10.14 Cryptography

Cryptography is the study of writing in secret code that goes back to ancient times. Modern cryptography intersects the disciplines of mathematics, computer science, and engineering.

Applications of cryptography include

- ATM cards
- Computer passwords
- and electronic commerce.

More precisely study of encoding and decoding of secret message is called cryptography.

Here we will use some terms:

- **Cipher text**: coded messages are called cipher text(CT).
- **Plaintext**: encoded messages are called plaintext and is denoted by PT.
- **Enciphering**: the process of converting from plain text to cipher text is called enciphering, also known as encoding.
- **Deciphering**: the reverse process of converting from cipher text to plain text is called deciphering, also known as decoding.

The simplest ciphers, called substitution ciphers, are those that replace each letter of the alphabet by a different letter. For example, in the substitution cipher

Plain 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

Cipher D E F G H I J K L M N O P Q R S T U V W X Y Z A B

the plaintext letter A is replaced by D, the plaintext letter B by E, and so forth. With this cipher the plaintext message

for example: NEED HELP becomes QHHG KHOS

ROME WAS NOT BUILT IN A DAY

Becomes

URPH ZDV QRW EX LOW LQ D GDB

A disadvantage of substitution ciphers is that it is relatively easy to break the code by statistical methods.

One method of encryption using linear algebra, specifically matrix operations, we call Hill ciphers. The method involves two matrices: one to encode, the encoding matrix, and one to decode, the decoding matrix (usually inverse of encoding matrix).

Before exploring further such a method, we should have basic knowledge of

1. Matrix multiplication
2. Inverse of a matrix
3. Modular arithmetic

Modular Arithmetic: In modular arithmetic we are given a positive integer n, called the modulus and any two integers whose difference is an integer multiple of the modulus, are regarded as "equal" or "equivalent" with respect to the modulus n. More precisely, we have

Definition: If n is a positive integer and a and b are any integers, then we say that a is equivalent to b modulo n, written as $a \equiv b \ (mod\ n)$, If $a - b$ is an integer multiple of n.

For example: $7 \equiv 2 \ (mod\ 5)$ here dividing 7 by 5 we have 2 remainder

$19 \equiv 1 \ (mod\ 2)$ here dividing 19 by 2 we have 1 remainder

$1 \equiv 25 \ (mod\ 26)$

$12 \equiv 0 \ (mod\ 6)$

Hill Ciphers

First, the characters in the original message or stream are assigned numerical values. For the purposes of this document, A-Z are represented by the numbers 1-26 (26 ≡ 0).

The encoding matrix can be generated using any integers that the user desires. It can be something as simple as a 2x2 or 3x3 matrix composed of random integers. The matrix must be invertible for use in decoding.

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	26

Example 1. Use the key matrix K= $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$, to obtain the Hill cipher from the plain text "**HELP**".

Solution: Step 1. Group successive plaintext letters into pairs and replace each plaintext letter by its numerical value. Here from the above table

$$H \rightarrow 8$$
$$E \rightarrow 5$$
$$L \rightarrow 12$$
$$P \rightarrow 16$$

Firstly, we will do work for HE and then we will do for LP.

Step 2

convert each plaintext pair into a column vector $P = \begin{bmatrix} H \\ E \end{bmatrix}$ plaintext vector.

Replacing each letter by its numerical value $P = \begin{bmatrix} 8 \\ 5 \end{bmatrix}$

Using formula for ciphertext vector

$$C = KP(mod26) = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}\begin{bmatrix} 8 \\ 5 \end{bmatrix} = \begin{bmatrix} 24+15 \\ 16+25 \end{bmatrix} =$$

$$= \begin{bmatrix} 39 \\ 41 \end{bmatrix}(mod26) = \begin{bmatrix} 13 \\ 15 \end{bmatrix}$$ (how)

Now again from the table of Hill Ciphers

$$\begin{bmatrix} 13 \\ 15 \end{bmatrix} = \begin{bmatrix} M \\ O \end{bmatrix}$$ ciphertext vector.

Step 3

Now we work for LP

using numerical values of alphabets for the pair LP,

$$P = \begin{bmatrix} L \\ P \end{bmatrix} \text{ implies } \quad P = \begin{bmatrix} 12 \\ 16 \end{bmatrix}$$

$$C = KP(mod\ 26) = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}\begin{bmatrix} 12 \\ 16 \end{bmatrix}(mod26) = \begin{bmatrix} 84 \\ 104 \end{bmatrix}(mod\ 26) = \begin{bmatrix} 6 \\ 0 \end{bmatrix}$$

Now

$$\begin{bmatrix} 6 \\ 0 \end{bmatrix} = \begin{bmatrix} F \\ Z \end{bmatrix}$$ ciphertext vector.

Hence, combining the ciphertext vectors the entire ciphertext message is **MOFZ.**

Example 2

Use the matrix

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$$

to obtain the Hill cipher for the plaintext message

I AM HIDING

Solution

If we group the plaintext into pairs and add the dummy letter G to fill out the last pair, we obtain

$$IA \quad MH \quad ID \quad IN \quad GG$$

or, equivalently, from Table 1,

$$9\,1 \quad 13\,8 \quad 9\,4 \quad 9\,14 \quad 7\,7$$

To encipher the pair IA, we form the matrix product

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}\begin{bmatrix} 9 \\ 1 \end{bmatrix} = \begin{bmatrix} 11 \\ 3 \end{bmatrix}$$

which, from Table 1, yields the ciphertext KC.

To encipher the pair MH, we form the product

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}\begin{bmatrix} 13 \\ 8 \end{bmatrix} = \begin{bmatrix} 29 \\ 24 \end{bmatrix} = \begin{bmatrix} 3 \\ 24 \end{bmatrix} = C\ X$$

The computations for the remaining ciphertext vectors are

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}\begin{bmatrix} 9 \\ 4 \end{bmatrix} = \begin{bmatrix} 17 \\ 12 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}\begin{bmatrix} 9 \\ 14 \end{bmatrix} = \begin{bmatrix} 37 \\ 42 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} 11 \\ 16 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}\begin{bmatrix} 7 \\ 7 \end{bmatrix} = \begin{bmatrix} 21 \\ 21 \end{bmatrix}$$

These correspond to the ciphertext pairs QL, KP, and UU, respectively. In summary, the entire ciphertext message is

$$KC \quad CX \quad QL \quad KP \quad UU$$

which would usually be transmitted as a single string without spaces:

$$KCCXQLKPUU$$

Because the plaintext was grouped in pairs and enciphered by a 2×2 matrix, the Hill cipher in Example 1, 2 is referred to as a Hill 2-cipher. It is obviously also possible to group the plaintext in triples and encipher by a 3×3matrix with integer entries; this is called a Hill 3-cipher. In general, for a Hill n-cipher, plaintext is grouped into sets of n letters and enciphered by an $n \times n$ matrix with integer entries.

Example 3

Encode the message TO GIVE

$$\text{using } A = \begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 0 & 1 & 1 \end{bmatrix}$$

Solution: Step 1

T	O	G	I	V	E
20	15	7	9	22	5

Group successive plaintext letters numerical values into 3x1 size vectors, as given coding matrix is of 3x3 size. Here we have combined the step 2 and 3 as

$$X=\begin{bmatrix}20 & 9\\ 15 & 22\\ 7 & 5\end{bmatrix}$$

Product AX will generate the coded message

$$AX=\begin{bmatrix}1 & 2 & 0\\ 0 & 1 & 2\\ 0 & 1 & 1\end{bmatrix}\begin{bmatrix}20 & 9\\ 15 & 22\\ 7 & 5\end{bmatrix}$$

$$=\begin{bmatrix}20+30+0 & 9+44+0\\ 0+15+14 & 0+22+10\\ 0+15+7 & 0+22+5\end{bmatrix}=\begin{bmatrix}50 & 53\\ 29 & 32\\ 22 & 27\end{bmatrix}(mod\ 26)=\begin{bmatrix}24 & 1\\ 3 & 6\\ 22 & 1\end{bmatrix}$$

Hence, the entire ciphertext message is **XCVAFA.**

Work to do

Q1. Encode the message **DARK NIGHT** using key matrix $\begin{bmatrix}1 & 3\\ 2 & 1\end{bmatrix}$.

Q2. Use the matrix $\begin{bmatrix}1 & 2\\ 0 & 3\end{bmatrix}$ to obtain Hill-Cipher from the plain text **ATTACK.**

Q3. Encode the message TIME UP using $A=\begin{bmatrix}1 & 2 & 4\\ 0 & -1 & 2\\ 0 & 1 & -1\end{bmatrix}$