CBCS SCHEME

USN										

17CS743

Seventh Semester B.E. Degree Examination, Jan./Feb.2021
Information and Network Security

Time: 3 hrs. Max. Marks: 100

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

Module-1

1 a. Define the basic terminologies of Crypo and Kerckhoff's principle. **(05 Marks)**

b. Using the letter encodings table, the following ciphertext message was encrypted with a one-time pad : KITLKE **(07 Marks)**

Letter	e	h	i	k	l	r	s	t
Binary	000	001	010	011	100	101	110	111

(i) If the plaintext is "thrill", what is the key?

(ii) If the plaintext is "tiller". What is the key?

c. Discuss the taxonomy of cryptography. **(08 Marks)**

OR

2 a. Encrypt the message "we are all together" using a double transposition Cipher with 4 rows and 4 columns. Using the row permutation (1, 2, 3, 4) → (2, 4, 1, 3) and column permuation (1, 2, 3, 4) → (2, 4, 1, 3). **(05 Marks)**

b. Write a short notes on:
(i) Project VENONA (ii) Codebook cipher (iii) Ciphers of Election of 1876 **(12 Marks)**

c. Given the Caesar's Cipher find the plaintext from the Ciphertext,
DOLFHLPZRQGHUODQG **(03 Marks)**

Module-2

3 a. Suppose that a secure cryptographic hash function generates hash value that are n bits in length. Explain how Brute force attack could be implemented. What is the expected work factor? **(07 Marks)**

b. Explain HMAC function with an example. **(07 Marks)**

c. Describe the techniques used in Information hiding. **(06 Marks)**

OR

4 a. Justify that Tiger hash is fast and secure, elaborating its working principle. **(10 Marks)**

b. Discuss the secret sharing in detail and its types. **(10 Marks)**

Module-3

5 a. List and explain different types of freshness mechanisms. **(10 Marks)**

b. Explain the stages and challenges of protocol design. **(08 Marks)**

c. List the components of cryptographic protocol. **(02 Marks)**

OR

6 a. Describe the idea behind the dynamic password scheme. With a neat diagram, explain the example of dynamic password scheme. **(10 Marks)**

b. Explain about Diffie-Hellman key agreement protocol. **(10 Marks)**

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-4

7 a. Define key management, policies, practices and procedures. (03 Marks)
b. Discuss the key life cycle. (07 Marks)
c. Explain the different types of key generation in detail. (10 Marks)

OR

8 a. Explain the different public key management models. (12 Marks)
b. With a neat diagram, explain generic unique key per transaction schemes and its types. (08 Marks)

Module-5

9 a. Briefly explain simple SSL handshake protocol with a neat diagram. (08 Marks)
b. List the security and design issues in SSL. (04 Marks)
c. With a neat diagram, explain GSM authentication and encryption. (08 Marks)

OR

10 a. What are the serious problem with WEP key management? (04 Marks)
b. Explain the process of issuing eID card with a neat diagram. (10 Marks)
c. What are the potential security concerns for file protection and email security? (06 Marks)

* * * * *