GALGOTIAS UNIVERSITY

ADMISSION NUMBER

School of Computing Science and Engineering

Master of Technology in Computer Science and Engineering
Semester End Examination - Jun 2024

Duration : 180 Minutes
Max Marks : 100

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) List out the design goals of firewalls. K1(2)

2) Show the working of Euclidean algorithm with example. K2(4)

3) Interpret the working of MAC with suitable block diagram. K2(6)

4) Given $a = 161$ and $b = 28$, find $\gcd(a,b)$ and the values of s and t. K3(9)

5) Discover the types of attacks addressed by message authentication? K3(9)

6) What is PKI? Evaluate different ways of public key distribution. K5(10)

7) Distinguish between symmetric and asymmetric-key cryptography with their advantages and disadvantages. K4(12)

8) Discuss Euler's theorem. What is Euler's totient function? Write rules of Euler's totient function. Evaluate Euler's totient of 10. K5(15)

9) Examine the mathematical foundations of the Digital Signature Algorithm (DSA). How does the DSA algorithm leverage modular arithmetic and group theory concepts for signature generation and verification? K5(15)

10) Construct a mathematical model to demonstrate the cryptographic principles behind RSA digital signatures K6(18)