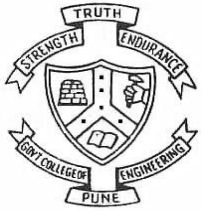
Cryptography and Network Security

Unit-III

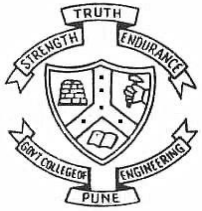
Session 15

Dr. V. K. Pachghare



Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

ENCRYPTION TECHNIQUES



Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

S-DES

Simplified Data Encryption Standard

- S-DES is a simplified version of DES, developed for beginners to learn the basic concept of DES
- It is only for educational purposes and not suitable for practical purposes due to security issues

- Plaintext block size: 8 bits
- key size: 10 bits
- Number of rounds: 2

Subkey Generation

Initial Permutation Table

3	5	2	7	4	10	1	9	8	6

1. The permutated key is divided into two halves, left half and right half
2. Left circular shift by 1 bit on each half.
3. Left half and right half are merged together
4. Apply compression permutation [8 bits]

6	3	7	4	8	5	10	9

5. This is first subkey

1. Take output of step 3 as input
2. Left circular shift by 2 bit on each half
3. Left half and right half are merged together
4. Apply compression permutation [8 bits]

6	3	7	4	8	5	10	9

5. This is second subkey

Encryption

Step 1 Block size of plaintext is of 8 bits in S-DES.

Step 2 Initial permutation is applied on the block of 8 bits plaintext

2	6	3	1	4	8	5	7

Round 1

Step 1 Divide the permuted bits into 2 halves

Step 2 The right half is permuted using Expansion Permutation (E/P), which gives 8 bits as output

4	1	2	3	2	3	4	1

Step 3 These 8 bits are XORed with the first key (K_1)

Step 4 Apply S-box substitution on output of step 3. There are 2 S-boxes, S_0 and S_1. Each S-box takes input as 4 bits and produces output as 2 bits.

S_0				
R/C	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

S_1				
R/C	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

Step 5 apply permutation on output of step 4

Permutation table

2	4	3	1

Step 6 Output of step 5 is XORed with Left half of the initial permutation step

Step 7 Swapping. Right half as left half and left half as right half

Repeat steps 1 to 7 for round 2

Inverse Initial Permutation

Inverse IP table

4	1	3	5	7	2	8	6

Lab Assignment 4

Implement Simplified DES algorithm for encryption and decryption of any message.

Count the time required for encryption/decryption of messages of different length.

Note: You have to use assignments 3 for various operations in S-DES

Last date for submission: 25 Sept 2020