M.Sc. Semester IV Examination, 2021 (CBCS)

Subject: Computer Science

Paper: MCSA-403 (E-II)
(Cryptography & Network Security)

Full Marks: 40 **Time: 2 Hours**

Answer any *eight* Questions: **5x8=40**

1. Discuss Vernam One Time Pad. How it is implemented in reality? 5

2. Explain how *confusion* and *diffusion* are achieved in DES. 5

3. Briefly discuss Extension field in the context of AES. 5

4. Discuss Miller-Rabin test for primality testing. 5

5. Discuss Elgamal encryption technique in brief. 5

6. Discuss digital signature in brief. 5

7. Discuss any one round of SHA-1 hash function. 5

8. Discuss PGP protocol in the context of email security. 5

9. If p=3 and q=19, compute the public exponent e, when d=23
in RSA cryptosystem. 5

10. Discuss Diffie-Hellman Key Exchange protocol in brief. 5