Reg. No. : □□□□□□□□□□□□

Question Paper Code: 6213132

M.C.A. DEGREE EXAMINATIONS, NOV/ DEC 2024
Third Semester
Master of Computer Application
P20CAE11 – CRYPTOGRAPHY AND NETWORK SECURITY
(Regulation 2020)

Time: Three Hours Maximum: 100 Marks

Answer ALL questions

PART – A (10 x 2 = 20 Marks)

1. Define the term "substitution cipher" and give an example.

2. Differentiate stream ciphers with block ciphers.

3. State Fermat's theorem and its significance in cryptography.

4. Find the encryption and decryption using RSA algorithm for the following P=7, q=11, e=19 and m=8.

5. Mention the requirements of message authentication code.

6. Compare digital signatures and message authentication codes.

7. List the key management schemes used in symmetric key distribution.

8. Infer the functions of X.509 certificates in PKI.

9. Identify the key components of IP Security architecture.

10. Describe the purpose of Intrusion detection system.

PART – B (5 x 16 = 80 Marks)

11. (a) Discuss any four Substitution Technique with suitable examples. (16)

(OR)

(b) Discuss the structure of Data Encryption Standard (DES) and its limitations. (16)

12. (a) Examine the procedure to solve a problem using the Chinese Remainder Theorem. Clearly explain the steps. (16)

(OR)

(b) Evaluate the security of the RSA algorithm in terms of its dependency on the discrete logarithm problem. (16)

13. (a) Illustrate the steps involved in generating a message authentication code (MAC) and its applications. (16)

(OR)

(b) Explain the Elgamal Digital Signature Technique and its advantages. (16)

14. (a) Compare and contest symmetric key distribution and public key distribution and Detail the Diffie-Hellman Key Exchange method with a practical example. (16)

(OR)

(b) Interpret the functioning of Kerberos for secure authentication. (16)

15. (a) Explain the role of Encapsulating Security Payload (ESP) in IP Security. (16)

(OR)

(b) Examine the working of Secure Electronic Transaction (SET) and its application in e-commerce. (16)

-----xxxx-----