Printed Pages: 02 **Sub Code: KCA011**

Paper Id:	2	3	2	3	1	0

Roll No.													

MCA
(SEM III) THEORY EXAMINATION 2022-23
CRYPTOGRAPHY AND NETWORK SECURITY

Time: 3 Hours ***Total Marks: 100***

Note: Attempt all Sections. If you require any missing data, then choose suitably.

SECTION A

1. Attempt *all* questions in brief. 2x10 = 20

(a) What are the drawbacks of placing the encryption function at application layer?
(b) What is Avalanche effect? Explain in brief.
(c) Compute the value of Φ (41) where Φ is Euler Totient function.
(d) What are the drawbacks of mono-alphabetic substitution cipher?
(e) Differentiate between weak collision resistance and strong collision resistance property of hash function.
(f) What are the Requirements for Public-Key Cryptography?
(g) What do you mean by Reply Attack?
(h) Define a hash function
(i) What do you mean by a Trusted System
(j) What is a virus? Describe WORM, Trojan horse.

SECTION B

2. Attempt any *three* of the following: 10x3 = 30

(a) Describe Block Cipher Modes Of Operation in DES.
(b) State the Chinese Remainder Theorem. Hence use it to solve following Congruence to obtain the value of X.
x≡2 (mod 3); X≡3 (mod 5); X≡2 (mod 7)
(c) What are the possible ways symmetric keys can be distributed? Describe a key distribution scenario between users A, B and KDC. Assume that users A and B share a unique master key with KDC.
(d) What is Kerberos? Explain the role of Authentication Server (AS) and Ticket Granting Server (TGS) in Kerberos authentication Protocol.
(e) Write down short notes on any two of following: --
(i) Secure Electronic Transaction (SET)
(ii) Firewall
(iii) Secure Socket Layer (SSL)
(iv) HTTPS

SECTION C

3. Attempt any *one* part of the following: 10x1 = 10

(a) What do you understand by network security attacks? Describe active and passive security attacks.
(b) Explain triple DES encryption and Decryption? Explain the term meet-in-the middle attack.

4. Attempt any *one* part of the following: 10 x1 = 10

(a) For a Deffie-Hellman scheme with common prime q = 11, and primitive root $\alpha = 2$, generate a set of public key and private key pairs between two users A and B. Make your own assumptions.

(b) Explain the term traffic confidentiality with suitable example.

5. Attempt any *one* part of the following: 10x1 = 10

(a) What do you understand by message authentication code? How it differs from one way hash function?

(b) Describe DSA (Digital Signature Algorithm).

6. Attempt any *one* part of the following: 10x1 = 10

(a) What is Pretty Good privacy (PGP)? Give the structure of Pretty Good privacy? Also explain the concept of key rings with their formats

(b) What are the major security aspects in the security of electronic mail system.

7. Attempt any *one* part of the following: 10x1 = 10

(a) What services does IPSec provide? What is the difference between transport mode and tunnel mode?

(b) What are the important features of Oakley Key exchange algorithm used for key exchange in the context of IPsec? What are the improvements in Oakley algorithm over Diffie Hellman Key exchange algorithm?