VIT
Vellore Institute of Technology

Continuous Assessment Test – II

Programme Name & Branch: B. Tech CSE

Course Name & Code: Cyber Security & CSE4003

Class Number: All **Slot: A2 + TA2** **Fall Semester 2019-20**

Faculty Name: All **Exam Duration: 90 mins** **Max Marks: 50**

Section – A (5 x 10= 50 Marks)*

S.No Question

1. a. In a public-key system using RSA, you intercept the ciphertext C = 20 sent to a user whose public key is e = 13, n = 77. What is the plaintext M? (5)

   b. In an RSA system, the public key of a given user is e = 65, n = 2881. What is the private key of this user? (5)

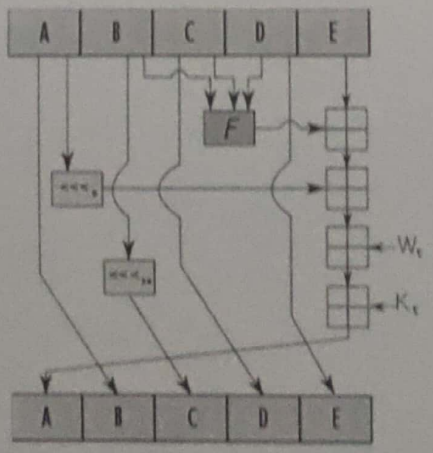
2. a. Demonstrate the DH key exchange methodology using following key values: p =11, g = 2, X_A = 9, X_B = 4. (6)

   b. Diffie–Hellman key agreement is not limited to negotiating a key shared by only two participants. Any number of users can take part in an agreement by performing iterations of the agreement protocol and exchanging intermediate. Write the steps and formulas to be followed for DH key exchange between Alice, Bob, and Carol. (4)

3. a. Let E be the elliptic curve $y^2 = x^3 + x + 6$ over Z_{11} and a point L(2,7) lies on this elliptic curve. Find 2L and 3L. (8)

   b. Find all the points lies in the elliptic curve $y^2 = x^3 + 2x + 3$ (mod 5) (2)

4. Let message = "2fd4e1c67a2d28fced849ee1bb76e7391b93eb12", h0 = 0x67452301, h1 = 0xEFCDAB89, h2 = 0x98BADCFE, h3 = 0x10325476, h4 = 0xC3D2E1F0SHA1. Compute F(B,C,D) in the round0 of the following SHA1.



5. Demonstrate the ElGamal cryptosystem where p = 23, g = 11, x = 6, k = 3 and M = 10.

****