Printed Pages : 2 **Roll No.** | | | | | | | | | | | **EEE024**

B.TECH.
THEORY EXAMINATION (SEM–VI) 2016-17
CRYPTOGRAPHY & NETWORK SECURITY

Time : 3 Hours ***Max. Marks : 100***

Note : *Be precise in your answer. In case of numerical problem assume data wherever not provided.*

SECTION-A

1 Explain the following : **(10×2=20)**

a) Compare and contrast between symmetric and asymmetric cryptography?

b) Discuss any two problems with one-time pad?

c) The hill cipher uses the following key for enciphering the message $K_{11} = 3$, $K_{12} = 2$, $K_{21} = 5$, $K_{22} = 7$,obtain the decryption key used for deciphering ?

d) Some block cipher modes of operation use only encryption while others uses both. Why?

e) Using Row Transposition technique &, given key as "2 5 4 1 3" generate the Cipher Text for the following plain text "a convenient way to express the transposition''.

f) Find at least two primitive roots of 19?

g) List the ways in which secret keys can be distributed to two communicating partners?

h) What is an authenticated Diffie–Hellman key agreement?

i) What requirements should digital signature scheme satisfy ?

j) Explain why PGP generates a signature before applying compression?

SECTION-B

2 Attempt any five of the following : **(10×5=50)**

(a) i)Briefly explain the design principle of Fiestel Cipher structure? Explain with example

(ii) Prove that in DES cipher, if plaintext block and encryption key is complemented bit wise then resulting cipher text block is the bitwise complement of the original cipher text block ?

(b) State and prove Euler's theorem. Compute the value of Euler's totient function for 300

(c) Define Chinese Remainder Theorem ? Find the value of x for the following set of congruence using Chinese Remainder theorem :

$X \equiv 2 \bmod 3$, $X \equiv 1 \bmod 4$, $X \equiv 3 \bmod 5$

(d) Differentiate MAC and Hash function. Assume client C wants to communicate server S using Kerberos procedure. How can it be achieved?

(e) Compare and contrast a conventional ink based signature and a digital signature. Describe the Elgamal scheme of digital signature generation and verification. Why do signatures of the same message, signed on different occasions differ?

(f) What is the key algorithms used in S/MIME? What are the headers fields define in MME?

(g) Why do we use X.509 authentication over PKC based authentication. Also explain the format ofX.509 and how is an X.509 certificate revoked?

(h) Who are the participants in SET (Secure Electronic Transaction System)? Describe in brief the sequence of events that are required for transaction ? Also Explain the dual concept of dual signature of SET?

SECTION-C

Attempt any two of the following : **(15×2=30)**

3 Describe how Diffie-Hellman algorithm used for keyexchangeis vulnerable to man in the middle attack ?Determine the shared secret key in a Diffie Hellman scheme with a common

prime **71** and primitive root **7**, Given the private keys of the comrnunicating parties A and B are **5 and 12** respectively.

4 i) Explain the significance of Firewall ? Discuss thedifferent types of possible configuration in firewall.

ii) Describe the term " Intrusion Detection" ? Briefly explain the different types of detection mechanism with example ?

5 Write short note on the following :-

i) Linear and Differential Cryptanalysis.

ii) IP Security (IPSec)

iii) Viruses and Related Threats