CLASSICAL CRYPTOGRAPHY COURSE
BY LANAKI

June 10, 1996
Revision 0

LECTURE 13

APERIODIC SYSTEMS
IMPROVING CRYPTOGRAPHIC SECURITY IN POLYALPHABETIC SYSTEMS

SUMMARY

Lecture 13 describes the difficult aperiodic polyalphabetic case and reconsiders the Principle of Superimposition. We diagram the topics (I consider the heart) considered in Lectures 10 - 13. We develop our subject via the following references [FRE3], [SACC], [BRYA], [SINK], [OP20] and [ELCY].

COURSE SCHEDULE CHANGES

In order to be more cost-efficient, I have been thinking how to condense some of my future lecture material. Here is how the schedule looks for the balance of my course:
Lecture 14 - Cryptarithms by LEDGE
Lecture 15 - Statistical Methods (Sinkov, Kullback, Friedman)
Lecture 16 - Transposition
Lecture 17 - Transposition
Lecture 18 - Fractionation, Advanced Monome - Dinome Systems
Lecture 19 - Law and Politics of Cryptography
Lecture 20 - Cipher Exchange Systems
Lecture 21 - Cipher Exchange Systems
Lecture 22 - Modern Crypto-Systems, Double Key Cryptography, Cipher Machines, PGP and PGPphone, Diamond Cipher Family
Lecture 23 - Volume I and II References / Resources, Index to Volume II Lectures 11 - 22. Table of Figures, Table of Tables; Presentation of Certificates of Achievement to my Students and Grateful Thanks form LANAKI!

LEDGE has done a marvelous job on the Cryptarithms section. I will leave open a slot for him if he consents to a third Lecture. Expect Lecture 23, which is devoted to Resources and References, to be more than 125,000 bytes download. Several of our class are helping out with an extra set of eyes, to correct my atrocious typing and other errors caused by crossing the different E-Mail gateways. I thank them for their valued help.

IMPROVING CRYPTOGRAPHIC SECURITY IN POLYALPHABETIC SYSTEMS

The last two chapters have explored the effects of repeating key ciphers and the periodicity that occurs in them. Establishing the period opens the wedge for solution of this type of cipher system. The difficulty of solution is related to the number of cipher alphabets employed and their type.

Two procedures suggest themselves to improve the cryptographic security of these systems. First, we can increase the length of the key. This is akin to what we do with modern public key systems. Second, since the first step in solution of a Viggy or other polyalphabetic cipher is to establish the period, hence the number of alphabets employed, we can eliminate the periodicity, and therefore eliminate the cryptanalyst's attack.

APERIODIC CIPHER SYSTEMS

What is the real nature of periodicity in polyalphabetic substitution systems? How do we remove periodicity from ciphers?

We understand the cyclic and repeating nature of a keyword based periodic system. However, we have taken for granted that the keying element acts on constant-length plain text groupings. If this were not true, there would not be any external manifestation of periodicity, despite the repetitive or cyclic use of a constant-length key. The key is of a constant or fixed character.

Two approaches for eliminating or suppressing periodicity come to bear: 1) by using constant-length keying units to encipher variable-length plain-text groupings or 2) by using variable-length keying units to encipher constant-length plain-text groupings.

In cases of encipherment by constant-length groupings, the apparent length of the period (found by factoring) is a multiple of the real length and the multiple corresponds to the length of the groupings, i.e. the number of plain-text letters enciphered by the same key letter. Periodicity still exists because in every system studied so far both the keying units and the plain-text groupings are constant in length.

EFFECT OF VARYING THE LENGTH OF PLAIN-TEXT GROUPINGS

Lets assume that the keying units are kept constant and vary the plain-text groupings. The effect is to suppress periodicity, even though the key may repeat itself many times in the cryptogram. This is true unless the law governing the variation in plain-text groupings is itself cyclic in character, and the length of the message is at least two or more times that of the cycle applicable to this variable grouping. [FRE3]

For example we encipher the following message using the keyword SIGNAL, but divide up the plain-text into groups:

```
S I   G   N     A    L S   I   G    N     A  L S   I     G
1 12 123 1234 12345  1 12 123 1234 12345  1 12 123 1234 12345
C OM MAN DING GENER  A LF IRS TARM YHASI  S SU EDO RDER SEFFE
Q UW UGT KFAH UWNWJ  L HN ARQ NGPU PGNVF  I TR OPE RFER OCBBC

N A   L   S    I     G N   A   L    S     I G  N   A    L
1 12 123 1234 12345  1 12 123 1234 12345  1 12 123 1234 12345
C TI VET WENT YFIRS  T AT NOO NDIR ECTIN  G TH ATT ELEP HONES
L HS QHS WOFZ KDARQ  N NU NMM YIDU OQZKF  C NZ NUU WPWL EXYHT

S I   G   N     A    L S  I
1 12 123 1234 12345  1 12 123...
C OM MAS WITC HBOAR  D SC OMM...
Q UW UGO RFUL TZMAJ  I AQ UWW...
```

Cryptogram

```
QUWUG  TKFAH  UWNWJ  LHNAR  QNGPU  PGNVF  ITROP ERFER
OCBBC  LHSQH  SWOFZ  KDARQ  NNUNM  MYIDU  OQZKF CNZNU
UWPWL  EXYHT  QUWUG  ORFUL  TZMAJ  IAQUW  W...
```

The cipher text above shows a tetragraphic and a pentagraphic repetition. The two occurrences of QUWUG (COMMA) are separated by an interval of 90 letters, the two occurrences of ARQN (=IRST) by 39 letters. The former is the true periodic repetition measured in grouping cycle rather than letters. The interval is the product of the keying cycle of 6 by the grouping cycle of 15. The latter repetition are produced by the same key letters I and G but do not have the same enciphering points and is considered a partial periodic as opposed to a completely periodic type.

Kasiski analysis focuses on the intervals between repetition letters and developing factors which indicate the number of cipher alphabets employed. We also can study the interacting cycles that produce the intervals directly. If we look at the above as counting according to groupings and not according to single letters, the two pentagraphs QUWUG are separated by an interval of 30 groupings. The separation of 30 key letters is made up of a key 6 letters in length and has gone through 5 cycles. So 30 is the product of the number of letters in the keying cycle (6) times the number of different-length groupings in the grouping cycle (5).

Friedman describes a clever little cipher system based on a lengthy grouping cycle which is guided by a key of its own. We can use the number of dots and dashes contained in the International Morse signals for the letters composing the phrase DECLARATION OF INDEPENDENCE. Thus, A(._) has 2, B(_...) has 4, and so on. So:

```
D E C L A R A T I O N O F I N D E P E N D E N C E
3 1 4 4 2 3 2 1 2 3 2 3 4 2 2 3 1 4 1 2 3 1 2 4 1
```

The grouping cycle is 3+1+4+4+.., or 60 letters long. If the same phrase is used as the enciphering key (25 letters) the complete period of the system would be the least common multiple of 25 and 60 or 300 letters. The length of the complete period is the least common multiple of the two component or interacting periods.

One drawback - the variable factor introduced above is subject to a law which itself is periodic in character.

SOLUTION OF SYSTEMS USING CONSTANT-LENGTH KEYING UNITS TO ENCIPHER VARIABLE-LENGTH PLAIN-TEXT GROUPINGS

APERIODIC GROUPINGS ACCORDING TO WORD LENGTHS

The simplest way to introduce aperiodicity is to encipher our message by actual word lengths. Although the average number of letters composing words of any alphabetical language is fairly constant, successive words comprising plain text vary a great deal in this respect, and the variation is subject to no law. In English, the mean length of words is 5.2 letters but the words may contain from 1 - 15 or more letters; successive words vary in length in an extremely irregular manner, no matter how long the text is.

The use of word lengths for determining the number of letters to be enciphered by each key letter of a repetitive key seems more secure than it is. The reasoning goes something like this: if there is no periodicity in the cryptogram, how can the letters of the cipher text, written in groups of five letters be distributed into their respective monoalphabets. If the first step is foiled, how can the cryptograms be solved? The answer: using a variation of the completion of the plain component sequence method discussed under the monoalphabetic cipher cracking.

SOLUTION WHEN DIRECT STANDARD CIPHER ALPHABETS ARE EMPLOYED

Since the individual separate words of a message are enciphered by different key letters, these words will reappear on different generatrices of the diagram.

Given:

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

First step: Run down the first 10 letters for a clue.

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

We place these over the first ten cipher letters to backout the keying letters of R E A. We can either set up the remaining letters of the message on a sliding normal alphabet scale or assume various keywords such as READ, REAL, REAM. The completed solution is:

```
  R      E      A        D             E             R

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

    S        D        I        G      E      S

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

        T

C O M M I S S I O N
V H F F B L L B H G.    Key = READERS DIGEST
```

The slide is very quick. We place the C(1) over T(2) and back out the index A(1) over the Key letter R(2). For the second group the Y(1) over C(2) will back out the A(1) over E(2). If reversed standard alphabets are employed we either convert

the cipher letter to normal alphabets or employ the reverse alphabet slide. The slides, if not out of stock, referred to are available from ACA for about $3. It may be used to aid solutions for the entire Viggy family.

SOLUTION WHEN ORIGINAL WORD LENGTHS ARE RETAINED IN THE CRYPTOGRAM

Given the enciphered message:

```
                                DIVISION
                                12324256
XIXLP  EQVIB  VEFHAPFVT  RT  XWK  PWEWIWRD  XM  NTJCTYZL

          BATTALIONS      ARTILLERY
          1233245678      123455627
OAS  XYQ  ARVVRKFONT  BH  SFJDUUXFP  OUVIGJPF  ULBFZ

           OCLOCK
           123124
RV  DKUKW  ROHROZ.
```

We crack the above using Idiomorphs and "Probable Word" analysis.

We note the Idiomorphs and use the Cryptodyct or TEA:

```
1) 12324256    = 32426 (8) = DIVISION
   PWEWIWRD
2) 1233245678  = 3328  (10) = BATTALIONS
   ARVVRKFONT
3) 123455627   = 55627 (9) = ARTILLERY
   SFJDUUXFP
4) 123124      = 3124 (6) = O'CLOCK
   ROHROZ
```

Using the assumed equivalents a reconstruction matrix is established on the hypothesis that the cipher alphabets have been derived from a mixed component against a normal sequence. Note that O(plain) = R(cipher) in both DIVISION and OCLOCK, so the same cipher alphabet has been used.

```
         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
DIVISION|-------------------------------------------------
OCLOCK   |  n O P   s t v W x Z H   D R a u   I     E f   j k
         |
BATTA-   |-------------------------------------------------
LIONS    |R A             F     K   N O       T V
         |
ARTILL-  |-------------------------------------------------
ERY      |
         |S       X       D     U           F   J         P
         |-------------------------------------------------
```

The interval between letters O and R in the first and second alphabets is the same at 12, therefore direct symmetry of position is assumed. We fill in the additional letters (lower case).

It is a short stretch to find the keyword HYDRAULIC and to decipher the equivalents based on the HYDRAULIC...Z sequence against the normal alphabet at any point of coincidence and completing the plain component sequence. The

words of the message will then reappear on different generatrices. The key letters may be ascertained and the solution completed. The first three words are deciphered as follows:

```
 XIXLP       EQVIB        VEFHAPFVT
 ---------------------------------
 YHYGS       KTWHJ        WKLAESLW
 ZIZHT       LUXIK        XLMBFTMX
 AJAIU       MVYJL        YMNCGUNY
 BKBJV       NWZKM        ZNODHVOZ
 CLCKW       OXALN        AOPEIWPA
 DMDLX       PYBMO        BPQFJXQB
 ENEMY       QZCNP        CQRGKYRC
             RADOQ        DRSHLZSD
Ap = Sc      SBEPR        ESTIMATE
             TCFQS
             UDGRT        Ap = Pc
             VEHSU
             WFITV
             XGJUW
             YHKVX
             ZILWY
             AJMXZ
             BKNYA
             CLOZB
             DMPAC
             ENQBD
             FORCE
             Ap = Uc
```

The key for this message is SUPREME COURT and the complete message is:

```
ENEMY  FORCE  ESTIMATED  AS  ONE  DIVISION  OF  INFANTRY
XIXLP  EQVIB  VEFHAPFVT  RT  XWK  PWEWIWRD  XM  NTJCTYZL

AND  TWO  BATTALIONS  OF  ARTILLERY  MARCHING  NORTH
OAS  XYQ  ARVVRKFONT  BH  SFJDUUXFP  OUVIGJPF  ULBFZ

AT  SEVEN   OCLOCK
RV  DKUKW  ROHROZ.
```

In the case of plain component in reverse normal alphabets. the procedure is the same , except the completion tableaux is created after the cipher letters are converted into their plain-component equivalents.

ILLUSTRATION OF THE USE OF ISOMORPHISM

Consider the following cryptogram which has been enciphered using the primary key word-mixed alphabet of (HYDRAULIC...XZ) against a normal sequence. I have retained word lengths for simplicity:

```
VCLLKIDVSJDCI   ORKD   CFSTV   IXHMPPFXU   EVZZ

FK  NAKFORA   DKOMP   ISE   CSPPHQKCLZKSQ   LPRO

JZWBCX   HOQCFFAOX   ROYXANO   EMDMZMTS

TZFVUEAORSL   AU   PADDERXPNBXAR   IGHFX   JXI.
```

We look at three sets of isomorphs:

```
 1)  a VCLLKIDVSJDCI            2) a IXHMPPFXU
     b CSPPHQKCLZKSQ               b HOQCFFAOX
     c PADDERXPNBXAR
                                 3) a NAKFORA
                                    b ROYXANO
```

Rather than identifying these from a TEA or Cryptodyct database, we build up the partial sequences of equivalents. [TEA], [CRYP]

>From 1a and 1b:
V = C, C = S, L = P, K = H, I = Q, D = K, S = L, J = Z

so: VCSLP DKH IQ JZ are constructed.

>From 1b and 1c:

C=P, S=A, P=D, H=E, Q=R, K=X, L=N, Z=B

We find:

CPD SA HE QR KX LN ZB

>From 1a and 1c:

V=P, C=A, L=D,K=E,I=R,D=X,S=N,J=B

and:
LDX VP CA KE IR SN JB

Noting that the three isomorphs may be combined (VCSLP and CPD make VCSLP..D; the latter and LDX make VCSLP..D...X), the following sequences are established:

```
   1 2 3 4 5 6 7 8 9 10 11 12 13
1. V C S L P A N D K H  .   X  E
2. I Q . . R
3. J Z . . B
```

Chain 1 contains exactly 13 letters and suggests a half-chain is disclosed. the latter represents a decimation of the original primary component at an even interval.

1 2 3 4 5 6 7 8 9 10

The placement of the letters V . S . P . N . K . suggests a reversed alphabet; we reverse the half-chain and extend to 26 places as follows:

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22
E     j K   N   P  q S     V     X  z  H      D r  A

23 24 25 26
L  i  C  b
```

We add the data from the two partial chains (JZ..B and IQ..R). [Small letters]

The keyword is HYDRAULIC. the full sequence is:

```
12345678910111213141516171819202122232425 26
HYDRAULIC B E F G J K M N O P Q S T V W X Z
```

We confirm from 2a and 2b that the interval between H and I is 7; same for O to X and Q and H, and C and M. From idiomorphs 3a and 3b, the interval between R and N is 13; which is the same for O and A and Y and K.

We now convert the ciphertext letters into plain-component equivalents then complete the plain component sequences.

Solution Key: Strike While The Iron is (Hot?)

>From the slide we put A/S which confirms O/S,M/L C/V etc.,

```
     S           T      R         I         K
COMMUNICATION   WITH   FIRST   ARTILLERY   WILL
VCLLKIDVSJDCI   ORKD   CFSTV   IXHMPPFXU   EVZZ

E     W        H       I        L           E
BE  THROUGH   CORPS   AND   COMMUNICATION   WITH
FK  NAKFORA   DKOMP   ISE   CSPPHQKCLZKSQ   LPRO

  T         H           E         I
SECOND   ARTILLERY   THROUGH   DIVISION
JZWBCX   HOQCFFAOX   ROYXANO   EMDMZMTS

     R        O          N          I       S
SWITCHBOARD   NO   COMMUNICATION   AFTER   TEN
TZFVUEAORSL   AU   PADDERXPNBXAR   IGHFX   JXI.
```

Four assumptions were made in the above:

1. The actual word lengths were known.
2. The words were enciphered monoalphabetically by different alphabets, producing isomorphs and lengths of isomorphs that are known.
3. Repetitions of plain-text words enciphered by different alphabets, produce isomorphs and the lengths of the isomorphs are definitely known as a result of this action.

What if the cryptogram is put in the form of a Patristocrat with 5-letter-groups?

Take the same problem as above and destroy the word lengths. The problem is a little more difficult and requires more trial and error.

```
VCLLK  IDVSJ  DCIOR  KDCFS  TVIXH  MPPFX

UEVZZ  FKNAK  FORAD  KOMPI  SECSP  PHQKC

LZKSQ  LPROJ  ZWBCX  HOQCF  FAOXR  OYXAN

OEMDM  ZMTST  ZFVUE  AORSL  AUPAD  DERXP

NBXAR  IGHFX  JXI.
```

The 13 letter isomorps are relatively easy to spot:

```
1. VCLLKIDVSJDCI
2. CSPPHQKCLZKSQ      Column ends IQR
3. PADDERXPNBXAR
```

Number 1 is the "header" and the left-hand boundary is known. The right hand boundary marked by IQR is fortuitous. Not knowing the exact length by one or two letters is not fatal to the solution because we are interested in reconstructing cipher equivalents not looking up the pattern words.

Isomorphism is not restricted to cases where secondary alphabets are derived from a primary component sliding against the normal. It is useful in all cases of interrelated alphabets no matter what the basis of their derivation may be. It is second only to the importance of the "Probable Word" method which has nearly universal applicability.

SOLUTION OF SYSTEMS USING VARIABLE-LENGTH KEYING UNITS TO ENCIPHER CONSTANT-LENGTH PLAIN-TEXT GROUPINGS

THE INTERRUPTED KEY CIPHER

Periodicity can also be suppressed by applying variable-length key groupings to constant length plain-text groups. One such method is the Interrupted Key Cipher which employs an irregularly interrupted key sequence, the latter may be of fixed or limited length and restarting it from its initial point after the interruption, so that the keying sequence becomes equivalent to a series of keys of different lengths.

Take the phrase BUSINESS MACHINES and expand it to a series of irregular-length keying sequences, such as BUSI/BUSINE/BU/BUSINESSM/BUSINESSMAC/ etc. Three usual schemes for interruption prearrangement are given by Friedman [FRE3]:

(1) The keying sequence merely stops and begins again at the initial point of the cycle.

(2) One or more of the elements in the keying sequence may be omitted from time to time irregularly.

(3) The keying sequence irregularly alternates in the direction of progression, with or without omission of some of the elements.

Using an asterisk to indicate an interruption, a sequence of 10 elements might look like this:

```
    Letter No     1 2 3 4  5 6 7 8 9 10  11 12 13  14 15 16
    Key Element No1-2-3-4*-1-2-3-4-5-6-* -1- 2- 3-*-1- 2- 3
    Letter No     17 18 19 20  21 22 23 24 25 26 27 28 29 30
(1) Key Element No-4 -5 -6 -7-* 1 -2 -3 -4 -5 -6 -7 -8 -9 -10
    Letter No       31 32 33   34 35
    Key Element No_*-1 -2 -3-*- 1 -2

    Letter No     1 2 3  4 5 6 7   8 9  10 11 12  13 14 15 16
    Key Element No1-2-3-*-7-8-9-10-1-2-*-4- 5- 6-*-3- 4- 5- 6
    Letter No     17 18 19 20  21  22 23 24 25 26  27 28 29
(2) Key Element No-7 -8 -9-10- 1-*-8- 9- 10 -1-2-* -5 -6 -7-*
    Letter No       30 31 32   33 34 35
    Key Element No - 9-10 -1-*-5 -6 -7-

    Letter No     1 2 3 4 5   6 7  8 9 10 11 12 13 14 15   16
    Key Element No1-2-3-4-5-*-4-3-*4-5 -6 -7 -8 -9-10 -1-*-10
    Letter No     17 18 19  20 21 22 23 24 25  26 27 28 29 30
(3) Key Element No 9- 8- 7-*-8- 9-10- 1- 2- 3-*-2- 1-10- 9-8-
    Letter No       31 32 33 34 35
    Key Element No *-9-10- 1- 2- 3
```

Method three is a key progression direction reversing method and if their were no interruptions in the key, it could be handled as a special form of the second method. However, combined with the second method, it represents a difficult cryptographic variant.

RETURNING TO THE PRINCIPAL OF SUPERIMPOSITION

If one knows when the interruptions take place in each cycle, then successive sections of the basic keying cycle in the three cases may be superimposed. Obviously, if one does not know when or how the interruptions take place, the then the successive sections of keying elements cannot be superimposed. See Table 13-1.

The interruption of the cycle keying sequence practically takes place according to some prearranged plan, and the three basic methods of interruption will be described in turn using a short mnemonic key as an example.

Suppose we agree to interrupt the keying sequence after the occurrence of a specified letter (called an interruptor- fancy that). This may be a plain or cipher text letter, agreed to in advance. Then since in either case there is nothing fixed about the time of interruption will occur - it will take place at no fixed intervals - not only does the interruption become quite irregular, following no pattern, but also the method never reverts back to one having periodicity. We have the LANAKI equivalent of a DOOSEY in the polyalphabetic arena.

We will use the mnemonic key BUSINESS MACHINES and the cipher alphabet HYDRAULIC...XZ sequence which slides:

```
  12345678910111213141516171819202122232425 26
  HYDRAULIC B E F G J K M N O P Q S T V W X Z
```

The keying set is a Viggy, so A(1)/K(2) = P(1)/C(1), where A is the index, K is the key letter, P is the plain text letter, C is the ciphertext letter, (1) and (2) subscripts refer to the top and the bottom slides.

Table 13-1

```
                          Method (1)
Keying Element No  1  2  3  4  5  6  7  8  9  10
                   ------------------------------
Letter No          1  2  3  4|
Letter No          5  6  7  8  9  10|
Letter No          11 12 13|
Letter No          14 15 16 17 18 19 20|
Letter No          21 22 23 24 25 26 27 28 29 30|
Letter No          31 32 33
Letter No          34 35

                          Method (2)
Keying Element No  1  2  3  4  5  6  7  8  9  10
                   ------------------------------
Letter No          1  2  3  -  -  -  4  5  6  7
Letter No          8  9| -  10 11 12|
Letter No          -  -  13 14 15 16 17 18 19 20
Letter No          21|-  -  -  -  -  -  22 23 24
Letter No          25 26|-  -  27 28 29| - 30 31
Letter No          32|-  -  -  33 34 35

                          Method (3)
Keying Element No  1  2  3  4  5  6  7  8  9  10
                   ------------------------------
Letter No          1  2  3  4  5| -  -  -  -  -
Letter No          -  -  7  6  -  -  -  -  -  -
Letter No          -  -  -  8  9  10 11 12 13 14
Letter No          15|-  -  -  -  -| 19 18 17 16
Letter No          23 24 25|-  -  -  -  20 21 22
Letter No          27 26 -  -  -  -  - |30 29 28
Letter No          33 34 35               31 32
```

PLAIN TEXT LETTER INTERRUPTOR

Let the plain text letter R be designated an interruptor. Interruption will occur immediately after and R occurs in the plain text.

```
Index  A(1)
Key    K(2) B U S I N E S S M A C H I|B U S|B U S I|B U S I
Plain  P(1) A M M U N I T I O N F O R F I R S T A R T I L L
Cipher C(2) B O L Y R P J D R O J K X K J F Y X S X D J U P

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

Index  A(1)
Key    K(2) N E S S M A C H I|B U S I|B U S|B U S I N E|
Plain  P(1) N I T I O N F O R T H I R D A R T I L L E R
Cipher C(2) R P J D R O J K X D G D X G U F D J U P S Y
```

```
Index  A(1)
Key    K(2) B U S I N|
Plain  P(1) Y . . . .
Cipher C(2) I
```

examples: with Index = A

group 1, plain letter 1 = A ; key B ; cipher B

```
Plain            ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher HYDRAULICBEFGJKMNOPQSTVWXZHYDRAULICBEFGJKMNOPQSTVWXZ
                 *
```

group 1, plain letter 2 = M ; key U ; cipher O

```
Plain        ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher HYDRAULICBEFGJKMNOPQSTVWXZHYDRAULICBEFGJKMNOPQSTVWXZ
             *           *
```

group 1, plain letter 3 = M ; key S ; cipher L

```
Plain                        ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher HYDRAULICBEFGJKMNOPQSTVWXZHYDRAULICBEFGJKMNOPQSTVWXZ
                             *           *
```

group 2, plain letter 1 = F ; key B ; cipher K

```
Plain            ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher HYDRAULICBEFGJKMNOPQSTVWXZHYDRAULICBEFGJKMNOPQSTVWXZ
                 *    *
```

group 2, plain letter 2 = I ; key U ; cipher J

```
Plain        ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher HYDRAULICBEFGJKMNOPQSTVWXZHYDRAULICBEFGJKMNOPQSTVWXZ
             *       *
```

group 3, plain letter 2 = S ; key B ; cipher Y

```
Plain            ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher HYDRAULICBEFGJKMNOPQSTVWXZHYDRAULICBEFGJKMNOPQSTVWXZ
                 *                   *
```

Cryptogram

```
B O L Y R   P J D R O   J K X K J   F Y X S X   D J U P S
Y I Y D P   Y F X U R   A F A E N   M J J V B   O L Y R P
J D R O J   K X D G D   X G U F D   J U P S Y   I X X X X
```

Instead of employing an ordinary letter for interruptor, we can use a low frequency letter like J. Actually any letter, no matter what frequency level will produce plentiful repetitions. The only advantage is that the intervals will be random and therefor suppress (or reduce) periodicity.

INTERRUPTOR CASES

The interruptor problem presents two cases for investigation. The first is when the system has been used several times and the cipher alphabets are known. The second case is when the cipher alphabets are not known but several messages have been intercepted.

Case 1 - Cipher Alphabets Known, Problem is to find specific key.

Attack: Probable word. Using probable word ARTILLERY on previous example, starting from first letter we have:

```
Cipher      B O L Y R P J D R
Plain       A R T I L L E R Y
'Key'       B H J Q P I B F U
```

failed. We move one cipher letter to right with assumed word. Continued failure until the following:

```
Cipher      S X D J U P S Y I
Plain       A R T I L L E R Y
'Key'       S I B U S I N E B
              *           *
```

We note the BUSINE suggesting BUSINESS. We also note the interruptor letter R. We use this key part on the first part of the message with success.

```
Key         B U S I N E S S B U S
Cipher      B O L Y R P J D R O J
Plain       A M M U N I T I U M T
```

The last three letters suggest that there is more to the key. Using Ammunition and back calculating the Key, we find MA. We use the cipher and the plain back and forth to find the total key, taking into account the interruptor letter R.

Case 2 - Cipher Alphabets Unknown, Problem is to find both cipher alphabet and specific key.

Assume that the repetitive key is very long and that the message is short. Solution is difficult because there are not enough superimposable periods to help line up the alphabets to yield monoalphabetic distributions that can be solved by frequency principles. This is the first step in the cryptanalytic attack. The superimposed periods essentially line up the letters in the columns so that the same treatment has been used to process both plain and cipher components.

Attack: Solution by Superimposition.

The second most important attack on cryptanalytic problems is the Solution by Imposition. First we need a sufficient number messages (25 - 30 for English) enciphered by the same key to work with. It is clear that if we superimpose these messages, 1) the letters in the respective columns will all belong to individual alphabets; and 2) a frequency distribution of the columnar letters can be solved without knowing the length of the key. In other words, any difficulties that may have arisen on account of failure to ascertain the length of the period have been circumvented. The second step in the solution is by-passed. (3) For a very long key employed, and a series of messages beginning at different initial points are enciphered by the same key, this method of attack can be employed after the messages are superimposed at the same initial point [done with the help of the Chi square test]. An example of this will be done in a later lecture on statistical techniques.

CIPHER TEXT LETTER INTERRUPTOR

If we use a cipher text letter, say Q, as the interruptor, we find a more difficult case with no significant repetitions available for superimposition.

```
Key    K(2) B U S I N E S S M A C H I N E S B U S I N E S S
Plain  P(1) A M M U N I T I O N F O R F I R S T A R T I L L
Cipher C(2) B O L Y R P J D R O J K X T P F Y X S X B P U U

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

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

Cryptogram

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

The attack is first to find the interruptor and then to recover the plain by method of superimposition. To accomplish superimposition a statistical test is essential and for this a good many letters are required.

THE AUTO-KEY CIPHER or AUTOCLAVE CIPHER

The purpose of the Auto-key Cipher or Autoclave Cipher is to eliminate periodicity and introduce a long key for the entire message. The Autoclave may be 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 the system involved. >From a purely theoretical standpoint, we are approximating the features of a One-Time Pad.

In practice, the Auto-Key is a nightmare. MASTERTON points out that the slightest difficulty in transmission of cipher letters destroys the communication. [MAST] Other authors [ELCY] and [BRYA] and ACA KREWE find the Auto-Key and Progressive Ciphers a real challenge. There are two possible sources for successive key letters: the plain text or the cipher text of the message itself. In either case, the initial key letter or key letters are supplied by pre-agreement between the correspondents; after which the text letters that are to serve as the key are displaced 1,2,3.. intervals to the right, depending upon the length of the prearranged key.

Lets review the methods.

Plain-text keying using the single letter X:

```
Index  A(1) A1
Key    K(2) X N O T I F Y Q U A R T E R M A S T E R . .
Plain  P(1) N O T I F Y Q U A R T E R M A S T E R . . .
Cipher C(2) K B H B N D O K U R K X V D M S L X V . . .
```

Plain-text keying using long phrase TYPEWRITER as initial:

```
Index  A(1) A1
Key    K(2) T Y P E W R I T E R|N O T I F Y Q U A R . .
Plain  P(1) N O T I F Y Q U A R T E R M A S T E R . . .
Cipher C(2) G M I M B P Y N E I G S K U F Q J Y R . . .
```

Plain-text keying using divided text [aka Running Key]:

```
Type  PORTA
Key    K(2) OFFICERSANDDIRE
Plain  P(1) CTORSOFTHELOCAL
Cipher C(2) WEMAEMNKUXZATVN
```

Cipher text auto key with single letter X:

```
Index  A(1) A1
Key    K(2) X K Y R Z E C S M M D W A R D D V O S . . .
Plain  P(1) N O T I F Y Q U A R T E R M A S T E R . . .
Cipher C(2) K Y R Z E C S M M D W A R D D V O S J . . .
```

Cipher text auto key with key phrase TYPEWRITER:

```
Index  A(1) A1
Key    K(2) T Y P E W R I T E R|G M I M B P Y N E I . .
Plain  P(1) N O T I F Y Q U A R T E R M A S T E R . . .
Cipher C(2) G M I M B P Y N E I G S K U F Q J Y R . . .
```

Cipher text auto key with key phrase TYPEWRITER using only the last letter of keyphrase to seed progression:

```
Index  A(1) A1
Key    K(2) T Y P E W R I T E R|I B F W I I A T X . . .
Plain  P(1) N O T I F Y Q U A R T E R M A S T E R . . .
Cipher C(2) G M I M B P Y N E I B F W I I A T X O . . .
```

SOLUTION OF CIPHER-TEXT AUTO-KEYED CRYPTOGRAMS WHEN KNOWN CIPHER ALPHABETS ARE EMPLOYED

Attack: Decipher the message beyond the key letter or key word portion and then work backwards.

Cryptogram

```
W S G Q V   O H V M Q   W E Q U H   A A L N B   N Z Z M P
E S K D
```

Write the cipher text as key letters (displaced one interval to the right) and decipher by direct standard alphabets yields the following:

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

Try the probable word REPORT on the initial group:

```
Key          F O R C E V O H V M Q . .
Cipher       W S G Q V O H V M Q . . .
Plain        R E P O R T T O R E . . .
```

A semi-automatic method of solving such a message is to use sliding normal alphabets and align the strips so that as one progresses from left to right, each cipher letter set opposite the letter A on the preceding strip. Take the letters VMQWEQUHA in the above example and note how the successive plain text letters of the word REGIMENT reappear to the left of the cipher letters MQWEQUHA.

SOLUTION OF AUTOCLAVE BY FREQUENCY ANALYSIS

REDUCED REPETITIONS

Repetitions are not as plentiful in the Autoclave Cipher Text as they are in the Plain text because in this system, before a repetition can occur, two things must happen simultaneously. First the plain-text sequence must be repeated and second, one or more of the cipher-text letters immediately before the second appearance of the plain text repetition must be identical with one or more of the cipher-text letters immediately before the first appearance of the group. This can only happen as a result of chance.

ex: Use single key letter X:

```
Key    X C K B T M D H N V H L Y...K D K S J M D H N V H L Y
Plain  F I R S T R E G I M E N T   T H I R D R E G I M E N T
Cipher C K B T M D H N V H L Y R .KD K S J M D H N V H L Y R
```

The repeated word REGIMENT has 8 letters but the repeated cipher text has 9 letters. The plain letter R must be M in cipher both times. The chances of this are 1/26. In general, an n-letter repetition in the cipher text, represents an (n-k) -letter repetition in the plain text, where n is the length of the cipher-text repetition and k is the length of the introductory key.

DOUBLETS

Define the 'base letter' as the letter opposite which the key letter is placed. We also know this as the index. For convenience, we have chosen A or the initial letter in the Viggy sequence. When the first key is a single letter, if the base letter occurs as a plain-text letter its cipher equivalent is identical with the immediately preceding cipher letter; there is produced a double letter in the cipher text, no matter what the cipher component is and no matter what the key letter happens to be for encipherment.

ex. use HYDRAULIC..XZ sequence for both primary components, with H, the initial letter of the plain component as a base letter, and using introductory X as key letter:

```
Key    X J O I I F L Y U T T D K K Y C X G
Plain  M A N H A T T A N H I G H J I N K S
Cipher J O I I F L Y U T T D K K Y C X G L
```

Each time the doublet appears it means the second letter represents H(plain), which is the base letter in this case (initial letter of the plain component). If the base letter happens to be high frequency in normal plain text, say E, or T, then the cipher text will show a high number of doublets. The number of doublets is directly proportional to the frequency of the base letter. If the cryptogram has 1000 letters, we should expect 72 occurrences of doublets, if the letter was A, and visa-versa. This observation acts as a check and a guess for new values in the cryptanalysis of the problem.

When the introductory key is 2 letters, the same phenomenon will produce groups of the formula ABA, where A and be may be any letters but the first and the third letters must be identical. Combine this phenomena with our use of idiomorphs and we have a powerful wedge into the problem. If we take BATTALION, it will be enciphered by AABCCDEFG formula. If the plain component is a mixed sequence and happens to start with an E, the word ENEMY would be enciphered by AABBCD formula. Used together, we have a powerful tool to open this cipher.

AMOUNT OF TEXT REQUIRED FOR FREQUENCY ANALYSIS

The Autoclave cipher essentially shifts the key text or "offsets" the key by at least one letter to the right of the cipher text. Every cipher letter which immediately follows the key letter in the cryptogram is monoalphabetically distributed. If 26 distributions are made, one for each letter of the alphabet, showing the cipher letter immediately succeeding each different letter of cipher text, then the text will be allocated into 26 monoalphabetic distributions which can be solved by frequency analysis. To do this effectively requires at least 680 letters of text. Friedman details a 6 page long solution by frequency analysis of a seven message problem which uses the above techniques to good form. [FRE3]

SOLUTION BY ANALYSIS OF ISOMORPHISMS

Of more interest to me, is when the message is short and does not have enough letters to solve by frequency analysis. Isomorphism is a frequent phenomena in the Autoclave cipher and generally leads to a reasonable solution.

Given the following intercepted cryptograms:

```
                          1.
USYPD  TRXDI  MLEXR  KVDBD  DQGSU  NSFBO
BEKVB  MAMMO  TXXBW  ENAXM  QLZIX  DIXGZ
PMYUC  NEVVJ  LKZEK  URCNI  FQFNN  YGSIJ
TCVNI  XDDQQ  EKKLR  VRFRF  XROCS  SJTBV
EFAAG  ZRLFD  NDSCD  MPBBV  DEWRR  NQICH
ATNNB  OUPIT  JLXTC  VAOVE  YJJLK  DMLEG
NXQWH  UVEVY  PLQGW  UPVKU  BMMLB  OAEOT
TNKKU  XLODL  WTHCZ  R.

                          2.
BIIBF  GRXLG  HOUZO  LLZNA  MHCTY  SCAAT
XRSCT  KVBWK  OTGUQ  QFJOC  YYBVK  IXDMT
KTTCF  KVKRO  BOEPL  QIGNR  IQOVJ  YKIPH
JOEYM  RPEEW  HOTJO  CRIIX  OZETZ  NK.

                          3.
HALOZ  JRRVM  MHCVB  YUHAO  EOVAC  QVVJL
KZEKU  RFRFX  YBHAL  ZOFHM  RSYJL  APGRS
XAGXD  MCUNX  XLXGZ  JPWUI  FDBBY  PVFZN
BJNNB  ITMLJ  OOSEA  ATKPB  Y.
```

Frequency distributions are made (26 x 26 matrix), based on the second letters of pairs. The data is relatively scanty and not promising.

Fortunately, there are several isomorphs available to work with.

```
Message 1     (1)  D B D D Q G S U N S F B O B E K . . .
              (2)  N E V V J L K Z E K U R C N I F . . .
              (3)  T N K K U X O L D L W T H C Z R| end of message

Message 2     (4)  C R I I X O Z E T Z N K| end of message

Message 3     (5)  C Q V V J L K Z E K U R F R F X ..
```

First, it is necessary to delimit the length of the isomorphs.

We confirm the isomorphs begins with the doubled letters. There is an E before the VV and within the isomorph. If E were included, then the letter preceding the DD would be an N to match its homolog E in the isomorph, which it is not. The evidence suggests a 10 letter isomorph, because of the tie in letter Z and the impossibility of 11 letters because of the recurrence of the letter R in isomorph (5). It is not matched with the recurrence of R in isomorph (2) nor by the recurrence of T in isomorph 3.

Applying the principles of indirect symmetry to the superimposed isomorphs, partial chains of equivalents may be constructed and most of the primary component can be established. So:

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
T E Z K R . I V F  .  .  . Q  . W  G .  N  U  S  B  X  J

24 25 26
D  O  L
```

The only missing letters are A, C, H, M, P and Y. We apply decimation on this partial reconstructed alphabet. The seventh decimation yields results:

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
T V W X Z . . D R  . U  L  I  .  B  E  F  G  J  K  .  N  O

24 25 26
.  Q  S
```

Our old friend HYDRAULIC...XZ returns to the surface. The plain component turns out to be just a normal sequence.

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

We assume a single letter key.

```
Key    ? U S Y P W T R X D I M L E X R K V D B D D Q G S
Cipher U S Y P W T R X D I M L E X R K V D B D D Q G S U
Plain  ? P H R F Y I V E F I R E O F L I G H T A R T I L ...
```

Our one letter assumption is wrong.

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

The first word suggest INTENSIVE coupled with FIRE. Plug it in and we have a key word of WICKER. The other two messages are recoverable in the same way.

```
Key    P R O M I S E R X L G H O U Z O ..
Cipher R E Q U E S T V I G O U R O U S
Plain  B I I B F G R X L G H O U Z O ....

Key    C H A R G E D R R V M M H C V B
Cipher S E C O N D B A T T A L I O N
Plain  H A L O Z J R R V M M H C V B
```

There are always several ways to skin a cat.

COMMANDANT BASSIERES

Both [ELCY] and General Givierge [GIVI] describe the two processes designed by Commandant Bassieres for solving the Autoclave cipher. He describes the preliminary process as one similar to the Kasiski analysis for determining the correct period. A search is made of the repeated letters standing exactly the group length interval apart. The single letter separation upon tabulation will present itself as one of the predominating periods.

Bassieres has two processes that follow the discovery of the period. Process 1 for a group length of 7 for instance, would take the 1st, 8th, 15th 22nd letters and consider them as a series or columns. The cryptogram is written into seven columns which permits decipherment straight down the column. Starting with key letter A the complete first column is deciphered and checked. Then we use B, C,.. until we have a good decipherment. Then on to series 2, etc. The Bassieres process no. 1 sets up the entire 26 possible decipherments for each series (column) and checks for "good" decipherments. The form of decipherment reduces to alternating Vigenere and Beauford groups. Alternate rows in his matrix of solutions reverse direction with respect to the keys.

Bassieres process no. 2 sets up a trial key of say 7 A's and this has the effect of introducing periodicity into the cryptogram at double the key length of the original key. Solution is based on periodic methods.

Phillip D. Hurst put together some tables to help solve the plain text keyed auto-key cipher. Where message and key are made up of ordinary text, both components will be subject to the 70% high frequency letter consideration - therefor, high frequency letters in the key and high frequency letters in the message will be paired again and again as the coefficients of cryptogram letters, so that cryptograms enciphered with this kind of key must contain a great many letters caused by this kind of coincidence. Tables 13 -2a,b,c show Hurst's observations for the Vigenere, Beauford and Porta ciphers. The alphabet across the top of any table is the list of possible cryptogram letters, each with its own column, each column containing only E,T,A,O,N,I,R,S,H and which if enciphered by another letter from the same group, would result in the cryptogram letter at the top of the column. The key is found to the left. Attacks are made on the second letter as discussed previously. [ELCY]

With Hurst's method the Index A(1) over Key O(2) for plain O(1) yields cipher C(2) for a Viggy. Hurst's Table 13-2a gets the answer on the first try.

Table 13-2a
Tables of High Frequency Coefficients for Autoclave Vigenere

Keys Cipher Letters

	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
E					A			E			H	I			N	O			R	S	T					
T	H	I				N	O			R	S	T						A			E					
A	A				E			H	I				N	O			R	S	T							
O		N	O			R	S	T					A			E			H	I						
N	N	O			R	S	T					A			E			H	I						
I	S	T					A			E			H	I					N	O			R			
S	I			N	O			R	S	T					A			E			H					
H	T					A			E			H	I				N	O			R	S				
R			N	O			R	S	T					A			E			H	I					
	6	4	1	-	4	4	4	4	4	2	3	4	3	2	3	2	1	4	4	2	2	6	4	4	2	4

Table 13-2b
Tables of High Frequency Coefficients for Autoclave True Beaufort/ Variant

```
Keys                    Cipher Letters

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

Table 13-2c
Tables of High Frequency Coefficients for Autoclave Porta

```
Keys                    Cipher Letters

     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
     ---------------------------------------------------
E  |     R S T             N O     A       E     H I
T  |         N O     R S T     E     H I         A
A  | N O     R S T             A       E     H I
O  |             N O     R S T   H I         A         E
N  | T             N O     R S H I         A         E
I  | R S T             N O             A         E     H I
S  |         N O     R S T     E     H I           A
H  |   R S T             N O         A       E       H I
R  |           N O     R S T       H I         A         E
     3 3 3 2 4 4 3 2 3 4 6 5 3 4 2 3 4 4 -2 3 3 3 3 3 3 2
```

C. Stanley Lamb also put out a table of rough estimate of rank and frequency of letters in cipher text for auto-key cipher. See Table 13- 3.

Table 13-3

Where Key is a Segment of Ordinary Plain Text Estimated Rank of Cryptogram Letters and Their Frequency per 10,000 Letters - from a Table of Ohaver

Vigenere

```
 V   A   I   S  ERL WHB XGM FOZ  K  N  T  P  U  J  Y  C  Q
344 314 304 296   intermediate  150112 84 84 84 72 72 64 49
```

Beaufort and Variant

```
 A   N   E   W   O   M   Z BQKJRTHVFGUDX  P   L   S  I   YC
480 262 246 246 196 196 191 intermediate 121 121 104 104 57
```

Porta

```
 K   N   L   E   RMF TWP UYQ XGC AVI BJZ   D   H   O
329 300 282 275    intermediate           132 113 97
```

SOLUTION OF PLAIN-TEXT AUTO-KEY SYSTEMS

Plain text auto-keying presents a different problem. So let me stop dancing and get on with the challenge. The mechanics of this method disclose that a repetition of n letters produces a repetition of (n-k) letters in the cipher text. When an introductory key is k letters in length then an n-letter repetition represents an (n+k) -letter repetition in the plain text. If key k equals 1, then there will be as many repetitions in the plain as in the cipher text except for true digraphic repetitions which disappear.

SINGLE KEY LETTER CASE

Look at the following plain-text encipherments of common military terms: COMMANDING, BATTALION, DIVISION, CAPTAIN.

```
Key    . B A T T A L I O N
Plain  B A T T A L I O N .
Cipher . B T M T L T W B .

Key    . C O M M A N D I N G
Plain  C O M M A N D I N G .
Cipher . Q A Y M N Q L V T .

Key    . D I V I S I O N .
Plain  D I V I S I O N
Cipher . L D D A A W B

Key    . C A P T A I N
Plain  C A P T A I N .
Cipher . C P I T I V .
```

Five observations:

1. The cipher equivalent of A(plain) is the plain text letter immediately preceding A(plain).

2. A plain-text sequence of the general formula ABA yields a doublet as a(cipher) equivalent of the final two letters; see IVI OR ISI in DIVISION.

3. Every plain-text trigraph having A(plain) as its central letter yields a cipher equivalent the last two letters of which are identical with the initial and final letters of the plain-text trigraph; see MAN in COMMANDING.

4. Every plain-text tetragraph having A(plain) as the initial and the final letter yields a cipher equivalent the second and fourth letters of which are identical with the second and third letters of the plain-text tetragraph; see APTA in CAPTAIN or ATTA in BATTALION.

5. For a single letter initial key, a repetition of n plain-text yields an (n-k) sequence of cipher letters. The simplest method of solving this type of cipher is by means of the probable word.

Message 1

```
B E C J I   B T M T L   T W B P Q   A Y M N Q   H V N E T
        B   A T T A L   I O N
W A A L C
```

The sequence BTMTLTWB fits the isomorph Battalion and we insert on the cipher text. We proceed backward and forward

```
B E C J I   B T M T L   T W B P Q   A Y M N Q   H V N E T
E A C H B   A T T A L   I O N C O   M M A N D   E R W I L

W A A L C
L P L A C
```

CRITICAL REVIEW

Masterton was right in his negative assessment of the Autokey or Autoclave cipher. Both cipher text and plain text versions have serious weaknesses which exclude them from practical or military use. They are slow to work with, prone to serious/disabling error and they can be solved even when unknown cipher alphabets are employed.

Recognition is not an issue. In both systems there are characteristics which permit of identifying a cryptogram as belonging to this class of substitution. Both cases show repetitions in the cipher text. In cipher text autokeying there will be far fewer repetitions than in the original plain text, especially when introductory keys of more than one letter in length are employed. In plain text autokeying there will be nearly as many repetitions in the cipher text as in the original plain text unless long introductory keys are employed. In either system the repetitions will show no constancy as regards intervals between them, and a uniliteral frequency distribution will come up as a polyalphabetic. Cipher text autokeying may be distinguished from its sister by the appearance of the frequency distributions of the second number of sets of two letters separated by the length of the introductory key. In the case of cipher text auto- keying these frequency distributions will be monoalphabetic in nature; its plain text keying sister will not show this characteristic.

EXTENDING THE KEY

We have looked at ciphers that suppress/destroy the periodicity, interrupt the key, and used variable lengths for grouping of plain text. We can also lengthen the key to the point where it provides insufficient text to decipher.

We can select a phrase from a book, a long mnemonic or long numerical key. However, any method of transposition applied to a single alphabetic sequence repeated several times will yield a fairly long key which approaches randomness. Another method of developing a long key from a short mnemonic one is shown below:

```
              Mnemonic Key   C H R I S T M A S
              Numerical Key  2-3-6-4-7-9-5-1-8

Extended key
               1 2  3       4             5     6         7
  C H R I S T M A|C|CH|C H R I|C H R I S T M|C H R|C H R I S|
               8           9
C H R I S T M A S|C H R I S T|
```

The original key was 9 letters and the extended one is 45 letters.

Another popular method is to take the reciprocal like 1/49 which has many digits = .02040815... as the interruptor for the key. 0 means use the first letter then use the next numbers as seeds to how many letters are to be enciphered.

RUNNING KEY CIPHER

The Running Key, aka Continuous Key, or Non Repeating Key systems in which the key consists of a sequence of elements which never repeats no matter how long the message to be enciphered happens to be. Once though indecipherable, this cipher is subject to the probable word attack and cryptanalysis when several messages with the same or superimposable initial keys are intercepted.

PROGRESSIVE KEY CIPHER

The basic principle is quite reasonable. Two or more primary elements are arranged or provided for according to a key which may be varied; the interaction of the primary elements results in a set of cipher alphabets; all the latter are employed in a fixed sequence or progression. If the number of alphabets is small, the text relatively long, this reduces to a periodic method.

The series of cipher alphabets in such a system constitutes the keying sequence. Once set up, the only remaining element in the key for a specific message is the initial cipher alphabet employed. If the keying system is used by a large group of correspondents, and employ the same starting point in the message, the cipher will fall to superimposition.

The probable word method still remains the best attack on this cipher. Suppose a cipher message contains the sequence HVGGLOWBESLTR.. and suppose we assume that the phrase THAT THE is in the key text, and find the plain text MMUNITI..

```
Assumed Key Text      . T H A T T H E
Cipher Text           . H V G G L O W B E S L T R . . .
Resultant Plain Text  . M M U N I T I
```

This suggests the word AMMUNITION. The ON in the cipher text then yields PR as the beginning of the word after THE in the Key Text.

```
Assumed Key Text      . T H A T T H E P R
Cipher Text           . H V G G L O W B E S L T R . . .
Resultant Plain Text  . M M U N I T I O N
```

PR must be followed by a vowel, perhaps O. The O yields W which may suggest WILL yielding OTEC.

```
Assumed Key Text      . T H A T T H E P R O T E C . . .
Cipher Text           . H V G G L O W B E S L T R . . .
Resultant Plain Text  . M M U N I T I O N W I L L . . .
```

This suggests the words PROTECTION, PROTECTIVE, PROTECTING, etc. We coerce a few letters in each direction.

When we have multiple messages, we can superimpose them assuming the correct reference point. Correct superimposition with reference to the key text will provide the addition of two to three letters to the key and assumptions for words in several messages. This leads to the assumption of more letters, etc.

SOLUTION OF A PROGRESSIVE-ALPHABET CIPHER WHEN CIPHER ALPHABETS ARE KNOWN

Use the cipher alphabet HYDRAULIC..XZ sequence sliding against itself continuously producing secondary alphabets in 1 - 26. Starting with alphabet 1:

```
Plain   HYDRAULICBEFGJKMNOPQSTVWXZHYD ...
Cipher  HYDRAULICBEFGJKMNOPQSTVWXZ

Letter 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21
Alpha  1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21
Plain  E N E M Y H A S P  L  A  C  E  D  H  E  A  V  Y  I  N
Cipher E O G P U U E Y H  M  K  Q  V  M  K  Z  S  J  Q  H  E

Letter 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39
Alpha  22 23 24 25 26 1  2  3  4  5  6  7  8  9  10 11 12 13
Plain  T  E  R  D  I  C  T  I  O  N  F  I  R  E  U  P  O  N
Cipher N  L  H  H  L  C  V  B  S  S  N  J  E  P  K  D  D  D

Letter 40 41 42 43 44 45 46 47 48 49 50 51 52 53
Alpha  14 15 16 17 18 19 20 21 22 23 24 25 26  1
Plain   Z  A  N  E  S  V  I  L  L  E  R  O  A  D
Cipher  G  P  U  H  F  K  H  H  Y  L  H  M  R  D
```

This method reduces to a periodic system involving 26 secondary alphabets and used in simple progression. The 1st, 27th, 53rd letters are in the 1st alphabet; the 2nd, 28th, 54th are in the 2nd alphabet and so on.

Solving the above, knowing the two primary components is not too difficult. We lack only the starting point. The solution becomes evident by completing the plain component and examining the diagonals of the diagram, the plain text becomes evident. Try:

Given: H I D C T E H U X I ; We complete the plain component sequences initiated by successive cipher letters, the plain text E N E M Y M A C H I is seen to come out in successive steps upwards in Figure 13-1. Had the cipher component been shifted in opposite directions during encipherment, the plain text would be visible downward on the diagonal. If the sliding strips had been set up according to the sequence of cipher letters on the diagonal, then the plaintext would be seen as one generatrix.

GENERAL SOLUTION FOR CIPHERS INVOLVING A LONG-KEYING SEQUENCE OF FIXED LENGTH AND COMPOSITION

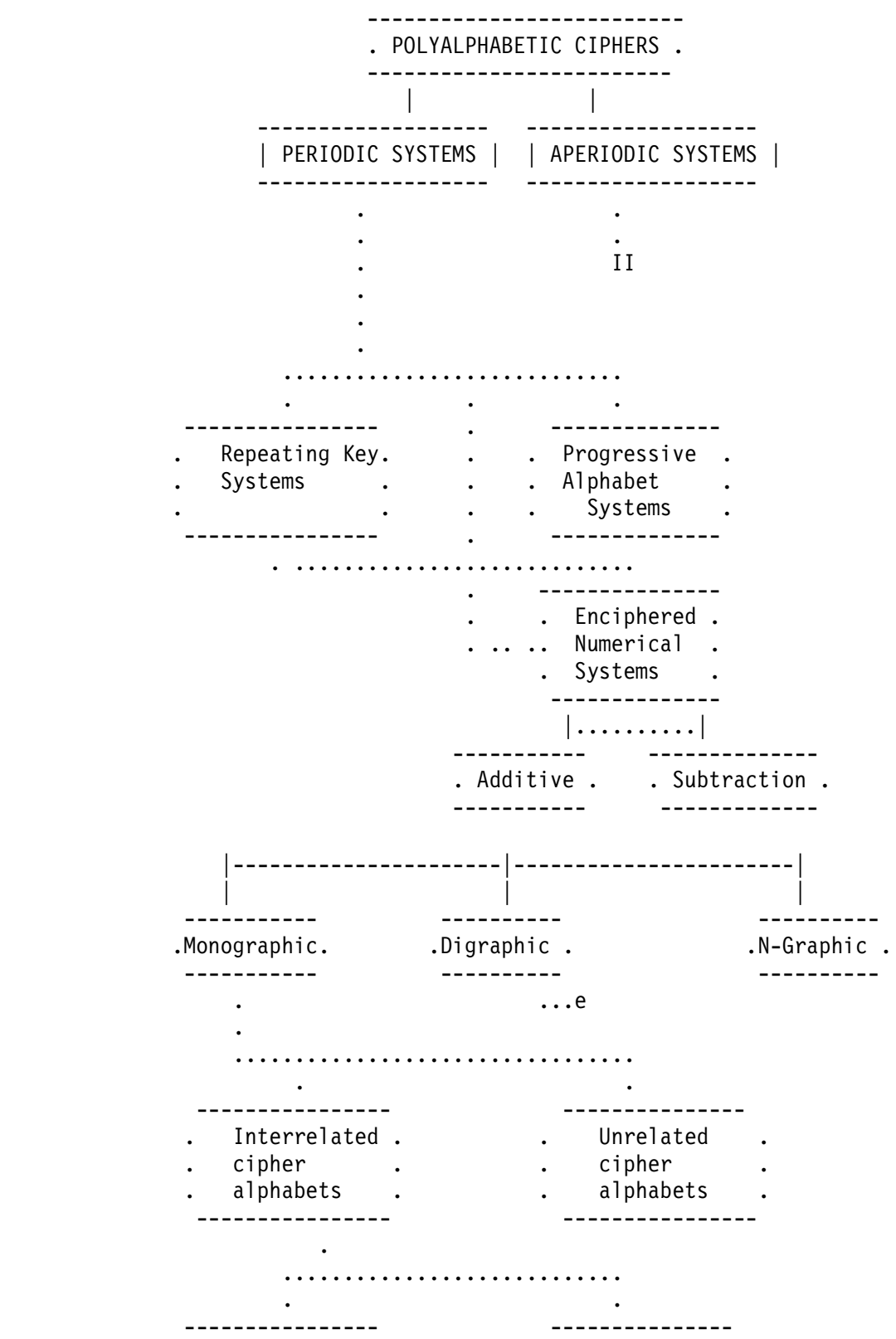
No matter how the keying sequence is derived, if all the same correspondents employ the same key, or if this key is used many times by a single office, and if it always begins at the same point, the various messages can be solved by superimposition. If there are sufficient messages than the successive columns can be solved by frequency analysis. This holds no matter how long the keying sequence and regardless of whether the keying sequence is intelligible or random text.

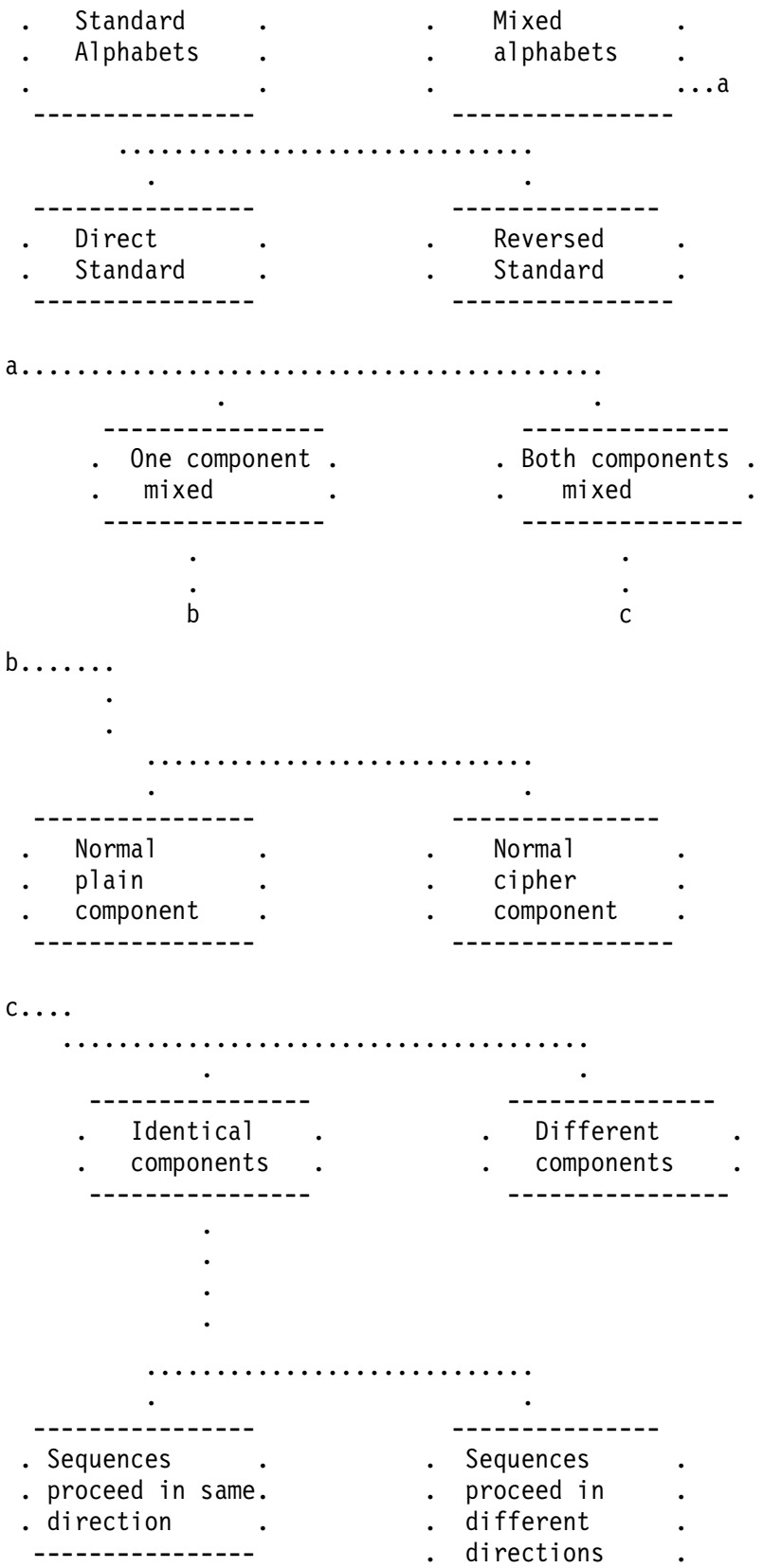
If the messages do not start at the same point, then we must find a tie element to line up the columns. The tie element is similar to the chemical engineering principle of material balance and provides a stable point for the text to be anchored for analysis. Find one 5 letter polygraph that is common to two messages and align the messages for super- imposition based on their position. Next we find a smaller tie group of say 4 letters and tie the second message with a third. We can extend the process to trigraphs or even digraphs between the messages. The first step then is to examine the messages for repetitions. If there are enough we can use the probable word method to set up plain - cipher equivalencies and to reconstruct the primary components. [FRE3]

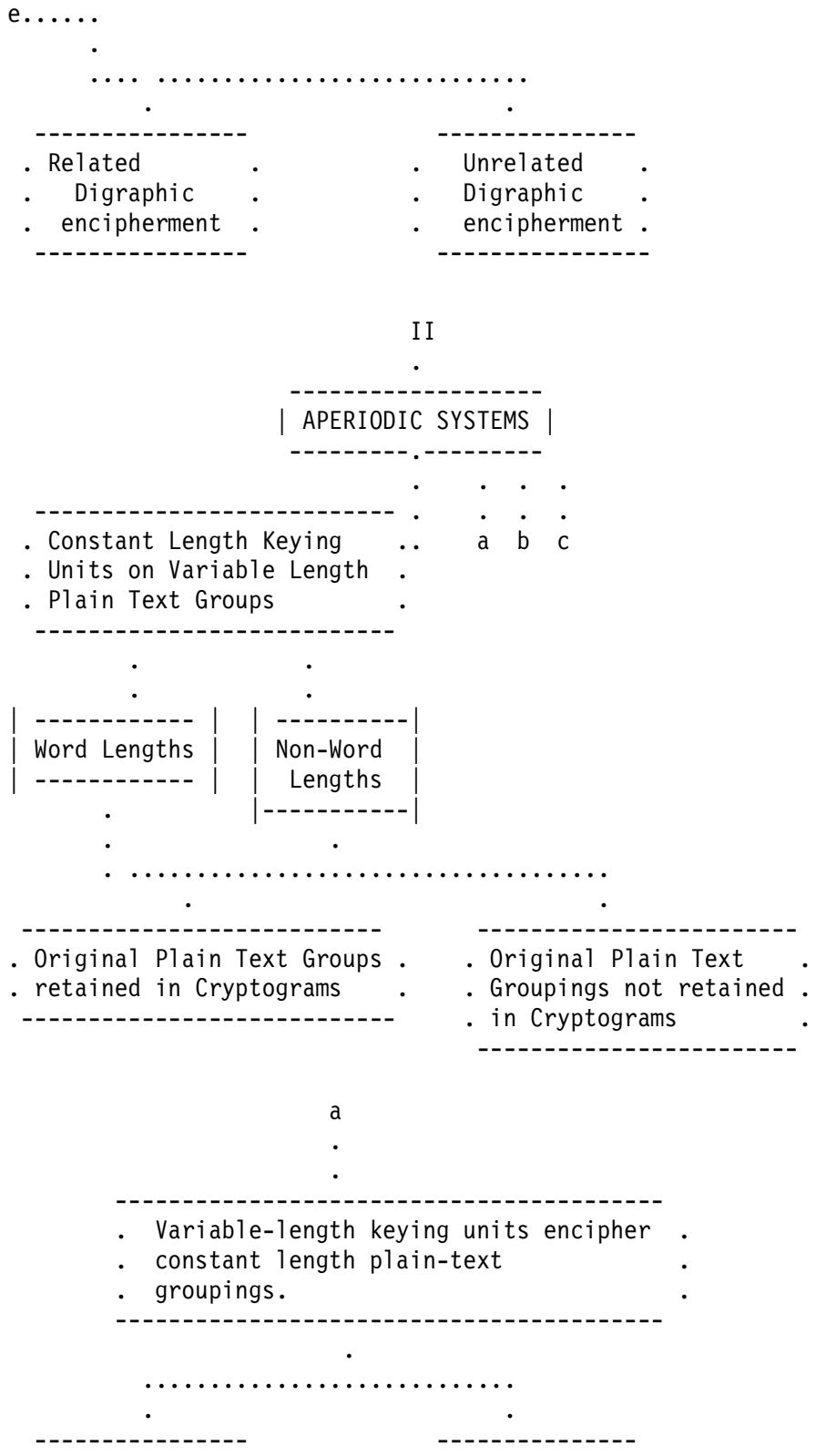
Figure 13-1

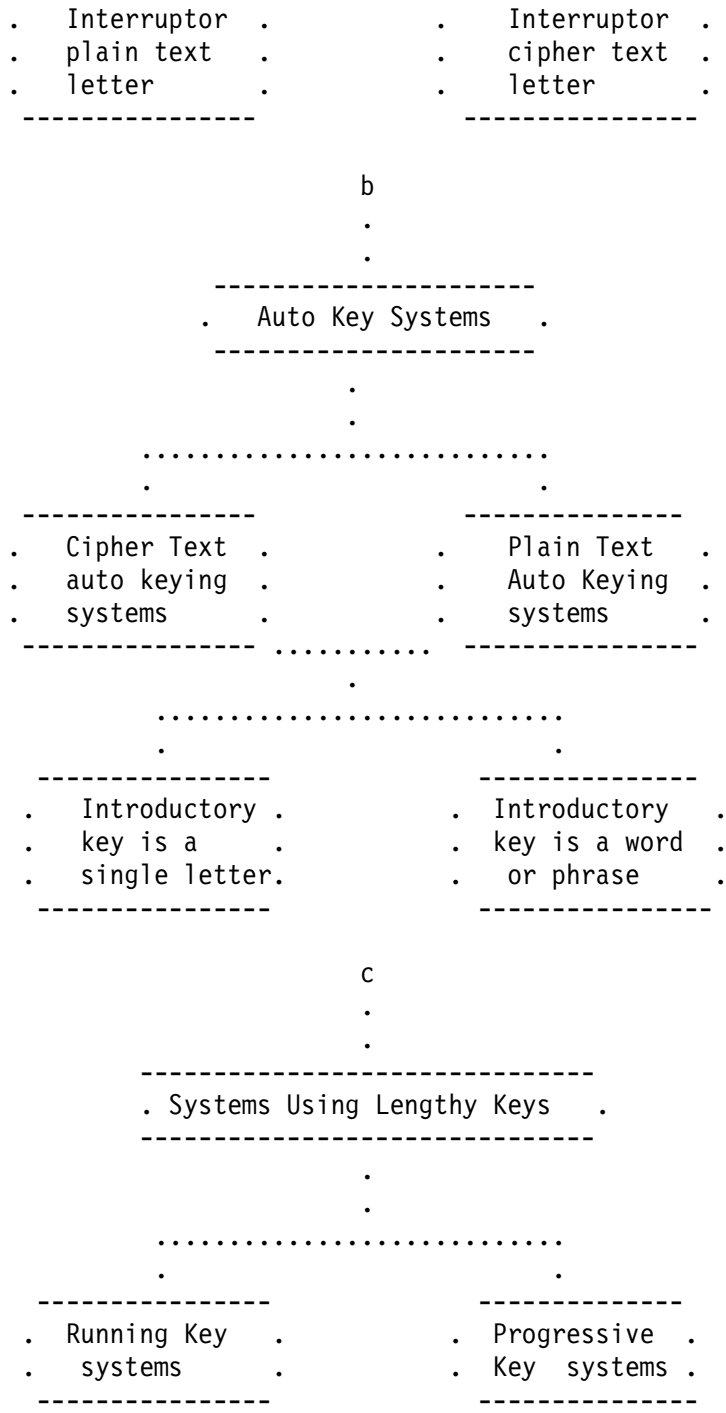
```
H I D C T E H U X I
Y C R B V F Y L Z I
D B A E W G D I H C
R E U F X J R C Y B
A F L G Z K A B D E
U G I J H M U E R F
L J C K Y N L F A G
I K B M D O I G U J
C M E N R P C J L K
B N F O A Q B K I M
E O G P U S E M C N
F P J Q L T F N B O
G Q K S I V G O E P
```

ANALYTICAL KEY FOR LECTURES 10 - 13




Standard Alphabets
Mixed alphabets
a
Direct Standard
Reversed Standard
a
One component mixed
Both components mixed
b
c
b
Normal plain component
Normal cipher component
c
Identical components
Different components
Sequences proceed in same direction
Sequences proceed in different directions


Related Digraphic encipherment
Unrelated Digraphic encipherment
II
APERIODIC SYSTEMS
Constant Length Keying
Units on Variable Length
Plain Text Groups
a b c
Word Lengths
Non-Word Lengths
Original Plain Text Groups retained in Cryptograms
Original Plain Text Groupings not retained in Cryptograms
a
Variable-length keying units encipher constant length plain-text groupings.


Interruptor plain text letter
Interruptor cipher text letter
b
Auto Key Systems
Cipher Text auto keying systems
Plain Text Auto Keying systems
Introductory key is a single letter.
Introductory key is a word or phrase
c
Systems Using Lengthy Keys
Running Key systems
Progressive Key systems

LECTURE 12 SOLUTIONS

Thanks to DAVLIN & DR FOX-G for their solutions for Lecture 12 problems:

12.1 Nihilist Substitution
When you are doing your addition and subtractions, work carefully to avoid mistakes.

Keywords: CAREFUL, GUIDANCE

12.2 Nihilist Substitution
Perseverance is the mark of a true cryptogram addict. Be patient and you can do it.

Keywords: SOLVE, CRYPTFANS

12.3 Porta
Conservative scientists have predicted the end of change at various times but they have always been proved wrong.

Keyword: CHANGE

12.4 Porta
In a leisure society constant rebuilding of your own home to your own taste, filling it with personal ingenuities and bold signs might become the fashionable thing to do.

Keyword: EQUALITY

12.5 Portax
Thank you for your letters and suggestions for the Novice Notes series. Keep them coming. (signed) LEDGE

Keyword: THANKS

12.6 Portax
Now, that the new year has come, might be the time to realize that even the best resolutions are meant to be broken.

Keyword: BROKEN

12.7 Gromark
The crazy person says "I am Abraham Lincoln" and the neurotic says "I wish I were Abraham Lincoln" and the healthy person says "I am I and you are you". Frederick Perls

Keyword: Neurotics

LECTURE 13 PROBLEMS

13-1 Beaufort

```
ABRVJ  UTAMP  YPLHZ  OZYAP  YPJNP  KNXUG
QRDPC  ELPNC  BVCEF  NLLSJ  LGOWC  VYCGA
EVGIX  XNDKY  U.  (butter) (INWVQH)
```

13-2 Vigenere.

```
DWNIT  KGEWZ  ENJQZ  WXLLZ  WZOKC  ETOWI  NXVQS
DQGAK  MGGBH  NAMWE  OWVAM  UJDVQ  IMDSB  VCCTR
YUIQX.  (making, UHVW)
```

13-3 Vigenere Running Key

```
YPOSC  DWVWY  CCHZT  AKALF  I.  (tolls -2)
```

13-4 Vigenere Progressive key. "Fungi"

```
IPGPUPX  GTIAKNP  AMEHLAW  SJSTROZ  TCGYUND  STNPJZM
OESWAXG  VLHSPZC  GNEIWHP  EKHNOWW  PMEQFVV  PDQAWCA
GGFRKSO  RCHZVKL  NBWHYBV  CUNBBBB  AVGCJFA  FLTMKUV  K.
```

REFERENCES / RESOURCES

I will issue additional references/resources at a later Lecture to conserve mailing costs and reduce file download size.