



QP CODE: 26800205



Reg No : .....

Name : .....

**I M C A DEGREE EXAMINATION, DECEMBER 2025****Seventh Semester**

INTEGRATED MCA

**CORE - IMCA7C04 - CRYPTOGRAPHY**

2020 ADMISSION ONWARDS

A26885C9

Time: 3 Hours

Maximum: 75 Marks

**Part A***Answer any **ten** questions**Each question carries **3** marks*

1. Write a note on block cipher with an example.
2. Use Caesar cipher with key =15 to encrypt the message "Hello".
3. Define the concept of a one-time pad in cryptography.
4. Discuss any vulnerabilities or attacks associated with Feistel structure.
5. How does substitution contribute to confusion in cryptographic systems? Provide examples of substitution techniques commonly used in encryption algorithms, and discuss their role in disguising the relationship between plaintext and ciphertext.
6. Describe the strength and weaknesses of the DES algorithm in terms of security.
7. Define prime and composite numbers. Give examples.
8. Discuss the security of ElGamal Crypto System.
9. Briefly explain Message authentication.
10. What is keyed hash function?
11. What are the properties that digital signature must have ?
12. Define Blockchain. Give any two applications.





(10×3=30 marks)

**Part B***Answer all questions**Each question carries 9 marks*

13. a) Generalize the security services classifications and security mechanisms in detail.

OR

b) Explain the Play Fair cipher algorithm? Encrypt the message 'MY BALLOON' using the key 'MONACHRY'

14. a) Describe the cryptographic operations involved in AES, including the SubBytes, ShiftRows, MixColumns, and AddRoundKey transformations. Analyze the key schedule algorithm used in AES to generate round keys.

OR

b) Compare and contrast different variations of Feistel ciphers, such as DES, Triple DES, and Blowfish, in terms of their design choices, security properties, and suitability for various cryptographic applications.

15. a) Explain RSA algorithm. Given  $p=17$ ,  $q=11$ , and  $e=7$  Use RSA algorithm to find  $n$ ,  $\Phi(n)$  and  $d$ .

OR

b) Define elliptic curves and explain their application in cryptography.

16. a) List and explain the possible attacks that are relevant to message authentication.

OR

b) Explain Symmetric Key distribution using symmetric encryption.

17. a) Provide three examples of cryptographic methods used to encrypt sensitive data stored on disk or in databases, and discuss their effectiveness in mitigating risks associated with unauthorized access or data breaches.

OR

b) What are the generic elements of Blockchain?

(5×9=45 marks)