CLASSICAL CRYPTOGRAPHY COURSE
BY LANAKI

September 9, 1996

LECTURE 17

HEADLINE PUZZLES, PLAYFAIR, FOURSQUARE FRACTIONATION AND DELASTELLE SYSTEMS

SUMMARY

I think this lecture is both interesting and perhaps difficult. We start off with PHOTON's Headliner Cipher which combines many of the principles found in Lectures 1 and 10 - 12 of this course. We then shift into Digraphic systems with the Playfair and Foursquare Ciphers. We develop the theory of fractionation and illustrate it with difficult classical systems known as the Bifid and Trifid ciphers. Both of these latter cipher systems were invented by the French cryptographer Delastelle. We develop our lecture with the help of the following references: [ELCY], [BOW1], [BOW2], [BOW3], [BOW4], [HITT], [LEWI], [NICH] and [PHOT]. At the end of my lecture is a special note regarding Diophantine equations, a subject which is a bit esoteric and has interested several of our class.

HEADLINE PUZZLES (PHOTON)

Thirty years ago, Paul Derthick began publishing the HEADLINE PUZZLE in the NSA monthly newsletter for professional cryptologists. Paul is no longer with us, but his puzzles continue to be written monthly by Larry Gray to challenge and frustrate his successors. We thank PHOTON for exposing us to this wonderful cipher. I have condensed his soon to be published paper. [PHOT]

Headline Puzzles demonstrate a variety of cryptographic principles. Each puzzle contains five headlines from recent daily newspapers. Each of the five is a different monoalphabetic substitution, and all five are derived from the same mixed alphabet at different settings against itself. A complete solution includes recovering the headlines, the key, the setting and the hat.

In Paul's words, "The use of headlines was a happily malicious thought. It permits the inclusion of outrageous proper names, and has the tendency to exclude the commonest words." But even though the five headlines may include some tough problems, finding the three words (key, setting and hat) needed for a complete solution may be even more challenging.

WALKING THROUGH A SOLUTION

Given:

1. AMHXZLX ALXNSTXO APYBX NLJXHXK LI ZJL AHWHMHBX BHUAUBIZ;

2. GHDMRJGB MCGHE CKXCDMCQH SP RLCEE OSEE, ZHMCGHE MSU DJCC EOSM;

3. WYNAJSM PYXMKANWAJKANB VNYLXPA MAFN-VANWAPK CXMLNAL LYQQFN IJQQB;

4. XOAJRH DOHU XFNIRA MPS GRNC RBQTSPBIRBHNF FNG RBMPSDRIRBH;

5. FRHRXIQ ALVTURXF RQX. VALPPF SI VXCMRLP XLVJ LPFPVLXU

The general outline of solution is to: 1) solve any two headlines and use them to find a mixed alphabet that solves all five headlines; 2) solve the rest of the headlines and use all five to recover the setting; 3) recover the key block and the sequence of transposition; 4) recover the original mixed alphabet by decimation; and 5) finally, recover the hat (the word whose alphabetic sequence of letters determines the transposition sequence from the keyblock).

Step 1:SOLVE ANY TWO HEADLINES

Since the initial step is to solve any two headlines, we look for nice wedges in any two. The first probable wedges to catch my eye in this example are the long pattern words in headlines 3 and 4. The 14 letter word in headline 3. has the pattern ABCDEFGHFIEFGJ, yielding "counterfeiters" from the pattern word dictionary. Substituting the letters in the headline produces a nice wedge! Then a little trial and error produces, "Foreign counterfeiters produce near-perfect hundred dollar bills":

```
   forei n counterfeiters  ro uce ne r- erfect  un re   o   r   i  s
3. WYNAJSM PYXMKANWAJKANB VNYLXPA MAFN-VANWAPK CXMLNAL LYQQFN  IJQQB
           ABCDEFGHFIEFGJ
```

The 13 letter pattern word in headline 4. has the pattern ABCDEFBGABHIJ, yielding "environmental" from the pattern word dictionary. Substituting the letters in the headline also produces a nice wedge; not as nice, but good enough to produce "Budget cuts blamed for weak environmental law enforcement":

```
       et    t    lame    or   ea   environmental  la   en or ement
4. XOAJRH  DOHU  XFNIRA  MPS  GRNC  RBQTSPBIRBHNF  FNG  RBMPSDRIRBH
                                     ABCDEFBGABHIJ
```

Solving the first two headlines is seldom this easy; but as you can see, long pattern words make nice wedges when they are available. We assume that the reader knows how to solve monoalphabetic ciphers with word divisions (Aristocrats - see chapter 1 in [NICH]).

The current recovery of plain-text to cipher-text is:

```
   a b c d e f g h i j k l m n o p q r s t u v w x y z
1.
2.
3. F I P L A W S C J     Q   M Y V   N B K X
4. N X D A R M J   T   C F I B P     S U H O Q G
5.
```

Figure 17-1.

Step 2:FIND A MIXED ALPHABET THAT SOLVES ALL FIVE HEADLINES

The columns in Figure 17-1 are arranged alphabetically by the plain letters for ease in building chains. Each vertical column is fixed, regardless of the sequence of the columns because each plain letter stands for only one cipher letter in each of the headlines. The purpose of chaining is to find an alphabetic sequence for the fixed columns that is the same in each row. The sequence we derive from chaining will not necessarily be the original mixed sequence; but it will solve all five headlines when the rows are set against themselves. For the rest of this section we will refer to the mixed alphabet derived from chaining as an equivalent alphabet.

Note that the equivalent alphabet is not unique. There are 6 equivalent alphabets which are odd decimations of the original (e.g. every third letter, every fifth letter etc. in a 26 letter cycle), 6 odd decimations that are the same as the first six, but in the reverse order; 6 even decimations that give two cycles of thirteen letters each (rather than a single cycle of 26 letters); 6 even decimations that are the same as the first six even decimations, but reversed; and a single decimation with the same two letters repeated 13 times. Only the 26-letter cycles are useful results from chaining, so we will look only for odd decimations when recovering the keyblock and the original mixed alphabet.

Chaining capitalizes on the symmetry of letter positions in the fixed columns and their relative distances apart in related alphabets. For example: if plain A equals cipher F in line 3, and plain F equals cipher W, then the distance between plain A and plain F is the same as the distance between cipher F and cipher W in their respective alphabets. A two-dimensional chain combines the relationships of the plain alphabet and two different cipher alphabets. In this example, we put line 3. cipher-text letters vertically under the plain- text letters; and put line 4. cipher-text letters horizontally to the right of the plain-text letters. In that way we generate a two-dimensional interactive chain with the same equivalent alphabet in each vertical line, and a different equivalent alphabet in each horizontal line. Please refer to Figures 17-2 and 17-3 for what the display looks like on graph paper.

Arbitrarily starting with the plain A and cipher F (line 3) gives me part of the vertical chain (A over F). Then looking at plain F over cipher W adds W to the chain (under the F). Looking at plain W, however, shows that no cipher letter has been identified in line 3 for plain W, so we show "." as a place-filler. Returning to cipher A (line 3), we find cipher A under plain E, but no cipher E to continue the chain, so we show "." as a place-filler. See the diagram in Figure 17-2 for the vertical chain fragment EAFW.

Then we make a horizontal chain on each of the letters of the vertical chain, using the plain alphabet and cipher line 4. The first horizontal line is from cipher R to the right of plain E, cipher S to the right of plain R, etc. giving the horizontal chain fragment ERSUOP. Similarly, completing the next three horizontal fragments looks like the matrix in Figure 17-2.

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

Figure 17-2

Continuing to expand the chains shows quickly that the horizontal chain repeats with a 13 letter cycle, indicating that it is from an even decimation (and therefore not useful a this time). The vertical chain, however, contains a full 26 letter mixed alphabet, indicating a useful decimation. The result looks like the matrix in Figure 17-3 after only a few iterations.

```
        I
        J
        U
        X
        T
        K
        O
        Y
        H
        C
        P
        V
        .
        D
        L
    Y V Q W G J K C D A N B X Y V  (13 LETTER CYCLE)
  I T H E R S U O P L F M I T H    (13 LETTER CYCLE)
J K C D A N B X Y V
    P L F M I T H .
      Q W G J K C D A N B X
      E R S U O P
  C D A N B X Y V
        M
        G
        S
        B
        I
```

Figure 17-3

Note how the chain fragments grow interactively, with the horizontal chain providing letters for the vertical chain and visa versa. Also note that all the vertical segments are parts of the same equivalent alphabet. When an overlap is discovered, the chain can be expanded by inspection. Look, for example, at the bottom vertical segment NMGSBI and see how it came from combining segments from the two columns to its right. Similarly, the horizontal chain segments are, by chance, part of two independent 13 letter cycles which can be expanded to other horizontal chains by inspection.

Only one letter eluded detection by two-dimensional chaining; so it isn't hard to identify it and fill in the "Z". There is no need to activate a third dimension or solve another aristocrat in this example. We have been able to find a complete 26-letter alphabet with only two solved headlines in almost every case. The equivalent alphabet in this example is:

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

Step 3: RECOVER THE SETTING AND THE INDEX LETTER

Any of the equivalent alphabets will solve the remainder of the headlines, so we'll use this one instead of waiting until recovery of the original alphabet. Now that we have an alphabet to slide against itself, we simply write out the alphabet on a sheet of graph paper, and write it twice on a second sheet that we slide along the first. Then we attack the unsolved headlines at their shortest (usually two letter) words. Recognizing that one of those letters will be a vowel, we simply try all the vowels on one letter until the second letter makes a good word. Then we keep that slide position and try another word to verify it. R. MASTERTON observes another type wedge, in "Solving Cipher Problems"; "You would be amazed at the number of times the second word ends with S and the third is a short word such as TO."

Attacking headline 1. with the slide setting in Figure 17-4 shows that LI = of (verified with ZJL = two), and the whole headline reads. "Clinton condemns Cuban downing of two civilian aircraft".

```
    i j u x t k o y h c p v z d l q e a f w r n m g s b
O Y H C P V Z D L Q E A F W R N M G S B I J U X T K O Y

H C . .
```

Figure 17-4

After applying the same technique to headlines 2 (SP = of) and 5 (SI = to), the setting for each headline is shown in Figure 17-5. The setting word "SHARP" shows clearly under the index letter "e". We'll need both the setting and the index later.

```
    i j u x t k o y h c p v z d l q e a f w r n m g s b
    -------------------------------------------------
 1. H C P V Z D L Q E A F W R N M G S B I J U X T K O Y
 2. F W R N M G S B I J U X T K O Y H C P V Z D L Q E A
 3. J U X T K O Y H C P V Z D L Q E A F W R N M G S B I
 4. T K O Y H C P V Z D L Q E A F W R N M G S B I J U X
 5. R N M G S B I J U X T K O Y H C P V Z D L Q E A F W

     Setting = SHARP  Index = E
```

Figure 17-5

Note: The setting might read up the column, rather than down, or be derived from plain-text alphabets under a single cipher-text alphabet, rather than cipher-text alphabets under a single plain-text alphabet.

Step 4:RECOVER THE KEY BLOCK

The literature suggests that we examine the equivalent alphabet looking for sequences of letters (like ABC in this example). Then examine the alphabet to see if another sequence is a uniform distance from each letter (viz: L is 3 before A, M is 3 before B, O is 3 before C) and decimate by the uniform distance. That works, but it's not always obvious (to me). So we force the display to show me sequences by aligning the equivalent alphabet vertically in strips. For convenience we order them across the middle in alphabetic sequence (similar to the sequence of unused letters in a

keyblock). Then the appropriate decimation is much more obvious. See Figure 17-6. Sometimes the key is in plain view. We made the matrix in Figure 17-6. by hand the first couple of times; and then wrote a short computer program to do the drudgery. The rows and columns are numbered for convenience in referring to them.

Since we look for the key word and for alphabetic sequences of unused letters in the key block, and for them horizontally in Figure 17-6. The highest concentration of alphabetic sequences are in rows -6, - 3, 3 and 6 indicating that a decimation of three might be a good choice. We call this a goodness test in the computer program; and it has always led me to the right decimation. The "goodness" column from PHOTON'S computer program is merely the sum of alphabetically adjacent letters in a horizontal row - indicating likelihood of finding significant pieces of the unused letters in a keyblock.

```
-12 k d g j t o v m l q w u p c r s x h z f e b y a n i
-11 o l s u k y z g q e r x v p n b t c d w a i h f m j
-10 y q b x o h d s e a n t z v m i k p l r f j c w g u
 -9 h e i t y c l b a f m k d z g j o v q n w u p r s x
 -8 c a j k h p q i f w g o l d s u y z e m r x v n b t
 -7 p f u o c v e j w r s y q l b x h d a g n t z m i k
 -6 v w x y p z a u r n b h e q i t c l f s m k d g j o
 -5 z r t h v d f x n m i c a r j k p q w b g o l s u y
 -4 d n k c z l w t m g j p f a u o v e r i s y q b x h
 -3 l m o p d q r k g s u v w f x y z a n j b h e i t c
 -2 q g y v l e n o s b x z r w t h d f m u i c a j k p
 -1 e s h z q a m y b i t d n r k c l w g x j p f u o v
Ref 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 f i p l a w s c j u o q g m y v e n b k x z r t h d
  2 w j v q f r b p u x y e s g h z a m i o t d n k c l
  3 r u z e w n i v x t h a b s c d f g j y k l m o p q
  4 n x d a r m j z t k c f i b p l w s u h o q g y v e
  5 m t l f n g u d k o p w j i v q r b x c y e s h z a
  6 g k q w m s x l o y v r u j z e n i t p h a b c d f
  7 s o e r g b t q y h z n x u d a m j k v c f i p l w
  8 b y a n s i k e h c d m t x l f g u o z p w j v q r
  9 i h f m b j o a c p l g k t q w s x y d v r u z e n
 10 j c w g i u y f p v q s o k e r b t h l z n x d a m
 11 u p r s j x h w v z e b y o a n i k c q d m t l f g
 12 x v n b u t c r z d a i h y f m j o p e l g k q w s
 13 t z m i x k p n d l f j c h w g u y v a q s o e r b

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

Figure 17-6

Note in column 1, for example, that the alphabetic sequence reading up the column from the reference line to -3 and -6 is ALV, and in column 2 it is BMW, and in column 3 it is COX (all in alphabetic sequence). So the apparent order of the key block is up the columns. Since we wrote the equivalent alphabets down the columns, the decimation must be in the opposite (minus) direction. Figure 17-7. shows the likely keyblock lines arranging from top to bottom for ease in reading.

In forming the keyblock, the columns must stay intact to maintain the integrity of the mixed alphabet, but the rows can be rearranged because the horizontal alphabetic sequence was artificially created to get a sense of order. The key word will be on the top line of the keyblock, perhaps wrapped around onto the second line.

```
  3 r u z e w n i v x t h a b s c d f g j y k l m o p q
Ref 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
 -3 l m o p d q r k g s u v w f x y z a n j b h e i t c
 -6 v w x y p z a u r n b h e q i t c l f s m k d g j o

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

Figure 17-7

Figure 8. shows the result of developing the keyblock from the information in Figure 17-7. Look at line -3 in Figure 17-7. and strike through the columns that were not in alphabetical sequence (columns 5, 8, 9, 14, 20, 21, 22, 23, 24, and 26). Then we looked at what remained in row 3, and saw the word "zenith". Noticing that the letter C was in the reference row under the Z in zenith, Terminate the first row at B. The resulting perfect keyblock confirms the decimation of minus three.

```
z e n i t h a b
c d f g j k l m
o p q r s u v w
x y

KEY =ZENITH
```

Figure 17-8

Step 5:RECOVER THE MIXED ALPHABET

The original alphabet in Figure 17-9 can now be read directly from Figure 17-6 by starting with the index letter "e" and reading every third letter vertically in any column:

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

Figure 17-9

Step 6:RECOVER THE HAT

Two essential elements are needed to recover the hat. First, the transposition sequence of reading columns from the keyblock. And second, the relationship between the words used for the setting, the key and the hat. The transposition sequence is the alphabetic sequence of letters in the hat word. The relationship of the hat to the setting and the key comes from your determination of the relationship between the setting and the key alone. The transposition sequence from the keyblock to the mixed alphabet can be read directly. From the original alphabet in Figure 17-9, refer to the keyblock in Figure 17-8. Start with the index letter "E", read down EDPY, then down TJS, then down NFQ etc. The full sequence is shown in Figure 17-10.

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

Figure 17-10

And now we know that the alphabetic sequence of letters in the hat word is 4 1 3 5 2 7 6 8; and that the word is related to the key word (ZENITH) and to the setting word (SHARP).

There are at least two ways to find the hat. The method illustrated in Figure 17-11 uses the alphabetic sequence of each letter position in the hat and defines the limits for each position. In the first text line of Figure 17-11 the letter A could be

at positions 1 and 2, but not at the other position. Only position 3 could have a letter as low as B, positions 4, 5 and 7 could have letters as low as C, depending on the letter in position, positions 7 and 8 could have letters as low as D, depending on the values above. Likewise at the high end, only positions 7 and 8 could have a letter as high as Z etc.

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

Figure 17-11

In each of the HEADLINE PUZZLES, research on the relationships recovers the hat faster and with more enjoyment than working the positional possibilities. Relating the words SHARP and ZENITH suggests manu - facturers of electronic stuff like computers and radios and television sets. So we examined the names of other manufacturers, like Toshiba, Panasonic, Motorola, Magnavox, Pioneer, Hitachi etc. only MAGNAVOX matches the length and alphabetic sequence. The name "HAT" came from the position of the transcription word on top of the keyblock.

```
M A G N A V O X          Hat = MAGNAVOX
4 1 3 5 2 7 6 8
Z E N I T H A B          Key = ZENITH
C D F G J K L M
O P Q R S U V M          Setting =SHARP
X Y

   e d p y t j s n f q z c o x I g r a l v h k u b m w
   -------------------------------------------------
1. S N F Q Z C O X I G R A L V H K U B M W E D P Y T J
2. H K U B M W E D P Y T J S N F Q Z C O X I G R A L V
3. A L V H K U B M W E D P Y T J S N F Q Z C O X I G R
4. R A L V H K U B M W E D P Y T J S N F Q Z C O X I G
5. P Y T J S N F Q Z C O X I G R A L V H K U B M W E D
```

Figure 17-12

Now that we've completed the solution, it's interesting to confirm that the original mixed alphabet in Figure 17-12 gives the same solution to the headlines as the equivalent alphabet developed earlier in Figure 17-5.

Step 7:Complete Solution:

1. CLINTON CONDEMNS CUBAN DOWNING OF TWO CIVILIAN AIRCRAFT;

2. KENTUCKY TAKES ADVANTAGE OF UMASS LOSS, RETAKES TOP NCAA SLOT;

3. FOREIGN COUNTERFEITERS PRODUCE NEAR-PERFECT HUNDRED DOLLAR BILLS;

4. BUDGET CUTS BLAMED FOR WEAK ENVIRONMENTAL LAW ENFORCEMENT;

5. SILICON GRAPHICS INC. AGREES TO ACQUIRE CRAY RESEARCH

Setting = SHARP Key = ZENITH Hat = MAGNAVOX

Along with Paul Derthick's notes, "Introduction to the HEADLINE PUZZLE", other references are: [LEWI], [NICH], [ELCY], [SINK], [FRE1] [FRE2]. The HEADLINE PUZZLES in this section are used with permission of PHOTON and the NSA monthly newsletter.

DIGRAPHIC CIPHERS: PLAYFAIR

Perhaps the most famous cipher of 1943 involved the future president of U.S., J. F. Kennedy, Jr. [KAHN] On 2 August 1943, Australian Coastwatcher Lieutenant Arthur Reginald Evans of the Royal Australian Naval Volunteer Reserve saw a pinpoint of flame on the dark waters of Blackett Strait from his jungle ridge on Kolombangara Island, one of the Solomons. He did not know that the Japanese destroyer Amagiri had rammed and sliced in half an American patrol boat PT-109, under the command of Lieutenant John F. Kennedy, United States Naval Reserve. Evans received the following message at 0930 on the morning of the 2 of August 1943:

29gps

KXJEY UREBE ZWEHE WRYTU HEYFS
KREHE GOYFI WTTTU OLKSY CAJPO
BOTEI ZONTX BYBWT GONEY CUZWR
GDSON SXBOU YWRHE BAAHY USEDQ

/0930/2

Translation:

PT BOAT ONE ONE NINE LOST IN ACTION IN BLACKETT
STRAIT TWO MILES SW MERESU COVE X CREW OF TWELVE
X REQUEST ANY INFORMATION.

The coastwatchers regularly used the Playfair system. Evans deciphered it with the key ROYAL NEW ZEALAND NAVY and learned of Kennedy's fate. Evans reported back to the coastwatcher near Munda, call sign PWD, that Object still floating between Merusu and Gizo, and at 1:12 pm, Evans was told by Coastwatcher KEN on Guadalcanal that there was a possibility of survivors landing either on Vangavanga or near islands. That is what Kennedy and his crew had done. They had swum to Plum Pudding Island on the Southeastern tip of Gizo Island.

Several messages passed between PWD, KEN and GSE (Evans). The Japanese made no attempt to capture Kennedy even though they had access to the various messages. The importance to them was missed even though many P-40's were spotted in the Search and Rescue (SAR) attempt. maybe the Japanese didn't want to waste the time or men because the exact location of the crew was not specified. A Japanese barge chugged past Kennedy's hideout. On 0920 a.m. on Saturday morning 7 August 1943, two natives found the sailors, who had moved to Gross Island, and had reported to find Evans. He wrote a brief message: Eleven survivors PT boat on Gross Is X Have sent food and letter advising senior come here without delay X Warn aviation of canoes crossing Ferguson RE. The square Evans used was based on the key PHYSICAL EXAMINATION :

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

The encipherment did not split the doubled letters as is the rule:

```
XELWA  OHWUW  YZMWI  HOMNE  OBTFW
MSSPI  AJLUO  EAONG  OOFCM  FEXTT
CWCFZ  YIPTF  EOBHM  WEMOC  SAWCZ
SNYNW  MGXEL  HEZCU  FNZYL  NSBTB
DANFK  OPEWM  SSHBK  GCWFV  EKMUE
```

There were 335 letters in 5 messages, in the same key beginning XYAWO GAOOA GPEMO HPQCW IPNLG RPIXL TXLOA NNYCS YXBOY MNBIN YOBTY QYNAI ..., for Lieut. Kennedy considers it advisable that he pilot PT boat tonight X ... These five messages detailed the rescue arrangements, which offered the Japanese a chance to not only get the crew (and change all history!) and the force coming out to save it. The Japanese failed to solve what an experienced crypee could solve in one hour. At 1000 hours that same day Kennedy and his crew was rescued.

Digraphic substitution refers to the use of pairs of letters to substitute for other pairs of letters. The Playfair system was originated by the noted British scientist, Sir Charles Wheatstone (1802 - 1875) but, as far as known, it was not employed for military or diplomatic use during his lifetime. About 1890 it was adopted for use by the British Foreign Office on the recommendation of Lord Lyon Playfair (1818-1898) and thereafter identified with its sponsor.

Encipherment

The Playfair is based on a 25 letter alphabet (omit J) set up in a 5 X 5 square. A keyword is written in horizontally into the top rows of the square and the remaining letters follow in regular order. So for the key = LOGARITHM, we have:

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

In preparation for encipherment, the plaintext is separated into pairs. Doubled letters such as SS or NN are separated by a null.

For example, "COME QUICKLY WE NEED HELP" we have

CO ME QU IC KL YW EN EX ED HE LP

There are three rules governing encipherment:

1. When the two letters of a plain text pair are in the same column of the square, each is enciphered by the letter directly below it in that column. The letter at the bottom is enciphered by the letter at the top of the same column.

```
Plain    Cipher
 OP        TW
 IC        CN
 EX        QG
```

2. When the two letters of a plain text pair are in the same row of the square, each is enciphered by the letter directly to its right in that row. The letter at the extreme right of the row is enciphered by the letter at the extreme left of the same row.

Plain	Cipher
YW	ZX
ED	FE
QU	SN

3. When two letters are located in different rows and columns, they are enciphered by the two letters which form a rectangle with them, beginning with the letter in the SAME ROW with the first letter of the plaintext pair. (This occurs about 2/3 of the time.)

Plain	Cipher
CO	DL
ME	HF
KL	CR
LP	ON

Decipherment, when the keyword is known, is accomplished by using the rules in reverse.

Identification Of The Playfair

The following features apply to the Playfair:

1. It is a substitution cipher.

2. The cipher message contains an even number of letters.

3. A frequency count will show no more than 25 letters. (The letter J is not found.)

4. If long repeats occur, they will be at irregular intervals. In most cases, repeated sequences will be an even number of letters.

5. Many reversals of digraphs.

Peculiarities

1. No plaintext letter can be represented in the cipher by itself.

2. Any given letter can be represented by 5 other letters.

3. Any given letter can represent 5 other letters.

4. Any given letter cannot represent a letter that it combines with diagonally.

5. It is twice as probable that the two letters of any pair are at the corners of a rectangle, than as in the same row or column.

6. When a cipher letter has once been identified as a substitute for a plaintext letter, their is a 20% chance that it represents the same plaintext letter in each other appearance.

The goal of recovery of the 5 X 5 square and various techniques for accomplishing this are the focus for solving the Playfair. Colonel Parker Hitt describes Lieutenant Frank Moorman's approach to solving the Playfair which addresses the keyword recovery logically. [HITT]. Other writers [ELCY], [BOW2], [FRE4], and [MAST] do an admirable job of discussing the process. However, W. M. Bowers Volume I on Digraphic Substitution presents the easiest protocol for students. [BOWE]

PLAYFAIR CRYPTANALYSIS

Our preliminary step is to perform individual letter frequency and digraphic counts. The former because high frequency ciphertext letters follow closely the high frequency letters they represent and will be located in the upper rows; similarly, low frequency letters follow their plain counterparts (UVWXYZ) and may be located at the last row of the square. A digraph count is useful because cipher digraphs follow closely the frequency of their plaintext digraphs. i.e. TH = HM. The frequency of HM must be high for a normal length message. Also tetragraphs may be tested THAT, TION, THIS for corresponding their frequencies in the square.

All the authors agree that a probable word is need for entry into the Playfair. Due to its inherent characteristics, Playfair cipher words will follow the same pattern as their plaintext equivalents; they carry their pattern into the cipher.

Given: Tip "er one day entere" Hampian. 10/1952

```
EU  SM  FV  DO  VC  PB  FC  GX  DZ  SQ  DY  BA  AQ  OB
ZD  AC  OC  ZD  ZC  UQ  HA  FK  MH  KC  WD  QC  MH  DZ
BF  NT  BP  OF  HA  SI  KE  QA  KA  NH  EC  WN  HT  CX
SU  HZ  CS  RF  QS  CX  DB  SF  SI  KE  FP  (106)
```

We set up a combined frequency tally with letters to the right and left of the reference letter shown:

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

This particular message has no significant repeats.

```
Cipher  GX  DZ  SQ  DY  BA  AQ  OB  ZD  AC
Plain   ..  ER  ON  ED  AY  EN  TE  RE  ..
```

Note the first and last pair reversal.

It is necessary to take each set of these pair equalities and establish the position of the four letters with respect to each other. They must conform to the above three rules for row, column, and rectangle.

The six different sets of pairs of know equalities are set up:

1	2	3	4	5
er = DZ	on = SQ	ed = DY	ay = BA	en = AQ
E D R Z	O S N Q	E D Y	Y A B	E A N Q
D	S	D	A	A
R E D	N O S	Y	B	N E A
Z Z R	Q Q N			Q Q N

6
te = OB
T O E B
O
E T O
B B E

The three possible relations of the letters are labeled Vertical (v), Horizontal (h), Diagonal (d). Our object is to combine the letters in each of the set of pairs.

Combine 1 and 3: E R D Z Y

1/v - 3/v	1/h - 3/h	1/d - 3/h
E	E D Y R Z	E D Y
D		Z R
Y		
R		
Z		

Combine 2 and 5: O N S Q E A

2/h - 5/d	2/d - 5/h	2/d - 5/d
O S N Q	E A N Q	S O
A E	S O	N Q
		A E

Note that all the equalities hold for all letters.

Set number 6 combines only with the last combination: T E O B N S Q A

```
 2/d - 5/d - 6/v                2/d - 5/d - 6/d
----------------                ---------------
         T                          S O T
       S O                          N Q
       A E                          A E B
         B
       N Q
```

which we now combine with 4:

```
                2/d - 5/d - 6/d - 4/h
                --------------------
                    S T O
                  Y A E B           (rearranged and
                    N   Q            equalities hold)
```

only one combination of 1 and 3 will combine with the above: S T O Y A B E D N Q Z R

```
              1/d - 2/d - 3/h - 4/h - 5/d - 6/d
              ---------------------------------
                     S T O
                   Y A E B D
                     N   Q
                         Z R
```

Arranged in a 5 X 5 square:

```
                    . . S T O
                    D Y A B E
                    . . . . .
                    . . N . Q
                    R . . . Z
```

We see that O is in the keyword, the sequence NPQ exists, the letters S T Y are in the keyword, and three of the letters U V W X are in needed to fill the bottom row.

```
                   ----------
                    . . S T O| C
                    D Y A B E|
                    . . . . .|
                    . . N P Q|
                    R . . . Z| U V W X
```

With the exception of F G H I K L M which must in order fill up the 3rd and 4th rows, the enciphering square is found as:

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

Our plaintext message starts off: YOUNG RECRUIT DRIVER ONE DAY ENTERED STORE ROOM ....

SERIATED PLAYFAIR

Perhaps the best known variation of the Playfair system, and one which adds greatly to its security, is called the Seriated Playfair.

The plain text is written horizontally in two line periodic groups as shown below in period six

```
C O M E Q U    E N E E D H    M E D I A T
I C K L Y W   (X)E L P I M    E L Y T O M
```

The vertical pairs are formed and enciphered by the regular Playfair rules. Based on the keyword LOGARITHM, the above message is enciphered:

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

we take the ciphertext off horizontally by the same route by which the plain text was written in for encipherment:

NLBCS PCDFG XZQQC DCMGC GQTBH CFTRH FGWHG B.

Solution of Seriated Playfair:

We assume a period of 4 - 10 which fits most of the cases encountered. Of prime importance is determination of the period. We test the various periods and eliminate any test where we find a vertical pair consisting of two appearances of the same letter.

If the message enciphered above is tested this way, in all periods from 4 - 10, it will be found that period 6 is correct. All others will show a doubled vertical pair.

Charles A. Leonard [PLAf] detailed a method to determine impossible periods mathematically:

$$\frac{S2}{S2 - S1} = Q \ \& \ R$$

where: S2 - S1 = Period, Q = quotient, R = remainder

Substituting known S values in this formula and solving for Q and R, a doubled vertical pair will occur in period S2 - S1 in the following cases:

1. When Q is an odd number and R is greater than zero;
2. When Q is an even number and R is zero.

Cipher letter position numbers in our message are:

```
A   B   C   D   E   F   G   H   I   K   L    etc.
    3   4   8       9  10  25           2
   24   7  16      27  19  30
   36  15          31  21  34
       17              32
       20              35
       26
```

```
Period  Letter  S2 - S1     Q   R   Result
  4       F     31 - 27     7   3   Eliminated-Case 1
  5       C     20 - 15     4   0   Case 2
  6       C     26 - 20     4   2   possible
  7       H     34 - 30             Eliminate-last gp
  8       D     16 - 8      2   0   Case 2
  9       C     26 - 17     2   8   possible
          G     19 - 10     2   1   possible
          H     34 - 25     3   7   Case 1
  10      C     17 - 7      1   7   Case 1
```

When a periodic group S2 - S1 does not occur in message the last group is inspected. If it is shorter than the regular groups of the period being tested, a double vertical pair may show at S2- S1 value equal to the length of this final group. If so, eliminate.

The mono and digraphic frequency counts are made. Plaintext high frequency digraphs and tetragraphs do not carry their identity over into the cipher and are not recognizable. Entry must be made with a probable word. Patterns do carry over to the two line groups and will repeat.

The placing of the probable word is important. Given a cipher text slice with period 6 found using the Leonard procedure:

```
   HKILVP   PBVBAA   BHRPOU   TBITFE   UCEVZK
   RNFTZU   HZWVFR   UDTKBD   UIBYNS   EXBZAR
```

and the probable phrase "is destined to", the word destined could be in any of the following positions when enciphered in period 6:

```
DESTIN  .DESTI   ..DEST   ...DES    ....DE
ED....  NED...   INED..   TINED.    STINED
```

The DE = ED reversal in all arrangements is noted and found in the cipher text portion:

```
            BHRPOU   TBITFE   UCEVZK
            UDTKBD   UIBYNS   EXBZAR
                     .desti
                     ned..
```

adding the additional information:

```
            BHRPOU   TBITFE   UCEVZK
            UDTKBD   UIBYNS   EXBZAR
                 .   sdesti
                 i   nedto.
```

we develop several equations:

```
                   ed = IB
 -I = UD, sn = TU, de = BI, ST = TY, to =FN, I- =ES
```

these translate to the following equalities:

```
   1          2          3          4          5
SN = TU    DE = BI    ST = TY    TO = FN    I- = ES
-------    -------    ------     -------    -------
S T N U    D B E I    S T Y      T F O N    I E - S
T          B          T          F          E
N   S T    E   D B    Y          O   T F    -   I E
U   U N    I   I E               N   N O    S   S -

   6          7
-I = UD    ED = IB
-------    -------
- U I D    E I D B
U          I
I   - U    D   E I
D   D I    B   B D
```

After some work (and with some assumptions to be tested we develop a tentative square for the system:

```
               1/d-2/d -3/h-4/v- 5/h -6/h
               -------------------------
                       -
                     O U N
                       I E
                       D B
                     F S T Y
```

check:

```
TO=FN+   + = yes
SN=TU+
ST=TY+                          letters left: A C E G H K
I-=ES -=t  IT =ES                             L M P Q R V
DE=BI+                                        W X Z
ED=IB+
-I=UD+
```

from here we need to expand on the cipher text or choose another probable word.

DELASTELLE SYSTEMS - FOURSQUARE CIPHER

The enigmatic Frenchman, Felix Delastelle created several nasty but very interesting cipher systems. We will discuss three of his systems. They are the Foursquare, Bifid, and Trifid. [DELA]

The Four Square employs four 25-letter alphabets set up in four 5 X 5 squares. The alphabets in the upper left and lower right squares are straight alphabets sans J.

Plaintext letters are found in these two alphabets when the message is enciphered. The opposite squares are used for ciphertext.

Encipherment follows only one rule. The plaintext letters are divided into pairs. The first letter is found in square 1, 2nd in square three. The two cells are thought of as opposite corners of diagonals of an imaginary rectangle. The first cipher letter is found in square 2 and the 2nd is found in square 4. The operation continues until all letters are enciphered.

For example, given:

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

Plain    CO ME QU IC KL YW EN EE DH EL PX
Cipher   LE WI XA FN EX CU DX UV DP GX HZ
```

Decipherment, when keywords are known is the reverse Using GEOM(E)TRY and LOGARITHM squares for the following cipher text:

```
Plain     XF WX PO DY DG GN AH
Cipher    SU PP LI ES AN DA MM
```

Identification of the Four Square

1. It is a substitution cipher.
2. It has an even number of letters.
3. Frequency count of 25 letters without J.
4. Doubled letters may occur eliminating a Playfair.
5. Long repeats occur at irregular intervals. Even sequences are most frequent.
6. Few reversals in comparison to Playfair.

Peculiarities of the Four Square

1. A plaintext can be represented by itself in the cipher.
2. Any ciphertext letter can be represented by five letters.
3. Any given plaintext letter can be represented by five ciphertext letters.
4. A cipher letter can represent itself or the other letter of the pair.
5. Every cell frequency is known or can be calculated because of the straight alphabets.
6. The fixed locations of the letters in squares 1 and 3 makes it possible to spot the location of probable words which form a pattern when enciphered by the Four Square.

Cell Frequencies

Bower and Meaker have derived the probabilities of the normal ciphertext based on the normal distributions for the straight alphabets in 1 and 3 based on 100 diagraphs. [BOWE]

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

The Four Square follows the normal distribution of letters:

```
                              High
Letter               E  T  A  O  N  I  R  S  H
Normal frequency    13  9  8  8  7  7  7  6  6

Normal 4-square freq.8  8  8  8  8  5  5  5  5  5
Square 2 cell       44 14 13 34 43 12 45 24 11 35
Square 4 cell       13 44 34 24 45 14 12 15 43 35

      Medium                        Low
 L  D  C  U  P  F    M  W  Y  B  G  V  K  Q  X  Z
 4  4  3  3  3  3    2  2  2  1  1  1  0  0  0  0
```

Square 2 cell = A
Square 4 cell = B

```
   4  4  4  4  4       2  2  2  2  2  1  1  1  1  1
A=31 33 32 23 15      25 41 21 42 54 22 55 53 51 52
B=31 41 23 33 11      22 32 42 21 25 54 51 55 53 52
```

The figures represent row X column frequencies.

Bowers presents an interesting Four Square problem known as the Stock Exchange Cipher. It supposedly is a message to a broker. The investor sold 'rails' and probable words such as Texas Eastern, Consolidated, and Columbia. The message deciphered represents the process fairly well:

```
UL RQ GW FO WQ CF PF FG EA GX LH DI OP MM LA LT
OF YQ CD HU GA LA FO EW EA VT YP QS UF WF RI CF
YQ QD LN QI WP YF OY MY AX FO WQ CF PF WF RC HQ
BT GW AQ SY QI WP GB BW HR WB EO EX GT LV PX OO
FO BQ HQ UM QS HE LT TM YM PN QI WP LB LO QO DP
SY BP QI YL LI MP DI OD NM UT ZH GT YM LQ HP HQ
QE IE XO MI.
```

Start with the frequency analysis:

```
 2nd letter                                    1st letter
 frequency                                     frequency

5             E L G L E .A. X Q                    2
3                 L W G .B. T W Q P                4
1                     R .C. F D F F                4
4               O O Q C .D. I P I                  3
3                 I Q H .E. A W A O X              5
10  W P C Y C W U O P C .F. O G O O O              5
1                     F .G. W X A W B T T          7
2                   Z L .H. U Q R Q E P Q          7
9     M D L Q Q Q Q R D .I. E                      1
0                       .K.                        0
2                   Y U .L. H A T A N V T B O I Q  11
6           Y N Y T U M .M. M Y P I                4
2                   P L .N. M                      1
8        X Q L F E F F F O. P F Y D D              5
9      H M B D W W W Y O P. F F X N                4
11H L H B A H W Y Y W R .Q. S D I I S I O I E      9
1                     H .R. Q I C                  3
2                   Q Q .S. Y Y                    2
7         G U L G B V L .T. M                      1
1                     H .U. L M F T                4
1                     L .V. T                      1
4               B G E G .W. Q F P Q F P B P        8
4               P E A G .X. O                      1
4               S S M O .Y. Q P Q F M L M          7
0                       .Z. H                      1
100                                                100

Long Sequences           Repeated Digraphs

FO WQ CF PE -2           FO-4   CF-3
QI WP       -3           QI-4   HQ-3
                                WP-3
```

Compare to normal square frequencies:

```
1st letter
    L Q W G H Y E F O B C M P U D R A S I N T V X Z K
Frequency square #2
    119 8 7 7 7 5 5 5 4 4 4 4 4 3 3 2 2 1 1 1 1 1 1 0
Normal
     88 8 8 8 5 5 5 5 5 4 4 4 4 4 2 2 2 2 2 1 1 1 1 1
Frequency square #4
    11109 9 8 7 6 5 4 4 4 4 3 3 2 2 2 2 1 1 1 1 1 0 0
2nd letter
    Q F I P O T M A D W X Y B E H L N S C G R U V K Z
```

Lets assume the word CONSOLIDATED.

```
     Plain     CO NS OL ID AT ED
     Cipher    LH DI OP MM LA LT
               *           *  *

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

LM and HI imply that the keywords have been written in vertically. Check against frequencies.

```
          Square #2             Square #4
Cell      14 24 31 43          15 24 33 34 41 43
Norm       8  5  4  8           5  8  4  8  4  5
Cipher     L  M  O  D           T  M  H  P  A  I
Freq.     11  4  5  3           7  6  2  9  5  9
```

The check works. Additional plaintext found:

```
           Cipher      Plaintext
            LI            ct
            MP            io
            MI            ht
            DP            on
```

Insert the new values into the cipher.

```
Cipher   QI WP LB LO QO DP SY BP QI YL LI MP DI OD NM
Plain                    ON             CT IO NS
```

This might imply 'directions' or 'instructions'.

Since O is in the keyword for cipher square 2, the letter after LM must be N P or Q.

>From our frequency chart:

```
       N P Q R S T U
       1 4 9 3 2 1 4
```

Tentatively, lets put P in cell 32 and Q in 34 giving us the new ciphertext pair QI =ST; the QIWP is repeated three times and might be the word STOP. We add to our partially filled in matrix.

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

So:

```
Cipher   QI WP LB LO QO DP SY BP QI YL LI MP DI OD NM
Plain    ST OP    DI TI ON       ST    CT IO NS
```

Cell 53 of square 4 is K. QO =ti, LO = di.

>From here it is not a far stretch to fill in the blanks:

```
Cipher   QI WP LB LO QO DP SY BP QI YL LI MP DI OD NM
Plain    ST OP    DI TI ON       ST    CT IO NS
              ad          al in    ru
```

Back to the Four Square to place additional values.

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

A righteous guess would be STOCK and BUY AND SELL for keywords. But we return to our analysis.

```
Cipher          FO WQ CF PF FG EA GX LH DI OP MM LA LT
Plain           th ou                co ns ol id at ed
'F' in 13               nd
'G' in 23                  sh
probable        th ou sa nd sh ar es co ns ol id at ed
```

Putting these in confirm our guess as to the keywords:

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

Keywords= STOCK EXCHANGE; BUY AND SELL

```
Cipher starts off: UL RQ GW
                   Bu yt en
```

Observations

1. Nulls are not required as in Playfair.
2. Probable position of letters can be spotted through cell frequency.
3. Probable words can be definitely placed if they produce a pattern.

There is no reason why all the squares can not be mixed for additional security. This destroys the frequency distribution attack; but digraphic and longer repeats will still show through to the ciphertext. The most reliable attack on the Four Square is via a probable word.

DELASTELLE SYSTEMS - BIFID CIPHER

Friedman, Bowers and Lewis discuss the intricacies of the Bifid cipher. [FRE4], [BOWE], [MAST] You will find many references to the Bifid cipher in the Cryptographic Resources Section, many of them developed from ACA materials. Dr. Linz (LEDGE) covers the BIFID in some detail. [LEDG]

The Bifid and Trifid ciphers represent a new and tougher breed of classical cipher - Fractionated Ciphers. The process of fractionation, whereby the substitute unit is 1/2 or 1/3 or 1/part for each letter represents a more involved problem for analysis that some of the ciphers presented to date. What we do is combine substitution and transposition processes to produce a clever mixed cipher. Modern ciphers do the same thing many times over (called rounds or S-Boxes in DES).

Method of Encipherment By Bifid

The secretive Delastelle designed the Bifid to use a checkerboard square with 25 letters, sans J. We start with a keyworded square:

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

Key = MANY OTHERS

The encipherment process is periodic and the number of letters in each group is usually an odd number. Even Bifids are actually easier to solve than odd. We will focus on the odd Bifid to illustrate the process. Period lengths of 7, 9, 11, or 13 are those most frequently employed.

Encipherment is a combination of substitution and transposition which is best shown by example. We will encipher the message COME QUICKLY WE NEED HELP in period 7.

Step 1: Period Length.

First divide the plaintext message into groups of 7 letters. Write the numerical equivalents for row and column vertically under the plaintext letters.

```
     C O M E Q U I   C K L Y W E N   E E D H E L P
Row  3 1 1 2 4 5 2   3 4 4 1 5 2 1   2 2 3 2 2 4 4
Col  2 5 1 3 5 1 1   2 2 3 4 3 3 3   3 3 3 2 3 3 4
```

Step 2: Horizontal Transposition and Take Off

The next step is a form of transposition, wherein the numerical substitutes are taken off horizontally by pairs. In each individual group this take-off continues, without interruption, through the two rows of numbers. The last number of the top row pairs with the first number of the bottom row. The first number of each horizontal pair indicates the row of a cipher letter and the second number of the pair indicates the column of that cipher letter.

Step 3:

Find the cipher letters in the square using the new row X column coordinates.

```
Plain         C O M E Q U I
  Row         3 1 1 2 4 5 4
  Col         2 5 1 3 5 1 1
Cipher        B A Q K U G M
```

31 = B; 12 = A; 45 = Q; 42 = K; 51= U; 35 = G; 11 =M

The process might be more clear if we look at the encipherment this way:

```
     Row              Column
C O M E Q U I    C O M E Q U I
3 1 1 2 4 5 4    2 5 1 3 5 1 1
 B   A   Q    K    U   G   M
```

We see that cipher 'B"' has the same row 3 as 'C' row and 'B' column (1) has the same number as O row (1). This reasoning holds for the second and third cipher letters 'A' and 'Q'. The fourth cipher letter 'K' has the same row (40 as plain 'I' and the same column number (2) as plain 'C', which are the last and first letters of the group. The fifth, sixth and seventh cipher letters are derived the same way, except that we deal with columns. The fifth cipher letter 'U', is the result of 'U' row (5) and 'M' column (1).

Each cipher letter results from the some combination of half values of the two plaintext letters. Due to this characteristic, the Bifid (and Trifid with thirds) is classified as Fractional Substitution.

Deciphering the Bifid with Known Elements:

Step 1: Fractionate the cipher letters into their row and column components.

Step 2: Write into two rows horizontally of periodic length.

Step 3: Write the numerical values into the two horizontal rows below the fractionated letters.

Step 4: Recover Plain text letters vertically.

```
Cipher Fractionated   Br Bc Ar Ac Qr Qc Kr
                      Kc Ur Uc Gr Gc Mr Mc
                      --------------------
Plaintext Row         3  1  1  2  4  5  4
Plaintext Column      2  5  1  3  5  1  1
Plaintext             C  O  M  E  Q  U  I
```

Identification of the Bifid

1. It is a substitution cipher with substitution units = to 1/2 of the cipher letter, represented by row or column index.

2. Frequency count of 25 letters (J omitted) but not more for 5 X 5 Bifid. MASTERTON describes a 6 X 6 Bifid with letters and symbols included. [LEWI]

3. Long repeats occur at irregular intervals.

4. Repeated patterns dependent upon the length of the repeated sequence and the period, ex.:

```
AB .. D          A .. CD
AB .. DE         AB . CD
```

5. A frequency count will show a flat profile compared to normal plaintext.

Peculiarities of the Bifid

1. When the cipher letters are set up in the correct period a few 'naturals' will occur. A natural is the term for a vertical cipher pair, arranged row-column order, in which both components are the same letter. When this happens the plaintext letter is revealed. This is not true when the cipher letters are column-row unless the letter happens to be one of the five on the diagonal of the square running from 1-1 to 5-5.

For:

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

```
Cipher   Hr hc Ar Ac Hr
         Hc Cr Cc Ar Ac
         --------------
Plain    H  E  A  T  H
         *
```

The first plaintext letter H is a natural but the T on the fourth is not. The great majority of naturals will be high frequency plaintext letters. If low frequency plaintext letters appear as naturals, it is almost a certainty that the cipher message is set up in an incorrect period.

2. Half-naturals occur quite frequently, when the cipher is set up in the correct period. One of the letters of the vertical pair, in row-column order, is the same as the plaintext letter it represents.

```
Cipher   Tr Tc Qr Qc Sr
         Sc Wr Wc Er Ec
         --------------
Plain    S  O   L  V  E
         *           *
```

The probability that one of the letters in row-column pair is a half-natural is 8 in 25, or 32% The probability of a half-natural in column-row order (along the diagonal) is 1/5 of 32% or 6.4% Half naturals are a function of the expected appearances of the plain text letter. For instance, in a cipher of 100 letters, we find 10 'E's and 10 'Z's.

```
Cipher Letter E = 10 X 0.32 = 3.2 half-naturals
Cipher Letter Z = 10 X 0.32 = 3.2 half-naturals
```

but the E is 13 times more likely than the Z. So the E is expected to appear 13 times in 100 letters so the 3-4 half-naturals is possible but the Z will occur only 1 time in 100, so we may expect no half-naturals.

3. Half-naturals are the Bifid's most vulnerable feature because it plays a large part in spotting probable words.

4. The Bifid, fractionated for decipherment, engenders two separate and different alphabets. One applies to odd numbered vertical pairs, found in the basic square and the other applies to even vertical pairs in each periodic group.

5. Repeated plaintext sequences produce patterns as long as the repeat starts in the same relative location in the group as of its first appearance.

```
          Odd                    Even
         1   3   5   7            2   4   6
Plain    H O M E I S A          A H O M E I S
         2 1 1 2 4 2 1          1 2 1 1 2 4 2
         2 5 1 3 1 5 2          2 2 5 1 3 1 5
         -------------          -------------
Cipher   T A K A U B V          A M R H S N O
```

```
           Odd                      Even
         1   3   5   7            2   4   6
Plain    G O H O M E N          T H E H O M E
         3 1 2 1 1 2 1          2 2 2 2 1 1 2
         5 5 2 5 1 3 4          1 2 3 2 5 1 3
         -------------          -------------
Cipher   B T A O V U F          H H M A E S N
```

The spacing for repeated cipher letters varies for different periods. For four letter repeats it is:

```
            Odd                    Even
Period 5   T A . U                M . S N
       7   T A . . U              M . . S N
       9   T A . . . U            M . . . S N
      11   T A . . . . U          M . . . . S N
```

Repeats of the other lengths generate their own individual patterns. For period 7 these are:

```
                     Odd              Even
3 letter repeats   A . . . D        U . . X
4                  A B . . D        U . . X Y
5                  A B . . D E      U V . X Y
6                  A B C . D E      U V . X Y Z
```

The search for repeated patterns is the first step to finding the correct period for solution of the Bifid. Patterns are formed by plaintext components which serve to make up complete cipher pairs. It does not make any difference what letters may be in other places of the group, the same patterns will always show for the word in question, whenever it is enciphered in the same period. For example, for period 9:

```
           Odd                      Even
         1   3   5   7   9        2   4   6   8
Plain    . . b i f i d . .      . b i f i d . . .
         . . 3 4 3 4 3 . .      . 3 4 3 4 3 . . .
         . . 1 1 4 1 3 . .      . 1 1 4 1 3 . . .
         ----------------       ----------------
Cipher   . F F . . . Y N .      . L L . . M I . .
```

THE THREE SQUARE TECHNIQUE

There are two basic ways to cryptanalyze the Bifid. One involves placing of a probable word after determination of the correct period and manipulating the rows and columns of the Bifid decipherment square until it is fully recovered or the keyword is found. Friedman discusses this method in detail. [FRE4] Bowers also covers this approach but introduces the reader to a more comfortable method for solution using the square itself as a indicator of the letter indexes. Developed by William A Lee (TONTO) in June, 1945, it uses three squares to eliminate the requirement for numerical indices.

The setup is as follows:

```
                        . . . . . . . .
                        . E S C L V .     Top Square
                        . N I D O W .     Row used as
                        . T A F P X .     Column
                        . H M G Q Y .     Indicators
                        . U B K R Z .
              . . . . . . . . . . . . .
              . E S C L V . E N T H U .
Left Square   . N I D O W . S I A M B .     Basic Square
Column used   . T A F P X . C D F G K .      Normal
as row        . H M G Q Y . L O P Q R .     row and column
indicator     . U B K R Z . V W X Y Z .
              . . . . . . . . . . . . .
```

Rules for encipherment and decipherment under three square approach

We are always starting with fractions of two letters and searching for the single letter that it represents by these half values.

For encipherment, pairs will be fractionated like this:

SrXr SrXc ScXc

For decipherment, the fractionated pairs will be:

SrXc ScXr

1. When one or both of the fractions is in the true position in a pair, it/they are found in the Basic Square.

   SrXc - both in basic
   SrXr S in basic
   ScXc X in basic

2. When one of the fractional letters of the pair indicates that its row designates a column of the letter it is to represent, then it will be found in the top square.

   SrXr - X in top square
   ScXr X in top square

3. When one of the fractional letters of the pair indicates that its column designates the row of the letter it is to represent, then it is found in the left square.

   ScXc - S in left square
   ScXr S in left square

Using the word SOLVE we visualize:

```
Sr Or Lr Vr Er
Sc Oc Lc Vc Ec

---   ----   -
S  O  L  V   E
-  ---   ----
```

SrOr - S row (basic); Orow as col (top),= M (basic)
LrVr -L row (basic); Vrow as col(top), = R "
ErSc -E row (basic); Scol (basic) = E "
OcLc- O col as row(left); L col (basic) = S "
VcEc - Vcol as row(left);E col(basic) = E "

The same rules apply in reverse when the vertical pairs are fractionated and the plain text equivalents are found at the intersections.

CHI-SQUARE

Karl Pearson's Chi-Square test, which we described previously, was adapted by D. Morgan in 1946 to determine the period of a Bifid. Excluding middle letters, letters fall into one of two families, the row and column. Chi-Square tests the dissimilarity of probable groups of different lengths. The periodic length for which the difference is the greatest represents the correct period. We calculate D**2/S, where S equals the sum of the appearances in both row and column families of any letter. D equals the difference between the family appearances of any letter.

When D**2/S is calculated for every letter, these values are summed and their sum is the Chi-Square value for period under consideration. If we were to find the following:

Period	Chi-Square
5	19.2
7	19.4
9	28.0
11	12.0

Our choice would be period 9. Morgan's article in the JJ 1946 Cryptogram details the procedure. [BIF3]

Lets try to solve an Odd period Bifid.

Given: The Master Spy Cipher - Concerning espionage, and the man who was Hitler's Chief of Intelligence during WWII.

```
FRIEN  ILOSV  FDYAE  MWDAH  IALTN  IBLVY  EQATP  TNTTI
XLPNP  HIVIR  TDZKK  LVNDE  ASBTI  CWDNH  YLZZK  LOEPE
ARFSI  VHILT  ZRKRS  ENTWE  ONXEN  CITOI  VRPMP  ENLEY
FQTLK  HZHIN  IPKHT  TLBDT  TPBOZ  OTKTD  SBTLF  TLRIW
YIHKV  DZPXT  FIIZ.
```

Inspection of this message reveals a repeat in the form of A B . . . C D. This 5 letter repeat at the odd position is in period 9. The fractionated cipher letters would be located as shown, depending on the starting position.

```
 1st position       3rd position       5th position
K K L L . . . . .  . . K K L L . . .  . . . . K K L L .
. E E A A . . . .  . . . E E A A . .  . . . . . E E A A
x x x x x             x x x x x             x x x x x
```

The first appearance of the repeat starts at letter 55 and the second at the letter 75.

55 / 9 = 6 plus 1
75 / 9 = 8 plus 3

Hence in period 9, the first repeat starts in group 7, position 1 and the second in group 9, position 5.

We accept the period and rewrite the ciphertext. Using the skip hit form of the three square, eliminate the even vertical pairs, recognizing that they are column - row pairs and that they may be visualized as a diagonal from the top letter to next bottom letter in the two rows.

```
F  R  I  E  N | V  F  D  Y  A | A  H  I  A  L |
N  I  L  O  S | A  E  M  W  D | L  T  N  I  B |


L  V  Y  E  Q | N  T  T  I  X | H  I  V  I  R |
Q  A  T  P  T | X  L  P  N  P | R  T  D  Z  K |


K  L  V  N  D | T  I  C  W  D | Z  Z  K  L  O |
D  E  A  S  B | D  N  H  Y  L | O  E  P  E  A |


R  F  S  I  V | Z  R  K  R  S | E  O  N  X  E |
V  H  I  L  T | S  E  N  T  W | E  N  C  I  T |


O  I  V  R  P | L  E  Y  F  Q | Z  H  I  N  I |
P  M  P  E  N | Q  T  L  K  H | I  P  K  H  T |


T  L  B  D  T | Z  O  T  K  T | L  F  T  L  R |
T  T  P  B  O | T  D  S  B  T | R  I  W  Y  I |


H  K  V  D  Z | I  I
Z  P  X  T  F | I  Z .
```

We have four naturals present: E-T-T-I. We know from the pattern repeat that:

```
K   L   Vr    and    K   L   Or
Dc  E   A            Pc  E   A
----------           ---------
```

represent the same five plaintext letters, so D and P are co-column and V and O are co-row. we start the recovery of the basic square.

```
D . . . .
P . . . .
. V O . .
. . . . .
. . . . .
```

we test the probable word ESPIONAGE.

```
Locations  E S P I O N A G E
   1-4              x x   x
   2-3     x          x
   5-7         x x
   6-4           x         x
   9-3     x   x       x       ***
  10-4       x   x
  10-9       x       x
  12-1     x               x
  12-9     x     x
```

```
        Z   K   L   O  | R   F
        E   P   E   A  | V   H
        --------------------
        E S P I O N A    G E
        *   *       *
```

3 half-naturals!

5 letter repeat: P I O N A and 3 half-naturals. Wow. Good hit.

Compare to location 6-8 (group and position):

```
        I   R | K   L   V   N
        Z   K | D   E   A   S
        ------------------
          E S   P I O N A G E
```

Combine both into one three square diagram:

```
                . - - - - - .
                . H - - L - .
                . P E R O - .
                . I Z S V - .
                . K N G A - .  - - - D -
. . . . . . . . . . . . . . .
. - - R L I . E - Z N - .
. - - - - N . O L V - - .  A - - - -
. - - V Z G . S R G - - .
. - E S O K . K I - - - .  - P H - -
. - - - - - . - - - - - .
  - - - - -               - D - - -
  - - - P D
  - - - - H
  - - - - A
```

When filling in the squares, we start with the even numbered pairs to fill in the left and top squares quickly. We then write in the known odd pairs. we write the odd pairs into unallocated rows and columns and then consolidate them.

Plaintext can be recovered which leads to new ciphertext square letters being recovered. The phrase FOR NINE YEARS at Groups 1 and 2; The Name HITLER in groups 17 and 18; the phrase FOR HITLERS THIRD REICH in groups 10-11-12.

Placed in our squares:

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

The entire message can be read. The letters which fall on the diagonal are known because they are repeated in the left square in the same long row and in the top square in the same long column. These letters can be shifted along the diagonal, but cannot be moved away from it. Doing so we have the enciphering square and the true transposition that generated it.

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

from:

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

The complete message reads:

```
F  R  I  E  N|V  F  D  Y  A|A  H  I  A  L
N  I  L  O  S|A  E  M  W  D|L  T  N  I  B
-----------------------------------------------
f o r n i n e y e a r s a d m i r a l w i l h i l m c

L  V  Y  E  Q|N  T  T  I  X|H  I  V  I  R
Q  A  T  P  T|X  L  P  N  P|R  T  D  Z  K
-----------------------------------------------
a n a r i s d i r e c t e d t h e m i l i t a r y e s

K  L  V  N  D|T  I  C  W  D|Z  Z  K  L  O
D  E  A  S  B|D  N  H  Y  L|O  E  P  E  A
-----------------------------------------------
p i o n a g e a n d t h e c o u n t e r e s p i o n a

R  F  S  I  V|Z  R  K  R  S|E  O  N  X  E
V  H  I  L  T|S  E  N  T  W|E  N  C  I  T
-----------------------------------------------
g e f o r h i t l e r s t h i r d r e i c h n o w i t

O  I  V  R  P|L  E  Y  F  Q|Z  H  I  N  I
P  M  P  E  N|Q  T  L  K  H|I  P  K  H  T
-----------------------------------------------
a p p e a r s t h a t t h e s s o f t g p o k e n l i

T  L  B  D  T|Z  O  T  K  T|L  F  T  L  R
T  T  P  B  O|T  D  S  B  T|R  I  W  Y  I
-----------------------------------------------
t t l e m a n b e t r a y e d h i t l e r a t e v e r

H  K  V  D  Z|I  I
Z  P  X  T  F|I  Z
----------------------
y o p p o r t u n i t y
```

The Even period Bifid is covered in copious detail in Bowers. [BOWE]

DELASTELLE SYSTEMS - TRIFID CIPHER

Both Bowers and Linz covers the Trifid in detail. [BOW2] [LEDG] Bowers covers the Trifid in detail. Topics include Keyword Block recovery, periodic group structure, Trifid patterns, pattern uncertainty, tetragraphic patterns and part naturals.

We know that P = n**r represents the permutations with repetitions, n = number of different things, r = number of things used at a time. The normal Bifid square shown below, thought of as a 5 X 5 block with external coordinates.

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

But 5 x 5 block is also 5 x 5 = n**2, the right hand portion of the formula. Look at it a new way:

```
    r=2
-----------------------------------------------------
Row     1         2         3         4         5
Col 1 2 3 4 5 1 2 3 4 5 1 2 3 4 5 1 2 3 4 5 1 2 3 4 5
    B I F D A L P H E T C G K M N O Q R S U V W X Y Z
-----------------------------------------------------
                    P = 25
```

In the case of the Trifid, the block takes the same form with an additional dimension.

```
    r=3
-----------------------------------------------------------
1         1                 2                 3
2   1     2     3     1     2     3     1     2     3
3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3
  T R I F D A L P H B E C G J K M N O Q S U V W X Y Z #
-----------------------------------------------------------
                    P = 27
```

I like to work with compact matrices so here is another way to show the structure in three directions:

```
                    2nd Comp

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

                     3rd Comp
```

For the purpose of this lecture, the Trifid setup will be shown as a 27 X 3 block containing all possible changes in order of the three numbers 1-2-3, taken three at a time and arranged in ascending order. The numbers within the block, when read vertically, serve as components of the letters of the alphabet which is added, externally, to the block. So:

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

The fact that 27 letters are required for the Trifid is a weak feature of the system. we can use a ZA and ZB to represent the 27 letter and the true Z respectively. A scrambled alphabet is always used to prevent some letters being represented all the time by the same combination. Based on keyword COUNTERSPY:

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

The letters are taken off vertically in order of columns. We set up two tables:

```
                    Deciphering Table

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

                    Enciphering Table

 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 1 1 1 2 2 2 2 3 3 3 3 1 2 1 3 1 3 3 2 1 1 2 2 3 2 3|
|1 2 1 3 3 1 2 3 1 2 3 3 1 1 2 2 2 1 2 2 3 3 1 2 3 3 1|
|2 2 1 2 1 2 2 2 2 2 1 3 3 1 1 3 3 1 1 1 1 3 3 3 2 3 3|
 -----------------------------------------------------
```

Method of Encipherment

Encipherment follows the same general pattern as the Bifid. the plaintext is divided into groups of a chosen periodic length and the numerical components are written vertically below each letter. Periods of multiples of 3+1 are popular such 7 -10- 13 , with 10 being the most popular. For example, with period = 10:

```
Plain     C O M E Q U I C K L|Y I N E E D H E L P
          -------------------|-------------------
          1 1 1.2 1 1.3 1 3.3|3 3 2.2 2 1.2 2 3.3
          1 2.1 3 2.3 1 1.3 3|3 1.1 3 3.3 3 3.3 2
          1.1 3 1.3 1 2.1 1 3|2.2 1 1.1 2 2.1 3 3
          -----------------------------------
Cipher    C N # I D R K U I M|Y T X K V L J N B V
```

The first letter C is represented by vertical 111; plain O by 121; M by 113; etc.

The first cipher letter C is derived by the horizontal take off 111. The dot represents the break between trigraphic units. Note that the C is derived from the 1st three components from COM. The fourth cipher letter I derives from the first component of the tenth letter L and the 2nd 2 components of CO. We go to the end of the row and back to the first letter on the second row, to the end and drop down to the third row first letter.

Decipherment

The decipherment process reverses that of encipherment, in that the numerical components of the cipher letters are written horizontally in three rows of periodic length and are then read vertically to produce the plaintext.

Identification of the Trifid

1. It is a substitution (fractionated) cipher with 27 letters.

2. If long repeats occur, they will be at irregular intervals.

3. Repeated patterns will occur:

```
   for period 10:

       6 letters    A D . . C . . B . .
       5 letters    A . . . C . . B . .
       4 letters    A . . . . . . B . .
```

Peculiarities of the Trifid

1. Naturals, similar to those of the Bifid, are extremely rare.

2. Each plaintext letter can be represented by 729 (**3) different arrangements of fractions of itself and other letters.

3. The table of numerical components is inflexible. Any given digit - 1 - 2 -3 must appear 1st, 2nd, and 3rd component for nine letters - no more, no less.

4. Not more than three letters can have the same two components identical; and for these three letters the other component must be a different figure in each case. This is a good rule for cryptanalysis.

5. Repeated plaintext sequences produce patterns that are recognizable. Bower devotes a substantial chapter to this rule. [BOWE] The surest way to determine the period is through repeat patterns.

6. Repeated cipher patterns do not always represent the same plaintext letters. The period is key.

SOLUTION OF A TRIFID WHEN PLAINTEXT WORDS ARE GIVEN

Solution of a Trifid cipher requires that the individual trio of numerical components having the correct arrangement of the components must be determined for each letter of the alphabet. Sacco advises that a probable word is essential. [SACC]

Given: Trifid, "The first" starts message and repeats at RQOTUILR.

```
HRNGQ  SSXDI  TSIZB  BZBZB  TUPRE  IMQYS
BJPKV  RQOTU  ILRSI  MKZBI  RUXPS  OGWQQ
FMKIC  ISXOY  BSFVP  HGHLZ  AOQEU  CRMNJ
BZBVO  LCUJB  AZBGL  FVUDH  AMYHK  VMRGZ
BRTID  XUJQN  IZBIL  CUFSF  FHDJZ  BHSCM
KECEF  QOMKY  PNSSV  GHFSB  BBOUJ  SQAXX
DWJMU  ZBBTX  HHRHV  ZAZBB  PTEGY  NHZBI
BRWNO  VODZA  TAJVL  KKIVZ  A.
```

The triple repetition of ZB, in groups of three and four. So set ZB = # and ZA = Z. We place the tip and repeat.

```
HRNGQ  SSXDI  TSI#  B##  TUPRE  IMQYS  BJPKV
thefi  rst

KVRQO  TUILR  SIMK#  IRUXP  SOGWQ
  the  first
```

We see a 6 letter repeat in period 10:

```
Letter 12:  S I # B # # T U P
Letter 41:  S I M K # I R U X
            * *     *     *
```

We accept the period as 10 and set up the message as such.

An accepted method of setting-up a Trifid for solution is to write the cipher message on quadrille paper leaving a minimum of five blank rows between the lines of letters. These are written horizontally in continuous order, limiting the number of letters in each row to a multiple of the periodic length.

```
HRNGQSSXDI    TSI#B##TUP    REIMQYSBJP
----------    ----------    ----------
----------    ----------    ----------
----------    ----------    ----------
thefirst
----------    ----------    ----------
KVRQOTUILR    SIMK#IRUXP    SOGWQQFMKI
----------    ----------    ----------
----------    ----------    ----------
----------    ----------    ----------
  thefirst
----------    ----------    ----------
```

We now fractionate the letters that we know to be present and then set-up chains of equivalents. Like Bifid, having two separate alphabets to contend with, the Trifid has three separate alphabets to recovery piece by piece. We must tabulate our known values.

The fractionated plaintext letters are to be vertically aligned and the fractionated cipher letters must be in horizontal alignment.

```
T1 H1 E1 F1 I1 R1 S1 T1 .  .
T2 H2 E2 F2 I2 R2 S2 T2 .  .
T3 H3 E3 F3 I3 R3 S3 T3 .  .

H1 H2 H3 R1 R2 R3 N1 N2 .  .
G2 G3 Q1 Q2 Q3 S1 S2 S3 .  .
S3 X1 X2 X3 D1 D2 D3 I1 .  .


.  .  K3 V1 V2 V3 R1 R2 R3 Q1
.  .  O1 O2 O3 T1 T2 T3 U1 U2
.  .  I2 I3 L1 L2 L3 R1 R2 R3
```

Set Chain of Equivalents

(a) T1 H1 K3 N2 Q1 Q2 F2 E2 O3 H2 V1 G3 O2

(b) T2 G2 O1 S3 U2 Q3 I2 T3 I1 R3 R2 R1 D2 S1 D3 N1 F1 V3

(c) H3 X1 I3 E1 V2 D1 L3

(d) E3 X2 L1

(e) F3 X3 L2

(f) S2 U1

All the above fractions are equivalent to each other. There are six separate sets of equivalents, which means three are duplicates and equal to each other. Set (a) and (b) are not equal. The latter contains R1 R2 R3 and Q3 ; while (a) contains Q2 Q3. If both sets were equal to each other they would violate the rule governing the same identical numerical components, an impossible condition. We can give both sets numerical values of 1 and 2 arbitrarily, then check the assignment as we fill in the holes.

Enciphering Table

```
 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 #
-----------------------------------------------------
          2   1 2         2 2   1 2 2 1   1
      2 1 1 2 1 2         1 1   1 2   2 2
      2     1       1       1   2 2 2 2   2
-----------------------------------------------------
```

Having established a few values, set (c) cannot have the value 1 because rule 4 for E1 and V1. Also it cannot have the value 2 because of a conflict with the letter D =222 which is already in use by T.

We set (c) with a value of 3 and add the fractions to our table.

Enciphering Table

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	#
3	3	2		1	2					2	2		1	2	2	1	3	1		3						
2	1	1	2	1	2					1	1		1	2	3	2	2	3								
2			1	3	3		1	3			1		2	2	2	2		2								

Further determinations are possible:

O = 211 , F is 212 or 213
N is 212 or 213

Rule 4 prevents S2 to be 1 since FNO are 21.

S2 cannot be 2 because it conflicts with R ; S2 =3.

So the (f) takes on the value 3 and U1 = 3; F3 = 2 or 3; D = 322 implies that U3 = 1 or 3. We set a decipher table with known and derived values. Letters are added externally.

Deciphering Table

Q	H		T		V		O			R	I		S				D							
1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3
1	1	1	2	2	2	3	3	3	1	1	1	2	2	2	3	3	3	1	1	1	2	2	2	3	3	3
1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
?			G					F	F	G					E	E	E	G								
								N	N											U		U				

We substitute know values in the message and recover more plain text.

Group 12 and 13 gives us the word RIVERS, which yields some new values.

L = 123
F = 212
N = 213
E = 311
U = 323
X = 3?2

Additional values are added to both tables.

Deciphering Table

Q	H		T	L		V		O	F	N		R	I		S		E			D	U			
1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3
1	1	1	2	2	2	3	3	3	1	1	1	2	2	2	3	3	3	1	1	1	2	2	2	3	3	3
1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
?			G						G						X		G				X			

Enciphering Table

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	#
			3	3	2			1	2			1		2	2		1	2	2	1	3	1		3			
			2	1	1	2	1	2				2		1	1		1	2	3	2	2	3					
			2	1	2	1	3	3		1	3			3	1		2	2	2	2	3	2		2			

We next look for the trigram THE. We hit a possible bonanza with groups 6,7, 9,11, 14, 17, 19, 21:

We are looking for the 1 1 3 components.

2	1	1
2	3	1
-	-	-
t	h	e

Group 7 tends to be the clincher with the words THE DIFFERENCE. We accept new values of B=131, C=332, P= 3??, Y=121 and W=1??. The word BETWEEN is logical for group 8. When placed we find G=321, P=313, W=133, Z=111. Only a few letter components are unknown and they fall when the known values are placed in the quadrille.

Deciphering Table

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

Enciphering Table

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	#
3	1	3	3	3	2	3	1	2	2	2	1	3	2	2	3	1	2	2	1	3	1	1	3	1	1	2
3	3	3	2	1	1	2	1	2	3	3	2	3	1	1	1	1	2	3	2	2	3	3	1	2	1	2
3	1	2	2	1	2	1	3	3	3	1	3	1	3	1	3	2	2	2	2	3	2	3	2	1	1	1

The first part of our message in detail reads:

HRNGQSSXDI	TSI#B##TUP	REIMQYSBJP
1132222133	1222322232	2223112233
2111223223	2113122122	3111212123
2312322223	1122323313	2131233313
thefirstda	yofspringi	sonethinga

The full message reads:

The first day of spring is one thing and the first spring day is another. The difference between them is sometimes as great as a month period. It is with rivers as it is with people, the greatest are not always the most agreeable nor the best to live with. Henry Van Dyke.

Keyword Recovery

A little inspection of the letters reveals that the take off method is reverse and decimates as follows:

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

we see:

```
   V -- W -- X -- Z

       -DV -FW - GX -HZ - I#

        F    G           B C       H I
        O    P    and    L M  and  Q R
        W    X           T U       Z #
```

which yields:

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

and finally;

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

So we have just a small glimpse at the Trifid. Read Linz and Bowers for a significantly better picture of this cipher. There are whole issues surrounding period, part-naturals, patterns and tetragraphic equivalents. [LEDG], [BOWE]. The Resources section has many ACA articles regarding the Trifid. Lastly, the reprints of three of Delastelle's books are the most interesting (in French) pertaining to the Trifid. Delastelle did not consider the 27th letter an issue. (Maybe in French it was not.) [DELA], [DEL1], [DEL2]

LECTURE 16 ANSWERS

1. Complete columnar transposition.

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

   ANS: ENGRAVE; A MAN WHO THINKS HE'S REALLY FLYING
   HIGH IS IN DANGER OF MELTING OFF HIS WINGS.

2. Nihilist transposition.

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

   ANS: 16384257; UNUSUAL PUNISHMENT ..

3. Incomplete columnar

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

   ANS: 64287153; SHALL I CONTINUE WITH ..

4. Myszkowski. Battlefield.

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

   ANS: APPETITE ; ....

5. Amsco.

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

   ANS: 4162375; MOST VIOLENT ANTISEMITE..

6. Tramp.

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

   ANS: CAN YOU PLACE EIGHT QUEENS .

7. Cadenus.

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

   ANS: ANDES; IN FLIGHT THE CONDOR

8. Railfence.

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

   ANS: TELEVISED FOOTBALL GAMES ..

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

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

   ANS: 6 - RAILS; THERE ARE NO ATMOSPHERIC

10. Turning grille.

    TIP = the most serious and; NQEJPGUU

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

    ANS: THE LEGEND OF LOCH NESS HAS

11. Swagman. Agreeable toil.

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

    ANS: WORK IS NOT IRKSOME WHEN I ..

LECTURE 17 PROBLEMS

17-1 Headline Puzzle

Paul Derthick's HEADLINE PUZZLE . by Larry Gray

The following are all headlines from a recent daily newspaper. Each of the five is a different mono -alphabetic substitution, and all five are derived from the same mixed alphabet at different settings against itself.

1. PXYWFXKLJE DFYMJYV VGHKJ `DFYM-US' GF ZYFGJVG PJEJYHW VLXGEFDS;

2. JUBHFGO EUHKEOF HR WEUDBGO, FHSJF DKD RO ZGI YRE FUNROI HUED;

3. NEZZY AEZYVKU AEVP NFUVLKY LR ALVVKU JLBPV ECKU AWGBKV;

4. ZEHCGOL LZCCOMMSS WEMSAQ MZALD AFB AZFMS MZ DZBZA MDZAGS;

5. PTQQU WQRKWCQBSD WQEKLLQUBX BZOKWEQ MKW ENJWSQX JUB BZ

In case you'd like to confirm your solution of this example, but not be influenced by seeing the answers beforehand, the setting, key and hat are provided here in a Caesar cipher, offset by 6.

Setting = GTURK Key = MKIQU Hat = INGSKRKUT

17-2 Playfair. While Rome Burns. BARRISTER: ON44:CE17
Tip= "ers are"

OCMAF ZDAPZ BYPGY BOKYT BYVMT AVIBY PVGPP RBCFH
XEAPI VTCPV VBKGV MEWCB IEGMQ PPBOL ENRHZ MRFSC
DRNAI ZEITN SUNA.

TWO HINTS: The title is significant and does not follow LANAKI's Red Herring rule and look for naturals such as PO = QP or OPQ. A Natural is a cipher digraph not in the keyword whose letters because of the standard alphabetical relationships stay in the natural alphabetical order in the cipher square.

17-3 Foursquare 'anasonly' ZEMBIE

UB XB MS SF SQ MS TH DE UB HM GL NL BW GB LW NQ NF UB FM
QH EM BW BI GT LD UQ IG WM CF TQ ET CT NF IP LS UQ FK UH
IZ UQ YF TN XP NS FF UV HV NF HI CE NQ UO UQ GK ET HT ND
PV BI BE ND BD YM DE LX UB GA CX ET XT DE PE NL BF PY IQ
NG QW IS NC CK XB TF GK ED LA EL LE RW MI EX SF MS UP XQ
NF EV FF BI KK NA MX.

17-4 Short Bifid. Clue - DIAMONDS is there somewhere and
the text talks about them being HIDDEN. Period = 7.

ETIALIG LDMNITV NFEMISI EEIDGEI
HPCEDUT PINOFLW INDLEEK

SPECIAL NOTE RE: DIOPHANTINE EQUATIONS

For some time now, Dr. Michael Anshel of CCNY and I have been following the development of crypto from some early roots. Here are short excerpts from our correspondence. Jump in if you can help us:

==========

>From Michael to LANAKI:

Let me thank you for your very detailed answer. John Wallis was involved in solving certain diophantine problems particularly the Fermat-Pell equation, which in turn led to the study on continued fractions, and ultimately to the study of automatic sequences which are of interest to contemporary cryptographers. Were these very gifted 17th century cryptographers aware of this possibility? - Michael Anshel.

==========

To Michael from LANAKI:

In RE WALLIS:

"Arithimetica Infinitorium" and Opera mathematica (Oxoniae, 1699), III 674,687,688,693 and 695 give solutions to nomenclators based on pre-calculus theory. Wallis' "Letter-Book" gives some of his important papers (Smith op cit, p32, p499)

Samuel Pepys Notes, Sir Christopher Wren's Discourses, Mr. Robert Hookes' Diary, and Dr. William Holder's notes all praise his mathematical ability and scholarly side but seem to put Wallis as a "extremely greedy of glorie, steales feathers from other to adorne his own cap." They do not give us a clue as to what Wallis might have in his hip pocket regarding diophantine problems.

In RE DIOPHANTINE EQUATIONS:

I did find some interesting references on this subject in my library.

>From the Seminaire de Theorie des Nombres, Paris 1980-81, Marie-Jose Bertin, ed.:

1) C. L. Stewart, "On some Diophantine Equations and Related Linear Recurrence Sequences." Univ. of Waterloo, Ontario, Canada.

2) R. Tijdeman, "Exponential Diophantine Equations" Proc. Intern. Congress Math., Helsinki (1978) p381-387.

3) T. N Shorey et al., "Applications of the Gel'fond-Baker method to Diophantine equations, Transcendence Theory; Advances and Applications," Academic Press, 1977.

plus 13 lesser references p321.ff. and,

>From the Seminaire de Theorie des Nombres, Paris 1984-85, Catherine Goldstein, ed.: Serge Lang {in FRENCH}: "Varietes Hyperboliques et Analyse Diophantienne," Univ of California, Berkley, 1986.

4) Kobayashi et T. Ochiai, "Meromorphic mappings into compact complex spaces of general type," Invent. Math. 31 (1975), 7-16.

5) S. Lang. - "Hyperbolic and Diophantine analysis, aparaitre," Bull. AMS, 1986.

6) D. Riebensehl, "Hyperbolische Komplex Raume und die Vermutung von Mordell," Math Ann. 257, (1981), 99-110.

plus 19 ancillary references.

==========

Further To Michael after intervening letters:

I have continued my search and found additional links in history to answer your question:

DIOPHANTUS

Diophantus of Alexandria (ca. 250) wrote three works that influenced greatly the later European number theorists. "Arithmetica", (6 out of 13 extant), "On Polygonal Numbers", (fragments survived), and "Porisms" which was lost. Translations of Arithmetica were made first by Xylander in 1575 [aka Dr. Wilhelm Holtzman at the Univ. Heidelberg] and then by Frenchman Bachet de Meziriac in 1621. A second carelessly printed edition in 1670 became historically important because it contained Fermat's famous marginal notes which stimulated extensive number theory research. Indeterminate algebraic problems where one must find only the rational solutions were named after him. Modern usage implies the restriction to integers. Diophantus did not originate problems of this sort but did originate the algebraic notation in the form of stenographic abbreviations.

FERMAT

Fermat (1601 -1665), of his varied contributions to mathematics, the most outstanding is the founding of the modern theory of numbers. He possessed nothing less than extraordinary intuition. Many of his contributions appear as marginal notes in Bachet's translation, including his last theorem that n>2 there do not exist positive integers x,y,z such that x**n +y**n = z**n. Fermat's famous "little theorem" regarding primes was dictated to Frenicle de Bessey, dated Oct. 18, 1640. It was not proved until 1736 by Euler. By 1770, Fermats theorems on prime numbers were proved by Euler and Lagrange.

Gauss conjectured the prime number theorem (distribution of primes) from both Fermat and Eulers work. J. H Rabin in 1659 published extensive factor tables for numbers up to 24,000 and in 1668 John Pell of England extended the table up to 100,000.

WALLIS

Wallis (1616-1703) was Newtons predecessor. His work with conics in "Arithmetica Infinatorum" was hailed for more than a century. His "De algebra tractatus, historicus & practicus", written in 1673 and published in 1685 was a serious attempt at the history of mathematics in England. Wallis edited parts of famous Greek mathematicians works for the Royal Society - one of which was our friend Diophantus. His contributions to the theory of integration are historic.

BARROW

Isaac Barrow (1630 - 1677) used Wallis' work to develop the theory of differentiation. He published his work in "Lectiones Opticae et geometricae." Wallis was a reviewer.

Newton (1642 - 1727) read Euclid's "Elements", Descartes' "La Geometrie", Oughtred's "Clavis", works by Kepler and Viete and the famous "Arithmetica infinitorum" by our boy Wallis. From his "Principia" has come much of our modern day math and physics.

ROSSIGNOL

Rossignol (1600 -1682) may have been familiar with Rene Descarte's (1596 - 1650) work on geometry and knew Pascal (1623 - 1662) from court and was aware of Pascal's letter to Fermat suggesting a solution to a problem proposed by Chevalier de Mere regarding the theory behind gambling. The correspondence between Pascal and Fermat regarding the "problem of points" laid the foundations of the science of probability. Rossignol used this theory for his cryptographic finds. Remember though it was the legendary William Friedman who did the pioneering work in the statistical side of crypto in the 1930's.

CONCLUSION

This historical tour leads me to believe that Wallis was aware of the preliminary implications of diophantine problems and that Rossignol was aware of the potential of probability in terms of cryptographic solutions. Could they have seen beyond the Fermat - Pell's work is difficult to prove.

REFERENCES

1) Meschkowski, H., "Ways of Thought of Great Mathematicians, tr by John Dyer-Bennet. San Francisco: Holden-Day 1948.

2) Ore, Oystein, Number Theory and Its History, New York: McGraw-Hill, 1948.

3) Pollard, H. The Theory of Algebraic Numbers, Carus Mathematical Mono., No. 9, New York: John Wiley, 1950.

4) Turnbull, H. W., The Great Mathematicians, New York: NYU Press, 1961.

5) Bell, E. T., Men of Mathematics, New York: Simon and Schuster, 1937.

6) David, F. Games, Gods and Gambling, New York: Haftner, 1962.

7) MacFarlane, A. Lectures on Ten British Mathematicians of the Nineteen Century, Math. Mono. No 17, New York: John Wiley, 1916.

8) Eve's H, Introduction to the History of Mathematics, 4th ed., New York: Holt, Rinehart and Winston, 1964.

==========

>From Michael to LANAKI
Subj: Diophantine revisited

There are several more threads in this search. What needs to be done is to trace back from contemporary (20th) century researchers to see what lines of work emerged. Lets see what can be found regarding D. E. Littlewood the prominent British mathematician and associate of G. H. Hardy and S. Ramanujan. The nineteenth century had Charles Babbage. The Willes family was prominent over several centuries but I do not know if Andrew Wiles is in this family tree. Tracing the men (women) and their methods around the Cambridge-Oxford researchers should reveal new information. Are their ACA members in England who could help? - Michael

==========

BINO, FOOT, G4EGG and THE DOC were suggested as possible contacts. Amazing where the links of cryptography spread. Like a giant spider. LANAKI

REFERENCES AND CRYPTOGRAPHIC RESOURCES

Volume II References were sent to the Crypto Drop Box (CDB) on 6 September 1996. They may be downloaded from there.