Code No.: DS621PE

R20	H.T.No.			8	R						

CMR ENGINEERING COLLEGE: : HYDERABAD
UGC AUTONOMOUS
III–B.TECH–II–Semester End Examinations (Regular) - May- 2023
CRYPTOGRAPHY AND NETWORK SECURITY (PE-2)
(CSD)

[Time: 3 Hours] **[Max. Marks: 70]**

Note: This question paper contains two parts A and B.
Part A is compulsory which carries 20 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 and may have a, b, c as sub questions.

PART-A **(20 Marks)**

1. a) Define plain text and cipher text. [2M]
b) Write two principles of security. [2M]
c) Differences between stream cipher and block cipher. [2M]
d) Write principles of public key cryptosystems. [2M]
e) What is digital signature? [2M]
f) What is key size of SHA-512. [2M]
g) What is wireless security? [2M]
h) What are web security considerations? [2M]
i) How security maintained for e-mail? [2M]
j) What is PGP? [2M]

PART-B **(50 Marks)**

2. Discuss about types of security attacks and mechanisms. [10M]

OR

3. Illustrate different types of substitution techniques. [10M]

4. Explain DES algorithm and mention the strengths and weakness of it. [10M]

OR

5. Discuss RSA algorithm and Perform decryption and encryption using RSA algorithm with p=3, q=11, e=7 and n=5. [10M]

6. Write about HMAC algorithm and its security. [10M]

OR

7. What is the motivation for Kerberos? Discuss Kerberos version 4. [10M]

8. Explain secure socket layer and transport layer security briefly. [10M]

OR

9. Discuss about IEEE 802.11 wireless LAN. [10M]

10. Explain the functionality of S/MIME. [10M]

OR

11. Discuss case study on “cross site scripting vulnerability”. [10M]

****