Course Code : CST 407 **CXDW/RW – 18 / 5583**

Eighth Semester B. E. (Computer Science and Engineering) Examination

INFORMATION SECURITY

Time : 3 Hours] [Max. Marks : 60

Instructions to Candidates :—

(1) Solve all questions.
(2) All questions carry marks as indicated against them.
(3) Due credit will be given to neatness and adequate dimensions.
(4) Assume suitable data and illustrate answers with neat sketches wherever necessary.

1. (a) Describe Network Access and Network security model for Encryption and Decryption. Also list four kinds of cryptanalysis attack. 5(CO1)

   (b) Apply Transposition cipher to decrypt the cipher text "EHUHPEHSNTRGTIEROOYDEUGTKINEATEDDDDI" from the given round key "HEALTH", Also Identify and write three primary security issues in CFB Mode. 5(CO1)

2. (a) Write down the process for function key generation in DES Encryption. Write the difference between Conventional and asymmetric cryptography. 10(CO1)

OR

(b) (i) If a plain text is "ATK" and Key matrix is Encrypt the given message using Hill Cipher And also show its decryption.

$$\text{Key} = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

5(CO1)

(ii) Apply S – DES algorithm to encrypt the following
i / p = 11110101
Raw Key = 1110010111
Permutation P10 on key is defined as {3 , 5 , 2 , 7 , 4 , 10 , 1 , 9 , 8 , 6}
Permutation P8 on key is defined as {6 , 3 , 7 , 4 , 8 , 5 , 10 , 9}
Permutation IP on i / p is defind as {2 , 6 , 3 , 1 , 4 , 8 , 5 , 7}
Expansion permutation is defind as {4 , 1 , 2 , 3 , 2 , 3 , 4 , 1}
Permutation P4 is defined as {2 , 4 , 3 , 1}
Inverse permutation is defined as {4 , 1 , 3 , 5 , 7 , 2 , 8 , 6}
The S – Box S0 and S1 is defined as

1	0	3	2
3	2	1	0
0	2	1	3
3	1	3	2

0	1	2	3
2	0	1	3
3	0	1	0
2	1	0	3

5(CO1)

3. (a) State Whether true or false, if computation of Diffie Hellman is hard its Discrete logarithm is also Hard. Demonstrate Diffie- Hellman scheme with a common prime q = 41 and a primitive root a = 7.

(a) If user A has public key Ya = 3, What is A's private key Xa ?

(b) If user B has public key Yb = 9, What is the shared secret key K ? 4(CO2,4)

(b) Can you use RSA to transmit public and private key ? If so describe how ? Consider RSA encryption with public key 55 and public exponent = 3.

(i) How many elements are in Z * 55 ?

(ii) Compute the private exponent d.

(iii) Compute the encryption of the meaasge m = 6.

(iv) Compute the decryption of the cipher text c = 2.
6(CO2 , 4)

4. Solve any **Two** :—

(a) Write the algorithmic method to perform a digital signature for any electronic document similarly, discuss the mathematical formulation used to verify the signature by presenting, a neat sketch with set of equation to analyse the difficulty level of efforts to be tried for modifying the signature. 5(CO3)

(b) Define trap door function. Differentiate MD5 and SHA – I. 5(CO3)

(c) What is the best way to calculate checksum for a file that is on your Machine ? Device its compression logic and Differentiate between any two such popular methods used for generating a checksum, in the same context brief its relation with the Birthday Attack. 5(CO3)

5. (a) Illustrate basic authentication service dialogues maintained between Kerberos Client's and Server's ? Design a flow of event which shows centralized authentication scheme for Kerberos functioning in distributed environment. 5(CO4)

(b) Describe the application usage of two key rings maintained by user in PGP protocol to secure your Email conversation. What steps are being followed by record protocol before attaching an SSL header to be included in IP packet ? 5(CO4)

6. Solve any **Two** :—

(a) Discuss Electronic payment process. State how tightly protocol security is built on such E-commerce transactions. 5(CO5)

(b) Define three classes of intruders. What is audit record analysis ? 5(CO5)

(c) Can you produce a sample of Virus Structure ? Show compression logic for virus programs. 5(CO5)