27/12

Code No.: (R22CS511PE) | R22 | H.T.No. | | | 8 | R | | | | | |

CMR ENGINEERING COLLEGE: : HYDERABAD
UGC AUTONOMOUS
III–B.TECH–I–Semester End Examinations (Regular) - December- 2024
CRYPTOGRAPHY & NETWORK SECURITY
(CSE)

[Time: 3 Hours] **[Max. Marks: 60]**

Note: This question paper contains two parts A and B.
Part A is compulsory which carries 10 marks. Answer all questions in Part A.
Part B consists of 5 Units. Answer any one full question from each unit. Each question carries 10 marks.

PART-A **(10 Marks)**

1. a) Define security mechanisms. [1M]
   b) Differentiate between symmetric and asymmetric cryptography. [1M]
   c) Explain the principle of DES encryption. [1M]
   d) What are block cipher modes of operation? [1M]
   e) Define message authentication codes. [1M]
   f) How does Kerberos ensure secure authentication? [1M]
   g) What is HTTPS, and why is it important? [1M]
   h) Mention two security features of IEEE 802.11i. [1M]
   i) What is the role of PGP in email security? [1M]
   j) How does IP Security achieve authentication? [1M]

PART-B **(50 Marks)**

2. Explain in detail the principles of security and types of attacks. [10M]

OR

3. Analyze the substitution and transposition techniques with examples. [10M]

4. Compare and contrast DES, AES, and Blowfish algorithms. [10M]

OR

5. Describe the RSA algorithm and explain its application in secure communication. [10M]

6. Explain SHA-512 and its role in cryptographic hash functions. [10M]

OR

7. Describe the Elgamal Digital Signature Scheme and its advantages. [10M]

8. Explain the architecture and working of SSL/TLS in detail. [10M]

OR

9. Discuss the security protocols implemented in IEEE 802.11i Wireless LAN. [10M]

10. Write a detailed note on IP Security architecture and its components. [10M]

OR

11. Explain S/MIME and its role in ensuring secure email communication. [10M]

****