PRACTICAL CRYPTANALYSIS

by

WILLIAM MAXWELL BOWERS

VOLUME III

THE TRIFID 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 III

THE TRIFID CIPHER

By

William Maxwell Bowers

AMERICAN CRYPTOGRAM ASSOCIATION

1961

To

William F. Friedman

The Master Cryptologist

C O N T E N T S

C O N T E N T S

INTRODUCTION

I'll tell thee everything I can;
There's little to relate.
Lewis Carroll

F. DELASTELLE - HIS LIFE AND TIMES.

The Trifid may not be the most complex of the numerous methods of encipherment devised by the clever Frenchman, F. Delastelle, but it will do, in so far as this student of the science is concerned, until someone produces a tougher one. However, no matter how secret and mystifying a message enciphered by Trifid may appear to be, the enigma of the man who originated the system, is greater.

F. Delastelle - who was he ? That is the question ! ! !

The writer's interest in this subject goes back to the winter of 1954-55, when the major portion of what is contained in the following pages was prepared. At that time it was believed that a short biographical sketch, of Delastelle, would be appropriate as introductory matter and also, would 'pep-up', to some extent, a treatise which was doomed to be rather heavy reading, at best.

With this thought in mind, various items of cryptologic literature were consulted for biographical information. From these sources, absolutely nothing was learned other than the fact that certain books, bearing the name of F. Delastelle as author, were published in Paris during the decade, 1892 to 1902. These are:

Cryptographie nouvelle assurant l'inviolabilité absolue des correspondances chiffrées. Paris: P.Dubreuil, 1893.

Cryptographie universelle. Paris: 1893.

Traité élémentaire de cryptographie. Mathématiques appliquées. Paris: Gauthier-Villars,1902.

Numerous authors gave descriptions of the Delastelle systems and made mention of his books,but nothing was said about the man who wrote them, except in Chiffrebyråernas insatser i världskriget till lands (Activities of Cipher Bureaus in the World War), Yves Gyldén, Stockholm, 1931, where he is referred to in this way.

> "Works of the various military authors, Viaris, Valerio, Kerckhoffs, and Bazeries, as well as some by the mathematician, Delastelle, may be considered to be standard within certain limits."

This comment seems, at least, to remove Delastelle from the military catagory. Also, it would appear to indicate that the name, F. Delastelle, was not merely a nom de plume. On the negative side, Commandant Bazeries, a contemporary, makes no mention, whatsoever, either of Delastelle or of his systems, in his book, Les chiffres secrets dévoilés (Cipher Secrets Unveiled)Paris, 1901.

When it was found that nothing could be unearthed by personal research, several friends in the A.C.A. were contacted. Results were zero. Following this, a governmental agency was requested to aid in the search for information. After about a month, this report came from that source.

> "I did not think that it would take as long as it has to get negative answers with regard to Delastelle. There is nothing on record in this country and I can say this as a result of a search by our library consultants among all available sources."

And later:

> "It seems that the man never existed, but for his books."

Meanwhile, the writer had been trying his luck in other directions. A letter was dispatched to the French Embassy in Washington, and an answer was received from the chief of their Cipher Division which said, in part:

> "The documentation the Embassy has on the subject did not prove sufficient and I therefore forwarded your request to the Ministry of Foreign Affaires in Paris and I will soon be in a position to send you, directly, the information you require."

That was encouraging news but, unfortunately, it was the last that was ever received from that correspondent, although several additional letters were written in the hope that at least some of the promised information might be pried out of him.

Delastelle's Paris publishing company, Gauthier-Villars, was also tried. A representative of that firm replied, in part:

> "Nous avons recherché dans nos archives si nous possédions des documents au sujet de M. Delastelle afin de pouvoir vous aider dans votre travail. Malheureusement, nos recherches sont restées vaines."

The above can be roughly translated thus:

> "Sorry - but we can't find anything on him."

Eventually, about a year and a half after the search started, an inquiry addressed to the U.S.Embassy in paris was referred to Miss Emma Jane Gammell, Asst. Director, USIS Library, Paris. From Miss Gammell came the first positive results. In a letter dated 29 March 1956, she said:

> "We are glad to be able to transmit the following information which the head of the Section du Chiffre, Etat-Major de l'Armée, has sent us."

> "Félix Delastelle was born at St. Malo, January 2, 1840 and died at Saint-Ideuc in Paramé, April 1, 1902. He was Inspector of Tobacco. No information on his education nor how he happened to be interested in cryptography."

Pursuing the search further, it was learned from Les Archives Nationales that Delastelle was an Inspector of Tobacco at St. Malo in 1878-1880. No other information was derived from that source.

At a still later date, Miss Gammell reported that a notice in Figaro, of April 1902, stated that a certain M. Delastelle died, enroute to the funeral of his brother in Brittany. She had hoped to find an obituary, but had not succeeded. Shortly after this, Miss Gammell left her station in Paris and her efforts to aid in the search were terminated.

In the Spring of 1961, when work on this treatise was resumed, a letter was dispatched to Gen. Luigi Sacco, at his Rome address, asking if he could supply any additional biographical information on Delastelle. As had been the case with others, his prompt reply was mostly negative, with the exception of this comment.

> "The French edition of Traité élémentaire de cryptographie of Delastelle is included in a series, 'Mathematiques appliquées', which seems to confirm the opinion expressed by Yves Gylden.

And also:

> "But, on the other hand, the 'Traité' allots the 'Septieme Partie' to the 'Cryptographie militaire', which shows a special military interest and seems to qualify Delastelle as a military engineer."

At about the same time that Sacco was consulted, a letter went to the Section du Chiffre, Etat-Major de l'Armée, from which office Miss Gammell had received the greater part of the information that she had been able to supply. This letter was not answered.

And so, as of this date, these few meagre facts represent all that is known about F. Delastelle on this side of the Atlantic.

WMBowers

Clarksburg, W.Va.
July 1961

THE TRIFID CIPHER

THE GENESIS OF THE TRIFID

The term, trifid, is not a coined word. It is to be found in any standard dictionary. Webster defines it thus:

> trifid (trī′fĭd) adj. (L. trifidus, from tri- plus root of findere, to split.) Three-cleft, tridentate.

Pursuing this bit of intelligence a step further, it will be found that 'tridentate' is defined as: "having three teeth, or points". And so, as it applies to the cipher system now under discussion, the word, trifid, may be considered to mean:

"Divided into three separate parts or components."

Felix Delastelle, the French mathematician who put the word into cryptographic glossaries, used it to describe one of a series of related methods of encipherment which he devised. In his Traité Élémentaire de Cryptographie, Delastelle outlines their development. Under the heading of Complex Substitution he takes up the encipherment of polygrams, a word which, for cryptographic purposes, may be defined as a related group or sequence of two or more letters or other characters. In explaining what he is trying to accomplish, Delastelle makes this statement:

> "Enciphering by polygrams is characterized by the fact that all the letters of a plaintext group participate in the determination of the letters which form the resulting cipher group."

From this, he goes on to say that the broad term, polygrams, includes digraphs (groups of two), trigraphs (groups of three), and other groups of higher order. Since a digraph is the polygram of lowest order, Delastelle considers it first. To obtain a table of digraphs for encipherment purposes, he lists all possible two letter arrangements of the letters of the alphabet. This consists of combining each letter with itself and with all other letters as shown below.

AA, AB, AC, - - - to - - - ZX, ZY, ZZ

He then places this list side by side with another list of the same pairs, arranged in some methodical order that is not alphabetically consecutive, as was the case with the first. One list represents the plaintext digraphs and the other, the corresponding cipher digraphs. As these tables must each contain 625 or 676 sets of digraphs, depending upon whether a 25 or 26 letter alphabet is used, and as both an enciphering and a deciphering table must be prepared, Delastelle came to the conclusion that such a

system was too cumbersome for practical cryptographic purposes and left much to be desired in other ways. In his own words, he says

> "These simple and easily applied procedures are not difficult in operation, but the formation of the table of digraphs is a long and laborious task. We must, then, find a process which is simple and practicable and which will allow us to do away with these tables; just as the sliding alphabets allowed us to do away with the Vigenere table and others of similar type. After very long research, the author has found the solution of this problem and has invented two procedures satisfying the demands; bigrammatic squares and bifid alphabets."

Delastelle seemed to be particularly pleased with the squares which he devised. He devoted many pages of Traité to the results which could be achieved from the use of his bigrammatic squares which he described in this way:

> "A simple alphabet square consists of a square having 25 sections, each of which contains, in a determined order, one of the letters of a normal (25 letter) alphabet. The union of four of these squares constitutes a full bigrammatic square."

Thereafter, follows a description of procedure on which the system, known to members of the A.C.A. as THE FOUR SQUARE, is assumed to be based. In regard to his other invention, Delastelle has this to say about bifid alphabets.

> "We may also encipher by means of alphabets which allow us to break each plaintext letter into two separate parts which, when each is combined with a part of another letter, produce two cipher letters. To form bifid alphabets, we attribute to each letter a group of two signs. As the most simple signs are Arabian numerals, we employ these. Each letter is thus represented by a number consisting of two figures. But, while it is necessary that a different group of figures corresponds to each letter, it is also important that there are as many letters in the alphabet as numerical groups used. If it were not this way, some arrangement of numbers, resulting from the breaking up of certain numerical groups, might not find itself represented and the enciphering would become impossible."

> "This controlling condition fixes, at five, the number of figures to be used. The total different arrangements to be made with five objects, grouped by twos in all possible manners, is 25. This determines the number of letters in the alphabet to be used."

To illustrate, Delastelle then forms a table as shown below.

A - 11	F - 21	K - 31	P - 41	U - 51
B - 12	G - 22	L - 32	Q - 42	V - 52
C - 13	H - 23	M - 33	R - 43	X - 53
D - 14	I - 24	N - 34	S - 44	Y - 54
E - 15	J - 25	O - 35	T - 45	Z - 55

In explaining the encipherment process, he takes plaintext letters from the table, by twos, and writes vertically, under each, its numerical equivalent. The digits of these numbers are then read, horizontally, to derive the cipher letters, thus:

Plaintext:	T R	Cipher ↓	A I	Cipher ↓	T E	Cipher ↓
	4 4	- S	1 2	- B	4 1	- P
	5 3	- X	1 4	- D	5 5	- Z

In all of this, Delastelle speaks only of 'bifid alphabets', and illustrates them, always, in tabular form. The examples he gives show scrambled alphabets but, nowhere, is there any indication that a keyword is used for that purpose. He merely says:

> "To transpose a bifid alphabet, it is sufficient to change the literal series or the numerical series, leaving the other in normal order."

This is OK, except that a random mixed alphabet cannot easily be committed to memory. For this reason, as with a code, Delastelle's alphabets had to be in written form in the possession of the persons who used them. For convenience, he sets up both an enciphering and a deciphering alphabet. One of these is arranged in consecutive alphabetic order with the numbers mixed, the other in numerical order with the letters mixed.

In a section entitled Division of Digraphs by Bifid Alphabets he describes the Bifid Cipher, as it is known to members of the A.C.A., wherein the message that is to be enciphered is divided into periodic groups. He also gives several variations including 'Conjugal Bifid Alphabets' (Conjugated Matrices), 'Multiple Key Series' (wherein a message is first enciphered in one period and the resulting cipher letters are then superenciphered in another period), and 'Irregular Groups' (where the periodic length varies in a single message, as: 9 - 5 - 9 - 5 - 9 etc.). Throughout this entire discussion, Delastelle continually speaks of 'bifid alphabets' in their tabular form. The relation between such alphabets and Bigrammatic Squares is stressed, time after time, but the familiar 5 X 5 square with rows and columns numbered, is neither mentioned or illustrated. Apparently, this convenient substitute for Delastelle's alphabetic tables was adapted to the system by someone else at a later date.

Having accomplished the 'division of digraphs' by his bifid alphabets, Delastelle's next project was the fractionation of the polygram next higher in order, the trigraph. Of this he says:

> "Trifid, or three-number alphabets, are the only practical means known of forming cryptographic trigraphs. Twenty five letters, combined by three in all possible arrangements, would give 15,625 groups. We do not try to compile two lists of this length as they would have to be arranged in tables or in triple entry volumes whose management would be involved and difficult."

Following this, he goes on to explain how letters must be divided into three parts in order to form usable trifid alphabets. To accomplish this, each letter must be represented by a set of three symbols or figures, arranged in such a manner that each

individual set is distinguishable from all others. Each arrangement of this type is called a 'permutation' which may be defined as: 'Any of the total number of changes in position or order possible within a group'.

As has previously been mentioned, the total number of permutations allowable is governed by the number of letters in the alphabet. Controlled by this restriction, Delastelle selected five as the number of different figures required to generate his bifid alphabets. This amount was not selected by chance, but was mathematically determined by the permutation formula which, when repetition is allowed (as 11, 22, 33, etc.) may be stated thus:

$$P = n^r$$

In which: P - Number of permutations with repetitions.
n - Number of different things.
r - Number of things used at a time.

This formula is read: The total number of permutations, with repetition allowed, of 'n' things taken 'r' at a time, is equal to 'n' to the 'r' power.

A normal alphabet contains 26 letters. For a bifid alphabet, the symbols used to generate the digraphs must be handled two at a time. This establishes 2 as the value of 'r' in the formula. The total number of permutations of the symbols employed is also established at 26, the numerical length of the alphabet. Hence, substituting known values in the formula:

$$26 = n^2 \qquad \text{or} \qquad \sqrt{26} = n$$

This will not give a whole number as the value of 'n', but that result can be accomplished if the length of the alphabet is reduced to 25. So that's just what Delastelle did, getting:

$$25 = n^2 \qquad \text{or} \qquad 5 = n$$

The five symbols selected were 1 - 2 - 3 - 4 - 5 and, for the purposes of a Bifid cipher, they are used in all possible arrangements, taken two at a time.

Getting back to Trifids, 'r' is established at 3, because it is trigraphs that are to be developed. This requires that the value of 'P' must be a cubic number, as close to 26 as possible. If one additional symbol is used, increasing the length of the alphabet to 27, then:

$$27 = n^3 \qquad \text{or} \qquad 3 = n$$

All mathematical requirements are now satisfied. Three different symbols are necessary. They must be used three at a time in all possible arrangements. A 27 letter alphabet will result.

Again, as with the Bifid, a set of numerals is used to represent each letter. For Trifids, each set contains three figures, customarily 1 - 2 - 3. Still sticking to the procedure that he devised for dealing with Bifids, Delastelle then prepared trifid alphabets in tabular form. They are illustrated in this way.

Enciphering Alphabet

# - 211	I - 313	R - 112
A - 321	J - 213	S - 322
B - 233	K - 131	T - 232
C - 122	L - 231	U - 133
D - 223	M - 311	V - 113
E - 212	N - 111	W - 121
F - 333	O - 323	X - 331
G - 123	P - 132	Y - 222
H - 332	Q - 221	Z - 312

Deciphering Alphabet

111 - N	211 - #	311 - M
112 - R	212 - E	312 - Z
113 - V	213 - J	313 - I
121 - W	221 - Q	321 - A
122 - C	222 - Y	322 - S
123 - G	223 - D	323 - O
131 - K	231 - L	331 - X
132 - P	232 - T	332 - H
133 - U	233 - B	333 - F

Following this, Delastelle briefly describes the enciphering process. This conforms, in method of procedure, with that which was outlined for the Bifid, the only difference being that the numerical substitutes are sets of three figures instead of two. In both cases the numerical values are written vertically under the plaintext letters and are then taken off, horizontally, to derive the cipher letters. Delastelle concludes by saying:

"Believing it useless to reproduce the details already given on the subject of bifid alphabets, which are perfectly applicaple to trifid alphabets, we content ourselves with giving an alphabet of a new type and with applying it to the enciphering of one message and the deciphering of a second."

And that's how the Trifid was born !

FURTHER DEVELOPMENT OF THE TRIFID

Delastelle's Traité was published in Paris in 1902. He died in April of the same year, perhaps even before his book came off the press. Whether or not his systems were ever employed by the French is not known although it is highly probable that they were not as, otherwise, his book would not have been published when it was. It is alleged that the Italians used the Trifid as a field cipher during World War II and this may well be the case, as the system seemed to find greater favor there than in other nations. The cryptographic manuals of Mario Zanotti (Milano, 1928) and of Gen. Luigi Sacco (Roma, 1936) both devote an appreciable amount of space to Delastelle's Bifid and Trifid systems although little or no information on how to solve them is to be found in either book.

During the period which intervened between the publication of Traité in 1902 and Zanotti's manual in 1928, the two systems had been refined to some extent. For his own purposes, Delastelle had been content to set up bifid and trifid alphabets and let it go at that. Some unknown successor was not satisfied with this seemingly crude method of operation. Cipher blocks were devised and keywords were employed which did away with the necessity of making and preserving random mixed alphabets in tabular form.

As has been shown, there is a definite mathematical relation between the length of the alphabet and the number of parts into which each letter to be enciphered is divided. These, of course, are 2 for Bifid and 3 for Trifid. The nameless cryptologist, who streamlined Delastelle's original methods, realized this fact and

devised cipher blocks for each system which conformed with the requirements of the permutation formula given on page 4:

$$P = n^r$$

The familiar Bifid square, shown below, is ordinarily thought of as a simple 5 X 5 block with external numerical coordinates.

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

It is true that this is merely a 5 X 5 block, but 5 X 5 = n^2, the right hand portion of the formula. This mathematical control can also be graphically illustrated if the same Bifid alphabet is set up in this way.

n = 5

r = 2

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

P = 25

In the case of the Trifid, the block takes the same form.

n = 3

r = 3

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

P = 27

The Trifid block can also be designed in different form for those who like to work with compact matrices. There are several ways of doing this but the block given below will serve to show the idea and its general similarity to the 5 X 5 Bifid square is immediately apparent.

2nd Comp.

1st Comp.

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

3rd Comp.

For the purposes of this treatise, the Trifid set-up will be shown as a 27 X 3 block containing all possible changes in order of the three numbers - 1, 2, 3 - taken three at a time and arranged in ascending order. The numbers within the block, when read vertically, serve as components of the letters of an alphabet which is added, externally, to the block. It looks like this.

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

The fact that 27 letters are necessary for a Trifid alphabet was passed over, lightly, by Delastelle, but it cannot be denied that this is a weak feature of the system. In some foreign languages an accented letter, such as É, is used as the 27th element. As the English alphabet contains no accented letters, an arbitrary symbol, such as #, is forced into service. The appearance of a symbol like that in a cipher message, immediately calls attention to the fact that a 27 letter alphabet is used and helps to identify it as a Trifid.

To overcome this, the 27th element is sometimes represented by selecting a rare letter, as Z, X, or Q, and adding identifying signal letters to it. Thus, if 'Z' is the letter selected, and 'A' and 'B' are the signal letters, then 'ZA' would represent true 'Z' and 'ZB' would represent the 27th element of the alphabet.

Prior to setting up such a message for decipherment, the signal letters must be eliminated, allowing 'Z' to represent itself and substituting a symbol in place of 'ZB'. This move reconverts the number of cipher letters in the message to their true total and allows them to be separated into the correct periodic groups.

This strategy does not mystify experienced cryptanalysts as the signal letter ruse is well known and, whenever a rare letter is always followed by one or the other of just two letters, the finger of suspicion points toward a Trifid.

There is one other matter to which attention should be called in these preliminary remarks. Due to the fact that the Trifid alphabet is written in one continuous line above the standard and never changing numerical tableau, it is always necessary to use a scrambled alphabet in order to prevent many of the letters from being represented, time after time, by the same numerical figures. If this were not done, '#' would always be represented by 333, and 'Z', unless in the keyword, by 332, etc.

One way to produce a scrambled alphabet is to write a keyword horizontally, thereby determining the length of the key block, and then write the remaining letters of the alphabet below the letters of the keyword. The example shown is derived from the keyword, C O U N T E R S P Y.

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

The letters are then taken off vertically to form a scrambled alphabet which is written above the table of numerical components.

Deciphering Table

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

Enciphering Table

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

There are numerous methods of scrambling the alphabet by the use of keyword blocks. Some of those commonly used are shown.

1 - Alphabetical Take-off

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

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

2 - Vacant cells for used letters. Straight take-off.

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

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

3 - Vacant cells with alphabetical take-off.

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

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

There are various other ways of doing this but the scrambling methods illustrated above are sufficient to show the form in which cipher alphabets may be expected to appear for Trifids.

METHOD OF ENCIPHERMENT BY TRIFID

As previously stated, encipherment follows the same general procedure as that prescribed by Delastelle for the Bifid system. The plaintext message is divided into groups of a chosen periodic length and the numerical components are written vertically below each letter. Periodic lengths which are multiples of 3+1, such as 7 - 10 - 13, are popular among constructors with 10 being the one most commonly used. The cipher letters are found by taking off the numerical values horizontally, by threes, and substituting the letter represented by this trio. This can be shown in an example using the original COUNTERSPY alphabet. Period is 10.

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

In the above it is seen that the first plaintext letter, 'C', is represented by the vertical trio, 111; plaintext letter, 'O', by vertical 121; plaintext 'M' by vertical 113; etc.

The first cipher letter, 'C', is derived from the 1st components of the first three plaintext letters, COM, which, when read horizontally, are 111. The second cipher letter, 'N', is derived from the 1st components of plaintext EQU, which are 211; the third cipher letter, '#', is found in the same way. The fourth cipher letter, 'I', derives from the 1st component of the tenth plaintext letter, 'L', and the 2nd components of both the first and second

plaintext letters, 'C' and 'O', which all add up to 312. This horizontal take-off continues, by trios, through the three rows of numbers until all have been converted into cipher letters.

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

It is well to familiarize one's self with the mechanics of the system and several examples for practice are given. The COUNTERSPY alphabet is used.

1 - Complete the Encipherment. Period 10.

D	E	L	A	S	T	E	L	L	E	O	R	I	G	I	N	A	T	E	D	T	H	I	S	S	Y	S	T	E	M
1	2	3							2				2	3	2														
3	3							3	3													1	2	2					
2														2	1	2													
Q	.	.	Z	.	.	Y	.	.	.	.	H	.	.	.	.	.	.	F	.	.	.	.	.	B	.	.	.	.	.

2 - Encipher - Period 7.

C	R	Y	P	T	O	L	O	G	Y	I	S	A	S	C	I	E	N	C	E
						3													
1	1											1	2	1	1	3			
							1												
.	.	R	.	.	.	.	.	.	.	.	O	.	.	.	.	M	.	.	.

Last group contains but six letters.

3 - Encipher - Period 10.

C	R	Y	P	T	O	L	O	G	Y	I	S	A	S	C	I	E	N	C	E
						3	1	2					3	1	3				
																		1	3
										2									
.	.	I	.	.	.	.	.	.	.	.	#	.	.	.	.	D	.	.	.

Same plaintext.

Different period.

Different cipher.

4 - Decipher - Period 10.

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

Accuracy of decipherment will be revealed by the plaintext recovered, which starts with 'The' and ends with 'Delastelle'.

IDENTIFICATION OF THE TRIFID

1 - It is a substitution cipher.

2 - The presence of an additional symbol or the use of signal letters will show that a 27 letter alphabet is used.

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

4 - Repeated patterns will occur, such as:

Period 10 -	Six letter repeat.	A D . . C . . B . .
	Five " "	A . . . C . . B . .
	Four " "	A . . . . . B . .

PECULIARITIES OF THE TRIFID

1 - Naturals, similar to those of the Bifid, are so rare that it is useless to expect to find one.

2 - Each plaintext letter can be represented by 729 (9^3) different arrangements of fractions of itself and other letters.

Note: Sacco states, "It follows that each trigram can be represented, not in 27^3 different ways, but in only 9^3 (729), obviously a number which is still large enough." The writer disagrees with the first part of what Sacco says but sees no need to pursue the matter further because the second part of his statement - "obviously a number which is large enough" - seems to adequately describe the situation, whatever the total may be.

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

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

5 - Repeated plaintext sequences produce patterns which can be recognized in the cipher message.

6 - Repeated cipher patterns do not always represent the same plaintext letters. This will be demonstrated later.

SOLUTION OF A TRIFID WHEN PLAINTEXT WORDS ARE GIVEN

As has been previously shown, the Trifid table of numerical components is composed of twenty seven 1's and a like number of 2's and 3's, tabulated in the 27 possible different arrangements of these three digits. Solution of a Trifid cipher requires that the individual trio having the correct arrangement of the components must be determined for each letter of the alphabet. Relative to this, Gen. Luigi Sacco states in his Manuale di Crittografia:

> "Such determination is to be made exclusively through knowledge of some plaintext word which can be identified in the cryptogram."

Recognizing the truth of Sacco's statement, most of the messages which are prepared for solution by amateurs carry with them one or more given words, together with their exact location in the cipher. The message which will be used to demonstrate solution of a Trifid under these conditions is one constructed by Herbert Raines, Piedmont, California. Mr. Raines, the originator of the Three Square Technique for dealing with Bifids, was at that time the leader of Circle 'B', an A.C.A. group whose members devoted much of their spare time to the study of various cipher systems and, in this connection, periodically constructed messages which were relayed around their circle for solution by all. The following cipher message is given just as it was submitted. Although it was not classified as a Trifid, its type was easily spotted because Circle 'B' was working on that type at that time.

Circle B - Round 56 - No, 1. Type: Unclassified.

Given: First words are "The first". Repeated at: RQOTUILR.

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

The first thing that catches the eye, when this message is but casually inspected, is the triple repetition of 'ZB' in groups three and four. On closer investigation it is observed that 'ZB' occurs no less than twelve times and that, in all other appearances of 'Z', it is followed by 'A'. The Trifid is immediately suspected and the message is re-written with the symbol '#' substituted for 'ZB' and the letter 'Z' for 'ZA'. This gives:

```
H R N G Q  S S X D I  T S I # B  # # T U P  R E I M Q  Y S B J P
t h e f i  r s t

K V R Q O  T U I L R  S I M K #  I R U X P  S O G W Q  etc.
    t h e  f i r s t
```

With the message re-written in this form it is found that the repeated plaintext clue, 'the first', gives no help in determining the period.* However, closer inspection reveals a repetition which is in the form of the pattern produced by a six letter repeat in period 10. The first appearance begins at letter 12 and the second at letter 41.

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

* Note: The surest way to determine the period is through repeat patterns.

On the strength of this the message is set-up in period 10.

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

A line should be drawn below each row of cipher letters and another line along the bottom of the third row of cells below that. This provides space for the numerical components to be written-in as they are determined. The plaintext is then written in the row of cells below the second line. The work sheet looks like this.

H	R	N	G	Q	S	S	X	D	I	T	S	I	#	B	#	#	T	U	P	R	E	I	M	Q	Y	S	B	J	P
T	h	e	f	i	r	s	t																						
K	V	R	Q	O	T	U	I	L	R	S	I	M	K	#	I	R	U	X	P	S	O	G	W	Q	Q	F	M	K	I

(And the remainder of the message, spaced the same way.)

Having now the knowledge, classified by Sacco as a requisite, of plaintext words which can be identified in the cryptogram, one attempts to make use of this information. The way to do this is to fractionate the letters of the known plaintext words and the corresponding cipher letters, and tabulate equivalent values.

The simplest procedure for this step, especially in the case of beginners, is to write the known plaintext in three lines to breakdown each letter into its component parts which are identified by sub numbers - 1, 2, 3,- used to designate 1st, 2nd, and 3rd components. These sub numbers are not to be confused with the true numerical components which are also the figures, 1, 2, 3. The sub numbers are employed only when matching known or probable plaintext with cipher letters in order to derive equivalents.

The corresponding cipher letters are likewise fractionated and similar sub numbers are assigned to each. In these steps it must be remembered that the fractionated plaintext letters are to be in vertical alignment and the fractionated cipher letters are to be written horizontally. Also, the limits of the periodic groups must be observed when the cipher letters are set down.

To procede with the solution of the cipher message now being worked on, the known plaintext words, "the first", are now written in fractionated form as described above and the corresponding fractionated cipher letters are written in the correct relative position below them. Each fraction of the breakdown is assigned a sub number for component designation. Fractions equivalent to each other are then tabulated. As each of these is tabulated it is circled, as shown below for the first series of equivalents.

	Set	Equivalents
$T_1 H_1 E_1 F_1 I_1 R_1 S_1 T_1$	(a)	$T_1 H_1 K_3 N_2 Q_1 Q_2 F_2 E_2 O_3 H_2 V_1 G_3 O_2$
$T_2 H_2 E_2 F_2 I_2 R_2 S_2 T_2$		
$T_3 H_3 E_3 F_3 I_3 R_3 S_3 T_3$	(b)	$T_2 G_2 O_1 S_3 U_2 Q_3 I_2 T_3 I_1 R_3 R_2 R_1 D_2 S_1 D_3 N_1 F_1 V_3$
$H_1 H_2 H_3 R_1 R_2 R_3 N_1 N_2 \cdot \cdot$	(c)	$H_3 X_1 I_3 E_1 V_2 D_1 L_3$
$G_2 G_3 Q_1 Q_2 Q_3 S_1 S_2 S_3 \cdot \cdot$		
$S_3 X_1 X_2 X_3 D_1 D_2 D_3 I_1 \cdot \cdot$	(d)	$E_3 X_2 L_1$
$\cdot \cdot K_3 V_1 V_2 V_3 R_1 R_2 R_3 Q_1$	(e)	$F_3 X_3 L_2$
$\cdot \cdot O_1 O_2 O_3 T_1 T_2 T_3 U_1 U_2$		
$\cdot \cdot I_2 I_3 L_1 L_2 L_3 R_1 R_2 R_3$	(f)	$S_2 U_1$

In the above tabulation, there are now six separate sets of fractional equivalents. As only three digits are employed in the table of numerical components, some of these six sets are equal to each other and must be combined. Just which these are will be determined later but it is already apparent from observation that Set (a) and Set(b) cannot be equal. This is because Set (b) contains $R_1 R_2 R_3$ and Q_3 and Set (a) contains $Q_1 Q_2$. If these two sets were equivalent to each other, both 'R' and 'Q' would have the same identical numerical components, which is an impossible condition. Consequently, numerical values can be given to Sets (a) and (b) and the construction of the table of numerical components can get under way.

The values which are now arbitrarily assigned to these sets may not be the same as those originally used when the message was enciphered but that makes no difference for solving purposes.

To start with the building of the numerical component block, let Set (a) equal 1 and Set (b) equal 2. These assigned numbers are then entered in their appropriate cells, thus:

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

Having established the values shown above, certain additional facts may now be determined from observation. These are:

1 - The third group of equivalents, Set (c), cannot have numerical value 1 for the following reasons. E_1 and V_2 as '1' would make four letters with 1st and 2nd components of '11'. Also, D_1 as '1' would make 'D' equal 122, a designation already preempted by the letter 'T'.

2 - Set (c) cannot have numerical value 2 because D_1, as 2, would make 'D' equal to 222, which has been assigned to letter 'R'.

3 - Thus, by elimination, it is found that Set (c) has numerical value 3. These values are added to the table.

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

Further determinations can now be made.

4 - Since 'O' is 211; then 'F' must be 212 or 213.
and 'N' must be 212 or 213.

5 - Since the 1st and 2nd components of 'F', 'N', 'O', are '21'; then the 2nd component of 'S' cannot be '1'.

Also, the 2nd component of 'S' cannot be 2 as 222 is 'R'.

Hence, the 2nd component of 'S' must be 3. Thus, 232 is 'S'.

6 - From the above, Set (f) takes numerical value 3. This makes U_1 equal 3.

7 - Since the 3rd component of 'F' must be either 2 or 3; then Set (e) - F_3 X_3 L_2- must have numerical value 2 or 3.

8 - As 'D' equals 322; then the 3rd component of 'U' must be 1 or 3.

All known numerical values are now shown in the above table, including those of S_2 and U_1 which were derived after numerical value 3 had been assigned. The deciphering table can now be set up with the known letters added externally.

Known		Q	H		T			V		O				R	I		S						D					
1st Comp.	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3
2nd Comp.	1	1	1	2	2	2	3	3	3	1	1	1	2	2	2	3	3	3	1	1	1	2	2	2	3	3	3	3
3rd Comp.	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	3
Possible				G							F	F	G						E	E	E	G						
											N	N										U		U				

Having determined all three numerical components of nine letters, as well as one or two components of several others, these values can now be substituted in the message to see what fragments of plaintext will be produced and what probable words might then be suggested. This entire procedure is shown below.

THE MESSAGE

H	R	N	G	Q	S	S	X	D	I	T	S	I	#	B	#	#	T	U	P	R	E	I	M	Q	Y	S	B	J	P
1	1	3	2	2	2	2	1			1	2	2	2	3	2	2	2	3		2	2	2	3	1		2	2	3	
2	1	1	1	2	2	3	2	2	3													1	1	2				2	3
2	3			3	2	2	2	2	3		1	2	2	3	2					2									
t	h	e	f	i	r	s	t																						
K	V	R	Q	O	T	U	I	L	R	S	I	M	K	#	I	R	U	X	P	S	O	G	W	Q	Q	F	M	K	I
		1	1	3	2	2	2	2	1	2	3	2	2	2	3					2	3	2	2	1	1		2	1	
1	2	2	1	1	1	2	2	3	2		1				2	2	3	2	2			1	1	2	1	1	2	2	1
	2	2	3			3	2	2	2	2	3	2		3												1	2	2	3
		t	h	e	f	i	r	s	t																		r	t	
C	I	S	X	O	Y	B	S	F	V	P	H	G	H	L	Z	O	Q	E	U	C	R	M	N	J	B	#	V	O	L
			2	2	3	2	3	2	3				1	1	3		2	1	1				2	2	2				2
		2	1	1						1	3			3				2	1	1									
	2	3	2	2	1		1	3	2	1	1	1	2	3	1		3	2			1	3	2	2	1	1			3
																		t											
C	U	J	B	A	#	G	L	F	V	U	D	H	A	M	Y	H	K	V	M	R	G	#	R	T	I	D	X	U	J
			3	2						3	2		3	2	2	1	1	3		2	2	2		2	1				2
									2									1	1	2	2		2	2	2	2	3	3	2
1			3	2	1		1	3	2	3			1	1	3	2				2	3			3	2				
																				r	i			i	t				
Q	N	I	#	I	L	C	U	F	S	F	F	H	D	J	#	H	S	C	M	K	E	C	E	F	Q	O	M	K	Y
1	1	2	2	1		2	2	3		2	1		2	1		1	1	3	3			1	3	1					3
		2	2	3			3			2	2							1	1	1		2	1		1	1	2	2	1
	3	2		2	1		2	3	2	3	2	3	2							1						1			
		r		v			s			i	t																		
P	N	S	S	V	G	H	F	S	B	B	B	O	U	J	S	Q	A	X	K	D	W	J	M	U	#	B	T	X	H
			2	1		2	3	2	2							2	1	1	3	3	2	2							
3	2	1	3	2		2	1	1	1	2					2	3	2	1	1			3	2						
3	2	1		2	3	2				2				3					1		1	2	2	3			1	1	3
				t		r																s							
H	R	H	V	Z	#	B	P	T	E	G	Y	N	H	#	I	B	R	W	N	O	V	O	D	Z	T	A	J	V	L
1	1	3	2	2	2	1	1	3	1		2	1				2	1		1	2	1	1	1	3	2	2	1	1	3
3	2									1	3				2	2	3			2	2				1	2	2		
				1	2	2	3	1			2	2	2				2	1						1	3	2			3
											s						v									r			
K	K	I	V	Z																									
		1																											
1	2	2	3	1																									
3	2																												

The above numerical values are derived from the plaintext words, 'the first', and are known to be correct. They can be inked in so that they will not become confused with values to be added later which may prove to be wrong and will have to be erased.

The plaintext values recovered from this numerical write-in are disappointingly meagre, but from them, in group 13, the plaintext word 'rivers' is suggested by the complete recovery of the letters 'r', 'v', and 's'. The presence of two components (22-) correctly placed for plaintext 'i'; one component (2--) correctly placed for the second 'r'; and one component (--1) which is possible for plaintext 'e'; all lend strength to this assumption.

In group 12, due to similar partial placements, plaintext 'ng' is suggested as the third and fourth letters.

	Group 12										Group 13									
	R	G	#	R	T	I	D	X	U	J	Q	N	I	#	I	L	C	U	F	S
	2	2	2		2	1				2	1	1	2	2	1		2	2	3	
	2	2	1	2	2	2	2	3	3	2			2	2	3			3		
	2	3			3	2						3	2		2	1		2	3	2
Actual Plain	r	i			i	t							r		v			s		
Probable			n	g										i		e	r			

Additional Equalities

From 'ng'				From 'rivers'			
N_3	equal	X_2 -	?	I_3	equal	U_3 -	3
G_1	equal	G_1 -	?	E_1	equal	N_3 -	3
G_3	equal	X_3 -	1	E_2	equal	L_1 -	1
				E_3	equal	F_2 -	1
				R_2	equal	L_2 -	2
				R_3	equal	F_3 -	2

As a control on the above, it is to be remembered that the equivalence, F_3 equal L_2, has already been determined, Set (e), and that F_3 must be either numerical value 2 or 3.

If the probable word, 'rivers', is correct, then the numerical components of F_3 and L_2 will be equivalent, as they are equal to R_3 and R_2 respectively, both of which equal 2. However, both F_3 and L_2 also equal X_3 from Set (e) above, and if the probable 'ng' in group 12 is correct, then X_3 must equal G_3, which has already been determined as numerical value '1'.

The value 2, for F_3 and L_2, seems to have more justification than the value '1' for X_3 and so the probable 'ng' will be discarded as an incorrect assumption.

And so, feeling reasonably confident that plaintext 'rivers' is correctly placed, the numerical components are written-in, with the new values indicated by circled letters and numerals.

	Group 12										Group 13									
	R	G	#	R	T	I	D	X	U	J	Q	N	I	#	I	L	C	U	F	S
	2	2	2		2	1				2	1	1	2	2	1	3	2	2	3	
	2	2	1	2	2	2	2	3	3	2			2	2	3	1	2	3		
	2	3		2	3	2	3					3	2	3	2	1	2	2	3	2
Actual Plain	r	i			i	t							r	i	v	e	r	s		
			o	t			1					h								
Possible			f	r			i			r		l							u	
			n	d			u			i										

New values from the above:

L	equal	123	E	equal	311
F	equal	212	U	equal	323
N	equal	213	X	equal	3-2

The additional values are added to both of the tables.

Known	Q	H		T	L		V		O	F	N		R	I		S		E					D	U			
1st Comp.	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3
2nd Comp.	1	1	1	2	2	2	3	3	3	1	1	1	2	2	2	3	3	3	1	1	1	2	2	2	3	3	3
3rd Comp.	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
Possible				G									G							X		G				X	

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

The new numerical values are now penciled into their proper cells in the message, in order to produce additional plaintext. This operation will not be reproduced in the text but it will be found that very few additional letters are recovered and those which are do not immediately suggest any other probable words.

One thing that is accomplished from this step is the determination of the 2nd component of 'X'. This is found in Group 1,

E_3 equals X_2 equals 1
Hence: X equals 312

To make further progress with the solution, the numerical components of additional letters must be identified. One obvious approach is through the plaintext word, 'the', which in all probability will be found to occur, in a message of this length, at places other than the two which have been identified.

Regardless of what cipher letters serve to generate them, the numerical components which produce plaintext 'the' must always be the same numbers, located in the same relative positions, thus:

Cipher	*	*	*	*	*	*	*	*	*	*	*
					1	1	3				
					2	1	1				
					2	3	1				
Plaintext					t	h	e				

There are several eligible possibilities which can be located by inspection. These are:

Groups 6 and 7

G	W	Q	Q	F	M	K	I	C	I	S	X	O	Y	B
		1	1	3		1	1	3						
		2	1	1		2	1	1						
		2	3	1		2	3	1						
		t	h	e		t	h	e						

Group 9

		C	R	M	N	J	B	#
1	1	3						
2	1	1						
2	3	1						
t	h	e						

Group 11

Y	H	K	V	M
	1	1	3	
	2	1	1	
	2	3	1	
	t	h	e	

Group 14

J	#	H	S	C	M
		1	1	3	
		2	1	1	
		2	3	1	
		t	h	e	

Group 17

Q	A	X	K
	1	1	3
	2	1	1
	2	3	1
	t	h	e

Group 19

Z	#	B	P	T	E
		1	1	3	
		2	1	1	
		2	3	1	
		t	h	e	

Group 21

V	O	D	Z	T	A	J
	1	1	3			
	2	1	1			
	2	3	1			
	t	h	e			

In the preceding groups the vacant cells have been filled with the precise numerical components necessary for decipherment as plaintext 'the' in each case. Some of these are bound to be wrong, but many of them are almost certain to be correct. A tabulation of the values thus derived shows possible equivalents.

Num'l. Comp.	Plain Letter	Group Number							
		6	6-7	8-9	11	14	17	19	21
1	T_1								
2	T_2				Y_2	$\#_2$		$\#_2$	Z_1
2	T_3	K_1				C_3	K_1		J_2
1	H_1		W_1						
1	H_2				Y_3	$\#_3$		$\#_3$	Z_2
3	H_3	K_2			M_1	M_1	K_2		J_3
3	E_1	G_1	C_1	C_1					
1	E_2							B_1	Z_3
1	E_3		B_3	$\#_3$	M_2	M_2			

None of the above values conflict with each other and several of them seem to confirm the assumptions on which they are based. They may now be consolidated for a check against the previously dertermined values shown in the numerical component tables.

B equal 1-1 Possible
C equal 3-2 Possible
G equal 321 Possible
K equal 23- Possible
M equal 31- Possible
W equal 1-- Possible
Y equal -21 Possible
equal -21 Possible

J equal -23 Impossible - Conflicts with L, I, U.
Z equal 211 Impossible - Conflicts with O.

As can be seen, many of the values are possible and some are highly probable. Those which will finally prove to be true values can be determined only by testing in the message and inspection shows that three of the unknown cipher letters of Group 7 are among those for which possible values have been derived in the above list. As it now stands, Group 7 shows this:

C	I	S	X	O	Y	B	S	F	V
			.2	2	3.2		3	2.3	
1	2.2		1	1.			.		
	.2	3	2.2		1	2.1		3	2
			f	f					

Taking Group 7, together with its adjoining groups, and filling in the blank cells with the possible values assigned to the letters B, C, G, K, M, W, Y, yields promising results. All of this is shown in the diagram below, with both the letters and numbers involved again circled, to call attention to these values. Actual plaintext is shown immediately below the numerical components and probable plaintext in the row below the actual.

Group 6										Group 7										Group 8									
S	O	G	W	Q	Q	F	M	K	I	C	I	S	X	O	Y	B	S	F	V	P	H	G	H	L	Z	O	Q	E	U
2	3	2.2		1	1	3	2	1	1	3		2	2	2	3	2	3	2	3				.1	1	3	3	2	1	1
		.1	1	2.	1	1	2	2	1	1	2	2	1	1.		2	1	.		1	3	1	2	3	.			.2	1
2	3	1		2	3	1	2	2	3	1	2	3	2	2	1	2	1	3	2	1	1	1	2	3	1	1	3	2	3
		o		t	h	e	r	t	h	e		i	f	f		r	e						t					t	h
											d				e			n	c	e									

It is now evident that the values derived from assumed plaintext 'the', and tested in Group 6, are possible; and that those tested in Group 7 are almost certainly correct. The plaintext word, 'difference', is so strongly suggested that it cannot be disregarded. Filling in the blank cells gives this.

Group 7

M	K	I	C	I	S	X	O	Y	B	S	F	V	P	H	G
	1	1	3	3	2	2	2	3	2	3	2	3	3		
	2	1	1	2	2	1	1	1	2	1	1	3	1		
	2	3	1	2	3	2	2	1	2	1	3	2	1		
	t	h	e	d	i	f	f	e	r	e	n	c	e		

From which these new values may be accepted as correct.

B equal 131 P equal 3-- W equal 1--
C equal 332 Y equal 121

In Group 8, all of the cells have been filled except those reserved for cipher letters 'P' and 'Z'. The first component of 'G' is as yet unproven, but all other values have been accepted as correct. As the group now stands, there are at least two numerical components for each plaintext letter. Knowing that not more than three letters can have two components identical, it should be possible to identify these unknown letters from context.

Group 8

P	H	G	H	L	Z	O	Q	E	U
3			1	1	3	3	2	1	1
1	3	1	2	3				2	1
1	1	1	2	3	1	1	3	2	3
e			t					t	h
	b	e			e	e	i		
		o			g	g	n		

It does not require a mastermind to visualize this as reading 'the difference between' and the vacant cells are filled in with the numerical values indicated.

Group 8

	P	H	G	H	L	Z	O	Q	E	U
Cipher										
	3	1	3	1	1	3	3	2	1	1
	1	3	1	2	3	1	1	1	2	1
	1	1	1	2	3	1	1	3	2	3
Plaintext	e	b	e	t	w	e	e	n	t	h

New values.

G equal 321
P equal 313
W equal 133
Z equal 111

This leaves only a few letters for which all three components are not positively identified. These can easily be recovered by inserting known values in the message and developing the missing components from results thus obtained. The entire table will be quickly reconstructed in final form as given below.

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

The message can now be read. It starts: "The first day of Spring is one thing and the first Spring day is another - - - -"

KEYWORD BLOCK RECOVERY

A Trifid message is never considered to be completely solved until the keyword block, from which the cipher alphabet is derived, has been recovered. Ordinarily, this is not too difficult to do.

In the preceding example, numerical values were arbitrarily assigned to the several sets of equivalents when they were first determined. The resulting alphabet was adequate for the solver's purpose, but it is not necessarily the same arrangement that was employed by the constructor. There are six possible ways in which the numerical values could be assigned and each of them will give the same result, in so far as deciphering is concerned.

Assuming that the sets a-b-c are the ones to which the numbers, 1-2-3, will be assigned, the assignments may be made in any of these combinations.

Number		Set Combinations					
1	-	a	a	b	b	c	c
2	-	b	c	a	c	a	b
3	-	c	b	c	a	b	a

Some authorities on the Trifid prefer to describe the six possible alphabet arrangements numerically. The method is shown on the right.

Set		Assigned Numbers					
a	-	1	1	2	2	3	3
b	-	2	3	1	3	1	2
c	-	3	2	3	1	2	1

There are several ways to change the recovered alphabet so that it will comply with the six possible assignments of the numbers. However, it has been found that the involved explanation, of the switches and reversals, tends to confuse many who are unfamiliar with the routine. To avoid this, the letters of the recovered alphabet (the a-b-c) may be numbered consecutively, 1 to 27, and then rearranged in a predetermined order as illustrated below.

No. 1 a-b-c Alphabet

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
Z	Q	H	Y	T	L	B	V	W	O	F	N	#	R	I	K	S	J	E	X	P	G	D	U	M	C	A

No. 2 a-c-b Alphabet

1	3	2	7	9	8	4	6	5	19	21	20	25	27	26	22	24	23	10	12	11	16	18	17	13	15	14
Z	H	Q	B	W	V	Y	L	T	E	P	X	M	A	C	G	U	D	O	N	F	K	J	S	#	I	R

No. 3 b-a-c Alphabet

14	13	15	11	10	12	17	16	18	5	4	6	2	1	3	8	7	9	23	22	24	20	19	21	26	25	27
R	#	I	F	O	N	S	K	J	T	Y	L	Q	Z	H	V	B	W	D	G	U	X	E	P	C	M	A

No. 4 b-c-a Alphabet (Reverse of No. 2)

14	15	13	17	18	16	11	12	10	23	24	22	26	27	25	20	21	19	5	6	4	8	9	7	2	3	1
R	I	#	S	J	K	F	N	O	D	U	G	C	A	M	X	P	E	T	L	Y	V	W	B	Q	H	Z

No. 5 c-a-b Alphabet (Reverse of No. 3)

27	25	26	21	19	20	24	22	23	9	7	8	3	1	2	6	4	5	18	16	17	12	10	11	15	13	14
A	M	C	P	E	X	U	G	D	W	B	V	H	Z	Q	L	Y	T	J	K	S	N	O	F	I	#	R

No. 6 c-b-a Alphabet (Reverse of No. 1)

27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
A	C	M	U	D	G	P	X	E	J	S	K	I	R	#	N	F	O	W	V	B	L	T	Y	H	Q	Z

One of the preceding alphabets is that used for enciphering this message and the problem, now confronting the solver, is to find out which it is. Several things, which will help in making this determination, are immediately noticed. These are:

1 - A scrambled alphabet was used.

2 - A straight columnar take-off was not employed as there is no rhythmic continuity of normal alphabet consecutive letters.

3 - An alphabetical Take-off is highly probable, particularly so since 'A' is in the 111 position of alphabets 5 and 6.

To quickly illustrate the method of keyword block recovery, the alphabets derived from the keyword, COUNTERSPY, may be used. The first of these is:

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

The first thing to look for is a relationship of alphabetically consecutive letters. Those of normal low frequency, which are not apt to be in the keyword, are checked first. If it is found that several of these appear at regular intervals, the 'rhythm' of of the alphabet can be recognized and established. In the above alphabet observe this regular continuity.

V - - W - - X - - Z - - #

This, alone, is sufficient to show that the keyword block is three cells deep and that 'Y' is a keyword letter. Then further observation discloses that these letters are preceded by another set which is also in alphabetic continuity. These are:

- D V - F W - G X - H Z - I #

Writing these vertically, together with the third letter of each set, produces the following sequences.

U N T E R
D F G H I
V W X Z #

Having thus determined the take-off method, the remainder of the keyword block is easily recovered.

In COUNTERSPY alphabet No. 3, probably the most difficult of the examples given, the same technique may be applied.

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

Inspection shows that no such continuous series of letters is present, as was the case with the other example. Consequently, the investigation must take the form of a search for isolated pairs of letters which may be related to a similar pair because of their regulated position in the keyword block. Immediately, some such pairs are noted, among them being AK - BL, LV - MW, and others. When these are written vertically the picture begins to form.

A	B						D			F	G
K	L			L	M						Q
				V	W		X			Z	#

These fragments, with adjoining letters attached, are then consolidated in their proper alphabetical sequence and they fall into position as shown below.

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

The above demonstration shows that the entire keyword block can be rebuilt by the solver, in spite of the fact that it is an alphabetical take-off and there are many vacant cells. With this knowledge of what to look for, one may now attempt to recover the keyword block of the message previously deciphered.

The experienced cryptanalyst will examine the six alphabets and, from observation, will select No. 6 as that most likely to be the original arrangement. This alphabet is:

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

The circumstances which influence the choice of No. 6 are based on familiarity with the construction of keyword blocks. Attention is immediately attracted by the alphabetical relationship, in descending order, of such consecutive combinations as:

F		G
O	and	P
W		X

Other similar combinations are found, taken out, and placed in proper alphabetical relation to each other. Some of these are;

B C		H I
L M	and	Q R
T U		Z #

The letters, which precede each of these groups of three, are added and all sets are arranged in alphabetical order, thus:

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

The remaining three letters are then placed, completing the block, and showing it to be formed from the keyword - VANDYKE. This is an example of alphabetical take-off, as shown below.

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

Keyword recovery is one of the most interesting phases of cryptography and, with a moderate amount of practice, anyone can quickly become adept in this field. The general principles of recovery, here given, will also apply to other scrambling methods.

THE STRUCTURE OF TRIFID PERIODIC GROUPS

A Trifid, in which plaintext words are given, can be deciphered by the identification and collection of equivalents. In such a message, recognition of plaintext repeat patterns is a help but not a requisite. However, if one attempts to solve a Trifid when no such clues are supplied, then a thorough knowledge of just how patterns are generated is not only helpful, it is mandatory. But before going into the subject of patterns, the structure of the various periodic group lengths should be investigated.

It has previously been stated that the Trifid is ordinarily enciphered in periodic groups which are multiples of 3, plus 1. Generally, this will be found to be the case, but it is by no means compulsory. Two other periodic lengths may be used. The three possible periodic classifications are:

Class I - Multiples of 3, plus 0 as: 3 - 6 - 9 - 12 etc.

Class II - Multiples of 3, plus 1 as: 4 - 7 - 10 - 13 etc.

Class III - Multiples of 3, plus 2 as: 5 - 8 - 11 - 14 etc.

Each class of this periodic division creates its own special arrangement of the cipher letter components when they are to be read as vertical trios. This is shown below. (COUNTERSPY alph.)

	Class I	Class II	Class III
Cipher	Z E N M A G	Z E S C S B T	Z E J C D N G W
Fractionated	$Z_1 Z_2 Z_3 E_1 E_2 E_3$	$Z_1 Z_2 Z_3 E_1 E_2 E_3 S_1$	$Z_1 Z_2 Z_3 E_1 E_2 E_3 J_1 J_2$
	$N_1 N_2 N_3 M_1 M_2 M_3$	$S_2 S_3 C_1 C_2 C_3 S_1 S_2$	$J_3 C_1 C_2 C_3 D_1 D_2 D_3 N_1$
	$A_1 A_2 A_3 G_1 G_2 G_3$	$S_3 B_1 B_2 B_3 T_1 T_2 T_3$	$N_2 N_3 G_1 G_2 G_3 W_1 W_2 W_3$
Numerical Comps.	2 3 3 2 3 1	2 3 3 2 3 1 3	2 3 3 2 3 1 3 2
	2 1 1 1 1 3	2 1 1 1 1 3 2	2 1 1 1 1 3 2 2
	1 1 2 2 2 2	1 1 2 2 2 2 1	1 1 2 2 2 2 1 3
Plaintext	t r i f i d	t r i f i d s	t r i f i d s x

From the foregoing it may be observed how, for each periodic class, the fractionated cipher letters fall into three different arrangements of their components for vertical reading. It may be noted also, that the numerical components which produce plaintext 'trifid' remain the same in all cases. These were originally derived from the six plaintext letters, when they were enciphered, and must always be the same when this alphabet is used. Substitution of numerical components for plaintext letters is in no way influenced by periodic length or class; but periodic class changes the combinations of these numbers when they are read horizontally, thus producing different cipher letters. Finally, the structure of periodic groups is important for these reasons:

1 - Each periodic class (I-II-III) generates its own individual cipher letter patterns for repeated plaintext.

2 - Each periodic length, of any class, will be found to produce its own distinctive patterns for repeated plaintext words.

3 - For any periodic length, three different pattern types are possible for the same plaintext sequence, depending on its location in the periodic group.

PART NATURALS - WHAT ABOUT THEM ?

Another topic, which may merit discussion at this point, is the occurrence of 'part naturals' in a Trifid cipher message. The expectation that a positive entry can be made into a Trifid by means of part naturals is, as a general rule, a forlorn hope. However, it must not be entirely overlooked and, in some special cases, it has to be given full consideration. One such occasion is when an actual cipher message, known to be a Trifid, is to be solved. If the cryptanalyst has sufficient background information to make logical assumptions in the probable word field, and in spite of the fact that the coincidence percentage is extremely unfavorable, he should certainly leave no stone unturned in his effort to spot a word which he believes to be in the message.

One actual situation in which one may hope, with some degree of confidence, to locate a word through part naturals, is when a plaintext word is given, but not definitely located, in a Trifid problem in The Cryptogram. The problems appearing in The Cipher Exchange of that magazine are, of necessity, so short that it is virtually impossible to make an entry unless a positive clue is given. Frequently, with Trifids, a word or sequence is given and correctly placed. On other occasions the plaintext clue is merely furnished and the solver must then try to find its location in the cipher. To assist in this search, a plaintext word or sequence, which creates 'part naturals' when enciphered, is often given as the 'tip'. Also, such 'tips' usually start at the beginning of a periodic group. Under these conditions some knowledge of how to recognize 'part naturals' is of great assistance to the solver.

The first thing that must be thoroughly understood and accepted is the fact that a 'part natural' must be exactly what the term implies - a part natural. By this it is meant that one cannot merely match probable plaintext words, letter for letter, against unfractionated cipher groups and hope to locate 'part naturals'. This is best illustrated by an example, thus:

If the given plaintext word is: T R I F I D S
And a cipher sequence is: Q R I X I D Z
Then the cipher letters in this group cannot be 'part naturals', although several of them seem to coincide.

The reason for this is immediately apparent when the cipher group is fractionated and matched with the plaintext word. From this it is seen that no cipher components coincide with components of the same plaintext letter.

Q_1	Q_2	Q_3	R_1	R_2	R_3	I_1
I_2	I_3	X_1	X_2	X_3	I_1	I_2
I_3	D_1	D_2	D_3	Z_1	Z_2	Z_3
t	r	i	f	i	d	s

Also, there can be no 'phony' part naturals. When cipher R_3 equals plain R_3- that is a true part natural. But when cipher R_3 equals plain R_2- it is not. Cipher R_3 may well equal plain R_2 but this fact does not create a part natural and, in addition to that, the equivalence of R_3 and R_2 is not yet established when one is trying to place a 'tip' at the beginning of his work. This can be shown by slightly rearranging the same cipher letters which were used above. Assume the cipher letters to be: Q I R X I Z D

Q_1	Q_2	Q_3	I_1	I_2	I_3	R_1
R_2	R_3	X_1	X_2	X_3	I_1	I_2
I_3	Z_1	Z_2	Z_3	D_1	D_2	D_3
t	r	i	f	i	d	s

When fractionated, there are still no part naturals as, in each case, the components of the cipher letters are found to be of different degree than are those of the plaintext.

Another thing to be remembered is this. Although each and every cipher letter could be a part natural, only certain specifically located plaintext letters can be partially represented in the cipher by their own fractional parts.

In addition to these general conditions, which apply in all cases, there are certain other controlling factors which vary with each of the periodic classes. This variation is due to the fact that, while plaintext components are always in vertical alignment of 1st, 2nd, 3rd; periodic classification creates, for each class, a different vertical alignment of the cipher components. This can best be shown by an illustration. In periods 3, 4, and 5, which are the simplest forms of the three classes, the vertical alignment of the cipher components is:

Class I	Class II	Class III
1st 2nd 3rd	1st 2nd 3rd 1st	1st 2nd 3rd 1st 2nd
1st 2nd 3rd	2nd 3rd 1st 2nd	3rd 1st 2nd 3rd 1st
1st 2nd 3rd	3rd 1st 2nd 3rd	2nd 3rd 1st 2nd 3rd

This same relationship maintains, in all classes, regardless of the length of the periodic group. The manner in which it affects the search for part naturals will be demonstrated for each periodic class. The original COUNTERSPY alphabet is used in the encipherment of the following examples which are constructed to show how part naturals may be recognized.

Starting with Class II (multiples of 3, plus 1) which is the periodic length most frequently used in amateur cryptography, this is how things shape up. The given word is: L E T T E R S
It is tested in various cipher groups, such as: J X L X Q C C

When this cipher group is in its fractionated form the various cipher components are in these locations.

$J_1\ J_2\ J_3\ X_1\ X_2\ X_3\ L_1$
$L_2\ L_3\ X_1\ X_2\ X_3\ Q_1\ Q_2$
$Q_3\ C_1\ C_2\ C_3\ C_1\ C_2\ C_3$

And, for matching purposes, the components of the plaintext word will be set up in this way.

$L_1\ E_1\ T_1\ T_1\ E_1\ R_1\ S_1$
$L_2\ E_2\ T_2\ T_2\ E_2\ R_2\ S_2$
$L_3\ E_3\ T_3\ T_3\ E_3\ R_3\ S_3$

From the above it is ascertained that L_2 cipher is equal to L_2 plain and, consequently, is a part natural if the plaintext word has been correctly spotted in the cipher message.

This illustration shows the set-up for matching cipher with plaintext components but, merely for 'tip testing', it will not be necessary to fractionate both groups as part naturals may be found by a more simple method. Inspection of the matched groups reveals the fact that there are only three plaintext letters which could be represented by part naturals. These are the letters in the 1st, 4th, and 7th positions of the periodic group when the period is seven, as it is in this case. Here, the only eligible letters are 'L', 'T', and 'S'. But it may also be observed that each of the three components of these three plaintext letters can be represented by a cipher part natural.

Assuming that the cipher message has been copied on squared paper with the period determined and marked off as seven, the search for a group, where a 'tip' may correctly be placed because of the presence of part naturals, resolves itself into the following routine.

Reference to the fractionated blocks shows the first line of cipher components to be: $J_1 J_2 J_3 X_1 X_2 X_3 L_1$. It is also seen that only J_1, X_1, and L_1 can coincide with 1st components of plaintext letters. And the 1st, 4th, and 7th plaintext letters are the only ones which can match 1st components with these three cipher letters. So, for 1st components, the set-up is this:

Cipher Group:	J X L X Q C C	Result:
Plaintext - 1st Comp.	$L_1 T_1 S_1$	No part naturals.

Continuing further, the second line of cipher components is composed of these letters: $L_2 L_3 X_1 X_2 X_3 Q_1 Q_2$. This also shows that only the 1st, 4th, and 7th plaintext letters could hope to match their 2nd components with any of the cipher letters in this line. But, in this case, the cipher letter components which may coincide are the 2nd components of the 3rd, 4th, and 5th cipher letters. Consequently, for search purposes, the eligible plaintext letters are added to the set-up in 3rd, 4th, and 5th positions, thus:

Cipher Group:	J X (L) X Q C C	Result:
Plaintext - 1st Comp.	$L_1 T_1 S_1$	2nd component of 'L'
2nd Comp.	$(L_2) T_2 S_2$	is a part natural.

To complete the demonstration, since the third line of fractionated cipher letters is: $Q_3 C_1 C_2 C_3 C_1 C_2 C_3$, it is again seen that only the 1st, 4th, and 7th plaintext letters can have a 3rd component which will coincide and, if this happens, it can be only with 3rd components of the 5th, 6th, and 7th cipher letters. So, once more, the same three plaintext letters are placed where they will show a part natural if one is present.

Cipher Group:	J X L X Q C C	Result:
Plaintext - 1st Comp.	$L_1 T_1 S_1$	No additional
2nd Comp.	$L_2 T_2 S_2$	part naturals.
3rd Comp.	$L_3 T_3 S_3$	

All of the above explanation boils down to this: To search for part naturals, write down on a separate piece of paper in the positions shown above, the eligible letters from the given plain text word or sequence. Slide this along under the cipher message matching each group for evidence of part naturals. When such are found to be present, the solver can select that which appears to be most promising and proceed from there. If positive results do not develop, then another choice must be tried.

An easy way to get the critical letters placed correctly is to write the plaintext word vertically, three times, in this way.

```
L T S t r e e
e e L T S t r
t r e e L T S
```

Part natural spotting requires an entirely different set-up for the other periodic group lengths - Class I and Class III. It has been shown that only the 1st, 4th, 7th, 10th, etc. plaintext letters are potential part naturals in Class II, but for Class I and Class III, all plaintext letters as well as all cipher letters are eligible. This can be verified if each line is analyzed as was done with Class II, but here, only the final arrangement will be illustrated. In Class I and Class III the position of the plaintext letters is not determined as easily as was the case with Class II, so it is recommended that three vertical write-ins, of the known plaintext sequence, be adopted by beginners.

In Class I, with cipher group: H D A # G C, and given plaintext word, 'figure', part naturals may be spotted by use of this arrangement of the plaintext letters.

Cipher:		H D A # G C	
Plaintext -	1st Comp.	F U f u f u	Result:
	2nd Comp.	i r I R i r	3rd component of 'G'
	3rd Comp.	g e g e G E	is a part natural.

In Class III, with cipher group: H W E B # G R C, and given plaintext word, 'fixtures', the same routine is employed.

Cipher:		H W E B # G R C	
Plaintext -	1st Comp.	F T E i u s x r	Result:
	2nd Comp.	i u s X R f t e	1st component of 'E'
	3rd Comp.	x r f t e I U S	is a part natural.

One concrete example of how this technique may be put to use can be given by applying it to a Trifid from the Cipher Exchange of The Cryptogram - issue of January-February 1961.

E-23. Trifid. No ice, no drinks. SODAKO
Period is shown to be 8.
Given sequence: "ourpartiesarelas".

		Group 9	Group 10
Cipher:		O P L R J V K A	E R A G X R J E
Plaintext -	1st Comp.	O P T u a i r r	E R A s e s a l
	2nd Comp.	u a i R R o p t	s e s A L e r a
	3rd Comp.	r r o p t U A I	a l e r a S E S

Six part naturals are found at this location of the 'tip'.

A slightly more difficult example of how knowledge of 'tip' spotting can be used to advantage, is the following problem from the March-April 1956 issue of The Cryptogram.

E-25. Trifid. Walkers all. S-TUCK
The period, as shown by repeats, is 10.
Given: "President Truman" (repeated).

A study of the message discloses what is, apparently, a long repeated sequence in Groups 3-4 and Groups 15-16. By starting the first letter of the 'tip' at the 4th letter position in the group, three part naturals show in Group 3 and one in Group 15.

		1 4 7 10	1 4 7 10
Cipher -	3 & 4	Y P # E M Z E A B J	W # E B G G A A R M
	15 & 16	H P # A T Z B A B J	W # E V G G A A R B
Plaintext:	1st	? P S E - e d - r i	N R A ? t m - t u n
	2nd	- r i ? P S E - e d	t u n N R A ? t m -
	3rd	- e d - r i ? P S E	t m - t u n N R A ?

This is sufficient to warrent a complete matching test and, when no conflicts occur, this location is accepted as the correct position of the given words and the solution proceeds from there.

PATTERNS IN THE TRIFID.

A 'pattern', as the term applies to Trifids, consists of two or more cipher letters spaced with such relation to each other that they can represent a plaintext sequence which lies within the limits of a periodic group. Patterns are not recognizable as such until they are repeated. Consequently, when a pattern is identified, it discloses the location of two occurrences of the same plaintext word or fragment of a word.

The pattern letters result from the fact that all three components of certain cipher letters are included among those which, when read vertically, produce the repeated plaintext sequence.

This is illustrated with an example enciphered by the COUNTERSPY alphabet.

- - - I X F O X A M N C B - - -
- - G I X X S X C W N C - - - -

The pattern is in the form of: A D - - C - - B E which is that generated in period 10 by a seven letter plaintext repeat, starting with the first or fourth plaintext letter of the group. When this example is set up for decipherment and the numerical components are written-in, the derivation of the recurring cipher letters is immediately apparent.

Cipher:	I	X	F	O	X	A	M	N	C	B
	3	1	2	2	2	3	2	1	2	1
	2	1	2	2	3	1	1	2	1	1
	3	2	1	1	1	1	1	1	2	2
Plaintext:	p	a	t	t	e	r	n	o	f	a

G	I	X	X	S	X	C	W	N	C
2	2	2	3	1	2	2	2	3	2
2	3	3	2	1	2	2	3	1	1
1	2	1	3	2	1	1	1	1	1
t	h	e	p	a	t	t	e	r	n

From the above it is observed that the repeated cipher letters come from certain numerical components of the repeated plaintext sequence which form complete letters when read horizontally.

Perhaps this can be better illustrated from the encipherment angle, showing only that portion of the plaintext which generates the cipher letter pattern.

	1	2	3	4	5	6	7	8	9	10
Plaintext:	p	a	t	t	e	r	n	-	-	-
	3	1	2	2	2	3	2			
	2	1	2	2	3	1	1			
	3	2	1	1	1	1	1			
Cipher:	I	X	-	-	X	-	-	N	C	-

1	2	3	4	5	6	7	8	9	10
-	-	-	p	a	t	t	e	r	n
			3	1	2	2	2	3	2
			2	1	2	2	3	1	1
			3	2	1	1	1	1	1
-	I	X	-	-	X	-	-	N	C

Using only the values given above, there are but five cipher letters which can be derived, and these are the ones which form the pattern. The other numerical components of the known plaintext letters (those not underscored) are but fractions of cipher letters, and what letters those will be depends upon the unknown numerical components with which they will combine.

It is this very fact that makes the pattern so important to the solver of a Trifid, because, it is from these partial values that equivalents may be derived. The five cipher letters, shown to be repeated in exactly the same relation to each other, virtually confirm the fact that seven consecutive plaintext letters of one group are repeated in the other group. None of the plaintext letters are known, but all of the cipher letters are there

to work with and that is all that is required at this time. Nine of the ten cipher letters in each group contributed one or more of their components to the twenty-one required to form the seven letter plaintext word, 'pattern'. Five of these nine contributed all three of their components, thus forming the pattern. The other four cipher letters contribute but one or two of their components. But it is these four letters that provide the information which allows the solver to get started. Although the numerical value of their components is not yet established, it is known that those of one group must be equivalent to those, of identical location, in the other group. This can be demonstrated by again reversing the two groups to their decipherment set-up.

Cipher:	I	X	F	O	X	A	M	N	C	B
	3	1	2	.2	2	3	2	-	-.-	
	2	1	.2	2	3	1	1	-.-	-	
	3	.2	1	1.1	1	1	.-	-	-	
Plaintext:	p	a	t	t	e	r	n			

	G	I	X	X	S	X	C	W	N	C
	-	-	-.3	1	2.2	2	3	2		
	-	-.-	2	1	.2	2	3	1	1	
	-.-	-	3	.2	1	1.1	1	1		
			p	a	t	t	e	r	n	

In which:

Cipher	F	is	2	-	-	Cipher	X	is	2	-	-
"	O	"	-	2	1	"	S	"	-	2	1
"	A	"	1	1	-	"	C	"	1	1	-
"	M	"	-	-	3	"	W	"	-	-	3

From this it can be seen that:

1st	component	of	F	equals	1st	component	of X
2nd	"	"	O	"	2nd	"	" S
3rd	"	"	O	"	3rd	"	" S
1st	"	"	A	"	1st	"	" C
2nd	"	"	A	"	2nd	"	" C
3rd	"	"	M	"	3rd	"	" W

Hence, it may be stated that, in period 10, the repetition of a seven letter plaintext sequence which starts at group position 1 or 4, produces, in each case, a series of nine consecutive cipher letters which bear a definite relationship to each other. In the above example the following conditions prevail with these letters.

1 - 2 - 5 - 8 - 9	Identical - produce pattern.
3	1st components same.
4	2nd and 3rd components same.
6	1st and 2nd components same.
7	3rd components same.

For comparative purposes these relationships can be indicated with symbols in this manner.

1	2	3	4	5	6	7	8	9	
	I	X	F	O	X	A	M	N	C B
G	I	X	X	S	X	C	W	N	C
·	□	□	⅂	⊢	□	⅂	L	□	□ ·

In which:

- ⅂ - 1st components same.
- ⊢ - 2nd components same.
- L - 3rd components same.
- ⅂ - 1st and 2nd components same
- ⊢ - 2nd and 3rd components same.
- Z - 1st and 3rd components same.
- □ - All three components same.
- · - No information.

It was previously stated that the position in the periodic group determines the pattern of a plaintext sequence. In the example the plaintext word 'pattern' started with the 1st letter of the group in one occurrence and with the 4th letter in the other. Had the word, "pattern", started with the 2nd or 3rd letter of the group, an entirely different pattern would have been formed in each case. The three possible patterns for this same word, when it is enciphered in period 10, are illustrated below.

Class II - Multiples of 3, plus 1.

1	2	3	4	5	6	7	8	9	10
p	a	t	t	e	r	n	-	-	-
3	1	2	2	2	3	2			
2	1	2	2	3	1	1			
3	2	1	1	1	1	1			
I	X	-	-	X	-	-	N	C	-

1	2	3	4	5	6	7	8	9	10
-	p	a	t	t	e	r	n	-	-
	3	1	2	2	2	3	2		
	2	1	2	2	3	1	1		
	3	2	1	1	1	1	1		
-	G	-	-	B	R	-	S	C	-

1	2	3	4	5	6	7	8	9	10
-	-	p	a	t	t	e	r	n	-
		3	1	2	2	2	3	2	
		2	1	2	2	3	1	1	
		3	2	1	1	1	1	1	
-	B	H	-	F	E	-	-	C	-

The other classes generate their own individual patterns.

Class I - Multiples of 3, plus 0.

1	2	3	4	5	6	7	8	9
p	a	t	t	e	r	n	-	-
3	1	2	2	2	3	2		
2	1	2	2	3	1	1		
3	2	1	1	1	1	1		
I	X	-	F	E	-	S	C	-

1	2	3	4	5	6	7	8	9
-	p	a	t	t	e	r	n	-
	3	1	2	2	2	3	2	
	2	1	2	2	3	1	1	
	3	2	1	1	1	1	1	
-	G	-	-	X	-	-	C	-

1	2	3	4	5	6	7	8	9
-	-	p	a	t	t	e	r	n
		3	1	2	2	2	3	2
		2	1	2	2	3	1	1
		3	2	1	1	1	1	1
-	B	H	-	B	R	-	N	C

Class III - Multiples of 3, plus 2.

1	2	3	4	5	6	7	8	9	10	11
p	a	t	t	e	r	n	-	-	-	-
3	1	2	2	2	3	2				
2	1	2	2	3	1	1				
3	2	1	1	1	1	1				
I	X	-	-	B	R	-	-	C	-	-

1	2	3	4	5	6	7	8	9	10	11
-	p	a	t	t	e	r	n	-	-	-
	3	1	2	2	2	3	2			
	2	1	2	2	3	1	1			
	3	2	1	1	1	1	1			
-	G	-	-	F	E	-	-	N	C	-

1	2	3	4	5	6	7	8	9	10	11
-	-	p	a	t	t	e	r	n	-	-
		3	1	2	2	2	3	2		
		2	1	2	2	3	1	1		
		3	2	1	1	1	1	1		
-	B	H	-	-	X	-	-	S	C	-

These examples illustrate how, with the same alphabet, nine different patterns are produced by the same seven-letter plaintext word. They also show just how these patterns are derived and with this information, one can develop the pattern for any plain text repeat under any condition. The amateur cryptanalyst will find that most of the Trifid messages he has the opportunity to work with are enciphered in period 10, and for that reason a list of the patterns generated by repeats of various length, possible for that period, will be given.

The repetition, at similar group locations, of a single plaintext letter, or of two consecutive plaintext letters, leaves no identifiable pattern in the cipher message. Repeats of three consecutive plaintext letters produce one repeated cipher letter but the occurrence of a single cipher letter, repeated at the proper location, is not sufficient evidence to establish the certainty of a three-letter plaintext repeat. However, a three-letter repeat will sometimes be very acceptable when there is doubt concerning a four-letter word, shown by a four-letter pattern.

The four letter (tetragraph) plaintext repeat produces two repeated cipher letters. This forms the basic pattern which is searched for when a Trifid message is investigated in this manner. It is the firm foundation to which longer repeats may be anchored. In period 10 there are three different types of 4-letter repeat patterns. These are:

Type.	Plaintext Starting Position.	Pattern.
I	1	□ ㄱ · ㄷ ㄱ · ㄴ □ · ·
	4	· □ ㄱ · ㄷ ㄱ · ㄴ □ ·
	7	· · □ ㄱ · ㄷ ㄱ · ㄴ □
II	2	ㄷ ㄱ · ㄴ □ · · □ ㄱ ·
	5	· ㄷ ㄱ · ㄴ □ · · □ ㄱ
III	3	ㄴ □ · · □ ㄱ · ㄷ ㄱ ·
	6	· ㄴ □ · · □ ㄱ · ㄷ ㄱ

From the above it may be observed that the starting position of the plaintext repeat governs the type of pattern and also, for patterns of the same type, controls the location of the pattern in its periodic group. Patterns of all possible lengths of repeated plaintext sequences, for period 10, are tabulated below. These patterns are shown as starting at positions 1, 2, 3, but it is to be remembered that the location in the periodic group must be subject to the other starting positions for that same type.

Period 10 Patterns.
(Plaintext indicated thus: a b c d)

	Type I.	Type II.	Type III.
1.	a - - - - - - - - - ㄱ · · ㅏ · · ㄴ · · ·	- a - - - - - - - - ㅏ · · ㄴ · · · ㄱ · ·	- - a - - - - - - - ㄴ · · · ㄱ · · ㅏ · ·
2.	a b - - - - - - - - ㄱ · · ㄷ · · ㄴ ㄱ · ·	- a b - - - - - - - ㄷ · · ㄴ ㄱ · · ㄱ · ·	- - a b - - - - - - ㄴ ㄱ · · ㄱ · · ㄷ · ·
3.	a b c - - - - - - - □ · · ㄷ ㄱ · ㄴ ㄱ · ·	- a b c - - - - - - ㄷ ㄱ · ㄴ ㄱ · · □ · ·	- - a b c - - - - - ㄴ ㄱ · · □ · · ㄷ ㄱ ·
4.	a b c d - - - - - - □ ㄱ · ㄷ ㄱ · ㄴ □ · ·	- a b c d - - - - - ㄷ ㄱ · ㄴ □ · · □ ㄱ ·	- - a b c d - - - - ㄴ □ · · □ ㄱ · ㄷ ㄱ ·
5.	a b c d e - - - - - □ ㄱ · ㄷ □ · ㄴ □ ㄱ ·	- a b c d e - - - - ㄷ □ · ㄴ □ ㄱ · □ ㄱ ·	- - a b c d e - - - ㄴ □ ㄱ · □ ㄱ · ㄷ □ ·
6.	a b c d e f - - - - □ □ · ㄷ □ ㄱ ㄴ □ ㄱ ·	- a b c d e f - - - ㄷ □ ㄱ ㄴ □ ㄱ · □ □ ·	- - a b c d e f - - ㄴ □ ㄱ · □ □ · ㄷ □ ㄱ
7.	a b c d e f g - - - □ □ ㄱ ㄷ □ ㄱ ㄴ □ □ ·	- a b c d e f g - - ㄷ □ ㄱ ㄴ □ □ · □ □ ㄱ	- - a b c d e f g - ㄴ □ □ · □ □ ㄱ ㄷ □ ㄱ
8.	a b c d e f g h - - □ □ ㄱ ㄷ □ □ ㄴ □ □ ㄱ	- a b c d e f g h - ㄷ □ □ ㄴ □ □ ㄱ □ □ ㄱ	- - a b c d e f g h ㄴ □ □ ㄱ □ □ ㄱ ㄷ □ □
9.	a b c d e f g h i - □ □ □ ㄷ □ □ Z □ □ ㄱ	- a b c d e f g h i ㄷ □ □ Z □ □ ㄱ □ □ □	None.

A study of the foregoing patterns will reveal several things which it is well to remember. These are:

1 - Until it exceeds the length of the period, there are always two more symbols in the pattern than the number of plaintext letters in the repeated sequence.

2 - The number of complete symbols (□) is always two less than the number of letters in the repeated plaintext sequence.

3 - Symbols which show 1st components to be the same (⅂) build to completes as the plaintext sequence increases in length.

4 - Symbols which show 3rd components (L) or 2nd and 3rd components (⊥) to be the same, remain unchanged, regardless of how many additional letters are added to the plaintext sequence, until it is one less than the periodic length.

5 - The two complete symbols of the tetragraph are the anchors for any identifiable plaintext repeat. It is this repeated occurrence of two related cipher letters, in their three different locations, that the solver seeks out when the search for patterns is being made.

6 - The identification of tetragraphic patterns automatically discloses the presence of longer plaintext repeats when such occur in a message.

LONG PLAINTEXT REPEATS.

The repetition of several words, which extends a repeat beyond the limits of one periodic group, creates a condition which is a veritable bonanza to the solver. Such an occurrence gives many equivalents which could not otherwise be recognized. An example will show how this is possible. Two plaintext fragments are:

|t h e D e l a s t e|l l e T r i f i d c|i p h e r

|c a n t h e D e l a|s t e l l e T r i f|i d b e s o l v e d|

When enciphered by the COUNTERSPY alphabet these groups show:

1st Fragment:		G	Q	D	X	L	I	E	F	D	C	Y	Z	E	V	S	C	#	R	B	T
2nd Fragment:	A	G	Q	C	Q	L	R	N	F	D	J	Y	Z	G	L	S	C	M	R	B	
Pattern:	·	□	□	⅂	⊥	□	⅂	L	□	□	·	□	□	⅂	⊥	□	⅂	L	□	□	

The above matched diagram discloses the pattern of a 7-letter repeat starting at plaintext position 1 of both of the groups in the first occurrence and at plaintext position 4 in both groups of the second occurrence. It will be noted that an additional 'complete', cipher letter 'C', is present in the second group of both occurrences but, as an 8-letter repeat is impossible in the second occurrence, the solver must settle for a 7-letter repeat in these groups. Situations similar to this frequently come up when one is working with Trifid patterns.

These four groups can now be set up in fractionated form for further comparison .

-	-	-	G_1	G_2	G_3	Q_1	Q_2	Q_3	D_1	D_2	D_3	X_1	Y_1	Y_2	Y_3	Z_1	Z_2	Z_3	E_1	E_2	E_3	V_1	-	-	-
-	-	-	X_2	X_3	L_1	L_2	L_3	I_1	I_2	I_3	E_1	E_2	V_2	V_3	S_1	S_2	S_3	C_1	C_2	C_3	$\#_1$	$\#_2$	-	-	-
-	-	-	E_3	F_1	F_2	F_3	D_1	D_2	D_3	C_1	C_2	C_3	$\#_3$	R_1	R_2	R_3	B_1	B_2	B_3	T_1	T_2	T_3	-	-	-
A_1	A_2	A_3	G_1	G_2	G_3	Q_1	Q_2	Q_3	C_1	J_1	J_2	J_3	Y_1	Y_2	Y_3	Z_1	Z_2	Z_3	G_1	-	-	-	-	-	-
C_2	C_3	Q_1	Q_2	Q_3	L_1	L_2	L_3	R_1	R_2	G_2	G_3	L_1	L_2	L_3	S_1	S_2	S_3	C_1	C_2	-	-	-	-	-	-
R_3	N_1	N_2	N_3	F_1	F_2	F_3	D_1	D_2	D_3	C_3	M_1	M_2	M_3	R_1	R_2	R_3	B_1	B_2	B_3	-	-	-	-	-	-

Accepting a 7-letter repeat, as shown by the pattern in each periodic group, the following equivalents are derived.

$X_2 = Q_2$	$X_3 = Q_3$	$D_1 = C_1$	$V_2 = L_2$	$V_3 = L_3$
$E_3 = N_3$	$I_1 = R_1$	$I_2 = R_2$	$\#_3 = M_3$	$E_1 = G_1$

And, under the existing circumstances, it can be assumed that the repeat is continuous and bridges the periodic break. If this is true, then these additional values are equivalent.

$D_2 = J_1$	$X_1 = J_3$	$E_1 = G_3$	$C_1 = C_3$	$C_3 = M_2$
$D_3 = J_2$	$I_3 = G_2$	$E_2 = L_1$	$C_2 = M_1$	

Referrence to the COUNTERSPY numerical component table will show that all of the above assumed equivalents are correct.

THE ELEMENT OF UNCERTAINTY IN PATTERNS.

Although they are the greatest source of information, patterns cannot be trusted, implicitly, in the Trifid. Due to the fact that there are nine letters which have the same 1st numerical component, and a like number having the same 2nd and 3rd numerical components, it is always possible that a combination of these numerical components will produce the same pattern when different plaintext letters are involved. This fact must always be kept in mind when one is working with patterns and the following example will show why this is necessary.

It may be well worthwhile, for the reader, to decipher this short message in order to see how patterns can sometimes lead the solver astray. It is enciphered with the COUNTERSPY alphabet and the apparent 6-letter repeat, occurring in groups 3 and 6, will illustrate the point to be made.

Pseudo Repeat Example.

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

However, in spite of the fact that patterns can deceive, they are the solver's main source of entry when no plaintext word is given. For that reason, dependence must be placed in them, and, the equivalent values which they disclose must always be tested, thoroughly and completely. Experience will soon teach the solver which to accept and which to regard with suspicion.

SOLVING THE TRIFID FROM SCRATCH.

The cryptanalyst who would endeavor to solve a Trifid without benefit of "knowledge of a plaintext word which can be identified in the message", is confronted with a project of major proportions. Even though he may thoroughly understand the method to be employed and be sufficiently skillful to put it into execution, there still remains plenty of work to do as a vast amount of tabulating and comparing is necessary before one can make a start on the gathering of equivalent values. However, the satisfaction derived from solving a cipher message without help, makes worthwhile all the time and energy expended.

The method for doing this, which will be demonstrated in an example to follow, is attributed to Rosario Candela of New York, who, during the decade prior to his death in 1954, was recognized as one of the premier amateur cipher experts of the entire world. The systems of Delastelle were favorites of Candela and were the subject of many of his lectures before the New York Cipher Society. The basic facts upon which the Trifid solution method is grounded are these:

1 - Repeated plaintext sequences, occurring at related locations in the message, produce a recognizable pattern of repeated cipher letters.

2 - Certain related cipher letters, which are not repeated, are also partially controlled by the plaintext sequence which generates the repeated letters.

3 - The related cipher letters, which are not repeated, must have one or more components which are equivalent.

4 - If a sufficient number of such equivalents can be collected, the table of numerical components can be recovered.

The method of procedure may be summarized in these words.

1 - The tetragram (four letter sequence) is the shortest plaintext sequence that will produce a recognizable pattern when it is repeated in the same relative periodic location.

2 - The tetragraphic pattern contains two cipher letters repeated at a known interval, depending on the location of the plaintext in the periodic group.

3 - In period 10, the repeated cipher letters of a tetragraphic pattern are located in the group positions listed below.

Pattern Type	Starting Position (Plaintext)	Repeated Cipher Letters
I	1	1 and 8
	4	2 " 9
	7	3 " 10
II	2	5 and 8
	5	6 " 9
III	3	2 and 5
	6	3 " 6

4 - All letters of the cipher message, occurring at the designated locations, are tabulated for the purpose of spotting tetragraphic patterns. This tabulation is demonstrated below, using the first six groups of the message shown on page 11.

Group No.	Type I			Type II		Type III	
	1-8	2-9	3-10	5-8	6-9	2-5	3-6
1	H X	R D	N I	Q X	S D	R Q	N S
2	T T	S U	I P	B T	# U	S B	I #
3	R B	E J	I P	Q B	Y J	E Q	I Y
4	K I	V L	R R	O I	T L	V O	R T
5	S U	I X	M P	# U	I X	I #	M I
6	S M	O K	G I	Q M	Q K	O Q	G Q

Repeats of the same type are underscored. Note that 'I-X' of Type I, Group 5, and 'I-X' of Type II, Group 5, although they are the same, do not constitute a repeat.

5 - The groups which contain repeats are then aligned in matching position and the tetragraphic pattern is applied to indicate probable equivalent values.

Example No. 1.

Type	Repeat	Group	Location
I	S-U	2	2 - 9
		5	1 - 8

	T	S	I	#	B	#	#	T	U	P
		S	I	M	K	#	I	R	U	X P
Tetragraphic Pattern - - - - - - -		□	⅂	·	⊢	⅃	·	L	□	· ·
Additional Supporting Values - - -			□			□				

Example No. 2.

Type	Repeat	Group	Location
I	I-P	2	3 - 10
		3	3 - 10

	T	S	I	#	B	#	#	T	U	P
	R	E	I	M	Q	Y	S	B	J	P
Tetragraphic Pattern - - - - - - -		·	·	□	⅂	·	⊢	⅃	·	L □
Additional Supporting Values - - -						None				

When two cipher groups are matched and the tetragraphic pattern is applied, two identical letters are necessary in order to conform with the requirements of the pattern. If one or more of the related letters also proves to be identical, then the plaintext tetragram may, tentatively, be accepted as an actual repetition of the same 4-letter sequence.

In the examples above, the first shows additional supporting values and may be accepted. The second example shows no supporting identicals and cannot, immediately, be accepted as a 4-letter plaintext repeat.

6 - Equivalent values are then collected from the matched groups.

Example No. 1,	T	S	I	#	B	#	#	T	U	P
		S	I	M	K	#	I	R	U	X P
Tetragraphic Pattern		□	⅂	·	⊢	⅃	·	L	□	· ·

Equivalent Values: $B_2 = K_2$ $B_3 = K_3$ $T_3 = R_3$

7 - It must always be kept in mind that apparent equivalent values, derived from patterns, are apt to be incorrect. Because of this, they must be kept, more or less, on probation until the status of their validity is confirmed. Because of this degree of uncertainty, no exact law can be stated for acceptance of equivalent values thus indicated. However, in every pattern for repeated plaintext sequences of two letters or more, except when the periodic length is a multiple of 3, plus 0, it may be observed that there are four symbols denoting partial equality of certain components. These are ⊓, ⊐, ⊏, ⊔, and they represent a total of six individual components. If three, or more, of these six potential equivalent values are confirmed by supporting identical cipher letters, then the plaintext sequence designated by the pattern may be assumed to be correct. If less than three of the unknown values are confirmed then the possibility of a plaintext repeat is questionable.

Referring once again to Example 1, this theory of acceptance may be illustrated.

Example No. 1.	T S I # B # # T U P S I M K # I R U X P	Number of Components.
Tetragraphic Pattern	□ ⊓ · ⊏ ⊐ · ⊔ □ ·	12
Required Identicals	□	6
Probable Equivalents	⊓ ⊏ ⊐ ⊔	6
Confirming Values	□ □	3
Unconfirmed	⊏ ⊔	3

Of the twelve components under consideration in this example, nine are confirmed and three are assumed to be the equivalent values indicated by the pattern. This is acceptable.

The reason for delayed acceptance in the case of Example #2 can be shown in like manner.

Example No. 2.	T S I # B # # T U P R E I M Q Y S B J P	Number of Components.
Tetragraphic Pattern	· · □ ⊓ · ⊏ ⊐ · ⊔ □	12
Required Identicals	□ □	6
Probable Equivalents	⊓ ⊏ ⊐ ⊔	6
Confirming Values		0
Unconfirmed	⊓ ⊏ ⊐ ⊔	6

Of the twelve components under consideration, six, or 50% of the total, remain questionable. This is not sufficient for acceptance. However, when a repeat fails to qualify as a tetragram, it may be tested as a trigram. If it again fails to pass the test, it may then be tested as a digraph, perhaps starting at a position further advanced in the group.

8 - When two cipher groups are fractionated, all cipher letter components are set down and may be compared individually. It requires a great deal more writing than merely applying the pattern, but this method has its advantages and is preferred by some authorities. Those components, which match exactly, are then segregated and, where two components of a vertical trio are identical, the third is accepted as being equivalent to its corresponding component in the other group. This will ordinarily give about the same result as the 'three confirmed' acceptance minimum described above.

In the message being used for demonstration purposes, there are no typical sequences which could be used to illustrate this method to best advantage. For that reason, two groups have been enciphered with the same alphabet (VANDYKE) in order that it may be demonstrated.

	1st Group	2nd Group
Plaintext:	t h e m e n c a m e	t h e m a y o r i s
Cipher:	H C A G B W X E V E	H M R # W F S E E S

Cipher Fractionated.

1st Group:	$\boxed{H_1 H_2 H_3} C_1 C_2 C_3 A_1 A_2 A_3 G_1$ $G_2 G_3 B_1 B_2 B_3 W_1 W_2 W_3 X_1 X_2$ $X_3 \boxed{E_1 E_2 E_3} V_1 V_2 V_3 E_1 E_2 E_3$	Accepted Equivalents.
2nd Group:	$\boxed{H_1 H_2 H_3} M_1 M_2 M_3 R_1 R_2 R_3 \#_1$ $\#_2 \#_3 W_1 W_2 W_3 E_1 E_2 E_3 S_1 S_2$ $S_3 \boxed{E_1 E_2 E_3} E_1 E_2 E_3 S_1 S_2 S_3$	$G_3 = \#_3$ $B_1 = W_1$

This same acceptance results if the 'three confirmed' method is employed with diminishing repeat patterns.

1st Group:	H	C	A	G	B	W	X	E	V	E	Number of Components.
2nd Group:	H	M	R	#	W	F	S	E	E	S	
Tetragraph:	□	⅂	·	⊢	⅃	·	⊥	□	·	·	12
Required:	□							□			6
Probable:		⅂		⊢	⅃		⊥				6
Confirmed:											0
Unconfirmed:		⅂		⊢	⅃		⊥				6
Trigraphic:	□	·	·	⊢	⅂	·	⊥	⅃	·	·	9
Required:	□										3
Probable:				⊢	⅂		⊥	⅃			6
Confirmed:								□			2
Unconfirmed:				⊢	⅂		⊥				4
Digraphic:	⊢	·	·	⊥	⅂	·	·	⅃			6
Required:											0
Probable:	⊢			⊥	⅂			⅃			6
Confirmed:	□							□			4
Unconfirmed:				⊥	⅂						2

Accepted: $B_1 = W_1$
$G_3 = \#_3$

The method, wherein the cipher groups are completely fractionated, was that employed by Rosario Candela in his admirable demonstration of Trifid solution, presented at a special meeting of the New York Cipher Society in honor of Gen. Luigi Sacco.

The more streamlined "three confirmed" procedure, in which the repetition of matching cipher letters controls the degree of acceptance, was originated by the author of this booklet and its application is first demonstrated herein. It will be found that the use of this inflexible control eliminates the element of personal judgement which sometimes tends to influence acceptance.

9 - When more than two groups contain the same repeated cipher letters, the entire lot may be combined for comparison. This feature, at times, helps to confirm doubtful components. To the two groups used above, add the following.

3rd Group -	Plaintext:	t h e m o r e f o r
	Cipher:	H D D # B O T E Y F

With the addition of the third group, one is now dealing with a total of 3 X 12 = 36 cipher components. When all three of these groups are compared, collectively, the result is:

1st Group:	H	C	A	G	B	W	X	E	V	E	
2nd Group:	H	M	R	#	W	F	S	E	E	S	Number of
3rd Group:	H	D	D	#	B	O	T	E	Y	F	Components.

Tetragraph:	□	⅂	·	⊢	⅃	·	⊥	□	·	·	12
Required:	□							□			6
Probable:		⅂		⊢	⅃		⊥				18/3 = 6
Confirmed:				□	□						12/3 = 4
Unconfirmed		⅂					⊥				6/3 = 2

Accepted: $C_1 = M_1 = D_1$ $B_1 = W_1$
$G_2 = \#_2$ $B_2 = W_2$
$G_3 = \#_3$ $X_3 = S_3 = T_3$

The fractionation method produces the same result, thus:

1st Group:	H_1	H_2	H_3	C_1	C	C	A	A	A	G
	G_2	G_3	B_1	B_2	B_3	W	W	W	X	X
	X_3	E_1	E_2	E_3	V	V	V	E	E	E
2nd Group:	H_1	H_2	H_3	M_1	M	M	R	R	R	#
	$\#_2$	$\#_3$	W_1	W_2	W_3	F	F	F	S	S
	S_3	E_1	E_2	E_3	E	E	E	S	S	S
3rd Group:	H_1	H_2	H_3	D_1	D	D	D	D	D	#
	$\#_2$	$\#_3$	B_1	B_2	B_3	O	O	O	T	T
	T_3	E_1	E_2	E_3	Y	Y	Y	F	F	F
Plaintext:	1	2	3	4	5	6	7	8	9	10

Equivalents.

$G_3 = \#_3$
$B_1 = W_1$
$G_2 = \#_2$
$X_3 = S_3 = T_3$
$B_2 = W_2$
$C_1 = M_1 = D_1$

The reasoning which would lead to acceptance of a repeated plaintext tetragram in the three groups would be something on the order of the following:

Plaintext Letter 2. The three vertical components are the same in the 2nd and 3rd groups. The 1st group has two of these components (1 and 3) identical with those of the other groups. Therefore, the non-identical component of the 1st group may be considered to be equivalent.

Hence: $G_3 = \#_3$

Plaintext Letter 3. By the same reasoning:

$B_1 = W_1$

Plaintext Letter 1. The 1st component in all three groups is the same and both 1st and 2nd components of two of the groups are identical (H_1 and $\#_2$). Consequently, the 2nd component of the

other group may also be assumed as equivalent.

Hence: $G_2 = \#_2$

And now, having accepted the equivalence of the 2nd components of this vertical trio in all three groups; it follows that, in each group, two of the components of the trio are identical or equivalent. Hence, the other component may be accepted as equivalent.

And so: $X_3 = S_3 = T_3$

<u>Plaintext Letter 4.</u> - By the same reasoning:

$B_2 = W_2$
$C_1 = M_1 = D_1$

10 - Patterns of longer repeats, such as those for six, seven, and eight letter plaintext sequences, may be handled with greater confidence than is the case with tetragraphs. This is because the longer repeats are actually a series of consecutive tetragraphs and, if the tetragraphs prove to be acceptable, then the longer repeats automatically qualify. This can be illustrated with groups 2 and 5 of the demonstration message.

Plaintext -	Group 2	.	.	.	s	p	r	i	n	g	.
	Group 5	s	p	r	i	n	g	.	.	.	.
Cipher -	Group 2	T	S	I	#	B	#	#	T	U	P
	Group 5	S	I	M	K	#	I	R	U	X	P
Cipher lined up for applying pattern.		T	S	I	#	B	#	#	T	U	P
			S	I	M	K	#	I	R	U	X	P

											Plaintext Repeat Indicated
Tetra. Type I, S - U		□	⅂	·	⊢	⅃	·	∟	□	·	·	spri
" Type II, # - U		⊢	⅃	·	∟	□	·	·	□	⅂	·	prin
" Type III, I - #		∟	□	·	·	□	⅂	·	⊢	⅃	·	ring
6-Letter - Type I		□	□	·	⊢	□	⅂	∟	□	⅃	·	spring

The three tetragraphic patterns all have supporting values and, when they are combined, the maximum values shown in each column produce the six letter repeat pattern.

11 - Equivalencies, from patterns, regardless of how they are derived, must always be considered as assumed values only, until their validity is proven by the recovery of acceptable plaintext. The solver must keep this fact in mind and continue to regard them as merely tentative until he is sure that they are correct.

- - - - - - - -

The foregoing is an outline of the procedure to be followed when one is forced to make his own entry into a Trifid cipher message. With this smattering of the 'know how', the attempt may now be made to solve a Trifid without the benefit of given plaintext words, placed in the message. Oddly enough, this seems to be easier to do with a Trifid than is the case with a Bifid.

THE CIPHER OF THE THREE WISE MEN.

The King desired to select the wisest member of his court for duty as an Ambassador. Three men, Mr. X, Mr. Y, and Mr. Z, were considered to be best qualified for the appointment and were summoned to his presence. The King spoke to them, saying: "I shall blindfold you and paint a spot of red or blue on your foreheads. After removing your blindfolds, if you see a blue spot anywhere, raise your right hand. Then, when you determine the color of your own spot, lower the hand. The first to do so shall be my Ambassador if his answer is correct."

The King then blindfolded the men, painted a blue spot on each forehead, removed the blindfolds, and watched three hands go up. A moment later the hand of Mr. Z descended.

Question: How did Mr. Z know that his spot was blue ?
Answer: Mr. Z reasoned thus:

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

Note: The example used for this demonstration is believed to be readily identifiable as a Trifid because of the fact that the 27th symbol is present and that characteristic Trifid patterns are quickly found. Repeat patterns occurring in Groups 6 and 10, 2 and 13, as well as elsewhere, determine the period as 10. And so, for convenience, the message has been set up in its periodic groups.

SOLUTION.

Having determined by observation that this message has been enciphered by Trifid, and that the period is 10, it is set up for decipherment in the manner described on page 11, thus:

The Three Wise Men.

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

The cipher letters occurring at the 'required identical' locations of the tetragraphic repeat patterns are then tabulated for all 37 groups. Only a small portion will be shown here. In the case of long cipher messages of 1000 letters, or approximately that number, such a tabulation should be made at the beginning of at least the first 250 letters. If sufficient information is not gained from this, to make an entry, then an additional 250 letters can be tabulated.

Group No.	Type I			Type II		Type III	
	1-8	2-9	3-10	5-8	6-9	2-5	3-6
1	W-S	D-Y	W-F	J-S	A-Y	D-J	W-A
2	K-M	M-L	A-D	J-M	K-L	M-J	A-K
3	Z-S	U-X	J-P	Y-S	Q-X	U-Y	J-Q
4	N-#	A-V	V-P	M-#	N-V	A-M	V-N
5	X-A	Y-F	B-U	U-A	R-F	Y-U	B-R
6	B-C	N-#	J-T	R-C	O-#	N-R	J-O
7	S-Y	X-C	X-E	B-Y	L-C	X-B	X-L
8	J-H	V-Z	W-F	J-H	G-Z	V-J	W-G
9	X-I	Z-S	U-X	J-I	Y-S	Z-J	U-Y
10	B-C	N-#	B-X	R-C	V-#	N-R	B-V
.							
.							
37	J-Z	U-X	N-O	W-Z	B-X	U-W	N-B

Repeats are then located, and the best way to locate them is to again tabulate the above pairs for contact. This tabulation, for the pairs shown above, can be done in this manner.

Type I

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

And the same for Type II and Type III.

The groups showing repeats are then collected and aligned in accordance with the location of the identical letters. All possible plaintext repeated tetragraphs are represented and the related groups may now be studied for the purpose of determining equivalent values and discovering the location of longer repeated plaintext sequences. Although all must be aligned and analyzed, only those which show the required minimum of three confirmed values will be listed in this text. This select collection of derived equivalents will also be separated into two classes.

Class A - More than three confirmed.
Class B - Not more than three confirmed.

The Class B values will receive additional study before they are fully and unconditionally accepted as correct.

GROUP MATCHING FOR TETRAGRAPHIC REPEATS.

Type I

Test No.	Group No.	Start. Pos.	Tetra. Pattern	Class 'A'	Class 'B'
1	2	7	K M A A J K Y M L D		
	13	4	M A L J K Y W L D M	$A_1 = L_1$	
			□ ⅂ · ⊢ ⅃ · ⊥ □		
2	2	7	K M A A J K Y M L D		
	17	1	A A C K Y A E D R O	$L_3 = E_3$	
			□ ⅂ · ⊢ ⅃ · ⊥ □		
3	6	1	B N J W R O E C # T	$W_2 = A_2$	
	10	1	B N B A R V E C # X	$W_3 = A_3$	
			□ ⅂ · ⊢ ⅃ · ⊥ □		
4	15	7	H Q D D M K J X F H		$D_1 = W_1$
	32	7	R O D W R K A L F H		$J_1 = A_1$
			□ ⅂ · ⊢ ⅃ · ⊥ □		$J_2 = A_2$
5	30	4	G I S M T P J V T K		$S_1 = J_1$
	31	7	O F I J L T U K V T		$P_1 = U_1$
			□ ⅂ · ⊢ ⅃ · ⊥ □		$P_2 = U_2$
6	2	4	K M A A J K Y M L D		
	13	1	M A L J K Y W L D M	$M_3 = W_3$	
			□ ⅂ · ⊢ ⅃ · ⊥ □		
7	6	4	B N J W R O E C # T		$J_1 = B_1$
	10	4	B N B A R V E C # X		$O_1 = V_1$
			□ ⅂ · ⊢ ⅃ · ⊥ □		$O_2 = V_2$
8	10	4	B N B A R V E C # X		
	14	7	U J N B X R V X G #	$C_3 = G_3$	
			□ ⅂ · ⊢ ⅃ · ⊥ □		
9	3	4	Z U J J Y Q J S X P		$J_1 = B_1$
	9	7	X Z U B J Y H I S X		$Q_1 = H_1$
			□ ⅂ · ⊢ ⅃ · ⊥ □		$Q_2 = H_2$
10	1	7	W D W A J A # S Y F		
	12	4	O W J W A # J Y F K	$A_1 = J_1$	
			□ ⅂ · ⊢ ⅃ · ⊥ □		
11	18	4	F W V I J Z I V S I		$V_1 = O_1$
	26	7	M L W O J J # A V S		$Z_1 = \#_1$
			□ ⅂ · ⊢ ⅃ · ⊥ □		$Z_2 = \#_2$
12	3	1	Z U J J Y Q J S X P		
	9	4	X Z U B J Y H I S X	$J_3 = I_3$	
			□ ⅂ · ⊢ ⅃ · ⊥ □		

Type II

Test No.	Group No.	Start. Pos.	Tetra. Pattern	Class 'A'	Class 'B'
13	1	5	W D W A J | A # S | Y | F		$D_2 = O_2$
	12	2	O W J W | A # J | Y | F K		$D_3 = O_3$
			⊢ ⊣ · ⊥ | ⊡ · · | ⊡ | ⊤		$J_3 = W_3$
14	15	5	H Q D D M | K J X | F | H		$Q_2 = O_2$
	32	5	R O D W R | K A L | F | H		$Q_3 = O_3$
			⊢ ⊣ · ⊥ | ⊡ · · | ⊡ | ⊤		$M_3 = R_3$
15	2	5	K M A A J | K Y M | L | D		
	13	2	M A L J | K Y M | L | D M	Long repeat.	
			⊢ ⊣ · ⊥ | ⊡ · · | ⊡ | ⊤		
16	18	2	F W V I | J Z I | V | S I		$F_2 = L_2$
	26	5	M L W O J | J # A | V | S		$F_3 = L_3$
			⊢ ⊣ · ⊥ | ⊡ · · | ⊡ | ⊤		$I_3 = J_3$
17	13	5	M A L J K | Y W L | D | M		$L_1 = A_1$
	17	2	A A C K | Y A E | D | R O		$L_2 = A_2$
			⊢ ⊣ · ⊥ | ⊡ · · | ⊡ | ⊤		$M_1 = R_1$
18	3	2	Z U J J | Y Q J | S | X P		
	9	5	X Z U B J | Y H I | S | X	Long repeat.	
			⊢ ⊣ · ⊥ ⊡ · · | ⊡ | ⊤		

Type III

Test No.	Group No.	Start. Pos.	Tetra. Pattern	Class 'A'	Class 'B'
19	2	6	K M | A | A J | K | Y M | L | D		
	13	3	M | A | L J | K | Y W | L | D M	Long repeat	
			⊥ | ⊡ | · · | ⊡ | ⊤ · | ⊢ | ⊣		
20	15	6	H Q | D | D M | K | J X | F | H	$Q_3 = O_3$	
	32	6	R O | D | W R | K | A L | F | H	$J_1 = A_1$	
			⊥ | ⊡ | · · | ⊡ | ⊤ · | ⊢ | ⊣		
21	30	3	G | I | S M | T | P J | V | T K	$G_3 = F_3$	
	31	6	O F | I | J L | T | U K | V | T	$P_1 = U_1$	
			⊥ | ⊡ | · · | ⊡ | ⊤ · | ⊢ | ⊣		
22	6	3	B | N | J W | R | O E | C | # T		
	10	3	B | N | B A | R | V E | C | # X	$O_1 = V_1$	
			⊥ | ⊡ | · · | ⊡ | ⊤ · | ⊢ | ⊣		
23	10	3	B | N | B A | R | V E | C | # X		$B_3 = J_3$
	14	6	U J | N | B X | R | V X | G | #		$C_2 = G_2$
			⊥ | ⊡ | · · | ⊡ | ⊤ · | ⊢ | ⊣		$C_3 = G_3$
24	3	3	Z | U | J J | Y | Q J | S | X P		
	9	6	X Z | U | B J | Y | H I | S | X	$Q_1 = H_1$	
			⊥ | ⊡ | · · | ⊡ | ⊤ · | ⊢ | ⊣		
25	1	6	W D | W | A J | A | # S | Y | F		
	12	3	O | W | J W | A | # J | Y | F K	$D_3 = O_3$	
			⊥ | ⊡ | · · | ⊡ | ⊤ · | ⊢ | ⊣		
26	18	3	F | W | V I | J | Z I | V | S I	$F_3 = L_3$	
	26	6	M L | W | O J | J | # A | V | S	$Z_1 = \#_1$	
			⊥ | ⊡ | · · | ⊡ | ⊤ · | ⊢ | ⊣		

The potential equivalent values derived from these tetragraphic patterns may now be collected and consolidated.

Class A.	$A_1 = L_1 = J_1$	$W_2 = A_2$	$L_3 = E_3$
	$P_1 = U_1$		$W_3 = A_3 = M_3$
	$O_1 = V_1$		$C_3 = G_3 = F_3 = L_3$
	$Q_1 = H_1$		$J_3 = I_3$
	$Z_1 = \#_1$		$Q_3 = O_3 = D_3$

Class B. (Excluding those duplicated in Class A.)

$D_1 = W_1$	$J_2 = A_2 = L_2 = F_2$	$J_3 = W_3 = B_3$
$S_1 = J_1 = B_1$	$P_2 = U_2$	$M_3 = R_3$
$M_1 = R_1$	$O_2 = V_2 = D_2 = Q_2 = H_2$	
	$Z_2 = \#_2$	
	$C_2 = G_2$	

The great majority of the above equivalents should prove to be correct but a few of them will surely be in error. Because of this, before attempting to build the table of numerical components, further corroborating evidence is sought. This will come from the longer repeats, several of which are indicated by the above listed group comparisons. In that tabulation it may be observed that tests No. 1, 6, 15, and 19 all apply to Groups 2 and 13. Special investigation of these groups discloses the occurrence of a long repeat (7-letter) starting with plaintext letter 4 of Group No. 2 and plaintext letter 1 of Group No. 13.

Test No.	Pt. Start. Pos. Gr. 2	Pt. Start. Pos. Gr. 13	Group 2 - K M A A J K Y M L D Group 13 M A L J K Y W L D M
6	4	1	□ ㄱ · ㅌ ㅋ · ㄴ □
15	5	2	ㅌ ㅋ · ㄴ □ · · □ ㄱ
19	6	3	ㄴ □ · · □ ㄱ · ㅌ ㅋ
1	7	4	□ ㄱ · ㅌ ㅋ · ㄴ □
Comb.	4	1	□ □ ㄱ ㅌ □ ㅋ ㄴ □ □

Since the indicated repeat starts with the 4th plaintext letter and ends with the 10th of Group No. 2, and starts with the 1st letter of Group No. 13, it is possible that an extra-long repeat may bridge the periodic division lines on both sides of Groups 2 and 13. As was previously explained on pages 31-32, this creates a situation which is always searched for in Trifid solution, as such an occurrence produces equivalents that could not otherwise be so readily developed.

Further investigation reveals that Groups 1 and 12 also contain a long repeat and, when this lead is pursued even further, the presence of repeated cipher letters in Groups 3 and 14 lends weight to the possibility that the repeated plaintext sequence extends into these groups also. Referrence to the complete group alignment tabulation (not included in this text - see Page 40), will show that a tetragraphic repeat was indicated in Groups 3 and 14 but was screened out by the 'three confirmed' test. As these two groups have now assumed a position of greater importance under the existing circumstances, they will be given consideration, in spite of the fact that the first test temporarily sidelined them. In this connection, one should always bear in mind these facts:

1 - Some of the tetragraphic repeats, derived from patterns, which pass the 'three confirmed' test, will be incorrect.

2 - Some of those which do not pass the 'three confirmed' test will be true tetragraphic repeats.

For a more detailed investigation, the groups which appear to contain the long repeated sequence are set up in their fractionated form and are aligned so as to bring the identical letters into their proper relation with each other. However, before doing this, it is of interest to align the two rows of cipher letters for the purpose of illustrating how the patterns clearly indicate the presence of a long repeat.

Plain. Pos.																														
6-Letter - 5 and 2											7-Letter - 4 and 1										4-Letter - 4 and 1									
W	D	W	A	J	A	#	S	Y	F	K	M	A	A	J	K	Y	M	L	D	Z	U	J	J	Y	Q	J	S	X	P	
	O	W	J	W	A	#	J	Y	F	K	M	A	L	J	K	Y	W	L	D	M	U	J	N	B	X	R	V	X	G	#
	⊏	⊐	⊓	⊔	⊐	⊓	·	⊐	⊐		⊐	⊐	⊓	⊏	⊐	⊓	⊔	⊐	⊐		⊐	⊓	·	⊏	⊓	·	⊔	⊐		

When the cipher letters are fractionated, this gives:

W_1	W_2	W_3	D_1	D_2	D_3	W_1	W_2	W_3	A_1	K_1	K_2	K_3	M_1	M_2	M_3	A_1	A_2	A_3	A_1	Z_1	Z_2	Z_3	U_1	U_2	U_3	J_1	J_2	J_3	J_1												
A_2	A_3	J_1	J_2	J_3	A_1	A_2	A_3	$\#_1$	$\#_2$	A_2	A_3	J_1	J_2	J_3	K_1	K_2	K_3	Y_1	Y_2	J_2	J_3	Y_1	Y_2	Y_3	Q_1	Q_2	Q_3	J_1	J_2												
$\#_3$	S_1	S_2	S_3	Y_1	Y_2	Y_3	F_1	F_2	F_3	Y_3	M_1	M_2	M_3	L_1	L_2	L_3	D_1	D_2	D_3	J_3	S_1	S_2	S_3	X_1	X_2	X_3	P_1	P_2	P_3												
										O_1	O_2	O_3	W_1	W_2	W_3	J_1	J_2	J_3	W_1	M_1	M_2	M_3	A_1	A_2	A_3	L_1	L_2	L_3	J_1	U_1	U_2	U_3	J_1	J_2	J_3	N_1	N_2	N_3	B_1
										W_2	W_3	A_1	A_2	A_3	$\#_1$	$\#_2$	$\#_3$	J_1	J_2	J_2	J_3	K_1	K_2	K_3	Y_1	Y_2	Y_3	W_1	W_2	B_2	B_3	X_1	X_2	X_3	R_1	R_2	R_3	V_1	V_2
										J_3	Y_1	Y_2	Y_3	F_1	F_2	F_3	K_1	K_2	K_3	W_3	L_1	L_2	L_3	D_1	D_2	D_3	M_1	M_2	M_3	V_3	X_1	X_2	X_3	G_1	G_2	G_3	$\#_1$	$\#_2$	$\#_3$

Inspection of the above arrangement shows a definite 7-letter repeat in Groups 2 and 13. In Groups 1 and 12 the experienced solver will content himself with a 5-letter repeat, rather than the 6-letter repeat which the pattern indicates. In Groups 3 and 14, there is sufficient evidence to show that the long repeat extends across the periodic division line. Four plaintext letters may be repeated in these groups, but, to play safe, the indicated repeat in 3 and 14 is reduced in length to a trigraph.

Equivalent values shown above are:

Groups 1-12	Periodic Bridge		Groups 2-13	Periodic Bridge		Groups 3-14
$D_3 = O_3$	$K_1 = J_2$	$A_2 = \#_3$	$M_3 = W_3$	$Z_1 = L_2$	$J_2 = Y_3$	$Y_2 = B_2$
$A_1 = J_1$	$Y_3 = K_1$	$K_2 = J_3$	$A_1 = L_1$	$J_3 = M_1$	$Z_2 = L_3$	$S_3 = V_3$
	$A_3 = J_1$	$M_1 = K_2$		$J_3 = W_1$	$S_1 = M_2$	$Y_3 = B_3$
	$K_3 = W_1$	$J_1 = J_2$		$Z_3 = J_1$	$Y_1 = W_2$	$Q_1 = X_1$
	$M_2 = K_3$			$S_2 = M_3$		

When these values are consolidated they shape up in this way.

$A_1 = J_1 = A_3 = J_2 = L_1 = Y_3 = Z_3 = K_1 = B_3$

$K_2 = J_3 = M_1 = W_1 = K_3 = M_2 = S_1$ $\qquad$ $S_3 = V_3$ $\qquad$ $A_2 = \#_3$

$M_3 = W_3 = S_3$ $\qquad$ $Q_1 = X_1$ $\qquad$ $Z_1 = L_2$

$D_3 = O_3$ $\qquad$ $Y_1 = W_2$ $\qquad$ $Y_2 = B_2$ $\qquad$ $Z_2 = L_3$

Another long repeat which, apparently, bridges the periodic division line is found at Groups 3 - 9 and 4 - 10.

Z_1	Z_2	Z_3	U_1	U_2	U_3	J_1	J_2	J_3	J_1	N_1	N_2	N_3	A_1	A_2	A_3	V_1	V_2	V_3	R_1				
J_2	J_3	Y_1	Y_2	Y_3	Q_1	Q_2	Q_3	J_1	J_2	R_2	R_3	M_1	M_2	M_3	N_1	N_2	N_3	H_1	H_2				
J_3	S_1	S_2	S_3	X_1	X_2	X_3	P_1	P_2	P_3	H_3	$\#_1$	$\#_2$	$\#_3$	V_1	V_2	V_3	P_1	P_2	P_3				
X_1	X_2	X_3	Z_1	Z_2	Z_3	U_1	U_2	U_3	B_1	B_1	B_2	B_3	N_1	N_2	N_3	B_1	B_2	B_3	A_1				
B_2	B_3	J_1	J_2	J_3	Y_1	Y_2	Y_3	H_1	H_2	A_2	A_3	R_1	R_2	R_3	V_1	V_2	V_3	E_1	E_2				
H_3	I_1	I_2	I_3	S_1	S_2	S_3	X_1	X_2	X_3	E_3	C_1	C_2	C_3	$\#_1$	$\#_2$	$\#_3$	X_1	X_2	X_3				

Additional equivalent values derived from this are:

Groups 3 - 9	Periodic Bridge		Groups 4-10
$J_3 = I_3$	$J_2 = B_1$	$Q_3 = A_2$	$H_3 = C_3$
$Q_1 = H_1$	$P_1 = E_3$	$J_3 = B_2$	$M_1 = V_1$
$J_1 = B_1$	$J_1 = A_3$	$P_2 = C_1$	
$Q_2 = H_2$	$J_1 = B_3$	$J_2 = R_1$	
	$P_3 = C_2$		

These values may also be consolidated in this manner:

$J_1 = B_1 = J_2 = A_3 = B_3 = R_1$		$Q_1 = H_1$	$P_2 = C_1$
$J_3 = I_3 = B_2$		$Q_2 = H_2$	$P_3 = C_2$
$Q_3 = A_2$	$H_3 = C_3$	$P_1 = E_3$	$M_1 = V_1$

All equivalent values derived from the long repeats and the Class 'A' tetragraphs may now be assembled. And, at this point, it might not be amiss to call attention to the fact that it is really surprising to see how many values have thus far been recovered without knowing a single word of the plaintext.

Set	Equivalents
(a) -	$A_1 = J_1 = A_3 = J_2 = L_1 = Y_3 = Z_3 = K_1 = B_3 = B_1 = R_1 = W_3 = M_3 = S_2$
(b) -	$K_2 = J_3 = M_1 = W_1 = K_3 = M_2 = S_1 = I_3 = B_2 = Y_2 = V_1 = O_1$
(c) -	$Z_2 = L_3 = C_3 = G_3 = F_3 = H_3 = E_3 = P_1 = U_1$
(d) -	$A_2 = \#_3 = Q_3 = W_2 = O_3 = D_3 = Y_1$

(e) - $Q_1 = H_1 = X_1$ (g) - $Q_2 = H_2$ (i) - $P_3 = C_2$

(f) - $Z_1 = \#_1 = L_2$ (h) - $P_2 = C_1$ (j) - $S_3 = V_3$

Numerical values may now be assigned to these sets of components of equal value. As set (a) is the longest and contains the greatest number of values:

Let set (a) equal numerical component '1'.

Inspection shows that set (a) contains $B_1 = B_3$ and $J_1 = J_2$.
and that set (b) contains B_2 and J_3.

Hence, as no two letters can have three numerical components

which are identical to each other, then these sets must be designated by different numerical values.

Hence: Let set (b) equal numerical component '2'.

The table of numerical components, with these values assigned, gives the following:

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

Examination of set (c) shows that it cannot have numerical value '1' as it contains six 3rd components. As there are already six 3rd components to which the value '1' has been assigned, no more than three 3rd components of numerical value '1' can be added. Nor can set (c) be '2', for it contains Z_2. If the vacant 2nd component of 'Z' was designated as '2', that would make four letters - B, M, Y, and Z, - having 2nd and 3rd components the same. Consequently, numerical value '3' is all that remains for set (c), but if it is thus designated, another conflict appears. This time the trouble is with set (d).

Sets (c) and (d) cannot be combined, as there are a total of ten 3rd components in the two sets. When set (d) is studied separately, the following controlling conditions are evident.

Set (d) is: $A_2 = \#_3 = Q_3 = W_2 = O_3 = D_3 = Y_1$

From the table above: A = 1-1 B = 121 Y = -21

Hence, set (d) cannot be '1' as that would make Y = 121, which combination is already pre-empted by 'B'. By the same reasoning set (d) cannot be '2' as that would also make A = 121. Therefore, set (d) can only be '3'.

It is now apparent that an error exists in set (c) or set (d). If one of them is accepted, then the other must be rejected. As the values contained in set (d) combine well with others already placed in the table of numerical components, that set will get the call and set (c) will be put on ice for the time being.

From this decision: Let set (d) equal '3'.

These values may now be added to the table.

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

And the Decipherment Table may also be set up.

Comp.		J		B	K		A						M			W						Y					
1st	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3
2nd	1	1	1	2	2	2	3	3	3	1	1	1	2	2	2	3	3	3	1	1	1	2	2	2	3	3	3
3rd	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
										S	S	S															
												O			O			O									

With seven complete letters represented and several others, of which one or two components have been recovered, the solver may now go to the message and test for possible plaintext fragments. The opening groups of the message shape-up as shown below.

Group 1										Group 2										Group 3									
W	D	W	A	J	A	#	S	Y	F	K	M	A	A	J	K	Y	M	L	D	Z	U	J	J	Y	Q	J	S	X	P
2	3	1.			3.	2	3	1.	1	1	2	2.	2	2	1.	1	3	1.	1			1.			.1	1	2.	1
3	1.	1	1	2.	1	3	1.			3	1.	1	1	2.	1	2	2.	3	2	1	2.	3	2	1.		3.	1	1
3.	2	1		.3	2	1.				1.	2	2	1.	1		.			3	2.	2	1	.		.			
						w				a				m								a						

In Group 2, it is observed that plaintext letter 'a' is followed by a doubled plaintext letter, represented by the vertical trio, 212. From numerical values thus far assigned, an excellent candidate for this combination is 'S', which is partially recovered as 21-. The letter 'S' frequently doubles, following vowels, and its presence at this location is looked on with favor because the plaintext sequence, 'ass-m', immediately suggests some form of the word 'assume', which is highly probable from what is known of the general nature of the subject matter of the message.

If this lead can be developed a definite entry will have been made and the solution of the message must, inevitably, follow.

Working with Group 2, alone, these possibilities exist.

Cipher:	K	M	A	A	J	K	Y	M	L	D
	1	2	2.	2	2	1.	1	3	1.	1
	3	1.	1	1	2.	1	2	2.	3	2
	1.	2	2	1.	1		.			3
Plaintext:	a				m					
	a	s	s	u	m	e				
Possible:	a	s	s	u	m	i	n	g		
	a	s	s	u	m	p	t	i	o	n

The word 'assume' fits without conflict.

The word 'assuming' is impossible because the third component of the letter 'I' has already been designated as '2'. Since the 1st and 2nd components of the plaintext letter following 'm' are shown to be 11, this would make 'i' equal 112, which combination is that representing the letter 'J'.

The word 'assumption' is also screened out as the components of plaintext 'o' of 'assumption' do not agree with the numerical components already assigned to the letter 'O'.

Consequently, the plaintext word 'assume' will be accepted for this location. This gives the following new values.

S = 212 U = 211 E = 11-

And from set (j) where $S_3 = V_3$ V = 2-2

Also derived from the above is the equivalence: $E_3 = L_2$.

Since both E_3 and U_1 (which is now known to be 2) are contained in set (c), it is now high time to locate the error in that set.

To attempt to search-out the error in set (c), it must first be broken up and the equivalencies from each original source must be collected separately. These are:

From Groups 1-2-3 and 12-13-14: $Z_2 = L_3$

From Groups 3-9 and 4-10: $P_1 = E_3$ $H_3 = C_3$

From Tetragraphic Patterns: $P_1 = U_1$ $L_3 = E_3$ $C_3 = G_3$
$G_3 = F_3$ $F_3 = L_3$

In set (c), the equivalent values collected from the tetragraphic patterns are the suspect group, as no conflicts have developed from the values which were derived from the long repeats. An opportunity to compare one source against the other is provided by the two equivalences, $P_1 = U_1$ and $P_1 = E_3$.

It has now been determined that $U_1 = 2$.

If $U_1 = P_1$ - then $P_1 = 2$.

If $P_1 = E_3$ - then $E_3 = 2$.

This would make 'E' equal 112; a combination pre-empted by 'J'.

Of the above equivalents, $P_1 = E_3$ is thought to be correct as it derives from a periodic bridge in which other satisfactory equal values have been found. For that reason, $P_1 = E_3$ will be accepted and $P_1 = U_1$ will be considered to be wrong.

Checking back to page 42 shows $P_1 = U_1$ comes from Test No. 21 which also contains $G_3 = F_3$. Both of these will now be thrown out as incorrect. The remaining equivalences of set (c) may now be re-assembled as two separate sets, thus:

Set (c-1) $F_3 = L_3 = Z_2 = E_3 = P_1$
Set (c-2) $H_3 = C_3 = G_3$

From plaintext 'assume' it has been found that $E_3 = L_2$ and, as L_2 is one of the values of set (f), then set (c-1) may be combined with set (f), giving:

Set (f) $Z_1 = \#_1 = L_2 = F_3 = L_3 = Z_2 = E_3 = P_1$

Now, if all values thus far determined are placed in the table, including set (f), a clear picture of the present status quo will be presented for further consideration and analysis.

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

Inspection of this table shows that (f) cannot be '1' as that would make E, L, and Z, all equal 111. Also, (f) cannot be '2' as that would make both 'E' and 'J' equal 112.

Hence, set (f) can only be '3'. When this numerical value is substituted for (f) in the table, no conflicts occur and so it is accepted as correct.

The table now shows these values.

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

And, rearranged numerically:

	J	E	B	K		A		L	U	S		M			W						Y			Z		
1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3
1	1	1	2	2	2	3	3	3	1	1	1	2	2	2	3	3	3	1	1	1	2	2	2	3	3	3
1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
											O		V	O		V	O			#			#			#

With this much of the table recovered, the remainder of the solution is mere routine. Substituting anywhere in the message gives additional values and the complete table is found to be:

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

Examination of the above shows many of the letters to be in alphabetic continuity, which indicates that this is the arrangement of the alphabet originally used by the constructor. It can be taken-off, vertically, from this keyword block.

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

Before leaving the cipher of The Three Wise Men, it might be well to investigate the circumstances which produced the error of equivalence in set (c). Here is what happened.

Gr. 30		G	I	S	M	T	P	J	V	T	K
Gr. 31	O	F	I	J	L	T	U	K	V	T	
		L	□	·	·	□	⊤	·	⊢	⊣	

Equivalents.

$G_3 = F_3$
$P_1 = U_1$

		G	I	S	M	T	P	J	V	T	K
		3	3	2	3	1	2	2	1	2	2
		2	1	1	2	3	3	1	3	1	1
		2	2	2	2	1	2	3	1	2	2
		h	i	s	h	a	n	d	a	s	s
O	F	I	J	L	T	U	K	V	T		
2	2	3	2	3	3	3	1	2	1		
1	2	1	3	3	1	2	3	2	1		
1	1	2	2	2	2	2	1	2	3		
u	m	i	n	g	I	h	a	v	e		

When the test was made there were sufficient identical cipher letters, covered by the pattern, to qualify this as a Class 'A', plaintext repeat. In spite of all this, the derived equivalents are incorrect - as shown when the groups are deciphered.

Particular attention is called to this because false leads of this nature are to be expected. When they are encountered they must be recognized as such and handled accordingly.

Another item of interest which may be checked, is the degree of accuracy of the "three confirmed" acceptance rule for equivalents indicated by tetragraphic patterns. In the cipher of The Three Wise Men, here is the box score.

EQUIVALENTS DERIVED FROM TETRAGRAPHIC PATTERNS.

	Total	Right	Wrong	%
Total Tabulated	47	38	9	.810
Class A - All, including repetitions	17	15	2	.882
Class B - All, including repetitions	30	23	7	.767
Class A - Repetitions omitted	16	14	2	.875
Class B - Repetitions omitted	28	21	7	.750
Class B - Duplicated in Class A	11	10	1	.909
Class B - Not duplicated in Class A	17	11	6	.647

This shows the high percentage of accuracy for this method of screening equivalents derived from patterns. It also shows that any assumed equivalence, thus derived, can be incorrect.

THE WRAP-UP.

Many amateur cryptanalysts have devoted a great deal of time, effort, and energy to devising methods for solving the Trifid. Frances A. Harris (S-TUCK) worked for countless weeks on a method based on spotting the plaintext word 'the'. Her system involves certain "must" letters which must be present in related position in order to produce this plaintext word. She had a great measure of success with it when working on Trifids of sufficient length.

Others have pet personal methods which they have devised. In some cases the use of three colors is favored to better identify the three different alphabets. Candela's approach to the problem was mathematical; or at least the descriptions of his technique, which have been publicized, are filled with mathematical terms and expressions - many of which are unintelligible to the average reader. His fetishism for Greek letters, frequently employed to the nth degree on his work sheets, might well lead one to believe that he first deciphered a Trifid in that ancient language, and then translated it into English.

In this modest booklet, the writer has tried to give a clear description of the Trifid system - how it operates and how it may be solved - in the simplest language at his command. Text of this nature is not easy to write - or read - but it is hoped that each and all who have had the patience to struggle through it, will be rewarded with an improved understanding of how to deal with this extremely interesting cipher system.

The End.

P R O B L E M S

TRIFIDS PROBLEMS

1 - Hot tip on how to solve Trifids in one easy lesson.

"homophones" repeated at locations underscored. Period is 10.

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

2 - Too bearish or too bare. B. NATURAL

Period is multiple of 3, plus zero.
Starts: "with whiskers". Last word: "before".
The sequence, "ecouldnev", can be spotted from part naturals

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

3 - Bibical data used by an American oil company. C-SHARPE

Period is 10. Starts: "A great".
Plaintext, "in the Bible", may be spotted by identification of two part naturals, I_2 and H_3. Repeat in Groups 24 and 25 will be helpful.

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

Note: In the above cipher an alphabetic take-off from a keyword block was employed to form the cipher alphabet.

4 - Cryptographic aid in bridge problem.

Period is 10. Given: "stmustwint". This can be spotted from part naturals. Solver should take full advantage of all aid to be derived from the repeat in Groups 12 and 16. A logical assumption can be made concerning the first word of the message. One part natural, which will show, should help.

♠ - none
♡ - J 8 7 6
◇ - A
♣ - A

♠ - 6
♡ - none
◇ - 10 7 6 2
♣ - Q

NORTH
W E
E A
S S
T T
SOUTH

♠ - 7
♡ - K Q 9
◇ - 5
♣ - J

♠ - J
♡ - none
◇ - J 9
♣ - 9 8 2

It is South's lead.

Spades are trump.

He must win five of the remaining tricks against any defense in order to make his bid.

His successful play is described in the message below.

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

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

5 - Quotation from a speech by C. Northcote Parkinson, relative to the Law he propounded.

Period is 10. A plaintext fragment will not be identified in this one but, knowing the grammatical structure of the cipher message, give some thought to what the repeat might be which leaves its pattern in Groups 1 and 20. And then, if you get anywhere with that, don't forget the name of the man to whom the quotation is credited.

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

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

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

Note: In No. 4 the cipher alphabet is a straight takeoff from a keyword block. In No. 5 an alphabetical takeoff from a keyword block is used to form the cipher alphabet.

6 - Concerning the finding of the Rosetta Stone and how a solution of its hieroglyphic inscriptions was finally achieved.

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

<u>SOLUTIONS</u> (Various types of alphabetic run-down.)

1 - Starts: ABQBOJFKXQFLK LC QEB QTBKQV . . . . . .
Keyword is: HKLTIBAD with SXZXKQ ZBIIP YBILT CLO RFBA IBQQBOP

2 - LBOFLA FP KFKB. RKPZOXJYIBA HBVTLOA XILEXYBQ FP RPBA. FQ FP: XCQBOTFPALJYZDE. . . etc.

3 - "in the Bible" FPFKD OLRMC LROQB BKUUU.
Group 24 is: B QEBOB TXP M

4 - QEKFJDNJOIQSZFOW. CEMMMTKMXFOPKPNA.

5 - ORKOY SKMPIMW.

6 - QFLKN ALAWP AZHVI TNCGY MQQQQ.