Printed Pages:2 | Sub Code: NIT701

Paper Id: 113711 | Roll No.

B. TECH

(SEM VII) THEORY EXAMINATION 2018-19

CRYPTOGRAPHY AND NETWORK SECURITY

Time: 3 Hours *Total Marks: 100*

Note: 1. Attempt all Sections. If require any missing data; then choose suitably.

SECTION A

1. Attempt *all* questions in brief. **2 x 10 = 20**

a. Define block cipher
b. What do you mean by cryptography?
c. Define hash algorithm.
d. What is stream cipher?
e. Differentiate between public key and private key.
f. Explain intrusion detection in brief.
g. What do you mean by mail security?
h. What is DSS in cryptography?
i. What do you mean by email security?
j. Describe birthday attack.

SECTION B

2. Attempt any *three* of the following: **10 x 3 = 30**

a. Draw the block diagram of DES algorithm. Also explain its functionality.
b. What is prime and relative prime numbers in cryptography and network security
c. Discuss the Message Authentication Codes. Also give the use of Authentication requirements in MAC.
d. What is Diffie-Hellman Key Exchange in key management?
e. Explain internet protocol security in detail.

SECTION C

3. Attempt any *one* part of the following: **10 x 1 = 10**

(a) List the Strength of DES in brief. Also explain the Triple DES.
(b) What is the Shannon's theory of confusion and diffusion in terms of information security?

4. Attempt any *one* part of the following: **10 x 1 = 10**

(a) States the Advanced Encryption Standard (AES). Also provide the functioning of AES.
(b) Explain the Chinese Remainder theorem with example. How Chinese Remainder theorem provide the security to online information sharing transactions.

5. Attempt any *one* part of the following: **10 x 1 = 10**

(a) What do you understand from hash functions? Discuss the working of Secure hash algorithm (SHA) in Message Authentication
(b) Explain the Digital Signatures. Also give a detail description of Elgamal Digital Signature Techniques.

6. **Attempt any *one* part of the following:** **10 x 1 = 10**

(a) Discuss X.509 Certificates in detail. What is the role X.509 Certificates in cryptography?

(b) What is Electronic mail security? Provide the application of pretty good privacy (PGP) in transaction Authentication

7. **Attempt any *one* part of the following:** **10 x 1 = 10**

(a) Explain Secure electronic transaction (SET) in internet protocol security in detail.

(b) What do mean by system security? Also discuss Viruses and related threats to system security.