Encryption and Decryption using orthogonal matrix

- Cryptography is the practice and study of techniques for secure communication in the presence of adversaries. It involves using mathematical concepts and algorithms to transform information into an unreadable format (**encryption**), ensuring only authorized individuals can access the original content (**decryption**). Encryption and decryption are methods used to protect information by encoding and decoding it. Encryption transforms readable data (plaintext) into an unreadable format (ciphertext) using an algorithm and a key, while decryption reverses this process to recover the original data.
- This process is vital for protecting sensitive data in various applications, including online transactions, secure messaging, and data storage.

Encryption

- **Represent the plain text:**

Convert the message into a numerical representation. For example, you could assign each letter of the alphabet a number (A=0, B=1, ..., Z=25) and spaces with a unique number. Assignment may be custom based. We assign 1 to A, 2 to B,.....26 to Z, 0 or ~~27~~ to space.

- **Form a matrix:**

Arrange the numbers into a matrix ~~or vector form~~ M (rows ~~size~~ should match with orthogonal matrix Q)

- **Choose an orthogonal matrix:**

Select a square orthogonal matrix Q (a matrix whose transpose is also its inverse). This matrix will act as the encryption key.

- **Encrypt:**

Multiply the plain text matrix M by the orthogonal matrix Q. The result is the ciphertext matrix. $C = Q.M$

Decryption

$M = Q^{-1} C$

- **Use the transpose:**

The inverse of an orthogonal matrix is its transpose. Multiply the ciphertext matrix by the transpose of the orthogonal matrix (the encryption key). $M = Q^{T}.C$

- **Form a matrix:**

Arrange the cipher text numbers into a matrix.

- **Recover plaintext:**

The result is the original plaintext matrix. Convert it back to its original form (e.g., letters of the alphabet).

why do we use orthogonal matrices for Encryption and Decryption

- **Easy Inversion:**

An orthogonal matrix's inverse is simply its transpose ($A^{-1} = A^{T}$). This simplifies the decryption process.

- **Preservation of Length and Angles:**

Orthogonal matrices maintain the original length of vectors and the angles between them when used in transformations. This property can be used to ensure that the encrypted data doesn't deviate significantly from the original data

- **Security:**

Orthogonal matrices can be used to create complex transformations that are difficult to reverse without the correct key, enhancing the security of the encryption.

- **Numerical stability**

From a computational standpoint, orthogonal matrices possess exceptional numerical properties. They have a condition number of 1, making them extremely stable for numerical algorithms.

Examples of orthogonal matrix of order 2

$Q = \begin{pmatrix}\cos\theta & -\sin\theta \\ \sin\theta & \cos\theta\end{pmatrix}$	For $\theta = 0$, $Q = \begin{pmatrix}1 & 0 \\ 0 & 1\end{pmatrix}$ For $\theta = 90$, $Q = \begin{pmatrix}0 & -1 \\ 1 & 0\end{pmatrix}$ For $\theta = 45$, $Q = \begin{pmatrix}1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2}\end{pmatrix}$
Identity Matrix	$Q = \begin{pmatrix}1 & 0 \\ 0 & 1\end{pmatrix}$
If $Q = \begin{pmatrix}a & b \\ c & d\end{pmatrix}$ **is orthogonal,** $ad - bc = \pm 1$ **and** $QQ^T = Q^TQ = I$	$Q = \begin{pmatrix}0 & 1 \\ 1 & 0\end{pmatrix}$ $Q = \begin{pmatrix}0 & -1 \\ 1 & 0\end{pmatrix}$ $Q = \begin{pmatrix}0 & 1 \\ -1 & 0\end{pmatrix}$ $Q = \begin{pmatrix}0 & -1 \\ -1 & 0\end{pmatrix}$ $Q = \begin{pmatrix}1 & 0 \\ 0 & 1\end{pmatrix}$ $Q = \begin{pmatrix}1 & 0 \\ 0 & -1\end{pmatrix}$ $Q = \begin{pmatrix}-1 & 0 \\ 0 & 1\end{pmatrix}$ $Q = \begin{pmatrix}-1 & 0 \\ 0 & -1\end{pmatrix}$

Example (short message of length 2)

C = Q M

EX-1. Encrypt and decrypt the message " HI " using the orthogonal matrix $\boxed{Q = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}$

Solution- Encryption (encode the message)

Step-1 Convert the message into a numeric format .

Let us use 1-based system, where

Letter	A	B	....	H	I	...
Value	1	2		8	9	.....

Step-2 Arrange the numbers into a matrix or vector form M (size should match with orthogonal matrix Q) $M = \begin{pmatrix} 8 \\ 9 \end{pmatrix}$

Step-3 Find $C = Q.M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 8 \\ 9 \end{pmatrix} = \begin{pmatrix} 9 \\ 8 \end{pmatrix}$

Step-4 The above message is transmitted into the linear form as 9 8

EX-1. Encrypt and decrypt the message " HI " using the orthogonal matrix $Q = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$c = \begin{pmatrix} 9 \\ 8 \end{pmatrix}$

Solution- Decryption (decode the message)

Step-1 Since $Q = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is orthogonal, $Q^{-1} = Q^T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Step-2 $M = Q^T . C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 9 \\ 8 \end{pmatrix} = \begin{pmatrix} 8 \\ 9 \end{pmatrix}$ (since $C = Q.M$, pre-multiply by $Q^{-1} = Q^T$)

Step-3 The columns of the above matrix are written in linear form as

8 9

Step-4 Convert it back to its original form (letters to alphabet)

Since 8 is assigned to H and 9 to I, the decoded message is "HI".

Exercise (short message of length 2)

Using a suitable orthogonal matrix, Encrypt and decrypt the following messages-

(i) OK, (ii) WE

Exercise (short message of length 2)

Using the orthogonal matrix $Q = \begin{pmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}$, Encrypt and decrypt the following messages- BE, NO, US

Example (long message by splitting into 2-character blocks)

EX-1. Encrypt and decrypt the message “HELLO “ using the orthogonal matrix $Q = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Solution- **Encryption (encode the message)**

Step-1 Convert the message into a numeric format .Let us use 1-based system

Letter	A	B	C	D	E		H	I	...	L	.....	O	.....	Z	space
Value	1	2	3	4	5		8	9	.....	12	......	15	.....	26	0 or 27

Split into 2-character blocks

Block 1: “HE“ → [8, 5] Block 2: “LL“ → [12, 12] Block 1: “O “ → [15, 0]

Step-2 Arrange the numbers into a matrix or vector form M (size should match with orthogonal matrix Q so that multiplication $Q.M$ is possible)

$$\text{M} = \begin{pmatrix} 8 & 12 & 15 \\ 5 & 12 & 0 \end{pmatrix}$$

EX-1. Encrypt and decrypt the message "HELLO " using the orthogonal matrix $\boldsymbol{Q} = \begin{pmatrix} \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} \end{pmatrix}$

Step-3 Find $C = Q.M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 8 & 12 & 15 \\ 5 & 12 & 0 \end{pmatrix} = \begin{pmatrix} 5 & 12 & 0 \\ 8 & 12 & 15 \end{pmatrix}$

Step-4 The above message is transmitted into the linear form as

5 8 12 12 0 15

Solution- **Decryption (decode the message)**

Step-1 Since $Q = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is orthogonal, $Q^{-1} = Q^T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Step-2 $M = Q^T.C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 5 & 12 & 0 \\ 8 & 12 & 15 \end{pmatrix} = \begin{pmatrix} 8 & 12 & 15 \\ 5 & 12 & 0 \end{pmatrix}$

Step-3 The columns of the above matrix are written in linear form as

8 5 12 12 15 0

Step-4 Convert it back to its original form (letters to alphabet)

Since 8 is assigned to H, 5 to E, 12 to L, 15 to O and 0 to space, the decoded message is "HELLO ".

Exercise (long message by splitting into 2-character blocks)

1. Using a suitable orthogonal matrix, Encrypt and decrypt the following messages-

MOVE, GOOD DAY, STUDY, NOW, RUN, BLACK

G O O A
O D D Y

Exercise (long message by splitting into 2-character blocks)

Using the orthogonal matrix $Q = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$, Encrypt and decrypt the following messages-

WE RUN, MUMBAI, WE PLAY, DISCUSS, HAPPY FRIENDSHIP DAY