Printed Pages:2 **Sub Code: EIT -701**

Paper Id: **113717** **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 cryptography.
b. What is polyalphabetic cipher?
c. What do you understand by chosen plaintext attack?
d. What is Hill cipher?
e. Give general format of a PGP message.
f. Explain malware in brief.
g. What is DSS in cryptography?
h. What do you mean by internet protocol?
i. Describe the encryption in cryptography. .
j. What do you mean by network security?

SECTION B

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

a. Define group. Give an example of group which is not a field.
b. What do you understand by chosen plaintext attack? Hill cipher is vulnerable to chosen plaintext attack?
c. What is permutation cipher? Whether permutation ciphers are susceptible to the statistical analysis or not?
d. State Chinese Remainder theorem. Use it to solve the following simultaneous congruence $x\equiv4 \bmod 7, x\equiv4 \bmod 13, x\equiv5 \bmod 12$
e. Describe RSA algorithm. Whether RSA encryption and decryption works or not if message m has common factor with modulus n of the scheme..

SECTION C

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

(a) Draw block diagram of DES cipher showing size of input/output of every block. How important is swapping step at the end of every round?
(b) State and prove Euler's theorem. Compute the value of Euler's totient function for 300.

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

(a) What is S/MIME? Why is it used? What are the main functions S/MIME provides?

(b) Write the signature generation and verification process of digital signature algorithm of Digital signature standard.

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) What is Kerberos? What requirements were defined for Kerberos? Describe the sequence of message exchanges of Kerberos Version 4.

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

(a) Discuss at least one approach that can be used to launch a birthday attack on message authentication code.

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

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

(a) Describe the approaches used for intrusion detection. How you can control this activity?

(b) Explain the concept of dual signature in context of secure Electronic Transaction (SET) . Briefly describe the sequence of events that are required for a SET transaction.