VARIABLE MATRIX SUBSTITUTION IN ALGEBRAIC CRYPTOGRAPHY

JACK LEVINE, North Carolina State College

1. Introduction. The use of algebraic methods in cryptography is well-known through two important papers by Hill [1], [2]. Briefly, the basic idea can be formulated in the following way. Consider the system of simultaneous congruences

$$y_i \equiv \sum_{j=1}^{n} a_{ij}x_j \pmod{26}, \qquad i = 1, \cdots, n, \tag{1.1}$$

where the constants a_{ij} are chosen so that the determinant $|a_{ij}|$ is *prime* to 26. By means of (1.1) the set of n variables $(x_1, \cdots, x_n)$ is transformed to the set $(y_1, \cdots, y_n)$ and, conversely, the set $(y_1, \cdots, y_n)$ will be transformed to the unique set $(x_1, \cdots, x_n)$ by means of the inverse transformation which exists by the assumption on $|a_{ij}|$.

To each of the 26 letters of the alphabet we associate an integer from the set $0, 1, \cdots, 25$, so that no two letters correspond to the same integer. For simplicity we illustrate with the correspondence (used throughout this paper)

	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)	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

Now to encipher a message, or plain text, by means of (1.1), first replace each letter of the text by means of its numerical equivalent, using for illustration, (1.2). Then divide the resulting sequence of numbers into groups containing n numbers each. Call these

$$p_{11}p_{12}\cdots p_{1n} \quad p_{21}p_{22}\cdots p_{2n} \quad \cdots \quad p_{i1}p_{i2}\cdots p_{in} \quad \cdots. \tag{1.3}$$

Each group of (1.3) is then used in (1.1) for $x_1 \cdots x_n$, and the transformed set

$y_1 \cdots y_n$ calculated. Call the sequence of these sets

$$c_{11}c_{12}\cdots c_{1n} \quad c_{21}c_{22}\cdots c_{2n} \quad \cdots \quad c_{i1}c_{i2}\cdots c_{in} \quad \cdots . \tag{1.4}$$

Convert the numbers of (1.4) into their letter equivalents by (1.2). These letters will constitute the cipher text corresponding to the given plain text.

The decipherment is accomplished by means of the inverse to (1.1).

As a concrete example, select $n=3$, and (1.1) as

$$\begin{aligned} y_1 &\equiv x_1 + 2x_2 + 3x_3 \\ y_2 &\equiv 2x_1 + 5x_2 + 6x_3 \\ y_3 &\equiv x_1 + 2x_2 + 4x_3 \end{aligned} \tag{1.5}$$

To encipher the text CRYPTOGRAPHIC, divide into sets of three letters, adding, say, XX to complete the last set:

C	R	Y	P	T	O	G	R	A	P	H	I	C	X	X
3	18	25	16	20	15	7	18	1	16	8	9	3	24	24

The sequence (1.3) is here 3 18 25 16 20 15 $\cdots$. Substitute the first set 3 18 25 ($=p_{11}p_{12}p_{13}$) in (1.5) for $x_1x_2x_3$ to give

$$\begin{aligned} y_1 &\equiv 3 + 36 + 75 = 114 \equiv 10 = \text{J}, \\ y_2 &\equiv 6 + 90 + 150 = 246 \equiv 12 = \text{L}, \\ y_3 &\equiv 3 + 36 + 100 = 139 \equiv 9 = \text{I}, \end{aligned}$$

Here the first cipher sequence $c_{11}c_{12}c_{13}$ of (1.4) is 10 12 9, which converted to letters by (1.2) gives JLI as shown.

The complete encipherment proceeds as above, and produces

JLI WNL TFU GVP SJQ

To decipher, obtain the inverse of (1.5),

$$\begin{aligned} x_1 &\equiv 8y_1 + 24y_2 + 23y_3 \\ x_2 &\equiv 24y_1 + y_2 \\ x_3 &\equiv 25y_1 + y_3 \end{aligned} \tag{1.6}$$

(The congruences are of course taken mod 26, in which $25 \equiv -1$, $24 \equiv -2$, *etc.*) The reciprocal of a prime p, mod 26, is q, where $pq \equiv 1 \bmod 26$.

Now using JLI = 10 12 9 as $y_1y_2y_3$ in (1.6) gives

$$\begin{aligned} x_1 &= 80 + 288 + 207 = 575 \equiv 3 = \text{C} \\ x_2 &\equiv 240 + 12 = 252 \equiv 18 = \text{R} \\ x_3 &\equiv 250 + 9 = 259 = 25 = \text{Y} \end{aligned}$$

or CRY, the first plain-text group. The rest of the plain text is found in like manner. (In actual practice we would use -1 for 25, -2 for 24, *etc.*, in (1.6).)

In Hill's papers the transformation (1.1) is generalized by the use of matrix coefficients, but the above is sufficient for our purpose.

(The author notes in passing that simultaneous equations were used by him for cryptographic purposes to a limited extent several years prior to the appearance of Hill's papers.)

2. Fixed substitution. The cryptographic method represented by (1.1) is known as a *fixed substitution system*. This means that any given plain-text group will always be replaced by the same cipher-text group. This is true because the coefficients a_{ij} remain fixed throughout the encipherment of a message.

From a cryptographic point of view there is a distinct advantage in using a *variable substitution* method, whereby the various appearances of a given plain-text group will be replaced by different cipher groups. It is our purpose to indicate some simple ways to accomplish this based on (1.1).

3. Variable substitution, first method. It is convenient to represent (1.1) as a matrix congruence

$$C \equiv AP \pmod{26}, \tag{3.1}$$

where matrices A, C, P are defined by

$$A = \begin{bmatrix} a_{11} \cdots a_{1n} \\ \cdot \quad\quad \cdot \\ a_{n1} \cdots a_{nn} \end{bmatrix}, \qquad P = \begin{bmatrix} p_1 \\ \cdot \\ p_n \end{bmatrix}, \qquad C = \begin{bmatrix} c_1 \\ \cdot \\ c_n \end{bmatrix} \tag{3.2}$$

and P, C are one-column matrices representing corresponding plain- and cipher-text groups.

Now in classical cryptography several variable substitution methods are well-known. These can be represented by the congruences

$$c_i \equiv p_i + k_i \pmod{26}, \qquad i = 1, \cdots, N, \tag{3.3}$$

where p_i is the numerical value of the ith plain-text letter according to some correspondence as (1.2), c_i is the numerical value of the corresponding cipher-text letter, N is number of letters in the message, and the sequence of numbers $k_1k_2 \cdots$ has one of the following properties:

(a) $k_1k_2 \cdots$ is a periodic sequence, say $k_1k_2 \cdots k_mk_1k_2 \cdots k_mk_1 \cdots$, where the numbers $k_1 \cdots k_m$ of the period are selected in any preassigned manner.

(b) The number k_i is chosen by the relation

$$k_i = c_{i-1} \tag{3.4}$$

so

$$c_i \equiv p_i + c_{i-1} \qquad (c_0 \text{ chosen in advance}). \tag{3.5}$$

(c) The number k_i is chosen by the relation

$$k_i = p_{i-1}, \tag{3.6}$$

so

$$c_i \equiv p_i + p_{i-1} \qquad (p_0 \text{ chosen in advance}). \tag{3.7}$$

Note that in each of the above three methods p_i is uniquely determined in the decipherment process. This is, of course, a prime requisite in any cryptographic system.

In matrix form (3.3) can be written as

$$C \equiv P + K \tag{3.8}$$

where the indicated matrices are each of one row and one column, since (3.3) represents encipherment one letter at a time.

Now to obtain a variable substitution analogous to (3.1) we generalize (3.8) to

$$C \equiv AP + BK \pmod{26}, \tag{3.9}$$

where $A = [a_{ij}]$, $B = [b_{ij}]$ are $n \times n$ matrices with fixed elements (and $|A|$ prime to 26). Matrices C and P are as given in (3.2), and K is a one-column matrix,

$$K = \begin{bmatrix} k_1 \\ \cdot \\ \cdot \\ \cdot \\ k_n \end{bmatrix}.$$

Corresponding to the three cases (a), (b), (c) above for choosing the k_i, we have:

(a′) Define matrices

$$C_i = \begin{bmatrix} c_{i1} \\ \cdot \\ \cdot \\ \cdot \\ c_{in} \end{bmatrix}, \qquad P_i = \begin{bmatrix} p_{i1} \\ \cdot \\ \cdot \\ \cdot \\ p_{in} \end{bmatrix}, \qquad K_i = \begin{bmatrix} k_{i1} \\ \cdot \\ \cdot \\ \cdot \\ k_{in} \end{bmatrix}, \tag{3.10}$$

using (1.3), (1.4), and

$$K_i = K_{i+m}, \qquad i = 1, 2, \cdots, \tag{3.11}$$

where $K_1, \cdots, K_m$ are chosen in any preassigned manner.

Then

$$C_i \equiv AP_i + BK_i, \qquad i = 1, 2, \cdots, \tag{3.12}$$

from (3.9) gives the substitution. Also,

$$P_i \equiv A^{-1}C_i - A^{-1}BK_i. \tag{3.13}$$

(b′) In this case we choose $K_i = C_{i-1}$, so

$$C_i \equiv AP_i + BC_{i-1} \qquad (C_0 \text{ chosen in advance}).$$

(c′) Choose $K_i = P_{i-1}$, so

$$C_i \equiv AP_i + BP_{i-1} \qquad (P_0 \text{ chosen in advance}). \tag{3.14}$$

To obtain involutory transformations (in which a transformation and its inverse are identical) we have from (3.12), (3.13),

$$A = A^{-1}, \qquad B = -A^{-1}B = -AB, \tag{3.15}$$

and (3.13) becomes $P_i = AC_i + BK_i$. A solution of (3.15) is

$$A^2 = I, \qquad B = A - I \qquad (I = \text{identity matrix}).$$

To obtain A such that $A^2 = I$, a formula in [2] may be used,

$$a_{ij} \equiv \delta_{ij} - \tau\lambda_i\lambda_j, \quad \sigma\tau \equiv 2 \pmod{26}, \quad \sigma \equiv \sum_1^n \lambda_i^2 \pmod{26}, \tag{3.16}$$

σ must be prime to 26.

We illustrate case (c′) using

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 5 & 6 \\ 1 & 2 & 4 \end{bmatrix}, \qquad B = \begin{bmatrix} 4 & 1 & 1 \\ 2 & 0 & 3 \\ 1 & 2 & 0 \end{bmatrix}, \qquad P_0 = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix},$$

$$\begin{bmatrix} c_{i1} \\ c_{i2} \\ c_{i3} \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 5 & 6 \\ 1 & 2 & 4 \end{bmatrix} \begin{bmatrix} p_{i1} \\ p_{i2} \\ p_{i3} \end{bmatrix} + \begin{bmatrix} 4 & 1 & 1 \\ 2 & 0 & 3 \\ 1 & 2 & 0 \end{bmatrix} \begin{bmatrix} p_{i-1,1} \\ p_{i-1,2} \\ p_{i-1,3} \end{bmatrix}. \tag{3.17}$$

To encipher CRYPTOGRAPHIC, we have

$$\begin{bmatrix} c_{11} \\ c_{12} \\ c_{13} \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 5 & 6 \\ 1 & 2 & 4 \end{bmatrix} \begin{bmatrix} 3 \\ 18 \\ 25 \end{bmatrix} + \begin{bmatrix} 4 & 1 & 1 \\ 2 & 0 & 3 \\ 1 & 2 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 19 \\ 23 \\ 14 \end{bmatrix} = \begin{bmatrix} \text{S} \\ \text{W} \\ \text{N} \end{bmatrix},$$

$$\begin{bmatrix} c_{21} \\ c_{22} \\ c_{23} \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 5 & 6 \\ 1 & 2 & 4 \end{bmatrix} \begin{bmatrix} 16 \\ 20 \\ 15 \end{bmatrix} + \begin{bmatrix} 4 & 1 & 1 \\ 2 & 0 & 3 \\ 1 & 2 & 0 \end{bmatrix} \begin{bmatrix} 3 \\ 18 \\ 25 \end{bmatrix} = \begin{bmatrix} 0 \\ 17 \\ 25 \end{bmatrix} = \begin{bmatrix} \text{Z} \\ \text{Q} \\ \text{Y} \end{bmatrix},$$

$$\begin{bmatrix} c_{31} \\ c_{32} \\ c_{33} \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 5 & 6 \\ 1 & 2 & 4 \end{bmatrix} \begin{bmatrix} 7 \\ 18 \\ 1 \end{bmatrix} + \begin{bmatrix} 4 & 1 & 1 \\ 2 & 0 & 3 \\ 1 & 2 & 0 \end{bmatrix} \begin{bmatrix} 16 \\ 20 \\ 15 \end{bmatrix} = \begin{bmatrix} 15 \\ 5 \\ 25 \end{bmatrix} = \begin{bmatrix} \text{O} \\ \text{E} \\ \text{Y} \end{bmatrix}, \textit{ etc.}$$

The complete encipherment is SWN ZQY OEY BMG VQW, using CXX as the last plain group.

The decipherment can be obtained from the inverse to (3.17),

$$P_i = \begin{bmatrix} 8 & 24 & 23 \\ 24 & 1 & 0 \\ 25 & 0 & 1 \end{bmatrix} C_i + \begin{bmatrix} 1 & 24 & 24 \\ 6 & 2 & 25 \\ 3 & 25 & 1 \end{bmatrix} P_{i-1}.$$

4. Variable substitution, second method. We return to the basic relation (3.1) and attempt to replace the matrix A of fixed elements by a matrix with variable elements. A general situation is obtained if the elements a_{ij} of A be considered as polynomial functions of a set of parameters $t, u, v, \cdots$ in such a way that the determinant $|A|$ of A is *independent of the parameters* and is a prime number mod 26. The inverse A^{-1} of A will then exist for all parameter values, and hence $P = A^{-1}C$ can always be found. We consider one of the simpler cases here.

Any triangular matrix

$$T = \begin{bmatrix} t_{11} & 0 & \cdots & 0 \\ t_{21} & t_{22} & \cdots & \\ \cdot & \cdot & \cdots & \\ t_{n1} & t_{n2} & \cdots & t_{nn} \end{bmatrix}$$

with $t_{ij}(t, u, v \cdots)$, $(i \neq j)$, such that t_{ii} is a prime mod 26 will have for determinant $|T| = t_{11}t_{22} \cdots t_{nn}$, a prime mod 26. If T be transformed by elementary transformations leaving $|T|$ unchanged we can obtain a general matrix A of the desired property.

For example, using

$$T = \begin{bmatrix} 1 & 0 & 0 & 0 \\ t & 3 & 0 & 0 \\ 2t+1 & 2 & 5 & 0 \\ 1 & t & t+1 & 7 \end{bmatrix}, \qquad |T| \equiv 1, \text{ mod } 26,$$

we can transform T to

$$A(t) = \begin{bmatrix} 1 & 1 & t & 2t \\ t & t+3 & t & 2t^2 \\ 2t+1 & 2t+3 & 2t^2+t+5 & 2t^2+2t \\ 1 & t+1 & 2t+1 & 2t+7 \end{bmatrix}, \qquad |A(t)| \equiv 1, \text{ mod } 26.$$

Place $C = A(t)P$. For each $P = P_i$ give t a value k_i determined in some preassigned manner,

$$C_i = A(k_i)P_i, \qquad P_i = A^{-1}(k_i)C_i. \tag{4.1}$$

Any of the methods (a'), (b'), (c') can be used, taking for example,

$$k_i = c_{i-1,1} \text{ or } k_i = p_{i-1,1}, \text{ or } k_i = p_{i-1,1} + p_{i-1,2}, \text{ etc.},$$

in the latter two cases.

One disadvantage of this procedure to obtain $A(t)$ is that the elements of $A^{-1}(t)$ will in general be high degree polynomials in the parameters, thus causing computational difficulties.

One way to avoid this difficulty is to assume $A(t)$ is linear in t and impose the condition that $A^{-1}(t)$ is likewise. Thus, place

$$A(t) = G + tH, \tag{4.2}$$

with G, H constant element matrices, and $|G|$ a prime mod 26. It is easily shown $A^{-1}(t)$ will be linear in t if $H=XG$, $X^2=0$. Then

$$A^{-1}(t) = G^{-1} - tG^{-1}X. \tag{4.3}$$

To obtain a general matrix X satisfying $X^2=0$, define N by

$$N = \begin{bmatrix} 0 & n_1 & & & & & & & \\ 0 & 0 & & & & & & & \\ & & 0 & n_2 & & & & & \\ & & 0 & 0 & & & & & \\ & & & & \cdot & & & & \\ & & & & & \cdot & & & \\ & & & & & & 0 & n_q & \\ & & & & & & 0 & 0 & \\ & & & & & & & & 0 \end{bmatrix}, \qquad q \leqq [n/2]. \tag{4.4}$$

N consisting of all zeros except $n_1, n_2, \cdots, n_q$ placed immediately to the right of the main diagonal terms in alternate rows as shown. The n_i are arbitrary constants. It is evident that $N^2=0$. X is now defined by

$$X = QNQ^{-1}, \tag{4.5}$$

Q being an arbitrary constant-term matrix with an inverse. From (4.5), $X^2=0$.

From (4.2) we then define $A(t)$ by

$$A(t) = G + tXG = G + tQNQ^{-1}G \tag{4.6}$$

$A^{-1}(t)$ being given by (4.3).

Example. Take

$$N = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \qquad Q = \begin{bmatrix} 17 & 6 & 12 \\ 6 & 13 & 24 \\ 12 & 24 & 23 \end{bmatrix},$$

$$X = \begin{bmatrix} 24 & 13 & 18 \\ 10 & 0 & 14 \\ 20 & 0 & 2 \end{bmatrix}, \qquad G = \begin{bmatrix} 25 & 2 & 16 \\ 2 & 25 & 10 \\ 16 & 10 & 3 \end{bmatrix} (= G^{-1}),$$

$$XG = \begin{bmatrix} 4 & 7 & 22 \\ 6 & 4 & 20 \\ 12 & 8 & 14 \end{bmatrix}, \qquad G^{-1}X = \begin{bmatrix} 4 & 13 & 16 \\ 4 & 0 & 16 \\ 24 & 0 & 18 \end{bmatrix},$$

$$A(t) = \begin{bmatrix} 25 & 2 & 16 \\ 2 & 25 & 10 \\ 16 & 10 & 3 \end{bmatrix} + t \begin{bmatrix} 4 & 7 & 22 \\ 6 & 4 & 20 \\ 12 & 8 & 14 \end{bmatrix},$$

$$A^{-1}(t) = \begin{bmatrix} 25 & 2 & 16 \\ 2 & 25 & 10 \\ 16 & 10 & 3 \end{bmatrix} - t \begin{bmatrix} 4 & 13 & 16 \\ 4 & 0 & 16 \\ 24 & 0 & 18 \end{bmatrix}.$$

Using these in (4.1) gives

$$C_i = \begin{bmatrix} 25 + 4k_i & 2 + 7k_i & 16 + 22k_i \\ 2 + 6k_i & 25 + 4k_i & 10 + 20k_i \\ 16 + 12k_i & 10 + 8k_i & 3 + 14k_i \end{bmatrix} P_i, \tag{4.7}$$

$$P_i = \begin{bmatrix} 25 + 22k_i & 2 + 13k_i & 16 + 10k_i \\ 2 + 22k_i & 25 & 10 + 10k_i \\ 16 + 2k_i & 10 & 3 + 8k_i \end{bmatrix} C_i. \tag{4.8}$$

Take $k_i = p_{i-1,1} + p_{i-1,2} + p_{i-1,3}$, $(k_1 = 1)$, and encipher CRYPTOGRAPHIC(XX),

$$C_1 = \begin{bmatrix} 3 & 9 & 12 \\ 8 & 3 & 4 \\ 2 & 18 & 17 \end{bmatrix} \begin{bmatrix} 3 \\ 18 \\ 25 \end{bmatrix} = \begin{bmatrix} 3 \\ 22 \\ 1 \end{bmatrix} = \begin{bmatrix} \text{C} \\ \text{V} \\ \text{A} \end{bmatrix}, \qquad k_2 = 3 + 18 + 25 \equiv 20,$$

$$C_2 = \begin{bmatrix} 1 & 12 & 14 \\ 18 & 1 & 20 \\ 22 & 14 & 23 \end{bmatrix} \begin{bmatrix} 16 \\ 20 \\ 15 \end{bmatrix} = \begin{bmatrix} 24 \\ 10 \\ 15 \end{bmatrix} = \begin{bmatrix} \text{X} \\ \text{J} \\ \text{O} \end{bmatrix}, \qquad k_3 = 16 + 20 + 15 \equiv 25,$$

$$C_3 = \begin{bmatrix} 21 & 21 & 20 \\ 22 & 21 & 16 \\ 4 & 2 & 15 \end{bmatrix} \begin{bmatrix} 7 \\ 18 \\ 1 \end{bmatrix} = \begin{bmatrix} 25 \\ 2 \\ 1 \end{bmatrix} = \begin{bmatrix} \text{Y} \\ \text{B} \\ \text{A} \end{bmatrix}, \qquad k_4 = 7 + 18 + 1 \equiv 0,$$

$$C_4 = \begin{bmatrix} 25 & 2 & 16 \\ 2 & 25 & 10 \\ 16 & 10 & 3 \end{bmatrix} \begin{bmatrix} 16 \\ 8 \\ 9 \end{bmatrix} = \begin{bmatrix} 14 \\ 10 \\ 25 \end{bmatrix} = \begin{bmatrix} \text{N} \\ \text{J} \\ \text{Y} \end{bmatrix}, \qquad k_5 = 16 + 8 + 9 \equiv 7,$$

$$C_5 = \begin{bmatrix} 1 & 25 & 14 \\ 18 & 1 & 20 \\ 22 & 14 & 23 \end{bmatrix} \cdot \begin{bmatrix} 3 \\ 24 \\ 24 \end{bmatrix} = \begin{bmatrix} 3 \\ 12 \\ 18 \end{bmatrix} \quad \begin{bmatrix} \text{C} \\ \text{L} \\ \text{R} \end{bmatrix}.$$

The cipher-text is thus CVA XJO YBA NJY CLR.

To decipher, use (4.8),

$$P_1 = \begin{bmatrix} 21 & 15 & 0 \\ 24 & 25 & 20 \\ 18 & 10 & 11 \end{bmatrix} \begin{bmatrix} 3 \\ 22 \\ 1 \end{bmatrix} = \begin{bmatrix} 3 \\ 18 \\ 25 \end{bmatrix} = \begin{bmatrix} \text{C} \\ \text{R} \\ \text{Y} \end{bmatrix}, \text{ etc.}$$

There is an advantage in using an involutory transformation (4.1), *i.e.*, one such that $A(t) = A^{-1}(t)$. To obtain this we require from (4.3), (4.6),

$$G = G^{-1}, \qquad XG = -GX. \tag{4.9}$$

Define matrix J by

$$\begin{bmatrix} 1 & j_1 & & & & & & & \\ 0 & -1 & & & & & & & \\ & & 1 & j_2 & & & & & \\ & & 0 & -1 & & & & & \\ & & & & \ddots & & & & \\ & & & & & 1 & j_q & & \\ & & & & & 0 & -1 & & \\ & & & & & & & a_1 & \\ & & & & & & & & \ddots \\ & & & & & & & & & a_r \end{bmatrix} = J, \tag{4.10}$$

constants $j_1, \cdots, j_q$ arbitrary, and $a_1, \cdots, a_r$ all $= \pm 1$, $(r+2q=n)$.

Then by (4.4), (4.10),

$$J^2 = I, \qquad JN = -NJ. \tag{4.11}$$

Place

$$G = QJQ^{-1}, \qquad X = QNQ^{-1}, \tag{4.12}$$

giving

$$G^2 = I, \qquad XG = -GX, \qquad (X^2 = 0),$$

satisfying (4.9).

From (4.12), $XG = QNJQ^{-1} = -QNQ^{-1} = -X$, since direct calculation shows $NJ = -N$. Hence (4.6) gives

$$A(t) = G - tX = A^{-1}(t), \tag{4.13}$$

which can also be expressed as

$$A(t) = Q(J - tN)Q^{-1} = A^{-1}(t). \tag{4.14}$$

Example. Use N, Q, X of the previous example, and

$$J = \begin{bmatrix} 1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}.$$

By (4.12), (4.13)

$$G = \begin{bmatrix} 3 & 9 & 10 \\ 6 & 19 & 2 \\ 12 & 14 & 3 \end{bmatrix}, \quad A(t) = \begin{bmatrix} 3+2t & 9+13t & 10+8t \\ 6-10t & 19 & 2+12t \\ 12+6t & 14 & 3+24t \end{bmatrix} = A^{-1}(t).$$

In case $n=2$ it can be verified that

$$A(t) = A^{-1}(t) = \begin{bmatrix} a+bt & c+dt \\ e+ft & -(a+bt) \end{bmatrix}$$

if $a = bcd' \pm 1$, $e = -b^2c(d')^2 \mp 2bd'$, $f = -b^2d'$, and b, c, d are arbitrary (d prime mod 26), and $dd' \equiv 1 \bmod 26$.

The modulus 26 used throughout this paper is not essential. Other moduli can be used with suitable modifications where necessary.

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.