Course Code : CCT 208 **QVRU/RS – 22 / 1166**

Fourth Semester B. Tech. (Computer Science and Engineering / Cyber Security) Examination

CRYPTOGRAPHY

Time : 3 Hours] [Max. Marks : 60

Instructions to Candidates :—

(1) All questions carry marks as indicated against them.

(2) Due credit will be given to neatness and adequate dimensions.

(3) Assume suitable data and illustrate answers with neat sketches wherever necessary.

1. (a) Which security mechanism(s) are provided in each of the following cases ?

(i) A company demands employee identification and a password to let employee log into the company server.

(ii) A company server disconnects an employee, if he is logged into the system for more than two hours.

(iii) A teacher refuses to send students grades by email unless they provide identification assigned by the teacher.

(iv) A bank requires the customer's signature for a withdrawal.

(v) A person signs a form he has filled out to apply for a credit card. 5 (CO 1)

OR

(b) Encrypt the message 'SECRET MASTER KEYS' using double transposition and 4 x 4 matrix. First transpose the columns according to the key (1, 2, 3, 4) → (2, 4, 1, 3).
Then transpose the rows according to the key
(1, 2, 3, 4) → (4, 1, 2, 3). Final ciphertext is read row by row.
5 (CO 1)

(c) What do you mean by Cryptanalytic and Non - cryptanalytic attacks ? List and give the examples of various attacks that are threatening to Confidentiality, Integrity and availability of information. 5 (CO 1)

2. (a) Can the set of residues $Z_6 = \{0, 1, 2, 3, 4, 5\}$ form a group for the multiplication (x) operation ? Is the group $G = \{1, 2, 3, 4, 5, 6\}$ under the multiplication modulo 7 cyclic with generator 3 ? 5 (CO 1, 2)

OR

(b) What do you mean by differential and linear cryptanalysis ? How differential cryptanalysis can be used by an attacker to guess the key values by using the difference relation between plaintext and cipher text. Give the analogy for differential analysis only. 5 (CO 1, 2)

(c) Define the meaning of full size or partial key size in modern block Cipher. If suppose the block size is 64 bits ? What would be the key size in terms of transposition and substitution block cipher ? Justify your answer with suitable example. 5 (CO 1, 2)

3. (a) Show how Chinese remainder theorem is used to solve the linear congruent equations. What is its application in Cryptography ? 7 (CO 2)

OR

(b) Using Fermat's Little theorem, find the results of the following :—

(i) 5^{15} and 13

(ii) 15^{18} and 17

(iii) 7^{14} and 13 7 (CO 2)

(c) Discuss with example the approaches used for placement of encryption function. 3 (CO 2)

4. (a) In the Diffie-Hellman protocol, what happens if x and y have same value, that is Alice and Bob have accidentally chosen the same number ? Are R1 and R2 the same ? Do the session keys calculated by Alice and Bob have the same value ? Give an example to prove your claims. 6 (CO 3)

OR

(b) What are Message Detection Code (MDC) and Message Authentication Code (MAC) ? Explain how Hash-based message authentication code is useful in cryptography applications. 6 (CO 3)

(c) Differentiate between Asymmetric-key Cryptography Vs. Symmetric-key Cryptography on the following aspects : Number of keys, Key distribution center, Computational overhead and Security. 4 (CO 2)

5. (a) In an RSA digital signature scheme p = 7, q = 11, public key = 13 :

(i) Determine the private key.

(ii) Compute the digital signature on the digest h = 8.

(iii) Verify the signature using the public key. 5 (CO 3)

OR

(b) What are the security requirements for cryptographic Hash function ? Clearly describe how these requirements can be satisfied by a secure hash function. 5 (CO 3)

(c) How centralized authentication is done by Kerberos ? Discuss ticket generation mechanism ? Is it used for user-to-user authentication ? 5 (CO 2, 3)

6. Solve any **Two** :—

(a) What is PGP ? Explain the format of private key ring table and public key ring table in PGP. List the inputs needed to extract information at the sender side in PGP. 5 (CO 4)

(b) Explain Transport Mode and Tunnel Mode in IPSec. List and describe the fields of Authentication Header protocol. 5 (CO 4)

(c) List and explain the contents of an X·509 certificate. Define certificate revocation process. 5 (CO 4)