Dipmay Biswas (2021CSB043)

**Indian Institute of Engineering Science and Technology, Shibpur**

B. Tech. (CST) 6th Semester Mid-Semester Examination, February 2024

## Information Security and Cryptography (CS 3204)

**Time: 2 Hours** **Full Marks: 30**

**[ Answer all the following questions. ]**

1. (a) Explain different phases of security life-cycle.
   (b) Explain different principles of security mentioning the names of different attacks that try to break these principles.

[ 4 + 6 ]

2. (a) Explain the working principle of Vigenere cipher with an example.
   Is there any drawback of Vigenere cipher?
   (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) What is the problem of Electronic Code Book (ECB) mode?
   How Cipher Block Chaining (CBC) mode solves this problem?

[ ( 2 + 1 ) + 3 + ( 2 + 2 ) ]

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) What is the role of L-Table and E-table in Advanced Encryption Standard (AES)?
   (d) Briefly explain the method of key expansion in AES.

[ 3 + 2 + 2 + 3 ]