SSN College of Engineering,
Department of Computer Science and Engineering
CS6711 Security Laboratory

Exercise 4:

To implement the Data Encryption Standard (DES) Algorithm.

Programming Language: Java

Hints:

Key Generation

1. Initialize the permutation tables, left shift schedules.
2. Read the 64 bit key.
3. 64 bits goes through a permutation called PC-1(permuted choice) resulting 56 bits.
4. 56 bits are divided into two halves
5. Each half will be rotated left by 1 or 2 bits depending on the round
6. Both sides go through permute choice 2 (PC-2) which selects 24 bits from left and right resulting a 48 bit round key.

Encryption Procedure for DES:

1. Initialize the permutation tables, S boxes, expansion tables, left shift schedules.
2. A block of 64 bits is permuted by an initial permutation called IP.
3. Resulting 64 bits are divided in two halves of 32 bits, left and right.
4. Right half goes through a function F (Feistel function)
5. Left half is XOR-ed with output from F function above.
6. Left and right are swapped(except last round).
7. If last round, apply an inverse permutation IP-1 on both halves and that's the output else, goto step 3.
8. Display the cipher text.

Feistel function F:

1. Expansion – 32 bits to 48 bits based on an expansion table.
2. Key mixing – round key combined with 48 bits from previous step by XOR operation.
3. Substitution – previous result divided into 8x6bits blocks before processed by s-boxes(substitution boxes)
4. Permutation based on a fixed permutation table.

Decryption Procedure for DES:

1. Use the cipher text as input.
2. Apply the same set of operations from step 2 to 7 of encryption procedure.
3. Use the keys K_i in reverse order (use K_{16} on the first iteration, K_{15} on the second until K_1 on last iteration).
4. Display the plain text.