B. E. Seventh Semester (Computer Technology) / SoE – 2014-15 Examination

Course Code : CT 1415 / CT 415 **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) Due credit will be given to neatness and adequate dimensions.

(4) Assume suitable data wherever necessary.

(5) Diagrams and chemical equations should be given wherever necessary.

(6) Illustrate your answers wherever necessary with the help of neat sketches.

(7) Use of Logarithmic tables, non-programmable calculator, Steam tables, Mollier's chart, Drawing instruments, Thermodynamic tables for moist air, Psychrometric charts and Refrigeration charts is permitted.

1. (A) (A1) Explain different cryptanalysis attack with schematic representation. 5 (CO 1)

(A2) Find the Multiplicative inverse of 11 in Z26. 3 (CO 2)

(A3) Determine result of the following operation :

(a) -78 mod 13 (b) 0 mod 15. 2 (CO 2)

OR

(B) (B1) Prove that G = {0, 1, 2, 3, 4} is an abelian group with respect to addition modulo 5. 5 (CO 2)

(B2) Discuss Security Goals. 3 (CO 1)

(B3) (i) Find gcd of (88, 220) using Euclidean algorithm. 2 (CO 2)

2. (A1) Why modern block ciphers are designed as substation cipher instead of transposition cipher ? Describe in detail. 2 (CO 2)

(A2) Compare Substitution and Transposition techniques. 3 (CO 2)

(A3) Discuss Keyed Transposition Cipher with suitable example. 5 (CO 2)

OR

(B1) Determine ciphertext for the Plaintext "play" using Hill Cipher, if the key for encryption is "GYBNQKURP". Also recover the original message. 3 (CO 3)

(B2) Define Caesar Cipher. 2 (CO 3)

(B3) Use hill Cipher to decrypt the message ‘POH’ given key matrix is

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$

5 (CO 3)

3. (A1) Compare round keys in DES and AES. In which cipher the size of round key is same as the size of the block. 2 (CO 3)

(A2) For the group G = $<Z_7*,X>$

(i) Find the order of a group.

(ii) Find the number of primitive roots in the group.

(iii) Find the primitive roots in the group.

(iv) Make a table of discrete logarithm. 5 (CO 3)

(A3) List the parameters (block size, key size and no.of rounds) for AES 192. 3 (CO 3)

OR

(B1) Determine the solution to the following simultaneous equations using Chinese remainder theorem x = 2 mod 3, x = 3 mod 5 and x = 2 mod 7. 5 (CO 3)

(B2) Using Eular’s phi function, find ϕ (240). 2 (CO 3)

(B3) Explain general structure of DES with diagram. 3 (CO 3)

4. (A1) Differentiate between digital signature and crypto system. 2 (CO 1)

(A2) Discuss various attacks on digital signature. 2 (CO 1)

(A3) In the Diffe-Hellman key exchange algorithm, public keys g = 5 and q = 11. Senders private key x = 2 and receivers private key y = 3 are used. Calculate the following:

(i) What is the value of R1 and R2 ?

(ii) What is the value of symmetric session key ? 6 (CO 3)

OR

(B1) Define biometrics and distinguish between two broad categories of the techniques. 4 (CO 1)

(B2) Explain how a client process can access process running on the real server in Kerberos. 4 (CO 1)

(B3) Draw diagram of X. 509 certificate format. 2 (CO 1)

5. (A1) List phases of IKE and the goal of each phase. 4 (CO 4)

(A2) What are the services provided by PGP services ? Explain detail. 4 (CO 4)

(A3) Give the application of IP sec. 2 (CO 4)

OR

(B1) Describe how to generate Master secret from Pre-Master Secret in SSL . 4 (CO 4)

(B2) Name three types of messages in PGP and Explain their purpose. 4 (CO 4)

(B3) Differentiate between session and connection. 2 (CO 4)

6. (A1) What is the difference between Firewall and IDS ? 4 (CO 1)

(A2) Describe different types of Intruders. 4 (CO 1)

(A3) List the types of firewalls. 2 (CO 1)

OR

(B1) Explain in brief following malicious programs (Any **four**) :

(i) Worms,

(ii) Logic Bomb

(iii) Spyware

(iv) Trojan

(v) Virus 4 (CO 1)

(B2) What is Intrusion Detection System ? List and briefly define three Classes of intruders. 4 (CO 1)

(B3) Define virus. Specify the types of viruses. 2 (CO 1)