QP Code: RJ21MCA019 | Reg. No | | | | | | | | | | | AR 20

GIET UNIVERSITY, GUNUPUR – 765022

M. C.A. (Third Semester) Examinations, January – 2023

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

a. Differentiate between Active and Passive Attacks.
b. Mention different application of cyber security?
c. Define public key cryptography?
d. What is RSA algorithm?
e. Differentiate between encryption and decryption?
f. Define various operation of block cipher?
g. What is Secure Hash Algorithm (SHA)?
h. Write the role of firewall in trusted system?
i. Define Electronic Mail security?
j. What is digital signature?

PART – B **(10 x 5 = 50 Marks)**

Answer ***ANY FIVE*** questions — Marks

2. a.	Briefly Explain about OSI Architecture in Network Security.	5
b.	Briefly Explain about list of Security Services and Mechanisms.	5
3.a.	Design the general structure of DES and explain the Encryption/ Decryption process.	6
b.	Explain Encryption/Decryption process in AES Algorithm	4
4. a.	Write short Notes on Firewalls and its Real-time Application.	5
b.	Differentiate Host-based & Network-based Intrusion Detection System.	5
5.a.	Encrypt the following using play fair cipher using the **keyword- MONARCHY, Plain Text- "I LOVE MY INDIA".**	7
b.	Explain in detail Transposition Technique With Example.	3
6. a.	What is substitution technique? Explain in details with examples.	5
b.	Differentiate MD5 & SHA Hash Algorithm.	5
7.a.	Write short notes on Fermat and Euler's theorem.	5
b.	Write short notes on Chinese Remainder theorem with examples.	5
8. a.	Differentiate IPV4 & IPV6.	5
b.	Mentioned the use of Protocols in Web security.	5

--- End of Paper ---