QP Code: R253F005 Regn. No. | | | | | | | | | | AY - 24

Gandhi Institute of Engineering and Technology University, Odisha, Gunupur
(GIET University)

M.C.A. (Third Semester - Regular) Examinations, November – 2025

MCA23321 – Cryptography and Network Security

Time: 3 hrs Maximum: 60 Marks

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

PART – A **(2 x 5 = 10 Marks)**

Q.1. Answer ***ALL*** questions	CO #	Blooms Level
a. Define the three security goals.	CO1	K1
b. What is the block size and the cipher key size in DES?	CO2	K2
c. Can we say that $\varphi(49) = \varphi(7) \times \varphi(7) = 6 \times 6 = 36$? Justify.	CO3	K4
d. List the main features of the SHA-512 cryptographic hash function.	CO4	K3
e. Define the man-in-the-middle attack.	CO5	K2

PART – B **(10 x5=50 Marks)**

Answer ***ALL*** questions	Marks	CO #	Blooms Level
2. a. Explain the relation between security services and security mechanisms.	5	CO1	K3
b. Given a = 25 and b = 60, find the gcd(a, b) and the values of s and t using the Extended Euclidean algorithm.	5	CO1	K4
(OR)			
c. Distinguish between a substitution cipher and a transposition cipher.	5	CO1	K3
d. Find the particular and general solutions to the given linear Diophantine equation of two variables, 20x + 5y = 100.	5	CO1	K4
3. a. What are the modes of operation needed if modern block ciphers are to be used for encipherment?	5	CO2	K2
b. Define a state in AES. List the parameters (block size, key size, and the number of rounds) for the three AES versions.	5	CO2	K4
(OR)			
c. What is double DES? What kind of attack on double DES makes it useless?	5	CO2	K2
d. What is the difference between a weak key, a semi-weak key, and a possible weak key?	5	CO2	K3
4. a. Define Euler's theorem and explain its application.	5	CO3	K2
b. Distinguish between public and private keys in an asymmetric-key cryptosystem.	5	CO3	K3
(OR)			
c. Distinguish between a Prime, Co-prime and a Composite number.	5	CO3	K3

	d.	Define a trapdoor one-way function and explain its use in asymmetric-key cryptography.	5	CO3	K2
5.	a.	Distinguish between Message Integrity and Message Authentication.	5	CO4	K3
	b.	What are the three kinds of attacks on digital signatures? Explain briefly.	5	CO4	K2
		(OR)			
	c.	Explain briefly about the different Cryptographic Hash Function Criteria.	5	CO4	K2
	d.	Compare and contrast existential and selective forgery.	5	CO4	K3
6.	a.	Distinguish between fixed and one-time passwords. What are the attacks on password-based authentication		CO5	K3
	b.	List the duties of a PKI and Explain briefly.		CO5	K1
		(OR)			
	c.	For entity authentication what are the different Biometrics techniques are used? Explain briefly.		CO5	K3
	d.	Name three types of messages in PGP and explain their purposes.		CO5	K1

--- End of Paper ---