will exhibit several idiomorphic sequences, namely:

1 2 3 4 5 6	
..Z K Z G G Z....	(1)
..W U W Z Z W....	(2)
... . I B B I....	(3)
... . F Y Y F....	(4).

Lacking the knowledge as to the type of substitution alphabet involved, one may well decide that the four sequences are isomorphs, the first two probably, bearing a common prefix. If one suspects a Caesar substitution the usual generating process will disclose the actual plain texts. A simpler test would be to compare the coincidences of various suspected isomorphs. For instance, comparing (1) and (2), by setting $\pi N/\pi N$ at Z→W one finds K→H and G→D which are different from the required K→U and G→Z, whence, under the hypothesis, the two sequences are not isomorphic. By following this process one finds that only (3) and (4) are isomorphs for I→F and B→Y coincide at $\pi N/\pi N_x$.

17. The same message transformed with the incoherent alphabet previously given, by means of key FIRE

	F					I					R						E	
πN:	E	N	E	M	Y	A	T	T	A	C	K	R	E	P	E	L	L	E	D	W	E
πM:	W	Z	W	K	U	I	V	V	I	Y	E	Z	F	C	F	X	X	F	O	N	R

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

will exhibit the same number of idiomorphic sequences

1 2 3 4 5 6	
..F C F X X F..	(5)
..R L R O O R..	(6)
... . I V V I..	(7)
... . F Q Q F..	(8)

and by the simple test described in the preceding section a Caesar substitution will immediately be ruled out. This time, however, the cryptanalyst will be able to segregate the four idiomorphs into two different classes for, ..FX.. in (5) and ..FQ.. in (8) are inadmissible if (5) and (8) represent the same plain text.[1] The two classes readily suggest themselves:

F C F X X F	(5)		I V V I	(7)
R L R O O R	(6)	and	F Q Q F	(8)

That (5) and (6) are not isomorphs, the cryptanalyst will discover

1 The reader easily understands that the repeated F in column 3 of (5) and (8) is not due to our having just used a π M in the denominator of the substitution. It is the effect of the encipherment E~R→F and A~A→F, that is, A...E in πN and R...F in πM, an instance which may be considered fortuitous.

after painful exertions. But he is accustomed to rebuffs and accepts them philosophically...sometimes.

QUASI-APERIODIC SUBSTITUTIONS

18. We will now consider a *progressive* type of cipher in which the denominator of the substitution is shifted to the left one element at a time at each element of the clear text. Clearly, this is a periodic cipher with a key of 26.

Using a $\pi N/\pi N$ at initial coincidence A→S the idiomorphic phrase TOMORROW (A_1ABBA) becomes:

πN : T O M O R R O W
πN_5: L H G J N O M V

It is observed that the idiomorphic construction of the clear text has disappeared altogether in its cipher version. Of course, if the cipher text were subjected to a πN - generating

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

one could easily read the equivalent plain text on an *upward diagonal* generatrix. With a $\pi N/\pi M$ this could not be accomplished as has been noted in Sec. 13.

19. On the other hand a non-idiomorphic word such as SOUTHERLY will, in a $\pi N/\pi N$ substitution, yield an idiomorphic construction of type A_1BB_3A as shown hereunder at initial coincidence A→J

πN : S O U T H E R L Y
πN_J: B Y F F U S G B P
* _ _ *

Any repetition of the word SOUTHERLY in a plain text will yield a cipher sequence which is isomorphic with BYFFUSGB at any of the other 25 possible coincidences the system affords, such as

πN : S O U T H E R L Y
πN_P: H E L L A Y M H V
* _ _ *

In fact, at $\pi N/\pi N_G$ all the elements of the two isomorphs coincide

πN : B Y F F U S G B | P
πN_G: H E L L A Y M H | V. B→H, Y→E, etc.

20. Finally, a clear idiomorphic word such as PARALLELISM (A_1ABB_1B) will, in this system, yield an idiomorph in the cipher of an entirely different type, namely, (AB_2AC_2CB), if enciphered by means of the $\pi N/\pi M$ given earlier. In the example below the initial coincidence is A→R

πN | P A R A L L E L I S | M
πM | C B M O C K H N K B | E
* . * – – .

CONCLUDING REMARKS

21. This is not the place to list the various types of aperiodic or quasi-aperiodic substitution systems which yield isomorphism in their cipher texts. It suffices to say that progressive ciphers of all types submit to it. These may be of such elementary construction as that illustrated in Sec. 16 or of more complex structure as those which utilize a *fixed* number *n* of *variable* displacements. If the sum of the n displacements is a number prime to the number *m* of elements in the substitution (generally, 26) a periodic but very long key, equal to *nm* elements, is obtained. For instance, a period of 8 with displacements

+1+3+2+4+2+1+3+5

adding to 21 will result, if we use a 26-element transformation, into a periodic polyalphabetic substitution with a key of 8x26=208 apparently incoherent elements, the first few of which are the substitutions

1, 4, 6, 10, 12, 13, 16, 21,
22, 25, 1, 5, 7, 8, 11, 16,
17, 20, 22, 0, 2, 3, 6, 11,
12, 15, ..., etc.

To obtain longer keying sequences one merely increases the number *n* of displacements of the initial key.

Manual operation of this cipher or of those cognate with it is long and tiresome but variable displacements are easily realized mechanically. Such variable displacements form the basis for many ciphering machines.

22. A final word of caution must be given to the student. When dealing with ciphers of this type his principal task consists in isolating *idiomorphic sequences* the text contains. These may or may not be *isomorphic*. In selecting them for analysis he must give his preference to the more substantial looking ones, that is, those which exhibit the greater number of repeated elements for, very seldom indeed do they fail to prove their isomorphism, especially with systems making use of a large number of substitutions. Idiomorphs of the type A...A are the most troublesome ones and should be shunned until their isomorphism has been proven elsewhere.

III
LINEAR CONGRUENCES

CONGRUENCE MODULO M

23. If a and b are any two integers, positive, negative or zero, and if upon division by an integer m they leave the same remainder, a and b are said to be *congruent modulo m.* Thus, for instance, 20 and 14 are congruent modulo 3, for upon division by 3 they both leave the remainder 2.

$$20 : 3 = 3\times 6+2$$
$$14 : 3 = 3\times 4+2$$

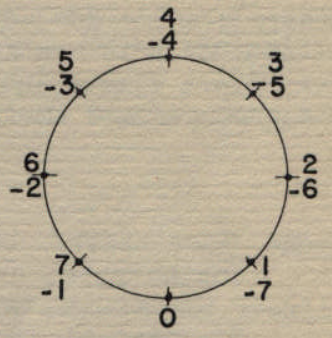
It is easy to see that the modulo m must be a divisor of the difference between a and b (20-14=6; 6=3x2), that is to say, the difference is a multiple of the modulo. The relation thus defined may then be written

$$a = b+cm$$
$$(20 = 14+2\times 3)$$

where c is an integer, positive, negative or zero.

The quantity c is not essential to the idea involved and it is more convenient to use a simpler notation due to Gauss, and write

$$a \equiv b \text{ modulo } m$$
$$(20 \equiv 14 \text{ modulo } 3)$$



which is read *a is congruent to b modulo m.*

24. Congruence in a physical sense, can be shown geometrically. If a directed circumference of a circle is divided into an equal number of parts, say 8, from an origin 0 and the points of division are associated with the integers 0,1...7, we can readily see that to transit 9 units from point 3 we land at point 4. This is because

$$3+9=12 \equiv 4 \text{ modulo } 8.$$

Moreover, in a closed ring the correspondences shown below hold, as can be verified in the illustration.

0	1	2	3	4	5	6	7
0	-7	-6	-5	-4	-3	-2	-1

Hence, if starting from point 4 we wish to travel 5 units in the direction opposite to the given one we reach station 7. This is because

$$4+(-5)= -1 \equiv 7 \text{ modulo } 8,$$

showing that the result of transit in any direction can be expressed by a *positive* quantity.

Furthermore, if from point O we wish to travel 3 distances of 6 units each we would reach point 2. This is because

$$3 \times 6 = 18 \equiv 2 \mod 8.$$

Summing up, the operations (+), (−), (×), on any integers, positive, negative or zero, can be carried out on any closed ring of m integers. The results thus obtained will be expressed with integers modulo m.

However, division, in the ordinary sense, is not possible in closed rings, but this difficulty can be overcome in some cases by using a special device, as will shortly be shown.

In cryptanalytics, we are most interested in modulo 26. A congruence table and a multiplication table both modulo 26 are given in Appendix I.

LINEAR CONGRUENCES

25. We shall, in the course of our work, be called upon to solve simple equations with one unknown, of the type

$$ax = c$$

where a and c are any integers. The solution $x = c/a$ exists, unless either a or c or both are zero, and may be an integer or a fraction.

In a finite system of numeration such equations are called linear congruences and the solution of the congruence

$$ax \equiv c \mod m$$

must, necessarily, be integral, for no fractions exist in the system.

Furthermore, depending on the parity of the integers a, c and m, linear congruences may have one or more or no solutions.

The general theorem governing the number of solutions of a given linear congruence is now given without proof.

Let

$$ax \equiv c \mod m$$

be any linear congruence and let a and m have the greatest common divisor d ($d \geq 1$). Then a necessary and sufficient condition for the existence of solutions of the congruence is that c be divisible by d. If this condition is satisfied the congruence has just d solutions, and all the solutions are congruent modulo m/d.

In accordance with this theorem the congruence

$$ax \equiv c \mod 26$$

has:

a) no solution	when a is even		and c is odd
b) no solution	when $a = 13$		and $c \neq 13$
c) one solution	when a is odd	except 13	and c is even or odd
d) two solutions	when a is even		and c is even
e) 13 solutions	when $a = 13$		and $c = 13$

26. The integral solutions of the congruence

$$ax \equiv c \pmod{26}$$

when a and c satisfy the relations shown above can be found in two different ways.

FIRST METHOD. Using the congruence table, modulo 26, write down the first few numbers congruent to c. Among them there is at least one which is a multiple of a. Divide such number by a. The quotient is the integral solution sought. It is evident that any other multiple of a congruent to c is also congruent to the quotient just found. For instance, let us solve the congruence

$$4x \equiv 22 \pmod{26}.$$

$$\begin{array}{lllllll} 22 \equiv 48, & 74, & 100, & 126, & 152, & 178, & 204 \ldots \\ \div 4 = 12 & & 25 & & 38 & & 51 \\ & & & & \equiv 12 & & \equiv 25 \ldots \end{array}$$

$$x = 12 \text{ or } 25$$

SECOND METHOD. This method is quicker and more direct. Moreover, it gives all the required solutions forthrightly. It consists in finding out which integer when multiplied by a is equal to c. Using the multiplication table modulo 26, look for c on row a. The integers at the top of the table opposite the various c's are the solutions sought. Here are a few examples:

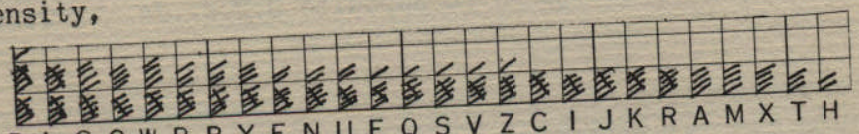
1) $5x \equiv 19$; on line 5, 19 is opposite 9, $\therefore x = 9$
2) $5x \equiv 18$; on line 5, 18 is opposite 14, $\therefore x = 14$
3) $6x \equiv 20$; on line 6, 20 is opposite 12 and 25, $\therefore x = 12$ or 25
4) $6x \equiv 17$; on line 6, there is no 17, $\therefore x$ has no solution
5) $13x \equiv 4$; on line 13, there is no 4, $\therefore x$ has no solution
6) $13x \equiv 13$; on line 13, 13 is opposite 1,3,5..25 $\therefore x = 1,3,5..25$
7) $13x \equiv 0$; on line 13, 0 is opposite 0,2,4..24 $\therefore x = 0,2,4..24$

IV
METHOD OF SOLUTION

27. We shall now investigate the cryptogram appearing hereunder. In it, the repeated sequences which emerge from the usual biliteral distribution, here omitted, are suitably underscored:

```
                5                  10                 15                 20                 25
F P N B O   A X Y Z N   I L Q E B   N D J Z U   V G K T V

               30                 35                 40                 45                 50
L W B I N   E J V O E   J G Q C P   D L W Z U   O B X O Y

               55                 60                 65                 70                 75
K S R D P   E S D G L   O Z D M O   E P U B G   F R R M K

               80                 85                 90                 95                100
A H N L F   G U Q M X   Y Q H L B   W K C W N   W Y V R G

              105                110                115                120                125
B Z L E F   C P C Y O   W O U D Y   L U S L A   D J I E I

              130                135                140                145                150
P D Z T D   B U X J S   W C L A D   Y S G R S   Q N M K W  =>

              155                160                165
<=  Y O T F D   P W Q I V   P G F G V
```

28. The uniliteral distribution of the elements, rearranged in descending order of density,



indicates that the cryptogram is a polyalphabetic substitution of some sort.

29. The question now arises whether the substitution is a periodic one or not. There is no way of telling ocularly from the material on hand. It is observed, however, that the repetitions in the cryptogram are numerous but *very short*, mostly digraphs, and that the graph is extremely *flat*. To an experienced cryptanalyst these characteristics suggest a multiplicity of transofmrations, that is to say, a keying apparatus of considerable length. Further analysis will disclose whether such an apparatus has been applied periodically or aperiodically.

30. The familiar factorization of the various repetitions shows that most

of them are separated by large, distinct, prime number of elements, LAD, 138-119=19; CP, 106-39=67; DP, 155-54=101; FG, 163-80=83; OE, 65-34=31) or by twice a large prime (MK, 148-74=74=2X27; PD, 126-40=86=2X43). The remaining ones are those which can only be considered as to a possible periodicity of the key:

			Possible Factors	
DJ:	121- 12 =	104	4 . . . 8 . .	13
DY:	140-114 =	26	. . . : . . .	13
EJ:	35- 31 =	4	4	.
GF:	162- 70 =	92	4	23
LW:	42- 26 =	16	4 . . . 8 . .	.
WY:	150- 96 =	54	. . 6 . . 9 .	.
XY:	85- 7 =	78	. . 6	13
YO:	151-109 =	42	. . 6 7 . . .	.
ZU:	44- 19 =	25	. 5	.

If we put any credence whatever in the flatness of the graph, we should disregard periods 4, 6 and 8 and apply the ϕ-test to period 13; if not, we should test them all!

We shall suppose that we have performed one or all such tests and that their results have proven negative. Our cryptogram is not, therefore, a periodic polyalphabetic substitution; at least, not one of common species.

31. We then institute a search for possible isomorphs,[2] that is, idiomorphic sequences which might eventually turn out to be real isomorphs. Unfortunately, our message does not exhibit any *substantial looking* ones; the best it can offer are the weak segments:

21-25: ...V G K T V...
61-65: ...O Z D M O...

Hopefully, we test the vertical pairs on a $\pi N/\pi N$ slide. The elements correspond at A→T. Hence, the sequences are truly isomorphic. We, of course, try to extend the sequences on both sides as far as such correspondence permits, thus isolating the isomorphs to a length of ten letters, forty elements apart.

21-30	..U	V G K T V L W B I N	E..
61-70	..L	O Z D M O E P U B G	F..

Since the cryptogram admits of isomorphs, we infer, if we feel prone, to disregard the class of monoalphabetic transformations on constant or variable sequences of plain text,[3] that the keying system of encipher-

1 This is a test for monoalphabeticity. The reader who is acquainted with it may find the table "ϕ - VALUES FOR SMALL DISTRIBUTIONS" given in Appendix I useful. This is not the place to explain the derivation of the test.

2 This is quite a tedious task for lone *amateurs* like ourselves who do cryptanalysis for sheer fun. The *professionals* who get paid to do it use computing machines which point out idiomorphic sequences in short time.

3 Incidentally, the step suggested in the section next following would readily uncover any system in this class.

ment is, structurally, a progressive one. Hence, there exists a *period*, however long, which governs the succession of the various substitution alphabets.

32. An industrious analyst would, at this point, try to *translate* the isomorphs by resorting to a modification of the familiar *generating* process used with the trivial Julius Caesar types of transformations.

$\pi N/\pi N_A$

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

$\pi N/\pi N_A^{-1}$

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

He would, of course, align the required number of vertical slides on *any* decipherment, (say A→A), of either isomorph, both on $\pi N/\pi N$ and $\pi N/\pi N^{-1}$

As we have seen in Sec. 18, if the keying sequence had consisted in a uniform rotation of the disc (or a uniform displacement of the slide), *one element at a time*, an upward 45 degree diagonal, from left to right, on either generating diagram, depending on the substitution alphabet used, would yield the equivalent plain text. Similarly, uniform rotations of 2 or 3 or n elements would merely increase the angle of the diagonal. With a series of variable rotations, the analyst's *knack* in anagramming letters from broken diagonals to form acceptable plain text would lead him to quick solution. In this he would be aided by the consideration that the variable coefficients of the displacements are generally small, which would limit his jumping up from column to column to short skewed steps.

We leave the reader with his experimentations. If he fails, he can console himself by following our footsteps to the end. He can later come back to this point to realize how simple the *trick* really is.

33. Having acquired the notion that the substitution alphabet is either $\pi N/\pi N$ or $\pi N/\pi N^{-1}$ it is possible to segregate *all* the isomorphic sequences the message may contain. This is accomplished by merely measuring on a normal alphabet the successive distances between the cipher elements in the scale, 0,1,...25. It is easy to see that isomorphic segments which cannot otherwise be identified through their literal representations *must* yield *repeated* numerical sequences. Furthermore, such repeated numerical sequences will, necessarily, be one element shorter than their corresponding isomorphs.

If a twice repeated πN denominator is made to slide against the scale 0,1...25 as a numerator, an easy and quick method of deriving the distance between a pair of elements is to set the first one of such pair under zero and to read in the scale the numeral which coincides with the second letter. Thus, the distance between F and P, the first two elements of the cryptogram, is found to be 10 by setting the slides as illustrated.

```
                0 1 2 3 4 5 6 7 8 9 10 11 12 . . .
A B C D E F G H I J K L M N O P Q R . . .
          *             *
```

The cryptogram with distances between elements, as defined, follows. Again, a binumerical distribution (not shown here) helps in exposing *all* repetitions. These are suitably marked.

```
          5                   10                  15                  20
F P N B O A X Y Z N I L Q E B N D J Z U
10 24 14 13 12 23 01 01 14 25 03 05 14 23 12 16 06 16 21 01

          25                  30                  35                  40
V G K T V L W B I N E J V O E J G Q C P
11 04 09 02 16 11 05 07 05 17 05 12 19 16 05 23 10 12 13 14

          45                  50                  55                  60
D L W Z U O B X O Y K S R D P E S D G L
08 11 03 21 20 13 22 17 10 12 08 25 12 12 15 14 11 03 05 03

          65                  70                  75                  80
O Z D M O E P U B G F R R M K A H N L F
11 04 09 02 16 11 05 07 05 25 12 00 21 24 16 07 06 24 20 01 ===>

          85                  90                  95                  100
G U Q M X Y Q H L B W K C W N W Y V R G
<== 14 22 22 11 01 18 17 04 16 21 14 18 20 17 09 02 23 22 15 21

          105                 110                 115                 120
B Z L E F C P C Y O W O U D Y L U S L A
24 12 19 01 23 13 13 22 16 08 18 06 09 21 13 09 24 19 15 03
```

```
                125                 130                 135                 140
D J I E I P D Z T D B U X J S W C L A D
06 25 25 04 07 14 22 20 10 24 19 03 12 09 04 06 09 15 03 21 →

                145                 150                 155                 160
Y S G R S Q N M K W Y O T F D P W Q I V
← 20 14 11 01 24 23 25 24 12 02 16 05 12 24 12 07 20 18 13 20

                165
P G F G V
17 25 01 15
```

34. A brief discussion touching upon repeated numerical sequences of the kind we have obtained is due. It was asserted in the preceding section that cipher isomorphs must yield repeated numerical sequences. On the other hand, the converse is not necessarily true; that is, repeated numerical sequences need not represent isomorphs. For, there exist *isomorphic plain-text* sequences, at some coincidence in $\pi N/\pi N$. These are, at times, of appreciable length. For instance, the clear pentagraphs THE TRue and ESPECially are isomorphic in $\pi N/\pi N_L$ as can readily be verified.

```
T H E T R -- ABCDEFGHIJKLMNOPQRST...
E S P E C -- LMNOPQRSTUVWXYZABCDE...
```

Hence, such pentagraphs, if transformed by means of *isomorphic keys*, must show isomorphism in their cipher equivalents. In fact, actual encipherments by such keys exhibit such an isomorphism.

```
KEY:      ..B D G H I..      ..M O R S U..
d_K::       2 3 1 2            2 3 1 2
PLAIN:    T H E T R          E S P E C
CIPHER:   U K K A A          Q G G W W
d_C:      16 0 16 0          16 0 16 0
```

Of course, these pseudo-isomorphs occur only too rarely and when they do, they do not hinder or retard solution. Strangely, their presence strengthens the proportion of the most common divisor in the factorization analysis.

35. The cryptogram, apparently, is replete with isomorphs. Most or all of them must descend from repetitions in the plain text. Obviously, the repetitions are collinear with isomorphic keying sequences. Hence, they must show a common divisor which represents the number of keying elements composing the various isomorphic keying periods.

The table hereunder exhibits the factorizations of the isomorphs.

METHOD OF SOLUTION

ISOMORPHS	LOCATION		DISTANCE	POSSIBLE FACTORS	
10,24	129	1	128	4 . . . 8	
01,14	80	8	72	4 . 6 . 8 9 ... 12	
03,05	58	11	47	. . . . .	47
11,04,09	61	21	40	4 5 . . 8 . 10. .	
09,02	95	23	72	4 . 6 . 8 9 . . 12	
09,02	95	63	32	4 . . . 8	
03,21,20	139	43	96	4 . 6 . 8 . . . 12	
06,09	136	112	24	4 . 6 . 8 . . . 12	
				7 · 1 4 . 7 2 1 . 4	

We note that the most preponderant divisors are 4 and 8, each appearing 7 times. In the absence of any isolated factor 4, it may safely be assumed that the isomorphic periods consist of 8 variable displacements the sum Σ of which is still unknown to us.

36. We re-write, side by side, both the cryptogram and the numerical distances between its elements in arrays of 8 columns. All isomorphic sequences are underscored in both arrays, similarly:

	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-1
1	10	24	14	13	12	23	01	01 ⟹
2	⟸ 14	25	03	05	14	23	12	16
3	06	16	21	01	11	04	09	02 →
4	⟸ 16	11	05	07	05	17	05	12
5	19	16	05	23	10	12	13	14
6	08	11	03	21	20	13	22	17
7	10	12	08	25	12	12	15	14
8	11	03	05	03	11	04	09	02 →
9	⟸ 16	11	05	07	05	25	12	00
10	21	24	16	07	06	24	20	01 ⟹
11	⟸ 14	22	22	11	01	18	17	04
12	16	21	14	18	20	17	09	02
13	23	22	15	21	24	12	19	01
14	23	13	13	22	16	08	18	06 ⟹
15	⟸ 09	21	13	09	24	19	15	03
16	06	25	22	04	07	14	22	20

	1	2	3	4	5	6	7	8
1	F	P	N	B	O	A	X	Y ⟹
2	⟸ Z	N	I	L	Q	E	B	N
3	D	J	Z	U	V	G	K	T →
4	⟸ V	L	W	B	I	N	E	J
5	V	O	E	J	G	Q	C	P
6	D	L	W	Z	U	O	B	X
7	O	Y	K	S	R	D	P	E
8	S	D	G	L	O	Z	D	M →
9	⟸ O	E	P	U	B	G	F	R
10	R	M	K	A	H	N	L	F ⟹
11	⟸ G	U	Q	M	X	Y	Q	H
12	L	B	W	K	C	W	N	W ⟹
13	⟸ Y	V	R	G	B	Z	L	E
14	F	C	P	C	Y	O	W	O ⟹
15	⟸ U	D	Y	L	U	S	L	A
16	D	J	I	E	I	P	D	Z

	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-1
17	10	24	19	03	12	09	04	06 ⟹
18	⟸ 09	15	03	21	20	14	11	01
19	24	23	25	24	12	02	16	05
20	12	24	12	07	20	18	13	20
21	17	25	01	15				

	1	2	3	4	5	6	7	8
17	T	D	B	U	X	J	S	W ⟹
18	⟸ C	L	A	D	Y	S	G	R
19	S	Q	N	M	K	W	Y	O
20	T	F	D	P	W	Q	I	V
21	P	G	F	G	V			

We shall now set up a system of equations (linear congruences) each of which will bind a given pair of isomorphs to its numerical equivalent in the following manner.

Trigraph (10,24) appearing in lines 1 and 17 corresponding to isomorphs FPN→TDB are 16 periods apart, (17-1). This means that the distance between the corresponding elements of the isomorphs (F→T. or P→D. or N→B) is equal to 16 times the sum of the displacements forming the period, that is, 16Σ. On the other hand, the generated distance between the same elements, F→T or P→D or N→B in πN is 14. Obviously the two distinct numerical values of the distance between identical pairs are congruent with respect to modulo 26. Hence

Line 1 FPN
Line 17 TDB : $16\Sigma \equiv 14$ (modulo 26) (1)

Similarly, trigraph (01,14) in lines 1 and 10 corresponding to isomorphs YZN→FGU are 9 periods apart, (10-1); that is 9Σ, but the generated distance between YZN and FGU is 7, whence

Line 1 YZN
Line 10 FGU : $9\Sigma \equiv 7$ (modulo 26). (2)

Treating all other isomorphs in like manner, we get:

Line 3 VGKTVLWBIN
Line 8 OZDMOEPUBG : $5\Sigma \equiv 19$ (modulo 26), (3)

Line 6 WZUO
Line 18 ADYS : $12\Sigma \equiv 4$ (modulo 26), (4)

Line 3 KTV
Line 12 NWY : $9\Sigma \equiv 3$ (modulo 26), (5)

Line 8 DMO
Line 12 NWY : $4\Sigma \equiv 10$ (modulo 26), (6)

Line 14 OUD
Line 17 WCL : $3\Sigma \equiv 8$ (modulo 26), (7)

Solving these congruences in accordance with the method given in

Sec. 26, we obtain the following integral values for Σ.

1 : Σ = 9 and 22
2 : Σ = 21
3 : Σ = 9
4 : Σ = 9 and 22
5 : Σ = 9
6 : Σ = 9 and 22
7 : Σ = 20

It is easy to see from the results just obtained that congruences (2) and (7) do not belong to the system. Hence the cipher sequences from which they emerge are pseudo-isomorphs; that is, they are not equivalent to identical plain text but to isomorphic plain text (Sec. 8), as we shall shortly be able to verify. On the other hand, all the other congruences with common integral solution 9 delineate true cipher isomorphs which yield repetitions in the plain text.

The value Σ=9, while possible, appears to be too small for a period containing 8 variable displacements. If this value is correct, and barring unseemly *null* (zero) displacements, seven of the eight displacements must have value 1 and the other, 2; that is, all the enciphering alphabets but one are adjacent in $\pi N/\pi N$. A quick verification can be made.

If the longest isomorph, the decagraph VGKTVLWBIN. is generated in $\pi N/\pi N$ we should be able to read its plain text equivalent on two adjacent 45 degree diagonals, the break taking place at displacement 2. In the worst case, if displacement 2 is located near the center of the isomorph, we should be able to read at least a plain text pentagraph on a single diagonal.

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

The search proves futile and we must, therefore, infer that the solution Σ = 9 in $\pi N/\pi N$ is not applicable to our problem. But since the cryptogram has yielded isomorphs in $\pi N/\pi N$ it is obvious that the substi-

tution alphabet must then be $\pi N/\pi N^{-1}$ in which case the value of Σ must be the negative of 9 (modulo 26); that is, 17. Therefore, the alternative solution.

$$\Sigma = 17 \text{ in } \pi N/\pi N^{-1}$$

is the one which must solve the cryptogram. Hence, the transformation is an ordinary, so-called, Beaufort.

37. The reading of the cryptogram is not yet at hand. We do not know the value of the partial displacements between the elements in each period. Nor are we interested in them, yet. But we do know that each keying element in each period is 17 *notches* forward of its corresponding element in the preceding period. In other words, period 1 (and its elements) is 1x17=17 forward of period 0; period 2 is 2x17=34 forward of period 0; period 3 is 3x17=51 forward of period 0, etc. Therefore, referring to the Multiplication Table (modulo 26) in the appendix we can get the successive multiples of 17 (modulo 26) which can be read across line 17. These are

17x...	0	1	2	3	4	5	6	7	8	9	10	11	12	13
= ...	0	17	8	25	16	7	24	15	6	23	14	5	22	13

17x...	14	15	16	17	18	19	20	21	22	23	24	25	26	27..
= ...	4	21	12	3	20	11	2	19	10	1	18	9	0	17..

after which the series recurs.

Now, it is easy to see that if we decipher all the elements in a given row of the cipher array by the multiple of Σ=17 (modulo 26) corresponding to that row, the elements so transformed will be in the *identical* keying sequence as the elements on the zero row. Therefore, if transformations so defined are carried out on all the rows, the resulting array will be a *periodic* polyalphabetic substitution with period 8. Hence, the elements on each of its columns will be *monoalphabetic* substitutions.

The transformation so described can be performed in two ways. The first utilizes a $\pi N/\pi N$ substitution and the transformed cryptogram will *remain* a $\pi N/\pi N^{-1}$ substitution (Beaufort). The second makes use of a $\pi N/\pi N^{-1}$ alphabet and the transformed cryptogram will then become an ordinary $\pi N/\pi N$ substitution (Vigenère). A mathematical proof of this statement will involve a symbolism beyond the nature of this paper. A practical demonstration will suffice. Thus:

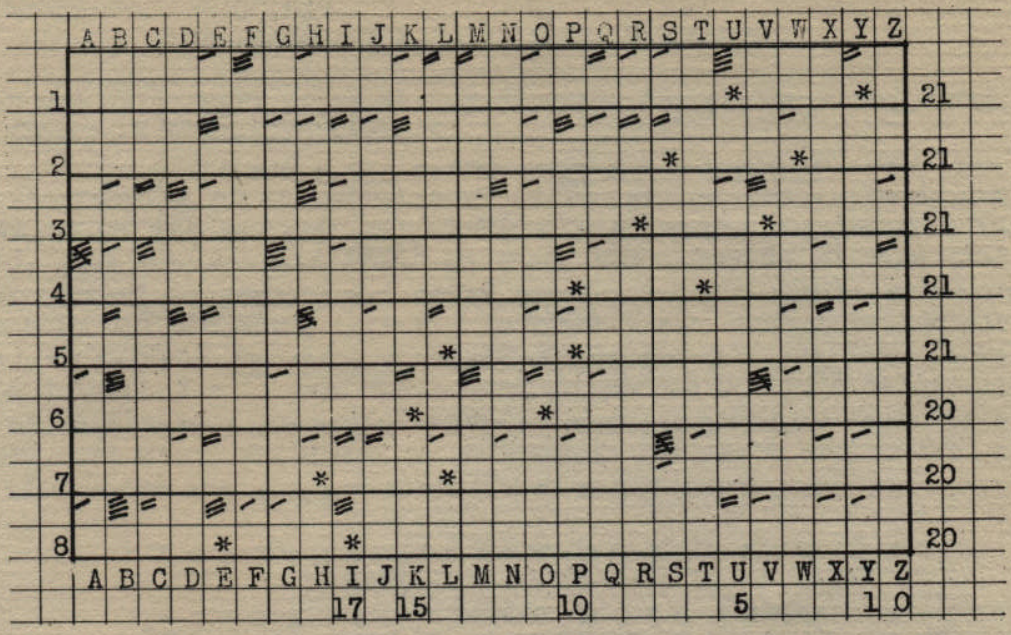
πN :	FATHER	πN :	PUBNQD	πN :	FATHER
πN_U^{-1}:	PUBNQD	πN_K^{-1}:	VQJXUH	πN_Q :	VQJXUH

38. We exhibit hereunder the cryptogram and its transformation in πN/πN:

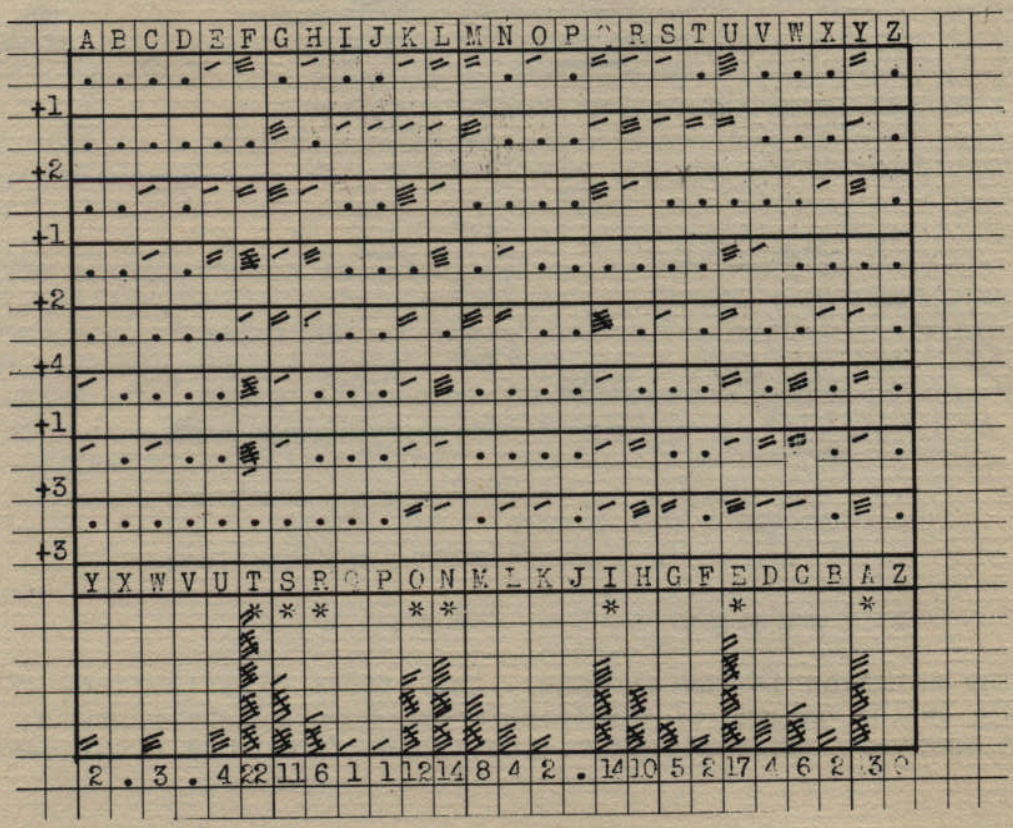
	CRYPTOGRAM	~ πN/πN →	PERIODIC TRANSFORMATION
	1 2 3 4 5 6 7 8		1 2 3 4 5 6 7 8
1	F P N B O A X Y	~ 0=A →	F P N B O A X Y
2	Z N I L Q E B N	~ 17=R →	Q E Z C H V S E
3	D J Z U V G K T	~ 8=I →	L R H C D O S B
4	V L W B I N E J	~ 25=Z →	U K V A H M D I
5	V.O E J G Q C P	~ 16=Q →	L E U Z W G S F
6	D L W Z U O B X	~ 7=H →	K S D G B V I E
7	O Y K S R D P E	~ 24=Y →	M W I Q P B N C
8	S D G L O Z D M	~ 15=P →	H S V A D O S B
9	O E P U B G F R	~ 6=G →	U K V A H M L X
10	R M K A H N L F	~ 23=X →	O J H X E K I C
11	G U Q M X Y Q H	~ 14=O →	U I E A L M E V
12	L B W K C W N W	~ 5=F →	Q G B P H B S B
13	Y V R G B Z L E	~ 22=W →	U R N C X V H A
14	F C P C Y O W O	~ 13=N →	S P C P L B J B
15	U D Y L U S L A	~ 4=E →	Y H C P Y W P E
16	D J I E I P D Z	~ 21=V →	Y E D Z D K Y U
17	T D B U X J S W	~ 12=M →	F P N G J V E I
18	C L A D Y S G R	~ 3=D →	F O D G B V J U
19	S Q N M K W Y O	~ 20=U →	M K H G E Q S I
20	T F D P W Q I V	~ 11=L →	E Q O A H B T G
21	P G F G V	~ 2=C →	R I H I X

The solution is now at hand. Uniliteral distributions of the elements in the columns of the transformed array are taken and $F_P \ldots A_P$ easily spotted. The successive positions of A_P show displacements

1,2,1,2,4,1,3,3 totaling to 17, which affirms the value of Σ previously found, analytically.



For curiosity's sake, the distributions are shifted at their proper superimposition. The consolidated diagram exhibits the monoalphabetic distribution of the entire plain text which appears to be fairly normal excepting for exceedingly strong T_p and M_p and very weak R_p.



39. The transformed cryptogram and its plain text are now given side by side. The reader will carefully note the pseudo-isomorphs derived from congruences (2) and (7)

(01,14) YZN → YQE → ..boo KIS wri..
FGU → CUI → ..led GEO r....

and

(06,09) OUD → BYH → ....c HAP ter..
WCL → IFO → ...th ATI s not

exhibit isomorphic plain text equivalent at $\pi N/\pi N_w$ and $\pi N/\pi N_T$ respectively.

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

And finally the weary reader may go back, if he so wishes, to the generating diagram of the decagraph VGKTVLWBIN in $\pi N/\pi N'$ and see how easily he could have extracted from it the corresponding plain text equivalent MATHEMATIC(ians, al).

APPENDIX I
PLATE 1

N	EXPECTED ϕ_r ALL LANGUAGES	EXPECTED ϕ_p				
		ENGLISH (.0667)	FRENCH (.0778)	GERMAN (.0762)	ITALIAN (.0738)	SPANISH (.0775)
11	4.2	7.3	8.5	8.3	8.1	8.5
12	5.0	8.8	10.2	10.0	9.7	10.2
13	6.0	10.4	12.1	11.8	11.5	12.0
14	7.	12.1	14.1	13.8	13.4	14.1
15	8.0	14.0	16.3	16.0	15.4	16.2
16	9.2	16.0	18.6	18.2	17.7	18.6
17	10.4	18.1	21.1	20.7	20.3	21.0
18	11.7	20.4	23.8	23.3	22.5	23.7
19	13.1	22.8	26.6	26.0	25.2	26.5
20	14.6	25.3	29.5	28.9	28.0	29.4
21	16.1	28.0	32.6	32.0	30.9	32.5
22	17.7	30.8	35.9	34.8	34.0	35.8
23	19.4	33.7	39.3	38.5	37.3	39.2
24	21.4	36.8	42.9	42.0	40.7	42.7
25	23.1	40.0	46.6	45.7	44.2	46.5
26	25.0	43.3	50.5	49.5	47.9	50.3
27	27.0	46.8	54.6	53.4	51.8	54.4
28	29.1	50.4	58.8	57.8	55.7	58.5
29	31.2	54.1	63.1	61.8	59.9	62.9
30	33.4	58.2	67.6	66.2	64.2	67.4
31	35.8	62.0	72.3	70.8	68.6	72.0
32	38.1	66.1	77.1	75.5	73.2	76.8
33	40.6	70.4	82.1	80.4	77.9	81.8
34	43.1	74.8	87.2	85.4	82.8	86.9
35	45.8	79.3	92.5	90.6	87.8	92.2
36	48.5	84.0	98.0	96.0	92.9	97.6
37	51.2	88.8	103.6	101.4	98.3	103.2
38	54.1	93.7	108.9	106.6	103.3	108.5
39	57.0	98.8	115.2	112.9	108.7	114.8
40	60.0	104.0	121.3	118.8	115.2	120.9
41	63.1	109.3	127.5	124.9	121.0	127.1
42	66.2	114.8	133.9	131.2	127.0	133.4
43	69.5	120.4	140.5	137.6	133.2	139.9
44	72.8	126.1	147.1	144.1	139.6	146.6
45	76.2	132.0	154.0	150.8	146.1	153.4
46	79.6	138.0	161.0	157.7	152.7	160.4
47	83.2	144.2	168.2	164.7	159.5	167.5
48	86.8	150.4	175.5	171.9	166.5	174.8
49	90.5	156.8	182.9	179.2	173.5	182.2
50	94.3	163.4	190.6	186.6	180.8	189.8

Ø-VALUES FOR SMALL DISTRIBUTIONS

CONGRUENCE TABLE
(MODULO 26)

0	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	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51
52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77
78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103
104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128	129
130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155
156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181
182	183	184	185	186	187	188	189	190	191	182	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233
234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259
260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285
286	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311
312	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337
338	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363
364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389
390	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415
416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441
442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467
468	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493
494	495	496	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519
520	521	522	523	524	525	526	527	528	529	530	531	532	533	534	535	536	537	538	539	540	541	542	543	544	545
546	547	548	549	550	551	552	553	554	555	556	557	558	559	560	561	562	563	564	565	566	567	568	569	570	571
572	573	574	575	576	577	578	579	580	581	582	583	584	585	586	587	588	589	590	591	592	593	594	595	596	597
598	599	600	601	602	603	604	605	606	607	608	609	610	611	612	613	614	615	616	617	618	619	620	621	622	623
624	625	626	627	628	629	630	631	632	633	634	635	636	637	638	639	640	641	642	643	644	645	646	647	648	649
650	651	652	653	654	655	656	657	658	659	660	661	662	663	664	665	666	667	668	669	670	671	672	673	674	675

X	0	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
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	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
2	0	2	4	6	8	10	12	14	16	18	20	22	24	0	2	4	6	8	10	12	14	16	18	20	22	24
3	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23
4	0	4	8	12	16	20	24	2	6	10	14	18	22	0	4	8	12	16	20	24	2	6	10	14	18	22
5	0	5	10	15	20	25	4	9	14	19	24	3	8	13	18	23	2	7	12	17	22	1	6	11	16	21
6	0	6	12	18	24	4	10	16	22	2	8	14	20	0	6	12	18	24	4	10	16	22	2	8	14	20
7	0	7	14	21	2	9	16	23	4	11	18	25	6	13	20	1	8	15	22	3	10	17	24	5	12	19
8	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18
9	0	9	18	1	10	19	2	11	20	3	12	21	4	13	22	5	14	23	6	15	24	7	16	25	8	17
10	0	10	20	4	14	24	8	18	2	12	22	6	16	0	10	20	4	14	24	8	18	2	12	22	6	16
11	0	11	22	7	18	3	14	25	10	21	6	17	2	13	24	9	20	5	16	1	12	23	8	19	4	15
12	0	12	24	10	22	8	20	6	18	4	16	2	14	0	12	24	10	22	8	20	6	18	4	16	2	14
13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13
14	0	14	2	16	4	18	6	20	8	22	10	24	12	0	14	2	16	4	18	6	20	8	22	10	24	12
15	0	15	4	19	8	23	12	1	16	5	20	9	24	13	2	17	6	21	10	25	14	3	18	7	22	11
16	0	16	6	22	12	2	18	8	24	14	4	20	10	0	16	6	22	12	2	18	8	24	14	4	20	10
17	0	17	8	25	16	7	24	15	6	23	14	5	22	13	4	21	12	3	20	11	2	19	10	1	18	9
18	0	18	10	2	20	12	4	22	14	6	24	16	8	0	18	10	2	20	12	4	22	14	6	24	16	8
19	0	19	12	5	24	17	10	3	22	15	8	1	20	13	6	25	18	11	4	23	16	9	2	21	14	7
20	0	20	14	8	2	22	16	10	4	24	18	12	6	0	20	14	8	2	22	16	10	4	24	18	12	6
21	0	21	16	11	6	1	22	17	12	7	2	23	18	13	8	3	24	19	14	9	4	25	20	15	10	5
22	0	22	18	14	10	6	2	24	20	16	12	8	4	0	22	18	14	10	6	2	24	20	16	12	8	4
23	0	23	20	17	14	11	8	5	2	25	22	19	16	13	10	7	4	1	24	21	18	15	12	9	6	3
24	0	24	22	20	18	16	14	12	10	8	6	4	2	0	24	22	20	18	16	14	12	10	8	6	4	2
25	0	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

MULTIPLICATION TABLE

MODULO 26

Exercise 1.

W B V A T N F G X A Z Z W I X Q Y I D B P D J F T Y Y Z T M

N D W O E C W Q M A O P G I T N Z Q J Q T T O L Z S J O O P

J C W N N Y R H Z X L I A P H X J X O P I B O W I O K S B R

Q B K Z X N L B U O M M D U U J Y N T M Q X P X Y A V K Z Z

S N K W L L W M I Z H H Q R E F A Z S E N S F O K B J N Q L

M E W D Y R B Q S G W K J I

Exercise 2.

D J I N Y W K E Z N R V K D I O Q V D W U A Q L J T V Q N M

M Y I B T C R V N G D Q V D R G S Z O Z V M K D J V L C S N

O Z P H A Q G A D U A W I Y X I T O M W H I O A Z A B C N O

V B D Q E D P B G O H F Y W G F O T V J V U E B Q W J S N Y

T S U X B Q E C N A R E N Q B F P Z O Q V S R U T E R V X O

M L L V K E N M Z I Y J Q G B W I K N R R S X V G H Q V P M

RESEARCHES IN CRYPTOGRAPHY AND DECRYPTING

A Series edited by Rosario Candela - Issue II

ISOMORPHISM

AND ITS APPLICATIONS IN CRYPTANALYTICS

By

ROSARIO CANDELA, A.I.A.

Visiting Lecturer in Cryptanalytics
Hunter College of the City of New York
1941-1943

CARDANUS PRESS

NEW YORK

1946

TABLE OF CONTENTS

FOREWORD

The Annual Convention of the American Cryptogram Association, of which I am a member, is to take place within the next three weeks, here, in the fair City of New York.

The New York Cipher Society, which I address very nearly every month and whose first President it was my privilege to be, is host to the Convention. The Committee on Arrangements is honoring me in requesting that I address the Convention on the evening of September first. This I hope to do and, if it will come to pass, I shall do it with pleasure indeed and in a manner, I again hope, befitting the occasion.

The topic of the address will be the one which is treated in this paper. This has been hastily gotten together from a broader study on MATHEMATICAL CONCEPTS AND THEIR APPLICATIONS IN CRYPTANALYTICS, now in preparation. Of these concepts, ISOMORPHISM is an exceedingly elegant one. Furthermore, it is an extraordinarily powerful tool for the solution of an entire class of fairly complex cipher systems.

For reasons which must seem obvious, the treatment in this paper has been confined, without loss of generality, to just one such system with the further restriction that the substitution alphabets involved are normal ones. To have extended the address to include cases utilizing incoherent substitutions would have taken me far on to those pastures of wonders where, judging from the material appearing in our organ, most of our members have not yet been brought to graze.

Even in its more elementary manifestations, isomorphism affords a stimulating, amusing and highly satisfying *exercitatio*. It is hoped that these types of quasi-aperiodic ciphers will, despite the greater exertion required in either preparing or solving them, find their way in the columns of our official publication to relieve the staple and, alas, stale diet on which our beloved *patres conscripti* continue to feed us.

At any rate, I am very happy for the opportunity of leading you to another[1] excursion *extra muros*.

R. C.

Harrison, N. Y.
August 1946

1 Pardonable pride. The current rage among the members of our Association centering around the *Bifid Cipher* is due solely to the untiring efforts of several of mypupils at Hunter College where Delastelle's *fractionating systems* were, for the first time, publicly exposed by me.

I
THE CONCEPT OF ISOMORPHISM

PAIRING

1. Mr. and Mrs. Jones' twenty-fifth anniversary of blissful wedlock is nearly at hand. They decide that this portentous event in their life should be fittingly solemnized by inviting their best friends to dinner at their home. Accordingly, Mrs. Jones busies herself with the not too easy task of selecting from among her friends those upon whom she can safely bestow the appellative of best. She jots down names, one after another. Now and then some are scratched off, others added. A final critical evaluation - she is satisfied. She then *counts off* the names on the list and finds that including herself and Mr. Jones there will be thirty persons at dinner. Rather a large party, but the Jones' are affluent citizens and their mansion is a palatial one.

James, who in the world of butlers is held a non-pareil, is an old hand at this sort of game; he knows how to arrange a dinner party properly. He sets up, as is his wont, a richly decorated table around which he disposes thirty chairs - no more, no less - for, his vast experience in baronial manors has taught him that at a properly arranged dinner party there must be no vacant chairs.

Dinner is served!

The guests file into the dining hall and proceed to their assigned places. Suddenly, *without counting,* James is aware that something is amiss; there are two more chairs than guests around the board. Had he committed such a plebeian error?

No. Mrs. Jones briefly explains that the Smiths who live in the suburbs will be delayed; their car broke down on the way.

How did James derive the knowledge that the number *of guests in the room was* smaller *than the number of chairs?*

Why! This is too silly, the critical reader will say, slowly arching his brow.

And we are prone to agree with him.

2. A process which dominates all mathematics consists in successively *pairing* off each object of a collection with one object of another collection until one of the collections or both are exhausted.

In our little story, guests and chairs were paired and in the process the collection of guests was exhausted before the collection of chairs. Had the Smiths not been delayed, the two collections would have been exhausted at the same time; that is to say, to each chair there would have corresponded a guest, and to every guest a chair. Hence, the two collections would have been *equal.*

CORRESPONDENCE

3. A collection of objects is known in mathematics as a *set*. The objects are usually called *elements*. A set is *finite* if its elements can be counted off; that is, if the set has a first and last element. Otherwise, a set is *infinite* if it has a first but no last element. Thus, the set of natural numbers:

(A): 1 2 3 4 5 6 7 8 . .

is infinite, for it lacks a last element and cannot, therefore, be completely counted off.

4. A *one-one*[1] *correspondence* between two sets (A) and (B) is established whenever there is a rule which pairs with *each* element of (A) *one* and *only one* element of (B), and conversely, with *each* element of (B), *one* and *only one* element of (A).

5. Two sets are called *equivalent* if a one-one correspondence exists between them.

In the earlier example involving the finite sets of guests and chairs the concept of *equivalence* reduces itself to what is ordinarily called *equality in number*. For, each set has a number: 30, if you include the absent Smiths, and the rule is that to each guest there corresponds a chair and to each chair a guest, irrespective of the guest's name or facial characteristics.

Infinite sets have no number, but the concept of equivalence can be made to apply to them equally as well. For instance, the set (A) of the natural numbers and the set (B) of the even integers

(A) 1 2 3 4 5 6 7 8 . .
(B) 2 4 6 8 10 12 14 16 . .

are equivalent if the elements to be paired off are in their *ordered succession*. For, as is evident, the rule of correspondence here is that to any element k of (A) there corresponds element $2k$ of (B) and conversely, to any element $2k$ of (B) there corresponds element k of (A). This rule which can be symbolized as $(k \leftrightarrow 2k)$ is universal, for it can be applied to every element in each set even though the sets are infinite. And it is precisely this rule, whose validity remains unimpaired whenever applied, which makes the one-one correspondence between the sets effective.

ISOMORPHISM

6. To each of two such equivalent sets let us associate a *relation* of some sort between its elements. For instance, let us consider the sets just discussed ($k \leftrightarrow 2k$) and the relation *addition* between the elements of each.

(A)+ : 1 2 3 4 5 6 7 8 . .
(B)+ : 2 4 6 8 10 12 14 16 . .

1 Modern mathematicians prefer this streamlined term ot the original *one-to-one*.

Evidently, two or more elements in either set can be added and the result is an element of the set. Now, if the *pair* of given relations are *independently* applied to *corresponding* elements of the two sets, is the one-one correspondence ($k \leftrightarrow 2k$) maintained between the two results? Let us check:

$$(A)+ : 2+4 = 6 \qquad 3+1+5 = 9$$
$$(B)+ : 4+8 = 12; \qquad 6+2+10 = 18; \text{ etc.}$$

The two results, $6 \leftrightarrow 12$ and $9 \leftrightarrow 18$ are corresponding terms in (A) and (B); that is, the rule ($k \leftrightarrow 2k$) when applied to the sums, holds. We say that the sets (A) and (B) are *isomorphic*[1] with respect to addition.

Similarly, the equivalent sets ($k \leftrightarrow k^2$)

$$(A)\times : 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ \ldots$$
$$(C)\times : 1\ 4\ 9\ 16\ 25\ 36\ 49\ 64\ \ldots$$

are isomorphic with respect to multiplication, for the product in (A) of any two or more elements of (A) and the product in (C) of the corresponding elements of (C) correspond. For instance

$$(A)\times : 2\times 4 = 8$$
$$(C)\times : 4\times 16 = 64,\ 8 \leftrightarrow 64.$$

On the other hand, the equivalent sets ($k \leftrightarrow k+3$), or the equivalent sets ($k \leftrightarrow 2k-1$)

$$(A) : 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ \ldots$$
$$(D) : 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ \ldots$$

$$(A) : 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ \ldots$$
$$(E) : 1\ 3\ 5\ 7\ 9\ 11\ 13\ 15\ \ldots$$

are not isomorphic with respect to addition for the sums of corresponding elements do not correspond. In fact, say,

$$(A) : 2+4 = 6$$
$$(D) : 5+7 = 12,\ 6 \not\leftrightarrow 12;$$

$$(A) : 3+5 = 8$$
$$(E) : 5+9 = 14,\ 8 \not\leftrightarrow 14.$$

7. The relation between the elements of a set need not be the same as the relation between the elements of the equivalent set. For instance, the equivalent sets ($k \leftrightarrow 2^k$)

$$(A)+ : 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ \ldots$$
$$(F)\times : 2\ 4\ 8\ 16\ 32\ 64\ 128\ 256\ 512\ \ldots$$

are isomorphic, if the relation in A is addition and the relation in (F) is multiplication. In fact, the sum in A of any two (or more) elements

---

1 From the Greek ἴσος, *equal*, + μορφή, *form*: same form, same structure.

in A and the product in F of the corresponding elements in (F) correspond. For instance,

$$(A)+ : 1+3+ 5 = 9$$
$$(F)\times : 2\times 8\times 32 = 512,\ 9 \leftrightarrow 512.$$

In a case of this sort, we say that set (A) and addition is isomorphic with set (F) and multiplication, or vice versa.

8. The relations between the elements of the equivalent sets need not be single ones; there can be a plurality of them. For instance, the set of integers, positive, negative or zero and the set of even integers, positive, negative or zero $(k \leftrightarrow 2k)$[1]

$$(A)\pm \ldots -5\ -4\ -3\ -2\ -1\ 0\ 1\ 2\ 3\ 4\ 5 \ldots$$
$$(B)\pm \ldots -10\ -8\ -6\ -4\ -2\ 0\ 2\ 4\ 6\ 8\ 10 \ldots$$

are isomorphic with respect to addition and subtraction, as can easily be verified.

9. We can now give a formal definition of isomorphism.

Two equivalent sets together with one or more pairs of corresponding relations between elements in each of them are called isomorphic if the equivalence between the sets is maintained with respect to the given relations.

The one-one correspondence between two systems, each consisting of a set and relations between its elements, which shows that the two systems are isomorphic, is called an isomorphism.

10. Isomorphism behaves like equality and can, therefore, be extended to three or more equivalent sets by following a rule parallel to the fundamental rule governing equalities. Thus if

$$A = B \mid (S_1)_{R_1} \leftrightarrow (S_2)_{R_2}$$

and

$$A = C \mid (S_1)_{R_1} \leftrightarrow (S_3)_{R_3}$$

then, it is

$$B = C \mid (S_2)_{R_2} \leftrightarrow (S_3)_{R_3}$$

For instance, we have seen in Secs. 6 and 7 that (A)+ and (B)+ are isomorphic as well as (A)+ and (F)×. We can now easily verify that (B)+ and (F)× are also isomorphic, the correspondence between them becoming $(K \leftrightarrow 2^{\frac{K}{2}})$.

$$(B)+ \ldots 2\ 4\ 6\ 8\ 10\ 12 \ldots ;\ 4+8 = 12$$
$$(F)\times \ldots 2\ 4\ 8\ 16\ 32\ 64 \ldots ;\ 4\times 16 = 64,\ 12 \leftrightarrow 64.$$

LINEAR ISOMORPHISM

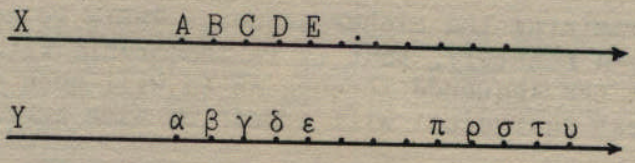
11. We have only dealt, thus far, with *numerical* equivalent sets. The relation associated with each of them in order to establish isomorphism

1. We must admit, in cases of this kind, the notion that *twice* zero is just zero.

between sets has consisted of some operation upon numbers.

Isomorphism can, however, be found in other realms of mathematics, as, for instance, in Geometry.

If on a directed straight line[1] X, a series of *unit* points B,C,D,.. are marked off from an arbitrary origin A, and if on another straight line Y, unit points $\beta, \gamma, \delta, ..$ are also marked off, (same or different unit) from an arbitrary origin α, a one-one correspondence between the two sets of points can be established at any coincidence, say, $(A \leftrightarrow \alpha)$. Now if the relation associated with each of these two sets of points is *order* between points, that is, distance between points, it is easy to see that the two sets of points are isomorphic with respect to *directed transit;* that is, addition of distances.



Thus, if in X we transit from A to B and from B to E and from E to D we reach D which is 3 units distant from A. In the corresponding transit in Y we reach δ which is also 3 units away from α showing that equality in unit distances is preserved. Geometrically, the two transits may well be represented as ABED and $\alpha\beta\varepsilon\delta$ respectively and we say that each is isomorphic with the other. This isomorphism in terms of directed unit distances can be exhibited as 0+1+3-1. Now, an identical transit in Y at correspondence $A \leftrightarrow \pi$ $(\pi=0)$ will take us through $\pi\rho\upsilon\tau$. Hence, $\pi\rho\upsilon\tau$ is isomorphic with ABED and conversely; it is also isomorphic with $\alpha\beta\varepsilon\delta$ and conversely. (See Sec. 10).

12. Isomorphism in ciphered texts must, of necessity, be of this nature, for, the symbols upon which we operate are not quantities but arbitrary marks of language sounds. Isomorphic manifestations in ciphers are, therefore, due to the order in which the alphabetic elements in *both* the numerator and denominator of any substitution whatever follow one another and also to the peculiar structural characteristics of language.

1 A directed straight line is a straight line upon which a point (origin) has been marked off and a direction given.

Plus que ca change, plus que c'est la même chose.

II
ISOMORPHISM IN CIPHERED TEXTS

MONOALPHABETIC SUBSTITUTIONS

13. Using a $\pi N/\pi N_Y$ correspondence, the phrase TODAY enciphered monoalphabetically will become:

πN : T O D A Y
πN_Y: R M B Y W

Upon examining the cipher sequence RMBYW we see nothing in it which suggests, even remotely, that it is isomorphic with TODAY. Of course, if we *generate*[1] the sequence through πN we will soon discover that it is, for the clear text equivalent will appear on some horizontal *generatrix*.

R M B Y W
S N C Z X
→ T O D A Y
U P E B Z
. . . . .

Similarly, utilizing a $\pi N/\pi M$ transformation such as

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

the same phrase, at coincidence A→Q, becomes

πN : T O D A Y
πM_Q: K X R Q P

Again, the cipher sequence not only does not exhibit its isomorphism with TODAY but a πN- generating will fail to show it too. Why? Simply because we do not know the *order* of the elements in πM. Naturally, if we were cognizant of such order, a decipherment of KXRQP at any coincidence, say $\pi N/\pi M_R$, followed by a πN- generating would show the relationship.

πM_R: K X R Q P
πN: Q L A X V
R M B Y W
S N C Z X
→ T O D A Y
. . . . .

Finally, if, in either case, the phrase TODAY would reappear in the plain text the two isomorphs in the ciphered text would be *identical*. The two cipher isomorphs will, according to Sec. 12, be (trivially) isomorphic too. Identical isomorphs are generally known as *repetitions*.

---

1 Usually known as *running down* process.

14. A word such as MUNITIONS in which some of the elements recur will reflect, when enciphered monoalphabetically, the recurring elements in the same order:

π N : M U N I T I O N S
π M_R : I D J W M W Y J N

Upon examining the cipher sequence IDJWMWYJN we are aware of the peculiar succession of the elements in the subsequence

* _ _ *
. . J W M W Y J . .
.

which forms a definite *pattern* easily symbolized as (AB_1B_1A), in which the numerals merely denote the number of non-recurring elements laying between the repeated ones.

This pattern, or *idiomorph*[1] as is better known, may not identify it, *ipso-facto*, as its isomorph ..NITION.. whence it springs, but will indeed associate it with *any one* of the small family of words having the identical idiomorphic construction.

A B 1 A 1 B
D E F E N D
S T A T E S
S U R V I V O R
M U N I T I O N S
. . . . . .

Frequency considerations arising from the frequency distribution of the message will finally isolate NITION as the proper isomorph.

15. Two idiomorphic words such as BAGGAGE and WINNING (ABBAB) when enciphered monoalphabetically will result into idiomorphic sequences.

πN :	B	A	G	G	A	G	E		W	I	N	N	I	N	G
πM_R	B	R	S	S	R	S	F		E	W	J	J	W	J	S

Clearly, upon examination, the cryptanalyst knows that these two arising from *distinct* words, for the frequency distribution of the message has told him that he is dealing with a monoalphabet substitution.

APERIODIC SUBSTITUTIONS

16. Let us consider the system in which each word of a message is enciphered monoalphabetically at a preassigned distinct coincidence (*key*) for each word, say FIVE. The message

	F					I						V							E	
πN:	E	N	E	M	Y	A	T	T	A	C	K	R	E	P	E	L	L	E	D	W	E
πN:	J	S	J	R	D	I	P	P	I	K	S	M	Z	K	Z	G	G	Z	Y	A	I

	F										I										
	C	O	U	N	T	E	R	A	T	T	A	C	K	T	O	M	O	R	R	O	W .
	H	T	Z	S	Y	J	W	F	Y	Y	F	H	P	P	W	U	W	Z	Z	W	E .

1 From the Greek ἴδιος, own, peculiar + μορφή, form, own form.