B. E. Eighth Semester PTDP (Computer Technology) Examination

Course Code : CT 415 / CT 811 **Course Name : Network Security**

Time : 3 Hours] [Max. Marks : 60

Instructions to Candidates :—

(1) All questions are compulsory.
(2) All questions carry marks as indicated.
(3) Assume suitable data wherever necessary.
(4) Illustrate your answers wherever necessary with the help of neat sketches.

1. (a) Differentiate between cryptography and steganography. Also discuss any two steganographic techniques. 5

OR

Encrypt the message "start up India" Using Hill cipher with the key

9 4

5 7.

Show your calculations.

Show the calculations to perform decryption to recover original result. 5

(b) Solve the following :—

(i) Find number of primitive roots in $<Z_{10}$ *, x>

(ii) 15^{18} mod 17 [using Fermat's Little theorem]

(iii) 27^{-1} mod 41 [using Fermat's Little theorem]

(iv) 16^{-1} mod 323 [using Euler's theorem]

(v) $\phi(100)$ [using Eulars phi function] 5

OR

(b) Write Fermat's Little theorem for exponentials and inverse. Solve 3^{12} mod 11 using Fermat's Little theorem. 5

2. (a) Explain CAST algorithm in detail. 5

OR

In the Diffie – Hellman protocol, what happens if x and y have the same value, that is Alice and Bob have accidentally chosen same number ? Are R1 and R2 are same ? Do the session keys calculated by Alice and Bob have same value ? Use an example to prove your claim. 5

(b) Explain properties of cryptographic hash functions with neat diagram. 5

OR

Sign and Verify message M = 25 using RSA digital signature scheme, If p = 3, q = 11 and d = 3. 5

3. Solve any **Five** :—

(a) Determine the cipher text using autokey cipher technique for the message "NMC election" key is 21.

(b) What is Rotor machine ?

(c) Find multiplicative inverse of 17^{-1} mod 3780 using extended Euclidean algorithm.

(d) Can we say that $\phi(49) = \phi(7) \times \phi(7)$? Find your answer.

(e) Briefly describe Sub Byte transformation in AES.

(f) Compare digital signature with conventional signature.

(g) In the SHA – 1 algorithm what is the number of padding bits required if the length of the original message is 2590 bits. 10

4. Solve any **Two** :—

(a) Differentiate between X·509 and PGP certificate format.

(b) Explain the concept of Cryptographic Message Syntax (CMS) in S/MIME.

(c) Draw and explain the diagram of Outbound processing of security policy database in IPsec protocol. 10

5. Solve any **Two** :—

(a) Discuss detection methodologies of IDPS technology.

(b) Explain in brief following malicious programs :

(i) Worms.

(ii) Logic Bombs.

(iii) Spyware.

(iv) Trojans.

(v) Viruses.

(c) Explain SET components with neat diagram. 10

6. Solve any **Five** :—

(a) What is key legitimacy in PGP ?

(b) Give any one real time application where SSL in used.

(c) Differentiate between virus and worms.

(d) What is trusted system ?

(e) Define the term false positive and False negative with respect to IDPS.

(f) Enlist different PGP messages.

(g) What is cipher suite ? 10