Course Code : CST 417 / CST 407 **KOLP/RW – 19 /9622**

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

INFORMATION SECURITY

Time : 3 Hours] [Max. Marks : 60

Instructions to Candidates :—

(1) All questions are compulsory.
(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. Solve any **Two** :—

   (a) Compare and contrast Symmetric and Asymmetric Encryption ? 5(CO1)

   (b) Recall the Term : Data Integrity, Non repudiation, Masquerading and Analyze Block cipher mode of operation with DES algorithm in short. 5(CO1)

   (c) Show an example of Transposition cipher for encryption and decryption of text using double columnar matrix. 5(CO1)

2. (a) List characteristics of AES algorithm considering Stream cipher and block cipher. 5(CO1)

   (b) State the importance of Avalanche Effect. Describe the steps of round key generation in brief with neat sketch. 5(CO1)

3. (a) Shweta uses the RSA Crypto System to receive messages from Rakesh. She chooses – $p = 13$, $q = 23$ – her public exponent $e = 35$

   - Shweta publishes Public key as $\{e , n\}$
   - Check that $e = 35$ is a valid exponent for the RSA algorithm.
   - Compute d, the private exponent of Shweta.
   - Now Rakesh wants to send to Shweta the (encrypted) Paintext $P = 15$.

- What does he send to Shweta ?
- Verify the same that she can decrypt this message.

5(CO2 , CO4)

(b) 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 $\alpha = 7$.

(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 ? 5(CO2 , CO4)

OR

(c) For a user workstation in a typical business environment, List the potential locations of confidentiality attack ? What is FEPs Function ? Give its sketch. 5(CO2 , CO4)

4. (a) List the disadvantages of HMAC authenticator Function. Write a valid reason to justify that why HMAC cannot be trusted to be used in digital signature. 5(CO3)

(b) 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 of both with set of equation to analyze the difficulty level of efforts to be tried for modifying the signature. 5(CO3)

OR

(c) Construct compression function of MD5 algorithm to find out hash Digest or Finger print. 5(CO3)

5. (a) Identify the requirement of inter realm Processing. How the workstation authentication is carried out in case of remote multiple Kerberos system ? 5(CO5)

(b) Identify the security mechanism or protocol applied to handle user email inbox protection and describe the functioning in sender and receiver side. 5(CO5)

6. Solve any **Two** :—

(a) Summarize the working of SET Model for secure Electronic payment and show the comparison analysis of SSL and SET protocol. 5(CO5)

(b) How is screened host firewall, Dual homed bastion different from screened host firewall, single homed bastion ? List out the limitation of firewall. 5(CO5)

(c) Define three types of intruders. Provide an example showing how intruders try to attack ? Illustrate Honeypots. 5(CO5)