GALGOTIAS UNIVERSITY

ADMISSION NUMBER												

School of Computing Science and Engineering

Master of Technology in Computer Science and Engineering
Mid Term Examination - May 2024

Duration : 90 Minutes
Max Marks : 50

Sem II - R1PV209T - Cryptography and Computer Security

General Instructions
Answer to the specific question asked
Draw neat, labelled diagrams wherever necessary
Approved data hand books are allowed subject to verification by the Invigilator

1)	Explain Two key cryptography.	K2	(2)
2)	Summarize vernam cipher with example.	K1	(3)
3)	Demonstrate the model of network security with a diagram.	K2	(4)
4)	Rephrase any symmetric key cryptography algorithm in detail with the help of block diagram.	K2	(6)
5)	How do block cipher design principles contribute to achieving cryptographic security?	K3	(6)
6)	Encrypt "QUESTION" using One Time Pad cipher using KEY "QHSPNGXB".	K3	(9)
7)	Compare cryptography and steganography. Discuss the types of steganography.	K4	(8)
8)	Consider the elliptic curve E11 (1, 6); that is the curve is defined by y2=x3+x+6 with a modules of P=11. Calculate all the points in E11 (1, 6). Start by calculation the right hand side of the equation of all the values of n?	K4	(12)
	OR		
	Examine the round operaton of AES. How AES differs from DES?	K4	(12)