Printed Pages: 3 | 150 | EIT-701

(Following Paper ID and Roll No. to be filled in your Answer Book)

Paper ID : 113702 Roll No. | | | | | | | | | | |

B.Tech.

(SEM. VII) THEORY EXAMINATION, 2015-16

CRYPTOGRAPHY & NETWORK SECURITY

[Time:3 hours] [MaximumMarks:100]

SECTION-A

Note : Attempt all parts. All parts carry equal marks. Write answer of each part in short. (2×10=20)

1. (a) Specify two differences between procedural and object oriented language.

   (b) What is a stream cipher?

   (c) What is an authenticated Diffie-Hellman key agreement?

   (d) Distinguish between an active and passive attack.

   (e) What are Message Authentication Codes (MACs)?

   (f) What requirements should a digital signature scheme satisfy?

(g) What type of security goals are used in cryptography?

(h) Define S/MINE.

(i) What are the requirements for the use of a public key certificates scheme?

(j) Explain briefly the two different approaches of Digital Signature?

SECTION-B

Note: Attempt any five questions from this section. (10×5=50)

2. What are the properties of modular arithmetic operation? What are the requirements of Message Authentication Code (MAC)? List and explain them.

3. Encrypt the message "THIS IS AN EXERCISE" using Playfair Cipher with Key=DOLLARS.

4. What is Kerberos? Discuss Kerberos version 4 in detail?

5. Define the Chinese remainder theorem? Find the values of x for the following sets of congruence using the Chinese remainder theorem.

   X=2 mod 7 and X=3 mod 9

6. What are the securities of RSA? Perform encryption and decryption using RSA algorithm for

   p=17, q=11, e=7, m=88.

7. What is the principle of public-key cryptosystems. Discuss the applications for public-key cryptosystems.

8. What are the properties of modular arithmetic operation?

9. Define group field and finite field of the form GF(p).

SECTION-C

Note: Attempt any two questions from this section.

(15×2=30)

10. Find the values of x for the following sets of Congruence using the Chinese remainder theorem.

    X=2 (mod 3)

    X=1 (mod 4)

    X=3 (mod 5)

11. Explain RSA algorithm. Perform encryption and decryption using RSA algorithm for p=11, q=13, e=7, m=9.

12. Draw block diagram of DES encryption. Also discuss the strengths of DES.

—x—