Total No. of Questions : 8] *[Total No. of Printed Pages : 1*

Roll No ....

MCIT-201

M.E./M.Tech., II Semester Examination, June 2020

Information Security System

Time : Three Hours

Maximum Marks : 70

Note: i) Attempt any five questions.

ii) All questions carry equal marks.

1. a) Why modular arithmetic has been used in cryptography?

   b) With a neat block diagram, explain the cryptography security model and the important parameters associated with it.

2. a) Draw the general structure of DES and describe how encryption and decryption are carried out and identify the strength of DES algorithm.

   b) State the Chinese Remainder Theorem and find X for the given set of congruent equations.

   X=2 mod 3, X=3 mod 5 and X=2 mod 7

3. Describe RSA algorithm and estimate the encryption and decryption values for the RSA algorithm parameters.

4. a) How key can be distributed in cryptography? What are the issues?

   b) Explain MD5 algorithm.

5. a) User A and B exchange the key using Diffie-Hellman algorithm. Assume $\alpha = 5$,q = 11, $X_A = 2$, $X_B = 3$. Find Y_A, Y_B and K.

   b) Discuss the discrete logarithm and explain Diffie-Hellman key exchange with its merits and demerits.

6. Explain Elliptic and Hyper-elliptic curve cryptography in detail.

7. a) What is zero knowledge protocol? Describe in detail.

   b) Discuss Hash functions. Where Hash functions are used?

8. Write short notes on:(Any three)

   i) PKI ii) MQV algorithm

   iii) SHA-1 iv) AES

******