Indian Institute of Engineering Science and Technology, Shibpur

B. Tech. (CST) 6th Semester Mid-Semester Examination, 2022

Information Security and Cryptography (CS 3204)

Time: 45 Minutes **Full Marks: 30**

1. Answer the following questions briefly:
   (a) What is masquerade? Which principle of security is breached because of that?
   (b) How fabrication attack can be prevented?
   (c) What is packet spoofing?

   [2 x 3]

2. (a) What do you mean by algorithm mode?
   (b) What is the problem of Electronic Code Book (ECB) mode?
   (c) How Cipher Block Chaining (CBC) mode solves this problem?

   [1 + 2 + 3]

3. (a) Consider that the 10-bit initial key in Simplified Data Encryption Standard (S-DES) is (1010000010). Find out the corresponding two 8-bit keys where the P10 and P8 boxes are as follows:

P10									
3	5	2	7	4	10	1	9	8	6

P8							
6	3	7	4	8	5	10	9

   (b) Explain the mechanism of S-box substitution in a round of Data Encryption Standard (DES).
   (c) Why S-box substitution is so important in DES?

   [3 + 2 + 1]

4. Considering $(10101)_2$ as the plain text in Merkle-Hellman hard Knapsack Cryptosystem, show the steps of both encryption and decryption. Assume a private key correctly and find out the corresponding public key for the above encryption and decryption.

   [6]

5. (a) Why AES is popular than DES?
   (b) What is the role of L-Table and E-table in AES?
   (c) Briefly explain the method of key expansion in AES?

   [1 + 2 + 3]