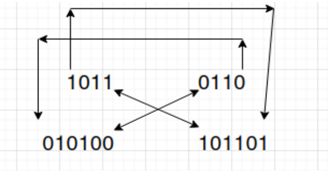
# Assignment 1 (Cyber Security, 2024)

Suppose two parties aim to communicate via a public channel. To ensure secure transmission, they employ a **Modified Data Encryption Standard (M-DES) algorithm.** Let's consider a scenario where a sender intends to transmit the message "Hi" to a recipient. Here's how the Modified DES algorithm would be applied:

Messages are segmented into 16-bit blocks.

1. Perform **initial permutation** (reverse order of data).
2. Divide the 16-bit block into two 8-bit parts: **LPT** and **RPT**.
3. Convert the 16-bit key (4 bits each block) into a 12-bit key by discarding the last bits of each block. (Students can choose a key consisting of 12 random bits), e.g: **101100101011**
4. Execute 4 rounds of the following steps:
   a. Convert the **8-bits RPT** to **12-bits RPT** (expansion permutation). **Check the figure.**
   b. Perform **XOR** operation between **RPT** and the **key**.
   c. Apply **S-Box substitutions** using the specified table (**below table**).
   d. Perform **P-box permutation,** swapping two consecutive bits.
   e. Perform **XOR** operation between RPT and LPT, then **swap** LPT and RPT.

   Repeat steps **4a-4e** for 4 rounds.
5. The **LPT** and **RPT** are joined, and perform **final permutation** (reverse order of data).



**Digital Signature:** Then apply the hash function MD = f(y) = x>>2 to generate a digital signature. The public and private keys are f(y) = x>>3

| | 0000 | 0001 | 0010 | 0011 | 0100 | 0101 | 0110 | 0111 |
|---|---|---|---|---|---|---|---|---|
| 00 | 1010 | 0110 | 1001 | 0011 | 0111 | 1011 | 1000 | 1110 |
| 01 | 0000 | 0001 | 1111 | 1100 | 1101 | 0100 | 0010 | 0101 |
| 10 | 1010 | 0110 | 1001 | 0011 | 0111 | 1011 | 1000 | 1110 |
| 11 | 0000 | 0001 | 1111 | 1100 | 1101 | 0100 | 0010 | 0101 |

| | 1000 | 1001 | 1010 | 1011 | 1100 | 1101 | 1110 | 1111 |
|---|---|---|---|---|---|---|---|---|
| 00 | 1010 | 0110 | 1001 | 0011 | 0111 | 1011 | 1000 | 1110 |
| 01 | 0000 | 0001 | 1111 | 1100 | 1101 | 0100 | 0010 | 0101 |
| 10 | 1010 | 0110 | 1001 | 0011 | 0111 | 1011 | 1000 | 1110 |
| 11 | 0000 | 0001 | 1111 | 1100 | 1101 | 0100 | 0010 | 0101 |