Cryptography

Shinichi Tokoro

December 12, 2001

Abstract

A method of encoding and decoding messages using matrix system and modular arithmetic is discussed; also, it shows how Gaussian elimination can sometime break down an opponents code.

1. Acknowledgement

Because I'm still learning English as a second language, my mathematical explanations would be clumsy and hardly make sense. Therefore, I have used many partially paraphrased explanations from my resources. These explanations and definitions are mostly works by Chris Rorres and Howard Anton. However, the examples are all mine.

2. Introduction

Cryptography is the study of encoding and decoding secret messages. Because of necessity to maintain the privacy of information passed over public, there is a recent surge of interest in cryptography. In this subject, codes are called *ciphers*, uncoded massages 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*. In this paper we will focus on encoding and decoding by the matrix system.

Home Page

Title Page

◀◀ ▶▶

◀ ▶

Go Back

Full Screen

Close

Quit

3. Hill Ciphers

The ciphers that we will discuss are called *Hill ciphers* after Lester S. Hill, who introduced them. The main idea of Hill cipher is to divide the plaintext into groups of letters and encipher the plaintext group by group, not letter by letter. A system of cryptography in which the plaintext is divided into sets of n letters, each of which is replaced by a set of n cipher letters, is called a *polygraphic system*. In this section we will look at a class of polygraphic systems based on matrix transformations.

In the following discussion, we assume that each plaintext and ciphertext letter except Z is assigned the numerical value that specifies its position in the standard alphabet. For reason that will become clear later, Z is assigned a value of zero.

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

Table 1: Cipher.

In the simplest hill ciphers, pairs of plaintext are transformed into ciphertext by the method below:

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. Successively 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.

Home Page
Title Page
◀◀ ▶▶
◀ ▶
Page 2 of 18
Go Back
Full Screen
Close
Quit

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

Example 1 Suppose, we use the following matrix A

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

to gain the Hill cipher for the following plaintext.

TAKE THE A TRAIN

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

TA KE TH EA TR AI NN.

Convert the alphabet to numbers

$$\begin{pmatrix} 20, 1 & 11, 5 & 20, 8 & 5, 1 & 20, 18 & 1, 9 & 14, 14 \end{pmatrix}.$$

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

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

Table 1, which leads the ciphertext MV.

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

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 leads to an integer has an alphabet equivalent. Therefore, we replace 143 by 13, which is reminder after dividing 143 by 26, and now it fits in Table 1. The ciphertext for TA is MV.

The computations for other ciphertexts are following:

Acknowledgement
Introduction
Hill Ciphers
Modular Arithmetic
Deciphering
Hill 3-cipher
Breaking A Hill Cipher

Home Page

Title Page

◀◀ ▶▶

◀ ▶

Page 3 of 18

Go Back

Full Screen

Close

Quit

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

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

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

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

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

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

These numbers correspond to the ciphertext sets NU, HJ, LG, LD, HS, and JP. Thus, the overall ciphertext message look like

MVNUHJLGLDHSJP.

This is called *Hill 2-cipher* because a plaintext was grouped in pairs and converted by 2 × 2 matrix. In general, *Hill n-cipher*, plaintext is grouped into sets of n letters and enciphered by an $n \times n$ matrix.

4. Modular Arithmetic

In Example 1 sometime integers are greater than 25 and they were replaced by their remainders after divided by 26. This method of working with remainders is at the core of mathematics called *modular arithmetic.* Because of its significance we need a brief lesson on some of the ideas.

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.

Definition 1 *If m is a positive integer and a and b are any integers, then we say that a is equivalent to b modulo m, written*

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

Home Page
Title Page
◀◀ ▶▶
◀ ▶
Page 4 of 18
Go Back
Full Screen
Close
Quit

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

Example 2

$$\begin{aligned} 9 &= 4 \pmod 5 \\ 15 &= 0 \pmod 3 \\ -7 &= 19 \pmod{26} \end{aligned}$$

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

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

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

$$Z_m = 0, 1, 2, \ldots, m-1$$

to indicate the set of residues modulo m.

If a is a *positive* integer, then its residue modulo m is just the reminder 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 devided by m. Then, the residue r of a modulo m is given by*

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

Let do an example.

Example 3 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 reminder of $R = 14$, so $r = 26 - 14 = 12$ by the Theorem 1.

$$-40 = 12 \quad \text{mod } 26$$

Acknowledgement
Introduction
Hill Ciphers
Modular Arithmetic
Deciphering
Hill 3-cipher
Breaking A Hill Cipher

Home Page
Title Page
◀◀ ▶▶
◀ ▶
Page 5 of 18
Go Back
Full Screen
Close
Quit

In general arithmetic every nonzero number a has a *reciprocal* or *multiplicative inverse*, devoted 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 $aa^{-1} = a^{-1}a = 1 \pmod{m}$.*

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.

Example 4 The number "5" posses a reciprocal modulo 26 because 5 and 26 have no common prime factors. This reciprocal can be gained by finding the number x in Z_{26} that satisfies the modular equation.

$$5x = 1 \pmod{26}$$

This equation can be solved by installing the possible solutions, 0 to 25, and it yield $x = 21$ because

$$5 \times 21 = 105 = 1 \pmod{26}$$

Therefore,

$$5^{-1} = 21 \pmod{26}$$

Also, there is another technique to find it. The procedure is following:

If det(A)is given such as 15 and modulus is 26 we can apply following method which is called Euclidean Algunrithm finding GCD(15,26) (greatest common divisor).

$$\begin{aligned} 26 &= 15 \times 1 + 11 \\ 15 &= 11 \times 1 + 4 \\ 11 &= 4 \times 2 + 3 \\ 4 &= 3 \times 1 + 1 \end{aligned}$$

Then,

$$\begin{aligned}
1 &= 4 - 3 \times 1 \\
&= 4 - (11 - 4 \times 2) \\
&= 4 - 11 + 2 \times 4 \\
&= 3 \times 4 - 11 \\
&= 3(15 - 11 \times 1) - 11 \\
&= 3 \times 15 - 4 \times 11 \\
&= 3 \times 15 - 4 \times 11 \\
&= 3 \times 15 - 4(26 - 15) \\
&= 7 \times 15 - 4 \times 26.
\end{aligned}$$

Thus, 1 is linear combination of 15 and 26.

$$\begin{aligned}
1 &= 7 \times 15 - 4 \times 26 \\
1 &= 7 \times 15 \pmod{26}
\end{aligned}$$

Because 26=0,

$$\begin{aligned}
\frac{1}{15} &= 7 \\
\frac{1}{\det(A)} &= 7,
\end{aligned}$$

as you can check in the following Table 2.

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: A table of inverses, mod 26

5. Deciphering

A 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

Acknowledgement
Introduction
Hill Ciphers
Modular Arithmetic
Deciphering
Hill 3-cipher
Breaking A Hill Cipher

Home Page

Title Page

◀◀ ▶▶

◀ ▶

Page 7 of 18

Go Back

Full Screen

Close

Quit

entries in Z_m is called *invertible modulo m* if there is a matrix X with entries in 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 ($\det(A) = 0$). Also, if and only if determinant of A has a reciprocal. Following theorem is similarity of its result by modular arithmetic.

Theorem 2 *A square matrix A with entries in Z_m is invertible modulo m if and only if the residue of $\det(A)$ modulo m has a reciprocal modulo m.*

Because the residue of $\det(A)$ modulo m have a reciprocal modulo m if and only if this residue and m don't have common prime numbers, so we can establish the following corollary:

Corollary 1 *A square matrix A with entries in Z_m is invertible modulo m if and only if m and the residue of $\det(A)$ modulo m have no common prime factors.*

Since the only prime factors of $m = 26$ are 2 and 13, we can assume a corollary below.

Corollary 2 *A square matrix A with entries in Z_{26} is invertible modulo 26 if and only if the residue of $\det(A)$ modulo 26 is not divisible by 2 or 13.*

Acknowledgement
Introduction
Hill Ciphers
Modular Arithmetic
Deciphering
Hill 3-cipher
Breaking A Hill Cipher

Home Page

Title Page

◀◀ ▶▶

◀ ▶

Page 8 of 18

Go Back

Full Screen

Close

Quit

If

$$A = \begin{pmatrix} a & b \\ c & c \end{pmatrix}$$

has entries in Z_{26} and the residue of $\det(A) = ad - bc \mod 26$ is not divisible by 2 or 13 such as 5,7 and 11, then the inverse of A $\pmod{26}$ is following

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

where $(ad - bc)^{-1}$ is the multiplicative inverse of the residue of $ad - bc \pmod{26}$.

Example 5 Find the inverse of the matrix A.

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

First, calculate the determinant of A.

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

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

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

Acknowledgement
Introduction
Hill Ciphers
Modular Arithmetic
Deciphering
Hill 3-cipher
Breaking A Hill Cipher

Home Page
Title Page
◀◀ ▶▶
◀ ▶
Page 9 of 18
Go Back
Full Screen
Close
Quit

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 platintext vectors

$$(20, 1 \quad 11, 5 \quad 20, 8 \quad 5, 1 \quad 20, 18 \quad 1, 9 \quad 14, 14)$$

and from the Table 1 these numbers have the following alphabet equivalents.

TA KE TH EA TR AI NN

This gives us the message

TAKE THE A TRAIN.

Acknowledgement
Introduction
Hill Ciphers
Modular Arithmetic
Deciphering
Hill 3-cipher
Breaking A Hill Cipher

Home Page

Title Page

◀◀ ▶▶

◀ ▶

Page 10 of 18

Go Back

Full Screen

Close

Quit

6. 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 7 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.

$$\left(20, 1, 11 \qquad 5, 6, 9 \qquad 22, 5, 5\right)$$

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

$$\left(10, 7, 12 \qquad 21, 5, 16 \qquad 10, 23, 16\right)$$

Home Page
Title Page
◀◀ ▶▶
◀ ▶
Page 11 of 18
Go Back
Full Screen
Close
Quit

$$\text{JGL} \quad \text{UEP} \quad \text{JWP.}$$

Then normally,

$$\text{JGLUEPJWP.}$$

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

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

Thus, A^{-1} is

$$\begin{aligned} A^{-1} &= 7\begin{pmatrix} 195 & -118 & 70 \\ -5 & 129 & -150 \\ -240 & 123 & 25 \end{pmatrix} \\ &= \begin{pmatrix} 1365 & -826 & 490 \\ -35 & 903 & -1050 \\ -1680 & 861 & 175 \end{pmatrix} \\ &= \begin{pmatrix} 13 & 6 & 22 \\ 17 & 19 & 16 \\ 10 & 3 & 19 \end{pmatrix} \pmod{26}. \end{aligned}$$

Acknowledgement
Introduction
Hill Ciphers
Modular Arithmetic
Deciphering
Hill 3-cipher
Breaking A Hill Cipher

Home Page

Title Page

◀◀ ▶▶

◀ ▶

Page 12 of 18

Go Back

Full Screen

Close

Quit

Let's check.

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

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

JGLUEPJWP.

Grouping three letters at a time,

JGL UEP JWP.

From the Table 1 these letters have numerical equivalent below.

$$\begin{pmatrix} 10, 7, 12 & \quad 21, 5, 16 & \quad 10, 23, 16 \end{pmatrix}$$

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

Home Page

Title Page

◀◀ ▶▶

◀ ▶

Page 13 of 18

Go Back

Full Screen

Close

Quit

TAK EFI VEE.

Therefore the message is

TAKE FIVE.

7. Breaking A Hill Cipher

In this section, I will discus one technique for breaking Hill ciphers. Suppose we can get some corresponding plaintext and ciphertext from an opponent's message. If we could deduce first a few words of message such as DEAR Mr.... because it's such a common start of letters, it might be possible to determine the deciphering matrix and eventually get access to the rest of massage.

In linear algebra, the values at a basis determine a linear transformation, and that means if we have a Hill n-cipher, and if

$$p_1, p_2, \ldots, p_n$$

are linearly independent plaintext vectors whose corresponding ciphertext vectors

$$Ap_1, Ap_2, \ldots, Ap_n$$

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

Theorem 3 *Let $p_1, p_2, \ldots, p_n$ be linearly independent plaintext vectors, and let $c_1, c_2, \ldots, c_n$ be the corresponding ciphertext vectors in a Hill n-cipher. If*

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

Home Page

Title Page

◀◀ ▶▶

◀ ▶

Page 14 of 18

Go Back

Full Screen

Close

Quit

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

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

is the n by n matrix with row vectors $c_1^T, c_2^T, \ldots, c_n^T$, 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, so let look at following example.

Example 8 Suppose, we intercepted following Hill 2-cipher:

$$\text{IX} \quad \text{UM} \quad \text{FQ} \quad \text{KB} \quad \text{PO} \quad \text{HJ}$$

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

According to Table 1, the numerical equivalent of these plaintext is

$$\text{NE} \quad \text{ED}$$

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

and the numerical equivalent of the ciphertext is

$$\text{IX} \quad \text{UM}$$

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

Therefore, the plaintext and ciphertext vectors are

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

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

Acknowledgement
Introduction
Hill Ciphers
Modular Arithmetic
Deciphering
Hill 3-cipher
Breaking A Hill Cipher

Home Page

Title Page

◀◀ ▶▶

◀ ▶

Go Back

Full Screen

Close

Quit

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:

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

Multiply row 1 by $9^{-1} = 3 \pmod{26}$.

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

Replace row1 by its residue modulo 26.

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

Add -21 times row 1 to row 2.

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

Replace row 2 by its residue modulo 26.

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

Multiply the row 2 by $9^{-1} = 3 \pmod{26}$.

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

Add 20 times row 2 to row 1.

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

Replace row 1 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 equivalents for them:

$$\begin{matrix} \text{IX} & \text{UM} & \text{FQ} & \text{KB} & \text{PO} & \text{HJ} \end{matrix}$$

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

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 massage from the plaintext pairs:

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

Home Page
Title Page
◀◀ ▶▶
◀ ▶
Page 17 of 18
Go Back
Full Screen
Close
Quit

NE ED MO RE MA TH

Finally,

NEED MORE MATH.

References

[1] Strang, Gilbert. **Introduction to Linear Algebra.** Sellesley-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.

Home Page
Title Page
◀◀ ▶▶
◀ ▶

Go Back
Full Screen
Close
Quit