2/8/2023

Indian Institute of Engineering Science and Technology, Shibpur

B. Tech. (CST) 6th Semester Mid-Semester Examination, 2023

Information Security and Cryptography (CS 3204)

Time: 2 Hours

Full Marks: 30

1. Answer the following questions briefly:

   (a) What is fabrication attack? Which principle of security is breached because of that?

   (b) Is there any drawback of Vigenere cipher?

   (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) Prove the correctness of Diffie-Hellman Key-exchange algorithm mathematically.

   (b) Alice & Bob want to establish a secret key using Diffie-Hellman Key-exchange algorithm assuming the following values:

   n = 11 (divisor), g = 5 (power), x = 2 (chosen by Alice), y = 3 (chosen by BoB);

   Find the value of the secret keys (k1 & K2) calculated by them.

   (c) Suppose, there are *n* number of persons who want to communicate with each other securely over insecure channels. Do you prefer symmetric / asymmetric key algorithm for very very large value of *n*? Give reason in support of your answer.

[2 + 2 + 2]

4. (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]

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?

[2 + 1 + 3]