CBCS SCHEME

USN □□□□□□□□□□ **18AD81**

Eighth Semester B.E. Degree Examination, June/July 2024

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 Symmetric encryption with a neat diagram. **(10 Marks)**

b. Explain the following with example :
i) Caesar cipher ii) Monoalphabetic cipher iii) Playfair Cipher
iv) Hill Cipher v) Polyalphabetic Cipher **(10 Marks)**

OR

2 a. Explain OES encryption algorithm with Avalanche effect. **(10 Marks)**

b. Explain Traditional Block Cipher Structure (Stream Cipher and Block Cipher) with example. **(10 Marks)**

Module-2

3 a. pExplain Man – in – the – Middle attack with example. **(10 Marks)**

b. Explain RSA Algorithm with example and list the different approaches to attack the RSA algorithm. **(10 Marks)**

OR

4 a. Explain the Diffie- Hellman key exchange with example. **(10 Marks)**

b. Explain public – key cryptosystems with public and private key encryption. **(10 Marks)**

Module-3

5 a. Explain the key distribution scenario in symmetric key distribution using symmetric encryption. **(10 Marks)**

b. Explain the general format of a X.509 public key certificate. **(10 Marks)**

OR

6 a. Explain PKIX Architecture Model along with PKIX management junction. **(10 Marks)**

b. Briefly explain the four general categories of schemes for the distribution of public keys. **(10 Marks)**

Module-4

7 a. Explain the key directions in the field of privacy preserving data mining algorithm. **(10 Marks)**

b. What is Randomization method? Explain. **(10 Marks)**

OR

8 a. Explain K-Anonymity Framework. **(10 Marks)**

b. Explain the ℓ-diversity method and t – closeness model. **(10 Marks)**

Module-5

9 a. Explain the applications of Privacy preserving Data Mining. **(10 Marks)**

b. Explain Distributed algorithm over horizontally and vertically partitioned data sets. **(10 Marks)**

OR

10 a. Explain the following briefly: i) Association Rule Hiding ii) Downgrading classifier effectiveness iii) Query auditing and Inference control. **(10 Marks)**

b. How does privacy – preserving Data mining help in Medical Data bases? Explain. **(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.