CBCS SCHEME

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

21CS733

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.

Module-1

1 a. Explain the simplified model of symmetric encryption. **(06 Marks)**
b. Write a note on types of attack on encrypted message. **(04 Marks)**
c. Explain Feistel encryption and decryption algorithm with neat diagram. **(10 Marks)**

OR

2 a. Using Hill cipher, perform encryption and decryption for plain text = "SAFE MESSAGES" using key = "CIPHERING" **(10 Marks)**
b. Explain with neat diagram the working of DES encryption algorithm. **(10 Marks)**

Module-2

3 a. Explain RSA algorithm. Using RSA algorithm perform encryption and decryption for p = 5, q = 11, e = 3, M = 9. **(10 Marks)**
b. Explain the public key crypto system with neat diagram. **(10 Marks)**

OR

4 a. With a neat diagram, explain the man-in-middle attack. **(10 Marks)**
b. Explain Elgamal cryptosystem. Perform encryption and decryption using :
$q = 19$, $\alpha = 10$, $K = 6$, $M = 17$, $X_A = 5$, $Y_A = 3$ **(10 Marks)**

Module-3

5 a. With relevant diagram, explain the key distribution scenario. **(08 Marks)**
b. Explain with a neat diagram the control vector encryption and decryption. **(06 Marks)**
c. Write a note on exchange of public key certificate. **(06 Marks)**

OR

6 a. Explain the various techniques used for distribution of public key. **(10 Marks)**
b. Write notes on:
(i) Decentralized key distribution (ii) Public key distribution of secret key **(10 Marks)**

Module-4

7 a. Explain X.509 certificate format. **(10 Marks)**
b. Illustrate the block diagram of PKIX architectural model. **(10 Marks)**

OR

8 a. Describe the certification path for forward and reverse certificates of X.509. **(10 Marks)**
b. Explain with a suitable diagram the overview of Kerberos. **(10 Marks)**

Module-5

9 a. Explain confidentiality and authentication for S/MIME functional flow. **(10 Marks)**
b. With a neat diagram, explain ESP packet format. **(10 Marks)**

OR

10 a. Write a note on IKE formats. **(10 Marks)**
b. Explain the architecture of IP/Sec architecture. **(10 Marks)**

* * * * *