SOME ELEMENTARY CRYPTANALYSIS OF ALGEBRAIC CRYPTOGRAPHY

JACK LEVINE, North Carolina State College

1. Introduction. By algebraic cryptography we mean the process of encipherment which converts a plain message into a cipher message by means of n simultaneous linear congruences, where n is an arbitrary integer ([1], [2], [3], [4]). The plain letters are written in blocks of n, and if $P_{i\beta}$ denotes the letter in position β of block i, then

$$C_{i\beta} \equiv a_{\beta 1}P_{i1} + \cdots + a_{\beta n}P_{in} \pmod{26}, \tag{1.1}$$

where $i=1, 2, \cdots$, $\beta=1, \cdots, n$, so that the encipherment of plain block $P_{i1} \cdots P_{in}$ is cipher block $C_{i1} \cdots C_{in}$.

In (1.1) the matrix $A=[a_{\alpha\beta}]$ of the coefficients is such that $|a_{\alpha\beta}|$ is prime to 26. It is convenient for cryptographic purposes to take A such that $A=A^{-1}$, and we assume A is so chosen. Hence we can also write

$$P_{i\beta} \equiv a_{\beta 1}C_{i1} + \cdots + a_{\beta n}C_{in} \pmod{26}. \tag{1.2}$$

The 26 letters of the alphabet are given numerical values according to some permutation of the normal sequence 0, 1, $\cdots$, 25; and it is these numerical values which are actually used for the $P_{i\beta}$ and $C_{i\beta}$ above. For the purposes of this article there is no loss of generality in using the normal sequence itself, giving

(1.3)

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	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

For illustrations in the actual use of (1.1), (1.3), [3] may be consulted.

In its most general form the cryptanalytic problem involved here may be stated in the following way. Given one (or more) cryptograms obtained by use of (1.1), but with no other information, to find the corresponding plain messages, and the matrix A. Even for such small values of n as $n=5$ this would ordinarily be a problem of very great difficulty.

Our purpose here is to treat what may be considered as one of the simplest special cases of the general problem. We assume as known the numerical values of the alphabet letters (see (1.3)), and also as known some portion of the plain message of a cryptogram. However, the exact location of this portion in the message is not known. This is an instance of the classical "method of the probable word," well known in the cryptanalytic art. The solution of this case involves two steps:

Problem (A): Determining the location of the known plain-text.

Problem (B): Determining matrix A.

The final test is of course deciphering the cryptogram based on the recovered matrix.

2. Some basic relations. Consider any $n+1$ blocks of plain-text $P_{i1} \cdots P_{in}$ for $i = i_1, \cdots, i_{n+1}$. By (1.2) we can write

$$P_{i\beta} \equiv \sum_{\sigma=1}^{n} a_{\beta\sigma} C_{i\sigma} \qquad (i = 1, \cdots, n+1), \tag{2.1}$$

where in (2.1), and hereafter unless otherwise stated, all congruences are taken mod 26. In (2.1) consider β as fixed (a value from $1, \cdots, n$). Regarding (2.1) as a system of $n+1$ congruences in n unknowns $a_{\beta 1}, \cdots, a_{\beta n}$, we may eliminate these to obtain the condition

$$\Delta_\beta = \begin{vmatrix} P_{i_1\beta} & C_{i_11} & \cdots & C_{i_1n} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ P_{i_{n+1}\beta} & C_{i_{n+1}\beta} & & C_{i_{n+1}n} \end{vmatrix} \equiv 0 \qquad (\beta = 1, \cdots, n). \tag{2.2}$$

In a like manner we derive from (1.1),

$$\Delta'_\beta = \begin{vmatrix} C_{i_1\beta} & P_{i_11} & \cdots & P_{i_1n} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ C_{i_{n+1}\beta} & P_{i_{n+1}1} & \cdots & P_{i_{n+1}n} \end{vmatrix} \equiv 0 \qquad (\beta = 1, \cdots, n). \tag{2.3}$$

Relations $\Delta_\beta \equiv 0, \Delta'_\beta \equiv 0$ will be found useful in our problem since they do not involve the (unknown) matrix elements $a_{\alpha\beta}$. Their use is illustrated below.

From (2.1) select any n values of i_s, say, $j_1, \cdots, j_n$, and form the determinant based on the resulting n^2 congruences (using $\beta = 1, \cdots, n$). This gives

$$|P_{j\beta}| \equiv |\sum a_{\beta\sigma} C_{i\sigma}| \equiv |a_{\beta\sigma}| \, |C_{j\sigma}|,$$

or

$$\begin{vmatrix} P_{j_11} \cdots P_{j_1n} \\ \cdot \quad\quad \cdot \\ \cdot \quad\quad \cdot \\ P_{j_n1} \cdots P_{j_nn} \end{vmatrix} \equiv \pm \begin{vmatrix} C_{j_11} \cdots P_{j_1n} \\ \cdot \quad\quad \cdot \\ \cdot \quad\quad \cdot \\ C_{j_n1} \cdots C_{j_nn} \end{vmatrix} \tag{2.4}$$

since $|a_{\alpha\beta}| \equiv \pm 1$, as follows from $A = A^{-1}$.

In (2.2), (2.3), (2.4), the cipher values are known. The plain values will be selected from the known probable text. Briefly, the correct location of this known text will be found by fitting it in all positions until one is obtained for which (2.2), (2.3), (2.4) are satisfied. The exact method for doing this with a minimum of trials is explained in the sections to follow.

3. Problem (A) and the use of modulo 2. Consider the system of n congruences (1.1) for a fixed i and for modulo 2. We write these as

$$C_\beta \equiv a_{\beta 1} P_1 + \cdots + a_{\beta n} P_n \pmod 2 \qquad (\beta = 1, \cdots n) \tag{3.1}$$

so that $P_1 \cdots P_n$, $C_1 \cdots C_n$ represent any block of n plain and corresponding

n cipher values. As $P_1 \cdots P_n$ assumes all possible sequences of n letters, (3.1) establishes a unique 1-1 reciprocal correspondence between the 2^n length n binary sequences of 0's and 1's. These 2^n sequences represent the 2^n integers (in base 2) from 0 through 2^n-1. Hence by (3.1) there is associated with each block of n plain letters and its corresponding block of n cipher letters a pair of numbers in the range 0 through 2^n-1. The number thus associated with a block of n letters is called its binary value.

The following example illustrates these pairings and their use in Problem (A).

(a_1)	CRY	PTO	GRA	PHY	BYA	LGE	BRA	ICE	QUA	TIO	NSX
(b_1)	SUI	RIM	AYG	DIK	VFG	LTE	RUK	KRC	QHA	JLY	JOB

(a_2)	3	18	25	16	20	15	7	18	1	16	8	25	2	25	1	12	7	5	2	18	1
(b_2)	19	21	9	18	9	13	1	25	7	4	9	11	22	6	7	12	20	5	18	21	11

(a_3)	9	3	5	17	21	1	20	9	15	14	19	24
(b_3)	11	18	3	17	8	1	10	12	25	10	15	2

(a_3)	101	001	101	001	011	011	001	111	111	011	010
(b_3)	111	011	111	011	001	001	011	101	101	001	010

(a_4)	5	1	5	1	3	3	1	7	7	3	2
(b_4)	7	3	7	3	1	1	3	5	5	1	2

Here, (a_1), (b_1) represent a plain-text with its cipher text; (a_2), (b_2) are the numerical values of the letters by (1.3); (a_3), (b_3) give these values (mod 2); and (a_4), (b_4) are the binary values according to the scheme

$$000 = 0,\ 000 = 1,\ 010 = 2,\ 011 = 3,\ 100 = 4,\ 101 = 5,\ 110 = 6,\ 111 = 7.$$

Thus, the binary value of CRY $= 5$, of SUI $= 7$, etc. Because of $A = A^{-1}$ the binary value pairing as in (a_4), (b_4), will always be such that $a \leftrightarrow b$, $0 \leftrightarrow 0$ where a may equal b. (In the above example it is seen that $1 \leftrightarrow 3$, $2 \leftrightarrow 2$, $5 \leftrightarrow 7$). It follows that the two binary-value sequences derived from any plain-text and its corresponding cipher text must always be of the same pattern. This pattern in the present illustration could be represented by the sequence *ababccbddce* (see (a_4), (b_4)). Furthermore, any portion of the plain-text must produce a common pattern with its associated cipher portion.

It is this last property which is used to obtain preliminary locations (apparent settings) of the probable text. The cipher text is converted to its binary values (as in (b_4) above), and the probable text is similarly converted, assuming it starts in each of the n positions of a block. There will thus be n such binary conversions, $B_1, \cdots, B_n$, each of which is then matched against the cipher text conversion for like patterns. Each such matching is an apparent setting of the probable text, and these are next tested against conditions (2.2), (2.3), (2.4), depending on the material available. This feature is taken up in the next section.

To demonstrate the pattern matching, consider the example,

	MIU	GNJ	WWU	YHZ	DNS	WVK	RFV	LLK	AMP	IGS	MIU
	7	4	7	4	1	5	0	1	6	7	7
(3.2)	WKN	OEM	IEK	ORW	WAE	KZB	APL	KYP	MEU	ZMO	ZIX
	6	7	7	5	7	4	4	6	7	3	6
	FHS	SJI	DDJ	KFY	BWW	HQP	KLI	NKG	TMJ	ROB	TZE
	1	5	0	5	3	2	5	3	2	2	1

The number under each group is its binary value. We assume the probable text THREE CONGRUENCES, but use the first 14 letters only. Let S_α indicate the first letter starts in position α of a block ($\alpha = 1, 2, 3$). We then obtain

S_1:	THR	EEC	ONG	RUE	NCx		S_2:	xTH	REE	CON	GRU	ENC
B_1:	0	7	5	3			B_2:		3	6	5	5

S_3:	xxT	HRE	ECO	NGR	UEN	Cxx
B_3:		1	7	2	6	

From (3.2) the cipher text binary sequence is

(3.3) 7 4 7 4 1 5 0 1 6 7 7 6 7 7 5 7 4 4 6 7 3 6 1 5 0 5 3 2 5 3 2 2 1

The B_1 pattern, 0 7 5 3, must obviously match at 0 1 6 7 or 0 5 3 2 of (3.3), giving

(3.3)	0 1 6 7	0 5 3 2
B_1:	0 7 5 3	0 7 5 3

Each of these matchings can be eliminated by inspection, the first by 7 paired with both 1 and 3, and the second by 3 with 2 and 5.

The B_2 pattern, 3 6 5 5, results in four apparent settings:

(3.3)	1 6 7 7	7 6 7 7	5 7 4 4	5 3 2 2
B_2:	3 6 5 5	3 6 5 5	3 6 5 5	3 6 5 5

of which all but the first can be eliminated at once. The first setting is kept for further testing.

The B_3 pattern is matched at

(3.3)	7 4 1 5	4 6 7 3	7 3 6 1	3 6 1 5
B_3:	1 7 2 6	1 7 2 6	1 7 2 6	1 7 2 6

all of which are inconsistent. If the probable text is actually present, then it must start in block 7 of (3.2):

		1	6	7	7
(3.4)	RFV	LLK	AMP	IGS	MIU
	xTH	REE	CON	GRU	ENC
		3	6	5	5

4. Problem (A) continued. Testing of apparent settings. In the above example only one apparent setting, (3.4), survived the binary pattern test. Ordinarily with longer messages, shorter probable texts, or larger values of n, a large number of apparent settings will remain, and these must be further eliminated.

Let λ equal the length of the probable text. Then the actual procedure used will largely depend on the value of λ.

Suppose first $\lambda \geqq n(n+1)+(n-1)$. For any starting point S_α write the probable text corresponding to an apparent setting beginning in block i and position α in an array of consecutive blocks vertically as given below (corresponding cipher blocks are also shown).

$$
(4.1)\qquad
\begin{array}{cccc|ccc}
x & \cdots & x & P_{i\alpha} \cdots P_{in} & C_{i1} & \cdots & C_{in} \\
P_{i+1,1} & \cdots & P_{i+1,\alpha} & \cdots P_{i+1,n} & C_{i+1,1} & \cdots & C_{i+1,n} \\
\vdots & & \vdots & \vdots & \vdots & & \vdots \\
P_{i+n+1,1} & \cdots & P_{i+n+1,\alpha} & \cdots P_{i+n+1,n} & C_{i+n+1,1} & \cdots & C_{i+n+1,n}
\end{array}
$$

Then regardless of the values of i and α there will always be at least $n+1$ complete blocks of (presumably) known plain-text as indicated in (4.1). Now if there are a large number of apparent settings with a common value of α, it will be found that (2.3), or $\Delta_\beta' \equiv 0$, is best to use to test these settings. For n columns of (2.3) can be kept fixed, these being selected from the array of plain-text columns in (4.1). The remaining column is chosen from the cipher-text array at the right in (4.1), and (2.3) then expanded using cofactors of this C column,

$$
(4.2)\qquad P_1 C_{i\beta} + \cdots + P_{n+1} C_{i+n+1,\beta} \equiv 0.
$$

The cofactors $P_1, \cdots, P_{n+1}$ being independent of i need be calculated only once as i varies through values corresponding to the apparent settings.

If (4.2) be first tested (mod 2), many apparent settings will be eliminated very easily. The remaining are then tested (mod 26).

If we apply these ideas to the apparent setting of (3.4) we have corresponding to (4.1),

$$
(4.3)\qquad
\begin{array}{ccc|ccc}
x & \mathrm{T} & \mathrm{H} & \mathrm{R} & \mathrm{F} & \mathrm{V} \\
\mathrm{R} & \mathrm{E} & \mathrm{E} & \mathrm{L} & \mathrm{L} & \mathrm{K} \\
\mathrm{C} & \mathrm{O} & \mathrm{N} & \mathrm{A} & \mathrm{M} & \mathrm{P} \\
\mathrm{G} & \mathrm{R} & \mathrm{U} & \mathrm{I} & \mathrm{G} & \mathrm{S} \\
\mathrm{E} & \mathrm{N} & \mathrm{C} & \mathrm{M} & \mathrm{I} & \mathrm{U}
\end{array}
$$

Forming Δ_1' gives

$$
\begin{vmatrix}
18 & 5 & 5 & 12 \\
3 & 15 & 14 & 1 \\
7 & 18 & 21 & 9 \\
5 & 14 & 3 & 13
\end{vmatrix},
$$

which is $\equiv 0 \pmod 2$ and $\pmod{26}$. It is found that Δ_1', Δ_3' are also both $\equiv 0 \pmod 2$ and $\pmod{26}$. In addition, (2.4) is satisfied for any choice of 3 rows from (4.3). This setting would next be used to obtain matrix A, (Problem (B)).

Suppose next $n^2 < \lambda < n(n+1)+n-1$. In this case certain starting points will not produce $n+1$ complete plain-text blocks in array (4.1), and the method described above will consequently fail. For such cases we can use (2.2), (and (2.4) when available), since, if $\lambda > n^2$, there must always be at least one column in the plain-text array of (4.1) containing $n+1$ letters, this column then being used in (2.2). Thus, for certain settings (values of α), (2.2) is used, and for the remaining (2.3) is used. In addition (2.4) is used when necessary.

We discuss again the previous example (3.2), this time using only 10 letters of the probable text (this being the minimum for $n=3$), or THREE CONGR. The three starting points give

S_1		S_2		S_3	
T H R	0	x T H	0/4	x x T	
E E C	7	R E E	3	H R E	1
O N G	5	C O N	6	E C O	7
R x x		G R x	4/5	N G R	2

The binary patterns are written at the right of each array. In S_2 we indicate the two possibilities 0/4, 4/5 as shown. These patterns are now matched against the cipher pattern (3.3), with the following preliminary matchings:

B_1: 0 7 5 0 7 5

0 1 6 0 5 2

B_2:				B_3:			
0/4	3	6	4/5		1	7	2
7	4	1	5		7	4	1
0	1	6	7		4	1	5
4	6	7	3		1	6	7
6	7	3	6		5	7	4
7	3	6	1		4	6	7
3	6	1	5		6	7	3
0	5	3	2		7	3	6
5	3	2	5		3	6	1
3	2	5	3		6	1	5
2	5	3	2		5	3	2
					2	5	3
					5	3	2

All but the following seven are eliminated by inspection,

0 7 5	0 3 6 4/5	4 3 6 5	4 3 6 4	1 7 2	1 7 2	1 7 2
0 1 6	0 1 6 7	7 3 6 1	5 3 2 5	5 7 4	6 7 3	5 3 2
$S_1(a)$	$S_2(b)$	$S_2(c)$	$S_2(d)$	$S_3(e)$	$S_3(f)$	$S_3(g)$

The corresponding arrays (4.1) are

T H R	R F V	x T H	R F V	M E U	K F Y	x x T	I E K	A P L	D D J
E E C	L L K	R E E	L L K	Z M O	B W W	H R E	O R W	K Y P	K F Y
O N G	A M P	C O N	A M P	Z I X	H Q P	E C O	W A E	M E U	B W W
R x x	I G S	G R x	I G S	F H S	K L I	N G R	K Z B	Z M O	H Q P
	$S_1(a)$		$S_2(b)$	$S_2(c)$	$S_2(d)$		$S_3(e)$	$S_3(f)$	$S_3(g)$

Since none of the S_α (plain-text) settings contain four complete blocks we must use text (2.2), first (mod 2). The column TEOR of length 4, from the probable text, is of course used as the plain-text column in (2.2) in all cases. Cases (c), (e), (f) are eliminated using modulo 2 and (2.2). The remaining four are tested (mod 26). This eliminates (d) and (g), leaving $S_1(a)$ and $S_2(b)$. We now use (2.4) on $S_1(a)$ as three complete blocks are present in the probable text, and this eliminates $S_1(a)$.

$S_2(b)$ is the only case left ((2.4) cannot be used on it) and the next step would be to recover matrix A. This is taken up in the next section.

5. Problem (B). Determination of matrix A. Assuming a probable text has been located (as in $S_2(b)$ above), (1.2) give a series of n^2 congruences for the determination of the elements $a_{\alpha\beta}$ of matrix A. For a fixed α, (1.2) determine at least n congruences in the n unknowns $a_{\alpha 1}, \cdots, a_{\alpha n}$. If their coefficient matrix contains an $n \times n$ determinant prime to 26, all these unknowns are determined uniquely. Otherwise, there will be several solutions possible. Finally the use of condition $A^2 = I$ will pick out the correct matrix which should decipher the cryptogram.

We carry out this procedure by completing the solution of above example (3.2). The setting $S_2(b)$ is to be used with (1.2). Convert all letters to numerical values, and write the corresponding (1.2) in matrix form:

$$(5.1) \qquad \begin{bmatrix} x & 18 & 3 & 7 \\ 20 & 5 & 15 & 18 \\ 8 & 5 & 14 & x \end{bmatrix} \equiv \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \begin{bmatrix} 18 & 12 & 1 & 9 \\ 6 & 12 & 13 & 7 \\ 22 & 11 & 16 & 19 \end{bmatrix}$$

or, $P \equiv AC$, the various rows of $S_2(b)$ now appearing as columns. The C matrix contains no 3×3 determinant prime to 26. The 10 congruences of (5.1) split into 3 sets of 3, 4, 3 respectively for the 9 unknowns $a_{\alpha 1}, a_{\alpha 2}, a_{\alpha 3}$ ($\alpha = 1, 2, 3$).

Solving the congruences of (5.1) using mod 2 and mod 13 gives

$$(5.2) \qquad \begin{aligned} a_{11} &= 7, \quad a_{12} = 8, \quad a_{13} = 16, \text{ or} \\ a_{11} &= 20, \quad a_{12} = 21, \quad a_{13} = 16; \end{aligned}$$

$$(5.3)\qquad \begin{aligned} a_{31} &= 6, \quad a_{32} = 9, \quad a_{33} = 3, \text{ or} \\ a_{31} &= 19, \quad a_{32} = 22, \quad a_{33} = 3. \end{aligned}$$

The 3 congruences for a_{31}, a_{32}, a_{33} have a zero determinant, so it will be simpler to use condition $A^2 = I$, taking each of the four pairs of solutions from (5.2), (5.3) for the first two rows of A. The choice

$$\begin{bmatrix} 7 & 8 & 16 \\ 6 & 9 & 3 \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \begin{bmatrix} 7 & 8 & 16 \\ 6 & 9 & 3 \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

is consistent, with $a_{31} = 20$, $a_{32} = 18$, $a_{33} = 11$. The other three cases give contradictions. We finally have then for matrix A,

$$A = \begin{bmatrix} 7 & 8 & 16 \\ 6 & 9 & 3 \\ 20 & 18 & 11 \end{bmatrix},$$

giving $P_1 = 7C_1 + 8C_2 + 16C_3$, $P_2 = 6C_1 + 9C_2 + 3C_3$, $P_3 = 20C_1 + 18C_2 + 11C_3$ to be used in deciphering the cryptogram. This is left for the reader.

6. Concluding remarks. In case the length of the probable text is $\lambda \leqq n^2$, the above methods are in general unavailable. Even assuming a correct location would involve a considerable amount of work, too lengthy to be discussed here. If two or more short probable texts are known, the simultaneous testing of assumed locations may enable the present methods to be used.

References

1. L. S. Hill, Cryptography in an algebraic alphabet, this MONTHLY, vol. 36, 1929, pp. 306–312.

2. ———, Concerning certain linear transformation apparatus of cryptography, this MONTHLY, vol. 38, 1931, pp. 135–154.

3. Jack Levine, Variable matrix substitution in algebraic cryptography, this MONTHLY, vol. 65, 1958, pp. 170–179.

4. ———, Some further methods in algebraic cryptography, J. Elisha Mitchell Sci. Soc., vol. 74, 1958, pp. 110–113.