CBCS SCHEME

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

18CS744

Seventh Semester B.E./B.Tech. Degree Examination, Dec.2025/Jan.2026
Cryptography

Time: 3 hrs. Max. Marks: 100

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

Module-1

1 a. Draw the simplified model of symmetric encryption and explain it **(06 Marks)**
b. With a neat schematic, explain the DES encryption algorithm. **(10 Marks)**
c. Encrypt he plaintext "ELECTRONICS" using a playfair cipher with a key "INDIA". **(04 Marks)**

OR

2 a. Encrypt the plaintext "CRYPTOGRAPHY" using HILL CIPHER technique with key matrix $K = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$ and decrypt the same. **(10 Marks)**
b. Distinguish between:
i) Confusion and Diffusion ciphers
ii) Block cipher and stream ciphers. **(06 Marks)**
c. Explain Caesar cipher with an example. **(04 Marks)**

Module-2

3 a. Explain Public – Key Cryptosystems. **(10 Marks)**
b. Explain the description of the RSA algorithm. **(10 Marks)**

OR

4 a. Explain the Diffie – Hellman key exchange algorithm. **(10 Marks)**
b. Describe Elgamal Cryptographic systems. **(10 Marks)**

Module-3

5 a. Discuss elliptic curve cryptography for analog of Diffie – Hellman key exchange and explain with neat steps. **(10 Marks)**
b. Explain psecudorandom number generation based on asymmetric cipher. **(10 Marks)**

OR

6 a. Apply the distribution of public key with respect to directory, authority and certificate. **(10 Marks)**
b. Explain secret key distribution with confidentiality and authentication. **(10 Marks)**

Module-4

7 a. With a neat diagram, explain the general format of X.509 certificate. **(10 Marks)**
b. With relevant diagram, explain the confidentiality and authentication services provided by PGP protocol. **(10 Marks)**

OR

8 a. Explain Kerberos version and message exchanges. **(07 Marks)**
b. With relevant diagram, explain the DKIM functional flow. **(08 Marks)**
c. Describe the various header fields defined in MIME. **(05 Marks)**

Module-5

9 a. Describe the application and benefits of IPsec. **(10 Marks)**
b. Describe IP Security Architecture, with neat diagram. **(10 Marks)**

OR

10 a. Explain Internet Key Exchange (IKE) Key determination features. **(10 Marks)**
b. Explain Basic Combinations of Security Associations. **(10 Marks)**

* * * * *