PRACTICAL CRYPTANALYSIS

VOLUME V

"CRYPTOGRAPHIC ABC'S"

by

WILLIAM G. BRYAN

VOLUME II

Periodic Ciphers -- Miscellaneous

THE AMERICAN CRYPTOGRAM ASSOCIATION

1967

PRACTICAL CRYPTANALYSIS

VOLUME V

"CRYPTOGRAPHIC ABC'S"

by

WILLIAM G. BRYAN

VOLUME II

Periodic Ciphers -- Miscellaneous

THE AMERICAN CRYPTOGRAM ASSOCIATION

1967

V O L U M E   II
C O N T E N T S

CHAPTER I. FINDING THE PERIODS IN A PERIODIC CIPHER

With a working knowledge of the monoalphabetical substitution ciphers (Aristocrats and Patristocrats) the next step is to learn how to solve Periodics. This type embraces the Vigenere Family: Vigenere, Variant, Beaufort, Gronsfeld, Porta, Portax, Nihilist, Slidefair, and the Quagmires, which will all be taken up in turn.

A Periodic ciphers means that a period is used for encipherment; that is, a keyword of a length agreeable to the constructor has been employed. Since the cipher is presented to you in groups of five letters, you have to find the period used in each case - they all vary in the use of keywords from three letters long up, though rarely do they extend past thirteen; however, it has been known to happen that a 20-letter key has been used.

To find such a period the Kasiski method is applied, and there are two sections of this: the short way and the long way. The short way is adapted when there are two- or three-letter repeats of the ciphertext for tabulations; the long way is required when there are no such repetitions and a single-letter tabulation is necessary.

Given, this sample cipher - system unknown for the moment, with the groups numbered (as is done with all solution work of this kind), and the repetitions underlined, for the sake of explanation:

```
    5    10    15    20    25    30    35    40    45    50    55
BGZEY DKFWK BZVRM LUNYB QNUKA YCRYB GWMKC DDTSP OFIAK OWWHM RFBLJ

   60    65    70    75    80    85    90    95   100   105   110
JQDRM PNIQA VQCUP IFLAZ HKATJ UVVQE EKESZ DUDWE KKESL IZQAT SBYUZ

  115   120   125   130   135   140
UUVAZ IXYEZ JFTAJ EMRAS QKZSQ FOPHM W
```

Tabulate all repetitions and write down the actual positions of the first letter of each unit:

BG 1-30; RM-14-59; KA 24-77; MR 50-127; QA 64-103; VQ 66-83; AZ 74-114; AT 78-104; UV 81-112; EK 86-95; KES 87-97; SQ 130-134.

Then, take the difference in each case, and factor this number:

```
BG 29 (unfactorable)
RM 45                     3 - 5 - - - 9 - - - -
KA 53        "
MR 77                     - - - - 7 - - - 11 - -
QA 39                     3 - - - - - - - - - - 13
VQ 17        "
AZ 40                     - 4 5 - - 8 - 10 - - -
AT 26                     - - - - - - - - - - - 13
UV 31        "
EK  9                     3 - - - - - - 9 - - - -
KES 10                    - - 5 - - - - - 10 - - -
SQ  4                     - 4 - - - - - - - - - -
```

Total each column, and the highest result indicates the true period - with reservations at times; in this case 26 for 13, seems plausible, but there is a trigraph KES, which, when weighed against digraphs holds preference. KES indicates that the period may be 5 or 10. Frequently in the cases of 6 (2x3), 8 (2x4), 10 (2x5), 12 (2x6), etc., it is difficult to know whether the smaller or the larger number is the period, but proceeding with solution clarifies this situation. It is so that this particular cipher has a 10-period.

(Sometimes in scanning ciphertext for repetitions, groups such as KFR, KVR; SXC, SAC turn up. In such cases, they may be treated as legitimate trigraphs so long as the first letter of such units is used for its position in the cipher.

But, suppose there are no repeats, or those that exist do not establish a period? What then?

```
    5    10    15    20    25    30    35    40    45    50    55
RNQJH AUKGV WGIVO BBSEJ CRYUS FMQLP OFTLC MRHKB BUTNA WYZQS NFWLM
   60    65    70    75    80    85    90    95   100   105   110
OHYOF VMKTV HKVPK KSWEI TGSRB LNAGJ BFLAM EAEJW WVGZG SVLBK IXHGT
  115   120
JKYUC HLKTU MWWK
```

Write in a vertical column the entire alphabet, and after each letter, show the actual position of each letter in the cipher as:

A 6 45 83 89 92 115
B 16 17 40 41 80 86 104
C 21 35
D --
E 19 74 91 93
F 26 32 52 60 87
G 9 12 77 84 98 100 109
H 5 38 57 66 108 116
I 13 75 106
J 4 20 85 94 111
K 8 39 63 67 70 71 105 112 118 124
L 29 34 54 81 88 103 117
M 27 36 55 62 90 121
N 2 44 51 82
O 15 31 56 59
P 30 69
Q 3 28 49
R 1 22 37 79
S 18 25 50 72 78 101
T 33 43 64 76 110 119
U 7 24 42 114 120
V 10 14 61 65 68 97 102
W 11 46 53 73 95 96 122 123
X 107
Y 23 47 58 113
Z 48 99

Now, take each difference and every difference in each case. For example: A 45 minus 6, 83-6, 89-6, 92-6, 115-6; and 83-45, 89-45, 92-45, 115-45; and 89-83, 92-83, 115-83; and 92-89, 115-89; and 115-92. And, then factor these difference setting up head-numbers from 3 to 12 inclusive, and marking down each time that the factor is used in each of the differences with a small tally. The final results with the total tabulations for each factor in each of the letters of the alphabet will be:

	3	4	5	6	7	8	9	10	11	12
A	3	1	-	1	1	-	1	1	2	1
B	9	7	4	5	3	7	4	2	1	2
C	-	1	1	-	1	1	-	1	-	-
D	-	-	-	-	-	-	-	-	-	-
E	1	1	1	1	-	-	1	-	1	1
F	2	3	3	1	2	1	1	1	1	-
G	5	5	4	1	4	3	2	1	3	1
H	6	3	2	2	3	1	1	2	1	-
I	1	-	-	-	-	-	-	-	-	-
J	3	1	2	1	1	1	3	1	-	-
K	13	10	4	9	8	5	3	1	2	3
L	4	3	4	1	4	1	3	1	2	-
M	4	2	3	2	6	-	3	1	1	-
N	1	1	1	1	3	1	-	1	-	-
O	1	3	1	-	1	1	-	-	1	-
P	1	-	-	-	-	-	-	-	-	-
Q	1	-	1	-	1	-	-	-	-	-
R	5	1	1	3	2	-	1	-	-	1
S	4	4	2	3	2	1	1	1	1	-
T	4	3	1	1	2	-	1	1	2	2
U	5	1	2	5	1	2	3	1	2	2
V	5	6	2	2	1	2	3	-	1	1
W	9	4	5	3	8	1	4	4	3	1
X	-	-	-	-	-	-	-	-	-	-
Y	2	2	3	2	1	2	-	1	3	1
Z	1	-	-	-	-	-	-	-	-	-
Columns' total	87	61	47	43	57	30	35	21	25	16
times head	x3	x4	x5	x6	x7	x8	x9	x10	x11	x12
Total	261	244	235	258	399	240	315	210	275	192

The period is 7. This outstanding number is correct 98% of the time. Occasionally this is slightly off, but one of two (or at most three) of the highest results, will give the true period.

Now, try your ability with the following; keep your tabulations handy, for they will be used later on for solving, when the periods have been identified; then, too, the type will be shown. Find the periods of:

A.
WMYYH RGGDF FVVVS CXAYY GYEGD WTEBJ CCYNP UBEFW DUYYS FRKYE ESATE
VSQJJ HETJP UCLUF UISFD SAUWQ CPDLB XEVSQ CAAKO QYQWG AXUPT FDGZV
TKXQD SFDAP JMDKR MEPEQ PFFVP CCMEW JFRFD BCGAF UPNQO SFFNG EDFDL
RBKRY ZMGYF WW

B.
ZIIBQ UJFQU QUOVQ NUDVQ PNGGZ PEYTD JFGJP WXFWZ EKGTE HQPSF VHKDR
DMYAW UXLNE KHVCJ TVGOH IGDRF VXTHY PVYHR XUVFP VGDXN QQUGF ZULTF
WXHUU NEQNS GSXXQ IZIIB QURE

C.
QERXZ UNJLD XRQEL SUVJN EPMYT YLXAN SKMGW VGBIQ RDUVY TINXA MZCFE
BOZED EKFMZ CZMTN LVALI IEVBD FSGFP OIVJL WRXFW DVBPO HJQGP NCLCV
XIFUF CPTVE JSKGZ GLBOT ABBBX MCNGF LGYZT TCDFY NJK

D.

PXIZH GVGEU UOXIX MYEEJ ZCOCM OWZCL FMTOR ISIGH LKWPS MSIDX WCFBR
KPYXO PRJIL HFMCR IHUDU LVRLJ FVVVS HTYFR RGPHQ WIIBL XQXMM TDVGU
EITFM QEEJH WUHFW

E.

JDYEN RAHTG OHPHD UAARO EBJJS WIFBC BMRNN INJLL SRIMT VGRCQ FNSYV
HCYQQ JWYIA IGRJA IWNGP LHZFY DCQCG RRCIX ZVVPD PZGYU XUPCQ ZJIJX
UGOYG WZJLU AQAWA YKOPB QR

CHAPTER II. THE VIGENERE CIPHER

Periodic Ciphers, of which you have learned to find periods, are actually a series of monoalphabetical substitutions such as the Aristocrats, but since a keyword is used, under each letter of that keyword, there is a separate simple substitution cipher (each) one different), using all letters, in such a manner, that the resulting cipher is a combination of several such substitutions. Hence, it is vital that the period length be determined, so that each separate substitution may be broken down and solved.

The Vigenere Cipher, the basic one for all of this group, originally used a tableau for both encipherment and decipherment. A row of the normal alphabet appeared at the top to represent the plaintext; and below these 26 letters, appeared a series of 26 more alphabets in normal order, but each one starting with the next consecutive letter, viz:

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

Since plaintext letters are represented by the top row, the key-letters are shown at the extreme left under the (/) or "A" of the top row; and where the two lines intersect in the body of the tableau, the ciphertext is found. For example:

PT	A N D
key	f e d
CT	F R A

By taking F, the first letter of the key which appears in the left-hand column, A-plaintext of the top row, and F at their intersection, F-ciphertext results.

The use of such a tableau as above, has been considered a bit unwieldy for some solvers in the past, and so slides have now been devised which do the same work and are simpler to operate. These slides may be made up for each of the systems in the Vigenere Family: Vigenere, Variant, Beaufort, for example, each one differing slightly in performance, which will be explained later on.

For the Vigenere, two slides are constructed, each bearing the normal alphabet "A-Z", and distinguishing the "high-frequency letters" in one of two ways: 1. they may be underlined; 2. they may be shades with colored pencil, thus:

A double-alphabet, in each case is more flexible for solutions:

ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ

GHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEF

With this setting at key-G, just check with the tableau and see for yourself that the results are identical: PT-N, CT-T; PT-I, CT-O. In other words, the plaintext is constant, but the lower slide is moved until the key-letter falls below the "A" of the upper (or stationary) slide. Then, reading from the plaintext letters of this upper slide, the ciphertext is read from the lower one.

Most solvers have their own sets of slides; some make them from stiff cardboard, others get strips of wood from a lumber company (or use plastic) from 3/8" to 1/2" wide and about 10" long. The alphabets are typed to insure durability and then pasted on these strips (if of wood). (The author's slides shade the high-frequency letters in red for the Vigenere, and green for the Beaufort, for instance.)

Let's see what happens in an encipherment: the message COME AT ONCE is to be used with the key TENT; the key length is four, so the message is set up in a block of four:

T	E	N	T
C	O	M	E
A	T	O	N
C	E	-	-

The lower slide is moved until the T falls below the "A" of the top slide, and the plaintext letters, in turn, going down the column: C A C are enciphered as V T V; then the lower slide is moved until the E falls below the "A" and O T E becomes S X I; with N, MO equals Z B; and with T, again, EN equals X G.

Since cipher messages are written in five-letter groups, this cipher would be "taken off" as VSZXA XBGVI, from left to right horizontally:

T	E	N	T
V	S	Z	X
A	X	B	G
V	I	-	-

Suppose, we look back, now, to Problem D in Chapter I on the Kasiski method of finding the period. By now, you will have learned that the key length is 7, so set up the cipher into a block of seven letters wide; and mark off a new block of the same dimensions, which, of course contains no letters at all. It is best to write this new block a little to the left (or right) and parallel with the cipher block for facility in decipherment (on quadrilled paper). Thus column and rwo-by-row may be written in as procedure advances:

P	X	I	Z	H	G	V
G	E	U	U	O	X	I
X	M	Y	E	P	J	Z
.	.	.	.	.	.	.

Remember, each column represents a separate simple substitution cipher, but since examples of this sort, as well as those found in "The Cryptogram" are often too short to take a general frequency and apply the customary technique for solution. Above all, while these substitutions are separate, they will not produce consecutive plaintext, but will merely show isolated letters in that particular substitution, to be coupled with those letters that fall on either side in other substitutions, to make the true plaintext sequence. Here's where the underlined high-frequency letters on the slide come in:

Go down column 1, and tabulate all letters which appear more than once: P-2, G-2, X-2, C-2, I-3, T-2. Then, rearrange them in their normal sequence: C G I P T X. The lower slide is then moved successively so the first letter C is under the high-frequency letters, in turn: A E H I N O R S T, and a reading is made of the other letters: G I P T X, to see if they, too, fall below other high-frequency letters. If they do, the letter below the A of the top slide is the key-letter for that column; if they don't, further trials are necessary (it might be added that high-frequency letters do not always show up here, but the middle-frequency letters might be acceptable). With C under A: G-E, I-G, P-N, T-R, X-V; with C under E: G-I, I-K, P-R, T-V; X-Z; with C under H, G-L, I-N, P-U, T-Y, X-c; C under I: G-M, I-O, P-V, T-Z, X-D; C under N: G-R, I-T, P-A, T-E, X-I (six hits) which are enough to accept without going further.

Set the slide with the P under the upper-A which is the accepted reading and decipher the whole column: A R I N N T H I A T T C D R M E E S, writing it into the blank block and into column 1 there.

Do the same for solumn 2: L-3, P-2, W-2, H-2; H L P W. There are no outstanding results, so perhaps, in this case, high-frequency letters do not predominate in this column; this is not unusual, however, and is one of the phases that a cryptographer runs into to hold him up at times. Try column 3: I-3, U-3, C-2, I-2, X-2, H-2; C H I U X; and find there are two passable settings at P and at U. So, tentatively, place these two letters at the heading for further consideration for solumn 3's letters. Column 4: M-3, G-2, F-3, Q-3; F G M Q, setting Y seems best. Column 5: H-2, O-2, P-2, U-2, F-2: F H O P U; setting B gives four hits and is taken as possible. Column 6: W-2, L-2, I-2, R-3, E-2: E I L R W, with setting E there are five hits and accepted. Column 7: V-3, I-3, Z-2, R-3, K-2, J-2: I J K R V Z; setting R gives six hits. The keyword thus recovered now looks like: P P Y B E R; not very promising is it? But the BER looks good. Decipher columns 5-6-7 using BER as the ending of the keyword to produce:

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

These are all good fragments with perhaps one or two questionable portions: SKA and WIV. But there is another hope: GHT, must be preceded by I or U. Try each one in turn, but this time, since cipher letter G is involved, place the G under the I of the upper row, which results in the Y we already had; G under U gives an M under the upper-A; and of the two possibilities, MBER seems more feasible. Deciphering column 4 with this M adds NII S A A U A T C T R T M E E U E V to the fragmentary plaintext. And, now NGCE (preceded by O; UGHT preceded by O; TANT preceded by OR; TLYA preceded by N; UTAR preceded by O or A; EWIV preceded by R/H) are all good ideas. Try them out and accept the one which gives additional good plaintext.

Just remember: with a Vigenere cipher, read the setting for the keyword letter below the A of the stationary slide; and the plaintext appears in the same slide as this A, while the ciphertext is in the lower slide.

Here are some Vigenere ciphers to solve. In "The Cryptogram, they are often referred to as "Viggies":

Problem 1.
AHGBR MQHGC WRTJH YGNVR DYAPM RYQPN IDJSJ PGJDF XGJKU KAHYD IEURV
PPNIG UMAOP CCFIQ AHTYH KFAHG KVVZL TYORR ROERV NCCYS RYVRR ZATOF
GMYEF GUILH PNKLI PWETW VXQAH GBVRE AOHKY PRVTJ OTVMB NF

Problem 2.
JRQVY AUBRW IHOCS SYWHK RPJFV CVNMM HGUKV UCVIL ZBVRG SXJLX IOZEM
CUADZ FABGK USUBN OXLEO QGZAL HBUNJ RVHLM RUWVD UVAFH EMGWA VQHBN
IYBVF VYAFJ PNTUU BVWWV YEBSP GCPME JWSFL LHDIG WHBUJ WFCGU HOMWM

Problem 3.
EAGLC ENQXW BDFUN KBNFE IEHVX ASDSL XXGDB NEPNX BNPQH RUDHO ODAHY
KMHFL QELFV AONSL IKBSU DTRIZ EAJXI DNEXI STRDY MXNEP RCYCK ONPRG
FXGDQ PVIIA UUUSI JIFGE EELEW XNSFM ICURL ERFST YXMTI PJILP MNFHW
OZQAE RFERL BEMZS IALQP ATPRR IIEEE TRINR GQVZX E

Problem 4.
JJBVU AWSYM YOBVP HASWI CMHTK GVMKR HTTZS HHOKJ UDHWM BHLME SHZIO
COLTE OJXVY XGSAC SJFBF EEIVW WNWLG DEOJA BCDGI UWWWT HBTDH CLLJN
XURTO VOWYX WEGCJ FAYXW MPYWV RMXEA SMAJQ CPMOG WUEUC IEUHH JECCL
GMPMT IJWZX PISV

Problem 5.
MHLVT HGDCA QXREA SMWCX VSCPK PDILL BLQOC SXSPR ALQSN ADSNF ZVEKW
UJVTL KDQIE UWNCZ HEDIE PMRFL YCDJD HTWMA OERZT EBEBY WWSGP OCMXF
LRBGM APUPW COZRI VPGTB JRAUZ XMDBV SIDXO AQEZH KWNZI SDOME KFCMP
EJSDE

CHAPTER III. THE VARIANT CIPHER; THE BEAUFORT CIPHER

The Variant Cipher, another part of the Vigenere Family, is just that: a variant of the Vigenere. While the same two slides are used as were used with the Vigenere, the keyword is obtained in a slightly different fashion, since the key-letter falls above the lower A, instead of below. For example, with the same encipherment of COME AT ONCE with the keyword TENT:

```
T E N T    T E N T
-------    -------
C O M E    J K Z L
A T O N    H P B U
C E - -    J A - -
```

The setting of the two slides, for say, the initial T of the keyword is:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
HIJKLMNOPQRSTUVWXYZABCDEFG
```

Actually solving a Variant is no different from solving a Vigenere, except that if the Vigenere procedure is followed through, a peculiar keyword results (mixed letters); that is, no true keyword is evident; something like JYUWFT appears, and is apt to confuse the solver; but if he ever runs into such a case, he knows that something is amiss, and that a Variant is before him instead of a Vigenere; so perhaps the cipher has been mistitled.

In the Variant, as in the Vigenere, the plaintext appears in the opposite slide from the one containing the key-letter; Vigenere, below the A; Variant, above the A. The application of the high-frequency letters in the slide is constant, however.

Problem 6.

UALOT SILKH RWEBN NRHNL THURD VPVCH DLSUC OABSM YMXFO QAUBR NFHFR
IBAOH YTMWT ENJVQ UPZHF AQWGZ MVHTB OENJD IGIMF SULUA BPMLZ RNFNX
SMJTG DJHAF EKKSZ QWDZQ CLVRN FZXBZ WISTJ LNRNH RZ

Problem 7.

OQWDL KFVQJ DMMLT RRQWY AZMEQ NKRPK ORGNT PHLQQ JWLFL XUENC GDHMS
HNCAL LFSYV WVYUV UFFWG UUSEY VVEYZ LUQZJ FYSDG FDXFR VSOHN CGKVX
SVQRF EHDAN AXXZY WMQOX LFLUT HMLZD YGYGC NXGYK FSMDA RZ

A third member of the Vigenere Family is the Beaufort, and while the same general procedure is applied, the slides are different. One is a normal alphabet, extending double length as before A-Z; the other is a reversed alphabet, also of double length Z-A. It will be noted then, thatthe substitutions are reciprocal, that is, if I equals T at a certain setting, then T equals I at the same setting.

Again, using the same simple encipherment and the keyword TENT:

```
T E N T    T E N T
C O M E    R Q B P
A T O N    T L Z G
C E - -    R A - -
```

In the Beaufort Cipher, it does not make any difference whether the top A or the bottom A is used for the indicator for each letter of the key; the results are always the same. Hence, the setting for T would be:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKL .......
TSRQPONMLKJIHGFEDCBAZYXWVUTSRQPONMLKJI .......
```

You have kept the "period finding" of the examples of Chapter I. Look at "E" for the next problem, which is a Beaufort.

Problem 8.

PGPNN JCPMA CIMYR BHFVN GBZRH HAUWL KFJHH GFFTI KJSIB AARAN JOIAE
JGXXE RYPFU XAEYW XPNJG XRZTL PVNRQ EWUEP QLPRY ZBPAA ZGZDA QVCUY
PEEYD BFTVX WYKUX RBZFT FRMCA IFGAO MGYAB JLNPK MEQRJ G

Problem 9.

LDYUP AKUPT LVDTO BXUFW SERZP QMQPD NITHA NXUHE UGZTG HMGSM SRCUF
LBQPZ XRYOB FDMNZ TGCUP QQUFB PANAQ HBOON XOOQP DJCJK TPFDV TBRKL
TTSZG ODUFB TETEL POIEB HRTSM DBGGA YUT

Problem 10.

QADNA TBCGB JBBYW WUAWN QLUUT MKFWD UEMVW BUAZR OEXVN NSPAD QGJRZ
AGHMP TZEWB LJPBE NKDYC SZVUI FRMYN DUAUC OUUFU WZKYW GMEGL KDSAB
NELCM EUCSU JAFQF AGHMP TOAZU BNLOA RAYGC BNAIZ GAKBO VNNJR EXBA

CHAPTER IV. THE GRONSFELD CIPHER

The fourth members of the Vigenere Family is the Gronsfeld Cipher. Here, again, slightly different slides are utilized to perform the needed jobs of encipherment and decipherment. One slide is the normal alphabet, either representing the top or the lower position. The other slide is in numbers:

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

One-half of these digits is used for the encipherment and the other half for the decipherment. This means that only ten alphabets comprise the Gronsfeld Cipher as against 26 in the Vigenere, Variant and Beaufort.

The normal method of encipherment is to write in a numerical key composed of any digits 0-9 (there may be repetitions), and of any length; some digits need not appear at all. Some constructors prefer to adapt a literal key (letters) and convert them to numerals) thus:

C	O	N	S	T	I	T	U	T	I	O	N
1	6	4	8	9	2	10	12	11	3	7	5

"1" is assigned to that letter which is foremost in the normal alphabet; 2 to the next in succession, 3 to the next, and so on. If there are two letters the same, the first one carries the lower number, and the second (or third) those next in sequence. (This information will come in handy at a later date, when other types of ciphers are involved).

Again using a sample numerical key with short text matter:

```
6 2 3 4
C O M E
A T O N
C E - -
```

Place the zero directly over (or under) the C, and jot down that letter which falls in juxtaposition with the 6 to the right, which is I; do the same for the A, which is G; and again for C. With the second column, set the zero with O, T and E taking those letters which fall to the right at 2. The finished block is them:

```
6 2 3 4
I Q P I
G V R R
I G - -
```

Decipherment of the Gronsfeld depends again on the high-frequency letters as before, but in a slightly different manner.

Look at Problem "B" in Chapter I; which period was found to be 6. Set it up in a six-block:

```
Z I I B Q U
J F Q U Q U
O V Q N U D
V Q P N G G
Z P E Y T D
. . . . . .
```

Now, having also set up a similar block with the same dimensions, but blank, tabulate the cipher letters which appear more than once in each column. Column 1: Z-3, J-2, X-2, G-4, R-3, U-3. Mark off a row of digits: 9 8 7 6 5 4 3 2 1 0. Place the digit-slide with zero over (or under) each of these six letters, and tally a mark under each head digit which coincides to the position of any high-frequency letter to the left. For each occurrence of the ciphertext more than once, tally extra marks in the proper columns. The results should be for Z: 3-6's, 3-7's and 3-8's; for J 2-1's, 2-2's, 2-5's and 2-9's; for X 2-4's, 2-5's, 2-6's and 2-9's; (while there are also 2-0's at the extreme last, disregard them, for the vital zero appears over the first letter examined). For G: 4-2's, 4-6's. For

R, 3-6's, 3-7's. The total results are:

9	8	7	6	5	4	3	2	1	0
7	3	6	11	4	5	9	6	5	3

and, since 6 with the 11 tallies is high, this is the proper setting for that column. Sometimes, there are an equal number of tallies for more than one digit, in which case trial and error of substitutions provides the correct setting; sometimes there are several which cannot be separated one from another; in this case, return to the column and tally the high-frequency letters which appear, as well as those appearing but once. This additional step often straightens out the confusion. (And sometimes the constructor reverses his process of encipherment, whereby the decipherer must work in reverse and follow his steps to the right. Remember, zometimes zero will appear as one of the key digits, when the plaintext is identical with the ciphertext.

Finish the solution of Problem "B" of Chatper I and then try:

Problem 11.
JCYMM HAZPP VXRJM SHWAU MQOOX HVVRG QTYJL FZLLK SELTS IBNNU HSXLV
KLAWU ALBNY JLTGD ZGGUL BPVRK BGSTS IKAYV VSUXW OXGSB TLARF BBMMD
VJFOL ULBAZ

Problem 12.
KOIKG HTDFW GRGQC OZGVB PPUMP JDYPP WZLWO GSJOW OPVUQ KQRYG EFEPL
NJUYN EQHEP QJKOP ONJXS IKCXS HCILD SZGVB AJFWK EULCG JCLRB TTTLH
DFNJL NXDUF JSSEU JJUMK WXUHJ WYXDW RFFXW

Problem 13.
EVKSA EAMMX REBTG CIAXO LBNIN IVGAG OERSA ZFWDF JEEHS XMLXE LMYMM
DKXHQ OHNMZ VCKPA AQXVL MQZLC BBIKQ ERUNH HILEA QTUSX NAKOY NYZLT
DRIGS CSTRG KZCRN GTOEX JWRYR BYWKP QOZNM CWOOR ANDLR AKZSP NGXMW

CHAPTER V. THE PORTA CIPHER

The Porta Cipher is still another member of the Vigenere Family. This cipher uses a special table in which there are thirteen divisions, each of which produces a reciprocal lot of thirteen more substitutions - each of which is slightly different from any other. However, in this cipher, an alternate of two letters is found for each key-letter, so that there are two (rather than one) possibilities, in establishing the keyword.

The table, or chart is;

AB	A	B	C	D	E	F	G	H	I	J	K	L	M	AB
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
CD	A	B	C	D	E	F	G	H	I	J	K	L	M	CD
	O	P	Q	R	S	T	U	V	W	X	Y	Z	N	
EF	A	B	C	D	E	F	G	H	I	J	K	L	M	FG
	P	Q	R	S	T	U	V	W	X	Y	Z	N	O	
GH	A	B	C	D	E	F	G	H	I	J	K	L	M	GH
	Q	R	S	T	U	V	W	X	Y	Z	N	O	P	
IJ	A	B	C	D	E	F	G	H	I	J	K	L	M	IJ
	R	S	T	U	V	W	X	Y	Z	N	O	P	Q	
KL	A	B	C	D	E	F	G	H	I	J	K	L	M	KL
	S	T	U	V	W	X	Y	Z	N	O	P	Q	R	
MN	A	B	C	D	E	F	G	H	I	J	K	L	M	MN
	T	U	V	W	X	Y	Z	N	O	P	Q	R	S	
OP	A	B	C	D	E	F	G	H	I	J	K	L	M	OP
	U	V	W	X	Y	Z	N	O	P	Q	R	S	T	
QR	A	B	C	D	E	F	G	H	I	J	K	L	M	QR
	V	W	X	Y	Z	N	O	P	Q	R	S	T	U	
ST	A	B	C	D	E	F	G	H	I	J	K	L	M	ST
	W	X	Y	Z	N	O	P	Q	R	S	T	U	V	
UV	A	B	C	D	E	F	G	H	I	J	K	L	M	UV
	X	Y	Z	N	O	P	Q	R	S	T	U	V	W	
WX	A	B	C	D	E	F	G	H	I	J	K	L	M	WX
	Y	Z	N	O	P	Q	R	S	T	U	V	W	X	
YZ	A	B	C	D	E	F	G	H	I	J	K	L	M	YZ
	Z	N	O	P	Q	R	S	T	U	V	W	X	Y	

Again, applying this technique to the TENT example:

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

A peculiarity of this system is that since half of the alphabet is represented by the other half's substitution, there never will be found the letters A-M of the plaintext appearing as A-M of the ciphertext; no N-Z plaintext as N-Z ciphertext. This phenomenon is often helpful in placing probable words, when no tips are given as to the direct placement. For example: THE, one of the most frequently used words in the English language is bound to show up in the ciphertext as (A-M) (N-Z) (N-Z) combination, and so certain positions may be eliminated completely for a placement of THE. (Of course this is most useful in longer words). Often these longer words are offered in "The Cipher Exchange" in "The Cryptogram" and placements found. Suppose we apply this theory to Problem C of Chapter I; a plaintext tip is given as BRITISHMUSEUM, and since the period of 9 has been found, the cipher is set up into this size block. Now, scan the cipher for letters which follow this pattern:

(NZ)	(AM)	(NZ)	(AM)	(NZ)	(AM)	(NZ)	(NZ)	(AM)	(AM)	(NZ)	(AM)	(NZ)
B	R	I	T	I	S	H	M	U	S	E	U	M

Remember for each letter of the key, if the first half of the alphabet letters are used for plaintext, the latter half must be ciphertext, and vice versa. The only place where all of them fit is at: XFWDVBPOHJQGP, so this plaintext tip may be written into the second (or blank block).

(It might be wise, as was done with the slide ciphers, to make up a Porta chart for your individual use. Such materials may be kept in a small box along with other paraphernalia, where it is always at your disposal).

Checking with the chart, then, using the known plaintext and comparing the cipher letters, putting this information through the chart, the keyword appears as:

B	R	I	T	I	S	H	M	U	S	E	U	M	PT
X	F	W	D	V	B	P	O	H	J	Q	G	P	CT
s	y	c	g	a	i	q	e	a'	s	y	d	g	key
t	z	d	h	b	j	r	f	b'	t	z	d	h	

The (') indicates the repetition of key letters, and so the keyword must precede this point, not necessarily in this complete sequence, for some of the letters needed may belong at the left-hand side.

Examining: S Y C G A I Q E A
T Z D H B J R F B certain letters may be taken out as impossible:

S Y C G A I ~~Q~~ E A
T ~~Z~~ D H B ~~J~~ R F B

Now, starting from the left SY/TY (no suitable letter follows (except Y, which may be set aside for the moment); so move one to the right: YC YD (not possible for the beginning of a legitimate word); one more to the right: CH CG DG DH, followed by AB, suggests CHA; and then the IR to follow, makes CHAIR. So much for one word; what is left is EA EB FA FB; AS AT BS BT; SY TY, and it doesn't take long to discover EASY, so that the entire keyword is EASYCHAIR.

So much for deciphering when tips are given. When they are not, but the period is known, again make a tally of repeated letters in a column. Go to the chart, and check through it, to see which horizontal paired row will give the best equivalents of the high-frequency letters found therein; then jot down the alternate letters found at the extreme left (or right) for keyword letters. (As in all ciphers, there are bound to be wrong assumptions; but constant manipulation of hunches, and the crossing out of impossible formations of fragmentary plaintext, soon establishes the correct one, and forwards solution.

Problem 14. EMPEROR
EYWRR MOTJJ QOHFA LTYQV SQFPG EPWTG RVGUC DVVBT EMLMN BYSOE OHFKW YARQL PEBSB ETVXM WVBCV XRTIT JJAMX EHADZ VCAXN MMWZR WALFY BTJSP RTLLP LZDVD FZHGE PBKQR RUKWQ AEAOP Y

Problem 15. ITALY
WSMZM LZURN THIDW LRHFC NMMAH VHRMU QJWHQ ZIYYU TKNRF AYKWF EQAIA GMJEQ XNHYP YIEJI SAQYL WRFBA AIPYA PEWJX IYZNC JAVHK HKVFY XQUCM OWPIT OMRGM JDGTV HXYME TNHGN NMCWN OAUTE XMZXI ARXE, OUTEA HLRYL

Problem 16. No probable word given.
PUPDC WXITI MZCWR VOFEZ BWMZJ BUPUO UBUHX ZLJSI WXKJQ TPVNW BTDAW WAPOX PIYTM HHZVN WTUBR GQXXI TVXRN WQZJN TMPJN XDENH CTXAR OEIEZ RSTTG WAHXH WJADC IUBUP DRPGR G

CHAPTER VI. THE PORTAX CIPHER

The Portax Cipher is an adaptation of the Porta Cipher which has just been explained; but uses pairs of letters as a unit for encipherment and decipherment as apart from single letters. A special slide is required for its operation, and a keyword is needed.

```
        A B C D E F G H I J K L M    (stationary)          )
.O P  Q R S T U V W X Y Z N O P Q R S T U V W .... )       ) PT
                                                   ) sliding
.C E G I K M O Q S U W Y A C E G I K M O Q S .... )        ) CT
 D F H J L N P R T V X Z B D F H J L N P R T .... )  key   )
```

(The above slide-setting is for G-H (key) directly under the A-indicator of the stationary alphabet)

If the digraph RE is to be enciphered, take the R in the upper row of letters (stationary) and the E from the lower pair of letters (sliding), and use the opposite corners of the oblong to obtain the ciphertext, or PI. However, if the digraph ER is to be enciphered, take the E from the stationary alphabet at the top, and the R from the sliding alphabet at the bottom to obtain FP. It will be realized then, that if the first letter of a digraph is in the range A-M, the equivalent ciphertext is dependent on where the slide is used for the key-letter; but if the first letter of the digraph is in the range N-Z it slides along with the paired rows of lower letters, and therefore all such digraphs having its first letter in the N-Z range are constant, without depending on the key used. The only exception is when the first and second letters fall in the same column, in which case the key-letter has to be known, for letters appearing above the needed letters are used for the ciphertext.

In enciphering, use a keyword of any length that is convenient, and then write the plaintext in two rows under it; continue to the end of the message. When the final group is reached, if there are not enough letters to make it complete (an even number), add a single null. It is not necessary to complete the full block, however. E. g.,

```
O F T E N  (key)
I N N O V
A T I O N
g w
e b
S A R E F
O U N D x
u i
k e
```

Set the O of the sliding pairs under the indicator A of the stationary alphabet, and encipher IA as GE (opposite corners of the oblong); then SO, going down the whole column to encipher all of it. Then, slide the strip until E-F (key) is under the stationary A-indicator and encipher that column. The resulting cipher is then taken off in five-letter groups as usual.

Finding the period in the Portax is dependent on possible fragments of plaintext which are known (through the N-Z combinations produced from the unchanged relationship of letters) which make sense without showing impossible combinations of letters.

For example, to decipher the following:
SNPOW LBAMP ISCWU OOBXC WKMAT ZKTOW JCBLN CBJGB TAAJD IWUKW HHVZN MNUFM APBJW PCBSX JCJQX TMVUB MDCBJ CGUGR (90)

There being 90 letters in all, if the keyword is five letters wide, there will be 10 rows of nine deep, paired; if the keyword length is six, there will be 7 paired rows plus an additional row of 6 (2 threes); if the key-length is seven there will be 6 paired rows with an additional row of 6 (two threes); if the keyword length is 8, there will be five paired rows plus an additional row of ten (two fives), etc. The cipher at hand will be tested for 5, 6, 7, etc. periods until conflictions result in fragmentary plaintext, or the true period is found.

```
For 5:
S N P O W
L B A M P
    n t u
    e c t  (possible)
---------
I S C W U
O O B X C
  u   y o
  k   t o  (possible)
---------
W K M A T
Z K T O W
z       y
t       m  (questionable)
---------
J C B L N
C B J G B  (nothing to add)
---------
T A A J D
I W U K W
r
m
---------
H H V Z N
M N U F M
    x p t  (Impossible so
    q z a  period is not 5)
```

```
For 6:
S N P O W L
B A M P I S
n   t u r
l   e d s      (good)
-----------
C W U O O B
X C W K M A
  o y s
  s o c        (still good)
-----------
T Z K T O W
J C B L N C
r o   s t o
n y   n d s    (better)
-----------
B J G B T A
A J D I W U
        y
        m
-----------
K W H H V Z    With the known
N M N U F M    values inserted,
  t     p t    now comes an as-
  s     r y    sumption or two:
-----------
A P B J W P
C B S X J C    N-T U R-L (natural)
  n     r o
  f     t e
-----------
J Q X T M V
U B M D C B
  n t o   n
  h u n   r
-----------
J C G - - -
U G R - - -
-----------
```

Setting the slide so that N-A may be used, finds them in the same column, which cannot be utilized until the key-letter is also known. But, setting the slide so that L-S may be used is a different story. With the stationary L, put the slide so that the sliding S is directly under the A-indicator; this gives A-O as the equivalent of L-S, and also shows that column 6, with the last letter of the keyword as S-T. With this setting, go down column 6 and write in <u>all</u> plaintext which heretofore had to be ignored owing to the fact that the first letter of each pair was in the A-M range.

In the third section of paired groups there is NY-NDS, which might be: NYaNDS, NYeNDS. If KB equals -A, and is tested, it is found that A and B are in the same column and until the key-letter is known, cannot be used. With KB to equal -E, this cannot be used either, since E is in the lower row, and B is in the upper row and no oblong results. NYeNDS is definitely wrong; and NYaNDS is the correct one, but nothing may be added for the present.

Looking at the final group of pairs: -NTON -HUN-R (hundr ?) If MC equals -D, again CD are in the same column and cannot be used until the key-letter is known.

Little can be tested with any assistance, so perhaps a trial on the key-word itself will prove something. With T in the final position, various letters which precede it: A C E F H I L N O P R S U, are tried, putting the slide in each case under the A-indicator, to see what pairs of plaintext result. At the E-setting, in group two OM becomes TC, making -OYST/-SOCCU with R in the next following group for OCCUR. Make all substitutions with key-letter E in the fifth column, and it will be seen that the D needed for HUNDR now falls into place. From here out, it should be fun to find the rest.

Problem 17. Keyword length 9.
PFPFWPOSB TRMGDONJO WDPTUTLYB SPMDITYNU WGBWLIPCM LNUAXZCXG
QWBWNKBGW CJCNKTRCB WHXVWKZFU JAALEQIUA SKJEXWKBD PWSACNKUI
ZAMNFK EXVMAM

Problem 18.
NKCNJ MLIIR UWQUX CPNMS RYQET KWBSL KOCLL ZJJSJ YTEWS MXUAD KOJPD
TBGKJ HVHXD SJAMR JNGOW KCLCK LCOLL JBMAR GNTFI BDR (98)

Problem 19.
LHZHP WOTKE DQDUM EMLIA LALSA IDAMD WKPQH NPMVS FIKSB NCFCW BOIIZ
BNMWF WNNSK WNOJX WKJAA JQNWL KBNIB RTUAK NKKNE TUOLS YMCBM N
(106)

Problem 20.
UELAM TMEJQ UALSO AHYQA VNQSX BUBHL JDCPV BIGIL INSNZ BBQYD ISUTA
ELXCG MPHIM BVAKH PKGUF TQKRK EGDWW BLXMT CKFMR SLCOL DEYU (104)

CHAPTER VII. THE NIHILIST SUBSTITUTION CIPHER

Another of the Periodic Ciphers - though not belonging to the Vigenere Family - is the Nihilist Substitution, which employs numbers to represent letters. The numbers are derived from a 5x5 Polybius square, and since this square is used for several different ciphers, an explanation is forthcoming. In order to account for the entire alphabet of 26 letters, in a block of but 25 cells, I-J are generally combines; but occasionally it is found that U-V or W-X occupy the same cell; or, even Q or Z may be omitted instead. A normal square would be, with digits assigned across the top and down the left side:

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

This A is represented by 11; L by 31 and T by 44.

However, all polybius squares are not normal; some contain a keyword, and the time seems right to explain this phase as well, which may also apply to other types of ciphers.

When the term "keyword alphabet" is used, it means that the normal alphabet sequence has been disrupted in some manner. The commonest way of doing this is to choose a keyword, with or without repeated letters. If there are repeated letters, jot down the keyword omitting the repeats and give the remaining letters of the alphabet in their natural order. For example, suppose the keyword: UNITED STATES OF AMERICA is selected; omitting the repeated letters becomes: U N I T E D S A O F M R C with the remaining letters of the alphabet B G H J K L P Q V W X Y Z added. Now, this new or "keyword alphabet" is set up as a Polybius square, thus:

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

The same numerical values are allotted as before, in accordance with the 1-5 at top and left.

If, for some reason a further mixed alphabet is required, a process known as a transposition block is employed. Take for example, the keyword of ten letters: BLACKSMITH, which is set up as:

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

and the resulting alphabet is then taken off by columns starting with 1:

BDVLEWAFXCGYNZSOMPIQTRHU

The Polybius square would then be:

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

Using a norma, or standard square, and using TENT for the keyword as before, and with the same plaintext example, select from the square at the top of this page, the digits to represent each letter of the key: T-44, E-15, N-33 and T-44; write them horizontally across the worksheet. Underneath them, show the message COME AT ONCE, also with their proper digits assigned to each letter:

T-44	E-15	N-33	T-44
C-13	O-34	M-32	E-15
A-11	T-44	O-34	N-33
C-13	E-15	--	--

The two parts of this encipherment, key and letter values are then added to produce the ciphertext: COME: 57 49 65 59; ATON: 55 59 67 77; CE: 57 30.

It will be noted that again each column is a monoalphabetical substitution in itself, and again the reading or value of these letters is dependent on the letters which fall on either side of them.

Finding the period in a Nihilist Substitution is slightly different from that method used with the Vigenere Family; but there are still two ways of doing so, a short way and a long way. The lowest number of any key-letter which may be added to the lowest valued plaintext letter is 11, with a total of 22; the highest combination is two 55's, or 10 (110); and, by the same token, 6, 7, 8 or 9 are not involved in either the tens' or the ones' additions - but they may result in a sum. There are certain phenomena: a cipher 22 can only mean 11 plus 11; and 10 can only mean the sum of two 55's. Zero in the ones' column means that two 5's have been added, naturally; and the same is true of the tens' column. All other sums involve alternates and there is no hard and fast rule to govern them.

The short way of finding the period: scan the ciphertext to see if 30 is to be found in more than one instance. If so, treat it as though it were a repeated digraph, and note its positions in the cipher. Find the difference and factor it. If 30 does not appear, try the lowest numbers represented; then the highest, and follow a similar procedure, as with two 26's or with two 94's.

The long way: assuming that a 3-period is to be tested: compare the 1st with the 4th number, the 2nd with the 5th, the 3rd with the 6th, etc. In doing so, watch to see if two numbers within the 1-2-3-4-5 range may be added to produce first the tens' sum and then the ones' sum. If, at any time, 6-7-8-9 is involved, that period is wrong. For a period of four, test the 1st with the 5th, the 2nd with the 6th, the 3rd with the 7th, etc., in the same manner. When conflictions arise, that period assumption is wrong. And eventually the true period is found.

This explanation may be best understood with an example:

64 38 35 73 29 54 44 30 54 85 25 65 27 39 54 64 29 76 27 57 22 73
45 97 23 50 46 73 38 58 26 59 45 53 27 77 44 47 56 75 38 56 23 59
35 76 47 86 27 48 55 86 48 57 27 50 22 84 58 75 27 48 55 65 29 54
26 58 35 86 38 86 57 58 26 56 38 76 25 57 65 77 58 77 34 57 22 77
37 97 56 49 43 57 25 76 23 48 65 55 38 78 35 30 53

There are 2 30's at positions 8-104; difference 96, factored 3, 4, 6, 8, 12; there are 3 22's, at 21-57-87; differences 36, 66, 30; factored 3 4 6 9; 3 6 11; 3 5 6 10. Six seems constant and may be assumed as the true period. But, if no such clues are offered, what then?

For a 3-period, compare the 1st (64) with the 4th (73). Within the limitations of the Polybius square, both have suitable numbers which may be added to produce each one; 2nd (38) and 5th (29); O.K O.K., again. 35-54, 73-44 and so on until 54-30 is reached. In the ones' digit to produce -4, would require 1-2-3; in the -0 of the 30, would require 5-6-7-8-9; so a 3-period is wrong.

With the above example in a 6-period, set it up as was done with the Vigenere Family ciphers, in block form. Now, scan column 1 for the lowest and the highest numbers therein: 23, 64. To produce the 2-, only 1 may be added to another 1; and this same 1 may be subtracted from the 6- to produce 5-. With the -3, 1 and 2 may be added; and for the -4, 1, 2, 3 may be added. Hence, the key-numbers for column 1 have alternates: 11 and 12. Putting A and B through the normal square brings out A and B. In column 2: the lowest number is 30 and the highest, 59. With 3-, 1 and 2 may be added; with the 5-, 1-2-3-4 may be added so 1 or 2 are acceptable; with the -0 and -9 only 5 may be added, so the alternates of this column for the key are 15, 25, or E, K. Set beside AB of the first column then, the keyword must commence with either AK or BE. (We seem to have overlooked the fact that 30 can only be the sum of 15 and 15, so AK may be discarded). But perhaps some plaintext will reveal which is right, in some other case. Subtract 11 (A) from say, the first three letters in the block: Q, that's a stopper right off the bat; try to subtract K from column 2 to see if U results; if not, then AK is wrong. And after this test is made, 1 shows QG, With BE as the keyword beginning, we get WH ME EI, all possible digraphs. So we are on the right track at last. Continue with this solution, and then try:

Problem 21.
43 46 48 44 55 74 46 68 45 47 35 67 66 54 38 58 76 47 29 77 69 64
56 68 65 46 49 67 48 55 67 65 66 66 27 56 35 64 47 78 76 66 25 46
39 65 47 77 74 58 46 48 38 67 65 68 65 46 58 56 39 35 47 86 45 69
57 48 67 35 57 77 75 48 57 77 39 36 57 65 76 47 56 48 39 35 57 77
56 37 25 64 59 46 54 75 43 66 57 75 39 65 67 68 65 46 48 66 35 65
47 77 54 55 29 68 58 36 47 89 64

Problem 22.
87 46 57 56 62 39 65 85 47 86 78 85 36 63 58 67 53 55 92 26 73 58
45 84 39 05 39 74 66 47 75 37 85 46 65 85 34 73 68 74 49 76 65 46
64 58 82 29 55 86 77 57 55 82 49 83 54 56 56 67 75 46 82 58 65 86
48 84 26 64 57 34 63 39 03 49 75 66 38 84 67 62 57 46 78 68 84 39
03 38 55 87 38

With a Polybius square that is mixed, that is, contains a keyword, the solution of a Nihilist Substitution cipher is slightly varied. While the period may be found, of course, in the accepted way described above, the actual substitutions must be assumed, for it is not known the format used in the square. Hence it will be necessary to convert the whole ciphertext into one long monoalphabetic substitution and then solve it as one would a Patristocrat. Some slight complications may arise in taking a frequency count of each two-digit number, for, in setting up key-letters, two or more alternates may result. However, this may be overcome in time, by establishing or finding certain plaintext which will read properly and show the solver he is on the right track. In such ciphers in "The Cipher Exchange", it is customary to give a tip or two. Here is such a problem with the tip: LAND AND WATER. Hint: try to establish which is "E", and then try to fit in the "E" of the tip into the various places, with corresponding high-frequency letters falling in their correct places from the frequency distribution.

Problem 23. LAND AND WATER
94 63 52 94 66 34 95 54 95 87 45 73 86 44 54 76 04 63 44 05 86 65
93 85 85 96 32 82 67 54 93 85 73 93 66 73 86 65 86 64 75 66 75 85
78 67 63 96 63 63 66 96 79 44 82 86 74 83 64 82 67 74 74 54 95 93
32 05 86 35 63 84 74 83 62 02 67 56 65 97 65 53 43 03 99 43 82 95
94 96 66 06 96 55 86 95 06 63 62 93 67 67 53 76 85 83 54 76 97 43
75 77 85 85 43 96 97 64 74 67 84 87 73 84 56 54 62 66 76 74 66 03
78 33 95 76 97 65 42 62 99 74 95 88 74 83 63 84 56 55 84 97 04 64
32 83 90 55 82 88 85 73 63 72 90 55 62 54 06 55 75 92 98 44 82 84
73 94 33 84 97 33 63 96 85 85

The following table is helpful with the use of a standard Polybius Square. At the top if the key-number, at the left is the plaintext letter; and where they intersent is the cipher-letter or number. In solving, knowing the key-letter and the cipher letter (number), set the key-number and go down that column to the cipher number, and move to the left to find the plaintext number.

		11	12	13	14	15	21	22	23	24	25	31	32	33	34	35	41	42	43	44	45	51	52	53	54	55
KEY		A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	11	22	23	24	25	26	32	33	34	35	36	42	43	44	45	46	52	53	54	55	56	62	63	64	65	66
B	12	23	24	25	26	27	33	34	35	36	37	43	44	45	46	47	53	54	55	56	57	63	64	65	66	67
C	13	24	25	26	27	28	34	35	36	37	38	44	45	46	47	48	54	55	56	57	58	64	65	66	67	68
D	14	25	26	27	28	29	35	36	37	38	39	45	46	47	48	49	55	56	57	58	59	65	66	67	68	69
E	15	26	27	28	29	30	36	37	38	39	40	46	47	48	49	50	56	57	58	59	60	66	67	68	69	70
F	21	32	33	34	35	36	42	43	44	45	46	52	53	54	55	56	62	63	64	65	66	72	73	74	75	76
G	22	33	34	35	36	37	43	44	45	46	47	53	54	55	56	57	63	64	65	66	67	73	74	75	76	77
H	23	34	35	36	37	38	44	45	46	47	48	54	55	56	57	58	64	65	66	67	68	74	75	76	77	78
I	24	35	36	37	38	39	45	46	47	48	49	55	56	57	58	59	65	66	67	68	69	75	76	77	78	79
K	25	36	37	38	39	40	46	47	48	49	50	56	57	58	59	60	66	67	68	69	70	76	77	78	79	80
L	31	42	43	44	45	46	52	53	54	55	56	62	63	64	65	66	72	73	74	75	76	82	83	84	85	86
M	32	43	44	45	46	47	53	54	55	56	57	63	64	65	66	67	73	74	75	76	77	83	84	85	86	87
N	33	44	45	46	47	48	54	55	56	57	58	64	65	66	67	68	74	75	76	77	78	84	85	86	87	88
O	34	45	46	47	48	49	55	56	57	58	59	65	66	67	68	69	75	76	77	78	79	85	86	87	88	89
P	35	46	47	48	49	50	56	57	58	59	60	66	67	68	69	70	76	77	78	79	80	86	87	88	89	90
Q	41	52	53	54	55	56	62	63	64	65	66	72	73	74	75	76	82	83	84	85	86	92	93	94	95	96
R	42	53	54	55	56	57	63	64	65	66	67	73	74	75	76	77	83	84	85	86	87	93	94	95	96	97
S	43	54	55	56	57	58	64	65	66	67	68	74	75	76	77	78	84	85	86	87	88	94	95	96	97	98
T	44	55	56	57	58	59	65	66	67	68	69	75	76	77	78	79	85	86	87	88	89	95	96	97	98	99
U	45	56	57	58	59	60	66	67	68	69	70	76	77	78	79	80	86	87	88	89	90	96	97	98	99	00
V	51	62	63	64	65	66	72	73	74	75	76	82	83	84	85	86	92	93	94	95	96	02	03	04	05	06
W	52	63	64	65	66	67	73	74	75	76	77	83	84	85	86	87	93	94	95	96	97	03	04	05	06	07
X	53	64	65	66	67	68	74	75	76	77	78	84	85	86	87	88	94	95	96	97	98	04	05	06	07	08
Y	54	65	66	67	68	69	75	76	77	78	79	85	86	87	88	89	95	96	97	98	99	05	06	07	08	09
Z	55	66	67	68	69	70	76	77	78	79	80	86	87	88	89	90	96	97	98	99	00	06	07	08	09	10
		A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

NIHILIST NUMBER TABLE

CHAPTER VIII. RECOVERING ALPHABETS

Before going into the Quagmire series, it might be well to explain how to recover keywords in many of the cipher types. In the Aristocrats, or Patristocrats, often these types are marked as "I", "II", "III", or "IV" after the title, and some eben have an "M" added. While the type is always given with the Quagmire, the "M" is not shown, and the solver has to determine that for himself.

I. This means that the plaintext alphabet contains the keyword and the ciphertext alphabet is the normal sequence as:

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

II. This is just the reverse with the keyword in the cipher alphabet:

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

To solve either of these, only some of the letters are found to be substitutes, in solving, and the rest have to be worked out. For either I or II:

```
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 - X Y Z - I N D - - O R M A B - E F G H - K - - -
```

Knowing that the keyword alphabet uses a keyword first, eliminating the repeated letters and then using the remaining letters, some guesses may be inserted automatically as:

```
U v X Y Z - I N D - - O R M A B c E F G H i K l p q
  w                             d               p q s
                                                q s t
```

and with a bit of juggling of assumptions the missing letters may be placed for the keyword WINDSTORM in the above.

III. This indicates that the same keyword is used in both of the alphabets:

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

It will be notices that each alphabet is identical with the other, but at a different spot; hence, any fragmentary substitutions will have to agree in that sequence somewhere; and, by this knowledge, this entire alphabet may be recovered, e.g.:

```
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
X - Y J O - - - B R Z W - U S A - K D E F - - - P -
```

The obvious place to look for as an opening wedge, is JK, PQ, or VWXYZ, the least-used letters in a cryptogram or cipher, if the latter uses this sort of an alphabet. Test each spot separately, and if the substitution offers a logical sequence - with letters omitted for a keyword - accept them. JK-DR, not bad. PQ, only P is shown and this is not enough to work on. VWXYZ, no V, but WXYZ-LACK, which looks fine. Hence on a worksheet, set up:

```
LACK             WXYZ
WXYZ and then, --P- which unfortunately doesn't help. So, now set
up:  -P-R             -Y-J
     LACK  and again -P-R testing each new fragment obtained. The
```

-P-R suggests -PQR, and the -Y-J, as -YZJ, the J starting the keyword if this is true. By returning to WXYZ and adding J, we get:

```
LACKD              -PQRS                      -YZJO-N
WXYZJ  and again LACKD  and still again -PQRSTU and then continu-
ing:
      LACKDEF   -PQRSTU   -YZJO-N
      WXYZJO-   LACKDEF   -PQRSTU  and finally:

             LACKDEFghimPQRSTUVWXYZJO-N
             WXYZJO-N-B-ACKDEF---P-RS-U  which results in
```

JOHNBLACK as the keyword and it appears in both alphabets.

IV. A IV-type indicates that a <u>different</u> keyword is used for each of the alphabets:

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

The general procedure of recovery is the same as III. Here, fragments are linked so that they contain letters of the alphabet sequences with gaps (for the keywords) and then continuing in the expected order. For instance:

```
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
O L X S N Y Z - R - - A - W T - - M C D F - V - I -
```

JK gives nothing, nor PQ, nor even VWXYZ. Hence, some other spot has to be examined. What about LMNO in the lower alphabet?

```
B R E A     I   O   W N S F G L   S D   U     Y
L M N O p q r s t u v w x y z a b c d e f g h i j k

B R E A     W N C F G     U v w Y z (then the start of keyword)
L M N O     V W X Y Z       w x
                          F G H I     or:

U v w Y Z B R E A - - D O - - W N C F G h i j k l m p q s t
  w x
F G H I J L M N O p q r s t u V W X Y Z - R - - A - - - C D
```

The upper keyword now looks like BREAKDOWN. Let's see what develops in the lower one:

B R E A K D O W N C F G H I J L M P Q S T U V X Y Z
L M N O p S T V W X Y Z - R - A - - - C D F g h I j
q k with the missing letters: B E K U (P-Q) (J-K). It isn't long before the keyword BREAKUP is revealed.

When an "M" is annexed to the significance of a keyword recovery it means that a transposition block was used to set up this alphabet, and two such alphabets may be devised. The first, is by taking off by columns in a normal 1-2-3- etc. order; the second by taking them off as was done with the Nihilist Transposition Cipher (Volume I, Chapter VIII):

1.

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

and the resulting alphabet:

BCJSUDKVOELWYFMXAGPYNHQZTIR

2.

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

and the resulting alphabet:

AFCVEDYIQKWLGOHRPSMTNUJZBX

The longer the keyword, the shorter the depth of the block and the harder to recover, but it can be done. Solution depends on separating the segments, which are handled as a unit; that is, allowing one (or two) letters to appear in a keyword, then the following letters to be in normal sequence with gaps, of course, as: B d l y, E f m z, etc. Here the BE would be in the keyword, and DF LM YZ would be the expected sequences to follow such a keyword. After the sections are determined, each is written vertically with a link tested for the final letters. As an example:

C X J S ' E F P W ' I T G Q Y ' M D L V ' N A H R Z ' O B K U

The S W Y V Z U lend themselves agreeably to such an arrangement and taking Z, then Y, then W V S in that order and writing them vertically:

			I	N
C	O	M	E	T	A

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

Numerical keys sometimes may be recovered to a keyword, but more often only random sequences are used by a constructor. Since obtaining such a keyword does not affect the solution, and such a key recovery is not required with the solution, some readers of "The Cryptogram" prefer to ignore the following. On the other hand, it is often fun to try to obtain a legitimate keyword in this fashion. Given: 5 1 3 7 2 6 4 (7 units) Since there are 26 letters in the alphabet, divide by 7 and show four (or more as the case may demand) under each digit, thus:

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

The test is to pick out just which letters in a row, when arranged in linking form, will give a legitimate word. When this is done, the keyword obtained might not be the exact one which the constructor used, but it will serve its purpose.

KEYWORD RECOVERY PROBLEMS:

Type I.
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
S - V W X - Z - R - - E - U L B - H I J K - N - P -

Type II.
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
H - K M Q R - - V - - Y Z P L - - O N I - - D - F -

Type III.
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
G H - O - Q - S - A B - U - - F X - Z - B M - N - J

Type IV.
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
L - O B G C - A Y - - H Z J M N - D R X Q - T - V -

Type "M" using a Transposition block.
1. B H T C M X E D O Z I K W L J V P F Q R A N Y U G S

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

3. A F T E C Q G B P Z I K W M O Y N H V R D S U L X (25 letters; this is a 5x5 Polybius square and I-J occupy the same cell)

In recovering some Polybius Squares, for example, with the Phillips Cipher (Volume I, Chapter XX), if the transposition block has been used to scramble the alphabetic sequence, it presents a formidble problem of recovery. Since the diagonals of such a square are known, and they must be kept as such, shifting rows and columns will eventually bring about a logical sequence from which to proceed. But remember, if a row is moved, say from the 5th position to the 2nd, then the column must be moved in like manner. Not to do so, results in the wrong diagonals, and the square cannot be recovered, then. After every move of row/column check to see that the original diagonals are held; if not, go back to the basic square and start over.

Constructors are known to complicate a 5x5 square when they can. Sometimes a route is used, as explained in Volume I Chapter VI in the Route Transposition Cipher; sometimes a mixed alphabet is employed which has been put through a transposition block. If you are A "recovery alphabet addict" test your wits against the constructor in each case.

CHAPTER IX. THE QUAGMIRE CIPHERS I AND II

The next three chapters will deal with the Quagmires, periodic ciphers similar to the Vigenere, but using one or more mixed alphabets instead of two normal ones. There are four Quagmires: I, II, III and IV respectively. Since "I" and "II" are the least complex, they will be handled in one chapter.

In "I", there is a stationary mixed alphabet for the plaintext against which is slid a normal unmixed alphabet for the ciphertext. Two keywords are needed for the encipherment and decipherment: the one which is used in the mixed alphabet; and the second which represents the width of the block (period). An indicator is also required; it may be the A of the stationary alphabet, or it may be any other arbitrary letter. Under this indicator will appear the "second" keyword letters. Using "QUAGMIRE" as the alphabet keyword for the mixed alphabet and the keyword CASH, encipherment is:

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

To encipher in Type I: slide the normal alphabet until the first letters of the keyword falls directly under the indication: C under G (as above); write in those letters which fall below the plaintext in this first alphabet for the ciphertext. Next, slide the normal alphabet until the second letter of the keyword falls below the G-indicator: A and encipher this column; etc.:

```
C A S H key  C A S H
W E W O PT   V E L W CT
R K T O      F M J W
M A K E      D Z E L
```

Solution of the Quagmires is a bit more involved, but research has provided some excellent ways in which to gain entrance and continue to find plaintext. The procedures for I and II are similar, but for III and IV are vastly different, so will be handled separately. As with other ciphers, ample tips are given, fragments which contain repeated letters for easy placement.

In working with all of this series, first the cipher is written into the proper size block and then a duplicate (blank) block is drawn up to the right (or left) for the encipherment. Below these diagrams is drawn a block with the normal alphabet at the top, and enough rows are left below as indicated by the keyword length, and the whole diagram is enclosed in lines (or not, as the solver chooses). The cipher is first written into the block and the tip placed in the accompanying blank block (on the following page):

The next step is to go to this skeleton block and write in for each <u>known</u> substitute the equivalent letter in each column, as well as into the tableau below. Check all known values and be sure that all ciphertext letters receive the correct plaintext. An oversight may lead to later confusion.

Since this is Quagmire I, the alphabet at the top represents the <u>ciphertext</u>, whereas the letters in the block are the <u>plaintext</u>.

For example, row 1:

```
Q - T   X - H   H - I
c   p   c   p   c   p
```

Do the same for each of the eight columns and the finished block is shown below the enciphering diagram:

-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
P	Y	E	J	I	Z	C	Q	-	-	-	-	-	-	-	-
F	T	A	C	W	I	N	W	-	i	-	-	-	i	-	-
H	B	J	V	F	I	Y	G	i	-	-	t	-	i	-	t
A	G	Z	R	F	C	M	R	-	-	-	-	-	-	-	-
Q	Q	S	E	V	C	N	T	t	-	-	-	-	-	-	-
H	B	T	J	H	B	C	K	i	-	-	-	-	-	-	-
B	O	T	M	G	B	J	R	-	-	-	-	-	-	-	-
L	C	Y	Y	D	I	E	X	-	-	E	X	H	I	B	I
Q	T	G	Q	S	G	D	G	T	I	O	N	O	F	A	T
X	M	Y	V	N	X	R	Z	H	L	E	T	I	C	S	K
H	M	U	G	R	E	R	O	I	L	L	-	-	-	s	-
N	Q	T	H	D	N	B	F	-	-	-	-	h	-	-	-
E	W	V	Q	V	Y	J	D	-	-	-	n	-	-	-	-
L	Q	B	V	D	F	B	G	-	-	-	t	h	-	-	t
X	Q	W	D	G	B	R	B	-	-	-	-	-	-	s	-
M	L	K	C	K	Y	O	P	-	-	-	-	-	-	-	-
P	Q	J	G	F	F	L	X	-	-	-	-	-	-	-	i
A	M	Y	I	I	Z	S	F	-	l	e	-	-	-	-	-
N	Q	Q	V	H	R	O	P	-	-	-	t	-	-	-	-
P	L	S	Q	N	M	S	C	-	-	-	n	i	-	-	-
Q	J	Y	V	D	N	A	P	t	-	e	t	h	-	-	-
B	X	X	U	L	N	B	G	-	-	-	-	-	-	-	t
X	Q	J	J	V	O	G	M	-	-	-	-	-	-	-	-
H	N	U	J	X	F	N	G	i	-	l	-	-	-	-	t
P	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Ø	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	CT
1								I									T							H			
2													L							I							
3							O														L				E		
4																	N					T			X		
5				H										I					O								PT
6							F		I															C			
7				A	B												S										
8							T																	I	'	K	

A peculiarity of both I and II Quagmires, is that these boxed alphabets will be identical in sequence, but at different settings under the stationary alphabet at the top (Ø). This is due to the keyword used vertically; and so these skeleton alphabets are apt to have one or more letters in common. For instance, in 1, there are I T H; and in 8, there are T I K. By checking it will be found that in both cases there are nine spaces between the I and the T. So that K, two spaces to the right of I - in 8 - may be added to 1 two spaces to the right of that I. Follow this reasoning for all alphabets, and add all of the possible letters. The working block will then be:

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

Now, return to the deciphering block, and write in all of the new substitutions which are found in the above tableau. This will look like:

```
- - - - - - - -
- O - - - - - L
F I - H - I - -
I - - T - I - T
T E - - - - - -
I - - E - L - -
- - - I L L - -
N T E X H I B I
T I O N O F A T
H L E T I C S K
I L L - N - S -
- E - - H O - -
E - - N - - - -
N E I T H E - T
H - - - - L - N
O - T H E H - -
- E - - - E - I
L L E - - - - -
- E C T - T - -
- - - N I N - O
T H E T H O - -
- N - - F O - T
H E - E - - - C
I - L E - E - T
-
```

There are now two alternatives: the one to try to fill the remaining gaps of the plaintext and add new letters to the block; or second, using the knowledge gained in Chapter VIII - "Recovering the Alphabets" - and try to reconstruct the entire keyword used in the mixed alphabet. If this can be accomplished, it means a short-cut, and the solution is that much quicker. Taking any one of the alphabets from the numbered rows:

```
L---EF-I-K-NO---T--X---'CH--
 aab  g J l  pqr uu YZZ
 bbc  h   m   rs vv     ' Keyword start ?
  od             w
```

J, Y and Z may be inserted into seven sequences, and if new plaintext results, so much the better.

Finish this cipher.

With the Quagmire II, the same general procedure follows, except that with the basic table (or rows), the stationary alphabet is the plaintext one and is normal; while the sliding alphabets are the ciphertext ones and are mixed. The resulting alphabets will still run parallel with the same sequence of letters throughout; and the keyword will show up under the selected indicator.

Problem 24. Type I. IT IS ONE OF THE MOST POPULAR; period 6
QNTZHP QNBLOO PZYBOF PGIAHC UPIOMD XLJQOZ SHHXMI LNUQGE FNYALD
UJTEIY RZCROZ AWHXFG HSGLGL PYTSLH KYGEVO UJGXMH BLGONY LKHQGZ
UJGEZX LLUMGD FWBSZB OYCKJW INLQUD LKJMVH ALXQUB LYCIOP PYCOHX
HZMQRX AZRMSY INHZFA JHHDSX OZT

Problem 25. Type II; A FORFEIT TO TRAVEL ACROSS THE; period 7
BSERPFO GDHHVTG CEIRFWG DSMUUAG ZNDSFSW ZDHPHBQ AQGAZMC VDPQSME
FBGYLFY KWNOSMQ FWSMXOW PDVAEXZ FJGGIFC RCVTLWD ZSNIZWC FQNZPWD
XEYHVNB HSAUNND ZETMCVQ ZMNONDW LQPMTLG RMMTEWN TUNRNDW USXHRHX
ARFMFXG TWSTMLN TLVV

CHAPTER X. THE QUAGMIRE CIPHER TYPE III

In the Type III Quagmire, the encipherment is done with a mixed pair of alphabets, one representing the plaintext and the other the ciphertext, but both will contain the same keyword; and also requiring an extra keyword for the width of the block. For examplw, suppose the keyword is OCEAN; and the mixed alphabets are based on:

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

and the indicator M, is chosen. For the encipherment of the first column, slide the lower alphabet until the O-key letter is directly under the M-indicator, and at this setting, encipher the entire first column; for column 2, slide the lower alphabet until the C-key is under the M-indicator, etc.

Decipherment follows a definite pattern, and an ample tip of the plaintext is given in "The Cryptogram" for ciphers of this type to get solvers started. For instance, following is a cipher of a six width (period) and the tips: ORTOMARKTHESITEOFABATTLE; and HAVEBEENERECTED are given. Placement of the first tip, once the correct period has been found (Kasiski - Volume II, Chapter 1) is determined by setting it up as - showing the repetitions:

```
ORTOMA
RHTHES
ITEOFA
BATTLE
```

Other plaintext letters in each column are inserted which are the same as those already known, and the second tip may be found from these additions in the enciphering block:

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

(continued)

Again, a tableau is set up, with the top alphabet normal, and six rows beneath it (the width). When completed, check from tableau to decipherment to see if all ciphertext letters have been given plaintext values:

Ø		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z		
1	'	Z				R													A	U								'	PT
2	'		W			L				Q						F			M									'	
3	'	C		F		M						S							V		A							'	
4	'					P			W												V							'	CT
5	'	Z				R			Y						I	P					X							'	
6	'				C	K	D						G	S									U					'	

Ratios, now enter the picture (which did not apply to I and II); Ø-alphabet letters are to be linked with each of the other rows, in turn, and the equations listed as Ø-1, A-Z, E-R, R-A, S-U for row 1. Make a new table, first with Ø-1 and its corresponding values, then Ø-2, then Ø-3 and so on, as:

Ø-A E R S'
1-Z R A U'

Ø-B W I O R'
2-W L Q F M'

Ø-A C E K R T'
3-C F M S V A'

Ø-E H T'
4-P W V'

Ø-A E H N O T'
5-Z R Y I P X'

Ø-D E F L M V'
6-C K D G S U'

The (') means that these letters are now found in the block, and as fast as this information is utilized, the letters should be underlined, to prove that they have been taken care of; if later, additional ratios appear but cannot be placed in the block, there are not underlined, until they can be used.

Now, look at Ø-1's ratios, and check each to see if the same ratios appears in any of the others, not only in the vertical position, but in the horizontal as well, in either the top or the bottom rows or sequences.

Ø-1, A-Z is found to be identical in position, with Ø-5, so this means that the substitutions in these two alphabets are identical; and the letters appearing in one may be transferred to the other. After this is accomplished, check with the deciphing block to see if any new plaintext may be added. In 1, for example, H-Y, N-I, O-P T-X may be added; in 5, R-A, S-U are new. Also add these new ratios to their respective listings, above (or, mark these two identical lists with (A or 1). This means that any new ratios added to 1, must also be added to 5. Since they are now placed in the deciphering block, underline them, and draw another separating line (or ') after them.

Now checking further: from Ø-1 with the other rows:

Ø-E   Ø-E R   Ø-E L
1-R   2 L M   or 1-R M, so add L-M to Ø-1

Ø-E   Ø-E R   Ø-E M
1-R   3-M V   or 1-R V, so add M-V to Ø-1

Ø-L   Ø-L M   Ø-L G
1-M   6-G S   or 1-M S, so add G-S to Ø-1

Take Ø-2:

Ø-E   Ø- E L   Ø-E K   Ø-A   Ø-R T   Ø-A T
2-L   6-K G   2-L G   2-V   3-V A   2-V R

Ø-T 3-A	Ø-A T 1-Z X	Ø-T X 3-A Z	Ø-R 2-M	Ø-R M 1-A V	Ø-R A 2-M V
Ø-T 2-R	Ø-R T 1-A X	Ø-T X 2-R A			

Take 3, 4, and 6 (5 is a duplicate of 1)

Return to the chart and add these new ratios, at the same time, checking with the block to see if new plaintext is found. This chart will now look like:

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

These alphabets appearing within the above table are nor normal, nor are they identical in sequence as they were in Types I and II, simply because a mixed alphabet was used in both plaintext and ciphertext alphabets. Hence it will be necessary to either: 1. Try to reconstruct the keyword from this skeleton; or 2. Establish more plaintext in the block by assumptions in sense.

Following the technique explained in Chapter I on "Recovery of Alphabets" as they apply to a mixed keyword type III, try to build up fragments from Ø and the various rows; if this keyword recovery is attempted, both sequences in Ø and in the table itself will be identical, with the rearrangement of letters applied. Therefore, fragments' found in one, may be tested in another. (Capital letters below indicate known values; small letters, are assumptions):

Ø	T	H	A	-	C	-	F	-	-	-	-	V	W	X	Y	Z	-	O	-	-	C	D	F
1	X	Y	Z					t	h	a		c		f									
2	R		V							m		t	h	A	-	c	-	f					
3	A		C		F					v	w	x	y	Z							F		
4	V	W	x	y	z																		
5	X	Y	Z					T	H	A		C		f									
6							D					U										C	D

and, combining:

Ø	O	-	-	-	-	-	-	-	-	L	-	-	-	R	-	V	W	X	Y	Z
1	P									M	-	T	H	A	-	C	-	F	-	-
2	F	-	-	-	P									M	-	T	H	A	-	C
3								L	-	-	-	R	-	V	W	X	Y	Z	-	O
4																				
5	P									M	-	T	H	A	-	C	-	F	-	-
6										G						U				

and, finally, with assumptions:

* (indicator)

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

It is soon discovered that JOKESMITH is the keyword, and under the S-indicator, that keyword is UNIQUE.

Problem 26. CANBEOBSERVEDATONETIMEFROMANYPOSITIONONTHEEARTHWHEN
VIVLKSWZF LIZRWSNSO SDRWSVHKK HLTFWBSZA PABRFCGDC XRBBGNIFE
AKWLGKXGH SCQZWRDTN JORYPXISO SYVCKVVFE VLHCXXDTM XDMMLKYDR
PBBFOVLGB LDBRUEIEX LNTSRTDZA JCASFKVFJ SFERCLGDC XLBYGABKV
SCPVWVLSO SLARLHTTI PKEZWKMSL GFXYRJTAX SFPLNFWSB UKZVZFIQA
HBQZTHZLI RLBB

Problem 27. DISAPPEAREDASCURRENTEXAMPLES; POPULARINNOVATION
VQMRFAA XZASFQO ZNJTTYO DDMMLQR BKLDIJO AZMFNSP VQNQJDD BZAQFGN
KHZMLQD WLJWAPF JNQNMBR BOVUKPX WRHWIDF WHQYPPJ RJTVJEN AHCNNAX
GBLMLQD RFAQFQE LQQCFNN LRMYHYK TAQZFLX GBKCDPQ FZMTKRV KEVNZQB
VTVCZRB X

Problem 28. THEDISTINGUISHINGMARKSOF; INFORMATION
GNNIVTZ OKUHKXS NYXQPOC AOYTJMS ANKHDEQ FINQKOO NLXQPEJ TABQPCJ
TALVHQG SERUQUJ MLNUKET SXQUPSJ RLUETEV WBYUKXX OEPGICN UPNKJTN
SEPWIYJ TKIYTLT SXLVIVA TPUUYAH WYAZVYE QVKUTTG FXFQKOP TSWXMYC
MBALRXZ FHZPIHJ DSYVIC

CHAPTER XI. THE QUAGMIRE CIPHER TYPE IV

The Quagmire Type IV Cipher uses two mixed keyword alphabets, each containing a different keyword. An indicator is also used, under which another keyword, the width of the block (period) is placed.

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

This setting is for the A-indicator, with V the first letter of the period keyword.

Encipherment is done by the same method as that employed with other periodics.

Decipherment needs the Kasiski method for finding the period. Finding actual plaintext values resembles in some ways the procedure of Type II with ratios, but this time, the Ø alphabet is ignored and the ratios are found in the box itself, vertically and horizontally. Ample plaintext as a tip is given in "The Cryptogram" as a rule; but assumptions must be made to fill in gaps between recovered letters. This is done, frequently, by trying to establish E T A, etc. The more frequently used letters of the alphabet in a given column, by guess, or by taking a frequency count of the column and fitting these letters to it.

For example, here is a Quagmire Type IV cipher with an 8-period; with the tip written in, and all duplicate substitutions of a column also marked:

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

Prepare a box as was done in Type III. Write in the normal alphabet at the top which represents the plaintext alphabet. Below is, list eight rows (numbered), and assign to each plaintext letter of the above deciphering block, the proper ciphertext letters in each row. Then, prepare a table showing the ratios of each row with every other row: 1-2, 1-3, 1-4, 1-5, 1-6, 1-7, 1-8; 2-3, 2-4, 2-5 etc.

```
1-R S      1-         1-S        1-B C      1-B R     1-S       1-C K R S
2-Z U      3-         4-N        5-K L      6-W J     7-F       8-P F Y R

2-         2-Y U      2-G        2-Y Z      2-U       2-Y Z U
3-         4-J N      5-E        6-I J      7-F       8-X Y R

3-X M      3-X M      3-         3-X M      3-
4-F O      5-S Y      6-         7-O D      8-

4-D F O    4-J        4-I N F O  4-J N
5-N S Y    6-I        7-P F O D  8-X R

5-K        5-S Y      5-L        6-K        6-I J     7-F
6-W        7-O D      8-P        7-C        8-X Y     8-R
```

Next, each vertical pair will be taken in turn, to see if any other ratios may be obtained for that pair, vertically or horizontally from any of the other notations, either from their top or bottom rows:

```
1. 1-S   4-D F   so 1-S F
   4-N   5-N S      4-N D

   1-F   4-N O   so 1-F N
   4-D   7-F D      4-D O

2. 1-S   1-S F   so 1-S N
   7-F   4-N D      7-F D

   1-S   4-F  (a reversal, so
   7-F   5-S   these two rows are
               marked "A")

3. 1-R   2-Z U   so 1-R U
   8-Y   8-Y R      8-Y Z

4. 2-Y   6-J  (another reversal
   4-J   8-Y   mark it "B")

5. 2-Y   2-Y X   so 2-Y J
   8-X   4-J I      8-X I

   2-J   4-J  (identical,
   8-I   6-I   "C")

6. 4-F   1-S Y   so 4-F S
   7-O   7-F O      7-O Y

   4-F   3-X M   so 4-F X
   7-O   4-F O      7-O M

   4-O   1-N Y   so 4-O Y
   7-D   7-P F      7-P I

7. 6-K   4-I N   so 6-F N
   7-P   7-P F      7-P I

   6-N   2-U K   so 6-N U
   7-I   4-N I      7-I K
```

8. After each new value has been found in the table, always follow these procedures:
   a. Place new letters in the deciphering block IF one of them already exists there in the proper row; otherwise do not try to use this pair.
   b. Check with the deciphering block if a new letter is placed in the box under the proper plaintext letter to see if any new plaintext results.
   c. Add any new ratios to the table.
   d. Check these new ratios for more ratios.
   e. Underline placed letters (pairs) from table to box.
   f. Draw a vertical line after all checked ratios.

9. 1-S F N
   4-N D O   D appears in row 4. so F may be added in row 1 under Ø-H, which gives H-plain in the deciphering block. Add ratio: 1-F / 5-N and underline.

   1-N
   4-O   O appears in row 4, so put N in row 1 under the Ø-T. Three plaintext letters are added to the block.

   Add ratios: 1-N / 3-M   1-N / 5-Y   1-N / 7-D   Check and underline if needed.

   1-N / 7-D is already there, so just underline.   1-Y / 7-O   O is in row 7, so put the Y in Ø-1 under R.

   Add ratios: 1-Y / 3-X   1-Y / 4-F   1-Y / 5-S

10. Continue in this manner for all new ratios, check for plain-text values, etc. The final table of ratios will then be:

```
1-R S B'
2-Z U P'

1-N Y J Z U P K I L C' (C)
3-M X I Y R O J F K B'

1-S F N Y R'
4-N D O F K'

1-B C F N Y D O P M' (D)
5-K L N Y S O F I X'

1-B R S X'
6-W J M C'

1-S N Y R J P' (A)
7-F D O B W Z'

1-C K R S U L M N F B'
8-P F Y R Z I J K B O'

2-Y'
3-Z'

2-Y U X R M Z O'  (B)
4-J N I M P K W'

2-G P'
5-E K'

2-Y Z N R U X M P' (F)
6-I J P L M F O W'

2-U X Z'
7-F P B'

2-Y Z U J N P F I L C' (C)
8-X Y R I M O J F K B'

3-X M Y Z N R U P' (F)
4-F O I J P L M W'

3-X M N P C L B'
5-S Y Z J M X L'

3-R Z N'
6-K I O'

3-X M R'
7-O D C'

3-M J F Z K B N'
8-K F C X I P L'

4-D F O P B W' (A)
5-N S Y Z R J'

4-J Y Z U N K I P L C' (C)
6-I X Y R M J F O K B'

4-I N F O S X Y K L' (D)
7-P F O D Y M N B C'

4-J N P O K D B L' (E)
8-X R L K Y B N Z'

5-K Z'
6-W O'

5-S Y'
7-O D'

5-L X R K Y B N Z' (E)
8-P J N O K D B L'

6-K F N U M J'
7-C P I X F B'

6-I J N M W O K' (B)
8-X Y U R O L Z'

7-F D B K C'
8-R K Y S Z'
```

(A) is a reversal
(B) is a reversal
(C) is identical
(D) is a reversal
(E) is a reversal
(F) is identical

Whenever a new value is added to one of these rows, check and write it into the paired one; IF one of these letters already appears in its proper row.

At this point, using the known values, an attempt will be made to recover both keywords, instead of just one as was done with Type III. In row 2: X Y Z looks promising. Below, is the forced method, with the small letters showing assumptions, or actual known values after the assumptions have been recorded:

Ø	A	I	N	c	-	o
1			R	u		s
2	X	Y	Z		r	u
3	Y	Z		r		
4	I	J	K	l		n
5						
6	F	I	J	k	l	m
7	P		B	c		f
8		X	Y	z		r

Working first with the XYZ and then with FIJKLM, both keywords may be found. Had the normal sequence of Ø been kept, this would not have been possible; but with a possible keyword lined up for Ø-alphabet, the rows in the box will follow the same pattern as they did in Type III, all containing the proper sequence.

Problem 29. WASNOTALWAYSCONFINEDTO; WEREFASHIONEDFROM
QANKCCOX ZXJLODEY YAKMTDEQ JWKMOHQL YXRCDIQM QQFLESAN OOCWDSAF
AZKXMIBY CMKAFQWY QQDGODLT OOOETDET SXRYEEZJ VXOECPFX AOOEOEON
EXENMZZJ VOUNXPOQ SMZCCSJD PXEOJBWL ODYIJRQU ZRINWUJA ZRKIPZOU
VLAZMPEJ ZSPTFGEQ TGECLIET BXJWSUZL YWKOCZBU AGFWSQ

Problem 30. BEINGAFOCALSITEFORNEW; FORTHEENTERTAINMENTOF
NJWXDLECP NKEHWUVMW UFCUOHFHZ NUVMCEVTY VPZOLBFKQ OAGHRENXR
QUQZPBUVC UFKDRGWHT NYWQWEGZA IPXTYHBAQ JISONBVIQ QAROYDMRY
JBVXNIDXY JKTOQWCBZ NGVXZEYRK VYZKPWCWW BDMHAPVHT TMXQNEFVV
NGUFYENHZ BXZUDBFMA BJZFSKVGW PILQIFBQY JKUHRBBAW UIVWCYYZZ
JQUVZBHVJ QYOOPW

Problem 31. WHENMORETHANTWENTYTHOUSAND; ALONETHEWEALTHYPAID
BZYJHJH BZHPQAR BZYZVVI KYYCJIT MQVKMJV SLRKPNR VECCOSE PYPVVAR
FLADDJV XWAOLNH SZYRSAG DYXOJIP DXWSLON UBHRZUY XYPUVLG RPXOJKD
GEAOESQ DFYYVSC XKPZXTI JWVOECU DKROEAE DYXCRNY VYXSTQU JKHRNAC
FCWKPND DXVAENH QUYNDFI QNHUVLH GMYFQOY ZBXFLOI ZBQJGSE JMHZLNG Q

CHAPTER XXII. THE AUTO-KEY CIPHER; THE RUNNING KEY CIPHER; THE INTERRUPTED KEY CIPHER

The Auto-key, Running Key and Interrupted Key Ciphers are used with the Vigenere, Variant, Beaufort, Gronsfeld, Porta, or the Nihilist Substitutions' basic principles. The overall picture is the same; its handling, however, depends on that particular system involved.

With the Auto-Key, a keyword is used, which is followed by the normal plaintext; and then, this keyword plus the plaintext, acts as the key; below it, the same plaintext is repeated which constitues the plaintext, and with the proper encipherment becomes the ciphertext. For example:

(Vigenere):
STOCKING'THENEWSERIESOFHYDROGEN .... key
THENEWSE'RIESOFHYDROGENBOMBSWER .... plaintext

LASPOEFK'KPIFSBZCUZSYSSIMPSGCIE .... ciphertext

Decipherment depends on using the tip, placing it, and working forward and backward to recover the entire plaintext.

With the Running Key Cipher, a lengthy plaintext is usually divided in half and written in two rows, one under the other; the tophalf acts as the key, the bottom hald as the plaintext and the encipherment as the cipher:

(Porta): OFFICERS AND DIRE - CTORS OF THE LOCAL
OFFICERSANDDIRE .... key
CTORSOFTHELOCAL .... plaintext

WEMAEMNKUXZATVN .... ciphertext

With the Interrupted Key Cipher, the keyword may be disrupted in either of two ways: 1. Each word of the plaintext may be enciphered by a separate and successive letter of the keyword; 2. The plaintext may be enciphered with 1, 2, 3 (or more) letters of the keyword, returning to the first letter each time a pause occurs. Here is a Beaufort in both ways, with the keyword: SNIPE.

```
1.   S      N        I     P         E          key
    THE COMPANY WAS COMPRISED OF         plaintext

    ZLO LZBYNAP MIQ NBDAYHXLM QZ         ciphertext

2.    S   N     I        S       N          key
    THEC OM PANYWA SCOMPOS EDOF          plaintext

    ZLOQ ZB TIVKMI AQEGDEA JKZI
```

Decipherment of these three types of ciphers is made by a tip which has to be slid along the ciphertext and fragments of the plaintext (or key) obtained in various positions; the correct placement will reveal legible text in the opposite row. When the proper placement is located, additional plaintext (or key) has to be recovered by working with a "trial and error" method both forward and backward.

As an illustration, here is a Running Key Vigenere, with the tip RSDURINGA:

SNKSC YOLDK VJHQF VGZOS IDVMG ZNRLH YCTMG YTZRR DIHSP GXSGK WAFRV IBJIU AEUKX EDEPB XYYGX FN

Set up the cipher on a worksheet single-spaced and by using the tip as the key (or the plaintext) put it through the Vigenere slide system; as impossible combinations appear, check off that decipherment and proceed with the ones that seem logical.

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

Then, setting up the recovered halves of the cipher, proceed to try to recover the rest on either side of the known text;

```
......... T S D U R I N G A .......
......... E R E W O N T T O .......
```

Problem 32. Porta Auto-key. EXCEEDINGLY SHY
PQWTE OERLU SHPXY URAON JHVJQ GCNQD QWNQR DKUAI TBXDX ZQETE SLONP
OXQRH OEXLW RAQAJ EIPVW XGNOY JXVFC VLNBS MFCNI SXFPD SUUHP RFKOQ
JYIDD V

Problem 33. Beaufort Interrupted Key. PLAYTHINGS
OBBFX RQYCG RTWIH RYMZW GGNOF TLSFM XHCCX WTBXD DORYY VNHXO KMIQX
WWYAZ UZAER HCABL WYRER BKHNW HQRDK LWENE PTQHE TEFAI XXBIA DYNBE
RORPY TAOOL YXXNQ LLQZK RXYLE BEDTS IPSIJ

Problem 34. Vigenere Interrupted Key. DOES NOT COME
EPQTM EGKLH YBZWZ AINBU NUSLY MLLWM AFGLV HFXMY VTOMF ECNYG LQBAF
SEWYK HFRPA NBAWU FGYUH CHAXA VVDWP MVKML ZWVHG YNLBH GPUFT QALIQ
NBGXT IVOCI OM

CHAPTER XIII. THE TRI-SQUARE CIPHER

The Tri-Square Cipher is just that: three Polybius squares for its encipherment and decipherment, with or without keywords written into the squares by either a normal or complex route. The resultant cipher has a three-to-two ratio since three ciphertext letters represent each plaintext digraph. This feature might be called unwieldy for security, but it does offer a fascinating problem.

Due to its operation, repeated groups are not constant: a plaintext digraph may have as many as 25 <u>different</u> trigraphs for the ciphertext. This is achieved in the <u>following</u> manner. Given three basic squares:

```
                  (II)
              'R E A D I'
              'N G B C F'
              'H K L M O'
              'P Q S T U'
              'V W X Y Z'
    'N S F M U'P A S T I'
    'O A G P W'N O Q R M'
(I) 'V B H Q X'L Y Z U E'
    'E C I R Y'K X W V B'
    'L D K T Z'H G F D C'
                  (III)
```

For the encipherment, plaintext is written out in digraphs. The 1st letter comes from square (I), the second letter from square (II), and where they intersect in square (III) in written the center letter of the trigraph. <u>But</u>, something more is added: two <u>more</u> letters: any letter in the same <u>column</u> with the first digraph letter <u>may</u> be used to precede the center letter; and any letter in the same <u>row</u> of the second digraph letter <u>may</u> be used as the third letter of the trigraph, as, using the above diagram:

WE WE RE RE PU LS ED BY RE IN FO RC ED
UOR YOI TXD QXA RMM NFF LVI AUV MXI HKF KIK TVF LVR

It will be noticed that there is another complexity: the same plaintext digraph may be repeated and yet have have entirely different ciphertext, <u>except</u> for the middle letter. Hence, this peculiarity is helpful <u>in</u> placing tips, for, knowing that a certain digraph must produce a certain center letter, when repeats are offered as a tip, it may be placed by utilizing this fact.

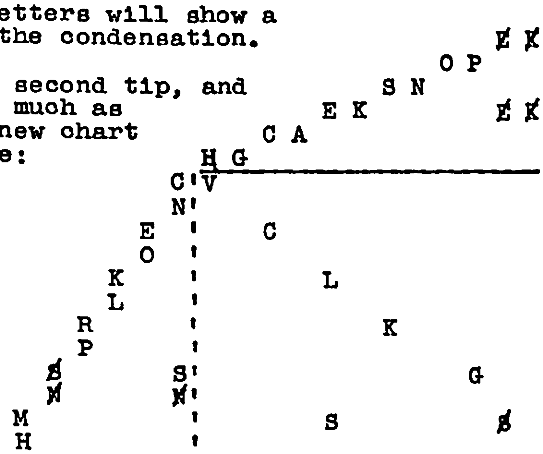
Given, this Tri-Square Cipher to be solved, and the tips: starts CHECKERS SOMETIMES CALLED D; SOME OF THESE EARLY P; and, as an extra tip in Caesar: KXKXMSOXDQKWO (for those who need it).

NVG OCA LLK PKN NGP HSK PCG KSO AKA IOG GBP ELA QFD RWI GOQ IKM
AFD IWB SIB NBO ASQ MUB KSR NGR KSO EZA PDG BCN BBO ANR KBX RXH
DCA DCN LRF ZYK BOP OEQ BHP RWU OKH SSP MYX TYQ AEB ISQ BZI EPQ
OFD UCH CWI PDP UDI NLK ZYO SSS DBO SSQ GPB BES RAS TLW FOP BHE
PLP AVM TKG NLQ AET HEC QBK TLW OEF UKN ABS VRC IFR GED ZBP FGF
XAN AKH IWM GNN HWD CHC BCH IWL IFB AML FEU

Write in the plaintext tips in digraph form under their proper trigraphs in the cipher. The second tip places at: NGR KSO EZA ... Draw up a skeleton three square (in blank) on the worksheet, and place the tips in the chart. For CH-NVG, place the C in square-I, the H in square II, and V at the intersection point in III. Then, write N below the C in the same column; and G in the same row as H. For EC-OCA, start a new column with E, with O below it; a new row with C and A to its right, with the C in III. Continue to do this for all of the known plaintext. The initial three squares for these first few steps will be:

Crossed out letters will show a beginning of the condensation.

(1)

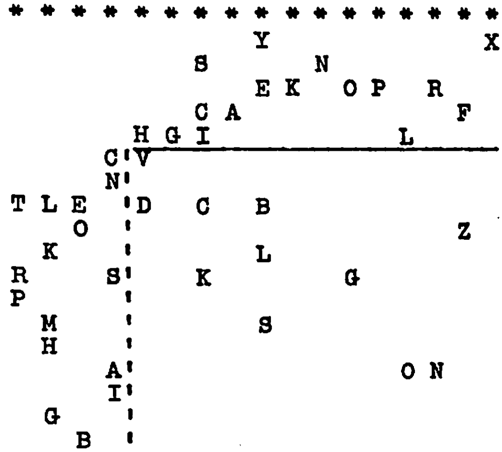


By adding the second tip, and condensing as much as possible the new chart will look like:

(2)

* *

(2)



Return to the cipher, and take each letter of III, in turn: V D C B Z L K G S O N, to see if more plaintext may be added, either a complete digraph, or just the first or third letter:

1. AVM-V; moving out into I on the same line, there is C, which is in the same column as A, so C is the first letter of this digraph; going upwards there is H, but no M in the same row, so there is no proof that H is the second letter of the digraph.
2. PDP-P. D to the left for T in the same column as P, so T is accepted; D upwards, there is no letter there in the same row, so nothing may be added.
3. DCA-C. C to the left, nothing; C up to C, in A's row, so -C is this digraph.
4. DCN-C, or -S.
5. UCH-C, or -I.
6. BCH-C, or -I.
7. NBO-B, or -E.
8. DBO-O, or -E.
9. QBK-B, or -E.
10. ZBP-B, or -E.
11. PLP-L, or -E.
12. TLW-L, or R-.
13. OKM-K, or S-.
14. OKH-K, or -I.
15. TKG-K, or RI.
16. UKN-K, or -S.
17. AKH-K, or SI.
18. KSR-S, or ME.
19. SSP-S, or -E.
20. ELA-L, nothing.

In the first tip, the final letter was W for a digraph D-, so this information may be used here. ELA-L is D- and D may be placed in the same column as E O B in (I). By the same token, look at the final letter of the second tip which is P- in group RXH-X. PR, in the same column, but this is merely proof, since it is already in place.

More condensation:

```
                 T                Q
                 Y            X
          'S       N
               E K   O P R
           C A                F   B   D
       H G I              L
      _____________________________________
      C'V       '
  M   N'   I W S'
T L E I'D  C   B'
    O  '        '
  K    '       L'
       _________
R     S'   K
P      '
  H    '
      A'
  G    '
    B  '
```

The cipher at this point, may be solved with no more information by some of the more expert solvers; but for the beginner, the additional tip in Caesar is to be used. Extend these letters in order through the full 26-positions of the alphabet, until a good word results, and AN ANCIENT GAME is found. This places at the ME spot of KSR. By adding this new plaintext and still condensing the three squares, the result is, as above.

While condensing the three squares is similar to the Bifid operation ("Practical Cryptanalysis", Volume II) so far as rows and columns are concerned, within each square, the procedure of having rows and columns agree in all three squares cannot be accepted.

Treat each of the three squares as separate units.

Checking back, now, the cipher with its recovered plaintext and half-groups, now reads:

```
CH EC KE RS SO ME TI ME SC AL LE D- -- -- -- S- SA NA NC IE NT GA
ME SO ME OF TH ES EE AR LY P- -C -S -- -- E- -- -- -- -I NE -- --
-- NT O- -- -- -I N- T- H- E- -- N- -E N- -- -- -- -- -- -- -E C-
RI -T -- -- -E R- -- -S I- -- -- -- E- -- -- SI N- -- MA -- EI N-
-- -- --
```

At this point, some assumptions should be made: P--C-S (PIECES?) And, perhaps, one of the keywords, say for (I) may be guessed. With the knowledge of one (or two) of the keywords, the third is eventually recovered.

```
Problem 35. ER VI SH FR AT ER NI TY; -E LA BO RA TE DA NC EO TH ER
            S-; Caesar: CFLJYVRCZEXGFNVKJO
QST PBG OBQ XWA UMI GPP ORH PBQ KAF RQV LXR PIP MAF SIS PEB UEL
QUU ENF TDC KKA CWA ESR TFT PRO ERH IVB ULP HPK OYZ PWA SYK LXL
PCH APP IEK GQC IGF DIM TYH RQB FGT LHB AEN USI PBU ULC HRI NKA
ZXC GEN HHK QML SBB OTX ESP TDQ OBQ HLC MRF RFC RXA PHK IFQ UEM
DQC QLQ QSL EVF YXC IBF TYT FER NMN RXP AXB OHM MXL CUR HOV ABP
TKW
```

```
Problem 36. WH IC HE ER ER EG AR DE DA SA MU LE TS; -C OU RA GE TO
            TH EW EA RE RS; Caesar: SVEFGZRAGVBARQ
ZWY IYC STK XIQ OFH GVR WMX GVB WGZ LYA ODX WYK KVF STA ODW KWI FVZ
MIM TMF KYY ZVB SPS OBW XQW QOC LYH MYE KXU YTH VIC BKP XCY LGG
MPH FSI TYC NCP ZRB IGL YTK ICO YNV RDS TTA MZE LFW QRT QTP UKO
YIR AAP SVR VIH AVT SWN FSC UKX HAM AIR OSW MWZ CIM OIR OPR LDS
MVI TYH WDC WVI ZVZ TIX CKP IXP RCO WXX TUD SQL KWE NYF SWN XIC
NSZ ODR MZH MWP GVW SVB
```

CHAPTER XIV. THE PERIODIC FRACTIONATED MORSE CIPHER

The Periodic Fractionated Morse Cipher is an adaptation of the regular Fractionated Morse (Volume I Chapter XII). The same Morse Code values are used for the plaintext letters, plus the usual "x" between letters and "xx" between words. However, this enciphering alphabet is composed of 27 letters, instead of 26, as "xxx" may appear; this extra character may be shown as (#), (&), or any other convenient symbol.

MORSE CODE

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

But from here on, the similarity of the two systems ends. This cipher is in period form (and so far, research has been unable to find a way to determine periods) so that in problems, the group lengths are given, with customary tips.

For encipherment, the plaintext is written in horizontally instead of vertically as was done with the Fractionated Morse, and the resulting vertical units are found in the enciphering alphabet (as before). For example, enciphering FIGURE; in a 6-period.

```
F I G U R E
. . - . x .    . x . x x
. x - - . x
. . - x . -
```

In decipherment, when a ciphertext letter has been found to represent the series of dots, dashes and x's, the plaintext letter is shown in the horizontal position within the group lengths and so far as cipher equivalents are concerned, may comprise only one or two elements of the required unit. Hence, there appear more gaps, and more guesswork is needed to place letters within these gaps.

In placing tips, patterns will show up, of course. In "The Cryptogram" often the tip is placed; if it is not, tests must be made to determine just where the tip goes, and in numerous trials. Decipherment, is therefore, a bit complex, as any given tip may begin at any one of several points. For example, a period length of six, would have 18 starting points; of eight, twenty-four, etc. Here is a tip NATIONALITY, to be used, say, in a six period; the first three tests are shown only; and the patterns which result noted:

```
      - . x . - x    . - x . - .
(1)   - x . . x -    . x . . x -
      - - x - . x    x - . - - x
            1          2     1 2

        - . x . -    x . - x . -
(2)   x - x . . -    . . x . . x
      - - - x - .    - x - . - -
              1          2   1 2

          - . x .    . x . - x .
(3)   - x - x . .    - . . x . .
      x - - - x -    x - x - . -
            1   2    1         2

                 etc.
```

Given, two ciphers, one with the tip placed, and the other merely showing in which group the tip occurs, that is, it will be found "somewhere" in that group.

Problem 37. Starts: THERE IS NO GOOD

DG#URUTI SZHFSWKT KYOQUOZQ XTLINNGU PJDTUURZ PYXGOTVC ZYYILUQH TLZOPXBY GOTKAOBG HJRKIEG# BVXTPZAK LYZEMBQQ PA#WMRBU KEVSIKEF EDG#HAAX INSGU

Problem 38. LOOK UPWARDS somewhere in group 5.

QGBQKXD #TFGGDS EZHKASM IWOKKIU WTPUII# CGGZBTW ZHUSLWS EKDSMVL LBVWZBQ TNBZZLJ DVZAYNZ JI#DERS MUKWHOD GZCALWB #BZ#GFF SDW#XIP PIQ

CHAPTER XV. THE SERIATED PLAYFAIR CIPHER; THE SLIDEFAIR CIPHER

The Seriated Playfair Cipher is merely a fractionations of th the more familiar Playfair ("Practical Cryptanalysis" Vol. I by Zembie). The plaintext is written in two rows, one under the other, in any period length, and the vertical digraphs are put through the Playfair square as usual. Nulls break up the identical vertical pairs when the same plaintext letter falls under its mate. The results are then written again vertically and the plaintext is read first from one row to the one below. This complicates matters somewhat, because it requires the first letters of the top row of the succeeding group to make legitimate plaintext.

Tips are given which show either vertical repeats or reversals so many spaces between one another; and the period is actually given in problems.

When a cipher is at hand, write the 2nd, 4th, 6th, etc. groups under the 1st, 3rd, 5th respectively before starting to solve. Encipherment then is done in this manner:

```
D E A T H V A L   A S S E S F O R   N E D H E A T A
L x E Y S U R P   T H E C O M B I   . . . . . . . .
```

and become as digraphs: DL EX AE TY HS VU AR LP etc.

```
Problem 39. Period 5: WORKI   PLEWE
                      NGPEO   REFOR  (reversal)
WGTFB DBFYE LOMHF YFGPY HTGXE MOVCG VFFUI GCOTF YBSGC MGTAF UNHGD
CSLBG CGAFD TEBCY PFGHU LRCSF HBFGD RPSNX ESDSK IHPLA WWCGH MYUDP
AWHXC UDQDF BDUUU HYESX NOSPF CCMYU CWDKC HGKDN
```

```
Problem 40. Period 7: THETWEL  URYOTHE
                      FTHCENT  RSTHATI   (repeat)
YKNNGFR UOPIEZW ZRORHBE HYFZQRA BIFSMYY QCGASHN IUXOTYX SYBNBBR
PQYOFYN KSBATRO MCOVANV UYBUPOM REZYSCO FASIVYR QCRLKXK MDOSXEP
UKSUEFP ZDBMXEB FYIEKGO IHQFZXK FVOBILR OMBSZWX EQVSZUO RRSQCSY
SBPOWUX ZORSESF BO AL
```

\- - -

The Slidefair Cipher may be adapted to the Vigenere, the Variant and the Beaufort systems of slides. It uses a keyword of any length. The plaintext is set off in digraphs, and the period may be found in many cases by the Kasiski method (Chapter I, Volume I) by catching repeated digraphs. However, due to the peculiarity of this system, repeated digraphs are not infallible, and so do not always show the true period, as the same digraph may represent two different plaintext digraphs. If a period cannot be obtained readily, the alternate method is by using the tip, obtaining one or more letters of the keyword, and eventually working out the entire keyword.

Slides are prepared for this work in each case; and the previous suggestion of owning proper slides in the work-equipment box will save a lot of writing later.

For example, here is a Vigenere Slidefair encipherment, using the keyword MOUTH. Set the lower slide so that the M falls below the indicator: A. Then, take each digraph (period 5) in turn in the column and encipher it, using the first letter in the upper row of the slide, with the second letter in the lower row of the other slide, and let them represent the corners of an oblong; the ciphertext coming from the opposite corners of this oblong. When a digraph shows letters one above the other, use that pair which appear directly to the right (vertically) in the two slides juxtaposed.

With the slide set at M, the plaintext would be for this sample, as shown by the first column; then moved to the O, U, T and H positions:

M	O	U	T	H	
th	ec	ar	to	on	PT
VF	OS	XU	VM	GV	CT
on	ce	re	ga	rd	
BA	QQ	KL	HZ	WY	
ed	as	av	en	om	
RQ	EO	BU	UX	FV	
ou	ss	cu	rr	il	
IA	EG	AW	YK	EB	
ou	sf	or	mo	fa	...
IA	RG	XI	VF	TM	...

Notice that doubled letters in a digraph do not require the null (x) but appear as they are.

This cipher is then taken off in horizontals.

Given the following Slidefair, in the Vigenere system, and the tip: CHRISTMAS, broken up as CH RI ST MA S-, or -C HR IS TM AS:

```
NT KG DQ XD UW LV RH TT TP RM RC DS PU BY FG HF GT SS QP UG MJ KD
FW LM SO JI LC UM CL XU JG OM RF YY LQ IQ MO XY MQ SE CF OQ FH DO
QD WL DS UB DH SL LC EX TW BZ RB LK BO GB BP QM WJ MT ZW UX KH YC
RJ UR EQ KL YS KH KF KF MF BX TA RA GA PL ND KZ PC OV IH TN DB AB
RF
```

The cipher is first written off in a horizontal row, since it will be assumed that no true period has been found by the Kasiski method. Then the tip is slid along the ciphertext, in reverse process from the encipherment to see if the cipher-digraphs agree. The first digraph NT is used with CH; the N and C must appear in the top slide, the T and H in the lower one, and the letter found under the indicator-A will be a letter of the keyword. If a cipher digraph agrees with the plaintext sliding - expectancy - the second pair of plaintext will be tested for the following pair; and if this, too, agrees, the third is tried. If they do not check with the first test, slide one of them to the right and do it over.

In this case, slide the second letter of the plaintext digraph until it is below the first letter of the ciphertext digraph; take the corners of the oblong produced by the two plaintext digraphs, and see if they agree with the pair being tested. Below are several trials, the plaintext in capitals, the ciphertext resultant digraphs in small letter, until the correct plaintext has been found:

```
NT KG DQ XD UW LV RH TT TP RM RC DS PU BY FG TT GT SS GP  (CT)
Cn Ck Cd Cx Cw Cl Cr Ct Ct Cr Cr Cd Cp Rb Sf Mt S-
wH hH gH mH nH yH sH qH qH sH sH gH uH yI gT tA
                                    S  H  O  T      (key)
```

It is not known if this is a four-letter keyword, or if it is longer, and so will be tested in itself, by sliding again. Place the S under the A-indicator, and write in the resulting plaintext for all successive ciphertext digraphs as was done in the Running Key (Chapter XII). Additional possibilities will appear on the diagonal as before.

```
(S)
(H) (S)     NT  KG  DQ XD  UW  LV  RH TT  TP RM RC DS
(O) (H) (S) bf  oc? yv lp? em? dd? pj bl? xl uj kj av?
(T) (O) (H)         jk     pb  os?        ia?
    (T) (O)                        tf?       yj
        (T)                           am?
                           EM  OS  TF AM
```

Counting now, from the first decipherment of S(EM) to the second known decipherment (CH), the interval is eight, the true period. The cipher may then be written into a period of eight, or separated by vertical lines of the same period, and the four known letters of the keyword used to decipher the rest. By that time additional plaintext will have been recovered, and assumptions will have been made for the balance of it on either side of the known values.

Problem 41. AC CO UN T-
YU AF XW CZ JS KD PC OS FQ XT WM CZ BD UW KX IZ YJ HL CV NN FI AO
AL ID QK YU BN QJ AL WE PG OB AV PK PS DT FP YU OS MU AT TC RF KB
BQ ND BM TS YJ YM CX YL AV UO MT NG PL IC JY HO CP ZR CL CN DW PP
RN OB PV WK NY PP BP OZ XQ FR PC TS MN KQ QV ZO AL HT LK UA AR UN
HE WE

CHAPTER XVI. THE HOMOPHONIC SUBSTITUTION CIPHER

The Homophonic Substitution Cipher is based on a four-letter keyword, a 25-letter alphabet (in which I-J occupy the same cell) and a series of numbers from 01 to 00 (100). The ciphertext may be presented in normal word divisions, or it may be continuous text broken into five-letter groups, or continuous without any break at all. There are four substitutions for each letter of the alphabet, depending on the constructor's whim; but only four such substitutions beneath each letter may be used, so governed by the keyword.

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W
20	21	22	23	24	25	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
38	39	40	41	42	43	44	45	46	47	48	49	50	26	27	28	29	30	31	32	33	34
66	67	68	69	70	71	72	73	74	75	51	52	53	54	55	56	57	58	59	60	61	62
96	97	98	99	00	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92

X	Y	Z
17	18	19
35	36	37
63	64	65
93	94	95

(Keyword here is: GOLF)

The plaintext receives any of the four alternates for each letter found in that column under the normal alphabet sequence. For example, in this arrangement of the keyword, E may be 24, 42, 70 or 00; T may be 13, 31, 59 or 89, etc.

To solve a cipher of this type, mark off on a worksheet a depth of four cells (quadrilled paper); leave a space or two and then continue with the overlap. At the heading of each row, mark in (until the system has been familiarized) 01-25, 26-50, 51-75, 76-00, to indicate these digits which must appear in these rows, and these rows only. Then, go to the cipher and pick up the various numbers that appear, assigning them to the proper rows throughout. Here is a cipher in this system:

```
17 95 24 47 82 21 84 81 04 13 47 85 34 81 10 17 02 43 47 91 54 47
20 11 26 74 04 17 40 75 51 53 05 55 66 95 86 60 35 87 74 99 56 04
79 17 38 53 76 26 96 23 30 53 72 54 70 34 82 41 94 78 30 64 06 32
47 49 21 39 25 55 89 47 39 35 74 49 21 62 64 17 36 05 84 29 35 05
65 58 05 53 04 18 45 74 35 48 78 21 54 17 80 20 31 34 76 28 69 10
09 81 27 86 00 21 68 17 53 40 26 84 70 04 67 87 32 72 50 84 21 85
54 47 34 65 78 62 10 26 38 63 15 03 25 20 96 72 66 62 23 21 50 32
17 50 76 21 85
```

The worksheet will show:

```
17    24       21       04 13
         47                      47 etc.
            82    84 81
   96
```

When this has been done, take a frequency of each row, and the results will be found to be:

```
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22
 -  1  1  5  4  1  -  -  1  3  1  -  1  -  1  -  8  1  -  4  7  -

23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44
 2  1  2  4  1  1  1  2  1  3  -  4  4  1  -  2  2  2  1  -  1  1

45 46 47 48 49 50 51 52 53355 55 56 57 58 59 60 61 62 63 64 65 66
 1  -  7  1  2  3  1  -  5  3  2  1  -  1  -  1  -  3  1  2  2  2

67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88
 1  1  1  2  -  3  -  4  1  3  -  3  1  1  3  2  -  4  3  2  2  -

89 90 91 92 93 94 95 96 97 98 99 00
 1  -  1  -  -  1  2  2  -  -  1  1
```

Each row represents a simple substitution frequency, and now the idea is to shift the normal alphabet over (or below) until the tallies lie under the best possibilities of all letters. For example, in the first row, there are 8 17's, which looks promising for E. Let's see what happens:

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22
-	1	1	5	4	1	-	-	1	3	1	-	1	-	1	-	8	1	-	4	7	-
	P	Q	R	S	T			W	X	Y		A		C		E	F		H	I	

23	24	25
2	1	2
L	M	N

The bad part is those 3 X's, which throw a curtain over this setting. Let's try again:

02	03	04	05	06	09	10	11	13	15	17	18	20	21	23	24	25
T	U	V	W	X	A	B	C	E	G	I	K	M	N	P	Q	R

This is somewhat better, but there is still one X and one Q. Let's try a third time:

02	03	04	05	06	09	10	11	13	15	17	18	20	21	23	24	25
L	M	N	O	P	S	T	U	W	Y	A	B	D	E	G	H	I

Here, both A and E are high-frequency letters, so this is evidently the correct setting. Now, go to the cipher and write in all of the substitutions for digits 01-25:

A..H..E..NW..TAL..DU..NA..O..N..A..G..P..E..I..E..A..O..O..O..NB..E..A..D..TS..E..A..N..E..T..YMID..GE..A..E, so try now, to align the second alphabet, where good placements seem likely and finish this cipher.

Problem 42. Normal word divisions. What is the keyword?

86 10 42 85=03 98 51 67 77 41   03 52 90 27 04 91 64 06 72 57 96
38 74 94 64 62 13   00 89 42 64 31 25 30   7   75 68 50 67 04 23-
38 51 31 56   31 45 46 56   81 90   60 71 98 57 13 26 07 42   40-
74 04 50 46 66 30   09 78 01 68 99   72 51   31 71 25 81 12   09-
58 91=53 64 31 72 68 51 91   64 50 67   00 01 56 92 38 48 57 36
41 68 87 21 55 14 75 42 85 14 56   38 50 67   91 45 15 13   71 21-
93 68   42 30 91 64 39 48 72 30 45 77 41   79 89 86 32 53 90   52-
69   87 42 26 10 06 68   25 95 10 68 40 91 46 85 79   70 12 98 57-
92 46 91 04 42 90

Problem 42. Continual text. What is the keyword?

21 24 02 85 38 00 20 29 69 15 32 46 35 24 06 41 91 68 74 56 64 68
12 90 63 32 88 60 36 45 66 03 01 79 74 28 73 90 88 60 97 65 08 33
34 41 82 59 20 05 80 40 60 69 33 78 56 74 02 32 72 64 07 62 77 36
72 60 28 07 31 90 63 76 23 03 39 32 97 45 46 35 20 90 02 73 91 23
31 60 84 38 18 01 44 85 16 84 21 44 80 01 02 74 49 64 90 35 09 56
66 76 28 24 88 36 97 82 77 05 20 67 32 90 79 56 46 59 88 03 15 60
45 75 86 02 03 78 79 32 72 74 35 76 38 75 72 80 00 83 80 89 74 45
93 35 80 30 79 28 66 82 74 63 24 07 03 78 64 46 73 05 85 84 62 52
32 44 76 21 44 24 97 12 46 80 68 62 00 20 44 65 72 56 15 03 40 76
45 28 40 23 99 69 15 24 88 46 73 21 97 88 24