CBCS SCHEME

USN □□□□□□□□□□ **17TE71**

Seventh Semester B.E. Degree Examination, Jan./Feb.2021

Cryptography and Network Security

Time: 3 hrs. Max. Marks: 100

Note: ***Answer any FIVE full questions, choosing ONE full question from each module.***

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and /or equations written eg, 42+8 = 50, will be treated as malpractice.

Module-1

1 a. Explain the procedure to calculate GCD using Euclid's algorithm. Determine the GCD of (24140, 16,762) using Euclid's algorithm. **(06 Marks)**

b. Encrypt the message "Work is workshop" using, play fair cipher with the keyboard "COMPUTER" and decrypt the cipher text to recover the original message. Give the rules for encryption and decryption. **(08 Marks)**

c. Develop a set of additive and multiplications tables for modulo 9. **(06 Marks)**

OR

2 a. Construct the finite field GF (2^4) multiplication table using the polynomial arithmetic modulo $(x^4 + x + 1)$, show the calculation steps. **(06 Marks)**

b. Using extended Euclidean, find the multiplicative inverse of 550 mod 1769. **(06 Marks)**

c. Define the following:

(i) Groups, rings and fields.

(ii) Fermat's and Euler's theorem.

(iii) Cryptology, Cryptoanalysis, Cryptography. **(08 Marks)**

Module-2

3 a. Compare AES to DES for each of the following elements of DES :

(i) XOR of subkey material with the input of the f function.

(ii) XOR of the f function output with the left half of the block.

(iii) f function

(iv) Permutation P

(v) Swapping of half of the block. **(06 Marks)**

b. Consider the elliptic curve defined over $E_{23}(1, 1)$. Let P = (3, 10) and Q = (9, 7). Find (P+Q) and 2P. **(08 Marks)**

c. Given p = 19, q = 23, m = 5 and e = 3. Use RSA algorithm to find n, $\phi(n)$, d and C(m). Also find M from decryption. **(06 Marks)**

OR

4 a. What are the 4 tasks performed in each round of AES cipher? Explain. **(06 Marks)**

b. Users A and B use the Diffie Hellman key exchange technique, a common prime q = 11 and a primitive root $\alpha = 7$ (i) If user A has private key $X_A = 3$. What is A's public key Y_A? (ii) If user B has private key $X_B = 6$. What is B's public key Y_B? What is the shared secret key? Write the algorithm as well? **(06 Marks)**

c. Given the plaintext [000102030405060708090A0B0C0D0E0F] and the key [01010101010101010101010101010101]. Show the (a) State matrix (b) Initial round key (c) Sub Bytes (d) Shift rows (e) Mix columns output states. **(08 Marks)**

Module-3

5 a. Explain MD5 algorithm steps. Compare it with SHA-1. (08 Marks)

b. Discuss the key components of digital signature algorithm. (06 Marks)

c. Explain the HMAC algorithm with a neat diagram. (06 Marks)

OR

6 a. Explain the Discrete Logarithm signature scheme. (06 Marks)

b. Describe SHA 512 algoritm in detail. (06 Marks)

c. Explain the following:
(i) Hash function and its requirements.
(ii) Role of compression function in Hash functions.
(iii) Difference between weak and strong collision resistance.
(iv) Advantages of HMAC over other hash based schemes. (08 Marks)

Module-4

7 a. Describe the four protocols defined by secure socket layer. (06 Marks)

b. Explain the Secure Shell (SSH) architecture. (06 Marks)

c. Explain the various phases of 802.11i. (08 Marks)

OR

8 a. Explain the parameters defined in SSL connection. (06 Marks)

b. Bring out the differences between SSL and TLS. (06 Marks)

c. Explain HTTPS elements encrypted connection initiation and connection closure. (08 Marks)

Module-5

9 a. Explain the services provided by PGP and the reasons for using PGP. (06 Marks)

b. Explain Encapsulating security pay load header. (06 Marks)

c. Explain the preparation of enveloped Data S/MIME entity. Write the functions of S/MIME and Enhanced Security Services of S/MIME. (08 Marks)

OR

10 a. Explain the IPsec architecture. (06 Marks)

b. Describe the following :
(i) Differences between Tunnel mode and Transport mode of IPsec.
(ii) Scope of ESP encryption and authentication. (08 Marks)

c. Explain IKE key determination protocol. (06 Marks)

* * * * *