Introduction to Information Security

Assignment 1

Total Marks: 80

Hard deadline: February 1, 2023 (Wednesday), 5:00 PM (in Class Room)

1. If the DES encryption key with parity bits (64 bits) in hexadecimal is 0123 AECF 2562 2897, find the fifth and tenth round keys $(K_5$ and $K_{10})$.

   [10 + 10 = 20]

2. Show the results of the hexadecimal data (48 bits) CBAD CBBC CDEF after passing it through the S-boxes in DES to produce 32 bits output.

   [15]

3. We know if the 16 round keys are $K_1, K_2, K_3, \ldots, K_{16}$, then the DES decryption algorithm is same as the DES encryption algorithm provided that the round keys are supplied in reverse order. Suppose we want to design a seperate DES decryption algorithm with the initial encryption/decryption key K of 56 bits. Design a sub-key generation algorithm which will produce all 16 round keys for DES decryption function. Prove the correctness of your sub-key generation algorithm.

   [10+10 = 20]

4. Fill in the remainder of Table 1 for different modes of DES, where P_j and C_j denote the j^{th} plaintext and ciphertext blocks, respectively, and K is the shared key.

   [10]

Table 1: DES modes of operation

Mode	Encryption	Decryption
ECB	$C_j = E_K[P_j], j = 1, 2, \ldots, N$	$P_j = D_K[C_j], j = 1, 2, \ldots, N$
CBC		
CFB		
OFB		
CTR		

5. A *linear cipher* is defined as follows. Using the encoding technique $A = 0$, $B = 1$, $C = 2$, . . ., $Z = 25$ and the blank space as 26, the encryption algorithm works as

$$C \equiv aP + b \pmod{27},$$

where P is the encoded plaintext letter and C the corresponding encrypted ciphertext letter, where a and b are integers with $\gcd(a, 27) = 1$.

(a) Design the corresponding decryption algorithm for this linear cipher.

(b) Using the linear cipher $C \equiv 5P + 11 \pmod{27}$, encrypt the plaintext message IT IS EASY.

(c) Decrypt the ciphertext message TZSVIW, which was produced using the linear cipher $C \equiv 4P + 7 \pmod{27}$. [5 + 5 + 5 = 15]

Submission Instructions

Copying in assignments leads to award ZERO marks in assignment marks. Also, the source from which you have copied, that source student will be treated under the same rule.

Please submit the assignment in hard copy stating the following at the top:

Introduction to Information Security

Assignment Set 1

submitted by

Name: XYZ, Roll No: abc