Computer Networking: Security

(CSE 3752)

Experiment 6

Aim:

Compare symmetric cryptographic process with respect to asymmetric cryptographic process by implementing AES and RSA algorithm.

Objectives:

1. An overview on AES (Advanced Encryption Standard) algorithm.
2. An overview on RSA algorithm.
3. Execution of AES algorithm for encryption and decryption of text message.
4. Execution of RSA algorithm for encryption using public key and decryption using private key.

Exercises:

1. Transform the plaintext "AES USES A MATRIX" into a state matrix form.
2. Compute the output of S-box with given input state matrix as $\begin{bmatrix} 4 & 5 \\ E & 2 \end{bmatrix}$ and S-box as

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

3. Perform ShiftRow transformation on the given current matrix

$$\begin{pmatrix} 63 & EB & 9F & A0 \\ C0 & 2F & 93 & 92 \\ AB & 30 & AF & C7 \\ 20 & CB & 2B & A2 \end{pmatrix}$$

4. Find the output of Mix Column if the input state matrix is $\begin{bmatrix} D & 1 \\ A & F \end{bmatrix}$ with the predefined matrix as $\begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix}$ and the irreducible polynomial for GF(16) is x^4+x+1.

5. Given the following values for the RSA algorithm:

   - Two prime numbers: p=61, q=53
   - Public key: e=17

   Calculate the private key d, where d is the modular inverse of e modulo ϕ(n).