CBCS SCHEME

USN □□□□□□□□□□ **18CB742**

Seventh Semester B.Tech. Degree Examination, Dec.2023/Jan.2024

Cryptography and Network Security

Time: 3 hrs. Max. Marks: 100

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. Name and explain the essential ingredients of a symmetric cipher model. **(10 Marks)**

b. Explain polyalphabetic cipher with an example. **(10 Marks)**

OR

2 a. Explain data encryption standard with neat diagram. **(10 Marks)**

b. Explain Feistel encryption and decryption for 10 rounds. **(10 Marks)**

Module-2

3 a. Illustrate the RSA algorithm for encryption and decryption for the given data p = 17, q = 11, e = 7 and M = 88. **(10 Marks)**

b. Explain Diffie-Hellman key exchange with an example. **(10 Marks)**

OR

4 a. With a neat diagram, explain mom in the middle attack. **(10 Marks)**

b. Explain Elganual crypto system. **(10 Marks)**

Module-3

5 a. Define key management. Explain the fields of X.509 certificate. **(10 Marks)**

b. Explain the Kerberos with message sequences. **(10 Marks)**

OR

6 a. Explain the user authentication principles. **(10 Marks)**

b. Explain automatic key distribution for connection-oriented protocol. **(10 Marks)**

Module-4

7 a. Explain the fields in the TLS protocol stack. **(10 Marks)**

b. Explain SSL handshake protocol. **(10 Marks)**

OR

8 a. Explain SSH transport layer protocol packet formation. **(10 Marks)**

b. Explain the elements of IEEE802.11i. **(10 Marks)**

Module-5

9 a. Explain

i) Pretty good privacy

ii) Multipurpose mail extensions. **(10 Marks)**

b. With an example, explain DKIM strategy. **(10 Marks)**

OR

10 a. Explain IP security policy. **(10 Marks)**

b. Explain transport level security and tunel mode encryption. **(10 Marks)**

* * * * *