PRACTICAL CRYPTANALYSIS

by

WILLIAM MAXWELL BOWERS

VOLUME II

THE BIFID CIPHER

THE AMERICAN CRYPTOGRAM ASSOCIATION

P R A C T I C A L C R Y P T A N A L Y S I S

A Series Edited by Members of
THE AMERICAN CRYPTOGRAM ASSOCIATION

VOLUME II

THE BIFID CIPHER

By

William Maxwell Bowers

AMERICAN CRYPTOGRAM ASSOCIATION

1960

To

Frances A. Harris
(S-TUCK)

Who introduced me to the Bifid.

Copyright, 1960, by

American Cryptogram Association

C O N T E N T S

	Page
THE BIFID CIPHER	1
Method of Encipherment	1
Identification	4
Peculiarities	4
Solving The Bifid	7
THE THREE SQUARE TECHNIQUE	12
Rules for Using	14
Mechanics of Solving	16
FINDING THE PERIOD	19
Method 1 - Repeated Patterns	19
Method 2 - Chi-square Test	20
SOLVING WITH THE THREE SQUARE	23
Demonstration Example	24
THE EVEN PERIOD BIFID	31
Peculiarities	31
Finding the Period	34
Solution of the Even Period	35
Demonstration Example	37
CONJUGATED MATRICES	44
CONTINUOUS ENCIPHERMENT CYCLE	45
PROBLEMS	46
PROBLEM SOLUTIONS	48

F O R E W O R D

The solution of the Bifid Cipher is not adequately covered in any existing textbook available to civilian cryptographers. 'ELCY' barely mentions it. Sacco devotes a good deal of space to it but does not guarantee that a solution will always result. Cryprographie ABC's describes the mechanics of the system at some length, but makes no attempt to cover all the routines involved in affecting an entry and carrying on, from there, until solution has been achieved. Delastelle's own books are, of course, not concerned with the solution of the systems which he devised.

There have been numerous short articles in The Cryptogram, which have dealt with various aspects of Bifid solution and, as far as is known by the writer, this is the sole source of any extensive information on the solution of this interesting cipher system. Rosario Candela, who was a great student of the principal Delastelle systems - Bifid and Trifid - wrote and lectured at length on both of them but, unfortunately, his treatises on these subjects never reached the printer.

Much of the material for this booklet was derived from the above mentioned articles which have appeared, from time to time, in The Cryptogram. This was supplemented by correspondence with the experts of the old Circle 'B' Group and tried out during the many, many hours spent in attempting to apply the information garnered from these sources toward the actual solution of Bifids.

In A.C.A. administrative circles, it has long been thought that there was a need for additional instructive material on this system and this booklet is the result of that thinking. It was prepared, primarily, as a guide for beginners in the realm of the Bifid, but, it is hoped that the 'old timers' may also find some items of interest in these pages.

W. M. B.

Clarksburg, W. Va.
June 1960

THE BIFID CIPHER

The Bifid is one of the many cipher systems devised by the ingenious French cryptologist, F. Delastelle. Very little is known about the originator of the method other than that he was the author of several treatises on cryptography, the best known of which is his Traité Elémentaire de Cryptographie, Paris, 1902. Delastelle's own books give no information about their author. His contemporaries, as well as later writers, speak only of his works and tell nothing about the man, himself. Whether he was a member of the military, the diplomatic service, the police, or merely an interested civilian, has not been revealed; nor is his first name known to be anything other than 'F'.

During the period in which Delastelle's books were published, France was particularly interested in cryptography and cryptanalysis. In addition to the military and diplomatic ministries several other governmental departments had their code and cipher bureaus. The proposal of new systems and methods was encouraged and many were submitted, all of which were tested by a military commission selected for that purpose. It may well be that Delastelle's Bifid and Trifid systems were originally submitted to this commission for their consideration.

Commandant Bazeries, of the French army, tried in vain for many years to persuade the military cryptographic bureau to adopt a new cipher system which he had devised. Whether or not Delastelle was more successful and whether or not his Bifid system was ever used by the military or diplomatic services, is not known. However, it is a most interesting type and several of the foreign writers include a description of the system in their manuals.

METHOD OF ENCIPHERMENT BY BIFID.

	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

Delastelle's Bifid system, like many others, is a member of the checkerboard cipher family with a 25-letter alphabet set up in a 5 X 5 square. As originally presented, it operated something like this. An alphabet (straight, keyword, or scrambled) is written in the square and the rows and columns are numbered. A typical square with a keyword alphabet is shown above. The keyword is MANY OTHERS.

The encipherment process is periodic and the number of letters in each group is usually an odd number. Period lengths of 7, 9, 11, or 13 are those most frequently employed. Bifids can also be constructed in groups of even number periodic length, as 6, 8, 10, 12, etc., but, for the present, this treatise will

be limited to a study of those with odd number period only. Even period Bifids will be considered separately in a section devoted to that type alone.

Encipherment is a combination of substitution and transposition which can best be explained by an example illustrating how it is accomplished. The message - COME QUICKLY WE NEED HELP - will be enciphered in Period 7. After the plaintext is divided into groups of the selected periodic length, the first step is a substitution wherein the numerical row and column indicators are written vertically under the plaintext letters.

Plaintext:	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 4	3 4 4 1 5 2 1	2 2 3 2 2 4 4
Column	2 5 1 3 5 1 1	2 2 3 4 3 3 3	3 3 3 2 3 3 4

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 indicates its column. The cipher letters are then found in the square. This is usually illustrated like this

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

But, perhaps, it can be more clearly presented if it is set down in this manner.

	Row							Column						
Plaintext	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
Cipher	B		A		Q		K		U		G		M	

From the foregoing it is seen that the cipher letter, 'B', results from the fact that 'B' row (3) has the same number as 'C' row (3), and 'B' column (1) has the same number as 'O' row (1).

The same reasoning explains the the derivation of the second and third cipher letters, 'A' and 'Q'.

The fourth cipher letter, 'K', has the same row number (4) as plain 'I', and the same column number (2) as plain 'C', which are the last and first letters of the group.

The fifth cipher letter, 'U', is the result of 'U' row (5) having the same number as 'O' column (5) and 'U' column (1) being the same as 'M' column (1).

The sixth and seventh cipher letters have the same relation to their plaintext equivalents as cipher 'U' has to 'O' and 'M'.

Thus it is shown that each cipher letter results from some combination of half values of two plaintext letters. Due to this characteristic, the Bifid is classified as Fractional Substitution.

To decipher a message enciphered by Bifid, the first step is to fractionate the cipher letters into their row and column components. These are written horizontally in two rows of periodic length. The numerical values are then written in two horizontal rows below the Fractionated letters. The numbers are then read as vertical pairs and thus the plaintext letters are recovered.

Employing the same message as was used to demonstrate encipherment, the procedure can be shown.

Cipher Fract'd.	B_R	B_C	A_R	A_C	Q_R	Q_C	K_R
	K_C	U_R	U_C	G_R	G_C	M_R	M_C
Plaintext Row	3	1	1	2	4	5	4
Plaintext Col.	2	5	1	3	5	1	1
Plaintext	C	o	m	e	q	u	i

Before attempting to solve a secret message enciphered by Bifid, one should first thoroughly familiarize himself with the mechanics of the system by enciphering a few short messages and also by deciphering messages which have been prepared by others. Examples for practice are given below. Use the MANY OTHERS square for enciphering and deciphering these examples. Certain cipher letters are given in the first problem to show whether or not the encipherment is being done correctly.

Encipher.

```
S o l u t i o   n o f a b i f   i d r e q u i   r e s i n g e
T . . O . . O   . B . . . T .   . . Q . F . .   . . . R . . .

n u i t y o n   t h e p a r t   o f t h e s o   l v e r
. K . . . . .   . . . . . K .   . . . O . . .   Q . . F
```

Decipher.

```
H E R A T E D C U   R K F F D D B Y N   K O H Y M V E P N

H H H I B F G M G   T K N F I P G K Y   H H F
```

Accuracy of the decipherment is revealed by the plaintext recovered which starts with 'The' and ends with 'her'.

Encipher.

```
T h e F r e n   c h a r e e n   t h u s i a s   t i c c r y p

t o g r a p h   e r s a n d c   r y p t a n a   l y s t s
```

```
T h e F r e n c h   a r e e n t h u s   i a s t i c c r y

p t o g r a p h e   r s a n d c r y p   t a n a l y s t s
```

IDENTIFICATION OF THE BIFID.

1 - It is a substitution cipher.

2 - A frequency count will show not more than 25 letters.

3 - In English, the letter 'J' will ordinarily be omitted.

4 - If long repeats occur they will be at irregular intervals.

5 - Repeated patterns will occur. These are dependent upon the length of the repeated sequence and the period. The patterns will be in various forms such as:

A B . . D	A . . C D
A B . . D E	A B . C D

6 - A frequency count will show a much flatter profile than that of normal plaintext.

PECULIARITIES OF THE BIFID.

1 - When the cipher letters are set up in the correct period a few 'naturals' will occur. The term 'natural' is used to describe a vertical cipher pair, arranged in 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 pair is in column-row order unless the letter happens to be one of the five on the diagonal of the square running from cell 1-1 to cell 5-5.

Example: Enciphered from the MANY OTHERS square.

Cipher	H_R	H_C	A_R	A_C	H_R
	H_C	C_R	C_C	A_R	A_C
Plain	h	e	a	t	h

The first plaintext letter, formed from cipher H_R H_C, is a natural. The fourth letter, formed from cipher A_C A_R, is not a natural.

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 - When the cipher letters are set up in the correct period many 'half naturals' will occur. The term 'half natural' means that one of the letters of a vertical pair, in row-column order, is the same as the plaintext letter it represents.

Example: Enciphered from the MANY OTHERS square.

Cipher	T_R	T_C	Q_R	Q_C	S_R
	S_C	W_R	W_C	E_R	E_C
Plain	s	o	l	v	e

The probability that one of the letters of a row-column pair is a half natural is high. In fact it is 8 in 25, or 32 percent. This is visually demonstrated below.

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

Combinations giving a half natural 'R'.

Cipher	R_R	R_R	R_R	R_R	T_R	H_R	E_R	S_R
	Y_C	F_C	P_C	X_C	R_C	R_C	R_C	R_C
Plaintext	r	r	r	r	r	r	r	r

3 - Half naturals, in the column-row vertical pairs, will occur only when one of the letters is on the diagonal. As only 5 of the 25 letters can be on the diagonal, the probability of a given column-row letter being a half natural is reduced to one fifth of 32 percent which is only 6.4 percent.

4 - The probability of half naturals is also dependent upon and proportional to the plaintext frequency of the various letters. Granting that each cipher letter has a 32 percent chance of being a half natural, it must be remembered that the actual number of cases, wherein one of the cipher components will coincide with the plaintext letter, is controlled by the number of expected appearances of that plaintext letter. To illustrate, let it be assumed that in a cipher message of 100 letters there are 10 cipher 'E's and 10 cipher 'Z's. By the law of coincidence probability, the following half naturals could be expected to appear.

Cipher Letter 'E' 10 X 0.32 = 3.2 half naturals
Cipher Letter 'Z' 10 X 0.32 = 3.2 half naturals

As the letter 'E' may be expected to appear about 13 times in 100 letters of plaintext, one is safe in assuming that 3 or 4 of the cipher 'E's are half naturals. But, as the letter 'Z' is not expected to appear more than one time at the most in 100 letters of plaintext, then it is obvious that none of the 10 cipher 'Z's should be assumed to be a half natural.

5 - Half naturals are the Bifid's most vulnerable feature as they play an important part in the spotting of probable words.

6 - The Bifid, when fractionated for decipherment, engenders two separate and distinctly different alphabets. One of these is that which appears in the basic square where $T_R X_C$ equals 'R'. Or, using the numerical indices, $2_R 4_C$ equals 'R'. This is the alphabet which applies to the odd numbered vertical pairs in each periodic group. The other alphabet applies to the even numbered vertical cipher pairs. In the even number location $T_C X_R$ equals 'O'. This can be read:

'T' column number (1) used as row number (1),
'X' row number (5) used as column number (5), equals 'O'

This row-column switch is taken care of automatically when decipherment of a message is performed by one having knowledge of the arrangement of the letters in the square, because the numerical indices do not seem to know, or care, whether they represent rows or columns. What actually happens can best be

illustrated by deciphering a group.

Cipher Group - Period 5	T	Q	S	W	E
Cipher Fractionated	T_R	T_C	Q_R	Q_C	S_R
	S_C	W_R	W_C	E_R	E_C
Substituting Numerical Indices	2_R	1_C	4_R	5_C	2_R
	5_C	5_R	3_C	2_R	3_C
Switching the R-C designation of vertical pairs 2 and 4	2_R	1_R	4_R	5_R	2_R
	5_C	5_C	3_C	2_C	3_C
Plaintext	s	o	l	v	e

Particular attention is called to this switch from column-row to row-column in order to thoroughly familiarize the reader with the mechanics of the Bifid process.

7 - Repeated plaintext sequences produce patterns which can be recognized in the cipher. For this to happen a repeat must start in the same relative location in a group as that of its first appearance. That is, if the first appearance starts at an odd numbered position, a repeat of that sequence, starting at any odd numbered location in any other group, will produce the same cipher letters. The same thing happens if both occurrences of a repeat start at even numbered locations.

	Odd	Even
Plaintext	1 3 5 7 h o m e i s a	2 4 6 a h o m e i s
Cipher	2 1 1 2 4 2 1 2 5 1 3 1 5 2 T A K A U B V	1 2 1 1 2 4 2 2 2 5 1 3 1 5 A M R H S N O
Plaintext	1 3 5 7 g o h o m e n	2 4 6 t h e h o m e
Cipher	3 1 2 1 1 2 1 5 5 2 5 1 3 4 B T A O V U F	2 2 2 2 1 1 2 1 2 3 2 5 1 3 H H M A E S N

The spacing of 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 other lengths generate their own individual patterns. For Period 7 these are:

	Odd	Even
3 letter repeat	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 one of the first steps to be taken in the solution of a Bifid and it is well to thoroughly understand just how patterns of any length, in any period, are generated. This can best be explained by an illustration.

For this example, the plaintext word 'Bifid' will be enciphered in period 9 using the MANY OTHERS square.

	Odd Position	Even Position
Plaintext	. . 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 . .

From the above it is seen that these 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 the other four places of the group, the same patterns will always show for the word 'bifid' whenever it is enciphered from this same square in period 9.

SOLVING THE BIFID.

With the exception of articles in The Cryptogram, official publication of the American Cryptogram Association, there is little or no material available to the amateur cryptanalyst on how to solve Bifid ciphers. The recent popular books on cryptography by American authors do not even mention the system, nor do the textbooks of Wolfe and Milliken. Elementary Cryptanalysis, by Helen F. Gaines, briefly describes the system but concludes: "We will make no attempt, here, to go into the decryptment of these ciphers."

General Luigi Sacco's Manuale di Crittografia devotes quite a few pages to the solution of the Bifid. In this he states that in long messages, or with a large volume of material to work with, there may be a sufficient number of repetitions to enable the solver to identify the plaintext equivalents of some of the vertical pairs of higher frequency. However, he goes on to say that in short individual messages this is not possible and a solution cannot be achieved without, as he calls it, "interviene qualche altro ausilio". This can be roughly translated to mean "without the intervention of some other auxiliary". And this broad term 'auxiliary', can be interpreted to denote 'help', 'a tip', etc.

This 'altro ausilio', which Sacco hopes for, can be nothing other than given plaintext words or correctly spotted probable words. In an example of solution, Sacco assumes that the words 'la situazione' are known, together with their correct location in the message. With his entry thus made, he developes his solution by the method of gathering equivalences.

When members of the American Cryptogram Association were first introduced to the Bifid, via an article by William A. Lee (TONTO) in the June 1945 issue of The Cryptogram; the method he presented was very similar to that described by General Sacco.

In conjunction with this article a short Bifid was given and the reader was invited to test his skill by attempting to solve it. This same cipher message can be used to demonstrate the method of solution as described by Mr. Lee.

BIFID. Period 7. Constructed by A.B.C.
The given word is 'diamonds' and when you have correctly located it, by a natural, you should guess the short word that precedes it.

```
E T I A L I G   L D M N I T V   N F E M I S I   E E I D G E I
H P C E D U T   P I N O F L W   I N D L E E K
```

To set it up for solution, the cipher message is first fractionated, by groups, with the row and column designation of each letter indicated by sub-letters 'R' and 'C'.

$E_R E_C T_R T_C I_R I_C A_R$ $L_R L_C D_R D_C M_R M_C N_R$ $N_R N_C F_R F_C E_R E_C M_R$ $E_R E_C E_R E_C I_R I_C D_R$
$A_C L_R L_C I_R I_C G_R G_C$ $N_C I_R I_C T_R T_C V_R V_C$ $M_C I_R I_C S_R S_C I_R I_C$ $D_C G_R G_C E_R E_C I_R I_C$
i
$H_R H_C P_R P_C C_R C_C E_R$ $P_R P_C I_R I_C N_R N_C O_R$ $I_R I_C N_R N_C D_R D_C L_R$
$E_C D_R D_C U_R U_C T_R T_C$ $O_C F_R F_C L_R L_C W_R W_C$ $L_C E_R E_C E_R E_C K_R K_C$

Inspection of the fractionated cipher reveals that there is but one natural in the entire message. This is in group #1 where the vertical cipher pair $I_R I_C$ equals plain 'i'. Note that in the 4th group the vertical cipher pairs $E_C E_R$ and $I_C I_R$ are <u>not</u> naturals as far as is now known. If it developes that one of these letters happens to be on the diagonal of the square, then that letter can also represent itself.

Having spotted the given word by means of an 'altro ausilio' the fractionated plaintext is now written below the fractionated cipher letters for the purpose of gathering equivalent values. As it was also stated that the short word which precedes 'diamonds' could be guessed, it will be assumed to be 'The'.

Cipher $E_R E_C T_R T_C I_R I_C A_R$ $L_R L_C D_R D_C M_R M_C N_R$
$A_C L_R L_C I_R I_C G_R G_C$ $N_C I_R I_C T_R T_C V_R V_C$

Plaintext $T_R H_R E_R D_R I_R A_R M_R$ $O_R N_R D_R S_R$
$T_C H_C E_C D_C I_C A_C M_C$ $O_C N_C D_C S_C$

The equivalent values, as shown by similar location of cipher and plaintext components, are then checked off and are tabulated as shown below. As these are checked, the letters are circled, as shown, for the first set taken off: E_R, T_R, and S_C. After all the equivalents are tabulated, arbitrary numerical indices are assigned to each set, starting with 1 for the set having the most values.

4 - E_R T_R S_C

2 - E_C H_R L_C N_R

3 - T_C D_R A_C G_R

1 - I_R D_C S_R I_C N_C O_C A_R M_R

5 - L_R H_C O_R

6 - G_C M_C

These equalities can then be written outside a 5 X 5 square and their location within the square is found at the intersection of the row and column of each individual letter as shown below.

	1	2	3	4	5						
1	I		A	S		M		I	S	A	M
2	N				H			H	N		
3	D					G		D	G		
4		E	T					E	T		
5	O	L						L	O		
	D	E	T	S	H	G					
	I	L	A			M					
	N										
	O										

When a letter is placed in the square it is checked off.or erased, on the outside. It will be noted that 'M' and 'G', which are in the same column,can be placed in either col.-2 or col.-5 as cells of these columns are vacant in both row-1 and row-3, in which rows these will have to be placed. Until it is definitely determined which one of these is the correct column, 'M' and 'G' must remain outside the 5 X 5 square.

The numerical values, thus obtained, are now applied to the remainder of the cipher pairs in the message, with the hope of being able to recover fragments of other words.

E_R	E_c	T_R	T_c	I_R	I_c	A_R	L_R	L_c	D_R	D_c	M_R	M_c	N_R	N_R	N_c	F_R	F_c	E_R	E_c	M_R	E_R	E_c	E_R	E_c	I_R	I_c	D_R
A_c	L_R	L_c	I_R	I_c	G_R	G_c	N_c	I_R	I_c	T_R	T_c	V_R	V_c	M_c	I_R	I_c	S_R	S_c	I_R	I_c	D_c	G_R	G_c	E_R	E_c	I_R	I_c
4	2	4	3	1	1	1	5	2	3	1	1		2	2	1			4	2	1	4	2	4	2	1	1	3
3	5	2	1	1	3		1	1	1	4	3				1	1	1	4	1	1	1			4	2	1	1
T	h	e	d	i	a	m	o	n	d	s	a				i				n	i						i	d

H_R	H_c	P_R	P_c	C_R	C_c	E_R	P_R	P_c	I_R	I_c	N_R	N_c	O_R	I_R	I_c	N_R	N_c	D_R	D_c	L_R
E_c	D_R	D_c	U_R	U_c	T_R	T_c	O_c	F_R	F_c	L_R	L_c	W_R	W_c	L_c	E_R	E_c	E_R	E_c	K_R	K_c
2	5					4			1	1	2	1	5	1	1	2	1	3	1	5
2	3	1			4	3	1			5	2			2	4	2	4	2		
						t									s		s			

A study of the results of this step show that only scattered plaintext letters have been recovered and these do not immediately suggest any additional plaintext words. However, one important item is noted. This is the fact that the vertical numerical pair, 2/2, is repeated three times, indicating that it may well be one on the high frequency plaintext letters. Checking back, it is found that practically all of the high frequency plaintext letters have been recovered and have coordinate values as shown.

Plaintext	E	T	A	O	N	I	R	S	H
Row	4	4	1	5	2	1		1	2
Column	2	3	3	1	1	1		4	5

The only high frequency letter unrecovered is 'R' and 2/2 could could be 'R', but, if such is the case, no particular progress has been made as there are no cipher 'R's to give additional numerical values. Investigating further, it is noted that these 2/2 pairs result from the following cipher letter combinations: H_RE_c, N_RL_c, N_RE_c. Both 'N' and 'E' are repeated in these pairs.

It is also noted that plaintext 'E' appears but once in the plaintext thus far recovered, and that there is only one other possible 'E' in the numerical coordinates that have been written

below the cipher letters. This is in the fourth group, where $E_R G_c$ equals 4/?. A plaintext 'E' could be derived from this combination by shifting 'M' and 'G' to column-2, but that also is not an entirely satisfactory solution of the problem as it would give but one additional 'E' and would, from the existing numerical pairs, create two additional 'M's.

As about six or seven plaintext 'E's may be expected in this message of 49 letters, the assumption is therefore inevitable that 'E' and 'T' should be moved from the fourth row to the second row making the coordinates of $E_R E_c$ equal 2/2 and, as $E_R = T_R = S_c$, then 'S' must also be moved to the second column.

These shifts can be made in the square without conflict. The square, with adjustments made, is shown below.

	1	2	3	4	5	
1	I	S	A			M
2	N	E	T		H	
3	D					G
4						
5	O	L				

Corrections must now be made on the cipher work sheet, changing all 4s to 2s. Any other plaintext letters which are recovered by means of this adjustment are then written in and the message is again studied to determine where the next attack shall be made. That part, which follows immediately after the plaintext words, 'The diamonds', looks like a favorable spot.

In this section there are numerous recovered plaintext letters as well as several half values. Under these half values, all of the possible plaintext letters are written, as there is a strong chance that additional plaintext may be anagrammed from these possible letters. This gives the following:

Cipher	M_R	M_c	N_R	N_R	N_c	F_R	F_c	E_R	E_c	M_R	E_R	E_c	E_R	E_c	I_R	I_c	D_R	H_R	H_c	P_R	P_c	C_R	C_c	E_R
	T_c	V_R	V_c	M_c	I_R	I_c	S_R	S_c	I_R	I_c	D_c	G_R	G_c	E_R	E_c	I_R	I_c	E_c	D_R	D_c	U_R	U_c	T_R	T_c
	1		2	2	1			2	2	1	2	2	2	2	1	1	3	2	5					2
	3				1	1	1	2	1	1	1			2	2	1	1	2	3	1			2	3
Plaintext	a				i			e	n	i	n			e	s	i	d	e						t
		n		n		i	i					n	n							i			s	
Possible		(e)		e		n	n					e	e							n			e	
		t		t		(d)	(d)					(t)	t							d			l	
		h		(h)		o	o					h	(h)							o				
Probable	a	r	e	h	i	d	d	e	n	i	n	t	h	e	s	i	d	e						

This makes good plaintext and the new equivalents are gathered and placed in the square as shown below.

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

Additional plaintext letters could be recovered by further anagramming of possible values but, as thirteen of the twenty five letters have been definitely placed in the square, and two others (R and V) have been partially placed, one can now attempt to rearrange the square as it was originally set up. If this can be accomplished the correct location of other letters will be indicated unless it should develop that the alphabet is scrambled.

Whenever the letters in a Bifid square are rearranged it must be remembered that all shifts must be of complete rows or columns; and that whenever a row is shifted the corresponding column must also be shifted to the same numerical position. That is, if row-5 is shifted to row-2, then column-5 must be shifted to column-2. In effect, this is merely a reassignment of numerical indices to a set of equivalents.

Inspection of the square, as now partially filled, reveals that in all probability an unscrambled keyword alphabet has been used. By this it is meant that a keyword has been written horizontally, starting in cell 1/1, and that the remaining letters of the alphabet have been placed in order following the keyword. This method of setting up the square by the presence of three alphabetically consecutive letters, D-F-G, located in the third row.

If the above assumption is correct, then 'E' will have to be in the keyword as it is located in another row. Therefore, D-F-G must be in adjacent cells in that order. This is accomplished by shifting column-1 to column-2 location. When this is done, row-1 must also be changed to row-2 location. Column-5 is then moved to column-4 bringing 'G' into the cell on the right of 'F'. Row-5 is also moved to row-4 position, completing the double shift.

Retaining the same numerical indices for the original rows and columns in their transposed position, the letters in the square are now arranged in this manner.

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

From what is now shown, it is evident that the letter 'V' must move up into the bottom row making this row contain V-W-X-Y-Z. Also, it does not require a great deal of ingenuity to now be able to guess the keyword - ENTHUSIA(S)M - and the complete square can now be reconstructed.

Having recovered the square, always the solver's goal in ciphers of this type, the solution is now complete. The decipherment of the remainder of the message is purely mechanical and it is left to the reader to do this if he really wants to know where "the diamonds are hidden".

* * *

In the foregoing pages the Bifid cipher has been described as it was originally presented to A.C.A. members, and the routine procedure of substituting numbers for letters and resubstituting letters for other combinations of these numbers has been explained in detail. Equivalents were gathered and numerical indices were assigned to them. Eventually, the complete square was recovered. This method of solution was used with the example because, having described the original routine for encipherment, it was considered necessary to show the steps of a solution using the same routine.

However, having acquainted the reader with the mechanics of a Bifid, it can now be stated, without fear of creating too much confusion, that the encipherment, decipherment, and/or solution of a Bifid by the above described method, is as obsolete as the dodo bird and as clumsy as the operation of an ancient abacus in comparison with that of a modern slide rule. Another way of doing all this will be described in the following section.

THE THREE SQUARE TECHNIQUE.

In the August-September, 1945, issue of The Cryptogram , an article by Herbert Raines presented a method for working with the Delastelle Bifid which he called The Three Square Technique, or The Bifid with Literal Indices Only. This system eliminates entirely the use of numerical indices as row-column indicators and allows the letters in the square to act in this capacity. This can be demonstrated using the square from the example just solved.

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

Basic Square

Reference to this square, which will hereafter be called the Basic Square, will show that the location of any given letter can be designated by the letters in its row and column as easily as by its row and column numbers. Thus, the letter 'G' can be identified as $C_R H_c = G$, $K_R Q_c = G$, $F_R Y_c = G$, as well as all other combinations ofletters of G-row and G-column.

To further illustrate this use of literal indices, the first group of the 'Diamond' message can be shown as it was deciphered.

$$\begin{array}{cccccccc} E_R & E_c & T_R & T_c & I_R & I_c & A_R & \\ \underline{A_c} & \underline{L_R} & \underline{L_c} & \underline{I_R} & \underline{I_c} & \underline{G_R} & \underline{G_c} & \\ t & & e & & i & & m & \end{array}$$

Inspection of the Basic Square will show that: $E_R A_c = T$, $T_R L_c = E$, $I_R I_c = I$, $A_R G_c = M$, thereby demonstrating that the substitution step of the Bifid can be accomplished without the use of numbers.

It will be noted that only the odd numbered pairs of the above group were deciphered. That is because, read as a pair as they are shown, the even numbered pairs do not locate the correct letter in the Basic Square. For example, reading the second pair as $E_c L_R$ would give 'L'. It is known that this is not true, because the second letter has been found to be 'H'.

This apparent falacy is easily explained. Item number 6 of the Peculiarities of the Bifid called attention to the alphabetic switch that occurs at this point in the encipherment or decipherment process. The second pair, $E_c L_R$ actually should be read:

E-column as row indicator,
L-row as column indicator,
equals 'H'.

Reverting back, momentarily,to numerical indices,it would be

E-column (1) used as row,
L-row (4) used as column,
equals 'H'.

It is for the handling of these even numbered pairs that Raines brings his other two squares into the picture. If 'H'is the result of E-column used as row and L-row used as column, then let these letters be so arranged that such is the case. To accomplish this he arranged the squares as shown on the next page.

By this arrangement, all plaintext letters are always found in the Basic Square at locations specified by the cipher pairs.

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

TOP SQUARE
Row used as column indicator

LEFT SQUARE
Column used as row indicator

BASIC SQUARE
Normal row and column

For the odd numbered cipher pairs the cipher letters are found in the Basic Square and their plaintext equivalent is located at the intersection of their row and column, thus:

Cipher					Plaintext
$E_R A_c$	is	E_R (Basic),	A_c (Basic)	equals	T (Basic)
$H_R X_c$	"	H_R " ,	X_c "	"	T "

For the even numbered cipher pairs the cipher letters are found in the Left and Top Squares, and the plaintext letters they representis then found in the Basic Square the intersection.

Inspection of the Three Square arrangement will show that in the Left Square the columns of the Basic Square are setup as rows in the order of their numerical values. Thus, the five letters of basic column-1 are set up in Left in line with row-1 of the Basic Square. In like manner, the letters of the other four columns are written horizontally in line with their respective rows of the Basic Square. With this arrangement, when 'E' column is used as row indicator, then the resulting plaintext letter will be found in the row of the Basic Square which is on line with the 'E' of the Left Square.

In the Top Square the rows of the Basic Square are set up as columns. These are also arranged in their numerical order above the corresponding columns of the Basic Square. Thus, when 'L' row is used as column indicator, the resulting plaintext letter is found in the column of the Basic Square that stands vertically under 'L' in the Top Square. To illustrate:

Cipher						Plaintext
$E_c L_R$	is	E_c as row (Left),	L_R as col.(Top),	equals	H (Basic)
$T_c I_R$	"	T_c " " " ,	I_R " " " ,	"	D "

Using the Three Square Technique, decipherment of the first group of the 'Diamond' message can now be completed.

	E_R	E_c	T_R	T_c	I_R	I_c	A_R
	A_c	L_R	L_c	I_R	I_c	G_R	G_c
Odd pairs	t		e		i		m
Even pairs		h		d		a	

From the above demonstration it is seen that the Bifid can be deciphered just as easily without the use of numerical indices as with them. The same thing is true for the encipherment prosess. The few simple rules which govern both encipherment and decipherment are outlined in the following section.

RULES FOR ENCIPHERMENT AND DECIPHERMENT - (Three Square)

The Three Square Technique is used for both encipherment and decipherment purposes. as the Bifid is a fractional substitution cipher, one is always starting with fractions of two letters and searching for the single letter that is represented by these half values. This single letter is always found in the Basic Square in both encipherment and decipherment. The only thing that it is necessary to learn is in which squares the fractional letters are to be found.

For encipherment, the pairs will be fractionated like this:

$S_R X_R$ $S_R X_c$ $S_c X_c$

For decipherment, the fractionated pairs will be:

$S_R X_c$ or $S_c X_R$

Three simple rules govern the location of the fractional letters. These are:

1 - When one (or both) of the fractional letters is in true position in a pair, it (or they) is found in the Basic Square.

Example: $S_R X_c$ - Both in Basic
$S_R X_R$ - S in Basic
$S_c X_c$ - X in Basic

2 - When one of the fractional letters of a pair indicates that its row designates the column of the letter it is to represent, then it shall be found in the Top Square.

Example: $S_R X_R$ - X in Top Square
$S_c X_R$ - X in Top Square

3 - When one of the fractional letters of a pair indicates that its column designates the row of the letter it is to represent, then it shall be found in the Left Square.

Example: $S_c X_c$ - S in Left Square
$S_c X_R$ - S in Left Square

In all cases the third letter will be found in the Basic Square at the intersection of the row and column indicated. Using the ENTHUSIA(S)M square, each of these conditions can be shown.

$S_R X_c$ - S row (Basic),	X column (Basic),	equals A (Basic)
$S_R X_R$ - S row (Basic),	X row as Col. (Top),	equals B (Basic)
$S_c X_c$ - S col. as row (Left),	X column (Basic),	equals T (Basic)
$S_c X_R$ - S col. as row (Left),	X row as col. (Top),	equals U (Basic)

Using the same square, the word 'solve' will be enciphered and its cipher equivalent will be deciphered in order to fully demonstrate the application of the method in each combination of the row and column indicators.

To encipher, one must work with the plaintext letters, two at a time, going through the periodic group twice. The reason for

this double trip is that, although the plaintext is written only one time - like this:

S O L V E

it is mentally visualized as being fractionated - like this:

S_R O_R L_R V_R E_R
S_C O_C L_C V_C E_C

Or, the plaintext group can be pointed off in this way:

$\overline{\underline{S}}$ $\overline{\underline{O}}$ $\overline{\underline{L}}$ $\overline{\underline{V}}$ $\overline{\underline{E}}$

whereby the overlining indicates row components and the underlining indicates column components.

Under this plaintext group the cipher letters are written after being found in accordance with the rules stated above.

Plaintext	$\overline{\underline{S}}$	$\overline{\underline{O}}$	$\overline{\underline{L}}$	$\overline{\underline{V}}$	$\overline{\underline{E}}$
Cipher	M	R	E	S	E

In this case, the cipher letters were found in this way.

S_R O_R - S row (Basic),	O row as col.(Top),	equals	M	(Basic)
L_R V_R - L row (Basic),	V row as col.(Top),	"	R	"
E_R S_C - E row (Basic),	S column (Basic),	"	E	"
O_C L_C - O col. as row (Left),	L column (Basic),	"	S	"
V_C E_C - V col. as row (Left),	E column (Basic),	"	E	"

When deciphering, the vertical pairs of the fractionated cipher letters are those for which the plaintext equivalents are to be found. The set-up is like this:

Cipher	M	R	E	S	E
Fractionated	M_R	M_C	R_R	R_C	E_R
	E_C	S_R	S_C	E_R	E_C
Plaintext	s	o	l	v	e

The plaintext letters are found by using the same rules.

M_R E_C - M row (Basic),	E column (Basic),	equals	S	(Basic)
M_C S_R - M col. as row (Left),	S row as col.(Top),	"	O	"
R_R S_C - R row (Basic),	S column (Basic),	"	L	"
R_C E_R - R col. as row (Left),	E row as col.(Top),	"	V	"
E_R E_C - E row (Basic),	E column (Basic),	"	E	"

With a little practice one soon becomes familiar with the proper handling of all row-column combinations and finds that the Three Square Technique is much easier and simpler to work with than the method requiring numerical indices. It is also far more compact, as the amount of necessary writing is greatly reduced.

There is another 'wrinkle' that is a time and labor saver and there is no reason why a beginner with the Bifid should not

immediately adopt it. In copying a Bifid message for solution, the cipher letters must be fractionated as has been demonstrated on numerous occasions previously. Cipher group - M R E S E -was fractionated in this way.

$$\begin{matrix} M_R & M_c & R_R & R_c & E_R \\ E_c & S_R & S_c & E_R & E_c \end{matrix}$$

More than half of this writing can be eliminated by omitt the even numbered pairs. To give the complete picture, all that it is necessary to write is this:

$$\begin{matrix} M & & R & & E \\ & E & & S & & E \end{matrix}$$

The solver reads the the written pairs (odd) as normal row-column combinations. The omitted pairs (even) can be visualized as indicated by the diagonal lines. These are always column-row combinations when the periodic length is an odd number as 9 or 11.

Another advantage of this 'hit-skip' method of copying the message for solution, is that it assists in the search for half naturals. The great majority of half naturals are found among the odd numbered pairs and the elimination of the even numbered pairs serves to remove from view these letters which, if present, would not only distract the eye when one is looking for half naturals, but might also influence the inexperienced solver to make false assumptions relative to probable words.

THE MECHANICS OF SOLVING WITH THE THREE SQUARES.

After the period has been determined, the message is written in 'hit-skip' fractionated form as shown above. If a given word has been provided, one is immediately ready to begin the recovery of the square. For this demonstration, the familiar message about 'The diamonds' will be used. The period is 7 and the location of plaintext 'the diamonds' is known. The solver starts with this:

$$\begin{array}{ccccccc|ccccc} E & & T & & I & & A & L & & D & & M & & N \\ & A & & L & & I & & G & N & & I & & T & & V \\ \hline t & h & e & d & i & a & m & o & n & d & s \end{array}$$

On quaqrille paper, two intersecting lines are drawnat right angles to each other. These two lines represent the dividing boundaries of the three squares. Five spaces should be allowed on the left of the vertical line and above the horizontal line, Unlimited space should be left below and to the right of these lines. As the upper left quadrant will receive no letters, the plaintext word being tested can be written there for future identity of the test.

It is advisable, when testing a probable word or deciphering a known one, to start with the even numbered pairs. This is in order to get letters in the Left and Top Squares immediately. In accordance with this recommended practice, the even numbered pairs of the above groups will be placed first, starting with the visualized number two pair of group #1, namely: $E_c\ L_R = h$.

'E' is written in the Left Square.
'L' is written in the Top Square.
'H' is written in the Basic Square at the intersection.

	L
E	H

The other even numbered pairs are then added, giving this:

The Diamonds

						L	I	G	T
					E	H			
					T		D		
					I			A	
					L		N		
					D				S

Note that when the fourth even pair, L_c I_R = N, is written in, 'I' has already been placed in the Top Square. The 'L' is placed in the Left Square and 'N' is written in its indicated location in the Basic Square to complete the equation.

The odd numbered pairs can now be written in. All of these letters, both cipher and plaintext, will be in the Basic Square.

	L	I	G	T	
E	H				
T		D			
I			A		
L		N			
D				S	
			T		E

E_R A_c = T

'E' is written in an unallocated row and column of the Basic Square.

'A' has already been placed in Basic from the even numbered pairs.

'T' is written at the intersection of E_R and A_c.

When this equation is added to those already spotted from the even numbered pairs, the additional letters are located as shown in the square on the left above.

The other odd numbered pairs are then added in the same manner. The final result is shown in the square on the right. These values should now be consolidated, placing all letters in all three of the squares. To do this, one must remember the make-up of the three squares. It is suggested that the reader prepare, on a separate sheet of paper, a copy of the Three Square diagram containing the ENTHUSIA(S)M alphabet which is shown on Page 13. This can then be readily referred to when reading the instructions which govern the placement of all letters in all squares.

	L	I	G	T		
E	H					
T		D				
I			A			M
L		N				
D				S		
			T		E	
		O			L	
						G
		I				

As previously stated, the Basic Square consists of the normal rows and columns. In the Left Square the letters of the separate Basic columns are written horizontally in line with their respective rows. In the Top Square, the letters of the separate Basic rows are written vertically above their respective columns. These conditions control the placing of letters in other squares.

Thus, 'E' in Left is the column (horizontal) of 'H' row in Basic. Also, 'E' in Basic is the column of 'H' row (vertical) in Top. Therefore, having located 'E' in Left in line horizontally with 'H' in Basic; and having also located 'E' in Basic; then 'H' can be placed in the Top Square in line vertically with 'E' of Basic.

E	H	
		E

Diagrammed separately, when a situation exists as shown on the left, then 'H' can be placed in the Top Square as illustrated on the right.

		H
E	H	
		E

		T
		S
	T	

Likewise, having 'S' in Basic under 'T' in Top, then 'S' goes into Left in line with 'T' of Basic.

		T
		S
S	T	

Making all adjustments in accordance with the above stated rules and combining, where letters are shown to be in the same row or column, gives the following arrangement in which all twelve of the recovered letters have been properly placed in each of the three squares. These have been placed at random, as they were recovered, but they can be rearranged symmetrically at any time.

The Diamonds

						S				
						M				
					O	A	D	E	N	
					L	I	G	T	H	
			L	E	H	N				
			A	T		D				G
	O	N	D	I		I	A	S		M
				S			T		E	
				H		O			L	
			G	M						

Reference to the diagram on page 9 will show that these are the same values which were recovered at this stage in the solution of this message by the numerical index system. By using the same reasoning as described in the step by step solution, additional values can be recovered until the three squares are completely filled.

This demonstration just about wraps up the discussion concerning how to operate with Bifids by means of the Three Square Technique. With a relatively small amount of practice, one can soon become proficient in its use. All who employ it consider it to be, by far, the simplest as well as the most efficient method method of working with cipher messages of this type.

FINDING THE PERIOD OF A BIFID.

METHOD 1 - REPEATED PATTERNS.

Knowledge of how to determine the period of a Bifid cipher is of prime importance to the solver. This is not at all difficult if the message contains repeated words which are 'in step' with each other. By 'in step', it is meant that the repeats start at the same relative location in the group. That is, if one of them starts at an odd numbered position, then the other must also start at an odd numbered position in order to generate a duplicate pattern. Likewise, if the repeated plaintext words start at an even numbered location, duplicate patterns will also appear.

The following message will be used to demonstrate how the period may be determined by repeats occuring therein.

L L S U T T C K Q D D I W E S L V A B E T L E L L

G T U M G D I I A K A A A N D I F E L L M U T T N

M N T T V I S H O C C C B E N S G S

The search is for patterns created in the cipher letters by repeated sequences of four or more plaintext letters. The form which such patterns take was shown on Page 6 in the section dealing Peculiarities of the Bifid and a return to that section will refresh the reader's mind with respect to what to look for.

Inspection of the above message shows a pattern duplication starting with letters #1 and #44. This is:

```
 1
 L L S U T T
44
 L L M U T T
```

In Bifid repeat patterns, the first part of the pattern (LL) is generated by the Plaintext row components and the second part (UTT) by plaintext column components. Having spotted a repeat, it is then necessary to find out in which period these repeated cipher letters will fall into place in such a way as to become row and column components of a plaintext word. The simplest way to do this is to try them in various periods and compare the results.

Period - 5

```
| L  L  S | T  C  K |
| S  U  T | K  Q  D |

| I  F  E | M  U  T |
| E  L  L | T  T  N |
```

Period - 7

```
| L  L  S  U |
| U  T  T  C |

| E  L  L  M |
| M  U  T  T |
  r  e  p  e  a  t
```

Period - 9

```
| L  L  S  U  T |
| T  T  C  K  Q |

| A  A  N  D  I | M  U  T  T  N |
| I  F  E  L  L | N  M  N  T  T |
```

Only in Period-7 do the do the pattern combine properly and so it is obvious that 7 is the correct period for this message. The pattern, which reveals the period, is formed by the plaintext word 'repeat', which occurs twice.

From information gained by knowledge of the location of the word 'repeat', the reader should be able to decipher the remainder of the message. By this, it is not meant that a beginner may expect to easily complete the decipherment from what has thus far been recovered. In a message as short as this one, that would be a rather difficult job for one who is experienced in working with Bifids. However, a study of the partially filled square should ring a bell in the mind of the solver, as there seems to be something familiar about it. When the reader determines just what this similarity is - then he will have the complete square.

Relative to periods, it can be safely said that a very great majority of the Bifid ciphers which the amateur cryptanalyst will have to deal with, will have the period given or will reveal it through repeated patterns in the cipher letters.

METHOD 2 - MATHEMATICAL

When repeats do not conveniently occur in a Bifid, the right period may still be determined. For dealing with this problem the mathematicians have come to the assistance of the solver. A procedure, known to statisticians as Karl Pearson's 'Chi-square Test', will do the trick nicely. This statistical test was adapted to the characteristics of fractional substitution and its operation in that field was admirably explained by D. Morgan in an article in The Cryptogram, June-July 1946. This method will be briefly outlined here and an attempt will be made to demonstrate that it is neither necessary to understand statistical theory, nor to be a mathematician, in order to determine the correct period of a Bifid by the Chi-square Test. The same old familiar message about 'The diamonds' will be used to illustrate the basic idea.

Plaintext	T H E D I A M	O N D S A R E
Cipher	E T I A L I G	L D M N I T V

Overlined cipher letters are derived from ROW components.
Underlined cipher letters are derived from COLUMN components.

As has been previously explained and as the above shows, the first section of letters of a cipher group are found from Row-Row combinations of the fractionated plaintext letters. Likewise, the last section of letters comes from Column-Column combinations. The middle letter of a cipher group always results from a Row-Column combination and, therefor, is not included in the Chi-square Test.

Thus, always excluding middle letters, each cipher group may be considered to be made up of two separate and distinct classes of letters. Of these, the first category derives from R-R combinations and may be called the Row family. The second class, being derived from C-C combinations, may be called the Column family.

It is logical to assume that the cipher letters of the Row family bear some group relation to each other and that, as a group, they are distinctly different from those of the Column family.

It is also indisputable that when all of the Row family are grouped together in one place, and all of the Column family are grouped together in another place close by; then, under these conditions, the dissimiliarity of the two families becomes most apparent and is more easily recognized.

By adding another group of cipher letters to the two shown above, in order to have more material with which to work, and by designating the two families by different symbols, the truth of this statement can be graphically illustrated.

Let 'x' represent cipher letters of the Row family.
Let 'o' represent cipher letters of the Column family.

Cipher:	E T I (A) L I G	L D M (N) I T V	N F E (M) I S I
Symbols:	x x x - o o o	x x x - o o o	x x x - o o o

Here, the cipher letters are arranged in their correct periodic groups. The two symbolic families are segregated, one from the other, and it is seen that they are entirely different.

Retaining the same symbol for each individual cipher letter the message will be set up in other periodic lengths to show that this segregation does not exist in any except the correct period.

The following is the message, with true family symbols substituted for all of the cipher letters.

x x x - o o o x x x - o o o x x x - o o o x x x - o o o etc.

Assuming the period to be unknown, the message is tested and the result is as shown below.

	Period-5	Period-7	Period-9
Group 1	x x | x | - o	x x x | - | o o o	x x x - | o | o o x x
Group 2	o o | x | x x	x x x | - | o o o	x - o o | o | x x x -
Group 3	- o | o | o x	x x x | - | o o o	o o o x | x | x - o o

In periods 5 and 9 the elements which comprise the two possible family groups are so intermingled that it cannot be determined which of the two symbolic families predominates. Only in period-7 is there complete dissimilarity between them.

That, of course, is because the families were established when the message was enciphered in period-7 and, once they have been established, any other periodic separation of these same elements will only serve to mix them up in such a manner that the resulting families will be of diminished individuality.

It is to measure the degree of dissimilarity of probable groups of different length that the Chi-square Test is employed. When that has been done, the periodic length for which this difference is shown to be the greatest, is selected as the correct period.

To perform the Chi-square Test, the cipher message must be separated into the various periods which are to be tested. For each period the number of appearances in the Row family of each letter is tallied and, below that, the number of appearances in the Column family. As it applies to finding the period of a Bifid the calculation for the Chi-square test is: D^2/S in which:

'S' - equals the sum of the appearances in both the Row and Column families of any letter.

'D' - equals the difference between the family appearances of any letter.

When D^2/S has been calculated for the entire alphabet, these values are added and their sum equals Chi-square, or the degree of dissimilarity between the probable Row and Column families for that period. The mathematics of all this is very simple and can be done mentally as will be shown.

The message to be tested for period is:

S S I N C F D T S I N N V O D H C E L D E N D M V

N C C S O T E V D L A P N R S N S C I G Q O L I A

W V H E T N S N B H C G S B S S M K Q T S A D Q L

M B K T T V L A N M N S H S R M E N T V C T.

Inspection fails to disclose any repeats which might tend to show the period. Consequently, the Chi-square Test will be applied in periods 5 - 7 - 9 and 11. The test in Period-7 will serve to demonstrate the method. The message is copied, the letters tallied, and the calculations are made as shown below.

S S I (N) C F D | T S I (N) N V O | D H C (E) L D E | N D M (V) N C C

S O T (E) V D L | A P N (R) S N S | C I G (Q) O L I | A W V (H) E T N

S N B (H) C G S | B S S (M) K Q T | S A D (Q) L M B | K T T (V) L A N

M N S (H) S R M | ~~E N T V C T~~

Tally and D/S calculations.

	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
Row	3	2	2	3	0	0	1	1	3	1	0	2	4	1	1	0	0	9	4	0	1	1	0	0	0	
Col.	1	1	4	3	2	1	1	0	1	1	5	2	5	2	0	1	1	4	2	0	2	0	0	0	0	Total
D/S	1	0.7		2		0		1		5		0.1		1		1		0.7		0.3		0		0		Chi-sq.
		0.3		0		1		1		0		0		0.3		1		2		0		1		0		19.4

After the tally has been made the D^2/S calculations can be performed mentally in this way.

A - Sum 4; difference 2; 2 squared is 4; 4 divided by 4 is 1.

(The value of 'I', the same, can also be written in.)

B - Sum 3; difference 1; 1 squared is 1; 1 divided by 3 is 0.3 (The value of 'O' and 'V' can also be written in.)

C - Sum 6; difference 2; 2 squared is 4; 4 divided by 6 is 0.7

D - Sum 6; difference 0; 0 squared is 0; 0 divided by 6 is 0 .

E - Sum 2; difference 2; 2 squared is 4; 4 divided by 2 is 2 .

And a few others at random:

L - Sum 5; diff. 5; 5 squared is 25; 25 divided by 5 is 5 .

N - Sum 9; diff. 1; 1 squared is 1; 1 divided by 9 is 0.1 .

S - Sum 13; diff. 5; 5 squared is 25; 25 divided by 13 is 2 .

Note that some of the D^2/S values are automatic, such as:

(a) When the same number of appearances occur in both families, the D^2/S value is zero. See D-G-M.

(b) When one family has no appearances, the D^2/S value is the number of appearances in the other. See E-F-H-L etc.

(c) When a D^2/S value has been calculated it may be written in for all other letters having the same characteristics.

Chi-square, for all periods to be tested, is calculated in the same way. The results are:

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

The message starts with the plaintext word 'statisticians'. Select the correct period and solve it. The word given should be enough to get the solver well started, but, if he gets stuck, he can try 'Chi-square Test' along towards the end of the cipher.

SOLVING THE BIFID WITH THE THREE SQUARE TECHNIQUE.

The Three Square process must not ever be considered to be a sorcerer's wand which, automatically, will solve a Bifid. It merely gathers the known equivalents into concise form and calls attention to probable equivalents, some of which might otherwise be overlooked.

The work of solution follows the same general plan as was outlined for solving with numerical indices. The first step is the determination of the period. When that is accomplished, by inspection or the Chi-square Test, the cipher letters are set up in fractionated form in the correct period. It is not necessary to leave open spaces between the groups as vertical lines, drawn

between them, serve just as well as dividers and, also, allow the plaintext to be written continuously. This last mentioned circumstance is of particular advantage when attempting to spot a probable word.

It has been found that it is of some help to make a digraphic frequency count of the vertical pairs. This should be made in two tables - one for the R-C pairs and the other for the C-R pairs. Perhaps not a great deal will be learned from a frequency count, but it at least serves to familiarize the solver with the message and to call attention to all repeats, which should be underscored.

Solution of the following message will be given, step by step, with the exception of a frequency count.

THE MASTER SPY CIPHER.

Concerning espionage, and the man who was Hitler's Chief of Intelligence during World War II.

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

Inspection of the message reveals a repeat in the form of A B . . . C D. This is the pattern of a 5-letter repeat at the odd position 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 letter #75.

55 divided by 9 equals 6 plus 1
75 divided by 9 equals 8 plus 3

Hence, in period-9, the first appearance of the repeat will start in group-7, position 1; and the second appearance will start in group-9, position 5.

These locations for the repeated cipher letters are most satisfactory and the message will be set up in period-9.

The Master Spy Cipher - Fractionated - Period 9.

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
										e				
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
t									t					
H	K	V	D	Z	I	I								
Z	P	X	T	F	I	Z								
					i									

The presence of four high frequency naturals (E-T-T-I) and the fact that not any low frequency letters show up as naturals, tends to confirm the period selection.

Assuming, with a fair degree of assurance, that the correct period has been determined, solution of this secret message can now begin and it is at this point that some of General Sacco's "interviene qualche altro ausilio" would, most certainly, be welcomed. However, as none has been provided in the form of a given word (such a clue is frequently furnished in amateur cryptography) the solver has to do what he can with the material at hand.

This is not much, but there is one thing of which the solver can be reasonably certain. That is that the repeat, by means of which the period was determined, showed the pattern produced by a five letter plaintext repetition.

Therefore:

K	L	V	and	K	L	O
D	E	A		P	E	A

represent the same five plaintext letters and, such being the case, this makes 'D' and 'P' co-column and 'V' and 'O' co-row.

D				
P				
	V	O		

From this information the recovery of the square may be started. The letters can be placed as shown on the left. This is not much of a start but it may prove to be of major value, as a control, when probable words are being tested.

As the next step, a diagraphic frequency count may disclose a sufficient number of high frequency cipher pairs to give a clue. Or, probable position of certain letters may indicate that they are in the same row or column with other letters. However, to quote General Sacco once more, this is hardly possible in a short individual message such as the above.

The best bet for making an entry is the probable word, and probable words are available because something is known about the subject matter of the message. It was stated that this message relates to: "Espionage, and the man who was Hitler's chief of intelligence during World War II."

It is highly probable that one or all of these words might be expected to occur in the message, together with numerous others that are suggested by this knowledge of the subject matter. Now, if one knew the name of Hitler's Chief of Intelligence, that would provide an almost certain entry. Assuming that the solver does not know that gentleman's name, other suggested words are: Espionage, Hitler, Intelligence, World War, Security, Germany, and any others that one can think of.

An attempt must be made to spot one or more of these words in the cipher message. This can best be done by writing the word to be tested at the edge of a piece of ruled paper so that the letters will be spaced exactly the same as those of the cipher. The test word is then shifted along under the cipher, in its fractionated set-up, and coincidence between plaintext and cipher letters is looked for.

Of the probable words to be tested, 'intelligence' will be tried first because it is the longest and, consequently, if found to be present in the message, will give more letters to work with. Coincidence of letters may be tallied as shown below.

	Group-3					Group-4				
Cipher	A L	H T	I N	A I	L B	L Q	V A	Y T	E P	Q T
Probable Word			i	n	t e l	l	i	g e n	c e	
Location (3 - 5)			x		x	x			x	

The following tabulation shows the results of the complete test for 'intelligence'. The location numerals indicate the group and position in the group, of the initial letter of the word which is being tested. Coincidence is marked with an 'x'.

	I	N	T	E	L	L	I	G	E	N	C	E
3 - 5	x				x	x						x
6 - 1			x				x					x
6 - 7	x					x				x		
18 - 3	x		x		x		x					

The possible locations of 'intelligence' are now tested to see if the letters will fit into the square without conflict.

Location 3 - 5

I	A	L	L	V	Y	E
N	I	B	Q	A	T	P
i	n	t e l	l	i	g e n	c e

When these letters are put into the square a conflict will occur almost immediately between 'I' and 'N'.

Location 6 - 1

H	I	V	I	R	K	L
R	T	D	Z	K	D	E
i	n	t	e	l	l	i	g	e	n	c	e

With the shift of 'D' to N-column in Basic, the resulting shift of 'Z' in Top to the vertical row of 'T' will cause a conflict when 'Z' is moved to T-row in Basic.

Intel. 6-1

				Z							
				T	D	Z	K	E			
			H	N	K						
			I		E		G			R	
			V	L		Z					V
			K					C			
									H	I	T
										K	
				D		D					
										Z	
					K						

The test of 'intelligence' at Location 6 - 7 proves that location to be impossible also, as six letters are forced into one column in the early stages of the test.

Location 18 - 3

F	T	L	R	H	K	V
I	W	Y	I	Z	P	X
i	n	t	e	l	l	i	g	e	n	c	e

This shows no conflicts but the letters, after being condensed as much as possible are still badly scattered. Very few additional plaintext letters are recovered when this arrangement is tried with the entire message. Consequently, it will be tabled for the time being while other tests are made.

Intel. 18-3

			F										
			R										
			I	K	P	V							
			L	N	Y	E				W	C		X
	Y	L	L	F				I	R				
	X	E	Y							P			
W	H	T			E						V		
	P	N				W							
		F								N	K		
		C			X								
		K										C	
						T							
						H							G
													Z

The word 'espionage' is tested next and the tally shows the following possible locations in the plaintext.

	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					x
10 - 9		x				x			
12 - 1	x								x
12 - 9	x			x					

Of the above, the one starting at (9 - 3) will be diagrammed first because it includes the sequence of five letters which are repeated in the message. If this test shows no conflicts, then it is possible that both appearances of the repeated five letter sequence are fragments of the longer word, 'espionage'. If this should prove to be the case, then the number of new values which can be recovered will practically be doubled.

Location 9 - 3

Z	K	L	O	R	F	
E	P	E	A	V	H	
e	s	p	i	o	n a	g e

Location 6 - 8

I	R	K	L	V	N	
Z	K	D	E	A	S	
	e s	p	i	o	n a	g e

Esp. 9-3

						L							
				K	Z	O							
				P	E	A	H	S	I		N		
			Z	S									
			K		I								
			L			N							
		I	R				E	Z					
			S						K	P			
			N				O				L	A	
					R								G
													V
		E	O											H

Esp. 6-8

				P									
				I	N	V	R						
				K	E	A	S				G		
		L	I	E		N							
E	S	O	K	K	I					P			
			V				G						
			G	S					R				
										D			
				O	L								
			N								V	A	

No conflict occurs in either of the above tests and so the next step is to check them against each other by attempting to combine them into one Three Square diagram if possible. This is done and it is found that they will combine as shown below.

Espionage 9-3 6-8

					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									

The fact that the two tests combine without conflict is particularly encouraging and this arrangement can now be tested with the message to see if any acceptable plaintext fragments will be developed.

For a clearer understanding of what is being done, the reader should have a work sheet on which the fractionated message has been set up. On this, he should now enter all of the plaintext letters thus far recovered.

When this is done the validity of this arrangement is immediately strengthened. The majority of the letters recovered are of high or medium frequency and, where they are grouped, a great many excellent plaintext fragments hold forth promise of further development. This can start with the plaintext letters that now show in groups #1 and #2.

	Group-1					Group-2		
	F	R	I	E	N	V	F	D
	N	I	L	O	S	A	E	M
Plaintext Recovered:		r	n	i	n e	e	a r	
Plaintext Suggested:	f o				y		s	

And further along, down near the end of the message:

	Group-17			Group-18		
	T	K	T	L	F	T
	S	B	T	R	I	W
Plaintext Recovered:			t	l e		
Plaintext Suggested:		H i			r	

These suggested plaintext letters derive from two sources.

First - They make acceptable plaintext.

Second - Continual reference to the Three Square arrangement shows them to be possible, without conflict, and highly probable because of agreement with letters previously placed. Note that a glance at the Three Square shows that the placing of letter 'F' in N-column will not only give 'F' as the first letter, but also O as the second. Had 'I' been located elsewhere in the Top Square, so that $F_C I_R$ would have resulted in 'V' or 'L' instead of 'O' as the second plaintext letter, then it would have been immediately apparent that 'F' should not be the first letter.

Accepting, as correct, these new values recovered from the above shown extension of the plaintext fragments, they are added to the Three Square diagram, giving this.

					Y									
					H	T	F	L						
					P	E	R	O						
					I	Z	S	V						
					K	N	G	A				D		B
		R	L	I	E		Z	N					T	
			F	N	O	L	V			A				
	Y	V	Z	G	S	R	G	F						
	E	S	O	K	K	I	Y				P	H		
											D			
			P	D										
				H										
				A										
												B		
				T										

And now, with this much of the square recovered, there are numerous additional plaintext letters which can be placed on the work sheet. Many new fragments and even what appear to be some short words, are developed. Suggested plaintext begins to pyramid and a favorable spot to take advantage of this is at the long run through Groups 10, 11 and 12.

	Group-10					Group-11					Group-12		
	R	F	S	I	V	Z	R	K	R	S	E	O	N
	V	H	I	L	T	S	E	N	T	W	E	N	C
Plaintext:			o r	i	l	e r s			i		e i		
Suggested:		f		H	t			t h	r	d r		c	h
		*		*	-			- *	-			*	*

Letters marked '*' result from moving 'H' to the 4th.column.
Letters marked '-' result from movint 'T' to the 2nd.column.

Placing these letters in the square gives this:

The remainder of the message can now be read without difficulty and the few cells of the square, still vacant, can readily be filled in. When this is accomplished the Three Squares present the appearance shown below. The entire message has now been deciphered but one thing still remains to be done before the job is finished. The Basic Square should be rearranged so that the rows and columns are in their correct position with relation to the diagonal.

Master Spy

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

Master Spy

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

The letters which stand on the diagonal are easily recognized as they are the Basic Square letters which are repeated in the Left Square in the same long row, and in the Top Square in the same long column. These are circled in the diagram for identification.

These letters of the diagonal play an important part in the Three Square method of dealing with the Bifid. They can be shifted to different positions along the diagonal of the Basic Square, but they cannot be moved away from it. The Basic Square, as recovered, and rearranged with relation to the diagonal, is shown below. This form of the true square can now again be rearranged by those familiar with the technique of keyword recovery. Always keeping the same five letters on the diagonal, the rows and columns are shifted around until they fall into position, with relation to each other, as shown on the right.

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

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

This scrambled square is the original true square which was formed by a vertical take-off of the letters from this block.

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 EVEN PERIOD BIFID.

When the Bifid is enciphered in even period length, resulting messages are considered by some authorities to be less secure than is the case with the odd period. This is because a great deal of the plaintext shows through in the form of 'identicals'. It is a well established fact that many 'identicals' occur, and that some of them are readily recognizable as such if the solver has some idea of the subject matter of the message, on which he can base a selection of probable words. But, when such helpful information is not available, then solution of the Even Period Bifid can well be extremely difficult and the statement that the type is easier to solve becomes highly debatable.

With the Even Period Bifid, the encipherment process follows the same principle as described for the odd period, that is, the first cipher letter of each group results from the combination of Row-Row components of the first two plaintext letters, etc. But, due to the fact that an even number of letters compose each group, a different situation exists when the cipher message is set up for decipherment. Decipherment is always concerned with 'double pairs', formed from Row-Row and Column-Column combinations of two letters. The entire cycle is illustrated below. (ENTHUSIASM square used.)

Encipherment							Decipherment						
Plain:	s	o	l	v	e	d	Cipher:	M_R	M_C	R_R	R_C	T_R	T_C
								N_R	N_C	E_R	E_C	N_R	N_C
Cipher:	M	R	T	N	E	N	Plain:	s	o	l	v	e	d

The above shows how, and why, the fractionated cipher letters automatically fall into position as double pairs of the same two letters. This characteristic of the even period Bifid then serves to generate certain peculiarities which are different from those of the odd period type.

PECULIARITIES OF THE EVEN PERIOD BIFID.

1 - 'Naturals', formed from Row-Column combinations of the same cipher letters, do not exist when the period is even.

2 - 'Half naturals', as defined for Bifids of odd period, do not exist when the period is even because there are no Row-Column combinations of the fractionated cipher letters.

3 - 'Identicals', wherein a double pair of fractionated cipher letters represent the same two plaintext letters, frequently occur when the period is even. Example: (ENTHUSIASM square)

Encipherment							Decipherment						
Plain:	s	h	r	i	m	p	Cipher:	S_R	S_C	O_R	O_C	M_R	M_C
								H_R	H_C	W_R	W_C	P_R	P_C
Cipher:	S	O	M	H	W	P	Plain:	s	h	r	i	m	p

An 'identical', so named because a plaintext pair reproduces

itself in the cipher, occurs when the first letter of the plaintext pair is in the column having the same numerical index as the row of the second letter of that pair. In the example, 'S' is in the column (1) of H-row (1); 'M' is in the column (4) of P-row (4).

Reverting to numerical indices for greater clarity:

Encipherment

Plain:	s	h	r	i	m	p
	2	1	4	2	2	4
	1	4	5	2	4	3
Cipher:	S	O	M	H	W	P

Decipherment

Cipher:	S_R	S_C	O_R	O_C	M_R	M_C
	H_R	H_C	W_R	W_C	P_R	P_C
	2	1	4	2	2	4
	1	4	5	2	4	3
Plain:	s	h	r	i	m	p

The probability, that any given cipher pair is an identical, is high. Disregarding the plaintext frequency of the letters involved, any cipher pair has a 5 in 25 (20 percent) chance of reproducing its plaintext equivalent. This fact can readily be demonstrated without recourse to mathematics.

Assume 'S' to be the first letter of a plaintext pair. Reference to the ENTHUSIASM square shows that 'S' is in the first column. Then, whenever the second letter of the pair comes from the first row of the square, an identical will result. The combinations wherein this will happen are with E, N, T, H, U.

Cipher:	S_R	S_C	S_R	S_C	S_R	S_C	S_R	S_C	S_R	S_C
	E_R	E_C	N_R	N_C	T_R	T_C	H_R	H_C	U_R	U_C
Plaintext:	s	e	s	n	s	t	s	h	s	u

When 'S', as first letter, combines with any one of the other twenty letters of the square, the resulting cipher double pair will not be the same as the plaintext pair it represents.

4 - 'Semi-identicals', wherein one of the letters of a plaintext pair reproduces itself in the cipher, will occur only when the letter, thus reproduced, is on the true diagonal of the square. There are two cases which will cause this result.

First - In encipherment, when the first letter of a plaintext pair is on the diagonal and the second letter is co-column, then the cipher letter derived from the plaintext column components will be the same as the first plaintext letter.

Example:	Plaintext:	F	A	R	M	E	R
	Cipher:	D	O	H	F	Y	U

In decipherment, this semi-identical will be found under the Row-Row combination of the fractionated cipher letters.

Cipher:	D_R	D_C	O_R	O_C	H_R	H_C
	F_R	F_C	Y_R	Y_C	U_R	U_C
Plaintext:	f	a	r	m	e	r

Second - In encipherment, when the second letter of a plaintext pair is on the diagonal and the first letter is co-row,

then the cipher letter derived from the plaintext row components will be the same as the second plaintext letter.

Example:	Plaintext:	H	E	R	O	I	C
	Cipher:	E	Q	A	L	W	S

In decipherment, this semi-identical is found under the Column-Column combination of the fractionated cipher letters.

Cipher:	E_R	E_C	Q_R	Q_C	A_R	A_C
	L_R	L_C	W_R	W_C	S_R	S_C
Plaintext:	h	e	r	o	i	c

The probability of semi-identicals is low, except in cases when vowels or high frequency consonants happen to be on the diagonal. Disregarding the plaintext frequency of any given letter, its chance of being a semi-identical is 1/5 X 1/6 = 1/30, or 3.3%.

It should be noted that, in both cases, the semi-identical subscript is always a Left or Top Square value, and never a true Basic Square column or row indicator. This is shown in the above examples where:

First Case:
D row (Basic), F row as column (Top), equals plaintext 'F'.

Second Case:
E Column as row (Left), L column (Basic), equals plain 'E'.

5 - When two plaintext letters, both of which are on the diagonal, are enciphered as a pair, the resulting cipher double pair will be a single letter repeated, as 'T' and 'T' below.

Example:	Plaintext:	E	F	F	O	R	T
	Cipher:	T	G	L	T	D	X

When set up for decipherment, this shows:

Cipher:	T_R	T_C	G_R	G_C	L_R	L_C
	T_R	T_C	D_R	D_C	X_R	X_C
Plaintext:	e	f	f	o	r	t

The letters 'E' and 'F' are both on the true diagonal of the ENTHUSIASM square and give 'TT' as a cipher double pair.

6 - The letters of any double pair of fractionated cipher letters reverse with the letters of the plaintext pair they represent. This condition can be illustrated with a double pair of cipher letters from those used in the example for Second Case, above.

First Situation.

Cipher:	A_R	A_C
	S_R	S_C
Plaintext:	i	c

Second Situation.

Cipher:	I_R	I_C
	C_R	C_C
Plaintext:	a	s

Hence, if double cipher pair 'AS' equals plaintext pair 'ic', then the double cipher pair 'IC' equals plaintext 'as'.

FINDING THE PERIOD OF THE EVEN PERIOD BIFID.

When the plaintext contains sequences of 2, 4, 6, or any even number of letters, repeated in step, then the resulting pattern in the cipher message reveals the period. To find it, the interval between the initial letters of the two parts of the pattern is determined. This interval, multiplied by 2, is the period.

Patterns in the cipher message take this form:

Length of Sequence	Period-6	Period-8	Period-10
2	A . . D . .	A . . . D . . .	A . . . . D . . . .
4	A B . D E .	A B . . D E . .	A B . . . D E . . .
6	A B C D E F	A B C . D E F .	A B C . . D E F . .
Interval	←3→	←4→	←5→

The above illustration shows the repeats starting with the first letter of the group, but it is to be understood that they can start with any letter that will allow the repeat pattern to be contained within the limits of a group. Hence, 4-letter repeats for example, could take the following positions in a group for the various periods shown.

Period-6	Period-8	Period-10
A B . D C .	A B . . D C . .	A B . . . D C . . .
. A B . D C	. A B . . D C .	. A B . . . D C . .
	. . A B . . D C	. . A B . . . D C .
		. . . A B . . . D C

In all cases, the interval between 'A' and 'D' is half the period length and the number of repeated letters is equal to the length of the plaintext sequence in a single group.

If a repeated sequence extends beyond the limits of a single group, those letters which are in the second group will form their own pattern

The Chi-square Test will also work on the Even Period Bifid but this test should be restricted to even period length against even period length; and odd period length against other odd period lengths. When even period length is tested against odd, it will usually be found that one even and one odd will give approximately the same result. The message shown on page 22, when tested for both odd and even period, gives the following values.

For message enciphered in Period-9.

Period:	5	6	7	8	9	10	11
Chi-square:	19.2	17.4	19.4	28.1	28.0	20.4	12.0

From the preceding tabulation it is seen that the period cannot be definitely determined, as Chi-square for period-8 and period-9 is almost exactly the same.

For this same message enciphered in Period-8.

Period:	6	7	8	9	10
Chi-square:	20.7	26.3	26.4	17.3	13.9

From the above it is evident that when the solver does not know whether a message has been enciphered in odd or even period, the true period length cannot, absolutely, be determined by Chi-square. However, it can be reduced to a choice between single period lengths of each type. Each of these must then be tested by other methods until the correct period is found.

If such a message is set up in the odd period, indicated by the Chi-square test, and low frequency plaintext letters appear as naturals; then this would indicate that the wrong period is used. If high frequency naturals appear, it would tend to confirm the choice of the odd period length. Digraphic repetitions will also aid in making this determination.

SOLUTION OF THE EVEN PERIOD BIFID.

As was previously stated, when the Bifid is enciphered in an even period, it is supposed to be less difficult to solve than is the case with the odd period type. This opinion is based on the fact that many identicals appear. It is certainly a fact that identicals are of great assistance to the solver when they can be spotted as such. However, when little or nothing is known of the subject matter of a message, definite recognition of identicals is not easy - and neither is the solution.

This fact was admirably demonstrated in an article on the Even Period Bifid which appeared The Cryptogram, Oct.-Nov., 1952. The example for solution, which accompanied this article, is reproduced below. It was introduced with these words.

> "The following 'Special' is appended for the benefit of those ACA members who desire to try their skill in adapting the authors' method. It is suggested that solution be first attempted without recourse to the Caesarized tips: C-------- and B------- "

(Note: The given Caesarized tips are omitted for the moment.)

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

From inspection, the period of this message is easily determined to be 10 and, when it is set up in that period, the cipher double pair 'HE' is repeated sufficiently to establish it, with almost certainty, as an identical. Also, cipher 'V', which twice precedes 'HE', can be assumed to represent plaintext 't'. This gives one an excellent start but, after this, where does one go? Actually, there is no place to go - except in search of probable words.

In this message there are a number of possibilities that various cipher double pairs are identicals, representing fragments of plaintext, but, as the solver knows nothing concerning the subject matter he is at a distinct disadvantage, in that he never knows whether or not he is on the right track. Here are a few examples of possible plaintext based on possible identicals.

Letters 41 to 50

Cipher:	U	U	E	E	L	L	E	E	G	G
	M	M	P	P	E	E	G	G	B	B
Possible		d	e	p	l	e	t	i	o	n
Words:	t	h	e	p	l	e	a	s	u	r e

Letters 74 to 88

Cipher:	K	K	T	T	N	N	Q	Q	W	W					
	Y	Y	I	I	C	C	G	G	V	V					
Possible			t	i	n	c	u	p							
Words:			t	i	n	c	t	u	r	e					

Letters 61 to 70

Cipher:	Q	Q	A	A	R	R	C	C	D	D
	M	M	P	P	A	A	T	T	W	W
Possible										
Words:	s	u	b	t	r	a	c	t		
	a	b	s	t	r	a	c	t		
				t	r	a	c	t	o	r
				p	r	a	c	t	i	c e
				f	r	a	c	t	i	o n

Letters 131 to 140

Cipher:	M	M	E	E	R	R	W	W	E	E
	Y	Y	A	A	T	T	A	A	F	F
Possible			e	a	r	t	h			
Words:		h	e	a	r	t				
		y	e	a	r	t	h	a	t	
		h	e	a	r	t	h	i	s	
		n	e	a	r	t	o			
	t	h	e	a	r	t	s			

Any or all of these and other words, that might be considered probable, can be tested - but it is a tedious and discouraging task. The solver has no assurance that his work will ever yield positive results and, consequently, the incentive to continue to 'cut and try' is slight. In most cases he will quickly resort to the Caesarized clues in order that he may have something definite to work from.

In this particular example the solver is confronted with a difficult and time consuming problem as it now stands. The entire picture changes if advantage is taken of the information available from the given Caesarized clues, which are long plaintext words easily spotted in the message. The point which the writer is attempting to emphasize is that when one had this king-sized tip to start with, this message ceased to be a problem for solution, and became merely an exercize in the mechanics of decipherment.

The great majority of qualified amateur cryptanalysts would have arrived at a solution of this example with almost equal ease but with a far greater sense of accomplishment if, in place of being furnished with these given words, (CENPGVPNY and BYULNQUM) an explanatory sentence had accompanied this message, given as an example with which to try out explained methods.

Something like the following would have been adequate.

> Concerning the traits and characteristics of an immortal President of the United States who kept intact the nation founded by our forefathers.

From the above, the solver logically assumes that the message concerns Abraham Lincoln. With this, probable, rather than known plaintext is available to work with and solution proceeds without the benefit of given words.

When background information is supplied but actual plaintext is not given 'for free', one has to employ logical assumptions in order to create an entry and to continue with the solution of an Even Period Bifid. The following example was constructed to demonstrate some of the lines of reasoning necessary in order to get started. Attention is also called to some of the characteristics of the system which will aid the solver and - opposed to this - the fact that recovered letters seem to resist being condensed into the limits of the 5 X 5 square.

SOLUTION DEMONSTRATION EXAMPLE - EVEN PERIOD BIFID.

Concerning the encipherment of the Bifid types.

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

Inspection of the message will reveal two repeated patterns.

```
Starting at letter 25:   L Z Z E Q Z I

Starting at letter 74:   L Z Z O Q Z I

                Interval:  |-- 4 --|

Starting at letter 35:   N N P N G U M E E O U

Starting at letter 59:   N N R I G U M T N M U

                Interval:  |-- 4 --|   |-- 4 --|
```

The second of these repeated patterns indicates that the repeated plaintext sequence carries over into the next group. The interval between the initial letters of the two parts of the pattern is, in all cases, four. This determines the period as 8 and the message can now be set up in that period for solution.

In setting up an Even Period Bifid a slightly different arrangement from that used for the odd period, is recommended.

When all fractionated cipher letters are written in, one has this set-up

$$\begin{array}{cccccccc} A_R & A_C & B_R & B_C & C_R & C_C & D_R & D_C \\ \hline W_R & W_C & X_R & X_C & Y_R & Y_C & Z_R & Z_C \end{array}$$

This can be streamlined, similar to the 'hit-skip' method used for odd.

$$\begin{array}{cccc} A & B & C & D \\ W & X & Y & Z \\ \hline \end{array}$$

In the streamlined diagram, all double pairs are indicated although only the true row and column component of each cipher pair is shown. Being familiar with the handling of the set-up for the odd period, one readily reads the first pair as A_R/X_R and the second pair as A_c/X_c. The other pairs, throughout the entire message, are Row-Row and Column-Column combinations.

Employing this method, the message is set up in period-8.

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

The selection of 8 is confirmed, as the correct period, when it is observed that the cipher letters of the two repeated patterns have fallen into place, in such a way, as to indicate the expected plaintext repeats. It is also noted that an additional double pair of cipher letters - VO - has been added to the twice occurring L Z Z - Q Z I.

Since something is known of the subject matter of the message the first step is a search for probable words which may show in the form of identicals. Group #2 immediately attracts attention as cipher 'PHER' could well be a fragment of plaintext words such as 'cryptographer' or 'cipher'. Like this:

Y	S	Z	L	E	D	P	E								
G	S	W	K	N	Y	H	R								
	c	r	y	p	t	o	g	r	a	p	h	e	r		
						c	i	p	h	e	r				

'Cryptographer' is tested first and is quickly eliminated because of conflicts in the square.

'Cipher' is tested next with better results and shows the following arrangement in the Three Square.

cipher 2-3												
									C			
			I	Y		H		R		D	P	E
			D	C								
		D			I							
		C			Y							
						P						
		P					H					
								E				
		E							R			
	I	Y										
		H										
		R										

All of these letters fit into the square without conflicts, but the letters are so scattered that no additional plaintext can immediately be recovered by means of the letters thus placed. So the solver goes back to the message and, on further examination, it is noted that the double pair, VO, repeats four times. On three of these appearances, 'VO' is followed by 'L' which is twice combined with 'Q' and once with 'R'. It is highly probable that 'VO' is plaintext 'th' and that 'L' represents plain 'e'.

Reference to the Three Square diagram set up to test the word 'cipher', shows that the cipher double pairs VO LQ and LR can be deciphered as plain 'the' without conflict. It is also found that in the case of VO LR, the letter 'R' has already been placed in the Top Square so that it can represent plaintext 'e'. If these values are added to those based on the test of 'cipher', then the square assumes this appearance.

cipher														
2-3							Q		C		L			T
the			I	Y		H	R		D	P	E	O		V
			D	C										
		D			I									
		C			Y									
						P								
	V	P					H							
								E					L	
		E							R						Q
	I	Y												
	O	H												
		R												
						V						T		
		T					O							
		L												
		Q												

Assuming all of this to be correct, and thus far none of it has been found to be in error, the letters are still so scattered that they are of little or no help in suggesting other plaintext fragments.

However, one additional probability is observed from the square as now set up. The fact reveals itself that some of the letters which have been placed are beginning to shape up as though the original square might have contained a standard (not scrambled) keyword alphabet. This idea is engendered by the co-row location of several sets of letters in alphabetical continuity. A glance at the above diagram shows this to be the situation with 'CD', 'QR' and 'T-V'.

Taking these letters, together with 'P' which is in the same column with 'V', the following row arrangements are possible.

With Short Keyword.

1								
2							C	D
3								
4				P	Q	R		
5		T		V				

With Long Keyword.

1								
2								
3	C	D						
4					P	Q	R	
5			T		V			

In the above elongated squares the only liberty that has been taken with the previously established location of these letters is the placing of 'P' in row with 'Q' and 'R'.

Having proceded this far, and still assuming that all is correct, it becomes more and more apparent that much yet remains to be done. The letters thus far placed are widely scattered and as no additional plaintext suggests itself, the search for probable words is again resumed.

When searching for probable words in the Even Period Bifid, one must keep in mind the peculiarities of the system. One looks first for identicals and, if none can be identified as such, then other even period characteristics must be considered. As true half naturals do not exist, one does not look for coincidence of individual letters, but for patterns, which are always possible when plaintext letters repeat at even intervals.

For an illustration of this, refer once more to the ENTHUSIASM square and, using it, check the encipherment of the word 'rarity'.

Plaintext:	R A R I T Y	Cipher:	O O U
			X W G
Cipher:	O O U X W G	Plaintext:	r a r i t y

Now, inspect a message enciphered from that square.

M	R	R	S	N	H	H	W	N	T	I	N	O	O	U
E	I	H	Z	C	Z	E	O	K	E	G	T	X	W	G
	r	a	r	i	t	y						r	a	r	i	t	y
	*		*									*		*			
	Impossible											Possible					

From this it is seen and understood that, in the search for probable words, coincidence must be avoided except when identicals are presumed to be present.

With this thought fresh in mind, one returns to the message and gives serious consideration to what probable words might be expected to be in it. The title stated that the message concerns "Encipherment of the Bifid Types." It is believed that plaintext 'cipher' has been spotted correctly and this word may, eventually, be expanded to become 'encipher', 'decipher', or some other word of similar combining form.

No attempt has as yet been made to spot the plaintext word, 'bifid', which is almost certain to be present. To do this, one first looks for possible identicals and one eligible double pair is immediately found in the eighth group. This is:

Cipher:	L		F		N		N	
		R		I		G		U
Possible Plaintext:	b	i	f	i	d			

This location for 'bifid' causes it to lap with one of the repeated sequences but that makes no material difference and it is diagrammed thus:

bifid 8-1						
			I	R		G
			L	B		
	F	L			I	
					R	
			F			
					N	D

This goes into its individual test square without conflict. The next step is to combine this arrangement with that derived from the words 'cipher' and 'the'. This step is then attempted, without success, as it is found that the letters 'B' and 'E' are forced into the same cell of the square. This circumstance does not prove that the selected spotting of plaintext 'bifid' is incorrect. It only proves that, of the three probable words tested - 'cipher', 'the' and 'bifid' - one of them is wrong. As no further progress can be made with the result of this test of 'bifid', it is put on ice for the time being, and another possible location of the word is looked for.

'Bifid' is a pattern word and, if present in the message, it can be in either of two forms, like this:

B I F I D . or . B I F I D

In the first separation, if 'B' and 'F' are co-column, then a pattern of this type would show.

```
 -   -   -
   X   X   -
```

In the second separation, if 'F' and 'D' are co-row, the resulting pattern would be like this.

```
 -   X   X
   -   -   -
```

It has already been established, in this particular message, that there is a good probability that the square contains an unscrambled keyword alphabet. If this is true, then 'D' and 'F' can very well be co-row. From this it naturally follows that, if the word 'bifid' is in the message, there is a chance that it has generated a pattern of the second form shown. Following through on this angle, inspection of the message discloses several such patterns. These are:

Group 3	Groups 4-10	Groups 5-8	Group 6
U V V	L Z Z	- N N	M E E
N O O	Q Z I	- G U	U X N
b i f i d	b i f i d	b i f i d	b i f i d

The first of the above is at once eliminated because cipher double pair 'VO' cannot represent both plain 'if' and 'id'.

The second, which appears in groups 4 and 10, is next tested.

bifid 4-2 10-4							
			I	D			
			Z	F	B	Q	L
		L	B				
			Q				
	I	D		I	Z		
	F	Z		D	F		
						L	
	B	Q					

This goes into its individual test square without conflict and so the test is continued to determine whether or not this arrangement will successfully combine with the test square based on the assumed location of the probable words 'cipher' and 'the'. When all values are collected in one square it is found that they will combine without conflict as shown in the diagram below.

cipher 2-3 the bifid 4-2 10-4															
								C							
						I		D						Q	
					Y	Z		F			O	H		R	B
				C		Y									
		Y	I	D		I		Z							
			F	Z	C	D		F							
				E									Q	R	
											T	V			
												P			
				L									B		
														E	L
			V	P											
				T											

From the individual test of 'bifid' in this location it is seen that if and 'F' are on the true diagonal of the original square if this spotting of the word is correct. For that reason they are now placed there and the other letters are arranged in alphabetical order, in so far as possible, with the hope that some light may be thrown on the manner in which the entire alphabet was arranged in the original square.

This move immediately bears fruit. It indicates that 'Z' is certainly in the keyword and that 'Y' probably is also. That being the case, then if 'V' is in row-5, it can be no further to the left than cell-3. It is placed there and, when this is done, the letter 'P' can then be placed in cell-3 of row-4 with a reasonable degree of certainty that it is located correctly.

The validity of these shifts is supported by the fact that the placement of 'V' and 'P' also moves 'H' to the 3rd row with CDF.

Acting on these suggested shifts, the square can again be rearranged in a more compact form, and 'W' and 'X' can be added as they are required in order to fill out the 5th row.

								H		T			
								C	P	V			
						I	D	Q	W				E
					Y	Z	F	R	X		O	B	L
				C		Y							
		Y	I	D		I	Z						
	V	P	F	E	C	D	F			H			
	Q	W	B	E			P	Q	R				
			R	X			V	W	X		T		
				L				B					
								E				L	
				T						O			
			O	H									

A study of the square as it is now set up suggests that even more shifts could logically be made. The letters 'B' and 'E' have been established in column-4, but their correct row location has not yet been determined. It is now evident that neither 'B' nor 'E' can go into the 3rd row, as such a location for either of them would disrupt the alphabetical continuity of those letters already placed and which apparently are beyond the keyword. Nor does 'B' fit well into the 2nd row. In that position it is not considered satisfactory as a letter of the keyword and, if it is not in the keyword, then it must be in the fifth cell of the 2nd row in order to be in alphabetical sequence with 'C', which has been placed in cell-1 of the 3rd row. Consequently, it would seem that 'B' must go into the 1st row.

With 'B' thus placed, 'E' would automatically be forced into the 2nd row as it has no place else to go.

All of the foregoing derives from logical reasoning but further rearrangement can be delayed until the square, as it is now set up, is tested with the entire message to see if any additional plaintext fragments can be recovered.

Y	S	Z	L	E	D	P	E	Z	U	V	V	L	Z	Z	E
G	S	W	K	N	Y	H	R	N	N	O	O	Q	Z	I	I
				c	i	p	h	e	r		t	h	t	h	e	b	i	f	i	d

A	E	N	N	M	E	E	O	W	I	N	V	L	F	N	N
P	N	G	U	U	X	N	T	I	Y	B	O	R	I	G	U
									i		t	h	e	d	d

M	T	N	M	V	L	Z	Z
U	Y	G	V	O	Q	Z	I
				t	h	e	b	i	f	i	d

When this test is made, it is seen that the only plaintext words which have been completely recovered, thus far, are the few which have been assumed, tested, and found not to be in error. However, it is felt that what has been developed up to this point is correct, because of the orderly manner in which the square has shaped up.

Twelve of the twenty five letters have been definitely placed but they are found to be of little or no assistance in the recovery of additional plaintext. And so, as long as this condition continues to exist, the solver's sole recourse is to make arbitrary placement of letters now outside the 5 X 5 square, or a renewed study of the message for other probable plaintext location.

With the exception of the words -'cipher', 'the', 'bifid'- the only plaintext letters recovered are an extra 'th', a single 'i', and the doubled 'dd'. Examining these unattached plaintext letters, it is noticed that the doubled 'dd' follows plaintext 'the' with one vacant cell intervening. Immediately to the right of 'dd' is the repeat, N/G N/U M/U.

Inspection of the other occurrence of this repeat shows that it is preceded by cipher pairs, E/I A/P E/N.

The complete picture is this:

Starting at 3 - 7:

V		L		Z		Z		E	A	E	N	N	M
	O		Q		Z		I	I	P	N	G	U	U
t	h	e	b	i	f	i	d						

Starting at 7 - 7:

V		L		F		N		N	M
	O		R		I		G	U	U
t	h	e		d	d				

In the above, plaintext 'the' may be assumed to be a complete word. Now, if the repeated sequence represents a complete word, then '-dd' must also be a complete word, and, from what is known of the subject matter of the message, it may be the word 'odd'.

In the other occurrence of the repeat, the cipher double pair which is immediately adjacent on its left is E/N. If this is an identical, it could be part of the plaintext word 'even' and the repeat would then, almost certainly, be the word 'period'.

Reference to the square shows that these values will fit in without conflict. When all are entered, and other obvious placements are made, the square presents this appearance.

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

With the correct spotting of the plaintext word, 'period', practically the entire square is finally recovered. The keyword is seen to be SYMBOLIZE, and the message reads:

"Messages enciphered with the Bifid in even period are not unlike the odd period type of Bifid."

The preceding step by step demonstration shows that the Even Period Bifid can resist solution, even when the solver has advance knowledge of the subject matter of the message. When such information is not available, the Even Period not only resists, - - - - it defies.

The foregoing is not to be considered a true solution of an Even Period Bifid message, as this example was constructed by the writer and the vulnerable points of entry were known in advance. It was used for this demonstration because Even Period examples are few and, of those available, either the entire solution is given away by tips which are too generous, or not sufficient information is furnished for a beginner to make a satisfactory entry.

For that reason an example was constructed which would call attention to the following facts.

1 - The making of assumptions, relative to probable plaintext, must continue until the solution is well underway.

2 - An attempt should be made, as soon as possible, to arrange the letters of the square in true alphabetical order.

3 - Characteristics and peculiarities of the system must be, continually, kept in mind and employed whenever possible.

4 - The structure of the system is digraphic and a digraphic frequency count is helpful.

5 - The manner in which the mechanics of the system differs from that of the Odd Period type must not be overlooked.

THE BIFID WITH CONJUGATED MATRICES.

In the writer's copy of a translation of F. Delastelle's book Traité Elémentaire de Cryptographie, there is a variation of the Bifid which is named and described in these words.

"CONJUGAL BIFID ALPHABETS. To increase secrecy, one may use two bifid alphabets at the same time. The first is employed to change plaintext into cipher and the second is used to change this cipher into another cipher."

"To encipher we must write vertically under each letter its numerical value from Alphabet-1, then extract the numbers horizontally and transfer them into letters using Alphabet-2."

As is always the case in any type of cipher, resistance to solution is greatly increased by super-encipherment. However, the chance of errors creeping into the encipherment of the message, which will tend to garble it, is also increased proportionally.

The Three Square Technique can be applied to the encipherment and decipherment of CM-Bifids. An excellent article describing how this may be done appeared in The Cryptogram, Jan-Feb, 1960.

THE BIFID CONTINUOUS ENCIPHERMENT CYCLE.

An interesting characteristic of the Bifid is the fact that, if encipherment is continued through a sufficient number of stages, the plaintext will eventually reappear.

By this it is meant that if the cipher message is enciphered with the same alphabet square; and the resulting super-enciphered message is, in turn, enciphered; etc., etc.; at some step along the line the original plaintext will appear as the cipher for the preceding assortment of letters.

Using a straight alphabet in the square, several examples of this phenomenon are given below.

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

Period-3

	t	h	e
1 -	R	D	P
2 -	Q	M	U
3 -	S	Q	K
4 -	T	H	E

Period - 4

	t	h	i	s
1 -	R	I	S	S
2 -	R	T	I	N
3 -	T	H	I	S

Period - 5

	t	h	e	i	r
1 -	R	B	T	P	R
2 -	Q	S	R	I	W
3 -	T	R	V	M	R
4 -	T	X	T	F	G
5 -	U	R	I	O	B
6 -	T	H	E	I	R

Period -6

	t	h	e	o	r	y
1 -	R	C	U	S	Y	I
2 -	Q	T	W	H	X	T
3 -	T	W	Y	D	H	O
4 -	U	V	H	R	T	O
5 -	U	I	S	V	M	T
6 -	R	U	O	Y	L	I
7 -	T	P	M	K	T	D
8 -	S	M	Q	U	K	T
9 -	S	T	I	M	E	Y
10 -	T	H	E	O	R	Y

Period - 7

	t	h	e	d	o	g	s
1 -	R	A	M	T	P	T	H
2 -	Q	O	O	G	B	U	S
3 -	S	M	D	Q	T	G	X
4 -	S	D	R	X	I	D	H
5 -	Q	U	F	H	R	O	S
6 -	T	G	S	Q	V	M	S
7 -	R	T	X	T	H	A	H
8 -	T	Y	F	G	S	S	C
9 -	U	G	T	D	Q	H	N
10 -	R	Q	R	P	I	Q	N
11 -	T	S	I	M	B	Y	C
12 -	T	H	E	D	O	G	S

Period - 8

	t	h	e	b	i	f	i	d
1 -	R	A	G	F	S	W	Q	T
2 -	Q	G	U	T	F	F	M	D
3 -	R	T	G	L	B	Y	A	I
4 -	T	H	E	B	I	F	I	D

PERIOD	CYCLE
9	8
10	18
11	6
12	11
13	20

The writer has attempted to adapt this cyclic characteristic of the Bifid to some use as an aid in solution, but thus far has been unsuccessful.

PROBLEMS

1. About lost mines and buried treasure and the prospectors and other old timers of the old frontier who searched for them. Many of the above words are probable. Among them 'buried treasure' can be located within the first twelve groups, although only two half naturals are there to indicate it. Once that is done, a repeat of 'treasure' can be spotted through similarity of several components. The message is set up in correct period.

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

2. How to identify an unclassified cipher of this type. 'cipher' is repeated. Patterns should show period.

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

3. This is about an insane fish that some how got the idea that it would rather live on land than in the sea. But mostly, it is about 'some how', so concentrate on that. Some help may be obtained from the knowledge that the words 'that we' and 'that it' are present, as well as the fact that 'the' occurs twice. Period is 7.

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

Note: The above ciphers and the Even Periods on the following page are all from old 'Circle-B'. None of them have ever been published before. All squares are scrambled, but one familiar with keyword recovery methods should have little trouble in recovering the original square and key.

4. Even Period Bifid. Concerning the traditions and enterprise of the British in connection with a national event of the early 1950's. Period can be determined by inspecting letters 40 to 60 and 100 to 120.

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

5. THE COLONIAL COCKTAIL CIPHER. Even Period Bifid.

"They were bold drinkers - our colonial ancestors - they thought nothing of mixing gin or rum with beer."
A New American History by W. E. Woodward.

The following is a recipe for one of these gin-beer mixtures, known to our forefathers as Rum Fustian.

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

6. Unpublicized Frenchman. Odd period Bifid.

For two years, 1955-56, the writer tried to get some biographical information on F. Delastelle. Finally, from the Cipher Section, Department of the Army, Paris, these meagre statistical facts were garnered.

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

Number 6 above was constructed to be solved. No tips are given. The period can be determined - obvious probable words will provide an entry. This is the final exam for beginners. Go to it and good luck.

S O L U T I O N S

PAGE 3 EXERCIZES.

1. T Q R O W M O M B F D X T Y L H Q I F G M H R N R G N W
   O K M N M Y W H R A T E K I N H H O I E Z Q H C F

2. The Delastelle Bifid is a very interesting type of cipher.

3. H E H M E P D C A H A H L D H V I T T U S R D T I

4. H E H N T E P D H A H A S H K D A O I H L C M S M

PAGE 19 TEST MESSAGE.

The ENTHUSIASM square is used.

PAGE 22 EXAMPLE.

Statisticians have long been accustomed to deal with prob-

PROBLEMS. (Answers enciphered by Caesar.)

1. A R A N U K J A Z N A W I O K B B E J E J C X Q N E A Z

2. F C F P R P M B Z Q X K R K Z I X P P F C F B A Z F M E

3. J I Z O C Z J M T K M J X G V D H Z Y W T O C Z H J N O

4. D P M K R F C D C C B G L E M D R F C Q G J I U M P K Q

5. X J L K D Q E B D F K Y B B O J F U Q R O B P T X P L K

6. Q E F P F P Q E B L K B V L R J R P Q A L X I L K B - -

AMERICAN CRYPTOGRAM ASSOCIATION

CRYPTOLOGIC REFERENCES

SOLVING SIMPLE SUBSTITUTION CIPHERS
By Frances A. Harris (S-TUCK)

CRYPTANALYSIS
By Helen Fouche Gaines (PICCOLA)

PRACTICAL CRYPTANALYSIS
Vol.I Playfair - Foursquare
Vol.II The Bifid Cipher
Vol.III The Trifid Cipher
By W.M.Bowers (ZEMBIE)

Vol.IV Cryptographic ABC's
Substitution and Transposition Ciphers
Vol.V Cryptographic ABC's
Periodic Ciphers - Miscellaneous
By William G.Bryan (B.NATURAL)

THE CRYPTOGRAM (Bi-monthly Magazine)
The Official Publication of the
American Cryptogram Association

Other titles available occasionally.

Editors-Publishers

E. & E. Rogot
9504 Forest Road
Bethesda, Maryland 20014

Sales

Robert Decker
RD #2, Box 341-A
Woodstown, New Jersey 08098

Treasurer

Edna Bickley
604 West Monroe Street
Mexico, Missouri 65265