QP Code: RN23MCA029 | Reg. No | | | | | | | | | | | AY 23

GANDHI INSTITUTE OF ENGINEERING AND TECHNOLOGY UNIVERSITY, ODISHA, GUNUPUR
(GIET UNIVERSITY)

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

MCA23321 – Cryptography and Network Security

(MCA)

Time: 3hrs | 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. What are the five security services provided by Network Security?	CO1	K1
b. What is the number of rounds used in DES and AES?	CO2	K2
c. What is the value of φ (13) & φ (10)?	CO3	K5
d. Distinguish between message integrity and message authentication.	CO4	K4
e. Name three types of messages in PGP and explain their purposes.	CO5	K3

PART – B **(10 x5=50 Marks)**

Answer ALL questions	Marks	CO #	Blooms Level
2. a. Distinguish between passive and active security attacks. Give some examples of passive and active attacks.	5	CO1	K4
b. Given a = 161 and b = 28, find gcd(a, b) and the values of s and t using the Extended Euclidean algorithm.	5	CO1	K5
(OR)			
c. Distinguish between a monoalphabetic and a polyalphabetic cipher.	5	CO1	K4
d. Find the particular and general solutions of the Linear Diophantine Equation 21x + 14y = 35.	5	CO1	K5
3. a. Distinguish between DES and AES. Which one is bit-oriented? Which one is byte-oriented?	5	CO2	K4
b. What is double DES? What kind of attack on double DES makes it useless?	5	CO2	K2
(OR)			
c. What are the modes of operation needed if modern block ciphers are to be used for encipherment?	5	CO2	K2
d. What is the difference between a block cipher and a stream cipher?	5	CO2	K4
4. a. Define the Chinese remainder theorem and its application.	5	CO3	K1
b. What are the potential attacks on RSA? Explain briefly.	5	CO3	K3
(OR)			
c. Define quadratic congruence and the importance of QRs and QNRs in solving quadratic equations.	5	CO3	K1
d. Explain the Encryption, decryption, and key generation process in RSA with a neat diagram.	5	CO3	K3
5. a. What are the different criteria of a cryptographic hash function? Explain briefly.	5	CO4	K2

b.	What different attacks can one apply to the RSA digital signature scheme to forge somebody's signature?	5	CO4	K3
	(OR)			
c.	List the main features of the SHA-512 cryptographic hash function. What kind of compression function is used in SHA-512?	5	CO4	K2
d.	Compare and contrast a conventional signature and a digital signature.	5	CO4	K4
6. a.	Distinguish between data-origin authentication and entity authentication.	5	CO5	K4
b.	Name seven types of packets used in PGP and explain their purposes.	5	CO5	K1
	(OR)			
c.	Define Kerberos and name its servers. Briefly explain the duties of each server.	5	CO5	K1
d.	Compare and contrast key management in PGP and S/MIME.	5	CO5	K4

--- End of Paper ---