Application of Matrices in Cryptography

(Note: First go through Multiplication, inverse of matrix with the help of below link https://www.studypug.com/algebra-help/multiplying-a-matrix-by-another-matrix)

https://www.cuemath.com/algebra/inverse-of-a-matrix/

https://byjus.com/maths/inverse-of-3-by-3-matrix/

NOTE:

- Matrices come in all possible rectangular shapes, the following are a number of examples of matrices

$$\begin{pmatrix} 1 & -1 & 0 & 4 \end{pmatrix} \quad \begin{pmatrix} 2 \\ -3 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 12 & -4 \\ 0 & 2 & 27 \end{pmatrix} \quad \begin{pmatrix} 9 & -2 \\ 0 & 3 \\ 3 & 0 \\ -1 & 5 \end{pmatrix}$$

- In general, we denote a matrix by

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \dots & & a_{i,j} & \\ a_{n,1} & a_{n,2} & \dots & a_{n,n} \end{pmatrix}$$

- Each a_{ij} is called an element of the matrix (or an entry of the matrix); this denotes the element in row i and column j. The entries of the matrix are organized in horizontal rows and vertical columns

NOTE:

- The size, or dimension, of the matrix is n x m, where,
  - n is the number of rows of the matrix,
  - m is the number of column of the matrix.

- For example, the following matrices are of dimensions 1x4, 3x1, 2x3, and 4x2 respectively

$$\begin{pmatrix} 1 & -1 & 0 & 4 \end{pmatrix} \quad \begin{pmatrix} 2 \\ -3 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 12 & -4 \\ 0 & 2 & 27 \end{pmatrix} \quad \begin{pmatrix} 9 & -2 \\ 0 & 3 \\ 3 & 0 \\ -1 & 5 \end{pmatrix}$$

- A special kind of matrix is a square matrix,
  - i.e. a matrix with the same number of rows and columns.
  - If a square matrix has n rows and n columns, we say that the matrix has order n.
  - The matrix $\begin{pmatrix} 1 & 2 & 0 \\ 0 & -1 & 3 \\ 2 & 4 & 5 \end{pmatrix}$ is a square matrix of order **3.**

Application of matrices to Cryptography

One of the important applications of inverse of a non-singular square matrix is in cryptography. Cryptography is an art of communication between two people by keeping the information not known to others. It is based upon two factors, namely encryption and decryption. Encryption means the process of transformation of an information (plain form) into an unreadable form (coded form). On the other hand, Decryption means the transformation of the coded message back into original form. Encryption and decryption require a secret technique which is known only to the sender and the receiver.

The key **matrix** is used to encrypt the messages, and its inverse is used to decrypt the encoded messages. It is important that the key **matrix** be kept secret between the message senders and intended recipients. If the key **matrix** or its inverse is discovered, then all intercepted messages can be easily decoded.

This secret is called a **key**. One way of generating a key is by using a non-singular matrix to encrypt a message by the sender. The receiver decodes (decrypts) the message to retrieve the original message by using the inverse of the matrix. The matrix used for encryption is called **encryption matrix** (**encoding matrix**) and that used for decoding is called **decryption matrix (decoding matrix)**.

We explain the process of encryption and decryption by means of an example.

- **Suppose that the sender and receiver consider messages in alphabets $A - Z$ only, both assign the numbers 1-26 to the letters $A - Z$ respectively, and the number 0 to a blank space, Also, we assign the number 27 to space between two words.**

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

EXAMPLE:

Let the encoding matrix be:

PREPARE TO NEGOTIATE

and the encoding matrix be:

$$\begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix}$$

Solution:

We assign a number for each letter of the alphabet.

Such that A is 1, B is 2, and so on. Also, we assign the number 27 to space between two words. Thus the message becomes:

P	*R*	*E*	*P*	*A*	*R*	*E*	*	*T*	*O*	*	*N*	*E*	*G*	*O*	*T*	*I*	*A*	*T*	*E*
16	18	5	16	1	18	5	27	20	15	27	14	5	7	15	20	9	1	20	5

Encoding

- Since we are using a 3 by 3 matrix, we break the enumerated message above into a sequence of 3 by 1 vectors:

$$\begin{bmatrix}16\\18\\5\end{bmatrix}\begin{bmatrix}16\\1\\18\end{bmatrix}\begin{bmatrix}5\\27\\20\end{bmatrix}\begin{bmatrix}15\\27\\14\end{bmatrix}\begin{bmatrix}5\\7\\15\end{bmatrix}\begin{bmatrix}20\\9\\1\end{bmatrix}\begin{bmatrix}20\\5\\27\end{bmatrix}$$

- Note that it was necessary to add a space at the end of the message to complete the last vector.
- We encode the message by multiplying each of the above vectors by the encoding matrix.
- We represent above vectors as columns of a matrix and perform its matrix multiplication with the encoding matrix

$$\begin{bmatrix}-3 & -3 & -4\\0 & 1 & 1\\4 & 3 & 4\end{bmatrix}\begin{bmatrix}16 & 16 & 5 & 15 & 5 & 20 & 20\\18 & 1 & 27 & 27 & 7 & 9 & 5\\5 & 18 & 20 & 14 & 15 & 1 & 27\end{bmatrix}$$

- We get

$$\begin{bmatrix} -122 & -123 & -176 & -182 & -96 & -91 & -183 \\ 23 & 19 & 47 & 41 & 22 & 10 & 32 \\ 138 & 139 & 181 & 197 & 101 & 111 & 203 \end{bmatrix}$$

- The columns of this matrix give the encoded messag
- Encoding is complete

Transmission

The message is transmitted in a linear form

$$-122,\ 23,\ 138,\ -123,\ 19,\ 139,\ -176,\ 47,\ 181,$$
$$-182,\ 41,\ 197,\ -96,\ 22,\ 101,\ -91,\ 10,\ 111,$$
$$-183\ \ 32\ \ 203.$$

Decoding

- To decode the message:
  - The receiver writes this string as a sequence of 3 by 1 column matrices and repeats the technique using the inverse of the encoding matrix.
  - The inverse of this encoding matrix is the decoding matrix.

$$\begin{bmatrix} 1 & 0 & 1 \\ 4 & 4 & 3 \\ -4 & -3 & -3 \end{bmatrix}$$

  - To decode the message, perform the matrix multiplication

$$\begin{bmatrix} 1 & 0 & 1 \\ 4 & 4 & 3 \\ -4 & -3 & -3 \end{bmatrix} \begin{bmatrix} -122 & -123 & -176 & -182 & -96 & -91 & -183 \\ 23 & 19 & 47 & 41 & 22 & 10 & 32 \\ 138 & 139 & 181 & 197 & 101 & 111 & 203 \end{bmatrix}$$

  - Matrix obtained is

$$\begin{bmatrix} 16 & 16 & 5 & 15 & 5 & 20 & 20 \\ 18 & 1 & 27 & 27 & 7 & 9 & 5 \\ 5 & 18 & 20 & 14 & 15 & 1 & 27 \end{bmatrix}$$

Decoded Message

- The columns of this matrix, written in linear form, give the original message

16	18	5	16	1	18	5	27	20	15	27	14	5	7	15	20	9	1	20	5
P	*R*	*E*	*P*	*A*	*R*	*E*	*	*T*	*O*	*	*N*	*E*	*G*	*O*	*T*	*I*	*A*	*T*	*E*

Message received:

PREPARE TO NEGOTIATE

EXAMPLE:
Let the encoding matrix be:

$$A = \begin{bmatrix} 1 & -1 & 1 \\ 2 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

Let the message to be sent by the sender be "**WELCOME**"

SOLUTION:

Step1: Since the key is taken as the operation of post-multiplication by a square matrix of order 3, the message is cut into pieces (WEL), (COM), (E), each of length 3, and converted into a sequence of row matrices of numbers:

[23 5 12],[3 15 13],[5 0 0]

Note that, we have included two zeros in the last row matrix. The reason is to get a row matrix with 5 as the first entry.

Step 2: Next, we encode the message by post-multiplying each row matrix as given below:

Uncoded row matrix	Encoding matrix	Coded row matrix
$[23\ 5\ 12]$	$\begin{bmatrix} 1 & -1 & 1 \\ 2 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$	$= [45\ -28\ 23];$
$[3\ 15\ 13]$	$\begin{bmatrix} 1 & -1 & 1 \\ 2 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$	$= [46\ -18\ 3];$
$[5\ 0\ 0]$	$\begin{bmatrix} 1 & -1 & 1 \\ 2 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$	$= [5\ -5\ 5].$

So the encoded message is [45 − 28 −23] [46 -18 3] [5 −5 5]

Step 3: The receiver will decode the message by the reverse key, post-multiplying by the inverse of A.

So the decoding matrix is

$$A^{-1} = \frac{1}{|A|}\text{adj } A = \begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 2 \\ 1 & -1 & 1 \end{bmatrix}.$$

Step 4:The receiver decodes the coded message as follows:

Coded row matrix	Decoding matrix	Decoded row matrix
$[45 \ -28 \ 23]$	$\begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 2 \\ 1 & -1 & 1 \end{bmatrix}$	$= [23 \ 5 \ 12];$
$[46 \ -18 \ 3]$	$\begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 2 \\ 1 & -1 & 1 \end{bmatrix}$	$= [3 \ 15 \ 13];$
$[5 \ -5 \ 5]$	$\begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 2 \\ 1 & -1 & 1 \end{bmatrix}$	$= [5 \ 0 \ 0].$

So, the sequence of decoded row matrices is [23 5 12] , [3 15 13], [5 0 0].

Thus, the receiver reads the message as “WELCOME”.

TASK:

TASK1: Encrypt the message **COVID,** using the encryption matrix $\begin{bmatrix} 1 & -1 & 1 \\ 2 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$

Hence decode the received message
Using the corresponding matrix.

TASK 2: Use matrix A= $\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}$ to encode the message: ATTACK NOW

We summarize:

TO ENCODE A MESSAGE

1. Divide the letters of the message into groups of two or three.
2. Convert each group into a string of numbers by assigning a number to each letter of the message. Remember to assign letters to blank spaces.
3. Convert each group of numbers into column matrices.
3. Convert these column matrices into a new set of column matrices by multiplying them with a compatible square matrix of your choice that has an inverse. This new set of numbers or matrices represents the coded message.

TO DECODE A MESSAGE

1. Take the string of coded numbers and multiply it by the inverse of the matrix that was used to encode the message.
2. Associate the numbers with their corresponding letters.