CBCS SCHEME

USN | | | | | | | | | | 15CS743

Seventh Semester B.E. Degree Examination, July/August 2022
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. List four classic Ciphers. Explain Simple Substitution Cipher, with an example. **(05 Marks)**

b. Encrypt the message "Attack at dawn", using a double transposition cipher with 3 rows and 4 columns, using a row permutation $(1, 2, 3) \rightarrow (3, 2, 1)$ and column permutation $(1, 2, 3, 4) \rightarrow (4, 2, 1, 3)$. **(03 Marks)**

c. Explain One – time pad is a provably secure. Also discuss why One – time pad can be used only once. **(08 Marks)**

OR

2 a. Differentiate between : i) Plain text and Cipher text ii) Block and Stream Cipher iii) Diffusion and Confusion. **(06 Marks)**

b. Write a note on Code book Cipher. **(05 Marks)**

c. Give the Taxonomy of Cryptography. **(05 Marks)**

Module-2

3 a. What is a Cryptographic Hash function? Demonstrate a Birthday Attack with an example. **(06 Marks)**

b. Justify Tiger Hash is fast and secure. Also explain its working. **(10 Marks)**

OR

4 a. Explain HMAC structure. With a neat diagram. **(08 Marks)**

b. Explain Stegnography and Digital Water marking methods of Information hiding. **(08 Marks)**

Module-3

5 a. Differentiate between Non deterministic and Deterministic generators. **(04 Marks)**

b. Explain different types of Freshness Mechanisms. **(10 Marks)**

c. What is Zero Knowledge Mechanism? **(02 Marks)**

OR

6 a. Explain how a simple protocol is analyzed, with an example. **(08 Marks)**

b. Explain Diffie – Hellman key agreement protocol, with an example. **(08 Marks)**

Module-4

7 a. Illustrate the Key Life Cycle in Key Management, with a neat diagram. **(06 Marks)**

b. Explain distribution of Public keys with relevant diagram. **(10 Marks)**

OR

8 a. Illustrate X.509 Public Key certificate. **(08 Marks)**

b. Explain the Certification Life Cycle. **(08 Marks)**

Module-5

9 a. Illustrate Handshake Protocol, with a neat diagram. (06 Marks)

b. Describe the application of Cryptography for Secure payment and Card transaction. (08 Marks)

c. List application of Cryptography on the Internet. (02 Marks)

OR

10 a. Explain about Cryptography use in Video broadcasting. (08 Marks)

b. Explain the applications of Cryptography in :

i) File protection ii) Email security. (08 Marks)

* * * * *