Computer Networking: Security

(CSE 3752)

Experiment 5

Aim:

Implementation of block ciphering process for secured transmission of digital information in computer network.

Objectives:

1. An overview on DES (Data Encryption Standard) algorithm.
2. Execution of DES algorithm for encryption and decryption of digital information.

Exercises:

Using DES find the following for the given 8-bit plaintext 10010111 and 10-bit key 1010000010

1. Find the permuted key using the P10 table given as 3 5 2 7 4 10 1 9 8 6 and the round 1 key (K1) using the P8 table 6 3 7 4 8 5 10 9
2. Find the output of initial permutation as L0 and R0 using the given IP table 2 6 3 1 4 8 5 7
3. Find the output of expansion permutation on R0
4. Find the output of XOR (EP(R0),K1)
5. Find the output of the given S-boxes

$$S0 = \begin{array}{cc} & \begin{array}{cccc}0&1&2&3\end{array} \\ \begin{array}{c}0\\1\\2\\3\end{array} & \begin{bmatrix}1&0&3&2\\3&2&1&0\\0&2&1&3\\3&1&3&2\end{bmatrix}\end{array} \qquad S1 = \begin{array}{cc} & \begin{array}{cccc}0&1&2&3\end{array} \\ \begin{array}{c}0\\1\\2\\3\end{array} & \begin{bmatrix}0&1&2&3\\2&0&1&3\\3&0&1&0\\2&1&0&3\end{bmatrix}\end{array}$$

6. Find the output of the permutation table using the P4 table 2 4 3 1