Code No.: CY514PE | R20 | H.T.No. | | | 8 | R | | | | | |

CMR ENGINEERING COLLEGE: : HYDERABAD
UGC AUTONOMOUS
III–B.TECH–I–Semester End Examinations (Supply) - May- 2023
CRYPTOGRAPHY & NETWORK SECURITY
(CSC)

[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.

PART-A **(20 Marks)**

1. a) What is avalanche effect? [2M]
   b) Define Asymmetric key cryptography? [2M]
   c) What are the drawback of Diffie and Helman key exchange algorithm? [2M]
   d) Write the difference between stream ciphers and block ciphers? [2M]
   e) What is a digital signature? [2M]
   f) What is message digest? [2M]
   g) What are the services provided by IP Security? [2M]
   h) What are the various PGP Services? [2M]
   i) What is the cross site scripting vulnerability? [2M]
   j) What are the intrusion detection system techniques? [2M]

PART-B **(50 Marks)**

2. List out the substitution techniques and explain any two techniques with example. [10M]

OR

3. Consider the following: [10M]
   Plaintext: "PROTOCOL"
   Secret key: "NETWORK"
   What is the corresponding cipher text using play fair cipher method?

4. Briefly explain the characteristics and operations of RC4 Encryption algorithm? [10M]

OR

5. Explain about DES algorithm with suitable examples and its advantages and limitations? [10M]

6. Explain about HMAC algorithm? [10M]

OR

7. Discuss Digital Signature Algorithm briefly? [10M]

8. What is MIME? Explain context types in detail? [10M]

OR

9. Explain about encapsulating security payload? [10M]

10. What is intrusion? Discuss intrusion detection system with neat diagram? [10M]

OR

11. Explain about Digital signature generation processes. [10M]

****