Printed pages: 02 **Sub Code: EIT701**

Paper Id: | 1 | 0 | 6 | 1 | **Roll No.** | | | | | | | | | | |

B.Tech.
(SEM VII) THEORY EXAMINATION 2017-18
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 x10 = 20

a. What are security mechanisms?
b. Find gcd (1970, 1066) using Euclid algorithm?
c. Define the steganography?
d. What is logic bomb?
e. Convert given text “UTTAR PRADESH” into cipher to using rail fence technique.
f. What are active and passive attacks in OSI security architecture?
g. What are birthday attacks?
h. What are two methods of testing prime number?
i. Define one way property in hash function.
j. What do you mean by WEB security?

SECTION B

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

a. Explain Chinese remainder theorem. Use it to solve $X \equiv 2 \text{ mod}3, X \equiv 3 \text{ mod}5, X \equiv 2 \text{ mod}7$?
b. Differentiate MAC and Harsh function. Assume the client C wants to communicate to server S using Kerberos procedure how can it be achieved?
c. Explain DES with Suitable diagram?
d. Differentiate b/w block cipher and stream cipher? What are different modes of block cipher operations? Explain any one of them.
e. Describe RSA algorithm? Encryption and decryption function? Find cipher text message while two primes are P=11,q=5,e=3and PT=9

SECTION C

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

(a) What is digital certificate? Give the format of X. 500 certificate showing important element of the certificate?
(b) What are the properties of hash functions? Briefly explain SHA-512.

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

(a) Write short a note on SSL.

(b) Describe diffie-hellman key exchange algorithm. The two entities A and B use the Diffie-Hellman primitive root $\alpha = 13$.
I. If user A private key 5 what is A’s public key?
II. If user B private key 12 what is B’s public.
III. What is shared key?

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

(a) Explain the concept of security association (SA) in IPSec what is the use of ISAKMP protocol.

(b) What are types of firewall? Explain them?

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

(a) Explain pretty good privacy in detail?

(b) Explain definition, phases, and types of virus. Structures of viruses?

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

(a) Explain digital signature standards with necessary diagram?

(b) Explain following

I. State fermat's theorem

II. Find 3^{21}mod 11 using fermat's theorem

III. State euler's theorem to find gcd with example?