GALGOTIAS UNIVERSITY

ADMISSION NUMBER												

School of Computing Science and Engineering

B.TECH CSE with specialization in Computer Science and Business Systems
Semester End Examination - Nov 2023

Duration : 180 Minutes
Max Marks : 100

Sem VII - CSBA3060 - Bigdata 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)	Write an explanation of "Security Services for E-mail," outlining its components such as authentication, confidentiality, integrity, and non-repudiation, and list potential email attacks.	K1 (2)
2)	Illustrate your understanding of network anomaly detection by explaining how this technique identifies deviations from expected network behavior, and offer examples like detecting unusual traffic patterns indicating potential security threats.	K2 (4)
3)	Provide an explanation of the Data Encryption Standard (DES), detailing its structure, substitution-permutation network, key generation, and its role as a symmetric encryption algorithm.	K2 (6)
4)	Demonstrate the utility of Machine Learning in ransomware detection and prevention, emphasizing how ML algorithms can learn patterns of ransomware behavior for effective identification and mitigation.	K3 (9)
5)	Illustrate the working of S/MIME (Secure/Multipurpose Internet Mail Extensions) in conjunction with IP Security (IPsec), showcasing how both protocols combine to provide secure email communication.	K3 (9)
6)	Evaluate the security features and limitations of security protocols like PGP, S/MIME, and IPSec, proposing improvements for stronger security	K5 (10)
7)	Examine the security features and limitations of security protocols like S/MIME (Secure/Multipurpose Internet Mail Extensions), discussing how they provide email message encryption, authentication, and integrity while considering potential vulnerabilities.	K4 (12)
8)	Design a Key generation algorithm for DES and draw block diagram to show the working of Key generation algorithm.	K5 (15)
9)	Evaluate the effectiveness and limitations of security protocols at the transport layer and recommend enhancements to ensure stronger security	K5 (15)
10)	Conjecture the vulnerabilities and attacks on RSA cryptosystem and its variations, suggesting alternative approaches for secure key exchange	K6 (18)

9)	Evaluate the effectiveness and limitations of security protocols at the transport layer and recommend enhancements to ensure stronger security	K5 (15)
10)	Conjecture the vulnerabilities and attacks on RSA cryptosystem and its variations, suggesting alternative approaches for secure key exchange	K6 (18)