Task T1

T1: Construct an Example of M1, M2, and M3 for N = 5

1: Define M1 (Permutation Vector)

M1 is a vector of length N that contains a random permutation of numbers from 1 to N.

(a) Example

- M1 = $\begin{bmatrix} 4 & 5 & 1 & 3 & 2 \end{bmatrix}$

2: Define M2 (Permutation Matrix for Encryption)

M2 is an N×N matrix, where each row is a random permutation of numbers from 1 to N.

(a) Example

- M2 = $\begin{bmatrix} 5 & 1 & 3 & 2 & 4 \\ 3 & 1 & 5 & 4 & 2 \\ 3 & 2 & 5 & 1 & 4 \\ 3 & 4 & 2 & 1 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{bmatrix}$

3: Define M3 (Permutation Matrix for Decryption)

M3 is also an N×N matrix, where each **column** is a random permutation of numbers from 1 to N.

Construct M3 such that the decryption property holds: M3(M2(M1(k),p),k) = p

(a) Example

- M3 = $\begin{bmatrix} 4 & 2 & 2 & 4 & 2 \\ 3 & 5 & 4 & 2 & 5 \\ 1 & 1 & 3 & 1 & 1 \\ 2 & 3 & 5 & 5 & 4 \\ 5 & 4 & 1 & 3 & 3 \end{bmatrix}$