CBCS SCHEME

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

21AD644

Sixth Semester B.E./B.Tech. Degree Examination, Dec.2024/Jan.2025
Data Security and Privacy

Time: 3 hrs. Max. Marks: 100

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

Module-1

1 a. Explain simplified model of symmetric encryption with neat diagram. **(10 Marks)**

b. List and briefly define types of cryptanalytic attacks based on what is known to the attackers. **(10 Marks)**

OR

2 a. Why is the Caesar Cipher substitution technique vulnerable to a brute-force crypto analysis? **(10 Marks)**

b. How does the use of random key in one-time pad provide security? **(10 Marks)**

Module-2

3 a. Briefly explain Diffie-Hellman key exchange protocol. **(10 Marks)**

b. Explain the principles of public-key cryptosystem. **(10 Marks)**

OR

4 a. Explain RSA algorithm? Briefly explain with an example. **(10 Marks)**

b. Explain Elgamal cryptographic system. **(10 Marks)**

Module-3

5 a. Explain the control vector encryption and decryption. **(10 Marks)**

b. Briefly explain the distribution of public keys. **(10 Marks)**

OR

6 a. Mention the advantages of simple secret key distribution scheme using public key encryption. **(10 Marks)**

b. Why is it sometimes desirable to revoke an X.509 certificate before it expires? **(10 Marks)**

Module-4

7 a. Discuss randomization method for privacy preserving data mining. **(10 Marks)**

b. Explain K-Anonymity framework. **(10 Marks)**

OR

8 a. Differentiate between personalized preservation and utility based privacy preservation. **(10 Marks)**

b. Write a short notes on :

i) The ℓ - diversity method ii) The t - closeness model **(10 Marks)**

Module-5

9 a. Explain distributed privacy preserving data mining. **(10 Marks)**

b. Explain association rule hiding. **(10 Marks)**

OR

10 a. List and explain the applications of privacy preserving data mining. **(10 Marks)**

b. Explain query auditing and interface control. **(10 Marks)**

* * * * *