CBCS SCHEME

USN □□□□□□□□□□ **21IS71**

Seventh Semester B.E./B.Tech. Degree Examination, Dec.2024/Jan.2025

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. Draw the simplified model of symmetric encryption and explain it. **(06 Marks)**

b. Explain caeser cipher with example. **(04 Marks)**

c. Explain playfair cipher algorithm. Find the cipher text for plain text = "instruments" with key = "MONARCHY". **(10 Marks)**

OR

2 a. Encrypt the plaintext "Cryptography" using Hill Cipher algorithm with key $K = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$ and decrypt the same. **(10 Marks)**

b. With a neat schematic diagram, explain the DES encryption algorithm. **(10 Marks)**

Module-2

3 a. With a neat diagram, explain the six ingredients of a public-key cryptography. **(06 Marks)**

b. Explain the requirements and applications for public key cryptography. **(04 Marks)**

c. Explain the Elganal crypto system. **(10 Marks)**

OR

4 a. Explain RSA Algorithm. Using RSA algorithm perform encryption and decryption using $p = 17, q = 11, e = 7$ and $M = 88$. **(10 Marks)**

b. Explain the Diffe-Hellman key exchange algorithm. **(10 Marks)**

Module-3

5 a. With a neat diagram, explain public key Authority and Public key certificates techniques for distribution of public keys. **(10 Marks)**

b. Explain the key distribution scenario with relevant diagram. **(10 Marks)**

OR

6 a. Explain secret key distribution with confidentiality and authentication, with a neat diagram. **(10 Marks)**

b. With a neat diagram, explain control vector Encryption and Decryption. **(10 Marks)**

Module-4

7 a. Describe Public key infrastructure, with neat diagram. **(10 Marks)**

b. Explain Remote user – Authentication principles. **(10 Marks)**

OR

8 a. With a neat diagram, explain the general format of X.509 certificate. **(10 Marks)**

b. Explain the differences between Kerberos version 4 and version 5 and also mention the technical deficiencies in Kerberos version 4 protocols. **(10 Marks)**

Module-5

9 a. Describe in detail PGP (Pretty Good Privacy) cryptographic functions. (10 Marks)

b. Describe the various header fields defined in MIME. (05 Marks)

c. List the important features of IKE key determination algorithm. (05 Marks)

OR

10 a. Explain the Applications and Benefits of IPsec. (10 Marks)

b. With a neat diagram, describe IKE header and payload format. (10 Marks)

* * * * *