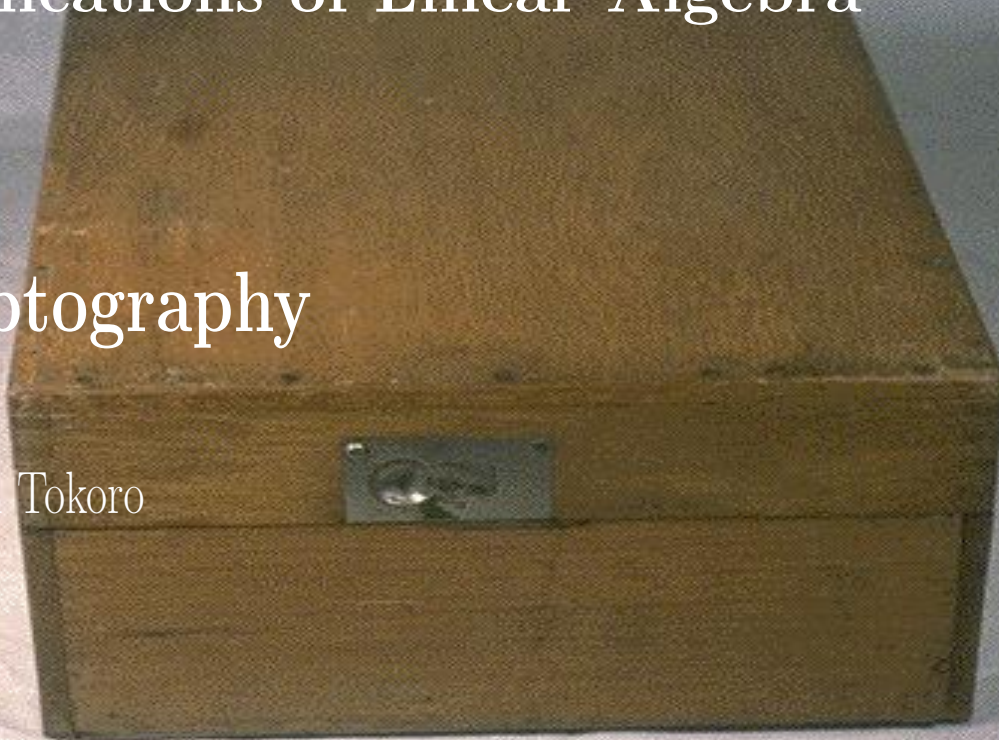


Applications of Linear Algebra

Cryptography

Shinichi Tokoro



1/36



Introduction

- Cryptography is the study of encoding and decoding private messages. Because its importance, there is a recent surge of interest in cryptography.
- In this subject, codes are called *ciphers*, uncoded messages are called *plaintext*, and coded messages are called *ciphertext*.
- The method of converting from plaintext to ciphertext is called enciphering, and the method of converting from ciphertext to plaintext is called deciphering.



Hill Ciphers

Hill cipher is the idea of encoding plaintext group by group, not just letter by letter. A system of cryptography in which the plaintext is divided into sets of n letters and replaced by a set of n cipher letters is called a polygraphic system. In this presentation, I will focus on a polygraphic system based on matrix transformation. In the discussion, assume each letter has numerical value based on its standard position. But we assume Z is a value of zero.

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

Table 1: Alphanumerics.





The general idea to produce ciphertext is following

- **Step 1.** Choose a 2×2 matrix with integer entries

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}.$$

- **Step 2.** Group plaintext letters into pairs, adding an arbitrary “dummy” letter to fill out the last pair if the plaintext has an odd number of letters, and replace each plaintext letter by its numerical equivalents.

- **Step 3.** Convert each plaintext pair $p_1 p_2$ into a column vector

$$p = \begin{pmatrix} p_1 \\ p_2 \end{pmatrix}.$$

and form the product Ap . We will call p a plaintext vector and Ap the corresponding ciphertext vector.

- **Step 4.** Convert each ciphertext vector into its alphabetic equivalent.



Enciphering

Suppose, we use the following matrix A

$$A = \begin{pmatrix} 7 & 3 \\ 1 & 2 \end{pmatrix}.$$

to gain the Hill cipher for the plaintext

(TAKE THE A TRAIN).

If we divide the plaintext into pairs and add the dummy letter N to fill out the last pair.

(TA KE TH EA TR AI NN).

and convert the alphabet to numbers

(20, 1 11, 5 20, 8 5, 1 20, 18 1, 9 14, 14).



To encipher these numbers of pairs, we put them in matrix form

$$\begin{pmatrix} 7 & 3 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 20 \\ 1 \end{pmatrix} = \begin{pmatrix} 143 \\ 22 \end{pmatrix} = \begin{pmatrix} 13 \\ 22 \end{pmatrix},$$

from Table 1, which leads the ciphertext MV.

In the above computation, we had a problem because the number 143 does not have any alphabet equivalent in the Table 1. To deal with these large numbers, we need the following rules.

- Whenever an integer is greater than 25, it must be replaced by the remainder that results when the integer is divided by 26(number of alphabet).
- After division by 26, we will obtain one of the integers 0, 1, 2, ..., 25, and this method always produces an integer with alphabet equivalent. Therefore, we replace 143 by 13, which is remainder after dividing 143 by 26, and now it fits in Table 1. The ciphertext for TA is MV.





The computation for other ciphertexts are following

$$\begin{pmatrix} 7 & 3 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 11 \\ 5 \end{pmatrix} = \begin{pmatrix} 92 \\ 21 \end{pmatrix} = \begin{pmatrix} 14 \\ 21 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 7 & 3 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 20 \\ 8 \end{pmatrix} = \begin{pmatrix} 164 \\ 36 \end{pmatrix} = \begin{pmatrix} 8 \\ 10 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 7 & 3 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 5 \\ 1 \end{pmatrix} = \begin{pmatrix} 38 \\ 7 \end{pmatrix} = \begin{pmatrix} 12 \\ 7 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 7 & 3 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 20 \\ 18 \end{pmatrix} = \begin{pmatrix} 194 \\ 56 \end{pmatrix} = \begin{pmatrix} 12 \\ 4 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 7 & 3 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 \\ 9 \end{pmatrix} = \begin{pmatrix} 34 \\ 19 \end{pmatrix} = \begin{pmatrix} 8 \\ 19 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 7 & 3 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 14 \\ 14 \end{pmatrix} = \begin{pmatrix} 140 \\ 42 \end{pmatrix} = \begin{pmatrix} 10 \\ 16 \end{pmatrix} \pmod{26}$$

These numbers correspond to the ciphertext sets NU,HJ,LG,LD,HS, and



JP. Thus, the overall ciphertext message look like

MVNUHJLGLDHSJP



Modular Arithmetic

In Example 1 sometime integers are greater than 25 and they were replaced by their remainders after being divided by 26. This method is called modular arithmetic. In modular arithmetic, one is given a positive integer m , called the *modulus*, and any two integers whose difference is an integer multiple of the modulus are regarded to be “equal” or “equivalent” with respect to the modulus. The definition is follows.

Definition 1 *If m is a positive integer and a and b are any integers, then we say that a is equivalent to $b \pmod{m}$, written*

$$a = b \pmod{m}$$

if $a - b$ is an integer multiple of m .



Example 1

$$9 = 4 \pmod{5}$$

$$15 = 0 \pmod{3}$$

$$-7 = 19 \pmod{26}$$

For any modulus m it can be proved that all number a 's are equal to exactly one of the integers

$$0, 1, 2, 3, \dots, m - 1$$

and this integer is called “the residue of a modulo m ,” and we write

$$\mathbb{Z}_m = 0, 1, 2, \dots, m - 1$$

to indicate the set of residues modulo m .

If a is a *positive* integer, then its residue modulo m is just the remainder of the result that a is divided by m . For a random integer a , we can find the residue by using the following assumption.





Theorem 1 For any integer a and modulus m , let R represent the remainder when $|a|$ is divided by m . Then, the residue r of a modulo m is given by

$$r = \begin{pmatrix} R & \text{if } a > 0 \\ m - R & \text{if } a < 0 \text{ and } R \neq 0 \\ 0 & \text{if } a < 0 \text{ and } R = 0 \end{pmatrix}$$

Example 2 Find the residue modulo 26 of (a) 77 and (b) -40 .

a) Dividing $|77| = 77$ by 26 gives a remainder of $R = 25$, so $r = 25$ by the theorem 1.

$$77 = 25 \pmod{26}$$

b) Dividing $|-40| = 40$ by 26 gives a remainder of $R = 14$, so $r = 26 - 14 = 12$ by the theorem 1.

$$-40 = 12 \pmod{26}$$

reciprocal or multiplicative inverse, denoted by a^{-1} , such that

$$aa^{-1} = a^{-1}a = 1.$$



In modular arithmetic we have the following corresponding concept:

Definition 2 If a is a number in Z_m , then a number a^{-1} in Z_m is called a reciprocal or multiplicative inverse of a modulo m if $aa^{-1} = a^{-1}a = 1 \pmod{m}$.

The following table is reciprocals modulo 26 for future reference.

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Table 2: Reciprocal modulo 26.

It can be proved that if a and m have no common prime factors, then a has a unique reciprocal modulo m , and conversely if a and m have a common prime factor then a has *no reciprocal modulo m* .



Deciphering

Functionable cipher must have a procedure for decipherment. In Hill cipher's case, decipherment uses the *inverse* (mod 26) of the enciphering matrix. If m is a positive integer, then a square matrix A with entries in \mathbb{Z}_m is called *invertible modulo m* if there is a matrix X with entries in \mathbb{Z}_m such that

$$AX = XA = I \pmod{m}.$$

Suppose,

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

is invertible modulo 26 and this matrix is used in a Hill 2-cipher. If

$$p = \begin{pmatrix} p_1 \\ p_2 \end{pmatrix}$$



is a plaintext vector, then

$$c = Ap$$

is the corresponding ciphertext vector and

$$p = A^{-1}c.$$

Therefore, every plaintext vector can be found by multiplying corresponding vector c and $A^{-1} \pmod{m}$ from the left.

In this subject, we must know which matrices are invertible modulo 26 and how to get their inverses.

In general arithmetic, a square matrix A is invertible if and only if its determinant is not zero ($\det(A) \neq 0$). Also, if and only if determinant of A has a reciprocal. If the matrix A has entries in Z_{26} ; also, the residue of $\det(A) = ad - bc \pmod{26}$ is not divisible by 2 or 13 such as 5, 7 and 11, then the inverse of $A \pmod{26}$ is following

$$A^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \pmod{26}$$



Example 3 To get the inverse of the matrix A

$$A = \begin{pmatrix} 7 & 3 \\ 1 & 2 \end{pmatrix} \pmod{26}.$$

Solution

$$\det(A) = ad - bc = 14 - 3 = 11$$

according to the table 2

$$(ad - bc)^{-1} = 11^{-1} = 19 \pmod{26}.$$

Therefore, according to the equation above

$$A^{-1} = 19 \begin{pmatrix} 2 & -3 \\ -1 & 7 \end{pmatrix} = \begin{pmatrix} 38 & -57 \\ -19 & 133 \end{pmatrix} = \begin{pmatrix} 12 & 21 \\ 7 & 3 \end{pmatrix} \pmod{26}.$$

now let's check,

$$AA^{-1} = \begin{pmatrix} 7 & 3 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 12 & 21 \\ 7 & 3 \end{pmatrix} = \begin{pmatrix} 105 & 156 \\ 26 & 27 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{26}.$$

Similarly, $A^{-1}A = I$.



Example 4 Decipher the 2-Hill cipher message below which enciphered by the matrix

$$A = \begin{pmatrix} 7 & 3 \\ 1 & 2 \end{pmatrix}.$$

MVNUHJLGLDHSJP

From the table 1, each alphabet has number equivalents below:

$$(13, 22 \quad 14, 21 \quad 8, 10 \quad 12, 7 \quad 12, 4 \quad 8, 19 \quad 10, 16)$$

To get the original plaintext messages, multiply each ciphertext vector by the inverse of the matrix A , which we already found in the previous example.

$$\begin{pmatrix} 12 & 21 \\ 7 & 3 \end{pmatrix} \begin{pmatrix} 13 \\ 22 \end{pmatrix} = \begin{pmatrix} 618 \\ 157 \end{pmatrix} = \begin{pmatrix} 20 \\ 1 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 12 & 21 \\ 7 & 3 \end{pmatrix} \begin{pmatrix} 14 \\ 21 \end{pmatrix} = \begin{pmatrix} 609 \\ 161 \end{pmatrix} = \begin{pmatrix} 11 \\ 5 \end{pmatrix} \pmod{26}$$





$$\begin{pmatrix} 12 & 21 \\ 7 & 3 \end{pmatrix} \begin{pmatrix} 8 \\ 10 \end{pmatrix} = \begin{pmatrix} 306 \\ 86 \end{pmatrix} = \begin{pmatrix} 20 \\ 8 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 12 & 21 \\ 7 & 3 \end{pmatrix} \begin{pmatrix} 12 \\ 7 \end{pmatrix} = \begin{pmatrix} 291 \\ 105 \end{pmatrix} = \begin{pmatrix} 5 \\ 1 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 12 & 21 \\ 7 & 3 \end{pmatrix} \begin{pmatrix} 12 \\ 4 \end{pmatrix} = \begin{pmatrix} 228 \\ 96 \end{pmatrix} = \begin{pmatrix} 20 \\ 18 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 12 & 21 \\ 7 & 3 \end{pmatrix} \begin{pmatrix} 8 \\ 19 \end{pmatrix} = \begin{pmatrix} 495 \\ 113 \end{pmatrix} = \begin{pmatrix} 1 \\ 9 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 12 & 21 \\ 7 & 3 \end{pmatrix} \begin{pmatrix} 10 \\ 16 \end{pmatrix} = \begin{pmatrix} 456 \\ 118 \end{pmatrix} = \begin{pmatrix} 14 \\ 14 \end{pmatrix} \pmod{26}$$

Now we got plaintext vectors

(20, 1 11, 5 20, 8 5, 1 20, 18 1, 9 14, 14)

and from the table1 these numbers have the following alphabet equivalents

(TA KE TH EA TR AI NN)



which gives us the message

(TAKE THE A TRAIN)



Hill 3-Cipher

Using Hill 2-cipher to encode and decode messages is relatively simple as we saw in previous example. However, using Hill 3-cipher is little more complex. I will show you a simple example.



Example

Suppose, we use the matrix

$$A = \begin{pmatrix} 15 & 8 & 6 \\ 25 & 15 & 20 \\ 21 & 3 & 17 \end{pmatrix}$$

and encode the message below.

(TAKE FIVE)

Group the plaintext into three letters and add the dummy to fill out last group.

(TAK EFI VEE)

Transform them to their equivalent numbers.

(20, 1, 11 5, 6, 9 22, 5, 5)



Multiply these plaintext vector by the matrix A.

$$\begin{pmatrix} 15 & 8 & 6 \\ 25 & 15 & 20 \\ 21 & 3 & 17 \end{pmatrix} \begin{pmatrix} 20 \\ 1 \\ 11 \end{pmatrix} = \begin{pmatrix} 374 \\ 735 \\ 610 \end{pmatrix} = \begin{pmatrix} 10 \\ 7 \\ 12 \end{pmatrix} \pmod{26}.$$

$$\begin{pmatrix} 15 & 8 & 6 \\ 25 & 15 & 20 \\ 21 & 3 & 17 \end{pmatrix} \begin{pmatrix} 5 \\ 6 \\ 9 \end{pmatrix} = \begin{pmatrix} 451 \\ 920 \\ 728 \end{pmatrix} = \begin{pmatrix} 21 \\ 5 \\ 16 \end{pmatrix} \pmod{26}.$$

$$\begin{pmatrix} 15 & 8 & 6 \\ 25 & 15 & 20 \\ 21 & 3 & 17 \end{pmatrix} \begin{pmatrix} 22 \\ 5 \\ 5 \end{pmatrix} = \begin{pmatrix} 400 \\ 725 \\ 562 \end{pmatrix} = \begin{pmatrix} 10 \\ 23 \\ 16 \end{pmatrix} \pmod{26}.$$

The corresponding ciphertext for above ciphertext vectors are

$(10, 7, 12 \quad 21, 5, 16 \quad 10, 23, 16)$

$(JGL \ UEP \ JWP)$

Then normally,

$JGLUEPJWP$



In order to decode these ciphertext, we need obtain the matrix A^{-1} .
At first, we need to get $\det(A)$ which is 15.

$$\det(A) = 15$$

From the result, we find $1/\det(A)$ which we can see in the table 2.

Then we apply these results to obtain A^{-1} and the formula is below:

$$A^{-1} = \frac{C^T}{\det(A)}$$

Cofactor matrix C is

$$C = \begin{pmatrix} 195 & -5 & -240 \\ -118 & 129 & 123 \\ 70 & -150 & 25 \end{pmatrix}.$$

$$A^{-1} = \frac{1}{15} \begin{pmatrix} 195 & -118 & 70 \\ -5 & 129 & -150 \\ -240 & 123 & 25 \end{pmatrix} = \begin{pmatrix} 1365 & -826 & 490 \\ -35 & 903 & -1050 \\ -1680 & 861 & 175 \end{pmatrix}$$



$$= \begin{pmatrix} 13 & 6 & 22 \\ 17 & 19 & 16 \\ 10 & 3 & 19 \end{pmatrix} \pmod{26}.$$

Let's check

$$AA^{-1} = \begin{pmatrix} 15 & 8 & 6 \\ 25 & 15 & 20 \\ 21 & 3 & 17 \end{pmatrix} \begin{pmatrix} 13 & 6 & 22 \\ 17 & 19 & 16 \\ 10 & 3 & 19 \end{pmatrix} = \begin{pmatrix} 391 & 260 & 572 \\ 780 & 495 & 1170 \\ 494 & 234 & 833 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \pmod{26}.$$

Now it's time to decode the message that we enciphered just before, and the ciphertext is

JGLUEPJWP

and divided to three letters of each group

(JGL UEP JWP)



From the table 1, these letters have numerical equivalents below:

$$(10, 7, 12 \quad 21, 5, 16 \quad 10, 23, 16)$$

To get plaintext, we multiply each ciphertext vector by A^{-1} .

$$\begin{pmatrix} 13 & 6 & 22 \\ 17 & 19 & 16 \\ 10 & 3 & 19 \end{pmatrix} \begin{pmatrix} 10 \\ 7 \\ 12 \end{pmatrix} = \begin{pmatrix} 436 \\ 495 \\ 349 \end{pmatrix} = \begin{pmatrix} 20 \\ 1 \\ 11 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 13 & 6 & 22 \\ 17 & 19 & 16 \\ 10 & 3 & 19 \end{pmatrix} \begin{pmatrix} 21 \\ 5 \\ 16 \end{pmatrix} = \begin{pmatrix} 655 \\ 707 \\ 529 \end{pmatrix} = \begin{pmatrix} 5 \\ 6 \\ 9 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 13 & 6 & 22 \\ 17 & 19 & 16 \\ 10 & 3 & 19 \end{pmatrix} \begin{pmatrix} 10 \\ 23 \\ 16 \end{pmatrix} = \begin{pmatrix} 620 \\ 863 \\ 476 \end{pmatrix} = \begin{pmatrix} 22 \\ 5 \\ 5 \end{pmatrix} \pmod{26}$$

As we can see the alphabet equivalents of these plaintext vectors are

$$(TAK \quad EFI \quad VEE)$$



Therefore the message is

(TAKE FIVE)



25/36



Breaking a Hill Cipher

In some certain circumstances, Gaussian elimination can break down codes if we could deduce first a few words of messages. In linear algebra that the values at a basis determine a linear transformation, and that means if we have a Hill n -cipher, and if

$$p_1, p_2, \dots, p_n$$

are linearly independent plaintext vectors whose corresponding ciphertext vectors

$$Ap_1, Ap_2, \dots, Ap_n$$

are known, then there is enough information to determine the matrix A , thus $A^{-1} \pmod{26}$. The following theorem give us a way to determine the matrix A .

Theorem 2 *Let p_1, p_2, \dots, p_n be linearly independent plaintext vectors, and let c_1, c_2, \dots, c_n be the corresponding ciphertext vectors in a*



Hill n -cipher. If

$$P = \begin{pmatrix} p_1^T \\ p_2^T \\ \cdot \\ \cdot \\ \cdot \\ p_n^T \end{pmatrix}$$

is the $n \times n$ matrix with row vectors $p_1^T, p_2^T, \dots, p_n^T$ and if

$$C = \begin{pmatrix} c_1^T \\ c_2^T \\ \cdot \\ \cdot \\ \cdot \\ c_n^T \end{pmatrix}$$

is the $n \times n$ matrix with row vectors $c_1^T, c_2^T, \dots, c_n^T$, then the sequence of elementary row operations that reduces C to I transforms P to $(A^{-1})^T$.



In other words, we can reduce from $[C|P]$ to $[I|(A^{-1})^T]$.

According to this theorem it is possible to find the deciphering matrix A^{-1} , but in the process it is required to find a sequence of row operations which reduce C to I and P to $(A^{-1})^T$ at the same time.



Example

Suppose, we intercepted following Hill 2-cipher:

$$(IX \ UM \ FQ \ KB \ PO \ HJ)$$

The message starts with “NEED” is given (which is totally unusual).

According to the table, the numerical equivalent of these plaintext is

$$(NE \ ED)$$

$$(14, 5 \ 5, 4)$$

and the numerical equivalent of the ciphertext is

$$(IX \ UM)$$

$$(9, 24 \ 21, 13)$$

Therefore, the plaintext and ciphertext vectors are

$$p_1 = \begin{pmatrix} 14 \\ 5 \end{pmatrix} \longleftrightarrow c_1 \begin{pmatrix} 9 \\ 24 \end{pmatrix}$$





$$p_2 = \begin{pmatrix} 5 \\ 4 \end{pmatrix} \longleftrightarrow c_2 \begin{pmatrix} 21 \\ 13 \end{pmatrix}$$

and then

$$C = \begin{pmatrix} c_1^T \\ c_2^T \end{pmatrix} = \begin{pmatrix} 9 & 24 \\ 21 & 13 \end{pmatrix}$$

and

$$P = \begin{pmatrix} p_1^T \\ p_2^T \end{pmatrix} = \begin{pmatrix} 14 & 5 \\ 5 & 4 \end{pmatrix}$$

We will reduce C to I and P to $(A^{-1})^T$, at the same time. Now we need establish an augmented matrix $[C|P]$, and reduce C until I . Then, consequently we get the matrix $[I|(A^{-1})^T]$, and calculations are following:

$$\begin{pmatrix} 9 & 24 & 14 & 5 \\ 21 & 13 & 5 & 4 \end{pmatrix}$$

multiplied the first row by $9^{-1} = 3 \pmod{26}$

$$\begin{pmatrix} 1 & 72 & 42 & 15 \\ 21 & 13 & 5 & 4 \end{pmatrix}$$



replaced row1 by its residue modulo 26

$$\begin{pmatrix} 1 & 20 & 16 & 15 \\ 21 & 13 & 5 & 4 \end{pmatrix}$$

added -21 times row1 to row2

$$\begin{pmatrix} 1 & 20 & 16 & 15 \\ 0 & -407 & -331 & -311 \end{pmatrix}$$

replaced row2 by its residue modulo 26

$$\begin{pmatrix} 1 & 20 & 16 & 15 \\ 0 & 9 & 7 & 1 \end{pmatrix}$$

multiplied the second row by $9^{-1} = 3 \pmod{26}$

$$\begin{pmatrix} 1 & 20 & 16 & 15 \\ 0 & 1 & 21 & 3 \end{pmatrix}$$

added 20 times the second row to the first row

$$\begin{pmatrix} 1 & 0 & -404 & -45 \\ 0 & 1 & 21 & 3 \end{pmatrix}$$



replaced row1 by its residue modulo 26

$$\begin{pmatrix} 1 & 0 & 12 & 7 \\ 0 & 1 & 21 & 3 \end{pmatrix}$$

Therefore,

$$(A^{-1})^T = \begin{pmatrix} 12 & 7 \\ 21 & 3 \end{pmatrix}$$

and the deciphering matrix is

$$A^{-1} = \begin{pmatrix} 12 & 21 \\ 7 & 3 \end{pmatrix}$$

In the process of deciphering, fist, we make the ciphertext into pairs and find the numerical equivalentents for them:

(IX UM FQ KB PO HJ)

(9, 24 21, 13 6, 17 11, 2 16, 15 8, 10)



Then, we multiply ciphertext vector and A^{-1} from the left side and find alphabet equivalents of plaintext pairs:

$$\begin{pmatrix} 12 & 21 \\ 7 & 3 \end{pmatrix} \begin{pmatrix} 9 \\ 24 \end{pmatrix} = \begin{pmatrix} 14 \\ 5 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 12 & 21 \\ 7 & 3 \end{pmatrix} \begin{pmatrix} 21 \\ 13 \end{pmatrix} = \begin{pmatrix} 5 \\ 4 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 12 & 21 \\ 7 & 3 \end{pmatrix} \begin{pmatrix} 6 \\ 17 \end{pmatrix} = \begin{pmatrix} 13 \\ 15 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 12 & 21 \\ 7 & 3 \end{pmatrix} \begin{pmatrix} 11 \\ 2 \end{pmatrix} = \begin{pmatrix} 18 \\ 5 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 12 & 21 \\ 7 & 3 \end{pmatrix} \begin{pmatrix} 16 \\ 15 \end{pmatrix} = \begin{pmatrix} 13 \\ 1 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 12 & 21 \\ 7 & 3 \end{pmatrix} \begin{pmatrix} 8 \\ 10 \end{pmatrix} = \begin{pmatrix} 20 \\ 8 \end{pmatrix} \pmod{26}$$



Therefore, we obtain the message from the plaintext pairs:

(14, 5 5, 4 13, 15 18, 5 13, 1 20, 8)

(*NE ED MO RE MA TH*)

Finally,

(*NEED MORE MATH*)



Conclusion

As I introduced, linear algebra could be applied to Cryptography even though it's relatively simple compared to other applications. However, if we apply it to other languages that have an extensive alphabet such as Japanese(71 alphabetical letters not including symbols), the computation would be a lot of work.



References

- [1] Strang, Gilbert. **Introduction to Linear Algebra**. Wellesley-Cambridge Press, 1998.
- [2] Arnold, David. His matlab and \LaTeX expertise.
- [3] Rorres, Chris and Anton, Howard. **Application of Linear Algebra**. John Wiley and Sons, 1984.

