Printed Pages:02 **Sub Code:KCS074**

Paper Id: 2 3 1 3 5 3 **Roll No.** □□□□□□□□□□□□□

B.TECH.
(SEM VII) THEORY EXAMINATION 2022-23
CRYPTOGRAPHY & 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)	Explain Shannon Confusion and Diffusion.
(b)	Apply the Caesar Cipher(p=D(3,C)) and Decrypt the cipher text “PHHW PH”.
(c)	Calculate Φ(35).
(d)	Find gcd(1970,1066) using Euclid’s algorithm.
(e)	What is Birthday attack?
(f)	Explain role of compression function in hash function.
(g)	What is realm?
(h)	What are the services provided by the PGP?
(i)	Why does ESP include a padding field?
(j)	Mention four SSL protocol.

SECTION B

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

(a)	Explain the concept of block cipher and stream cipher in cryptography. Discuss the modes of operations of block cipher.
(b)	What do you understand by Chinese Remainder Theorem? Solve the following congruent equations by Chinese remainder theorem: i. X ≡ 2 mod 3 ii. X ≡ 3 mod 5 iii. X ≡ 2 mod 7
(c)	Why Message Authentication is required? Discuss working of MAC with suitable block diagram.
(d)	What is Digital Certificate? Give the format of X.509 certificate showing the important elements of the certificate. How is an X.509 certificate revoked?
(e)	Explain the concept of dual signature in context of Secure Electronic Transaction(SET). Briefly describe the sequence of events that are required for a SET transaction.

SECTION C

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

(a)	Explain Playfair technique and encrypt the following message "hide the gold in the treestump"' using the key - " playfair ".
(b)	Draw a block level diagram to depict the signature of one round of DES. Prove that if plaintext block and encryption key are complemented then resulting ciphertext block of DES encryption is also complemented.

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

(a)	Explain AES algorithm. What is the difference between the AES encryption algorithm and the DES algorithm.
(b)	State and prove Fermat's theorem. Use Fermat theorem to find a number 'a' between0 and 72 with $a \equiv 9794 \bmod 73$.

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

(a)	Explain Hash Function? Discuss SHA- 512 with all required steps, round function & block diagram.
(b)	Explain the idea of Digital Signature for the authentication. Discuss signing & verifying process of Digital Signature Algorithm (DSA) in detail with suitable steps.

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

(a)	Explain the full service of Kerberos environment. What are the principle differences between version 4 and version 5 of Kerberos?
(b)	Describe how Diffie-Hellman algorithm used for key exchange is vulnerable to man in middle attack? Determine the shared secret key in a Diffie-Hellman scheme with a common prime 71 and primitive root 7. Given the private keys of the communicating parties A and B are 5 and 12 respectively.

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

(a)	Describe RSA algorithm in detail. Calculate the private key of A wherein RSA cryptosystem a particular A uses two prime numbers p = 13 and q =17 to generate her public and private keys. Let the public key of A is 35.
(b)	Explain the following: (i) Intrusion detection (ii) Firewall