Reg. No.: | | | | | | | | |

G. VENKATASWAMY NAIDU COLLEGE (AUTONOMOUS), KOVILPATTI – 628 502.

PG DEGREE END SEMESTER EXAMINATIONS - NOVEMBER 2024.

(For those admitted in June 2023 and later)

PROGRAMME AND BRANCH: M.Sc., COMPUTER SCIENCE

SEM	CATEGORY	COMPONENT	COURSE CODE	COURSE TITLE
III	PART - III	CORE ELECTIVE-3	P23CS3E3A	NETWORK SECURITY AND CRYPTOGRAPHY

Date : 15.11.2024 / FN **Time : 3 hours** **Maximum: 75 Marks**

Course Outcome	Bloom's K-level	Q. No.	SECTION – A (10 X 1 = 10 Marks) Answer ALL Questions.
CO1	K1	1.	Which term best describes the study of secure communication techniques to protect information from unauthorized access? a) Cryptography b) Cryptanalysis c) Steganography d) Decryption
CO2	K2	2.	What is the input block size in the DES algorithm? a) 64 Bit b) 64 Byte c) 56 Bit d) 56 Byte
CO2	K1	3.	Which congruence is correct according to Fermat's theorem if p is a prime and a is a positive integer? a) $a^p \equiv 1 (\text{mod } p)$ b) $a^p \equiv a (\text{mod } p)$ c) $a^p \equiv p (\text{mod } a)$ d) $a^p \equiv p (\text{mod } 1)$
CO2	K2	4.	What is called the assurance that the data received are exactly as sent by an authorized entity? a) Authentication b) Integrity c) Confidentiality d) Availability
CO3	K1	5.	Which encryption standard is commonly used in S/MIME for securing emails? a) RSA b) DES c) AES d) MD5
CO3	K2	6.	What are the two main modes of IPsec? a) Transport and Session b) Transport and Tunnel c) Packet and Tunnel d) Encryption and Authentication
CO4	K1	7.	Which program contains unexpected additional information that can be harmful to a system's security? a) Trojan Horse b) Virus c) Worm d) Kit
CO4	K2	8.	What SSL protocol is responsible for authenticating both the client and server, and negotiating encryption methods and keys? a) Record Protocol b) Change Cipher Spec Protocol c) Handshake Protocol d) Alert Protocol
CO5	K1	9.	What is the main advantage of quantum cryptography? a) Faster Encryption b) Better Compression c) Detection of Interception d) Simpler Implementation
CO5	K2	10.	Which document outlines the scope and objectives of a security audit? a) Audit report b) Security policy c) Audit plan d) Risk assessment

Course Outcome	Bloom's K-level	Q. No.	**SECTION – B (5 X 5 = 25 Marks)** **Answer ALL Questions choosing either (a) or (b)**
CO1	K2	11a.	Explain different types of security attacks in detail. **(OR)**
CO1	K2	11b.	Explain the IDEA algorithm.
CO2	K2	12a.	State and prove Euler's theorem. **(OR)**
CO2	K2	12b.	Explain RSA algorithm.
CO3	K3	13a.	Show how the HMAC algorithm creates a MAC for a message using a key. **(OR)**
CO3	K3	13b.	Outline the X.509 certificate format.
CO4	K3	14a.	Describe how the SSL protocol stack works and its components. **(OR)**
CO4	K3	14b.	Describe how different firewall configuration mechanisms work.
CO5	K4	15a.	Analyse a network forensic case and its methods. **(OR)**
CO5	K4	15b.	Analyse different watermarking techniques and their effectiveness.

Course Outcome	Bloom's K-level	Q. No	**SECTION – C (5 X 8 = 40 Marks)** **Answer ALL Questions choosing either (a) or (b)**
CO1	K4	16a.	Explain the DES algorithm in detail. **(OR)**
CO1	K4	16b.	Explain the AES algorithm in detail.
CO2	K5	17a.	Assess Diffie-Hellman key exchange mechanism with an example. **(OR)**
CO2	K5	17b.	Evaluate the Digital Signature Standard (DSS) and algorithm in detail.
CO3	K5	18a.	Discuss the Kerberos 4 dialogue and its security implications. **(OR)**
CO3	K5	18b.	Evaluate how PGP ensures e-mail security and analyse its components with a block diagram.
CO4	K5	19a.	Assess the Secure Electronic Transaction (SET) protocol's security features and components. **(OR)**
CO4	K5	19b.	Assess various Intrusion Detection techniques.
CO5	K6	20a.	A mid-sized company, TechCorp is having IT security issues and wants to conduct a security audit. They are considering various audit methods. • Discuss how each audit method would work for TechCorp, including their pros and cons. • Evaluate how well these methods can find security problems and compliance issues at TechCorp. • Choose one method, explain why it's the best choice and suggest ways to improve its effectiveness. **(OR)**
CO5	K6	20b.	Discuss the security and applications of DNA cryptography.