PRACTICAL CRYPTANALYSIS

by

WILLIAM MAXWELL BOWERS

VOLUME I

DIGRAPHIC SUBSTITUTION

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 I

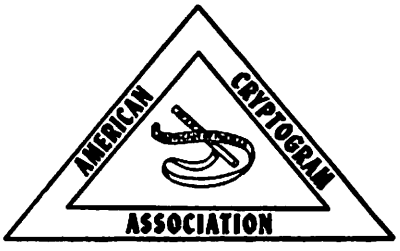
DIGRAPHIC SUBSTITUTION

THE PLAYFAIR CIPHER

THE FOUR SQUARE CIPHER

By

William Maxwell Bowers



To

MARGARET

Who helped by not interrupting.

C O N T E N T S

F O R E W O R D

"What one fool can do, another can."
Ancient Simian Proverb.

The literature of cryptology is definitely limited. Prior to the publication of Elementary Cryptanalysis by Helen Fouché Gaines (1939), there was no comparable book printed in the English language which was available to the civilian cryptographic enthusiast. This classic work familiarly known as 'ELCY', was originally sponsored by the American Cryptogram Association and is still considered to be its official textbook.

In 1952, an effort was made by the A.C.A. to bring out another textbook which would supplement the information contained in 'ELCY' and demonstrate methods for the decipherment of various other cryptographic systems not contained therein. This book was to be called Practical Cryptanalysis but, in book form, it never came to life. However, certain 'chapters'were prepared during the days when its publication was deemed possible and the present plan is to bring these out separately, in booklet form, retaining the name, Practical Cryptanalysis, as the general title for the entire series. That title was originally selected because the book was to be designed, primarily, for the instruction of amateur cryptanalysts who would have to be self taught.

In spite of a rather widespread opinion to the contrary, cryptanalysis is not a 'black art'. Its fundamentals can be acquired by almost any individual who has the desire to decipher secret writing and an opportunity to learn how to proceed. The object of this series is to attempt to outline, in simple language, the routine and basic methods that have come down to us from antiquity, and also, to incorporate into these classical methods some 'tricks of the trade' that have been devised by the members of the American Cryptogram Association.

W.M.B.

Clarksburg, W. Va.
October 1959

THE PLAYFAIR CIPHER

Substitution of cipher letters in pairs for pairs of plaintext letters is called digraphic substitution. One of the most interesting of the several systems based on this method is the Playfair. This system was originated by the noted British scientist, Sir Charles Wheatstone (1802-1875) but, as far as is known, it was not employed for military or diplomatic use during his lifetime. About 1890 it was adopted for use by the British Foreign Office on the recommendation of Lord Lyon Playfair (1818-1898) and thereafter was identified by the name of its sponsor.

The characteristics of the Playfair combined to make it one of real worth at that time as a military field cipher. Paper and pencil, a knowledge of the method, and a keyword which can easily be remembered, are all that is necessary for its employment. It was used by the British Army up to and through World War 1 and was also used, to some extent by the U. S. Army in 1917 and 1918.

METHOD OF ENCIPHERMENT BY PLAYFAIR

The Playfair system is based on a 25-letter alphabet set up in a 5 by 5 square. In its simplest form, a keyword is written horizontally into the top rows of the square and the remaining letters follow in regular alphabetical order. In English, the letter "J" is omitted from the square and when "J" appears in the plaintext it is enciphered as though it were the letter "I". For example, the word "just" becomes "iust" for encipherment purposes. Using the keyword LOGARITHM, a typical Playfair square is shown below.

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

In preparation for encipherment, the plaintext is separated into pairs. When a pair would consist of a doubled letter, as "SS" or "NN", a null is inserted between the doubled letters.

For example, the message, "COME QUICKLY WE NEED HELP" is set up:

CO ME QU IC KL YW EN EX ED HE LP

Note that an "X" has been inserted to split what would have been a doubled "E" in the eighth group.

The following rules govern the encipherment.

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

Example:	Plain	Cipher
	OP	TW
	IC	CN
	EX	QG

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

Example:	Plain	Cipher
	YW	ZX
	ED	FE
	QU	SN

3 - When the two letters of a plaintext pair are located in different rows and columns, they are enciphered by the two letters which form a rectangle with them, beginning with the letter in the same row with the first letter of the plaintext pair.

Example:	Plain	Cipher
	CO	DL
	ME	HF
	KL	CR
	LP	ON

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

IDENTIFICATION OF THE PLAYFAIR

Certain distinctive features assist in identifying the Playfair as a cipher of that type. Among these are the following:

1. It is a substitution cipher.
2. The cipher message will contain an even number of letters.
3. A frequency count will show not more than 25 letters.
4. In English, the letter J will ordinarily be absent.
5. When the message is separated into pairs, no doubled letter will occur.
6. If long repeats occur, they will be at irregular intervals.
7. In most cases, repeated sequences will be composed of an even number of letters.
8. Many reversals of digraphs.

PECULIARITIES OF THE PLAYFAIR

1. No plaintext letter can be represented in the cipher by itself.
2. Any given letter can represent 5 other letters.
3. Any given letter can be represented by 5 other letters.
4. Any given letter cannot represent a letter that it combines with diagonally.
5. It is twice as probable that the two letters of any pair are at the corners of a rectangle, than that they are in the same row or column.
6. When a cipher letter has once been identified as the substitute for a plaintext letter, there is a one-in-five chance that it represents the same plaintext letter in each other appearance.

SOLVING THE PLAYFAIR

Methods of solving Playfair ciphers have been discussed by many writers. The goal is the recovery of the 5 by 5 square and various techniques for accomplishing this have been developed.

In addition to noting the above-mentioned peculiarities and characteristics it is recommended, by practically all authorities on the subject, that a frequency count be made, both of individual letters and of digraphs.

The individual letter frequency count will show probable position in the square, as high frequency cipher letters attain their high count by being in row or column with high frequency plaintext letters. Conversely, low frequency cipher letters are apt to be in row or column with two or more low frequency plaintext letters. This last circumstance frequently occurs in the bottom row of the square, where, if the alphabet is not scrambled, five of the last six letters, U V W X Y Z, will often be indicated due to their alphabetical order and mutual low frequency.

A digraph count is considered to be an aid to solving because cipher digraphs closely follow the frequency of the plaintext digraphs they represent. The reason for this similarity is, that when enciphered from a given square, any plaintext digraph which appears as a Playfair pair, must be represented by just one, and always the same, cipher digraph. Thus, in the square given above, cipher "HM" must always equal plaintext "TH". As "TH" is the English plaintext digraph of highest frequency it can logically be expected that, in a message of sufficient length enciphered from this square, the frequency of the cipher digraph "HM" will be correspondingly high.

Other advantages can be derived from a digraph frequency count. For instance, when two cipher digraphs of distinctive frequency are consecutive, they may be tested for plaintext tetragraphs of corresponding frequency. Such plaintext tetragraphs as THAT, THIS, THER, TION, ERED, and others may sometimes be located in this way.

A method of taking both a single letter and digraph frequency count simultaneously will be illustrated in connection with a demonstration of the solution of a Playfair message. This method is particularly recommended because it also gives a visual picture of the cipher alphabet and draws the eye immediately to letters of both high and low frequency.

Frequency counts are helpful in attempting to solve a Playfair but what must actually be accomplished, in order to make an entry and get underway, is the location in the cipher message of the true position of a plaintext word. This fact is recognized by all authorities on the subject.

Due to its inherent characteristics, Playfair cipher words will follow the same pattern as their plaintext equivalents. When properly divided, such words as MA IN TA IN IN G-, EV ER MO RE, AT TA CK, and many others carry their pattern into the cipher. Consequently, the search for probable words is of prime importance.

In order for the solver to select probable words, something must be known concerning the reason for the message being in cipher. In police work, known facts of the case with which the cipher is connected, will suggest probable words. In diplomatic and military circles, cryptanalysts can try words from their particular field, such as A MB AS SA DO R- and - B AT TA LI ON respectively.

In the messages which the amateur cryptanalysts encounters, such as those in the A. C. A. publication, The Cryptogram, there is usually nothing, other than the title to suggest probable words. These messages might be on any subject, selected at random by the constructor, and in most cases they are too short to reveal very much when frequencies are analyzed. To compensate for this a plaintext fragment which can be spotted in the cipher message is given, in order that the solver may get started with some degree of assurance that he is on the right track.

A message of this latter classification has been selected to demonstrate the technique of Playfair solution. The example is from The Cryptogram, Oct. 1952, No. E-9, Playfair, by Hampiam.

Title - About Dry; Given clue - "er one day entere".

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

The message is copied on quad-ruled paper, leaving at least two blank spaces between the lines. The pairs can be kept intact and space saved if the first letter of each pair is written close to the right side of its cell and the second letter of the pair is written at the left side of the adjoining cell. In this way all cells are used but a distinct space shows between the pairs.

The frequency count is then taken. To do this, write vertically a 25-letter alphabet (J omitted) in the middle of a work sheet and draw a vertical line on each side of it. Write the letters of the cipher pairs to left and right of this alphabet, that is: "E" left of "U" and "U" right of "E"; "S" left of "M" and "M" right of "S". As the pairs are tallied, underscore in the message all repeats, and overscore all reversals. If the message is of sufficient length to make it worthwhile, tabulate the number of occurrences of each repeat and reversal and write that number under these pairs in the message. The frequency count for the above message is shown below.

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

In this particular message the frequency count is of little value as far as digraphs are concerned, as no pair repeats more than once. The individual letter count indicates probable position of several letters, but the main thing that has been gained is general familiarity with the message and the location of the repeats and reversals, which have been marked.

An attempt is now made to spot the location of the fragment of plaintext which was given as a clue. This is divided into pairs, thus:

ER ON ED AY EN TE RE

It is immediately noted that the first pair and the last pair constitute a reversal with five pairs between. The message is then inspected for a similar pattern and it is found that there is but one place where the given plaintext fragment will fit. It is written in below the cipher pairs thus:

Cipher	GX	DZ	SQ	DY	BA	AQ	OB	ZD	AC
Plaintext	..	er	on	ed	ay	en	te	re	..

It is next necessary to take each set of these pair equalities and establish the position of the four letters with respect to each other. They must conform with one of the three basic rules of Playfair and be (1) in column, or (2) in row, or (3) a rectangle.

The six different sets of pairs of known equalities may be set up as shown below. The sets are numbered for future reference.

1	2	3	4	5	6
er = DZ	on = SQ	ed = DY	ay = BA	en = AQ	te = ob
E D R Z	O S N Q	E D Y	Y A B	E A N Q	T O E B
D	S	D	A	A	O
R E D	N O S	Y	B	N E A	E T O
Z Z R	Q Q N			Q Q N	B B E

Working with the three possible relations of the letters in each set of pairs, the different sets are now combined with each other. In making these combinations the sets used will be referred to by number and the various possible positions will be indicated as being Vertical (v), Horizontal (h), or Diagonal (d).

Inspection shows that 1 will combine with 3, thus:

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

Other sets will combine with the 1-3 combinations but before adding to them look at sets 2 and 5. Both contain "NQ", located in the same row or column. They can be set up:

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

Set Number 6, which contains two of the same letters included in 2 and 5 (E and O), will not combine with either the first or the second of the 2-5 combinations, but it will combine with the third.

2/d - 5/d - 6/v

```
  T
S O
A E
  B
N Q
```

2/d - 5/d - 6/d

```
S O T
N Q
A E B
```

The 4th set will combine with only the second of the above, thus:

2/d - 5/d - 6/d - 4/h

```
  S T O
Y A B E
  N   Q
```

And now, if the combinations of 1 and 3 are inspected, it will be found that only one, 1/d - 3/h, will combine with the combination of 2 - 4 - 5 - 6. This gives:

1/d - 2/d - 3/h - 4/h - 5/d - 6/d

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

ARRANGED IN 5 X 5 SQUARE

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

From the above it is evident that, as "O" is one of the letters of the keyword, the cell between "N" and "Q" can be filled only with the letter "P". Also, as letters "S", "T", and "Y" are in the keyword, three of the letters "U", "V", "W", and "X" are required to fill the open cells in the bottom row. These can be written outside the square on the bottom row. Next, inspection shows that "C" must be in the keyword, which appears to end with "DY" in the second row. So "C" can be placed outside the square in the first row. This gives:

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

Now, with the exception of the letters placed and tentatively placed, all that remain are F, G, H, I, K, L, M. These seven letters, in their alphabetical order, are required to fill the open cells in the third and fourth rows between "E" and "N". The square is now:

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

C

U V W X

With this much of the square recovered it can be seen that the keyword must surely be CUSTODY, and the complete original square is:

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

The entire square is thus recovered from the fragment of plaintext which was given. The decipherment of the message is now merely a matter of employing the rules for decipherment when the keyword is known.

The following example for practice should yield to the same method of attack.

TYPE - Playfair TITLE - About Ciphers TIP - "ng and solving"

NC GM RN UQ TO LK ZQ CT PT QN TL FQ NC TW NQ IO AI GE LM IO
IL QF EK QN HD DX CL GA IL TA HP NU XA IL SG OV BO AG KH TM
TQ LM RT PN GE XT NC KG TB IO MT

\- * - * - * - * -

Both the demonstration cipher and the practice problem given above are examples of the Playfair in its simplest form. A much more difficult cipher, and one requiring a far greater display of ingenuity on the part of the solver, is the following which appeared in The Cryptogram, Oct.-Nov. 1944; No. 17 of The Cipher Exchange; Constructor - Barrister; Type - Playfair; Title - While Rome Burns; Given clue - "ers are".

OC MA FZ DA PZ BY PG YB OK YT BY VM TA VI BY PV GP PR BC FH
XE AP IV TC PV VB KG VM EW CB IE GM QP PB OL EN RH ZM RF SC
DR NA IZ EI TN SU NA

In starting the solution the first step is to make the frequency count. This will be omitted from this demonstration but it should be done because, even though nothing else is revealed thereby, it serves to familiarize the solver with the cipher and shows the location of the various repeats and reversals.

Next, the location of the tip, "ers are", is spotted. It is found that it can fit at only one place, under cipher BY PG YB. The equalities derived are then set up.

1 - ER = BY

E B R Y
B
R E B
Y Y R

2 - SA = PG

S P A G
P
A S P
G G A

Since the two equations have no letters in common they cannot, immediately, be combined. For the time being assistance from the given clue is exhausted, and it is necessary to look elsewhere for an entry. Assuming that a standard keyword square was employed the message is inspected for "naturals". "Naturals" are cipher digraphs, not in the keyword area of the square, which are in natural alphabetical relation to each other and which will furnish acceptable plaintext digraphs. The cipher pair "QP" catches the eye as a possible substitute for plaintext "PO". If this assumption is correct the relation of the three letters can only be horizontal, thus:

3 - PO = QP

O P Q

Equations 2 and 3 can now be combined in two ways.

```
  S
O P Q
  A
  G
```

```
    A   G
O P Q S
```

The second of the above appears to be more promising than the first, and also, it will combine nicely with equation 1/v. This is done and all letters are placed in the square as shown below.

			E	
	A		B	G
O	P	Q	R	S
			Y	Z

(Keyword eight letters, containing C, D, F)
H I K L M N (One letter in keyword)

T U V W X (Two letters in keyword)

This partial square seems to be entirely possible and there is a strong inclination on the part of the beginner, at this point, to try to complete the square by guessing the keyword. With no more to go on than is shown above, his efforts along that line are, almost without exception, doomed in advance to failure, and much time will be wasted by such an attempt. Trying to guess the keyword without sufficient information is apractice always to be shunned, the more particularly so because there are other ways of using one's imagination which will yield results far more tangible.

With the square partially filled as shown, the message is again inspected for equations that will make acceptable plaintext. The first possibility encountered is the fifth cipher pair, "PZ". With the set-up adopted, "Z" was forced into the last cell of the fifth row, under "S", and the letters "U", "V", or "W" are the only ones that can be placed under "P".

The cipher pair, "PZ", immediately preceeds those where the given fragment of plaintext was spotted. The known plaintext values have been written under their cipher substitutes and the first part of the cipher shows this.

```
OC MA FZ DA PZ BY PG YB OK YT BY VM TA VI BY PV GP PR BC
                  er sa re       er          er    as
```

Assuming that a word division falls between "s" and "a" of the plaintext, it would be: -- ers are -- .

For the "PZ" cipher pair the possibilities are:

```
U under P gives plaintext - - -  suers are
V under P gives plaintext - - -  svers are
W under P gives plaintext - - -  swers are
```

Any of these coule be possible though none of them immediately suggest more plaintext. Leaving them for the moment and investigating further, the cipher pair "PV" is noted between two pairs already deciphered. In the square, as now set up, if "V" is in the fifth row it can be located under "O", "P", or "Q". This gives the following possible equalities for cipher "PV".

```
V under O gives plaintext - - -  er ow as
V under P gives plaintext - - -  er -p as
V under Q gives plaintext - - -  er qu as
```

Studying the above, the first thought is that the set-up which makes cipher "PV" equal plain "QU" is the best bet. On pursuing this further, it is found that this relation foces "W" and "X" into the keyword and also that "quas" starts only two ordinary English words (quash and quasi) and their derivatives. This is not so good.

The second equation, "PV" equals "-P", has possibilities but is incomplete.

The first equation, "PV" equals "OW", is studied and inspiration strikes. The situation is this:

Cipher:	VI BY PV GP
Plain:	er ow as

Remembering that the title of the cipher is "While Rome Burns", what word could be more probable than "Nero"? This is a perfectly logical assumption and, if correct, will provide a positive entry which can be developed with confidence. The new equations are:

4 - OW = PV

O P
V W

5 - -N = VI

- V N I
V
N - V
I I N

The new values are entered in the square and, immediately, difficulty is encountered. It is found that OW = PV can be placed but -N = VI will not go into the square as it is now partially established. The square now is:

			E	
	A		B	G
O	P	Q	R	S
V	W	X	Y	Z

The trouble is this. Only equations 5/v or 5/d can be used in this square.

If 5/v is used, with "N" in the first row and "I" in the second, then only four letters, H, K, L, M, are available for the third row. If "N" is placed in the second row and "I" in the third, only K, L, M, remain for the four open cells. If it is assumed that the keyword extends into the third row, testing for plaintext will give nothing acceptable. Consequently, 5/v is abandoned.

Equation 5/d meets the same fate for the same reasons. It becomes evident that an incorrect assumption has been made and it must be discovered and corrected.

Equations 1 and 2 were given and are known to be correct.

Equations 3, 4, and 5 are based on logical assumptions which have not been disproved and are still thought to be good. These assumed equations, together with 2, can be assembled as shown below.

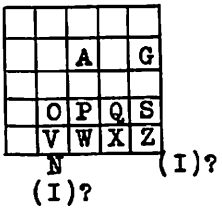
2/d - 3/h - 4/d - 5/v

```
N
I
  A   G
O P Q S
V W
```

2/d - 3/h - 4/d - 5/d

```
I N
    A     G
  O P Q   S
  V W
```

Knowing that the partial square as previously set up was not correct, the vertical relation of ER = BY is reluctantly abandoned. This means that both "R" and "Y" must be in the keyword and would place "X" and "Z" in the fifth row, following "W", and giving this square.



Equation 1, ER = BY, can be fitted into this square in either its horizontal and its diagonal arrangement. The only way to determine its true location is to place it at its various possible positions and test for probable plaintext.

It is axiomatic of the Playfair that if any cipher letter has once been identified as a substitute for a certain plaintext letter, it is highly probable that it will again be found as a substitute for that same letter. With this thought in mind, consider the consecutive cipher pairs, QP PB. This could easily be "po o-".

When equations 1 and 3 are combined as shown below, cipher QP PB gives plaintext "poor".

E B R Y
O P Q

This arrangement will fit into the square and it is placed there. It now looks as if the alphabet is based on a long keyword and the square is tentatively arranged to conform, thus:

I					
	E	B	R	Y	
			A		G
		O	P	Q	S
		V	W	X	Z

This arrangement also confirms the value of the cipher pair, "PZ". Letting PZ = SW, the original fragment of plaintext can be further extended.

Cipher: DA PZ BY PG YB
Plaintext: sw er sa re
(an)

From the above, one can visualize "answers are", making DA = AN. This last equality can be placed in only one way - horizontally. To accomplish this, letters "I" and "N" must be moved to the same row with "A", and "D" must be put into that same row following "A". The square now shows:

	E	B	R	Y	
	I	N	A	D	G
		O	P	Q	S
		V	W	X	Z

Referring again to the cipher and testing for plaintext with the partial square as now established, a veritable bonanza is struck at the end of the cipher.

Cipher:	RF	SC	DR	NA	IZ	EI	TN	SU	NA
Plaintext:			ay	in	g-	-e			in
Probable:	by	pl			t	h	vi	ol	

It is found that the various letters forming these equations will fit into the square, making it practically complete. It now is:

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

The keyword is recognized as: HUCKLEB(E)R(R)YFIN(N). The complete message is deciphered as follows:

> Pupils' answers are que(x)er, to wit: Nero was a cruel tyrant who would torture his poor subjects by playing the violin.

The above cipher is an example of what the amateur cryptanalyst may expect to encounter. The following features should be noted:

1. The message may be on any subject, whatsoever.
2. The keyword bears no relation to the message.
3. The message is too short for analysis by digraph frequencies.

The solution of the above cipher was given step by step in order to call attention to certain routine procedure which can be followed.

1. Entry is ordinarily made through a probable word.
2. Assumptions must be based on logical indications.
3. The possibility of "naturals", resulting from an unscrambled alphabet should be explored.
4. The possibility of a given cipher letter representing the same plaintext letter two or more times should be kept in mind.
5. Various combinations of equation relationship must be tested to see if they give good plaintext.
6. Combinations which give good plaintext digraphs must be developed regardless of how strange they look in the square.
7. Combinations which merely look good must be discarded if they fail to produce.
8. Many blind alleys will be explored in search for the correct combinations.
9. Trying to guess the keyword is no good.

PLAYFAIR VARIATIONS - THE SERIATED PLAYFAIR

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

In this type the plaintext is written horizontally in two line periodic groups as shown below in period six.

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

From the above example it is seen that vertical pairs are formed and these are then enciphered by the routine Playfair method. When a vertical pair would normally be a doubled letter - as "E" at the beginning of the second group - a null is inserted to prevent this repetition. Using the square based on the keyword LOGARITHM, the above message is enciphered thus:

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

N L B C S P Q Q C D C M H C F T R H
C D F G X Z G C G Q T B F G W H G B

For transmission, the message is taken off horizontally by the same route by which the plaintext was written for encipherment.

NLBCS PCDFG XZQQC DCMGC GQTBH CFTRH FGWHG B.

In the solution of a Seriated Playfair the determination of the period length is of first importance. This can be accomplished by writing out the message in various periods and eliminating those which result in a vertical pair consisting of two appearances of the same letter. When this occurs the period being tested is immediately proven wrong. If the message enciphered above is tested in this way, in all periods from 4 to 10, it will be found that all except period 6 will show a doubled vertical pair.

In the vast majority of cipher messages of this type, apt to be encountered by amateur cryptanalysts, the period length will be in the range of 4 to 10.

Impossible periods can also be determined mathematically. This method was explained in detail in an article by Chas. A. Leonard in the Oct.-Nov. 1951 issue of THE CRYPTOGRAM. It will be summarized briefly below. The determination is made by use of this formula:

$$\frac{S_2}{S_2 - S_1} = Q \text{ \& } R$$

Where: S_1 and S_2 = Serial numbers of two appearances of the same letter.

$S_2 - S_1$ = Period Q = Quotient R = Remainder

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

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

The use of this formula can also be illustrated with the message above.

Cipher letter serial numbers are:

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

Period	Letter	S_2	-	S_1	Q	R	Result
4	F	31	-	27	7	3	Eliminated - Case 1
5	C	20	-	15	4	0	Eliminated - Case 2
6	C	26	-	20	4	2	Not eliminated
7	H	*34	-	30			Eliminated - Last group*
8	D	16	-	8	2	0	Eliminated - Case 2
9	C	26	-	17	2	8	Not eliminated
	G	19	-	10	2	1	Not eliminated
	H	34	-	25	3	7	Eliminated - Case 1
10	C	17	-	7	1	7	Eliminated - Case 1

* When a periodic value of S - S does not occur in the message the final group should be examined. If the final group is shorter than the regular groups of the period being tested, a doubled vertical pair may show at an S - S value equal to the length of this final group. If such is the case it eliminates the period being tested.

The above tabulation shows that all periods, 4 to 10, are eliminated except period 6, which is accepted as the correct seriation length of the message.

Solution of a Seriated Playfair is far more difficult than is the case with regular Playfair. After the period has been determined the message is set up in two line groups of period length. A digraphic frequency count is made of the vertical pairs, for, as in regular Playfair, this will be helpful in determining probable position of letters and, to some extent, will indicate whether or not the square is standard or scrambled.

Plaintext high frequency digraphs and tetragraphs do not carry their identity over into the cipher and, consequently, are not recognizable. Entry must be made by means of a probable word and in most cases, in amateur cryptography, such an entry will be given.

Although plaintext digraphs do not show in the cipher, plaintext words or phrases which form a pattern, when set up in two line groups, repeat that pattern in the cipher. This characteristic provides a method of making an entry if the solver has sufficient ingenuity, skill, or luck, to select the correct probable word to fit the pattern. However, as stated above, in ciphers of this type for solution by amateurs, a probable word or group of words that form such a pattern is usually given. Once the entry has been made the solution follows the same general routine as used in regular Playfair. Though more difficult, because the pairs do not give consecutive plaintext, sound assumptions and logical reasoning will bring the desired results.

The following example is from THE CRYPTOGRAM, Oct. - Nov. 1951. Type: Seriated Playfair. Given word: "Destined" by Sellwyn White:

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

THE TEST FOR PERIOD

Per.	Let.	S_2	-	S_1	Q	R	Result
4	E	55	-	51	13	3	Eliminated
5	D	98	-	93	19	3	"
6	B	63	-	57	10	3	Not eliminated
	B	86	-	80	14	2	" "
	U	49	-	43	8	1	" "
7	H	26	-	19	3	5	Eliminated
8	C	105	-	97	13	1	"
9	E	51	-	42	5	6	"
10	B	35	-	25	3	5	"

The period 6 is accepted and the cipher is set up in two line groups, thus:

HKILVP PBVBAA BHRPOU TBITFE
RNFTZU HZWVFR UDTKBD UIBYNS etc.

The given word, "destined", could be in any of the following positions when enciphered in period 6.

D E S T I N . D E S T I . . D E S T . . . D E S . . . . D E
E D . . . . N E D . . . I N E D . . T I N E D . S T I N E D

The DE - ED reversal in all arrangements is noted and inspection of the cipher shows that the second of the above will fit the cipher digraphs of group 4 as shown below:

B H R P O U T B I T F E U C E V Z K
U D T K B D U I B Y N S E X B Z A R
d e s t i
n e d

Correctly locating the given word has produced one complete equality and four partial equalities. These are set up:

1	2	3	4	5
.n TU	de BI	s. TY	t. FN	i. ES
- T N U	D B E I	S T - Y	T F - N	I E - S
T	B	T	F	E
N - T	E D B	- S T	- T F	- I E
U U N	I I E	Y Y -	N N -	S S -

Progress, from here on, follows the routine procedure of solving a regular Playfair. The solution will not be given, step by step, as the only difference is that the cipher pairs do not give consecutive plaintext.

The experienced cryptanalyst will take what he has, which in this case is the plaintext word "destined", and will consider what else can be developed. He will try to think what words might precede or follow it and he will decide that in normal English, unless separated by an adverb, one of the following sequences might be expected.

is)		(
was)		(for
are)	destined	(
were)		(to
have been)		(

By elimination, he will finally accept "is destined to" and will be able to fill in the unknown letters of equations 1, 3, and 4; and also to add another partial equality: - I = U D. With this additional information and the perseverance necessary to solve any difficult cipher, a solution will reward his efforts.

There are several other variations of the Playfair cipher system, but, like the Seriated, they are merely variations. The basic characteristics remain the same and when it is known wherein the variations differ from the original system, they will all yield to the same general method of attack by the cryptanalyst.

N O T E

The ciphers selected for use as problems in this book have never appeared in The Cipher Exchange of THE CRYPTOGRAM.

Those which follow, both Playfair & Four Square, were constructed and circulated by the members of Circle-B, a 'Friendly Group' which flourished during the 1940's.

Membership in this group was limited to eight and, for various reasons, the personnel changed from time to time. Among those who were members during its 'golden years' were:

X-GOTKY	Herbert Raines, Leader.
EMPTY	Mrs. Herbert Raines
S-TUCK	Mrs. Frances A. Harris
C.SHARPE	Mrs. Charles P. Proudfit
TRYIT	Richard Hayes
GALUPOLY	Mrs. Harris K. Lyle
I.N.JOYUM	Mrs. Walter A. Simond
TONTO	William A. Lee
JUSTINIAN	Walter L. Schiffman
DOT	Dorothy K. Thomas
FIDDLE	Col. F. D. Lynch
ZEMBIE	W. M. Bowers

PROBLEMS

1. Copy cat. "that is" repeated. EMPTY

YC LF XD LK VU PD YK QL IO RL ZD RX KP OV DP HD KV AC KC SX EA
AS DS HQ IY CS XE RV OP SM DF OD AO LN AH OC ZQ IS VK AR NL FT
LQ RM XE RV OP QL LK DA BK.

2. Universal ailment "common" GALUPOLY

KS GI NE KS SH OS FU KG AD QB SO CF FC GU KI QG QG EI QT CF AD
CA QB ZL QU CE AD RB DU KX OB GU FP GK FT GR AS GU HI FS OS IC
TM YB CA KX GK QT NE QG CD KX EW.

3. Crafty Yankee. "a man aske" (Can be spotted) C-SHARPE

FM NX PE WX CM PL WD TW YG OB OA XY VP LG QC BK EK KO NA FQ BV
FM GC NY ZU NY CA PA CN FM YX YN NE BK YL SF KV BP OG NY XC BA
OP SY NY XC CB ZP NY CA PA CN FM YX BC PL NB UF WK HV PL WD TW
YG XY CO CB FD UW UQ YX PI PD XA NL.

4. Ancient sport. "claimhailc" JUSTINIAN
Alphabet is written-in diagonally from lower left corner.

DW FI PI QU SQ TH UT PC IC UE KU HS IU QU AI LH BW TU ET BD UC
YQ UA FX VH DQ IP UZ IP QD UK KO ZQ YT RU OP KU QA NU QU GD KE
FB NU KS UA QU IF WZ BF GD UB CS EK HU SH DI NW ET OP TH OP IP
EK UE KN PQ FR DI DZ DW FS KE DI OI BF KR.

5. First Principles. ZEMBIE
Opening words of an address on Cryptography to Boy Scouts.
X. GOTKY made entry by Probable Word Method.
C-SHARPE made entry by correctly assuming QZ to be a "natural".

CK SC MT BK CH PR CG CR ZS PR EC KT CM CS UN CS TQ SZ OI CR NA
Z6 SC NU HT QT HN OB IS RG HY EC QZ OC MH EY CB EI EC QZ OC YE
IN RH RB PZ KC HL ET TM OS TA UT SK YM SC CB QT SP BE BE RG BL
CO UT YH RS CR BO QS EB FT OC ZQ EC QZ OC SK BU KD EN YA CB EI
NH OI CR HR LR NU KC EI EK BA OC SO DO MI EY SF QF BA GS RH KE
GX DE LC QZ.

6. Oswald Jacoby on Poker. "opponent" GALUPOLY

TC SU NQ PL AM GV TD BC AM UG NA MU TM TN FN EH XO IT QT NE FT
IA RD RI TM EA QH XA XN QO NX AM FE TA QH UR HB AW AL NA AS UQ
AW AL RK SU SN QD CT FE TG XA CR TK SN FB CT PQ QP ES EA UT NE
ZU NE ES MF TH ST RU ST.

7. Scientific thinking. "htsthath" I. N. JOYUM
Square is not standard horizontal write-in.

OT TG BO AZ TC TO ST ZV TR QY TQ AO PF HL TC KS YS TC LI IZ FZ
CL SO IK QS PZ YP TC PK QV LC TC IK CL MI ZE BP BO XI CM UA VG
AY PF SK YM DS OP ZC PF AV MB.

8. Curative properties of plants. "other ills" ZEMBIE

OF ES OP KV RK BU XE QZ CO BC VZ HG FO UG BZ LN NA FK UA DR ZW
LH RD OG UA YK PO RX VZ HG MF PA ZN ZY QI FW AH MK QK RB BZ LN
NZ CZ KE RB MV NC RK KR KM PE ZC CT OG AN LR WC ZE ZU ZK NF OF
KR UD QK RX OF KF LA RP RW GZ GZ GZ RN WQ GP HP RD RZ OF DX ZY
KV PU UM ZW OF FK MW KB QZ NR WO VZ KV OF KF WZ.

9. Fancy Dressed Early Californians. GALUPOLY
"Velvet" A good operator should be able to spot this word but for those who can't, try "QEBYLQQL" (Caesar)

KF TN YB BG QL KV FX LS AE IH TB TB AE BG AV NR ER FH GS GZ AH
ZN IP CH EK YR HX TY SN HM TY AV PI CZ VE TO OF RN AC KI FK GH
KI GB NH DL GS IE NQ KF GD FU UF QP AE AH NU MI KF RN AG GF EY
FR FD BZ NU RH HO QF DN KF GB GC FU PN AE OK RG PA KG IH ES PQ
TF YT BX NU RH AO YR DK.

10. Item of Early American History. C-SHARPE
Most frequent digram runs true to form.

XL XW TM CS UV TS IR SN KR CT OR RD NI XS TH NX BV YX NX UZ EZ
UV CA BA UN PBGN NI RK EZ HX CL BL NW RT UC HL EY VN BN TV OR
MW EY GY OB HT NI XA XY HT DR FW DT TO XQ BE NI MT NX NB AX CT
NX NW ZN HF RP UI RD NI PN TM CQ YE XR IK YO XP NB UN XY NE.

11. Seriated Playfair. "simpleisn" ZEMBIE
Capt. Parker Hitt gives four requirements for success when working "with unknown" cryptographic systems.

QCEPF CTKML RMLUB MSEEZ CRCZR CETWM PKMAB OMRBR DRELE
TRKLC MSACM KKOYK MUUFX KYHIS EEQMX DCBKQ BYPHU LUPNB
HEHCS RPMIO IBRBH UUTDD NPSFR MVKKB AKULM IWPBZ IRNQM
REDVK GTFRB LFRBG XHMYA BFCSH MUTQI ONPKB MRDMS TFPCS
RBNCE NYAEY FMRPA CARER CTULC HLSKD BEFIL MEOPO VXBMU
NIRIF KOULR LMLRI ONSYU TNOXB KBJJJ

12. Where is Cleopatra? ZEMBIE
A bit of verse by Don Marquis on the subject of boy meets girl in ancient Egypt. Think about: Antony - Ptolemy - Nile.

FN GU RA UM FM ST MI NG RL LW QU AM LP MR CU BR QU UN OB IN IP
TG QE FL RS LF RL OB BV IV LF HT GL AF TN MQ EO FN KY YT AF TN
MO GU IP BZ HS IF MB IN IP NT CY LB DR LQ RC TI QA SR AL BR GS
OE RG UC OB ED IY QU OQ CI LN VB CI TF RL OB BV GA YI QU DR QN
MR NG IV QO IW QO BR QU MB OS RG BF AG UO LY OS RI AQ QU SO OQ
BD IR MB IP OE DN PI QU NS SO RF DM UO AQ OA ZM NG BE MO BI VT
QU CI IT OS RD BT NG ZX QU OR.

PLAYFAIR SOLUTIONS

Note: In order that these answers may not, inadvertently, spoil the fun for those who really want to solve the problems they are enciphered by various Alphabet Run-down methods, i.e. separate word lengths or groups, diagonal letters, words or groups, zig-zag, steps, etc. However, all will readily yield the answer when the run-down is carefully inspected.

Practice Example, Page 9.

0. (QDFTKZSHNM) SGD OKZXEZHQ RXRSDL HT NMD * * * * * *

Problems.

1. (OXAFLNRFW) PLJB TFPB JXK FP ZOBAFQBA TFQE * * * *
2. (ZEWCJKOA) DAWZW YDAEO YKILH WEJPO KYKII * * *
3. (CLTI ZQLHEYEPU) TEBK YWHREJ ZLLIFADB SWO MOBP * * * *
4. (YKJMQ FPQXA KNAO-) DIXAF WPKNO BKQBO EJCPD BXOBK * *
5. (TMPTN RYZJC) XPFQP LYKCG LOKHD QQGKN IBPRY * * * *
6. (AHPBSLQSYMAD) Q H L B C O M J C Q Z X G S Q U C Q W M
7. (BPVOO ZJFVZ) ZQZEZ MRFOO RYVOY HQZQN RGLJ- * * * * *
8. (HTGPEJ BQWCXGU) JGTDCNKUVU FQYP VJG CIGU JCXG * * *
9. (OLWJEOD ZXIFCLCKFX) PDAU TBOB ZWNGHU EXKAPLJB * * *
10. (XQIETGTMHKR) Y KGPMDWPN QJQI QEB KMRRM NE * * * * *
11. (BYOCESIKDREMCQ) M Y Q I B P G G Q R Z S Q F N L D Z *
12. (OEYQOXJOEQDIKNEXJRJZE) EXKZCKJBJWNXRPXJPKKV * * * *

THE FOUR SQUARE CIPHER

Like its British counterpart, the Playfair, The Four Square is an example of digraphic substitution. The origin of this interesting system is somewhat shrouded in mystery. Hitt's Manual (1918) makes no mention of it although he devotes several pages to the Playfair. In like manner it is found to be "included out" in the cryptographic manuals of the foreign authorities, Mario Zanotti (Milan, 1928) and General Luigi Sacco (Rome, 1937). It is also ignored by the popular U. S. cryptographic authors of the early nineteen forties, as Fletcher Pratt's Secret and Urgent and Laurence Dwight Smith's Cryptography say absolutely nothing of such a system.

First mention of the Four Square, for the benefit of the public at large, was probably made by Helen Fouche Gaines in Elementary Cryptanalysis (1943). This reference is rather vague and does not give a name to the system. It merely says:

> "Another common method pair encipherment can be understood from the following description. Picture a chart of 100 cells which is divided sharply into four quarters. Each of the four quarters is a 5 x 5 square and contains a 25-letter alphabet. At least two of the alphabets are mixed, usually with different keys. To encipher a pair, find its two letters in two different squares and substitute two others which occupy certain related positions in the other two squares."

That's all that "Elcy" had to say about the Four Square but during this same year, 1943, Major Donald Millikin's textbook, Elementary Cryptography and Cryptanalysis, carried a brief description of the system which he called "The Four Square Matrix Cipher". At about the same time Prof. J. M. Wolfe of Brooklyn College published his own textbook, A First Course in Cryptanalysis, and in it he devoted a full lesson to "Four Quadrant Matrix Digraphic Substitution".

The first appearance of the Four Square in The Cryptogram, the official publication of the American Cryptogram Association, was in the issue of Aug.-Sept. 1947. This cipher was constructed by C. SHARPE, (Mrs. Charles P. Proudfit of Chicago) and a brief explanation of the system was given at that time by the editor. Since then numerous Four Squares have appeared in the Cipher Exchange of that magazine, as well as several excellent articles about this system.

Due to the secrecy which surrounded its early days, it may well be assumed that the Four Square was adapted by U. S. Army personnel for use as a field cipher in World War I days. This supposition is somewhat strengthened by the fact that students in Major Millikin's classes at New York University during World War II recall that he always spoke the words, "The Four Square Matrix Cipher", with a certain tone of reverence in his voice not bestowed upon the name of any other system.

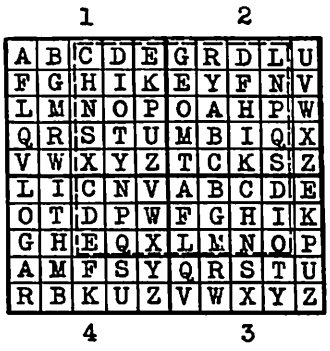
Actually, the basic idea of the Four Square must be attributed to that mysterious Frenchman, F. Delastelle, who devised the Bifid, the Trifid, and numerous other cryptographic systems. In his interesting book, Traite Elementaire de Cryptographie (Paris-1902) he says:

> "- - the formation of that table of digraphs is a long and laborious task, especially when reciprocity must be obtained. We must, then, find a process which is simple and practicable, which allows us to do away with these tables just as the sliding alphabets allowed us to do away with the Vigenere and similar tables. After long research the author has found the solution of this problem and has invented two procedures satisfying these demands, bigrammic squares and bifid alphabets."

Delastelle then gives an illustration of his "bigrammic square" which is formed with four 25-letter alphabets, and describes how it may be used in much the same general terms as the description of the Four Square method which follows below:

METHOD OF ENCIPHERMENT BY FOUR SQUARE

As its name indicates, the Four Square employs four 25-letter alphabets set up in four 5 x 5 squares. The alphabets in the upper left square and in the lower right square are straight alphabets with "J" omitted. It is in these two alphabets that the plaintext letters are found when a message is to be enciphered. The alphabets in the upper right square and in the lower left square are mixed alphabets and from these the cipher substitutes for the plaintext letters are taken. A typical square is shown below:



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

Encipherment by the Four Square method is relatively simple as one rule governs the entire operation.

The letters of the message to be enciphered are divided into pairs. The first letter of the plaintext pair is located in Square #1 and the second letter in Square #3. These two cells may be assumed to be diagonally opposite corners of a rectangle. The cipher substitutes for these two letters may then be found at the other two corners of this imaginary rectangle, the first in Square #2 and the second in Square #4. Using the square shown above, the message, "Come quickly, we need help", would be divided and enciphered thus:

Plaintext: **Co me qu ic kl yw en ee dh el px**
Cipher: **LE WI XA FN EX CU DX UV DP GX HZ**

As can readily be seen, in the first pair, plaintext "C" in Square #1 and plaintext "O" in Square #3 are represented by cipher "L" in Square #2 and cipher "E" in Square #4, these four letters being at the corners of the imaginary rectangle established by the location of the two plaintext letters. All other cipher pairs are derived in the same way.

Decipherment, when the keywords are known, is accomplished by reversing the encipherment process. The cipher letters of each pair are located in Squares #2 and #4 respectively and the plaintext letters which they represent are then found in Square #1 and #3. This can be illustrated by the decipherment of the following message:

X F W X P O D Y D G G N A H I X N S N Q A K E Q A
L L V Q H W X L V Q Q G N K U.

Divide the above message into pairs and decipher, using the GEOM(E)TRY - LOGARITHM square. The solution is:

Cipher:	XF	WX	PO	DY	DG	GN	AH	
Plaintext:	Su	pp	li	es	an	da	mm	etc.

IDENTIFICATION OF THE FOUR SQUARE

The following characteristics help to identify the Four Square as a cipher of that type.

1. It is a substitution cipher.
2. The cipher message will contain an even number of letters.
3. A frequency count will show not more than 25 letters.
4. In English, the letter "J" will ordinarily be omitted.
5. When the cipher message is separated into pairs, doubled letters may occur, which eliminates the possibility of a Playfair.
6. If any long repeats occur they will be at irregular intervals.
7. In most cases repeated sequences will be composed of an even number of letters.
8. Few reversals in comparison with Playfair.

PECULIARITIES OF THE FOUR SQUARE

1. A plaintext letter can be represented in the cipher by itself.
2. Any given cipher letter can represent 5 plaintext letters.
3. Any given plaintext letter can be represented by 5 cipher letters.
4. A cipher letter can represent itself or the other letter of its pair.
5. The fact that the plaintext squares of the Four Square arrangement contain straight alphabets makes it possible to calculate the probable frequency of every cell in both cipher squares.
6. The fixed positions of the letters of the plaintext alphabets (#1 and #3) makes it possible to definitely spot the location of probable words which form a pattern when enciphered by Four Square.

SOLVING THE FOUR SQUARE

As is the case in the solution of all ciphers of this general type, the solver's goal is the recovery of the cipher alphabets. Having determined, by means of the identity tests listed above, that a message has been enciphered by Four Square, the initial steps of the solution are practically the same as those recommended in the solution of a Playfair.

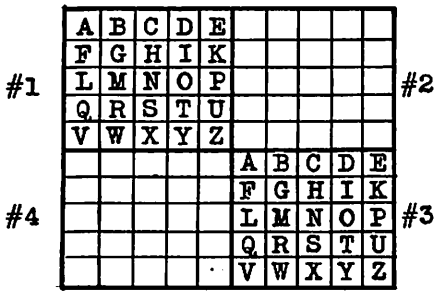
The individual letter frequency count will yield positive results in revealing probable position of cipher letters, as the fixed letters in the plaintext alphabets reflect their frequency in the cipher letters which represent them. Letters of high, medium, and low frequency can all be placed with an amazing degree of accuracy.

A digraph frequency count is also important because, as in the Playfair, any given plaintext digraph has but one cipher digraph substitute. In the square used to illustrate the method of encipherment, the plaintext digraph "TH" must always be represented by the cipher digraph "IP". Thus, in a message of sufficient length enciphered from this square, the cipher pair "IP" may be expected to be found among the cipher digraphs of highest frequency.

A vast amount of statistical work has been done by cryptographers to determine the normal frequency of both individual letters and digraphs in English text. Tables have been compiled which are available to the solver for reference, such as Meaker's Charts in Elementary Cryptanalysis.

As mentioned above, the fact that the plaintext squares contain straight alphabets, makes it possible to calculate the probable frequency of every cell in both cipher squares. The method of accomplishing this has been explained by several writers on the subject and will be briefly summarized here.

In Four Square the standard set-up of the square is always the same and is known to the solver. It is illustrated below:



In accordance with the rule for encipherment, if any plaintext letter of Row 1, Square 1 (A B C D E) is paired with a letter of Column 1, Square 3 (A F L Q V), then the first letter of the resulting cipher pair must be found in Row 1, Column 1 of Square 2. There are 25 such plaintext combinations which, when enciphered, will produce this result. These are listed below:

AA	BA	CA	DA	EA
AF	BF	CF	DF	EF
AL	BL	CL	DL	EL
AQ	BQ	CQ	DQ	EQ
AV	BV	CV	DV	EV

Reference to Meaker's Digraph Frequency Chart shows the values for these pairs, based on a count of 10,000 letters of English text. However, before giving these values, it is considered advisable to point out that Meaker's table is based on a continuous digraphic count wherein every letter of the 10,000 (except the last) is used as the first letter of a digraph, the second letter of which is the next letter on its right. This can be illustrated with a short example, thus:

Text: Come quickly
Digraphs: CO OM ME EQ QU UI IC CK KL LY

This continuous count results in 9,999 digraphs from Meaker's 10,000 letters; 10 digraphs from the 11 letters in the above example; and in text of any length, just one less digraph than the total number of letters. Thus, Meaker's count may be considered to be based on 9,999 first letters and 9,999 second letters of digraphs as each letter is used twice, except the first and last.

In a Four Square cipher the digraphic separation is not the same as the example of Meaker's count shown above. Therefore, since in Four Square the plaintext is separated into pairs before encipherment, it follows that only the odd numbered letters may serve as first letters of a digraph. For the same reason, only the even numbered letters may be the second letter. Hence, frequency of the cipher letters in each square is based on half the total number of letters in the message, or, on the number of digraphs.

Meaker's chart, based on a count of approximately 10,000 digraphs, shows the following values for the 25 plaintext digraphs which force the first letter of the resulting cipher pair into the cell at the intersection of Row 1, Column 1, Square 2.

AA - 1	BA - 8	CA - 44	DA - 45	EA - 131
AF - 10	BF - 0	CF - 1	DF - 12	EF - 23
AL - 77	BL - 21	CL - 16	DL - 7	EL - 46
AQ - 1	BQ - 0	CQ - 0	DQ - 1	EQ - 14
AV - 24	BV - 0	CV - 0	DV - 4	EV - 16
113	29	61	69	230

Total 502

As shown by this tabulation, if 10,000 pairs are enciphered by Four Square, there are 502 expected appearances of the cipher letter which would fall in the cell at the intersection of Row 1, Column 1, of Square 2. Thus, as 502 is approximately 5% of 10,000, this cell may be considered to have a frequency expectation of 5 per 100 digraphs.

In like manner, the probable frequency of every cell of squares 2 and 4 may be calculated. Approximate whole number results of such calculations are the values shown in the square below and these figures represent normal Four Square cipher letter frequency per 100 digraphs. That is, a message of 200 letters (100 digraphs) should show approximately 5 appearances of the cipher letter in Cell Row 1, Column 1, of Square 2; and approximately 4 appearances of that in Row 1, Column 1, of Square 4.

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

2

The Four Square cipher frequency values have, for convenience, been streamlined into five groups of five; and all the cells of each group have been assigned the same numerical value. In using these values it must be remembered that they are merely probable values and, in short messages, a variation from them must be expected. Such a variation is particularly likely to occur between adjoining groups. However, in most cases, frequency can be relied upon and, if a choice for location in the cell at Row 2, Column 2, Square 2, lies between two cipher letters having frequencies of 6 and 2 respectively, one is safe in selecting the letter of lower frequency as the most probable candidate for that location.

It is also interesting to note that the normal Four Square frequencies closely follow the normal distribution of plaintext letter frequency, as illustrated below:

	High									
Letter	E	T	A	O	N	I	R	S	H	
Norm. Plain Freq.	13	9	8	8	7	7	7	6	6	
Norm. 4-Sq. Freq.	8	8	8	8	8	5	5	5	5	5
Square #2 - Cell	44	14	13	34	43	12	45	24	11	35
Square #4 - Cell	13	44	34	24	45	14	12	15	43	35

	Medium						Low									
	L	D	C	U	P	F	M	W	Y	B	G	V	K	Q	X	Z
	4	4	3	3	3	3	2	2	2	1	1	1	0	0	0	0
	4	4	4	4	4		2	2	2	2	2	1	1	1	1	1
Sq. #2	31	33	32	23	15		25	41	21	42	54	22	55	53	51	52
Sq. #4	31	41	23	33	11		22	32	42	21	25	54	51	55	53	52

In the above tabulation the cell numbers indicate their row and column, the first figure being the row and the second the column, that is: Cell 32 indicates Row 3 and Column 2. This numeration will be used hereafter in all cases for cell identification.

Although combined into groups of equal value, the cipher square cells are listed above in the order of their actual calculated frequency value, which is in some cases greater or less than the streamlined value adopted.

In addition to the foregoing strictly analytical process of attacking a Four Square, there is, as in all ciphers, the "probable word" method of making an entry; and the Four Square lends itself admirably to solution by means of probable words.

There are several different procedures for spotting probable words all of which are variations of the same basic idea and all of which arrive at exactly the same result. One example will serve to demonstrate how a probable word may be located in the cipher.

The following message is enciphered by Four Square. It is thought that the word "Colorado" may be in the message.

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

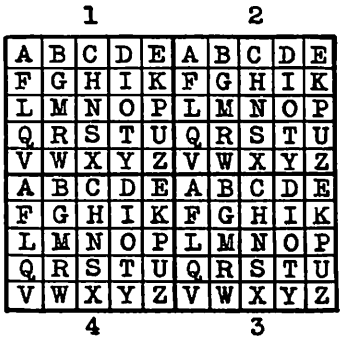
Divided into pairs this is:

BY DG VS OT WS PC FQ QE QY VC IH LE PG MI LQ WI LY WI LA UN
OK RY PH PC LR

Now, if the word "Colorado" is present, it must be divided in one of these two ways.

CO LO RA DO or -C OL OR AD O-

Set up a standard Four Square with straight alphabets written in all of the squares.



Test for the probable word "Colorado" by enciphering it in both separations, thus:

Plaintext: Co lo ra do
Cipher: DN OL QB DO
* *

Note that the first letter of both cipher pair one and cipher pair four is the letter "D" which occupies Cell 14 of Square 2.

It is an inherent characteristic of the Four Square that, with straight alphabets in the plaintext squares, regardless of how the cipher alphabets may be written, whenever CO LO RA DO is enciphered the initial letter of these two cipher pairs will always be the letter located in Cell 14 of Square 2.

The other separation is tested in like manner.

Plaintext: -C ol or ad o-
Cipher: LO MT DA

No pattern is disclosed for this separation of the probable word.

Inspect the message for the pattern *- -- --*- which was shown to be that of the separation CO LO RA DO. It will be found that there is one such occurrence of this pattern at LE PG MI LQ in the message and this group of letters may be accepted as the encipherment of the plaintext word, "Colorado".

With a knowledge of these fundamentals, one can attempt the solution of a secret message enciphered by Four Square. The following example will serve to demonstrate how this knowledge may be applied:

THE STOCK EXCHANGE CIPHER

The following message was sent to a stockbroker by one of his customers. The Four Square system was employed by them for such confidential correspondence. The investor was known to be selling "rails" and was believed to be interested in gas pipe lines and utilities, particularly, Transcontinental, Texas Eastern, Consolidated, and Columbia. The message was written in pairs as shown below.

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

SOLUTION

The message is copied on quad-ruled paper, leaving at least two blank spaces between the lines. The pairs can be kept intact and space saved if the first letter of each pair is written close to the right side of its cell and the second letter of the pair is written at the left side of the adjoining cell. In this way all cells are used but a distinct space shows between the pairs.

A frequency count is made employing the method illustrated. The vertical center alphabet serves to show the second letter of pairs formed with the letters on the left and the first letters of pairs formed with the letters on the right. This gives, in one operation, both an individual letter and a digraph count. The result shows that the message contains 100 digraphs formed from two alphabetically different sets of 100 letters each, distributed as shown.

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

As there are exactly 200 letters (100 digraphs) in the message, the number of appearances of each letter in each alphabet gives its actual cipher frequency. Thus, for this message, cipher "A" has a 1st Letter (Square 2) frequency of 2, and a 2nd Letter (Square 4) frequency of 5. A comparison with Normal Four Square Frequency is shown below:

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

The frequency count has also revealed the repeats in the message and it is well to set these down for future reference.

Long Sequences

FO WQ CF PE - 2
QI WP - 3

Repeated Digraphs

FO - 4 CF - 3
QI - 4 HQ - 3
WP - 3

Reviewing the known facts concerning the message, it is obvious that one or more of the names of the companies listed might be present in the cipher. They are tested in both possible separations with the following results:

Plain: Tr an sc on ti ne nt al T ra ns co nt in en ta
Cipher: RT CL SC NO TI PC OS AL QB NS DN OS HO CP QD
(* under CL, AL, QB, QD)

Plain: Te xa sE as te rn T ex as Ea st er n
Cipher: UD VC UC CQ UD SM CZ CQ AE TS BU
(* under VC, UC, CZ, CQ)

Plain: Co ns ol id at ed C on so li da te d
Cipher: DN NS LO ID DQ DE NO TN OF AD UD
(* under DN, DQ, DE)

Plain: Co lu mb ia C ol um bi a
Cipher: DN PQ MB FD LO RP DG

The cipher message is inspected to see if any of these patterns appear and it is found that the pattern for TRANSCONTINENTAL does not show for either of the two separations. The fancy pattern for TEXAS EASTERN in its first separation does not show but the rather common pattern of the second separation (*- *-) shows in four places.

Plaintext: T ex as Ea st er n
Test Pattern: *• *• •• •• ••

Message - 1 LP LT OF YQ CD Satisfactory.
(* under LP, LT)

Message - 2 EW EA VT YP QS Satisfactory.
(* under EW, EA)

Message - 3 EO EX GT LV PX No good - two patterns.
(* under EO; *- under EX; - under PX)

Message - 4 LB LO QO DP SY No good - two patterns.
(* under LB; *- under LO; - under QO)

The pattern for CONSOLIDATED, in its first separation, shows at:

Plaintext: Co ns ol id at ed
Test Pattern: *• •• •• •• *• *•

Message LH DI OP MM LA LT
(* under LH, LA, LT)

The second separation of CONSOLIDATED and both of those for the last probable word, COLUMBIA, fail to show a pattern.

As the pattern for CONSOLIDATED is of a more unique form than that of TEXAS EASTERN, it will be tried first. The Four Square is set up and the cipher letters are placed in the proper cells, thus:

Cipher: LH DI OP MM LA LT
Plaintext: co ns ol id at ed

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

This looks very promising and the consecutive letters, L and M in Square 2 and H and I in Square 4, indicate that in all probability, vertical keyword alphabets were used in the cipher squares. A check against the cipher frequency expectancy tabulation shows this:

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

This comparison shows that the frequency of all of the ten cipher letters, with one exception, closely approximates the normal Four Square frequency of the cell it occupies. As only cipher letter "D" in cell 43 of Square 2 is at variance with the expected frequency, the existence of the plaintext word, "consolidated", is not only probable but is now highly possible. The other digraphic combinations of these cipher letters are made and the following additional values are found. All of these give acceptable digraphs.

Cipher	Plaintext
LI	ct
MP	io
MI	ht
DP	to

These plaintext pairs are written below their cipher substitutes in the message and it is observed that a long fragment of another plaintext word is formed. This not only confirms the fact that the assumed word, "consolidated", is correct but opens up another avenue to explore.

The fragment of the new word is located in that part of the message shown below:

Cipher: QI WP LB LO QO DP SY BP QI YL LI MP DI OD NM
Plaintext: on ct io ns

The letters "ctions" could end any of several plaintext words such as "connections", "directions", "constructions", "productions", etc. This is a positive result from the assumption of the existence of "consolidated" in the message and must be exploited to its fullest extent. However, instead of idle guessing, one should try to develop the plaintext from the facts available.

As mentioned previously, the position of "L" and "M" in square 2 and "H" and "I" in square 4 indicate a vertical write-in of the cipher squares. Assuming such to be the case and working first with square 2, "L" and "M" in column 4 must be followed by letters from among "N", "P", "Q", etc., as the letter "O" is already placed in Col. 1. Reference to the square showing normal Four Square cipher frequency discloses that cells 34, 44, and 54 of Square 2 have a probable frequency of 8, 8, and 2, respectively.

The frequency count for this message is shown below for the square 2 cipher letters which are eligible for these cells.

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

Of the above, the frequency of "N" is obviously too low for cell 34 and that "Q" is too high for cell 54. It would seem that the best choice of possible letters for the remaining cells of Col. 4 are "P" in cells 34, "Q" in cell 44, and one of the remaining low frequency letters in cell 54.

Tentatively placing "P" and "Q" in these cells, the only plaintext pair that can be added is:

Cipher QI = Plaintext ST

This not a very great addition to what is already known, but it is interesting for these reasons.

Cipher QI has a digraphic frequency of 4.

Cipher QI is certainly part of the plaintext word ending "ctions".

Cipher QI WP is repeated 3 times.

Consider the thrice repeated Q I QP. Cipher "P" has already been located in cell 34 of square 4. Then, still assuming that the cipher alphabets are written vertically, the possible plaintext for QI WP, with "W" in all possible positions, would be:

"W" in:	1st Col.	2nd Col.	3rd Col.	4th Col.	5th Col.
	st dl	st dm	st dn	-- --	-- --
	st il	st im	st in	-- --	st ip
	-- --	st om	-- --	-- --	(st op)
	st tl	st tm	-- --	-- --	st tp
	st yl	st ym	-- --	-- --	st yp

Plaintext "stop" is accepted for several reasons, namely:

1. It is good probable plaintext.
2. It is logical because "stop" may well have been used several times as a sentence divider.
3. Cipher "W" is located in a proper cell.

And so, with the acceptance of "stop" as a correct plaintext word, cipher letters "P", "Q", and "W" are placed in Square 2 giving this:

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

Returning to the cipher, the additional plaintext pairs can be written in as shown.

```
QI WP LB LO QO DP SY BP QI YL LI MP DI OD NM
st op          on       st    ct io ns
```

Inspecting the squares as now partially filled, it is evident that only "K" or "L" can be placed in cell 53 of Square 4. "K" is more probable for this spot due to its zero frequency, but "L" also is of low frequency, so neither can yet be placed with certainty.

In column 4 of Square 4 only "N" or "O" can go into Cell 24. Testing "O" at this location gives:

Cipher QO = Plain TI and Cipher LO = Plain DI

The above fits well with the adjoining pair giving this:

```
Cipher:    LB LO QO DP SY
Plain:        di ti on
```

Also in Column 4 of Square 4, "Q" and "R" by their frequency practically place themselves in Cells 44 and 54 respectively.

Having located "O" at Cell 24 of Square 4, the high frequency digraph "FO" can be considered and the probability that it is the substitute for plaintext "TH" becomes almost a certainty when it is noted that this combination results from placing cipher "F" below "D" in Column 3 of Square 2.

Above "D", in the same column, only "C", "B", or "A" can be placed. When it is observed that cipher "BP" gives plaintext "IN", "B" is accepted for Cell 23 of Square 2 and the recovered plaintext is expanded, thus:

```
Cipher:    QI WP LB LO QO DP SY BP QI YL LI MP DI OD NM
Plaintext: st op    di ti on    in st    ct io ns
Probable:       ad          al       ru
```

Placing all of these letters in their proper cells builds up the square to this extent:

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

Several new plaintext values can now be located in the message. Examine the first part of it which shows this:

Cipher:	UL	RQ	GW	FO	WQ	CF	PF	FG	EA	GX	LH	DI	OP	MM	LA	LT
Plain:				th	ou						co	ns	ol	id	at	ed

The three pairs, CF PF FG, all of which contain "F", appear to be the best spot to continue the attack. If "F" of Square 4 is not in the keyword it must be in either Cell 13 or 23. These are tested thus:

Cipher:	FO	WQ	CF	PF	FG	EA	GX	LH	DI	OP	MM	LA	LT
Plaintext:	th	ou						co	ns	ol	id	at	ed
If "F" is in 13				nd									
Then "G" is in 23					sh								
Giving	th	ou		nd	sh			Co	ns	ol	id	at	ed
Probable			sa			ar	es						

This is accepted and the additional letters are placed in the cipher squares, further completing the recovery, as shown below:

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

With this much recovered, no black magic is needed to visualize the plaintext which starts the message. Testing cipher letters in their most logical cells gives the following for the opening words:

Cipher:	UL RQ GW
Plain:	Bu yt en

The completion of the solution is now purely mechanical and the remaining open cells of the cipher squares are filled in without difficulty, revealing keywords STOCKEX(C)HANG(E) and BUYANDSEL(L).

Having completed the solution of a Four Square cipher, the following items may be noted.

1. Nulls are not necessary for encipherment as in Playfair.
2. Probable position of letters can be spotted through cell frequency.
3. Probable words can be definitely placed if they produce a pattern.
4. The Normal Cipher Frequency Squares are of great assistance in verifying position of letters.
5. As in all ciphers, a probable word provides the surest method of making an entry.
6. Analysis produces more concrete results than is the case with the Playfair.

THE FOUR SQUARE WITH MIXED ALPHABETS

The foregoing was an example of the solution of a standard Four Square. Messages enciphered by this system can be made more difficult of solution if the cipher squares are scrambled. If all four of the squares are scrambled, and there is no reason why they should not be, then the solver is confronted with a still tougher problem as assistance from the Normal Four Square Frequency tabulation is lost when straight alphabets are not employed. Also, probable words cannot be spotted with the pin-point accuracy that is possible when straight plaintext alphabets are used.

However, digraphic and longer repeats will still show and experienced cryptanalysts will be able to make an entry by means of the frequency count and the old reliable "probable word".

The possibility of success under these conditions is greatly enhanced when the solver has sufficient material to work with, that is: a very long message or a number of messages enciphered from the same four mixed alphabets. The amateur solver is not apt to have access to a large volume of material, identically enciphered, as is the case with military cryptanalysts. As a single short message enciphered by Four Square with all alphabets scrambled would present an extremely difficult problem for even the experts, no attempt will be made here to outline the solution of a message enciphered by that more elaborate process.

FOUR SQUARE PROBLEMS

1. Natural Resources. 'gas but gas' ZEMBIE

QL HY LG NV LN TV PK PY AK HD SC CD PY CY BL CX EY YA ED CV BK
IO OM CO CM HD PY TO OC PB RY OC QB KP CO CY MK IB II RG HF BH
AK IG BL QL HY LG NV CD TR SV DU CD QL TX HD CY RQ DK HV TZ TX
KM HV FM EP LL QB TO HX BF XK PY GM LN CV CX RS TV QN OB ZP SK
CE IF IO YA CO NK HF IF IT CG HF DC GM HV RM EN GM OC HI RY YQ
PH YK NY SB.

2. Random Thinking. 'anasonly' ZEMBIE

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

3. Math. II at Pyramid U. 'column' many times. ZEMBIE

Ancient Egyptians used a much different method for multiplication than that with which we are familiar. Strange to say, it seems to have worked just as well. The examples show how they did it. As you can see, the number below the second column of figures is the product of the two numbers at the top of the columns. The method is described in the message below.

6 X 3	10 X 10	19 X 43	43 X 19
3 6	5 20	9 86	21 38
1 12	2 40	4 172	10 76
18	1 80	2 344	5 152
	100	1 688	2 304
		817	1 608
			817

EH GS MB YQ QO KF WL FD KF OO EH XT QH KS RI SP KV BX FP AH LG
QH GS DK MT XG QO HA LH DK BK SG GG AH LG GK QS OI QS BO KT GT
KT QH FH DR QH OB OO VY XY KF OY KF WL FD KH BT WE GS DK BK SG
XG DE NO YH DR QH FR BQ VS KK QR MT DN WO AG PR EH GS DR DT FH
DP LH BK AW NN DN EQ WH OK QN XP DC MZ DK WO AG PR EH GS MB YQ
QO KF WL FD QO WH KE KQ VY XG LG EH EH ED BK SG GM EH GS DR DT
FH DP LH BK FW.

4. A Prophet with Honor. 'istoin' ZEMBIE

OH OR CE HO RS CG OL XY HA FB LO CM UA MQ ET GR GA OM DG LQ EA
TF BB HQ QQ MM OB SR IE BG DE FD MR GI NP SO IT TN MH HF OB RR
CI NP SN HG PT KT CK RM RR NE KO LG NT MI HS BQ RZ QQ MB TE BG
OL UG TD HC RP EA ST HG FF TP RR SI ML CE SI OK ML BA FB KU SI
MR OL FP TF NT BQ TG BG LH KS TX BG KQ ET QV GQ RQ ZP TD.

5. Popular Flavor Source. 'dollars' repeated. S-TUCK

QK AW HP TH ZB NW RL ZE LC NT SM QK AZ GP KE SP QK VZ NT BM FE
LC NT CP SP BC QK AY IS NT AM AR DS TH AH YP DI FI RK ZE RB ET
NZ SH GQ DI TC CP TB FE KD OL KT PY SP CD DI LC NT OI TC UE MR
IS IR TH FI MC RO VI KI FM FE QV MS RV CB QY NT IK KD DI OC XV
OH TH NT VH TC YF RV BL RF MC ME ZE KD KP ZC FA IS FM FE QV MS
TF MP KI VX TH RV DI UH TC AP DH VH KI LD TC NQ.

6. Characteristics of Pets. 'people' C.SHARPE

NP YZ LC UN IE FH HI RH TG PU QR EC SR RX MA KR IC BQ BA PG YR
EC SR TD AC ME QY VA CV BQ YU GR QK RW DN PD YF QH BQ DA IR EC
KU KQ KD XL NP WL GQ NP YZ IO ZD YD GQ PX QP CC IE FH GS TQ GD
PU GQ OV IQ YQ MH YD SI PG DW NA IS RC HK DR TT YW NA RR IV PQ
IR HQ IS PD YF QH BQ DA GT TC QP NR FH QK OX RN PD EC QE MN QX
CG QF BQ RH RF HQ RC QQ WL YI DR MF PI RN QL NM.

7. Berry Picking Time. 'hidden' 'shade' I.N.JOYUM

OS UK RU NC UU QR RU IE CK OS UK RU QM AF HT QT BI FI NI QG XR
BC EC DA VL YM QU DS QI SR QT CA XS RF BR II UZ PN LK PH OU TC
OP KU TG KB SM OS RU GA EC NT RF MH OK RN OC QR HP HM XR UU PK
TQ FA PK HL LO RI RU OS UN LM DA IB IG GE LO SM OS LD IQ QG ET
LQ BM IQ DS LE QR QH NU DB IA.

8. Pseudo Science. ZEMBIE

An accident in a laboratory demonstrates an unaccepted law of nature which may be stated briefly in these words: A result produces the cause there-of.
Probable words: EXPERIMENT-EXPLOSION-UNIVERSITY-PROFESSOR

TV LT FA DE LI FA AG TO KF OI CM IQ QP KM PQ PO CM MI MP FT RP
AB OK QY AU PA PY PQ NK EC TO AG TG GQ PT CI SI KT IC UN HB BA
IQ CI DS TC ME PF PW OP AU TU CI BF IL EI OU TO OP RK HO EF TU
IP UP QC RU QI SC IV RB AM PC NH BQ GF TL AU PR EC HO AL OP SL
HG TU ZE IQ ZM UP BQ CQ II SE AF QF RU PD PU BD KB AZ YF SR TA
PY.

FOUR SQUARE SOLUTIONS

Note: In order that these answers may not, inadvertently, give unwanted help to those who want to solve the problems, they are enciphered by various Alphabet Run-down methods, separate word lengths or groups, diagonal letters, words or groups, zig-zag, steps, etc. However, all will readily yield the answer when the run-down is carefully inspected. In no case is it necessary to run-down more than ten letters.

Practice Example. Page 31.

0. (FDNLDSQX - KNFZQHSGL)
TQZMHTL ENTMC HM RNTSGDQM * * * * * * * * * * * * *

Problems.

1. (PAYDJ LILDV - LNKZQ ZQFLK)
PDAPD OBBDO AWPPN BXPRO AO--- * * * * * * * * * * *

2. (ISUPV OMPAY - UGBSK NGKPN)
ZKXJO GGKGN SFXPC DYJKP MRPPJ * * * * * * * * * * *

3. (EMDLAHDQ - XZRIMCTGL)
CH OCZ BENOP ZLIRJK AMLRGLSC SN * * * * * * * * * *

4. (EMOKHBXYKC - JCSYMFXQFA)
Z E B P L Y K Q B F L J Z P T F N A X J B S I Y S C A

5. (RWJFIIY ZCWJO - BUQPYAP KB SXKGJJW)
PDB JLQR CTLAKPFTC ZAWJ FK QFC * * * * * * * * * *

6. (XJKT YWPO - YJBDNCGT)
PDAU NVT WJEIWHO MZAGZXO PDAEN * * * * * * * * * *

7. (OTQOKD EPYNCQ - YIXZH XANNEAO)
OCZ ADRS ZCPPGCQ IFHB PDA WZNO * * * * * * * * * *

8. (AXP PEO QXI A-PC EPK KDP WMF)
WVM QKE IXL AKE WDC ZFL OZG AKR ECG C-- * * * * * *

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