CBCS SCHEME

USN □□□□□□□□□□ 15CS743

Seventh Semester B.E. Degree Examination, June/July 2023

Information and Network Security

Time: 3 hrs. Max. Marks: 80

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. With a neat diagram, explain crypto as a block box. **(05 Marks)**

b. Using vernam cipher encrypt the Plaintext "heihilter" to cipher text and from Ciphertext to plaintext using the key
110 101 110 101 111 100 000 101 110 000
And the corresponding binary representation of letter as below table :

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

(06 Marks)

c. Explain the taxonomy of cryptography. **(05 Marks)**

OR

2 a. Write a brief note on double transposition with an example. **(05 Marks)**

b. Explain the taxonomy of cryptanalysis. **(06 Marks)**

c. Write a short notes on :
i) Project VENONA
ii) Codebook cipher. **(05 Marks)**

Module-2

3 a. What is a Cryptographic Hash Function? Explain the properties of Hash Function. **(08 Marks)**

b. Demonstrate Birthday problem with example. **(08 Marks)**

OR

4 a. Illustrate the Birthday Attack with example. **(06 Marks)**

b. Explain the uses (Non Standard) for Hash Functions. **(10 Marks)**

Module-3

5 a. Explain different types of Freshness mechanisms. **(08 Marks)**

b. Explain Dynamic password scheme with an example. **(08 Marks)**

OR

6 a. List the components of cryptographic protocol. Also mention the stages involved in protocol design. **(08 Marks)**

b. Explain about Diffie – Hellman key agreement protocol. **(08 Marks)**

Module-4

7 a. What are the reasons for cryptographic key with finite lifetime? What are the measures taken for choosing a key length? Explain. **(08 Marks)**

b. With a neat diagram, explain generic unique key per transaction schemes and its types. **(08 Marks)**

OR

8 a. What are the various techniques that can be used to provide tamper resistance? Explain. **(05 Marks)**

b. With a neat diagram, explain key storage risk zones. **(06 Marks)**

c. With a neat diagram, explain identify–based public–key cryptography. **(05 Marks)**

Module-5

9 a. Explain how cryptography is used in SSL. **(06 Marks)**

b. Discuss about SSL handshake protocol. **(06 Marks)**

c. List the design issues in SSL. **(04 Marks)**

OR

10 a. Explain about Cryptography use in magnetic stripe cards. **(06 Marks)**

b. Discuss in detail, Cryptography for home users with respect to File protection and Email security. **(10 Marks)**

* * * * *