CBCS SCHEME

USN | | | | | | | | | | |

15CS743

Seventh Semester B.E. Degree Examination, Dec.2023/Jan.2024
Information and Network Security

Time: 3 hrs. Max. Marks: 80

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

Module-1

1 a. Differentiate between : i) Substitution and Transposition Cipher
ii) Symmetric and Asymmetric Cipher iii) Block and stream Cipher
iv) Cryptography and Cryptanalysis v) Plaintext and Cipher text. **(10 Marks)**

b. 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 the column Permutation (1, 2, 3, 4) → (2, 4, 1, 3). **(06 Marks)**

OR

2 a. Using the letter encodings in the Table the following two cipher text messages were encrypted with the one-time pad "KHHLTK" and "KTHLLE". **(08 Marks)**

Table : Abbreviated Alphabet

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

Find all possible plaintext for each message and the corresponding one-time pad for the key

111	101	110	101	111	100

b. Explain the following :
i) Code book cipher ii) Ciphers of the election of 1876. **(08 Marks)**

Module-2

3 a. Elaborate Birthday problem and correlate it with hash functions. **(06 Marks)**

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

OR

4 a. Discuss different schemes used in secret sharing with special reference to key Escrow. **(08 Marks)**

b. Mention the significance of generating proper random numbers, with special reference to Texas Hold'em Poker. **(08 Marks)**

Module-3

5 a. Illustrate the dynamic password scheme based on challenge response. **(08 Marks)**

b. Explain the clock based and sequence numbers freshness mechanisms. **(08 Marks)**

OR

6 a. Explain the stages in protocol design and its challenges. **(08 Marks)**

b. Illustrate Authentication and Key establishment protocols. **(08 Marks)**

Module-4

7 a. With suitable diagram, illustrate the key life cycle in key management. **(10 Marks)**

b. Explain the key storage risk factors. **(06 Marks)**

OR

8 a. Illustrate X.509 public key certificates. **(08 Marks)**

b. Explain the Certificate Life Cycle. **(08 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 Crypotography 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)**

* * * * *