QP Code: RJ20MCA097 | Reg. No | | | | | | | | | | | AY 22

GIET UNIVERSITY, GUNUPUR – 765022

M. C. A (Third Semester) Regular Examinations, January – 2024

MCA20305 – Cryptography and Network Security

Time: 3 hrs | Maximum: 70 Marks

(The figures in the right hand margin indicate marks.)

PART – A **(2 x 10 = 20 Marks)**

Q.1. Answer ***ALL*** questions	CO #	Blooms Level
a. What do you mean by public key infrastructure?	CO3	K1
b. Differentiate between mono-alphabetic cipher and polyalphabetic cipher.	CO1	K1
c. Write down two disadvantages of Caesar cipher.	CO1	K1
d. What are the properties of hashing functions?	CO3	K1
e. What is meant by Fabrication?	CO1	K1
f. Mention the disadvantages of CBC.	CO1	K2
g. Differentiate between active attack and passive attack.	CO1	K1
h. What is initial permutation in DES?	CO2	K1
i. What is onetime pad cipher?	CO1	K1
j. What do you mean by traffic analysis?	CO1	K1

PART – B **(10 x 5 = 50 Marks)**

Answer ***ANY FIVE*** questions	Marks	CO #	Blooms Level
2. a. Briefly explain the block cipher modes of operations.	5	CO1	K1
b. Explain Data Encryption standard (DES) in detail.	5	CO2	K1
3.a. Describe Triple DES and its applications.	5	CO2	K2
b. Explain MD4 algorithm with its design principle.	5	CO3	K1
4. a. Write a short note on i. Onetime-pad cipher ii. Vigenere cipher	5	CO1	K2
b. Write down the algorithm of play fair cipher. Mention its strength.	5	CO1	K2
5. What is transposition technique? Explain with suitable examples.	10	CO1	K1
6. a. Explain the feistal cipher encryption process in detail with proper diagram.	5	CO1	K1
b. How T- Des is different from DES? Draw the diagram wherever necessary.	5	CO2	K1
7.a. Explain the Play Fair cipher algorithm? Encrypt the message 'MY BALLOON' using the key 'MONACHRY'.	5	CO2	K1
b. Explain secure hashing in detail.	5	CO3	K1
8. Explain the encryption process, sub-key generation and output transformation in IDEA with necessary diagrams.	10	CO2	K2

--- End of Paper ---