Code No.: DS621PE	**R20**	**H.T.No.**			**8**	**R**						

CMR ENGINEERING COLLEGE: : HYDERABAD
UGC AUTONOMOUS
III–B.TECH–II–Semester End Examinations (Supply) - January- 2024
CRYPTOGRAPHY AND NETWORK SECURITY
(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 the terms security attacks? [2M]
b) Discuss about security mechanisms? [2M]
c) Differentiate between block cipher and stream cipher? [2M]
d) What primitive operation is used in RC4? [2M]
e) Sketch out X.509 certificate general format. [2M]
f) List out four general categories of schemes for the distribution of public keys? [2M]
g) Describe SSH. [2M]
h) Differentiate between IEEE 802.11&802.11i. [2M]
i) What are the different fields of authentication header? [2M]
j) What are the key algorithms used in S/MIME? [2M]

PART-B **(50 Marks)**

2. Draw the model for Network Security? Explain various components. [10M]

OR

3. Illustrate in your own words about the security services by a protocol layer of any communicating systems. [10M]

4. It is possible to use a hash function to construct a block cipher with a structure similar to DES. Because a hash function is one way and a block cipher must be reversible (to decrypt), how is it possible? [10M]

OR

5. Explain in detail about Diffie-Hellman key exchange Algorithm. [10M]

6. What are the steps involved in message digest generation using SHA-512? [10M]

OR

7. Explain the format of the X.509 certificate in detail. [10M]

8. What is the difference between TLS and SSL security? [10M]

OR

9. What are the services provided by SSL Record protocol and explain its operation? [10M]

10. Explain about IP Security Architecture. [10M]

OR

11. Explain the concept of Encapsulating Security Payload (ESP) in IP Security. [10M]

****