Printed Page 1 of 1 **Sub Code:NIT701**

Paper Id: 113711 **Roll No:** □□□□□□□□□□□□□

B. TECH.
(SEM VII) THEORY EXAMINATION 2019-20
CRYPTOGRAPHY & NETWORK SECURITY

Time: 3 Hours ***Total Marks: 100***

Note: 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 cipher text with the help of an example.

b. Categorize Passive and Active attack.

c. State Fermat's theorem.

d. Write any two applications of RSA algorithm.

e. What type of security goals are used in cryptography?

f. Explain briefly two approaches of Digital Signature.

g. List any two applications of X.509 Certificates.

h. Write a simple Authentication dialogue used in Kerberos.

i. Define S/MINE.

j. What are the protocols used to provide IP security?

SECTION B

2. Attempt any *three* of the following: 10x3=30

a. Draw the block diagram of DES encryption.Also Explain strength of DES in brief.

b. What are the securities of RSA? Perform encryption and decryption using RSA algorithm for $p=17, q=11, e=7, m=88$

c. Explain SHA-512 algorithm with a neat diagram.

d. Give the structure of PGP message generation. Explain with a diagram.

e. Write short notes on any two of the following:
(i) Secure Socket Layer, (ii) Modes of IP Sec, (iii) Intrusion Detection.

SECTION C

3. Attempt any *one* part of the following: 10x1=10

a. Differentiate between following:
(i) Block cipher and Stream Cipher
(ii) Steganography and Cryptography
(iii) Authentication and Authorization

b. Explain Shannon's theory of confusion and diffusion in terms of information security.

4. Attempt any *one* part of the following: 10x1=10

a. Illustrate the concept of Chinese remainder theorem. By using Chinese Remainder Theorem solve the simultaneous congruence $X \equiv 2 \bmod P$ for all $P \in \{3,5,7\}$

b. What is the application of public key cryptosystems? Discuss the applications for public key cryptosystems.

5. Attempt any *one* part of the following: 10x1=10

a. Describe signing and verification in Digital Signature Algorithm.

b. What are the requirements of a Message Authentication code (MAC)? Discuss the logical structure, components and algorithmic steps of MD5 algorithm.

6. Attempt any *one* part of the following: 10x1=10

a. Explain Diffie-Helman key exchange technique with an example.

b. What is Kerberos? Discuss the principle differences between version 4 and version 5 of Kerberos.

7. Attempt any *one* part of the following: 10x1=10

a. List the participants in SET (Secure Electronic Transaction) system? Describe in brief the sequence of events that are required for a transaction.

b. What are different types of firewall? Also discuss viruses and related threats to system security

www.aktuonline.com

http://www.aktuonline.com