I S T I
O N U S E N
R F I B D G
I F E R T R
F O E B O O
O W O N E P
```

8. Counterclockwise
```
N O R I F E
U N I T O R
S G H S W B
E R O I O I
D O P E N F
T O B E O F
```

Once the message has been put into a block, it is written off for a cipher starting in the upper left-hand corner and proceding horizontally to the right.

Solution of a Route Transpsotion Cipher depends on the ingenuity of the solver to produce the identically sized block and the same route as the constructor. The rules governing this type of cipher are limited: if a horizontal, reversed horizontal, vertical or reversed vertical route is involved, the percentage of vowels in a row or column respectively will be approximately 20% of the total number of letters in that row or column. If any of the other routes are used, the sequence is so upset that this percentage figure fails to apply.

Take for example:

MYELP DTDAH IEDRL ILANI ANOBR MWCES WITGA REAEO AARAI SOARV ONNAN D (56)

Two blocks are drawn up, one 7x8 and the other 8x7 for such a length message, and the various routes are tried for each position in both blocks.

```
 Horizontals: 7x8                     Horizontals: 8x7
M Y E L P D T (Vowel 1)(y = 2)        M Y E L P D T D (1, 2)
D A H I E D R        3                A H I E F R L I   4
L I L A N I A        4                L A N I A N O B   4
N O B R M W C        1                R M W C E S W I   2
E S W I T G A        3                T G A R E A E O   5
R E A E O A A        6                A A R A I S O A   6
V O N N A N D        2                R V O N N A N D   2
```

It might be said here, that the vowel percentages (or actual count) of either rows or columns should be fairly parallel. A "1" in one row/column and a 6 elsewhere is much less favorable than a 3-4-4-3-4-4-3 series.

Neither of these setups looks good, so another route is tried; verticals result in another poor guess. Next, alternate verticals, and here we find:

```
M I L I T A R     and the correct route is found, with the solu-
Y L A W G O V     tion of the cipher. The distribution of vowels
E R N S A S O     in rows is: 3 2 4 3 4 3 3 3, which substanti-
. . . . . . .     ates the expect vowel occurrences.
```

Now, for some workouts, with probable words in capitals:

Problem 15. MUTILATION
CGGEP PIDEM RTOSR PNEIU EHFIE IGCRT NECSV NARVI NMODE GNEAL EIION ODALA LLNNT RTSUT LLEEC FHEEI IIDTL IUTIO NNGOI LSHNN (100)

Problem 16. DELICACY
THAAC RTYIR DTEAL EOSKL RLCAE ELOIA NETYT ICNDT HEHTL APSAG ASCAM SYNIU IEPKN LATFI TTOTU RIRAE X (81)

Problem 17. RIBBONS
MILSY LAGTM AIHIN IVELD NAREL WETAS OIAIN SINDB LNRUD EEBGO NHTLO RRINO OATNV SELSX YX (72)

Problem 18. OUTSTANDING
FMANI EMDIE HIEVE MENTC TKNJR DANET IHWRU OARON OAINC TURAL AIIIA UNEIM ELBRE UGFHA GARCH RNTTA RASTT FTAAS TIEAT SEHL (99)

A double encipherment in a Route Transposition presents a true problem. This means that the message is first written into a block by one of the routes explained, and taken out in cipher form by one of the other routes. Little can be said about procedure, except to try various routes in the apportioned blocks; however, after jotting down a few letters in the route method selected, it can be determined whether or not this is right, and so save a lot of time.

Problem 19. MILITARY
NNOAE ALMIT LVSIA RMAER AOYIR GSECW ODRNH NAINW RDEIT ABADO AEADP L (56)

Problem 20. MILLING OF COINS
CNGOP LIHEN RIOTR INTIO ELFEE FGERI NLCNV RASVT NIOOE ONAAA EMIDN
GDELL LENST NTRUI LHEIC IMCET ITDSL PUEIU NGGEI PSDNM (100)

Problem 21. DELICACY
LARSL TAKLF CAEOI LNEYO ATYNT TNLHI AEERL RTDTD HHITX ACRTG ICEEO
PAATU AISYT UCASN IEMPS REKIT A (81)

Problem 22. GIVES US THE WORD
RDMIL LINMO NSAND GEIWO LYINL RLEBN XXHOA AHBOS TAVDV TITON SEEIS
RNIRE LATUS EVIGY LA (72)

Problem 23. ACHIEVEMENT
TNAEA RMIGE EDNFA VNIME SEIDE IATIN NLRNT RHIAB UWAUI CLTRO HRRKA
ASAFI EEILH TMTTO NAAUE SFGRM OATAU JNHRT AECCT HEIT (99)

CHAPTER VII. THE COMPLETE COLUMNAR TRANSPOSITION CIPHER

A Complete Columnar Transposition Cipher uses any size block which is factorable, and the block is completely filled with the letters - the message, and/or nulls to fill out the figure.

A keyword is employed from which a numerical key is derived thus: for instance, say an 8-letter word is to be the key: QUICKSET. Set up the keyword on a piece of scratch paper, and assign "1" to that letter appearing foremost in the alphabet, in this case "C"; follow with "2" for either a repetition of this "C" or the next in order appearing letter, here "E"; continue to add numerals: 3-I, 4-K, 5-Q, 6-S, 7-T 8-U and the resulting numerical key then becomes: 5-8-3-1-4-6-2-7. This method is one way, but an arbitrary sequence may be preferred. The only requirement is that every number of the entire length must be used; there can be no duplications and no omissions.

Ciphers of this type are always written into a block by straight horizontals. The "routes" do not apply to this system.

Given, the message and the numerical key: 4-5-1-3-2: COMEA TONCE ANDBR INGYO URBROTHERX:

4	5	1	3	2
C	O	M	E	A
T	O	N	C	E
A	N	D	B	R
I	N	G	Y	O
U	R	B	R	O
T	H	E	R	X

The cipher is taken out by Column 1: M N D G B E; 2: A E R O O X; 3:E C B Y R R; 4: C T A I U T; and 5: O O N N R H. It is then divided into the customary 5-letter groups. In this case, there are 30 letters in all, which indicates to the solver that a block 5x6 or 6x5 has been used. He would set up this cipher ib both sized blocks, but writing them in vertically:

5x6

M	A	E	C	O
N	E	C	T	O
D	R	B	A	N
G	O	Y	I	N
B	O	R	U	R
E	X	R	T	H

6x5

M	E	O	Y	A	O
N	A	X	R	I	N
D	E	E	R	U	N
*G	R	C	C	T	R
B	O	B	T	O	H

Scanning both blocks to see if a phenomenon such as (*) occurs, he can soon tell which of the blocks is the better one to work with. The (*) shows that no vowels exist in the row, an impossible combination (except in shorter widths); so he aliminates the 6x5 block and concentrates on the 5x6 one. Each row of that seems to have enough vowels in each case: 1-3; 2-2; 3-1; 4-2; and 5-2, a mean average. His next step is to try to pair two columns with good digraphs. "Elcy" on page 218 gives some valuable information for transposition work but a list of the most probable digraphs is here appended:

TH	AT	OU	SA	CO	NA
HE	ST	TE	HI	BE	RO
AN	EN	OF	LE	DI	OT
IN	ND	IT	SO	LI	TT
ER	OR	HA	AS	RA	VE
RE	TO	SE	NO	MA	NS
ES	NT	ET	NE	TA	UR
ON	ED	AL	EC	CE	ME
EA	IS	RI	IO	IC	WH
TI	AR	NG	RT	LL	LY

TH is undoubtedly the most popular digraph in the English language, for THE, THIS, THERE, WITH, etc. and while LY at the end of the list is often used, there are many more which occur more often.

The most popular trigraphs are:
THE THA ION FOR HAS EDT OFT MEN AND ENT TIO NDE NCE TIS STH

The more one familiarizes himself with transposition, the more he will get to recognize first-hand, the best digraphs and trigraphs to test.

Getting back to the problem at hand: the solver notices that "X" is at the end of the cipher, and since this is a good null, chances are good that it is just that and that this column is the last one to the right. Hence, he tries to link columns 1, 3, 4 and 5, to get the best set of digraphs with 2. 1-2 give: MA NE DR GO BO EX; 3-2: EA CE BR YO RO RX; 4-2: CA TE AR IO UO TX (the UO is poor); 5-2 OA OE NR RO HX (the OE is poor). He then concentrates on suitable trigraphs: 3-1-2, 4-1-2, 5-1-2; 1-3-2, 4-3-2, 5-3-2; 1-5-2, 3-5-2; 4-5-2, until he is assured of the correct ones.

(It is an accepted fact in working with any transposition, that the first letter of a cipher is also the first letter of some column; and that the last letter of the cipher is the final letter of some column. Both of these data are helpful in solving.)

Now, for the usual workouts, with probable word heading each example:

Problem 24. DWELLING PLACE
EIEUD HIIFU ESAEH DOOBR EAMES ERTMH NCASL ETZLT HXAAS DDOWL ESRDE
RTHAI BSGEO EOTFB OWWCY ALCPI ABTAE INETD PXMOR HOBSC DPEIN SRRFO
NS (112)

Problem 25. ADMITTED
LIOOT EHSCE IYEEF CPNIN ANSYO HDCST DENTM AHIED MEUDT HFLIE EEEDC
DSSOA YNRLS SAAUY TWNFS ORAND OTGRL NEDHE EEOEE DFJHY NSEOF AVNTW
THJRP ROLTA EALDC SAAOR AVADO HTSTL RRAEA DNCAR DRYEE EEEES RMWCA
OSEEH MRDGO CEORE (180)

Problem 26. OPENING
HEAHU IENAO LNNEL IEANT LNESE HARTE BKHVT PAISF HTPNT AXTEA DUEDO
NNMEX NUDOT UEFRL OPTMC WOTHE GITIO RLMTN ISAEB DTTSP RHTAT EUNER
NOGNO ICNEG WCENM NBOOU RIEON IOORO EOIP (144)

Problem 27. ACCUSTOMED
ASEMA LLDDA TEIRN SIKOE SMUUE THNIP OCSMN SCEEE EWDDE HATTN ERLDC
MEUHO SILEE OIIDG RHHDT WAFIE HGNOV THEIS NCMPI LNISP IERSL CTREV
ASTET OLOCR GTMHN EPTMA IURES ADCOF NIGU (144)

CHAPTER VIII. THE NIHILIST TRANSPOSITION CIPHER

The Nihilist Transposition Cipher also uses a complete block, but it must be a square, <u>not an oblong</u>. And this cipher involves a double transposition, <u>after the numerical</u> key is assigned. Both rows <u>and</u> columns bear the same key. For example, an ordinary Columnar Transposition is:

```
1 2 3 4 5   with the numerical key:   4 2 5 1 3
C O M E A                             E O A C M
T O N C E                             C O E T N
T O M Y G                             Y O G T M
A R A G E                             G R E A A
T O D A Y                             A O Y T D
```

But, if the rows are also given the same numerical sequence, the text becomes:

```
  4 2 5 1 3
4 G R E A A
2 C O E T N
5 A O Y T D
1 E O A C M
3 Y O G T M
```

and the cipher is taken out by columns, starting with 1, then 2, and so on:

GCAEY ROOOO EEYAG ATTCT ANDMM

Solution, is of course, the reverse. Given a cipher of 36 letters, the block known to be 6x6:

TTEEA GSMAF ESERT OARIS SDDEN IHTRA NIHOS O and is so written into the block:

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

The procedure to try to link each column with every other one, to produce good digraphs, then, trigraphs, is vital, until finally the rows are gotten to read properly. The next step is to switch rows until continual text is achieved. In this example, scanning the block, shows that in row 3 there are E T H H, which looks well for a possible THE. These assumptions are then set up:

```
ERT   ENT
RIT   RIT
THE   THE
OTE   OOE*
ARA   ASA
RAG   ROG
```

(*) will designate discarded assumptions; in this case OOE isn't very promising. This leaves but one partial block as a working part. Again scanning the fragments: working with row 2, we try I S M in turn for column 4:

```
E R T I   E R T H   E R T N
R I T S   R I T I   R I T I
T H E S   T H E H   T H E H
O T E D   O T E T   O T E O
A R A D   A R A R   A R A S
R A G E   R A G O   R A G O
```

These are all acceptable, so the next step is to try to link one of the remaining columns in each case:

```
ERTIN ERITS ERTRN* ERTRS* ERTNN* ERTNS*
RITSI RITSM
THESH THESA
OTEDO OTEDF
ARADS ARADE
RAGEO RAGES
```

Now, add the final column for each block:

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

The third step is to try to link certain rows with certain other rows, to make continued text. Take the first block:

ERTINS OTEDOF; ERTINS ARADSE*. With the second block: ERTISN OTEDFO (r?). Then, ERTISN OTEDFO RITSMI RAGESO and the other rows may be added ahead of the ERTISN to make the entire cipher now read: THE SAHARA DESERT IS NOTED FOR ITS MIRAGES O; the final "O" being a null. The numerical sequence is: 351426.

Problem 28. (9x9) MISSION
SPFHE ICNTS AAORE RHOMG IOTND ESIHR AATOD HSAAK SWSAN NCCGA GENSW LANEO YAUOI ISSHV IEIRN RHDIH I (81)

Problem 29. FIFTEEN
VIEBO UIFOM HPBRP HWAEH RIVRT DAEVI APLIR OANSE ETEII MYEIS MNNTU ARFNS TSREV ISNGS EAAUD SEIFI ODDAC NWTAS SIATY TEHLT (100)

Problem 30. VALUABLE
ERVNA SRNNS ESUON SESLT ABNTL TEEBO BAOGT YADCI CKOAA ALCUC TIATR KTADB UELSI PFDSA ECTOR EBURR HELRE YHUBU SRYIA EOIAT (100)

Problem 31. EARLY BLACK
ESAEO IPNEI RROAH EETID ORNMA ATTMD BALRI RRRGC HOKDT EUEOE YDNEA OISDE NINTR HNOTA BONRH EFULH OGNAF RLEOB ERHNE BBTUA TTCNG NSCDA RSSRP FWONS ZTEHT EAWHT UODKO RAEAA NEGN (144)

CHAPTER IX. THE CADENUS CIPHER

The Cadenus Cipher is a transposition cipher using a completely filled block, which is always 25 rows deep, although the keyword length may not be limited; that is, the total number of letters in the cipher must be divisible by 25; nulls are added if the plaintext does not quite fill the block. An indicator is used for encipherment, consisting of a vertical column of the alphabet letters, but in reverse order, starting with A Z Y X (W-V) etc., ending with B. A keyword is selected of a convenient length and the plaintext enscribed below it for the complete block. Using the indicator, letters in the columns are marked (underlined or encircled) so that each letter of the keyword is identical with that of the placement letters of the indicator. For actual encipherment the letters of the keyword are rearranged according to their normal appearance in the alphabet, i.e., for TALK, they would become AKLT. Under this rearranged keyword, appear in each column the cipher letters, at the point of the indicator marked. For example:

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

The cipher is then taken off horizontally, instead of vertically as are all other transposition, and the result is:

AHERD IOEWE TTRDA ARTOO etc.

For decipherment: given the following cipher which is 150 letters long, divisible by 25 indicates a keyword of six; and which is so written into the block; with the suggested tip: PICKED. To solve such a cipher, write in the tip, in horizontal form. There is but one K and three C's, one of which falls in the same column with the K and may be discarded. Each of the other C's is then linked with the K to give:

```
(Cipher)                           (Assumed Columns)

                                       2 5              4 5
R S T L O A                            V O              E O
U I O R N U                            I N              I N
H E S C T E                            D T              E T
E P D G I E                            S I              D I
G T W S H R                            T H              A H
E O A E T E                            A T              A T
H S R S P O                            A P              W P
L L R I A T                            I A              N A
F T N R A E                            T A              N A
A N R S F E                            O F              E F
E V T D F P                            R F              L F
Z I V D T T                            I T              R T
A D R N K S                        P I C K E D      P I C K E D
O S S I E O                            E E              G E
E T N I E O                            H E              S E
N A F E T I                            S T              E T
E A O I N E                            I N              S N
H I S E A N                            E A              I A
D T S D E D                            P E              R E
P O I A O O                            T O              S O
G R P A L B                            O L              D L
A I F W L U                            S L              D L
N C R N Y F                            L Y              N Y
E E I N O F                            T O              I O
I H T E C I                            N C              I C
```

Both pairs of columns are acceptable, so a third column will be tried to determine which of the above is actually correct. In the remaining columns there are: one I in column 1; two in column 3; four in column 4; two in column 6, each to be tested with 2-5. The one in column 1; four in column 2, two in column 3 and two in column 6 are to be tested with 4-5.

At this point, it might be recommended that for those who prefer, a double length column may be written up into a strip, and such strips slid for the various letters selected, against established groups. Such strips will not be used in the following explanation; instead a visual or finger-tip comparison will be employed; but the results are the same:

Column 1 with 2-5: ICK REE UHE HST EIN GEA EPE HPE LTO FOL ASL ELY ZTO (n.g.) so column 1 is dropped.

Column 3 with 2-5: ICK PEE FHE RST IIN (n.g.)

ICK TEE THE OST SIN DEA WPE ATO RSL NLY RTO TNC (n.g.) so column 3 is discarded

Column 4 with 2-5: (the first one is acceptable and is written in vertically):

Now, for P, Column 1 (one; column 3 (one); column 6 (one)

With Column 1: with 4 2 5: PICK GREE ADST NDIN EDIN INEA RIPE UITO HEOL EISL GELY EDTO HANC LAVO FWIN ANDT ENSI ZETH ALAT OPAR ECIA NGTA ESOF HERF DSIT, all most acceptable, and which offer such additional tips as: GREEN, FRUITO, FLAVOR, etc.

The following finished block indicates the state of the plaintext, with the indicator at the left; also with the first letter starting with the plaintext, and the underlined letters showing where in the indicator the keyword was employed to show the transposition which made up the ciphertext:

```
I C K
R E E
S H E
D S T
D I N
N E A
I P E
I T O
E O L
I S L
E L Y
D T O
A N C
A V O
W I N
N D T
N S I
E T H
L A T
R A P
C I A
G T A
S O F
E R F
S I T
4 2 5
```

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

Using the underlined letters, to represent the head letters of the encipherment, it can readily be seen that the keyword is VIANDS.

Problem 32. AMERICAN
BKIIA SAYAO MNHSM LONDI OVOSI YSEOT MRAAR RNAEO EENUT ESDMN EOOFR
EENDP TRBBR EINOR OBTTO SATWH BEVNA GEOTR EDIIM NMNSD TUMBA HTUXN
IANET EEIRA APNIA TDCAE AFRLI UACAO SGOIH NEVOE (150)

Problem 33. NEAR THE
VITAT OSLIE GRDCA OTETA LRNBS GSLRI KRLIE PMLVH UHPTR THDEI LDETU
CEOOE NNNUD TCROO OEOSI LEOTS SENAE RFTNG SRIHC EGAAI EAROA GSZNE
MLAHF EENRI EDBLA (125)

Problem 34. RESSWITH
ETTWR TOFHO HMYNL LNSRE LNMNA WTEME OSTON CEIRO FDSOT IONBI YLDND
EHIMT ETTNM TGHLI NCEYT NAUYI LEVRD AEBPE NOEOH RECAC TCBHR RHETM
FEHAE RATOE OIMCM AFOTI UORES RTSBS ANDEI UINWR NRAME CSHTN NSEEY
EIAAW PGACN (175)

CHAPTER X. THE AUTO-TRANSPOSITION CIPHER

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 which controls the following group with a literal sequence. In some cases, anagramming is an aid, but, due to the peculiarities of this system, this factor is not always dependable.

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; the second group of plaintext with the numerical sequence and then the literal affects the third group, and so on, until the end of the cipher is reached. The final ciphertext group will appear in the lower line, as:

```
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
PT   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
CT   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
```

The complete cipher may be written either in group lengths of the usual five letters, or in their true period length. A tip is required in the former grouping, although anagramming trials may result in solution without one. Placing the tip or guessing the arrangement of a group is but a minor step. True, the plaintext following may be recovered with a fair amount of success, but what of the plaintext preceding with an unknown numerical sequence? The subject matter of any cipher is often helpful here, but anagramming with trial and error is vital.

Given, in true period and the tip: EIGHTE ENEIGH TYSEVE

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

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

```
CT  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   4 6 3 1 5 2
PT  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   (?)
```

From group 14 on, to the end, the solution is automatic. Now, look at group 12: B T D O U A, suggests D A B O U T and checks. Group 11: N E N E V T. N or E should be in the 6th position. If the N, the remaining letters anagram V E N T E N, but a better arrangement is N V E N T E, and so on.

Problem 35. REMAINING INDIANS
DTMEOHS IFIFSOH SNGOAFR NOMINTL ECUOHLM AIBVREI BTREHRY IENIAMN
IIGNADN ASOHNST GHCEAND ITSHECN IRLEEEA TRSROCE HEFSDOT IITAVCR
ISITSES (119)

Problem 36. HIEROGLYPH

EIETX HTSET ELHTT NEOUO FRRAP EAHBS TLFRS TEMMO LAIGH OREYI CPIHH
ESRHE CERPE ETNDH TEOHI UMTHT LTAIH EANAH ELIBT PPICT OCEUE TSFNE
FIEPA LBTHC (120)

CHAPTER XI. THE BAZERIES CIPHER

The Bazeries Cipher is a simple substitution cipher (some of the plaintext may stand for itself) with a transposition system based on a prearranged order; the cipher also employs three additional letters as a signal to designate the substitution plan.

A normal Polybius square is used for the plaintext, but the alphabet is written in, in verticals, not horizontals. Another Polybius square is used for the ciphertext, based on a three or four digit number converted into letters, which are written in, in horizontals. For example: 376 or THREEHUNDREDSEVENTYSIX becomes: THREUNDSVYIX in the square followed by the remaining letters of the alphabet (I-J combining as usual). A number employing a "thousand" may be used, but any number above "two thousand" or "two hundred" with a zero in second place must be avoided, for this reason: the 376 above is converted into letters bearing their positions in the normal alphabet: 3-C, 7-G, 6-F so 376 is CGF. Such a number as 408, cannot be converted into letters, for there is no "O". This signal group is inserted somewhere in the ciphertext, and untransposed.

To encipher, using 376, prepare two Polybius squares with the message, and make the proper substitutions:

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

O F T E N I N T H E S E T I M E S W ...
K H L'O A G A L X O'B O L G S O'B Y ...

Divide the ciphertext into 3, 7, 6 sections: KHL, OAGAKXO, BOLGSO. Then, reverse the order of each section: LHK, OXLAGAO, OSGLOB. This, now constitutes the ciphertext, and is so taken off. (A variation of the reversal procedure, may be to utterly disregard the numerical key, and to use sections as 3-4-5-3-4-5 or 2-6-3-5-2-6-3-5 but this sequence must be repeated all through the cipher).

To solve a Bazeries cipher, take a frequency count as is done with an Aristocrat or Patristocrat. Since this is a transposition, it may be expected to show the usual variation of occurrences, with E predominant, unless odd or manipulated plaintext has been used.

Given the following cipher to solve, without a tip, to show that this cipher may be solved without one:

VCHWI EIMVK GNYEM NLRCF TMOKR LGITR OFEMC BKGYI WKRYY CMOII NGMYC
RKMLN MMKDN MGITC GSFGR KIKMV KLYMT TOFGI FKGYE KMBCI CTIMK OCGOT
FBYPM TGIID MKOPA FEYIM CVMQM BNGNE YCRKA VA (147)

The frequency count shows:

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W
3	4	11	2	6	7	12	1	14	14	4	19	7	5	2	1	7	1	7	-	5	2

X	Y	Z
-	10	-

Set up two Polybius squares, one with the normal alphabet (PT) in-verticals, and the other one blank.

From the frequency chart is looks as though M-c is E-p, so write in the M in cell 51 of the ciphertext square, and mark all M's in the cipher as E-plain. The procedure to follow, is to build up the ciphertext square as far as possible. Unlike other ciphers where the recovery of a keyword is done at the last, with the Bazeries it is done first. With the gained knowledge threby, the resulting plaintext may then be transposed.

There are a few limitations which are helpful in building up the ciphertext square:

1. S O F T E N are the only letters occupying cell 11.
2. B C J K M P Q Z are never used in the numerical key.
3. A appears only in THOUSAND.
4. D appears only in HUNDRED, THOUSAND, but is never used if H and U are not (unless AND is used as a connective).
5. G appears only in EIGHT, EIGHTEEN, EIGHTY, and is never without I H T E.
6. X appears only in SIX, SIXTEEN, SIXTY; and S and I must also be used.
7. L appears only in ELEVEN, TWELVE; it cannot be used without V.
8. U appears only in FOUR, FOURTEEN, HUNDRED, THOUSAND.
9. V appears only in SEVEN, SEVENTEEN, SEVENTY, FIVE, ELEVEN, TWELVE.
10. F appears only in FOUR, FOURTEEN, FORTY, FIVE, FIFTY, FIFTEEN.
11. W appears only in TWO, TWENTY, TWELVE; never without T.
12. Y never appears without T.
13. The first few letters (and thus the top row of the square) of all numerals under a million, take one of the following 38 forms:

EIGHT	FIFYE	FITYW	NIEHU	SEVNT	TENHO	TWENY
ELVN	FITYH	FIVEH	NIETH	SIXHU	THIRE	TWOHU
ELVNH	FITYN	FIVET	NIETY	SIXTE	THIRY	
ELVNT	FITYO	FORTY	ONEHU	SIXTH	THREO	
FITEN	FITYS	FOURH	ONETH	SIXTY	THREU	
FITY	FITYV	FOURT	SEVNH	TENHU	TWELV	

Returning to the ciphertext square, with M in cell 11, rule 2 says that it must be followed by P Q Z; from the frequency chart, it seems plausible that P-c is K-p, having but two occurrences; and Q-c is P-p with only one; and Z with none for Z-p. So assign P to cell 52, Q to cell 53 and Z to cell 55. Both W and X are doubtful for cell 54. Now, write in the additional plaintext for P-K, Q-P.

Go back to the plaintext square. Q, being in the top row, should have one of the missing letters from the frequency chart (or one with but one occurrence). These missing letters are U X Z; Z has already been placed. From the 38 possibilities of "top row letters", none of these letters show for cell 14, so this idea is discarded. H S have only one tally. S does not appear in any top row sequence, but H does, so, as a trial insert H in cell 14 and lightly mark it so throughout the ciphertext.

Now, a check of the 38 possibilities again show: NIEHU, ONEHU, SIXHU, TENHU, TENHO and TWOHU. In five of the previous six groups

H is followed by U (and with no tallies, this looks good; O can also follow H, but with 5 tallies, the U is preferable). In N is to appear in cell 21, to complete HUNDRE, there are 7 Ns to equal Bp, which doesn't seem right, so apparently N precedes the HU and the only number that can be is ONE, or O-c A-p 7; F-c N-p 7; E-c L-p 6. Before accepting this as true, go back to the HUNDRED. When N is eliminated, D-c B-p 2 looks good; R-c G-p 7 is passable, so all these may be lightly added, to the cipher square for ONEHUDR.

It is not known that the signal is a three-letter group starting with A-1. Go through the cipher for such a combination with A-? There is only one, AFE, which converted to numerals gives 165, to indicate the numerical keyword, and the remaining letters of the alphabet follow, as: ONEHDRSIXTYVABC .....

A little ingenuity for anagramming is now necessary; in the first group the QU must come together and must be followed by a vowel. Here I, so the numerical sequence is set up: 342. But, the first letter S must be used somewhere, so 1342 will give SQUI. If this is followed by the remaining R, the sequence 13425 for group 1 is established. Try this numerical sewuence in group 2: LESRT, which is bad. Return now to 1342 and complete the cipher. (Note, here is the case where the original numerical sequence was <u>not</u> used to transpose the sections of the cipher, but a different one).

Problem 37. ROYALTY
BAEAO PMTID AMYKC LSBTS KCEMR NOQMW EQMQO PPTOS WSASE KOYSC ERLSL BKTMA SWPLL ITWTI MPOEW TRMTM WOCTW EBOBS YPIAO PSLMS UOEMP LBYLW SDMSP SBAEA LPPLH (130)

Problem 38. PERFORM
PIXCW BBUEE WUSRW AMCFA OOUBY MWEBW NWMQI MCANN VWESM NEMGG MSEBN QWQSM GSSNF MCXXU EMSWU GIWMW BBEEU XRFGX EOSWV EMMHC MERGS WYYUG FFECM GNWGS UMFDL (125)

CHAPTER XII. THE FRACTIONATED MORSE CIPHER

The Fractionated Morse Cipher uses the Morse Code for its base, and, by adding "x" between letters of the plaintext and "xx" between words, presents a fascinating problem.

The Morse Code, with the 2-unit, 3-unit and 4-unit groups is:

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

A keyword alphabet is used for encipherment and decipherment; which may be normal, or mixed; thus:

```
R O U N D T A B L E C F G H I J K M P Q S V W X Y Z
. . . . . . . . . - - - - - - - - - x x x x x x x x   (There is no
. ... - - - x x x . . . - - - x x x . . . - - - x x    xxx)
. - x . - x . - x . - x . - x . - x . - x . - x . -
```

To encipher a sample text: COME AT ONCE. The Morse Code equivalents are applied with an "x" between letters and an "xx" between words,and the sequence divided into 3-unit groups:

```
-.-'.x-'--x'-xx'.-x'-xx'---'x-.'x-.'-.x'.xx'
```

This series of dots, dashes and x's is then written in vertical form, limiting the units to three deep; and from the above enciphering alphabet, cipher letters are assigned to the various units:

```
- . - - . . - - x x - .
. x - - x - x - - - . -
- - x x x x x - . . x x
C B I I L T M H V V F L
```

In this particular case, the final group came out even for three; but often a final "x" or "xx" is necessary to complete the group (however if a message ends with an "X" in the top row, add a 2-unit symbol as a null). By the same token, a constructor may commence his cipher with one or more x's. But the resultant 3-unit groups are constant.

Decipherment is dependent on patterns. A short tip is usually ample which is placed in the ciphertext. Take for example, the following cipher with the tip: FURNITURE. The cipher is written on the worksheet (either solid or letter-spaced) with four rows below (three for the characters, and one for the plaintext).

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

(This type of cipher is usually long; and about one-half as much longer as the plaintext).

From the original Morse Code table, assign dots and dashes and x's (at the beginning and end) of the tip FURNITURE. There will be three such setups:

```
  F U R N I T U R E
  . . . . x x x . x . x
x . x - - - . - . . x x
x - . x . . . x - - .
  1 2           1 2
```

(1) This is in normal position with no x's to start the group, but with two before the word, itself. Repeated are indicated.

```
  F U R N I T U R E
  x - . x . . . x - - .
  . . . . x x x . x . x
x . x - - - . - . . x x
  1 2     3   3 1   2
```

```
F U R N I T U R E
x . x - - - . - . . x x
x - . x . . . x - - .
. . . . x x x . x . x
  1   2 3 3   2   1
```

All three above setups are required in placing any tip, since each tip appears somewhere in the middle of the cipher, but it is unknown just how it begins.

The next step is to check to see where any of these particular patterns fall in the ciphertext. On a small piece of scrap paper, write in the pattern, with the numbers falling at the same distance apart as the letters written on the worksheet. (3) looks the most promising, for there are two 3's, indicating a doubled letter in the cipher. (But the most obvious is not always right). Slide the strip along. PP is the first spot; the two 2's show up as B, but the 1's as T and E, so this is wrong. EE is the next; 2's at I Y so this is not right, either. BB is third, again 2's are F B, and wrong. EE the last, with I O as 2's; (3) is not the correct grouping.

(2): 3 indicates a spot where a letter occurs and then a skip before the same letter appears again to form this pattern, so look for these in the cipher. MGM is the first, but 1's show as B K; UWU is next, but 2's show as G B; EVE, 1's as P U; UEU, 1's as J F; MGM, 1's as M I; BGB, 1's as Z Y; IMI, 1's E E, is good; but 2's Y H, so (2) is not the setup, either.

(1) This is a slower process, since the repeats are not as easily checked, but sliding letter by letter along the cipher will reveal at:

```
T B P N E K C T I B A
1 2           1   2
```

the proper patten and the only place, too, in the cipher.

Copy down from (1) the placement in the cipher where the prop-groups go:

Now, write a tableau for the decipherment; and assign the cipher text letters to their proper places:

```
I J T B P N E K C T I B A
    . . . . x x x . x . x
  x . x - - - . - . . x x
  x - . x . . . x - - .
    f   u r n i t u r e
```

```
. . . . . . . . . - - - - - - - - - x x x x x x x x
. . . - - - x x x . . . - - - x x x . . . - - - x x
. - x . - x . - x . - x . - x . - x . - x . - x . -
  T   N   P B                       K I   E   C
```

The next step is to go through the entire cipher and mark all the T N P B K I E C with their proper dots-dashes and x-groups.

When known plaintext-ciphertext letters are found and come together, check with the Morse Code table to write in new plaintext values; e.g., whenever a (xx) occurs it might be wise to designate it by a (/), so that word-endings may be spotted.

FURNITURE now is placed at its proper spot; at TEC we get: ..-x-x-x or ? x N x T. Why the (?). Because from the Morse table, there are three sets of units of 2-length, 3-length and 4-length. Hence this ..- might be -..- or ...-; as well as ..-. A check with the table shows that ..-. is P and PNT is bad; ...- is V, so VNT is equally as bad; but ..- is U, and UNT is good. Hence an X may be placed as the final unit of the cipher, and is so marked. Notice that J has been marked ending with two xx's; and A as starting with the two xx's as explained above.

At TKBBPPNB, we get USUAL, and then a gap; but since a letter starts with a dot, this is not the end of the word, so LY may be tested. If this is true, O- cipher is -..; and X is --x. Mark them throughout the cipher and add O andX to the deciphering alphabet. At CIEEJ we have x-xx.-x-.x-- or T (end of word). Mark it accordingly. At FBBM only I-P may be noted. At BOI, p-L. At ZIB, only R. At XNEBGB, RD? At BOIMIEEJO, ?L AND At NIE, ?A?

Returning to the beginning of the cipher, after the tip FURNITURE, there is ???UNT. The -- of M makes MUNT, which doesn't look good. But with --- for O, we would get OUNT, which is much better. Now, towards the end at ZIB, we can add a T to the R already there, making TR. Back to FURNITURE - ?OUNT; check each 2-unit group from the Morse Code table, to which is best suited to fit this gap: AOUNT, MOUNT so A is xx-, and Z is -x-. Mark them.

Now the section ~~ZIB~~ becomes TRAORD, which looks like EXTRAORDINARY. Add the necessary cipher text group and the new plaintext letters to the message and to the deciphering alphabet.

The keyword alphabet now looks like: ..... Q U - - X Y Z with T in the keyword; V W may be inserted between the U and the X.

The message now reads: ....RMO..U..E..FOR FURNITURE MOUNT.NGS ...C...RE USUALLY CA..TANDT..ENC..I..EL..WIT..EXTRAORDINARY..KI L..AND DELICACY. The completed keyword is SKILEDCRATMNP or SKIL~~L~~ ED CRAFT~~S~~M~~A~~N~~S~~H~~I~~P.

Problem 39. WAS THE FIRST

MSDTP LOLVY MUXPN CTBQY YDPLC YFYZU QCBXQ LPZUV NKAWF YZGFJ TOCEN UVJCL PZUVZ UHJUJ CTBPL QJZWN UQBIY YDICB XDINC TYYDC TXIYZ CBSPG DJDXU BWYIC JJUJT QLJGT SPGVN VFTXP CYYVC GINUQ FBQYF LPYFY JBQYD YZZTP

Problem 40. THE MOST FAMOUS

BQGJJ BSDRY CCURE YTGIS BHKSX VHUEH PESMR HEKZS EZFKY SEYZZ IEYZZ IJYKQ LZEMI XUMRY IOJPE SMQEH LSSIN ZXEHH YYCYS FBQJD WGVGH FKSQB EMOEI GXQKY IIHGW PWJBI NLSBC G

Problem 41. AUSTRALIA

HPVAN AUQWR PDGQT AXVDC NSBBD SZJOT AOPIQ BKSPQ ZJEXL IJDCM OYJLI JUVOP QVSPT AUIJJ IVURL XWMTK LRWBD GPMIV XLBZK KSRLY FREPD GQINS QUUDV DFYMI PUDLZ WNAMQ BMEXX LBPQT JAKPT

CHAPTER XIII. THE MORBIT AND BIT-MORE CIPHERS

The Morbit Cipher, in its original introduction was a simple substitution cipher based on the Morse code, plus a designation by numbers of nine different symbols. These numbers are arranged in order (perhaps a keyword is used):

1	2	3	4	5	6	7	8	9
.	.	.	-	-	-	x	x	x
.	-	x	.	-	x	.	-	x

To encipher, plaintext is given its true Morse code values, with an "x" between letters and an "xx" between words; the resulting series is then broken up into two-unit groups and the proper numbers assigned to each group. Using the above tableau:

```
O      N     C        E     U        P        O        N
- -'- x'- .'x -'. -'. x'. x'x .'. -'x .'- -'. x'- -'- x'- .'x x'
 5  6  4  8  2  3  3  7  2  7  5  3  5  6  4  9
```

With a given tip, or even anticipating common words, as AND, THE, FROM, FOR etc., this phase of the Morbit makes comparatively simple solving, so a variation has been introduced to offer solvers a little more of a workout; it is called the Bit-More cipher. Instead of using just nine letters of the alphabet for the assigned numbers, the entire alphabet is used with a keyword followed by the remaining letters as:

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

The first step is followed as with the Morbit, but with this exception: <u>any</u> of the three vertical letters may be given to the same two-part unit. This breaks up the ordinary frequency and the solver has to determine what the keyword is. But this resulting cipher is literal, not numerical.

Take for example, the following cipher, a Bit-Mor, with the tip: FROM TENDRILS OF. Set this tip up in the positions required (as in Fractionated Morse), but this time, there will beonly two such set-ups as only two-part units are involved:

```
WANIM CQIFE PASDZ OPHJB PGFAP ZRXUM ESVJE UXXNY BJFBF PXVSO SHWGA
IWQAY BCLEW LWOTC KYCUK UTRZD LITFQ FBFNX GSNPT RKEPI ADCZS SNFLR
XUMAP ATJAK GSOIG YCGXF QCXUL HKOKN MOGIG PBTPJ NSXJQ ZNMJB PFFAF
```

The tip will be found at CUKUTRZD.....EPI. Write in the tip, keeping to the method outlined for the encipherment with the "x" between letters and the "xx" between words; and assign the ciphertext letters to their respective positions in the keyword block, which will look like:

```
. . . - - - x x x
. - x . - x . - x
-----------------
C B F U R D K T Y
N E S Q     I Z
    P G     X L
```

Now, go through the entire cipher and mark all ciphertext letters their plaintext values; if any complete extra plaintext results in adjacent positions, write them in. Combining the procedure of the Fractionated Morse and similar systems, the rest of the plaintext may be recovered as well as the keyword.

Problem 42. LOYALTY

```
GXQTA ZPRIU KJHWY FEFCM BKVIH PYUEA RLNSO COLRA TIDHI VJUII DGKHE
YBTTA OPEQR PIRWK OGYQR FROWM FNYHY NKNEN ZWDCS UPLVZ IAEAR WLRNM
CXNPS HNDCZ BXQKF TXUVS QGRBY ADKEP PYMUF LGRHR PKJCT EYCFL WSXHI
AOJNW RBTAX BNDEE NEAE
```

Problem 43. MATERIALS

```
JQYKB EPAKZ COUEF ISYET YXRQF JHRXQ AFGKY VONDC XALYZ JMWFR YAGMS
QFHXL PPUNF ZQMRI JGYAE ZOXBN KAZPT KGIAZ OOSOE AOVPQ KGWOV HDAAY
NUXOJ ERFQI DGPTX GLECI CNXKL EBSOP UFVEY JXRYB KAIE
```

CHAPTER XIV. THE GRAND PRE CIPHER

The Grand Pre Cipher is a numerical substitution cipher, each letter of the plaintext having one or more substituted values for its encipherment. A square 8x8, numbered from 1-8 at both top and left, containing 8-letter words is used. In.the orâginal introduction of this cipher, every letter of the alphabet was used in the words of the square; but this phase offered two faults: 1. Plaintext was inapt to contain J, Q. X and Z, so the recovery of the full square was hampered. 2. There are only a limited number of 8-letter words containing infrequent letters so repetitions were often found, so the square recovery became less fascinating.

Today, the square may be composed to any 8-letter words, which are left to the choice of the constructor. This permits more alternate substitutions for the plaintext letters. The only rule to be held is that in each square a keyword must occupy the first column. The old and new-style squares are appended, so that the reader may judge for himself the advisability of the change:

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

It may readily be seen that in the "old" style E has but two equivalents but in the "new" style it has seven. Hence, the upsetting of frequency expectancy is more pronounced.

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

To encipher, write the plaintext, with ample space between letters. Then, by using the numbers: left-to-top in the block, assign each letter its proper and various substitution.

Using the "old style" block and an example:

```
E  V  E  R  Y  O  N  E  E  V  E  R  Y  W  H  E  R  E
61-45-82-71-14-54-38-61-82-62-61-71-75-73-48-82-71-61
```

Note the repetitions.

Using the "new style block":

```
E  V  E  R  Y  O  N  E  E  V  E  R  Y  W  H  E  R  E
14-32-22-34-28-31-52-33-48-32-56-26-28-55-24-72-58-81
```

Note that the E has differences.

Now, for an example for solution: tip: NEITHER A MONKEY NOR

```
24 71 36 48 77 32 63 14 21 76 25 61 37 58 77 46 31 44 85 68 27 41
53 35 41 13 52 16 87 62 24 51 14 41 71 34 72 66 51 14 27 61 37 14
22 68 42 87 83 84 75 17 82 18 63 27 82 17 43 71 33 56 24 23 35 41
37 57 63 51 28 13 88 75 23 63 35 42 33 73 16 27 67 25 85 78 65 14
76 24 51 63 41 27 12 67
```

(using the "old style block"

Repeated letters indentical with the repeated numbers, place a tip, but, doe to the multiple substitution, perhaps only one set of repeated letters may "click". Hence, trial placements must be tested, and the resulting letters placed in their correct positions in a blank square which has been drawn up.

It will be found that the tip, here, places at 63-27-82-17-43-71-33-56-24-23-35-41-37-57-63-51-28; so write in the letters known to their respective squares in the decipherment block:

	1	2	3	4	5	6	7	8
1		Y					T	
2			O	M			E	R
3			R		N		E	
4	K		H					
5	O					A	Y	
6			N					
7	E							
8		I						

Now, go through the ciphertext and mark all letters (numerals) taken from this skeleton block. Scanning the plaintext after this operation, will show fragments: -NK-; -MO-KE-; -TI-; -ONN-; -MONKE-. Of the lot, the last group seems to have the best information to work with. The ending of the cipher must be either: MONKEYS or MONKEYX. Add the Y to the block. If 67 is X, then there is another X fourteen letters from the end, which seems improbable, so 67 is S. Now, take a look at -MO-KE-. Does an N fit between the O and K? Try it. If N is 14, then since there are three other 14's, additional fragments appear: -ONE-, -NN-, -EN-, all of which look good.

The procedure now, is to guess either one (or more) of the 8-letter words in the block, or more plaintext, working one against the other until a complete solution is reached. Remember, the left-hand column contains a keyword, too.

As a suggestion, what is word 4?

Also remember that every letter of the alphabet must appear in this type of block. So, why not try to place QU? 81 may be S, R, or D. Try each one in turn to see if suitable plaintext restuls. There is no 81, so this is no help. 18 may be S, H, or E, the latter preferable; or even, perhaps A or I. If 18 is S, just before the tip, there is: -TIS-. 58 must surely be S, also, and suggests the word OJIBWAYS. This fifth word of the block adds something to the plaintext. Finish the solution and try the following which will employ the "new style" block without J, Q, X, or Z.

Problem 44. IDENTIFYING SYM-
47 77 32 58 15 55 27 84 33 45 53 11 17 41 12 74 85 42 55 28 61 31
15 11 28 56 22 44 65 11 61 45 21 41 57 63 68 65 72 38 56 82 31 67
18 55 36 18 87 25 46 23 37 26 17 63 82 16 28 13 12 71 57 43 35 85
32 87 57 11 21 62 41 42 77 83 16 86 77 68 27 28 84 11 77 64 36 42
53 26 68 41 51 61 35 52 85 34 12 48 32 45 57 18 55 43 21 85 42 72
62 46 27 61 11 87

Problem 45. WHICH KNOWS NO
22 36 78 82 43 75 78 54 13 41 78 45 33 48 15 45 55 61 51 23 57 22
15 66 45 72 43 15 64 63 52 42 82 68 14 43 84 32 22 26 44 56 43 44
47 78 25 74 68 78 38 68 54 83 33 25 78 18 64 45 43 18 87 73 48 28
41 16 53 15 57 27 15 45 26 44 15 78 63 18 84 76 81 17 77 55 45 57
18 42 48 86 38 26

CHAPTER XV. THE RAG BABY CIPHER

The Rag Baby Cipher divides its words into normal lengths, but uses an alphabet of 24 cells which may be setup in an oblong 6x4 and in each case, combining I-J and W-X. The encipherment is progressive, that is, each word starts one advanced position from the preceding one, for the substitutions.

This keyword block is used for both solving the cipher and recovering the keyword; but for the sake of simplicity in both enciphering and deciphering, a double-length strip showing the entire keyword alphabet for enciphering and merely numbers for the deciphering is far easier to manipulate. Prepare such a strip of numbers: 24 23 22 .... 1 0 1 2 3 4 ...... 22 23 24. In enciphering write the first letter of the keyword under the "O" and continue for the rest of the alphabet. Then, by using those numbers to the right, encipher letter by letter.

For example, with this keyword and sample cipher:

```
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
G R O S B E A K C D F  H  I  L  M  N  P  Q  T  U  V  W  Y  Z  G

      T H I S   C I P H E R   I S   U N I Q U E
      1 2 3 4   2 3 4 5 6 7   3 4   4 5 6 7 8 9     etc.
```

To encipher T, take that letter which appears 1 to the right; assuming that T, itself is "O". For H, take the second letter to the right or 2. This fragment then, becomes:

```
T H I S   C I P H E R   I S   U N I Q U E
1 2 3 4   2 3 4 5 6 7   3 4   4 5 6 7 8 9
U L N K   F N V P H C   N K   Z V T A S M    etc. The strip may be
```

slid to account for a starting number of 20, let's say, remembering that 24 is the same as zero.

In deciphering, place the O at the ciphertext letter and pick up letters to the left for the plaintext.

A problem to solve, with the tip: DISCARDED

```
 Z L C U   V P S D   P Z   T V H B Z T N  V    N H B F
 1 2 3 4   2 3 4 5   3 4   4 5 6 7 8 9 10 11   5 6 7 8

L B P D F  M  R    F S C N  Q    B W N    D E  F  Q  U
6 7 8 9 10 11 12   7 8 9 10 11   8 9 10   9 10 11 12 13

K  F  S  P  E  O  F    T  N  D  U    U  S  U  R
10 11 12 13 14 15 16   11 12 13 14   12 13 14 15

 Z  A  D  O  V  O  K  Y  R     Q  D     H  P  T  Q  B  F  M  P  Q
 13 14 15 16 17 18 19 20 21    14 15    15 16 17 18 19 20 21 22 23

 N  E  O  O  T  R  P    U  W  V    O  O  T  E  F    E  M  W  O
 16 17 18 19 20 21 22   17 18 19   18 19 20 21 22   19 20 21 22

 R  F  C  Z  Y    V  Z    Z  L  E    G  U  P G D D L   F  L H M E
 20 21 22 23 24   21 22   22 23 24   23 24 1 2 3 4 5   24 1 2 3 4

 M E D I T   P A U P
 1 2 3 4 5   2 3 4 5
```

Be sure to remember that whenever 24 appears, it is plaintext, identical with the ciphertext or zero.

1. Go through the cipher and every time a 24 appears, mark down the letter itself: RFXZY, ZLE, GUPGDDL, FLHME.
   y e u f
2. The above phenomenon is one weakness of this type of cipher. Another is, that every time a letter shows the same digit below it, it represents the same plaintext letter.
3. By using the tip DISCARDED which, while it can be expected to place in one of the two 9-letter words, it places at the first; ZADOVOKYR. Set up a table of pairs, with the plaintext first, the digit, and the ciphertext last, as:

D-13-Z
I-14-A
S-15-D
C-16-O
A-17-V
R-18-O
D-19-K
E-20-Y
D-21-R

4. Since D shows up in four pairs, it seems the logical place to start for recovering the keyword alphabet. Put the strip of digits so that Ø is under the D. Now, D-13-Z means that D-plain is 13 spaces away from Z-cipher (to the right). So put Z at the 13th mark. D-19-K, or K at the 19th mark. Check these pairs off. Then, S-15-D, means that S is at the 15th mark to the left. Check off this pair. D has been taken care of. But, there is an R-18-O. Slide the strip so that Ø is under the R and (due to the double alphabet length which has been adopted) place O at the 18th spot to the right of R. With C-16-O, slide the strip until the Ø is under the O and mark the C to the left at the 16th place. This takes care of all the letters that may be placed now.

5. Slide the strip back to D, with the Ø (zero) under it. It will be found that K appears at 5 spaces to the left, as plaintext. Examine the cipher to see if D-cipher has a 5 beneath it. There is one in the second word, so D-5 is K. Slide the strip under each of the other letters in the alphabet now recovered, to see if any more plaintext letters can be written in (with the double alphabet; it is wise to repeat these written-in letters so that they appear in duplicate). D-1 c; D-3 r; D-5 k; D-9 o; D-15 s. With Ø under C: C-2 r; C-4 k; C-8 o, etc. Write in any plaintext letters which agree with the digit needed.

6. There are a few plaintext letters in words, but nothing significant. Look at ALE: Ø-E, which could be THE, ONE, ARE, etc.

7. Look at word 2, ending in K. It must be preceded by C, L, R or N. That means that C-4 s; L-4 s; R-4 s or N-4 s should appear in the alphabet. But C and R show somewhere else, so either L or N belong before the K. However, if from (6) or ONE, N-23 l, meaning that in the alphabet proper LN come together, this looks a bit promising, with M in the keyword. Assume L-4 s, and N-23 l.

8. With each new letter being added to the keyword alphabet, place the digital strip with the Ø at that letter, to see if any new plaintext develops.

9. Back to the cipher: with ONE followed by -U--R-D, and an E being required between the R and D, the word HUNDRED suggests

itself. E can then be placed in the alphabet, and more plain-text letters added.

10. By working forward and backward, first with the fragmentary keyword alphabet to the left for plaintext; and from the suggestive plaintext words, with their letters to the right for ciphertext, the entire alphabet may be recovered.

11. In the present case, it is found to be TOYMAKES' and the cipher: "When silk is unrolled ..... etc."

Problem 46. TATTERED at word 7
GDL VMLOQU TF AQHSQ HM BHUVUI RIPLVISN IRH SMSWSN GYKSTZ
HQDXSRSHLH ICHES TYQ AMFAPOKYK LF LSHB YF BI QVHN WFNG. *FSGN
*VIEAVPV CADYE *EQIBQPT LDHS.

Problem 47. WARRIORS at word 9
*CSWYFWV *EYIE KDZE YICNP IOYUGTY IU SNT *NKWTQR BNNPVNUO IUPW
VNTWB QI *CNCIRHB *MBKO *OVOHU WEA DVL *LHWPU GKRRIS QAHI SAMARAO
ITBFWDN RNF WHWTN VT LT FFWDDGLT EGNNFANAUMAK EDOPG YDSAQYVK USG
HDTO

Problem 48. ROMANCES (Not a standard write-in of keyword)
DSA RDRPFMA DN *BQPLYL CBM *CZWRIN KNBWP WY *WCUYHR LNRNUD
NLTHHHHV EVKR DHLWBK VOYHR QO MHDC HLATWNBNNNF WH DBZNRADTOB
EB HRB COIII NNF *ABHMKPP TNLB

CHAPTER XVI. THE INCOMPLETE COLUMNAR TRANSPOSITION CIPHER

With the Incomplete Columnar Transposition Cipher, a block is employed, but an incomplete block; that is, the last line is shorter than the width of the block, and no nulls are added to fill the area. For example, a cipher of 118 letters may mean that the block is seven letters wide for 16 rows plus a 17th row of only six letters; or a block of nine letters wide for 13 rows and a 14th row of a single letter. In other words, in attacking a cipher of this type, the solver has no way of knowing the width of the block, but must estimate it and work according to his assumptions. This makes the Incomplete Columnar Transposition a rather difficult problem. However, is it a single transposition and not a double one as is the Nihilist Transposition, which simplifies solution to some extent.

An example of this system, with a simple numerical key:

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

3	7	4	1	6	2	5
E	R	O	S	I	G	N
S	A	W	A	Y	H	I
S	S	O	U	L	-	-

Rearranged for taking out the cipher:

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

1	2	3	4	5	6	7
S	G	E	O	N	I	R
A	H	S	W	I	Y	A
U	-	S	O	-	L	S

The cipher, when taken out by column 1, 2, 3 and so on, is:

HEHLA MERHT SAUSE EGTOI TSEGH etc.

Given a new cipher:

SEOTE AHSNS OAASA IMMTN TOGWK SMMHR SNHSE DHTTT FYMFO EAASA ASNIO
INCMI HDTFA ANREE AWNIN TEURN WERUI CSEMA EPEUO RTCAI CILIC IONLL
(110)

Solution of this type of cipher has various methods depending on the individual solver. "Elcy" suggests that the length of an unknown cipher be factored for various possible blocks, in this case: 6 width, 18 rows plus 2; 7 width, 15 rows plus 6; 8 width, 13 rows plus 6; 9 width 12 rows plus 2; 10 width and 11 width are even, so may be discarded; 12 width, 9 rows plus 2; and so on. Strips are then prepared from the cipher text for each assumed block, and the letters from this ciphertext are written onto each strip, allowing for an overlap of perhaps five letters (or six) which are duplicated at the ends of all strips except the last one with the tops of all other strips but the first one. These strips are laid beside one another and slid, in order to obtain good digraphs, trigraphs, and tetragraphs (four-letters) to make good plaintext.

The second method is to write the cipher out horizontally in as many lines as are necessary to complete the ciphertext, and then visually check the digraphs, trigraphs and tetragraphs from one spot to another arriving at the same destination as in the first method.

The third method, which the author prefers, is a combination of the two aforementioned; that is, the ciphertext is written into an arbitrary block (in this case of 110 letters, a 10x11) in a continual sequence, from left to right by columns, but in a horizontal manner to start with. For example, with the above problem:

1	2	3	4	5	6	7	8	9	0
S	A	G	S	O	I	N	U	M	I
E	A	W	E	E	N	R	R	A	C
O	S	K	D	A	C	E	N	E	I
T	A	S	H	A	M	E	W	P	L
E	I	M	T	S	I	A	E	E	I
A	M	M	T	A	H	W	R	U	C
H	M	H	T	A	D	N	U	O	I
S	T	R	F	S	T	I	I	R	O
N	N	S	Y	N	F	N	C	T	N
S	T	N	M	I	A	T	S	C	L
O	O	H	F	O	A	E	E	A	L

As in all transpositions, one fact may be relied upon: the first letters of a cipher appears somewhere in the top line of the plaintext; and the last letter of the cipher appears somewhere in the final line of the plaintext. When no tips are given, these two points may be used as entrance points.

However, valuable tips are given in "The Cryptogram", and if this cipher were to appear there, the chances are that SUCH PAGAN might be the tip.

Since this is the case, on a work sheet write S U C H P A G A N, leaving plenty of space above and below this row. Scan the ciphertext to see if any of these letters appear but once (or twice). Both G and P appear but once, so above each, write those letters which are before and after them in the ciphertext block above, in a column, for say, about eight letters, making the column 17 letters long; and lightly draw a lone through the letters used, (lightly, because some of them at either the top or the bottom may be later found to belong to some other column).

```
        U A
        I I
        C M
        S M
        E T
        M N
        A T
        E O
S U C H P A G A N
        E W
        U K
        O S
        R M
        T M
        C H
        A R
        I S
```

Now, check back to the cipher for an A needed between the P and the G and see how the letters on either side of the A in the cipher look as trigraphs for the section thus started: Column 1: AHSNS...PAG, EHW*; 2 AASAA...PAG EIW*; ASAIM ... PAG ESW UAK*; ASAAS...PAG EIW*. Column 5: AASAA...PAG EAW*; ASAAS...PAG ESW UAK*; AASNI...PAG EAW*; ASNIO...PAG ESW UNK OIS ROM; below PAG EAO* (but perhaps this is an encipherment error, since the other trigraphs seem good), AST MAN EAT SEM COM IFI UMA. Now, perhaps the EAO is good; it is worth an acceptance until we are definitely proven wrong. Write in this column, as is.

Scan the trigraphs for clues: UNK, must be preceded by R (?) or by N (?). Loos at the cipher text left intact (not marked out) for H - R for RUNK, or A - N for UNKN. There is no HR, but there is an AN in columns 5-6. Of the two, the 6 position seems better, so write that one in. The top row UMAN suggests HUMAN, the third row COMM (a) or COMM (on), COMM (end) etc. Try each one until the proper combination of additional plaintext letters is assured, crossing out lightly letters used.

With 7 columns listed, the worksheet now loks like:

```
      H U M A N S A
      R I F I C E W
      S C O M M O N
      N S E M I T I
      H E A T H E N
      S M A N D A T
      E A S T T H E
      D E A O F S U
S U C H P A G A N R
      T E S W A S N
      T U N K N O W
      F R O M E A R
      Y T I M E S'a
      m o a h a c i
      f a i r
      o i m s
```

It will be then noticed that the SU occurs above the placed tip, so this is an overlap, making the correct width of the block 8 and 13 deep plus 6.

Of course, when starting to solve, one never knows if the tip overlaps or not. If it is more than six letters it is worth a trial to assume this is the case; for IF it does, a lot of time may be saved, as:

6	7	8
SUCHPA	SUCHPAG	SUCHPAGA
GAN	AN	N

and such cipher digraphs as 6: SG, UA, CN; 7: SA, UN; and 8: SN may be tested to see if they appear normally in the ciphertext. When they do, solution has a shortcut.

Problem 49. MAKINGHATCHET
GUIAE FYTEB NRETS EEIIH RUEOD SATMT SYSHD FEERA LDDCU OBOTI ACEFN SRONO TAFAS ENMEI LOSAH ERMHA LIRRI OMEEE DNNEM RDCYH RAENB EGAOR EHPEA NSRSG KTOCR DOGEN IGNOR CSRYD OTFNM O (146)

Problem 50. ERPARTADORN
EEORI IEHEI ERMBS OAONA ECOEX AETID NTEEI EHOLC EEHRW IIOMD KLTML ELLTA DODEA OESED SNTLW POEYR RSFOT ICFWI NUATE GHNAS TSNAI FOHPE RAMNM RFIAN PASTR NBEOR HDRHN AOIBD PDHRO ET (147)

Problem 51. DESIRABLE

FODCM ITUNT RESNS AEESR RSSEN LAOOS NUDLO SRITS TIKNF TSSTT ECREA
EIATS AEMNT ONUOO IOSEE YMDLE AEALO OTMIT CSGSA MSKSA IDBEE MIASC
LUUPN IHEIS SUHCI ORABT THFAS VDSTB RHG (143)

CHAPTER XVII. THE AMSCO CIPHER

The Amsco Cipher is another type using an incomplete transposition block. Besides that, its column-letters are not limited to a column of single letters, but rather alternating: single, double, single, double throughout the plaintext length. A numerical key is employed. For example:

```
3  1  4  2  5       2  4  6  1  5  3
TH E  WE A  RI      T  HE W  EA R  IN
N  GO F  DE C       GO F  DE C  OR A
OR A  TI V  EM      T  IV E  ME D  AL
E  DA L  SW A       SW A  SC O  MM O
SC O  MM O  NI      N  IN E  NG L  AN
N  EN G  LA N       DD U  RI N  GT H
DD U  RI N  GT      E  RE I  GN O  FH
H  ER E  IG N       EN R  YT H  EE I
OF H  EN R  YT      G  HT H  12 12 12
H  EE I  GH T              (B)
HX    15 15         13 14 13
17    (A)
```

Note that in (A) the alternating pattern of 2-1-2-1 follows from one end of one line to the next line; but that in (B) it is possible to have two 1's or two 2's in the continuation of one line to the next. These variations are peculiarities of this cipher. The cipher text is taken out by columns starting with 1, then 2, 3, and so on.

Solution is done similarly to the Incomplete Columnar Transposition; strips are slid (if this method is preferred) or the cipher is left in a horizontal row (if) this method is used. Writing this cipher into an arbitrary block, however, is so uncertain that it will not be considered at all.

Given, a cipher and a tip - since tips are vital for solution, until the system is more familiar: PRECIOUS.

```
    5    10    15    20    25    30    35    40    45    50    55
NTTIN OENOE NTUSD PRTTE RIUUN TOLIV EDCIS ORDEW LLTIL STSII CRTOL
   60    65    70    75    80    85    90    95   100   105   110
NKOOU XHKIG NALHE ENEOL ESERY GSPDL SRWIO ANSWI AAENS LEIFS RHPSA
  115
FIHRR
```

First, the tip PRECIOUS is divided into the pattern 1-2-1-2 in the alternative ways: -P RE C IO U S- and PR E CI O US; and the ciphertext is scanned to see if either of the digraphs appear, and where. RE, no; IO at 89. PR 16, CI 33, US 13. The second division seems better with three hits and will be assumed to be correct. Now, as before with the tip in the Incomplete Columnar Transposition, write in the tip as herewith divided and then write in those letters which appear on either side of the known pairs: PR CI and US, to the extent of some eight or none letters, thus:

	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

Lightly cross out letters used, as you go along. (The existence of PR here, shows that the PR of PRECIOUS - appearing but once in the cipher - can not be used here; so it is then assumed that the tip is found on two lines instead of just one).

Now, return to the cipher and test the O's all through, using the alternate pattern of 1-2-1-2 wherever an O occurs; and see if something plausible may be added below that O given in the tip; skip all O's which have been lightly crossed out: O-54: O LN K OO U XH gives CIOUS SLN*; O-58: O OU X HK gives CIOUS SOUD 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 write in the new column, adding letters above and below the tip; and crossing out more letters.

Note, that toward the bottom of the columns thus linked, after the plaintext EWATE, the rows seem to go bad, which indicates that that EWATE is the bottom row of the block. Now, return to the letters crossed out, and, knowing that EWATE is the last row, now erase any letters crossed out which pass this point. Also, notice that the arbitrary length of the columns is 14, and that ahead of the IN O EN, there are but three letters remaining. This shows that this column should be extended up to the first letter of the cipher, for (remember that "the first letter of the cipher of this type will be found somewhere in the top row of the plaintext")

The recovered plaintext thus far, now suggests: (G)OLDEN; (SIL) VERN; DWIT(H) in the two places and EWATE(R).

By testing each spot for these assumed additional letters from those remaining in the cipher, the block may be recovered as:

	O	RI	E	NT	A	LL
	UX	U	RY	T	EN	T
	H	UN	G	IN	S	IL
	KI	T	SP	O	LE	S
	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	--

Now, notice that PR which had been originally assumed to be a digraph was not that at all, but was broken up as -P R in the line above.

Problem 52. PERSONS

CALTV ETHEM ECUTI GONLO PRINI BSETO ONENI RSVEI OREAP RIAVY LESEH RLASS FNYAI OTNSF HTROT LPORE NEDOE ETLIN YORTS TMIOE NGWEN RIO (108)

Problem 53. OWING

ENAUT AANNG EOOIS GHMME IPIHE DDSEH FIRRD TBEOL YTWID FRTLD NNSEU THNDD GTRMC LANEO NNNYD ORORU DODEY IEWOL RASNT EPODI NRBUG RIAGA STOYI HINDA VOFUE REUTH MILGC AY (137)

Problem 54. STATES

HSTNP RSUSR RMNIN LTELO RICIT HETIL ESAST OOFDO TODOG MOETE AHIMA MENUL SBTAI RETIT IGETE NULTD YOYON OOPIS ADSUN STUBA LACTM DB (107)

CHAPTER XVIII. THE MYSZKOWSKY CIPHER

The Myszkowsky Cipher is an incomplete transposition cipher with variations. A keyword is used, one in which there are one or more repeated letters, and so the resulting cipher has an erratic method of taking out. The following examples show first, the minimum complexity, and second, the maximum. The plaintext is identical, but different keywords have been used to show the possibilities of this system. From the keyword FICTION, assign 1 to that letter foremost in the alphabet, C; 2 to the next-in-order letter, F; then there being two I's, assign 3 to both of them; 4 to N; 5 to O and 6 to T. With the keyword PAPILLA, similar designations are shown, with repeated letters treated in like manner:

```
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 - - -
```

The first cipher is:

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

The second cipher is:

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

Compare these two ciphers, to see how the normal sequence by columns has been disrupted.

Numbers representing letters which do not repeat are taken out in the usual way, as with the Incomplete Transposition; and by this token, these columns are handled identically with the foregoing cipher; but those letters that do have repeats are taken out first with the first letter, then with its mate; then back to the first one, and again to its mate, and so on. In the ciphertext, such relation gives what is called a 2-decimation, that is, every other letters must be regarded as in a normal sequence, not every letter. If it were a 3-decimation (with three columns bearing the same digit), every third letter would have to be considered.

Ample tips are always given in "The Cryptogram" for solvers: the first tip in capitals, or quotation marks; the second tip in Caesar - so that if the solver does not want to use the latter tip, he needn't. Ofttimes the period, too, is given.

```
    5    10    15    20    25    30    35    40    45    50    55
UEIES OCOSH IEIDF AIPLH MLCAU SSRTT OTMUE NRAAN NROSA XSREF KPNEL
   60    65    70    75    80    85    90    95   100   105   110
OINEN OCMII FOAGZ NADEM CLPRO SITOM RMCYS NIIAA AKEFT OSINL ATTSQ
  115   120   125   130   135   140   145   150   155   160
ESHON YLETD RTNEF TUESE BEMGA AICRT PONHG OEPAA HOARD RRAFR NET
```

Given this sample cipher for solution, with a period of 6 and the tip: ERMEDICAL. Since the period is known, the size of the block may be drawn up as 6: 27 deep plus 1.

Knowing that it is a 6-period, the tip is then set up as:
This means that the sequences EC RA and ML appear in that order (with or without decimation) in the cipher and such columns may be placed. Scan the text for EC; there is none! But the tip said there was! What's amiss? Decimation! Now, rescan the ciphertext for an E - C or 2-decimation; or E--C for 3-decimation. At 74, there is E-C; at 4 and 59 an E--C. Jot down both points for future reference. Take RA: 37, 157. ML: 21, the only one. Now, as was done with the incomplete transposition, write the tip out in a horizontal row, and for the ML pair, extend the letters before and after it in a column for some eight or nine letters (or enough to fill in the block drawn up); and lightly mark out these used letters. It will be noted that the column with nine preceding letters results in only a few extra letters until the beginning of the cipher. Again, recall, "that the first letter of a cipher in transposition appears somewhere in the top row of the plaintext", so continue upward to include this beginning letter. Return to the two placements of RA: 37, 157. Check each one with the established column to see which gives the better plaintext digraphs; 37: RM AL AR NS NT RM OM SY AN below and ND EN UG MA TI OM TO TE RI above; 157: AM FL RR NS ET TM -M -Y -N (end of cipher) below and RD DN RG AA* above. The conflicting AA indicates that the first grouping is preferred, so write it in. (It might be said here, that sometimes such an occurrence as AA or some similar "odd" digraph might be correct in the plaintext, so, until any assumption is disproven, hang onto it.) Again, cross out letters used. Now, try the EC combination.

```
R E M E D I
C A L
```

Since placement 4 has now been crossed out for ML, placement 74 and 59 will be tested. 74 with a 2-decimation seems to give logical trigraphs with the already established columns:

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

These trigraphs offer many ideas: NTE(R); (I)NTO; COM(M); ITI(ION); (O)FMA; OUG(HT); (A)ZEN - (I)ZEN; PAR(T), etc.

If nothing feasible develops, go back to the single letters of the tip, and proceed as you did with the incomplete transposition, checking those spots where these single letters appear (not having been crossed out) to see if you can fit the proper columns together. And watch, too, for another decimation; there might be another! When completed, the numerical key will be found to be: 3 5 4 1 3 2.

Problem 55. Period 8. BRAZILIANCITY; ACROSSTHE

SEFAI BINYU FETET NNIIB IROEE WRRSE IRASE HDCTE SRSAO TENRT ITARI CSLNR AFDGY SEEGA TIDAA IARHE RSROR OYNME LDOOC ELYAI LEOAH AYRTE SATUU IRDTT ECLII BELVN NACBT CIERO ALSEN LAFTR UFSTH SRKBO SSMBL REIPZ TOSOI WRSHE RWDHL NNOCH (190)

Problem 56. EVILINFLUENCE

BIEEF EUAMT FHELJ LENNA VIIRL MSALR DFEFI NIOIO ROPIT LCIOT YAHAI
EUEKQ TTTAR ATTTW AWMOR OMIEH EAHRO RNANC LEARI IBAEE RTFFD BFEWF
OINTK EOODM TSELV LFECF WSOLR SUVET TIEPT INAMI ALUHH IMAHO MNANO
FILEE FE (172)

Problem 57. PRIMITIVE; Caesar: TGNKIKQP

IOTIU PEFHN SEOAD HGNSI AARDR PIRGD IHPAI ENHGL GTEHP NTMNI IFESY
OARST ETHRL NFEOG FSHCD OBRIE OFEIT SSIWE EIOHO ERDEA WPTTS NILEI
ADLIA LTNNI POANR SBOOM RMOEV TTIES ANENS HCTEF TAHHY HTDVE GGLTI
NNEIS OLLOT SLIRR DEEIE MIHLH FGDIV ARLAF RODSA SARMS SETFO OOTEA
MIRST TRIWA HST (233)

CHAPTER XIX. THE TURNING GRILLE CIPHER

The Grille is an ingenious cipher using a mask with cut-out cells, in four positions to write letters into a square block. At each setting of the mask, the plaintext letters are written into the cut-outs; then the mask is turned one-quarter rotation, and another set of letters written in; a third and fourth rotation complete the encipherment and the resulting cipher is then taken off by horizontals.

Since the basic cipher block is square, one-fourth of the cells must comprise the holes in the mask, and hence it means that there should be an even number of letters on each side; the total number of letters must be the square of any given number: 4, 16; 5, 25; 6, 36; 7, 49; 8, 64, etc. (Note that this series includes odd numbers; but they require special technique and will be explained later). The position of the holes cut into the mask is by an arbitrary selection, but must follow a certain method. For instance, suppose a cipher of 36 letters is to be made into a grille. On a work sheet, draw a block 6x6, and divide it into quarters, of 9 cells each. Then, number each quarter thus:

```
1 2 3 ' 7 4 1
4 5 6 ' 8 5 2
7 8 9 ' 9 6 3
-------------
3 6 9 ' 9 8 7
2 5 8 ' 6 5 4
1 4 7 ' 3 2 1
```

It will be noticed that each numbered digit occupies the same relative cell in each quarter; 1: the corner position; 9 the inner-center position, etc.

To select holes for the mask, take the number 1, then 2, through 9 from any separate square, in succession, alternating where needed; but do not use two 6's, for example, in two different squares. For instance:

```
1 - - ' - - -
4 - - ' - 5 -
- 8 - ' - - -
-------------
- 6 - ' 9 - 7
2 - - ' - - -
- - - ' 3 - -
```

To prepare the final cipher, either of two methods may be followed: 1. By using transparent tissue paper; 2. By cutting out the holes with a razor blade.

Letter the four positions as upright I; a quarter turn (to the right) as II; another quarter-turn to the right as III; and the final position IV. At I, write in the first nine letters of the cipher; at II the next nine and at III and IV the third and fourth nines. Then, take off the resulting letters horizontally for the ciphertext.

Solving a Grille is a bit more complicated, since only fragmentary text may be gathered at any one time; from but two positions, the normal and the reversed, as I-III, or II-IV.

There will be other letters recovered, but they will be unrelated until gaps are filled, as will be demonstrated as the procedure is shown.

Here is a cipher to be solved. It is 64 letters long and is, whe when written into an 8x8 block: The tip is HAVE GREAT WEALTH

```
T W E T ' O R A R
E A L T ' S E H S
H A E M ' K T E T
O E R R ' H T E A
-----------------
I O P H ' N S C I
A V A E ' H E G R
E N S G ' T H O D
A E A A ' T F A B
```

Examine the tip and check with the cipher-block: H: there are 6 H's, a poor start, to know which one is correct. A: 10 A's; V: 1 V; E 11 E's; G: 2 G's; R: 5 R's; T: 8 T's; W: 1 W; L: 1 L. So, the logical spot to try to get into this cipher, is by using the single W and the single L.

Now, not knowing in which turn of the mask the the tip is to be found, assign A B C D to the four turns of the grille. For clarity, this will be shown in diagrams; but this is not particularly necessary in actual operation. Looking at the basic block: W-cell 2; E: cells 3 and 9; A cells 7, 10; L: cell 11; T cell 12; H cells 15, 17. Now, by using either that piece of tissue paper, or planning to cut out the recovered squares with that razor blade, sketch out a vacant block the same size as the cipher block, to be laid over the cipher and assumptions made. Letter the four corners as A B C D, to separate the various positions.

At cell 2 (W), 11 (L) and 12 (T), mark these three out, so that the tentative mask looks like:

```
B
- W e - ' - - a -
e a L T ' - - h -
h - - - ' - - - -
- - - - ' - - - -
-----------------
- - - - ' - - - -
- - - - ' - - - -
- - - - ' - - - -
- - - - ' - - - -
```

It is not known for sure just which cells are to be accepted for the in-between letters, so turn the grille half-way around, that is, two quarter turns, to the reverse position, at D:

```
- - - - ' - - - -
- - - - ' - - - -
- - - - ' - - - -
- - - - ' - - - -
-----------------
- - - - ' - - - -
- - - - ' - - - r
- n - - ' T H o d
- e - - ' - f A -
                D
```

Determine for yourself, just which of these doubtful cells to accept; RN may be disregarded for the nonce; THOdefa doesn't look good; but TH E FA does. Mark or cut out the proper holes of the grille and the four positions will now show up as:

```
A                    B
- - - - ' - - - -    - W E - ' - - A -
E A - - ' - - - -    - - L T ' - - H -
- - - - ' - - - -    - - - - ' - - - -
- - - - ' - - - -    - - - - ' - - - -
-----------------    -----------------
- O - - ' - - - -    - - - - ' - - - -
A V - - ' - - - -    - - - - ' - - - -
E - - - ' - - - -    - - - - ' - - - -
- - - - ' - - - -    - - - - ' - - - -
```

```
C                          D
- - - - ' - - - -          - - - - ' - - - -
- - - - ' - - - S          - - - - ' - - - -
- - - - ' - - E T          - - - - ' - - - -
- - - - ' - - - -          - - - - ' - - - -
-----------------          -----------------
- - - - ' - - - -          - - - - ' - - - -
- - - - ' - - - -          - - - - ' - - - -
- - - - ' - - O D          - N - - ' T H - -
- - - - ' - - - -          - E - - ' - F A -
```

re-examination of the tip and checking with the positions, indicates that undoubtedly A has the rest of it: HAVE GREAT. So, test tentatively what A has to offer:

```
A
- - - - ' - - - -
E A - - ' - - - -
- - - - ' - - - -
- - - - ' - - - -
-----------------
- O - H ' - - - -
A V - e ' - e G R
E - - - ' - - - -
a e a a ' T - - -
```

and check with position C to see if other good fragments appear in its reverse position. If the proper cells have been accepted after the placement of the entire tip HAVE GREAT WEALTH, the four positions and their letters will be, now:

```
A                          B
- - - - ' - - - -          - W E - ' - - A -
E A - - ' - - - -          - - L T ' - - H -
- - - - ' - - - -          - - - - ' - - - -
- - - - ' - - - -          O - R R ' - - - -
-----------------          -----------------
- O - H ' - - - -          I - - - ' - - - -
A V - E ' - - G R          - - - - ' - - - -
E - - - ' - - - -          - - S - ' - - - -
- - - A ' T - - -          - - A - ' - - - -

C                          D
- - - T ' O - - -          - - - - ' - R - -
- - - - ' - - - S          - - - - ' - E - -
H A - - ' K - E T          - - - - ' - - - -
- - - - ' H - E -          - - - - ' - - - A
-----------------          -----------------
- - - - ' - - - -          - - - - ' N S - I
- - - - ' - - - -          - - - - ' - - - -
- - - - ' - - O D          - N - - ' T H - -
- - - - ' - - - -          - E - - ' - F A -
```

These four positions and texts are beginning to take shape:

A: O HAVE GREAT
B: WEALTH ...OR RI
C: TO SHAKE THE... OD
D: R E A N SI N THE FA

Assumptions are now tried, marking lightly in pencil at any cell taken as a text; but marked heavily when they have been proven. At this point, it might be wise, to use the present mark, and cross out all those letters which are used; leaving only those which can yet be tested. This permits more accurate use of the remaining letters. With a little "hit or miss" technique, the complete cipher is soon found.

Problem 58. JUST PLAIN; DISSOLVING
VAROM MHAMC ERTAT NOAUI RIRIN SNHPG ENTUI MISJM SUSAD INNTE ELBPL COINA MSMYI ANDIS WSSEP AEDIO TLEOR VIRAB CNILG COITC (100)

Problem 59. BROKEN INTO
HBAFT RÓLRI KOSET EANID ETRII NCHGN IIVCN ACTEO ELLNB LYYIN WIATR HEGPN APCDE KPOIA ENCED LCAUS RICRS WEHRX IEEXX CNAXS (100)

Problem 60. GENERALLY
GHTWY EUEMR MTENA AGINS OEIAN GUNSE EMRAR NOSAD IRBLN LOOAY FRPNT EHCRT IEHEI FNVEO ATUNT AEANT MIHDE NSEES ROTNC FCSIT (100)

CHAPTER XX. THE PHILLIPS CIPHER

The Phillips Cipher employs the Polybius Square as its base, but in cyclic form to produce eight (in the standard form) squares up to twenty-one as the maximum. The basic square (1) carries as its numerical indicators 1-2-3-4-5 for its five rows; the following squares shift a row at a time to produce a new square as the patterns below show:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1	2	2	2	2	3	3	3	3	4	4	4	4	5	5	5	5	1	1	1	1
2	1	3	3	3	2	4	4	4	3	5	5	5	4	1	1	1	5	2	2	2
3	3	1	4	4	4	2	5	5	5	3	1	1	1	4	2	2	2	5	3	3
4	4	4	1	5	5	5	2	1	1	1	3	2	2	2	4	3	3	3	5	4
5	5	5	5	1	1	1	1	2	2	2	2	3	3	3	3	4	4	4	4	5

and in solving, these phenomena are taken into account.

Some of these numerical orders are identical but in a slightly different sequence as noted: 1-5-9-13-17-21; 2-8; 4-18; 6-12; 10-16.

Encipherment is done by letter-by letter. Plaintext may be of any length, with or without nulls added to complete the final group. For the standard use, eight squares are used, and the plaintext goes for 40 letters before overlapping on itself for the second line, third line, etc. In this encipherment, the ciphertext is taken from the letter on the downward diagonal to the right; where the plaintext letter occupies cells 15-25-35-45, the ciphertext is taken from cells 21-31-41-51 respectively; where the plaintext is taken from cells 51-52-53-54-55, the ciphertext comes from cells 12-13-14-15-11. For decipherment, to find plaintext, read that cell in an upward diagonal to the left.

For example, showing but two of the squares, and with the keyword WATCHDOG written in verticals; and fragmentary plaintext which has overlapped in the first two squares only:

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

  A P A R T     F R O M T
  g x g z b     q z f p b
  D E F E A     T S S I Z
  i f p f g     b v v n a
  A C O M P     L E X S Y
  g e k n x     s i c v h
```

It will soon be noted that each set of squares to the depth of the message constitutes a simple substitution; but that each such substitution varies in the subsequent square-form.

For the sake of explaining the decipherment of a sample message an 8-square setup will be described. Since this cipher uses five-letter units to represent the cipher as it would appear in "The Cryptogram", it will be shown in place rather than re-written.

I	II	III	IV	V	VI	VII	VIII
ZVDZK	DWGHG	APZFW	PXQDZ	ZKFRD	VZYNI	UQNFQ	QBXWZ
VBFGX	BNNBO	DYQYI	BWBRB	FRDXD	FYBXZ	SPXUB	RIXTG
NNLXB	SWGLB	WHRGW	TZRBS	NWFXD	FSXCQ	NFQPS	IDUSW
FZZVD	ZHDQG	ZPDGW	ZBPPN	DDBWF	ZYCBX	D----	

Write the cipher out 40 letters wide, and skip a space between lines; skip another space before writing the second row of ciphertext so that a line is left for plaintext in each row.

Two tips are offered: THERE ARE SOME and SMALL STREAMS. The first tip indicates that a pattern appears somewhere in a certain row of one of the squares and so it is necessary to rewrite the tip into its various possibilities, as:

THERE ARESO ME   -THER EARES OME   --THE REARE SOME

---TH EREAR ESOME   ----T HEREA RESOM E

The first one is found at DRDXD FYBXZ SP in squares V-VI-VII, second line. Write in the plaintext under the proper letters, and also substitute where possible in each block where other known plaintext appears, in these three squares only. In the third line in V under NWFXD may be seen --TRE, which also appears placed in IV-V-VI, so that second tip may be placed here.

Underneath these four squares write in the plaintext-ciphertext pairs thus:

IV	V	VI	VII
SZ	TF	AF	MS
MR	HR	RY	EP
AB	ED	EB	
LS	RX	SX	
	LN	OZ	
	SW	MS	

Now, draw up a row of blank squares under the entire width of the cipher, 5x5 (and assign the numerical sequences to each).

Examination of these pairs reveals that in IV is SZ and LS, which means that they may be combined as LSZ; under VI is SX and MS, to be combined as MSX. When such trigraphs occur, they are preferred as opening wedges. Note, now that SX is in VI; but that SW is in V and SZ is in IV. This means that whatever rows are assigned to the SX, the X-row in V and the X-row in IV cannot be the same row as in V. Hence it will be necessary to find out which row is proper by calculation:

LSZ can be (IV)	SW can be (V)	MSX can be
5 2 3	2 3	3 2 4
2 3 4	3 4	2 4 5
3 4 1	4 5	4 5 1
4 1 5	5 1	5 1 3
1 5 2	1 2	1 3 2

Since SZ in IV as 2 3, and SW in V also is 2 3, this can not be, so it is scratched off. The same is true of 3 4. SW in V is 4 5 but S X in VI is also 4 5 so this may be cancelled as well. The same is true of 5 1. This leaves only SW in V as 1 2.

Under the V in the vacant squares, write in S in cell 11 and W in cell 22 on the diagonal to the right. Write these letters also into the other seven squares in their proper places, keeping in mind that the order of these rows is a bit different in each one. Check off SW as being used. Now, go to VI for the MSX. The sequence of rows is 3-2-4-5-1. If S is in cell 51, X must be in cell 12; and M must be in cell 45; since S is in the first column, M must be in the fifth, and so on. Returning now to IV, there is an MR so R may be placed. If M is in cell 55, R must be in cell 11. In V, HR; if R places in cell 11, H must be in cell 55. In V, LN; if L is in cell 35, N must be in cell 41. Continuing with half-values already placed, write in all other possible equivalents, until the I-square now looks like:

```
S - - - H    and the other seven squares have the same letters in
R W - - -    them in their proper rows.
- X - - -
O Y - - L    The plaintext at this point looks like:
N Z - - M
```

```
O - - O - - - - - - - - - - - O O N - R - - S O - - H - - O R L
- - - - - - - - S N O - - - - - R - L L - - - S - S - - N - M
- T H E R E A R E S O M E S - - M - S - - L L - R - - N - -
- N - N - N - S M A L L S T R E A M S - - - - - - - M - - - -
N - O O N - O - - - - - O - - - N S - - - H - - - S - O R - -
```

If, by now, the route for the write-in of the basic square has not been guesses, and a few additional letters written into it, checked for more plaintext, look at -H-- ORL-- (the world?); -OON- (to one, so one?) Try these assumptions, and decide which is correct, and then write in new plaintext in all blocks. The finished square will develop to have TEACUP written in by alternate verticals.

Problem 61. (8 blocks) SEVENTEENTH CENTURY; ALWAYS BEEN
TLDWY LNINO NRPNS DWTTO SFSOZ XYWUL FWWUW WYMPH VIWNL XXRTP KVWTI
TUTOV WWOVI GWIPA ABLIW ZLHTP GLVTZ LOKPU TYSYL KINOX QPPYS FLEWT
SUWLS ETWNY PYKWZ MTYAS TLOVW ZDWRT SESOZ LHQXR WAXOI TXRNW ZSVVI
TVILH ZKLOX ZUZXM SFTLO QXVWK

Problem 62. (10 blocks) OF ALL NATIONS; BY THIS MEANS
CRFHG DTWOH UHSGQ MKWLF BUVHS RHYVC FBICW PTDCT FGVRH IDNCD VFNBU
HYYOH UHSGV HPZFT RNIVC ESUSV DIXYA TWVHY LHKCH BRNFO HGFTH VDTOA
FUSAQ EDEVR HVEFN RVGHW YXWBC FUIHW HBZVC BRWKS VKNGK FGGZO HKQUF
CHVRF NVFNG IZRIS BCDHX LMOS

Problem 63. (21 blocks) ADVANTAGES; THAT THIS
AYFPS NNDLL OVCNW ZCHFA BQUQX EXCAT GVMHU GFSQD BOYAF CUXSU MFSMA
BIEQU BUFGU MDWDM EHURH OCFAF NQZZF HOSDG GZAGF GCVPF MDFKG AAFUA
SZQUZ HFOWH OSRGW AYGUF RCDEZ ANGHI DHSNG UBPAY WSAES LTLKG AUZET
UABHU FDCHI NWDRI ICFDA HGAFD AYDAA NTRYT XDWRV NCDQB FNAEF NGUDG
QGNLV DGSAW GAGNQ AEZMG CCDZQ SUGAD HWXQS DXSUM FCMWT FFBZU MQHHG
CPPRV CCRYF YSHWB UGABQ QIXAY TRYFG DRPRC SNASD FYGPE DQDXS LLFXL
YFPFK UBAFM AEGEC RPZAN XSQGQ NBGHH IFUMC NQZQW BNGFF WGUMY DPEFR
RFDFX RDFUA CQDAQ ASIQX DOTHT RVFPN QDGHH NQSUA HSDLZ OLYFK IHGN-

CHAPTER XXI. THE CHECKERBOARD CIPHER

The Checkerboard Cipher uses a single Polybius Square to both encipher and decipher; but the single plaintext letter becomes a ciphertext digraph. Actually, such resulting digraphs offer a problem which is similar to a Patristocrat, an undivided Aristocrat. Frequencies may be taken of these digraphs, as is done with simple substitution to find out the high-frequency ones and the low, and thus assign values.

There are two keys used to determine each digraph, which may be literal, or numerical, one at the side of the square and the other at the top; and where the two interlock, is the plaintext letter. In the more complex forms, two keywords appear at the side and at the top (and there may even be no keyword, but arbitrary letters), giving alternate values for ciphertext digraphs.

In the first six diagrams below, the simpler forms are shown: five with the keyword alphabet written in normally and the final one with the keyword alphabet written in counter-clockwise. The seventh diagram shows the more complex method of the Checkerboard Cipher:

```
   A B C D E        1 2 3 4 5        V A L E T        A C B E D
F 'B U C K E'    6 'B U C K E'    S 'B U C K E'    F 'B U C K E'
G 'T S H O P'    7 'T S H O P'    H 'T S H O P'    J 'T S H O P'
H 'A D F G I'    8 'A D F G I'    O 'A D F G I'    H 'A D F G I'
I 'L M N Q R'    9 'L M N Q R'    W 'L M N Q R'    I 'L M N Q R'
J 'V W X Y Z'    0 'V W X Y Z'    Y 'V W X Y Z'    G 'V W X Y Z'
    (1-a)            (1-b)            (1-c)            (1-d)

   2 5 1 3 4        A B C D E           W I N D Y
8 'B U C K E'    F 'B L I G F'          S T O R M
0 'T S H O P'    G 'U M Y X D'     M G 'B U C K E'
9 'A D F G I'    H 'C N Z W A'     A R 'T S H O P'
6 'L M N Q R'    I 'K Q R V P'     T E 'A D F G I'
7 'V W X Y Z'    J 'E T S H O'     C Y 'L M N Q R'
    (1-e)            (1-f)         H S 'V W X Y Z'
                                         (2)
```

Encipherment is given for plaintext: IMMEDIATE in each of the squares:

I	M	M	E	D	I	A	T	E	
HE	IB	IB	FE	HB	HE	HA	FA	FE	(1-a)
85	92	92	65	82	85	61	71	65	(1-b)
OT	WA	WA	ST	OA	OT	OV	HV	ST	(1-c)
HD	IC	IC	FD	HC	HD	HA	JA	FD	(1-d)
94	65	65	84	95	94	92	02	84	(1-e)
FC	GB	GB	FE	GE	FC	HE	JB	FE	(1-f)
x	y	y	z	x				z	

It will be noticed that in "x-y-z" blow this diagram, repeated digraphs appear, which bear out the frequency being comparable to single letters in a simple substitution cipher; but

I	M	M	E	D	I	A	T	E	
TY	CT	YI	MM	TI	EM	EW	RS	GY	(2)

there are no such repeats, for alternate values have been used to obtain these digraphs.

It will also be noted that if, when solving a cipher of this type, a tabulation of the first letters, and then the second letters of the digraphs be taken, there will be only five different characters (letters or numbers) for the 1-variations, but there may be five or more for the 2-variation. By this means, it is discovered whether the simpler or the more complex system is involved.

Here is a sample cipher, with the tip ANCIENT and its placement, underlined:

```
YC EM HR YR ER YC YR EH EH AC YR NA NA YC EH YR YC YH ER YR EC YH
                                                a  n  c  i  e  n
AC YA YC AM EH AC NC EC ER HH YH AC YR YN EC YH AC AA NC EC HR EC
t
AC NC EC HH EH AC HR YR ER NC ER NC YR EC EM NA AM EM NA HH HA HR

YR EH NC EC EH
```

A tabulation of the different letters of the first half of each digraph shows: Y E H Y E E A N Y E Y A N H A H for the side; and C M R R R H C A H C A M C H A A for the top.

First, try to transpose each set of letters and make a legitimate word: side (HYENA?); top: CHARM or MARCH. Draw up two blank squares, and assign HYENA to the side of each, with CHARM at the top of one, and MARCH at the top of the other; then write in the plaintext letters derived from the placed-tip digraphs. Thus:

	M	A	R	C	H
H	-	-	R	-	O
Y	-	-	I	A	N
E	F	-	C	E	S
N	-	-	-	-	-
A	-	W	-	T	-

	C	H	A	R	M
H	-	O	-	R	-
Y	A	N	-	I	-
E	E	S	-	C	F
N	-	-	-	-	-
A	T	-	W	-	-

The second square lends itself more readily to the probably way of the write in: ..CF, T.W..

Go through the cipher and write in any plaintext letters which result from the letters in the square with the known key-letters at the side and top. Checking with the tabulation frequency:

YC - a 5
YH - n 6
ER - c 5
YR - i 9
EC - e 8
AC - t 7

The results aren't too far off, and most acceptable. Now:

1. AC NC EC is repeated, as T -E and may be THE. If so, NC is H.
2. The end of the cipher: HE (EH). EH must be D, R, or S; but up above EH HE coming together with the known plaintext cannot be D or S, so must be S.
3. -H E -E (WHERE?), then AA is W and HR is R.
4. HH is O.   5. EM is F.

By now the first square may be disregarded as no route write-in is plausible (but we had discarded it earlier). The foregoing procedure merely proves this point. In the second square, the one we have accepted, T-W suggests TU-VWX-Y-YZ as the row. And the rest is a simple matter to solve.

Problem 64. BEFORE

AI AA AK SS PK PI IK IA PI PK PT AA PS PI AI AA AT PK PT IT PS PI
PK II IA PK AA IK RK SK PS AK RK RK AK SI PK PA AS SK AI IT PK PI
PT PK IT AK PS PA AI AA AT PK IK IA AA PK IT AS PK PS AK PI PK IK
RI PK AT IA PI IK AI PT AA PI PT IT PK IT AI IK IK RI PK AK IS PK
PI AI

Problem 65. TWOFEET

UA PO EO PK JD EO UV PD JO UA PA EA JK EO JV PK UK EK LD PA UK JO
UA JO JO PO UA PD PD UA JO JK LD LA EA LD PK LK UD EA JO PD EO PK
JD EO PA UA JO UD JV JD EA UA JO JA UV EO JK EA EA JA PD EO PK JD

Problem 66. COLLEGE; TONTHE

LP YN LI EI LI PN ET TJ TI TI LP LG LI YI PP EN LJ DJ YW EW LW LP
LU EG SE SI PI TP EI LI PJ EJ EI PP TE TP LP EP TJ AW EI LS LI EG
PT EJ LS DN DG DN LJ AP US UP ES GT AI SE GS EW EP US PT PN EI UI
UI AW UT YU AW UW GN UP UU UJ DN SU GH AI LP LI AU

It may said here, that in "The Cryptogram" sometimes the constructor will reverse the order of his digraphs, so that, for instance, GB and BG will represent the same plaintext letter.

CRYPTOLOGICAL REFERENCES

For Sale by

THE AMERICAN CRYPTOGRAM ASSOCIATION

SOLVING SIMPLE SUBSTITUTION CIPHERS By Frances A. Harris (S-TUCK)		Paper	$1.00
CRYPTANALYSIS By Helen Fouche Gaines (PICCOLA)		Cloth Paper	$3.00 $2.00
PRACTICAL CRYPTANALYSIS By W. M. Bowers (ZEMBIE)			
VOLUME I	PLAYFAIR - FOUR SQUARE CIPHERS	Paper	$1.00
VOLUME II	THE BIFID CIPHER	Paper	$1.00
VOLUME III	THE TRIFID CIPHER	Paper	$1.50
THE CRYPTOGRAM (Bi-monthly magazine) The Official Publication of the American Cryptogram Association		(Back issues)	$ .50

Frederic C. Flindt, Treasurer
405 William St. S.W.
Decatur, Alabama 35601

I. L. Genud, Librarian
8239 Fayette St.
Philadelphia, Pa. 19150