Printed Page 1 of 1 **Sub Code: RIT701**

Paper Id: 113721 **Roll No:**

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

Time: 3 Hours ***Total Marks: 70***

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

SECTION A

1. Attempt *all* questions in brief. **2 x 7 = 14**

a. Explain Active and Passive attack.
b. State Fermat's Theorem.
c. Specify the benefits of IPSec.
d. Determine the GCD (24561,17892) using Euclid's Algorithm.
e. Why is trap door one way function used?
f. Explain role of compression function in hash function.
g. What are the services provided by the PGP ?

SECTION B

2. Attempt any *three* of the following: **7 x 3 = 21**

a. Perform Encryption and Decryption using Hill cipher for the following. Message PEN and key :ACTIVATED.
b. Explain MD5 processing of a single 512 bit block.
c. Analyze various types of virus and its counter measures.
d. Explain Triple DES and its applications.
e. State and prove the Chinese remainder theorem. What are the last two digit of 49^{19} ?

SECTION C

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

(a) Explain Elliptic curve cryptography with an example.
(b) Find the secret key shared between use A and user B using Diffie Hellman algorithm for the following.
q=353, α(primitive root)=3, X_A=45 and X_B=50.

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

(a) Explain SHA2 in detail with diagram.
(b) Explain the concept of Digital signature algorithm with key generation and verification in detail.

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

(a) Explain secure electronic transaction (SET) protocol with their components.
(b) Explain IDS in detail with suitable example.

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

(a) Explain in detail about S/MIME.
(b) Explain briefly about the architecture and certification mechanism in Kerberos.

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

(a) Explain public key infrastructure in detail.
(b) Discuss authentication header and ESP in detail with their packet format.