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.

1. (A) (A1) Prove that G = {0 , 1 , 2 , 3 , 4} is an abelian group with respect to addition modulo 5. 4(CO2)

(A2) Using the extended Euclidean algorithm, find the multiplicative inverse of

(i) 1234 mod 4321 (ii) 24140 mod 40902 4(CO2)

(A3) Illustrate the relationship between services and mechanisms. 2(CO1)

OR

(B) (B1) Define security mechanisms. What are different security mechanisms ? 6(CO1)

(B2) Differentiate between passive and active Attack. 2(CO1)

(B3) Find multiplicative inverse of 38 in Z180 using extended Euclidean Algorithm. 2(CO2)

2. (A) (A1) Determine ciphertext and also perform decryption using the Hill cipher technique. Message = "meet me at the usual place at ten rather than eight oclock" key = $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$ 6(CO2)

(A2) What are the components of modern block cipher ? 2(CO1)

(A3) Distinguish between feistel and non – feistel block cipher. 2(CO1)

OR

(B) (B1) Encrypt the message "the house is being sold tonight". Using Vigenere Cipher with key : "dollars". 6(CO2)

(B2) Differentiate between stream and block cipher. 2(CO1)

(B3) Define diffusion and confusion. 2(CO1)

3. (A) (A1) Solve the following :

(i) Find the order of the group G = < Z20*, X>

(ii) Number of primitive roots in the group G = < Z17*, X>

(iii) 45617 mod 17 Using Fermat's little theorem. 6(CO2)

(A2) In RSA, ciphertext $C = 10$ send to a user whose public key is $e = 5$, $n = 35$, what is plaintext M ? 2(CO3)

(A3) Why does the DES function need and expansion permutation ? 2(CO1)

OR

(B) (B1) Determine the solution to the following simultaneous equations using Chinese remainder theorem $x = 7 \bmod = 13$, $x = 11$ and mod 12. 5(CO2)

(B2) Convert "AES USES A MATRIX" into AES state matrix. 3(CO3)

(B3) Compare symmetric and asymmetric key cryptography. 2(CO1)

4. (A) (A1) In the Diffie – Hellman key exchange algorithm, public keys $g = 5$ and $q = 11$. Senders private key $x = 2$ and receivers private

key y = 3 are use. Calculate the following :

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

(ii) What is the value of symmetric session key ? 4(CO3)

(A2) Discuss biometric entity authentication techniques. 4(CO1)

(A3) Define Kerberos and name its servers. 2(CO1)

OR

(B) (B1) Write the steps of HMAC and give its schematic representation. 6(CO2)

(B2) Define cryptographic hash function. 2(CO1)

(B3) List the security services provided by a digital signature. 2(CO1)

5. (A) (A1) Discuss Authentication Header Protocol with its diagram. 5(CO4)

(A2) Name all the content defined by CMS and their purposes. 3(CO4)

(A3) Distinguish between session and connection. 2(CO1)

OR

(B) (B1) What is security association database and give its all parameters ? 6(CO4)

(B2) Distinguish between two modes of IPSec. 2(CO4)

(B3) List ISAKMP payload type and the purpose of it. 2(CO4)

6. (A) (A1) Write in detail about the types of firewall with advantages and disadvantages. 6(CO1)

(A2) What is the difference between worms and viruses ? 2(CO1)

(A3) Define system and the components of system. Reflect on the statement "Encryption provides system security". 2(CO1)

OR

(B) (B1) Write in detail about the different IDS techniques. 6(CO1)

(B2) What are parts of computer virus ? 2(CO1)

(B3) What is the difference between a firewall and IDS. 2(CO1)