GALGOTIAS UNIVERSITY

ADMISSION NUMBER

School of Computing Science and Engineering

Master of Computer Applications
Semester End Examination - Jun 2024

Duration : 180 Minutes
Max Marks : 100

Sem II - E1PAA201T - Cryptography

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)	What is linear feedback shift registers (LFSR)? For n-bit LFSR, what is the longest possible sequence?	K1(2)
2)	Encrypt the plain text WATERMELON using HILL cipher with the appropriate key of 2*2matrix.	K2(4)
3)	Explain the First Add Round Key Step of DES?	K2(6)
4)	Analyze the functionality of ROTOR machine.	K3(9)
5)	Analyze the Brute force attacks complexity in Decryption.	K3(9)
6)	Apply HILL cipher techniques to encrypt message "NAMEIS" considering 3*3 matrix as a key.(assume)	K5(10)
7)	Using RSA algorithm, Encrypt the message M = 5 where the following values are given as p =3, q = 11, d = 7.	K4(12)
8)	List four general categories of schemes for the distribution of public keys & explain it with diagram.	K5(15)
9)	Estimate the value of the padding field in SHA-512 if the length of the message is-1) 2942 2) 2943 3)2944	K5(15)
10)	Derive Primitive roots for number 7 & 5.	K6(18)