QP CODE: 24803247

24803247

Reg No : ....

Name : ....

I.M.C.A DEGREE EXAMINATION, MAY 2024

Seventh Semester

Integrated MCA

Core - IMCA7C04 - CRYPTOGRAPHY

2020 Admission Onwards

0C1CA9C2

Time: 3 Hours | Maximum: 75 Marks

Part A

*Answer any **ten** questions*

*Each question carries **3** marks*

1. “Passive attacks are very difficult to detect”- Justify this statement.
2. Explain the role of a trusted third party in network security.
3. Explain the symmetric key encryption model with neat diagram.
4. Explain how the round function and key scheduling contribute to the resilience of Feistel ciphers.
5. Discuss the relationship between confusion and diffusion in cryptographic algorithms. How do these two concepts work together to resist attacks and ensure the confidentiality of encrypted data?
6. Discuss the keying options available in Triple DES (3DES). What are the different modes of operation for 3DES, and how do they affect the security and performance of the encryption process?
7. Determine whether 1601 is a prime number.
8. What is Public key Infrastructure?
9. Define the term MAC.
10. What is message digest?
11. Define malicious software (malware) and distinguish between viruses, worms, and trojans.

12. Distinguish Public and Private Blockchain.

(10×3=30 marks)

Part B

*Answer **all** questions*

*Each question carries **9** marks*

13. a) Write about Security Mechanisms in cryptography.

OR

b) Explain Classical Encryption Techniques.

14. a) Investigate the Cipher Block Chaining (CBC) mode of operation for block ciphers comprehensively. Describe the encryption and decryption processes in CBC mode, highlighting the chaining mechanism and the role of the initialization vector (IV). Evaluate the strengths and weaknesses of CBC, including its resistance to certain attacks such as plaintext manipulation and its susceptibility to others like the padding oracle attack. Compare CBC with other modes in terms of security, efficiency, and suitability for various applications.

OR

b) Evaluate the security strengths and weaknesses of Feistel ciphers, considering their vulnerability to various attacks such as differential and linear cryptanalysis. Discuss the practical applications of Feistel ciphers in modern cryptography and their relevance in both academic research and real-world cryptographic implementations.

15. a) Compare and contrast the security assumptions and computational complexity of various public-key algorithms, such as RSA, ECC, and Diffie-Hellman.

OR

b) Describe about public and private keys in ECC system and explain about security of ECC.

16. a) List and explain the requirements for a message authentication code.

OR

b) Discuss the principles of key management and distribution in public-key cryptosystems.

17. a) List and describe the different type of attack that can be made on digital signatue.

OR

b) How does the blockchain work?

(5×9=45 marks)