Cryptography

Lecture No. 5

Aniqa Naeem

University of Central Punjab

aniqa.naeem@ucp.edu.pk

November 17, 2022

Presentation Overview

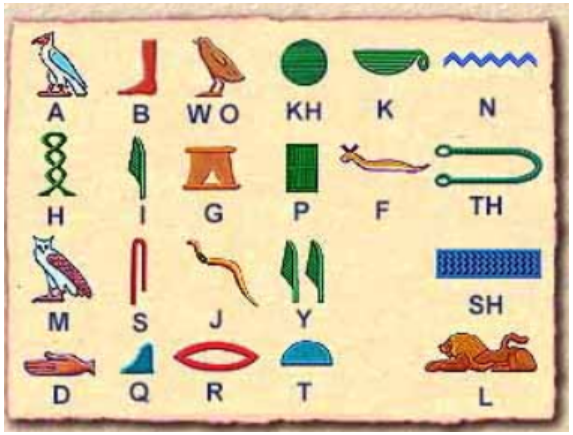
History of Cryptography

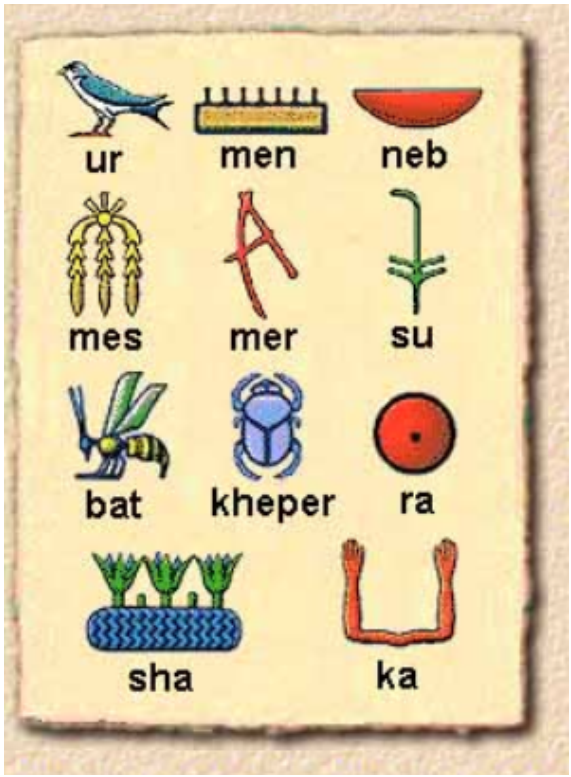
- As civilization evolved, human beings get organized in tribes, groups, and kingdoms.
- This led to the emergence of ideas such as power, battles, supremacy and politics.
- These ideas further fueled the natural need of people to communicate secretly with selective recipient which in turn ensured the continuous evolution of cryptography as well.
- The roots of cryptography are found in Roman and Egyptian Civilization.

Hieroglyph

Hieroglyphic

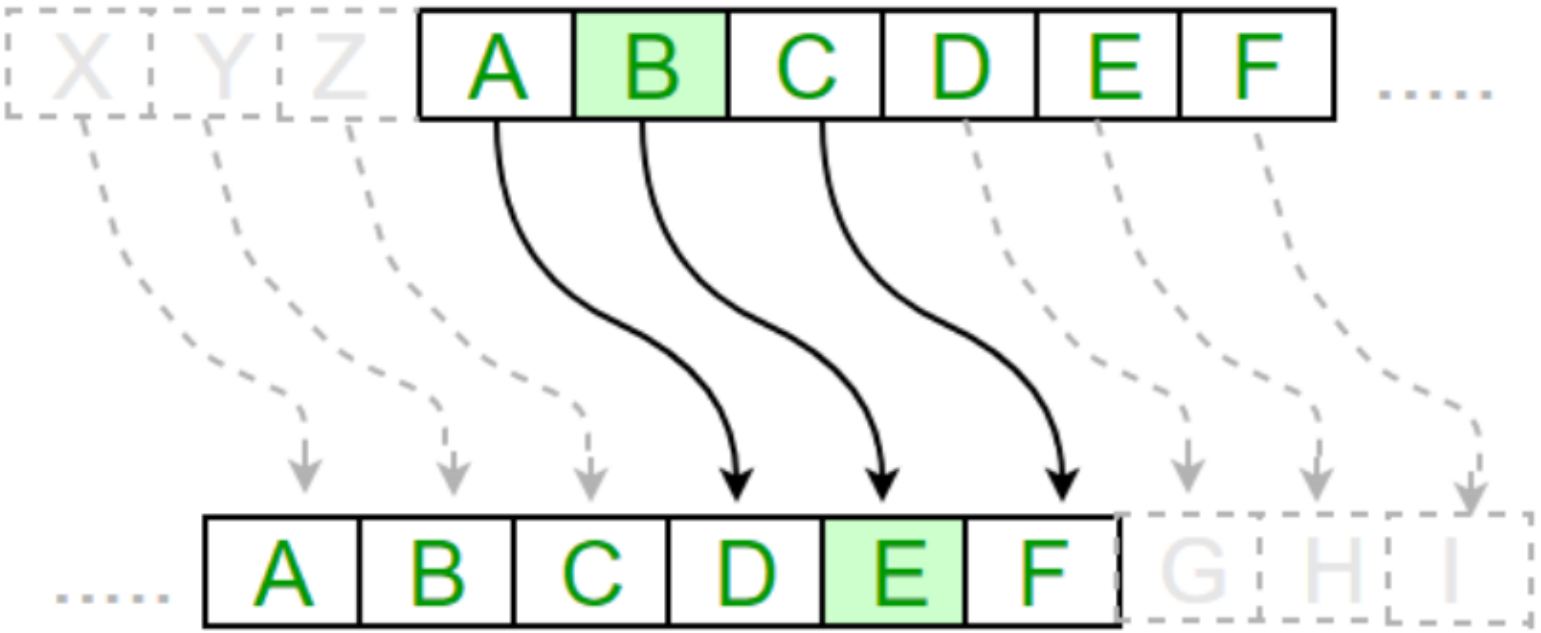
The first known evidence of cryptography can be traced to the use of Hieroglyph.Some 4000 years ago, the Egyptians used to communicate by messages written in Hieroglyph.


A
B
WO
KH
K
N
H
I
G
P
F
TH
M
S
J
Y
SH
D
Q
R
T
L


ur
men
neb
mes
mer
su
bat
kheper
ra
sha
ka

Caesar Shift Cipher

- Caesar Shift Cipher, relies on shifting the letters of a message by an agreed number (three was a common choice), the recipient of this message would then shift the letters back by the same number and obtain the original message.
- The Caesar Cipher is named after Julius Caesar, who used it with a shift of three to protect messages of military Significance.


X
Y
Z
A
B
C
D
E
F
A
B
C
D
E
F
G
H
I

Cryptography

- Cryptography is the science of using mathematics to encrypt and decrypt data (**Phil Zimmerman**)
- Cryptography is the art and science of keeping messages secure. (**Bruce Schneier**)
- The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography.
- The study of encoding and decoding messages is called cryptography.

Applications of Cryptography

- ATM CARDS
- Computer Passwords
- Electronic Commerce.
- This is the grooming area of linear algebra applications because agencies such as the CIA use cryptography to encode and decode information.

Terminologies of Cryptography

Plain Text

A message is **Plain Text** (sometimes called **clear text**).

Encryption

The process of disguising a message in such a way as to hide its substance is **encryption**.

Cipher Text

An encrypted message is called **Cipher Text**.

Decryption

The process of turning cipher text back into plain text is **decryption**

Cipher

A Cipher (or Cypher) is an algorithm for performing encryption or decryption- a series of well-defined steps that can be followed as a procedure.

Substitution Cipher

The simplest ciphers, called **Substitution Ciphers**, are those that replace each letter of the alphabet by a different letter.
Example in substitution cipher the plain text A is replaced by D, the plain text letter B by E, and so forth.

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

Example:

- NEED HELP
  becomes
  QHHG KHDS
- ROME WAS NOT BUILT IN A DAY
  becomes
  URPH ZDV QRW EXLOW LQ D GDB

Disadvantage of Substitution Cipher

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

Continue...

One method of encryption using linear algebra, is matrix operations , we call it 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 explaining further such a method, we should have basic knowledge of

- Matrix Multiplication
- Inverse of a Matrix
- Modular Arithmetic

First two methods are discussed in earlier lectures.Here we will discuss Modular Arithmetic

Modular Arithmetic

When we divide two integers we will have an equation that looks like the following:

$$\frac{A}{B} = Q \text{ remainder } R$$

Here
A is the dividend
B is the divisor
Q is the quotient
R is the remainder

Sometimes, we are only interested in what the remainder is when we divide A by B.
For these cases there is an operator called the **modulo operator(abbreviated as mod)**.
Using the same A,B,Q and R as above, we would have:

$$A \ mod \ B = R$$

Example:
$\frac{13}{5}$=2 remainder 3
OR
13 mod 5=3.

Modulo

Modulo

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.

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

Hill Cipher

Hill Cipher

Hill cipher is a poly-graphic substitution cipher based on linear algebra.Each letter is represented by a number modulo 26. Often the simple scheme $A = 1, B = 2, \ldots, Z = 26 (26 \equiv 0)$ is used, but this is not an essential feature of the cipher. To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible $n \times n$ matrix, against modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption. The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible $n \times n$ matrices (modulo 26).

Continue...

It can be something as simple as a 2×2 or 3×3 matrix composed of random integers. The matrix must be invertible for use in decoding.

Plain	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Cipher	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Plain	P	Q	R	S	T	U	V	W	X	Y	Z				
Cipher	16	17	18	19	20	21	22	23	24	25	26=0				

Example

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 plain text letters into pairs and replace each plain text 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 plain text pair into a column vector

$P = \begin{bmatrix} H \\ E \end{bmatrix} \rightarrow$ plain text vector.

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

Using formula for cipher text vector

$$C = KP(mod 26) = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 8 \\ 5 \end{bmatrix} = \begin{bmatrix} 24 + 15 \\ 16 + 25 \end{bmatrix} = \begin{bmatrix} 39 \\ 41 \end{bmatrix} (mod 26) = \begin{bmatrix} 13 \\ 15 \end{bmatrix} \text{(how)}$$

Now again from the table of Hill Ciphers

$\begin{bmatrix} 13 \\ 15 \end{bmatrix} = \begin{bmatrix} M \\ O \end{bmatrix} \rightarrow$ cipher text vector

STEP 3: Convert each plain text pair into a column vector

P = $\begin{bmatrix} L \\ P \end{bmatrix}$ $\rightarrow$ plain text vector.

Replacing each letter by its numerical value P = $\begin{bmatrix} 12 \\ 16 \end{bmatrix}$

Using formula for cipher text vector

$C = KP(mod26)$ = $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$ $\begin{bmatrix} 12 \\ 16 \end{bmatrix}$ = $\begin{bmatrix} 36+48 \\ 24+80 \end{bmatrix}$ = $\begin{bmatrix} 84 \\ 104 \end{bmatrix}$ $(mod26)$ = $\begin{bmatrix} 6 \\ 0 \end{bmatrix}$

Now again from the table of Hill Ciphers

$\begin{bmatrix} 6 \\ 0 \end{bmatrix}$ = $\begin{bmatrix} F \\ Z \end{bmatrix}$ $\rightarrow$ cipher text vector.

Hence, combining the cipher text vectors the entire cipher text message is MOFZ

Examples

Example 2: Use the matrix k= $\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$ to obtain the Hill Cipher for the plain text message **I AM IN DANGER**.

Solution:

If we group the plain text into pairs and add the dummy letter R to fill out the last pair, we obtain

IA MI ND AN GE RR

From Table we have

91 139 144 114 75 1818

To encipher the pair IA we form the product

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

which from Table, yields the cipher text KC.

Continue...

To encipher the pair MH, we form the product.

$$\begin{bmatrix}1 & 2\\ 0 & 3\end{bmatrix}\begin{bmatrix}13\\ 9\end{bmatrix}=\begin{bmatrix}13+18\\ 0+27\end{bmatrix}=\begin{bmatrix}31\\ 27\end{bmatrix}(\text{mod } 26)=\begin{bmatrix}5\\ 1\end{bmatrix}$$

$$=\begin{bmatrix}E\\ A\end{bmatrix}$$

Now, the remaining computations are

$$\begin{bmatrix}1 & 2\\ 0 & 3\end{bmatrix}\begin{bmatrix}14\\ 4\end{bmatrix}=\begin{bmatrix}14+8\\ 0+12\end{bmatrix}=\begin{bmatrix}22\\ 12\end{bmatrix}(\text{mod } 26)=\begin{bmatrix}22\\ 12\end{bmatrix}$$

$$=\begin{bmatrix}V\\ L\end{bmatrix}$$

$$\begin{bmatrix}1 & 2\\ 0 & 3\end{bmatrix}\begin{bmatrix}1\\ 14\end{bmatrix}=\begin{bmatrix}1+28\\ 0+42\end{bmatrix}=\begin{bmatrix}29\\ 42\end{bmatrix}(\text{mod } 26)=\begin{bmatrix}3\\ 16\end{bmatrix}$$

$$=\begin{bmatrix}C\\ P\end{bmatrix}$$

Continue..

$$\begin{bmatrix}1 & 2\\ 0 & 3\end{bmatrix}\begin{bmatrix}7\\ 5\end{bmatrix}=\begin{bmatrix}7+10\\ 0+15\end{bmatrix}=\begin{bmatrix}17\\ 15\end{bmatrix}(\text{mod } 26)=\begin{bmatrix}17\\ 15\end{bmatrix}$$

$$=\begin{bmatrix}Q\\ O\end{bmatrix}$$

$$\begin{bmatrix}1 & 2\\ 0 & 3\end{bmatrix}\begin{bmatrix}18\\ 18\end{bmatrix}=\begin{bmatrix}18+36\\ 0+54\end{bmatrix}=\begin{bmatrix}54\\ 54\end{bmatrix}(\text{mod } 26)=\begin{bmatrix}2\\ 2\end{bmatrix}$$

$$=\begin{bmatrix}B\\ B\end{bmatrix}$$

The cipher text is now

K CE AV LCPQOBB

Continue...

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

Continue...

Example 3:

Encode the message **TO GIVE** using $k = \begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 0 & 1 & 1 \end{bmatrix}$

Solution:

Replace each plain text value with its numerical value

TO GIVE

From table

2015 79225

Group successive plain text letetrs numerical values into 3×1 size vectors, as given coding matrix is of size 3×3 size. Here we have combined the step 2 and 3 as

Continue...

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

Product kX will generate the coded message

$$kX=\begin{bmatrix}1 & 2 & 0\\ 0 & 1 & 2\\ 0 & 1 & 1\end{bmatrix}\begin{bmatrix}20 & 9\\ 15 & 22\\ 7 & 5\end{bmatrix}=\begin{bmatrix}20+30+0 & 9+44+0\\ 0+15+14 & 0+22+10\\ 0+15+7 & 0+22+5\end{bmatrix}$$

$$=\begin{bmatrix}50 & 53\\ 29 & 32\\ 22 & 27\end{bmatrix}\ (\text{mod}26)=\begin{bmatrix}24 & 1\\ 3 & 6\\ 22 & 1\end{bmatrix}$$

Hence, the entire cipher text message is XC VAFA.

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 $K = \begin{bmatrix} 1 & 2 & 4 \\ 0 & -1 & 2 \\ 0 & 1 & -1 \end{bmatrix}$

Deciphering/Decryption

Decryption

The process of converting from cipher text to plain text is called deciphering.

Example

The following example will explain the procedure for deciphering.

Example 1: Decipher the cipher text **MOFZ** for key matrix k= $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$

Solution: The formula used for enciphering is:

$C = kP(mod26)$

Formula for deciphering

$P = k^{-1}C(mod26)$

$K^{-1} = \frac{adjK}{detK}(mod26)$

Thus each plain text vector can be recovered from ciphertext vector by multiplying it on the left by $K^{-1}(mod26)$.

Continue...

Step 1:

First find K^{-1}, so $det(K) = |k| = \begin{vmatrix} 3 & 3 \\ 2 & 5 \end{vmatrix} = 15 - 6 = 9$

$$K^{-1} = \frac{\begin{vmatrix} 3 & 3 \\ 2 & 5 \end{vmatrix}}{9}(mod 26) = 9^{-1}\begin{vmatrix} 3 & 3 \\ 2 & 5 \end{vmatrix}$$

What is the inverse of 9 modulo 26?

Let it be x, then $9x = 1(mod 26)$

$9.1 = 9 \neq 1(mod 26)$

$9.2 = 18 \neq 1(mod 26)$

$9.3 = 27 = 1(mod 26)$

Continue..

Hence,$9^{-1} = 3(mod 26)$

Therefore,

$$K^{-1} = 9^{-1}\begin{vmatrix} 5 & -3 \\ -2 & 3 \end{vmatrix} = 3\begin{vmatrix} 5 & -3 \\ -2 & 3 \end{vmatrix} = \begin{vmatrix} 15 & -9 \\ -6 & 9 \end{vmatrix}(mod 26) = \begin{vmatrix} 15 & 17 \\ 20 & 9 \end{vmatrix}$$

Step 2: Now, we will decipher MO first, then we will decipher FZ.

For this we take C= $\begin{bmatrix} M \\ O \end{bmatrix} = \begin{bmatrix} 13 \\ 15 \end{bmatrix}$

P = $K^{-1}C(mod 26)$

P= $\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}\begin{bmatrix} 13 \\ 15 \end{bmatrix} = \begin{bmatrix} 450 \\ 395 \end{bmatrix}(mod 26) = \begin{bmatrix} 8 \\ 5 \end{bmatrix}(mod 26)$

Alphabets equivalent of the vector is $\begin{bmatrix} H \\ E \end{bmatrix}$

Continue...

Step 3: Now, we will decipher FZ.

For this we take C= $\begin{bmatrix} F \\ Z \end{bmatrix} = \begin{bmatrix} 6 \\ 0 \end{bmatrix}$

P = $K^{-1}C(mod26)$

P= $\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 6 \\ 0 \end{bmatrix} = \begin{bmatrix} 90 \\ 120 \end{bmatrix} (mod26) = \begin{bmatrix} 12 \\ 16 \end{bmatrix} (mod26)$

Alphabets equivalent of the vector is $\begin{bmatrix} L \\ P \end{bmatrix}$

So all plain text is HELP.

Example 7. Decode the following Hill 2-cipher, which was enciphered by the matrix $K = \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix}$

GTNKGKDUSK

Solution: We first find the inverse of K (mod 26) as

$$K^{-1} = 3^{-1}\begin{bmatrix} 3 & -6 \\ -2 & 5 \end{bmatrix} = 9\begin{bmatrix} 3 & -6 \\ -2 & 5 \end{bmatrix}$$

$$= \begin{bmatrix} 27 & -54 \\ -18 & 45 \end{bmatrix}(mod 26) = \begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix}$$

Next we write numerical equivalent of cipher text, which is

7 20 14 11 7 11 4 21 19 11

To obtain the plaintext pairs, we multiply each ciphertext vector by the inverse of A (obtained in Example 6):

$$\begin{bmatrix}1 & 24\\ 8 & 19\end{bmatrix}\begin{bmatrix}7\\ 20\end{bmatrix}=\begin{bmatrix}487\\ 436\end{bmatrix}=\begin{bmatrix}19\\ 20\end{bmatrix} \pmod{26}$$

$$\begin{bmatrix}1 & 24\\ 8 & 19\end{bmatrix}\begin{bmatrix}14\\ 11\end{bmatrix}=\begin{bmatrix}278\\ 321\end{bmatrix}=\begin{bmatrix}18\\ 9\end{bmatrix} \pmod{26}$$

$$\begin{bmatrix}1 & 24\\ 8 & 19\end{bmatrix}\begin{bmatrix}7\\ 11\end{bmatrix}=\begin{bmatrix}271\\ 265\end{bmatrix}=\begin{bmatrix}11\\ 5\end{bmatrix} \pmod{26}$$

$$\begin{bmatrix}1 & 24\\ 8 & 19\end{bmatrix}\begin{bmatrix}4\\ 21\end{bmatrix}=\begin{bmatrix}508\\ 431\end{bmatrix}=\begin{bmatrix}14\\ 15\end{bmatrix} \pmod{26}$$

$$\begin{bmatrix}1 & 24\\ 8 & 19\end{bmatrix}\begin{bmatrix}19\\ 11\end{bmatrix}=\begin{bmatrix}283\\ 361\end{bmatrix}=\begin{bmatrix}23\\ 23\end{bmatrix} \pmod{26}$$

From Table 1, the alphabet equivalents of these vectors are

ST *RI* *KE* *NO* *WW*

Which yields the message STRIKE NOW

Example 8 Decode the Hill 3-cipher **XCVAFA** which was enciphered by the matrix key

$$K = \begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 0 & 1 & 1 \end{bmatrix}$$

Solution:

First we have to calculate the inverse of K

$$\left[\begin{array}{ccc|ccc} 1 & 2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right]$$

.

.

.

Important Note:

EXAMPLE 5 A Number with No Reciprocal mod 26 ◀

The number 4 has no reciprocal modulo 26, because 4 and 26 have 2 as a common prime factor (see Exercise 8).

For future reference, in Table 2 we provide the following reciprocals modulo 26:

Table 2 Reciprocals Modulo 26

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

Work to do

Question 1. Determine whether the matrix is invertible modulo 26. If so, find its inverse modulo 26 and check your work by

$$AA^{-1} = A^{-1}A = I(mod\ 26)$$

a) $A = \begin{bmatrix} 9 & 1 \\ 7 & 2 \end{bmatrix}$ b) $B = \begin{bmatrix} 1 & 8 \\ 1 & 3 \end{bmatrix}$ c) $A = \begin{bmatrix} 2 & 1 \\ 1 & 7 \end{bmatrix}$

Question 2.

Decode the following Hill 2-cipher which was enciphered by the matrix $\begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix}$

SAKNOXAOJX

Question 3.

Decode the Hill 3-cipher **LQVGKE** which was enciphered by the matrix key

$$K = \begin{bmatrix} 1 & 2 & 4 \\ 0 & -1 & 2 \\ 0 & 1 & -1 \end{bmatrix}$$