SOME FURTHER METHODS IN ALGEBRAIC CRYPTOGRAPHY

By Jack Levine

Department of Mathematics, State College, Raleigh, North Carolina

1. *Introduction.* In a previous paper, [3], the author has presented several methods of algebraic encipherment which have the property of providing a variable substitute for any given sequence of n letters. This was accomplished through a matrix transformation, the matrix being defined in terms of one or more parameters, these providing the means for the variable substitutions.

In this paper we discuss two new methods of this kind of encipherment. While the transformations involved were not intended to be primarily of the matrix types, it is a matter of interest that they may be so considered. This will be shown below.

2. *Some General Considerations.* One object of algebraic cryptography is to find methods of encipherment based on mathematical operations. The best known of these, and one of great generality, is that of matrix multiplication, (see [1], [2], [3]). By this method a sequence of n plain-text letters is converted into a sequence of n cipher-text letters through the matrix congruence

$$C \equiv AP \pmod{26}, \tag{1}$$

where $A = [a_{ij}]$ is an $n \times n$ matrix; C and P are one-column matrices (vectors),

$$C = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}, \qquad P = \begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{bmatrix}. \tag{2}$$

The components $p_1, p_2, \cdots, p_n$ of vector $P(p_1, \cdots, p_n)$ are the n numbers representing numerical values of the n plain-text letters according to some 1–1 reciprocal correspondence between the 26 letters of the alphabet, and the 26 numbers 0, 1, 2, $\cdots$, 25.

Likewise, $c_1, \cdots, c_n$ represent the numerical values of the n cipher letters as determined from (1) and this correspondence. The elements a_{ij} of matrix A are also integers from the range 0, 1, 2, $\cdots$, 25.

To obtain a unique decipherment, the determinant $|A|$ of A must be prime to 26, whence $P \equiv A^{-1}C$ will produce the plain-text.

A rather general formulation of the problem under consideration can be made in this way:

Given an ordered sequence of vectors $P_1, P_2, P_3, \cdots$, to find transformations T converting P_i to a vector $C_i = T(P_i)$, $(i = 1, 2, 3, \cdots)$. The transformation T is to have the properties:

(a) For any value of i a unique inverse T^{-1} must exist, so that $P_i = T^{-1}(C_i)$,

(b) If two of the vectors P_i, P_j are identical, the corresponding transforms C_i, C_j are not necessarily identical,

(c) The components of any vector $P_i(p_1, p_2, \cdots, p_n)$ being integers in the range 0, 1, 2, $\cdots$, 25, a similar statement must be true of the transform components $C_i(c_1, c_2, \cdots, c_n)$.

The matrix transformations of [3] satisfy these conditions. We turn now to the new methods of transformation mentioned above.

3. *Method of polynomial division.* The plain-text letters are grouped in sets of n letters and converted to numerical form by a correspondence as mentioned in section 2. Let $p_1, p_2, \cdots, p_n$ be any one such converted group. Now form the identity congruence

$$\begin{aligned} &\frac{p_1 x^{n-1} + p_2 x^{n-2} + \cdots + p_{n-1}x + p_n}{a_1 x^{k-1} + a_2 x^{k-2} + \cdots + a_{k-1}x + a_k} \\ &\equiv q_1 x^{n-k} + q_2 x^{n-k-1} + \cdots + q_{n-k+1} \\ &+ \frac{r_1 x^{k-2} + r_2 x^{k-3} + \cdots + r_{k-1}}{a_1 x^{k-1} + \cdots + a_k}, \pmod{26}. \end{aligned} \tag{3}$$

In (3), $k \leq n$; $a_1, a_2, \cdots, a_k$ are arbitrary integers with a_1 prime to 26. (This a-sequence is to vary from one group to the next in some preassigned manner.) The quotient and remainder coefficients in some preassigned order are taken to be the cipher values $c_1, c_2, \cdots, c_n$ of the n cipher letters corresponding to the n plain letters.

To decipher, we consider (3) in the equivalent form

$$\begin{aligned} p_1 x^{n-1} + \cdots + p_n &\equiv (a_1 x^{k-1} + \cdots + a_k) \\ &(q_1 x^{n-k} + \cdots + q_{n-k+1}) + r_1 x^{k-2} \\ &+ \cdots + r_{k-1}, \pmod{26}, \end{aligned} \tag{4}$$

carry out the indicated multiplications and additions on the right side, and thus determine $p_1, \cdots, p_n$, and hence the plain letters. (Since n and k are known it is of course easy to distinguish between the quotient coefficients q and the remainder coefficients r in the set $c_1c_2 \cdots c_n$.)

All operations in both (3) and (4) can be performed rapidly using detached coefficients and a multiplication table modulus 26. Such a table lists all products $c = ab$, mod 26 ($a, b \leq 25$).

An example will explain the details of the procedure. Example. To encipher the plain-text

SYNTHETIC DIVISION,

using the correspondence

(5)

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	0

Use $n = 5$, and divide the text in groups of 5 letters:

(6)

S	Y	N	T	H		E	T	I	C	D
19	25	14	20	8		5	20	9	3	4

I	V	I	S	I		O	N	X	Y	Z
9	22	9	19	9		15	14	24	25	0

(XYZ added to complete the last group).

To determine sequences of coefficients a_1, a_2, $\cdots$ in (3) which vary from one group of (6) to the next, first choose a basic key-sequence, say

(7) 5 8 19 6 12 17.

This is expanded into a longer sequence by repeating its elements in a cyclic manner, and then grouping the resulting numbers in lengths indicated by a secondary key-sequence, say 4, 2, 3, 5. This would give

(8)

(4)	(2)	(3)	(5)
5 8 19 6	12 17	5 8 19	6 12 17 5 8

(4)	(2)	(3)	··
19 6 12 17	5 8	19 6 12	...

The various groups in (8) constitute the coefficients a_i to be used in (3). The encipherment of the first group of (6) proceeds then:

					|				
19	25	14	20	8	|	5	8	19	6	
19	20	15	2		|	9	1			
5	25	18	8							
5	8	19	6							
17	25	2								

All calculations are performed modulus 26. The first division $19/5 = (\frac{1}{5})(19) = (21)(19) = 9$, (as $5 \cdot 21 = 1$).

The quotient and remainder coefficients 9, 1, 17, 25, 2 in this order yield by (5) the cipher group I A Q Y B as the encipherment of the first plain group S Y N T H.

To encipher the second group the divisor coefficients $a_1a_2 = 12\ 17$ must be used. Since $a_1 = 12$ is not prime to 26 we adopt the convention of using the next higher prime, 15, to give a_1. The calculations are

					|				
5	20	9	3	4	|	15	17			
5	23				|	9	5	14	19	
	23	9								
	23	7								
		2	3							
		2	4							
			25	4						
			25	11						
				19						

This gives 9, 5, 14, 19, 19 or I E N S S, the second cipher group. The complete encipherment is IAQYB IENSS GNJKA QRURT.

Decipherment is by means of (4). Since k and the coefficients $a_1, \cdots, a_k$ are known in every case it is easy to separate the q_i and r_i coefficients. Thus, to decipher the first group A I Q Y B = 9 1 17 25 2, we know $k = 4$, $a_1a_2a_3a_4 = 5\ 8\ 19\ 6$; hence there must be $n - k + 1 = 2$ q-coefficients, 9, 1; and $k - 1 = 3$ r-coefficients, 17 25 2. This gives, from (4)

	5	8	19	6	
	9	1			
19	20	15	2		
	5	8	19	6	
19	25	23	21	6	
		17	25	2	
19	25	14	20	8	
S	Y	N	T	H	= first plain group.

From (4) it is easy to obtain the matrix relation

$$\begin{bmatrix} p_1 \\ p_2 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ p_n \end{bmatrix} \equiv \begin{bmatrix} a_1 & & & & & & \\ a_2 & a_1 & & & & & \\ \cdot & \cdot & \cdot & & & & \\ \cdot & \cdot & \cdot & a_1 & & & \\ a_k & \cdot & & \cdot & 1 & & \\ & a_k & & \cdot & & \cdot & \\ & & & \cdot & & & \cdot \\ & & & a_k & & & 1 \end{bmatrix} \tag{9}$$

$$\begin{bmatrix} c_1 \\ c_2 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ c_n \end{bmatrix}, \pmod{26}.$$

The first $n - k + 1$ columns of the triangular matrix contain the sequence $a_1 a_2 \cdots a_k$, beginning with a_1 on the main diagonal. The last $k - 1$ columns contain only 1's, and these on the main diagonal.

The triangular property of this matrix constitutes a cryptographic weakness which the cryptanalyst would be quick to use. This weakness can to a great extent be eliminated in a large variety of ways, one of which is to vary the order of writing the quotient and remainder coefficients. (In the above example this order was fixed throughout the encipherment.) However, since it is not our purpose to treat this phase of the subject here, we refrain from further remarks along this line.

4. *Method of Synthetic Division Algorithm.* By this method we encipher a plain group $p_1 p_2 \cdots p_n$ to $c_1 c_2 \cdots c_n$ by means of the transformation

$$\begin{aligned} ax^n + p_1 x^{n-1} + p_2 x^{n-2} + \cdots + p_{n-1} x + p_n \\ \equiv a(x-h)^n + c_1(x-h)^{n-1} + c_2(x-h)^{n-2} \\ + \cdots + c_{n-1}(x-h) + c_n, \pmod{26}. \end{aligned} \tag{10}$$

In this identity congruence a and h are two numbers selected in advance. To obtain the coefficients c_i we use the well-known process of continued synthetic division. The following example illustrates the method.

Example. To encipher

SYNTHETIC DIVISION APPLICATION

using $n = 5$, $a = 1$, $h = 12$ throughout the encipherment. Divide the plain-text in groups of 5 and convert letters to numbers by the correspondence (5),

S	Y	N	T	H		E	T	I	C	D
19	25	14	20	8		5	20	9	3	4

I	V	I	S	I		O	N	A	P	P
9	22	9	19	9		15	14	1	16	16

L	I	C	A	T		I	O	N	X	X
12	9	3	1	20		9	15	14	24	24

The first group 19 25 14 20 8, with $a = 1$ gives the polynomial $x^5 + 19x^4 + 25x^3 + 14x^2 + 20x + 8$. We divide this by $x - 12$, ($h = 12$), using mod 26 calculations,

1	19	25	14	20	8	[12]
	12	8	6	6	0	
1	5	7	20	0	[8]	
	12	22	10	22		
1	17	3	4	[22]		
	12	10	0			
1	3	13	[4]			
	12	24				
1	15	[11]				
	12					
1	[1]					

giving 1 11 4 22 8 = $c_1 c_2 c_3 c_4 c_5$ = A K D V H as the first cipher group. The remaining cipher groups are obtained in a like manner, the final result being AKDVH MJUQT QVMWK WPMNN TWYEX QOZJT.

To decipher the first group AKDVH, convert to numbers and divide by $x - 14$ (since $-12 \equiv 14$),

1	1	11	4	22	8	[14]
	14	2	0	4	0	
1	15	13	4	0	[8]	
	14	16	16	20		
1	3	3	20	[20]		
	14	4	20			
1	17	7	[14]			
	14	18				
1	5	[25]				
	14					
1	[19]					

giving 19 25 14 20 8 = S Y N T H, the first plain group, etc.

In decipherment, of course, the division is always by $x + h$, or by $-h = 26 - h$, synthetically.

From (10) or the equivalent

$$\begin{aligned} &ay^n + c_1y^{n-1} + c_2y^{n-2} + \cdots + c_{n-1}y + c_n \\ &\equiv a(y+h)^n + p_1(y+h)^{n-1} + p_2(y+h)^{n-2} \\ &\quad + \cdots + p_{n-1}(y+h) + p_n, \pmod{26}, \end{aligned} \tag{11}$$

it is not difficult to obtain the matrix relations

$$\begin{bmatrix} c_1 \\ c_2 \\ \cdot \\ \cdot \\ \cdot \\ c_n \end{bmatrix} \equiv \begin{bmatrix} 1 & & & \\ \binom{n-1}{1}h & 1 & & \\ \binom{n-1}{2}h^2 & \binom{n-2}{1}h & 1 & \\ \cdot & \cdot & & \\ \cdot & \cdot & & \\ \cdot & \cdot & & \\ \binom{n-1}{n-1}h^{n-1} & \binom{n-2}{n-2}h^{n-2} & \cdots & 1 \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ \cdot \\ \cdot \\ \cdot \\ p_n \end{bmatrix} + a \begin{bmatrix} \binom{n}{1}h \\ \binom{n}{2}h^2 \\ \cdot \\ \cdot \\ \cdot \\ \binom{n}{n}h^n \end{bmatrix}, \pmod{26} \tag{12}$$

or

$$C \equiv A(h)P + aB(h), \pmod{26} \tag{13}$$

where matrix $A(h)$ is a triangular matrix whose elements in its column m are the successive terms in the expansion of $(1 + h)^{n-m}$ with the 1 on the main diagonal, and $B(h)$ is a column vector as shown.

If $n = 4$, (12) would be

$$\begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 3h & 1 & 0 & 0 \\ 3h^2 & 2h & 1 & 0 \\ h^3 & h^2 & h & 1 \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \\ p_4 \end{bmatrix} + a \begin{bmatrix} 4h \\ 6h^2 \\ 4h^3 \\ h^4 \end{bmatrix}. \tag{14}$$

The inverse to (12) or (13) is easily written down as

$$P \equiv A(-h)C + aB(-h). \tag{15}$$

On solving (13) formally for P and comparing with (15) there is obtained the interesting matrix relations

$$\begin{aligned} A(-h) &\equiv A^{-1}(h), \\ B(-h) &\equiv -A^{-1}(h)B(h). \end{aligned} \tag{16}$$

The fact that corresponding plain and cipher values are related through a triangular matrix by (13) repeats the situation of the first method in the previous section. To offset this apparent fault, the following variations are suggested, these strengthening the cryptographic result.

(A) Use a different h and a from one plain group to the next (n fixed),

(B) Vary all three, a, h, and n from group to group.

(C) Perform a rearrangement of the cipher letters within each group after encipherment by the division algorithm (using (A) or (B) in addition).

(D) Use the polynomial

$$\begin{aligned} &ax^n + a_1p_1x^{n-1} + a_2p_2x^{n-2} \\ &\quad + \cdots + a_{n-1}p_{n-1}x + a_np_n \end{aligned}$$

in (10), where the a_i are prime to 26 (but kept fixed from group to group.

Of course, many other variations are possible.

LITERATURE CITED

HILL, L. S. 1929. Cryptography in an algebraic alphabet. American Mathematical Monthly **36**: 306-312.

———. 1931. Concerning certain linear transformation apparatus of cryptography. Amer. Math. Monthly **38**: 135-154.

LEVINE, J. 1958. Variable matrix substitution in algebraic cryptography. Amer. Math. Monthly **65**: 170-179.