Code: 15A05702 **R15**

B.Tech IV Year I Semester (R15) Regular & Supplementary Examinations November/December 2019

INFORMATION SECURITY

(Computer Science and Engineering)

Time: 3 hours Max. Marks: 70

PART – A

(Compulsory Question)

*****

1 Answer the following: (10 X 02 = 20 Marks)

(a) What is the difference between passive and active security threats?
(b) Name any two dimensions on which cryptographic systems are characterized.
(c) Give a brief note on integer division.
(d) Define congruence and compare with equality.
(e) What characteristics are needed in a secure hash function?
(f) What basic arithmetical and logical functions are used in SHA?
(g) List ways in which secret keys can be distributed to two communicating parties.
(h) What are the essential ingredients of a public-key directory?
(i) What protocols comprise SSL?
(j) For what applications is SSH useful?

PART – B

(Answer all five units, 5 X 10 = 50 Marks)

UNIT – I

2 Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system and in each case, indicate the degree of importance of the requirement.

OR

3 (a) What is the OSI security architecture? Explain
(b) List and briefly define categories of security mechanisms.

UNIT – II

4 Demonstrate whether each of these statements is true or false for polynomials over a field:
(i) The product of monic polynomials is monic.
(ii) The product of polynomials of degrees m and n has degree m+n.
(iii) The sum of polynomials of degrees m and n has degree max[m, n].

OR

5 (a) What requirements must a public key cryptosystems fulfill to be a secure algorithm?
(b) In a public-key system using RSA, you intercept the cipher text C = 10 sent to a user whose public key is e = 5, n = 35.What is the plaintext M?

UNIT – III

6 (a) Explain about Cipher Block Chaining
(b) State the value of the length field in SHA-512 if the length of the message is:
(i) 1919 bits. (ii) 1920 bits. (iii) 1921 bits.

OR

7 (a) Explain about block ciphers and list the requirements for message authentication codes.
(b) What happens if a value used in creating a DSA signature is compromised? Explain.

Contd. in page 2

UNIT – IV

8 (a) Explain the Symmetric Key Distribution Using Symmetric Encryption.
(b) Explain about Email Security.

OR

9 (a) How Kerberos V5 addressed the deficiencies of Kerberos V4? Explain.
(b) In Kerberos, what does the Ticket contain that allows Alice and Bob to talk securely?

UNIT – V

10 (a) List and briefly define the SSH protocols.
(b) List and briefly explain four techniques used by firewalls to control access and enforce a security policy.

OR

11 (a) In SSL and TLS, why is there a separate Change Cipher Spec Protocol rather than including a change_cipher_spec message in the Handshake Protocol?
(b) Explain about Buffer overflow with an example.

*****