**MANGALORE INSTITUTE OF TECHNOLOGY & ENGINEERING**
(A Unit of Rajalaxmi Education Trust®, Mangalore)
Autonomous Institute affiliated to VTU, Belagavi, Approved by AICTE, New Delhi
Accredited by NAAC with A+ Grade & ISO 9001:2015 Certified Institution

**Model Question Paper**

**Second Semester MCA Degree Examination**

**Cryptography and Cybersecurity**

**Time: 3 Hours** **Max. Marks: 100**

***Note: 1. Answer any FIVE full questions, choosing ONE full question from each module.***
***2. M: Marks, L: RBT (Revised Bloom's Taxonomy) level, C: Course outcomes.***

| | | Module -1 | M | L | C |
|---|---|---|---|---|---|
| Q1 | a. | You are part of a security team responsible for designing the security framework for a new Automated Cash Deposit Machine (ACDM) that will be deployed in 500 public locations across the country. The ACDM allows users to deposit up to ₹2,00,000 in cash directly into their bank accounts using their debit card and a secure 6-digit PIN. The machine processes an average of 200 transactions per day at each location, with peak transactions during weekends and public holidays. The bank is concerned about potential security threats such as unauthorized access, fraud, data breaches, and physical tampering, particularly in high-traffic and unsupervised areas.<br>Based on the scenario provided:<br>Design and implement a comprehensive security framework for the ACDM addressing the following security requirements: encryption of sensitive data (debit card and PIN), user authentication, physical security measures (against tampering), network security, and fraud detection. | 10 | L3 | CO1 |
| | b. | You are tasked with securing a communication system for a financial application that processes 1 million transactions per day, using a 128-bit key block cipher. The organization is concerned about potential attacks on the encryption system. Apply the two general approaches used in attacking a cipher by identifying specific techniques used for each approach. Additionally, categorize the different types of cryptanalytic attacks based on the information available to the attacker. | 10 | L3 | CO1 |
| | | **OR** | | | |
| Q2 | a. | Make use of Hill Cipher Technique to encrypt the plain text given below:<br>Plain text: **Paymoremoney** using the key:<br>$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$ | 10 | L3 | CO1 |
| | b. | Apply the Playfair cipher to encrypt the following:<br>**Keyword: MONARCHY Plain Text: CRYPTOGRAPHY**<br>Explain the rules of the Playfair cipher as you work through the example, and demonstrate the step-by-step process of generating the ciphertext. | 10 | L3 | CO1 |
| | | **Module- 2** | | | |
| Q3 | a. | Apply the principles of Feistel ciphers and key scheduling algorithms to decrypt the following ciphertext using a single query to an encryption oracle:<br>**3F1A2B6C8D9EFA7BFE4C3D2A1B4F6E8D.** | 10 | L3 | CO2 |

| | | | | | |
|---|---|---|---|---|---|
| | | Assume a Feistel cipher with 16 rounds, a block length of 128 bits, and a key length of 128 bits, where the round keys for rounds 9 to 16 are the reverse of the keys used in rounds 1 to 8. Explain how this approach demonstrates a vulnerability to a chosen plaintext attack. | | | |
| | b. | You are a security engineer tasked with implementing the AES encryption process for a secure communication system in a financial application. Your goal is to ensure that all sensitive data, including user transactions and account details, is encrypted before being transmitted or stored. Given the scenario, how would you apply the AES encryption process to encrypt the given plaintext.<br>**Plaintext: FinancialData123**<br>**Key: SecureKey12345678**<br>Illustrate the steps with a block diagram and provide a detailed explanation of each step in the process. | 10 | L3 | CO2 |
| | | **OR** | | | |
| Q4 | a. | You are working as a cryptography expert for a legacy system that still uses the Data Encryption Standard (DES) for encryption. Your task is to model the general structure of the DES encryption algorithm and encrypt a the given 64-bit plaintext block using a specified 64-bit key.<br>Given the details:<br>**Plaintext**: You are given a 64-bit plaintext block to encrypt. For this scenario, the plaintext in binary is 11010011 10010100 11010001 00100010 01010101 10101010 11110000 01101101.<br>**Key**: The 64-bit key provided for encryption is 10101011 00110100 11110000 11001100 10101010 01100110 11110000 10101010.<br>Construct a block diagram that illustrates the overall structure of the DES encryption process, highlighting each step. | 10 | L3 | CO2 |
| | b. | You are a network security specialist tasked with securing a communication channel between two parties: Alice and Bob. They need to exchange sensitive messages over the internet, but the communication channel is vulnerable to tampering and unauthorized access. Your goal is to implement a Message Authentication Code (MAC) to ensure the integrity and authenticity of the messages exchanged between Alice and Bob.<br>**Scenario Details:**<br>1. **Message Exchange**:<br>o Alice wants to send a message to Bob: "Transfer Rs.5000 to account XYZ."<br>o Both Alice and Bob share a secret key known only to them: SecretKey123.<br>2. **Threats**:<br>o An attacker on the network may intercept and modify the message during transmission.<br>o The attacker could also attempt to send a forged message pretending to be Alice.<br>Based on the scenario, describe how you would apply the principles of Message Authentication Code (MAC) to secure the communication between Alice and Bob. | 10 | L3 | CO2 |
| | | **Module - 3** | | | |
| Q5 | a. | A retail company's e-commerce website allows customers to log in using their email address and password. Recently, there has been a significant increase in unauthorized access to customer accounts.<br>**Identify** the type of attack that occurred in this scenario and construct the working of such attacks to bypass the authentication system. Also r**ecommend** defensive | 10 | L3 | CO2 |

| | | | | | |
|---|---|---|---|---|---|
| | | measures to prevent these types of attacks in the future, ensuring that the system properly handles user inputs and prevents unauthorized access. | | | |
| | b. | A major online food delivery service provider handles thousands of orders every hour. Recently, the company's website and mobile application experienced multiple outages, particularly during peak hours. Customers were unable to place orders, resulting in significant revenue loss and damage to the company's reputation. **Identify** the type of attack described in this scenario and model the working of such attacks to overwhelm the company's infrastructure. **Recommend** strategies and defensive measures the company should implement to protect its website and mobile application from similar kind of attacks in future. | 10 | L3 | CO2 |
| **OR** | | | | | |
| Q6 | a. | A mid-sized company recently suffered a data breach due to a combination of IP spoofing and phishing attacks, resulting in the exposure of 10,000 customer records. Following the breach, the company's stock price dropped by 15%.<br>Apply risk management principles to develop a defense strategy against future IP spoofing and phishing attacks. Identify the layers of security that should be implemented, including network defense, user education, and monitoring systems to detect and mitigate such attacks before they can cause harm. | 10 | L3 | CO3 |
| | b. | An investment firm managing ₹2000 crore in assets noticed unusual network activity where financial data was being intercepted without disruption, followed by a series of unauthorized modifications to financial records. Identify the type of attacks involved in this scenario. Distinguish between these two types of attacks faced by the firm. Analyze the potential impact of each attack type on the confidentiality, integrity, and availability of the firm's financial data. Propose methods to mitigate both attack types and prevent future occurrences. | 10 | L3 | CO3 |
| **Module - 4** | | | | | |
| Q7 | a. | A pharmaceutical company, which is developing a new drug projected to generate ₹500 crore in revenue, recently noticed that confidential research and development data related to the drug had been leaked online. Upon further investigation, it was discovered that unauthorized access to the company's internal network had occurred, and the data may have been sold to a competitor. As a result, the company's competitive advantage in the market is at risk, and they are facing significant financial and reputational damage. Identify the type of cyber-attack that the pharmaceutical company is facing and Recommend security measures the company should adopt to protect its sensitive data and prevent future incidents of this kind. | 10 | L3 | CO3 |
| | b. | An e-commerce company that generates ₹200 crore in annual revenue relies heavily on social media for marketing and customer engagement. Recently, customers began reporting suspicious activity on the company's official social media accounts. Fraudulent discount offers and links were posted, leading to customer accounts being compromised, and several customers reported falling victim to phishing attacks. Additionally, there has been a noticeable decline in customer trust, and the company's online sales have dropped by 10% in the past month. Identify the type of cyber security issue the company is facing with its social media marketing. Explain how this type of attack affects both the company and its customers. Recommend security measures the company should implement to safeguard its social media accounts and protect customers from future attacks. | 10 | L3 | CO3 |
| **OR** | | | | | |
| Q8 | a. | A large multinational company encourages employees to use internal social computing tools, such as collaboration platforms and social intranet networks, to share knowledge and resources across departments. However, several security incidents have occurred where sensitive corporate information was accidentally | 10 | L3 | CO3 |

| | | | | | |
|---|---|---|---|---|---|
| | | shared with unauthorized users, leading to data leaks and intellectual property exposure. Evaluate the challenges of using social computing tools within organizations and suggest security measures that can be implemented to reduce the risk of data leakage. | | | |
| | b. | A global retail company that processes over ₹500 crore in online sales annually has experienced a series of cyberattacks that disrupted its online payment systems. These attacks caused several hours of downtime during peak shopping periods, leading to an estimated ₹10 crore in lost sales. The company also faces potential fines due to non-compliance with payment data protection standards. Assess the financial and reputational impact of the cyberattacks on the organization. Recommend strategies the company should adopt to strengthen its cyber defenses, focusing on securing payment systems and ensuring compliance with industry standards like Payment Card Industry Data Security Standard (PCI-DSS). | 10 | L3 | CO3 |
| **Module - 5** | | | | | |
| Q9 | a. | A well-known Indian software company discovered that its proprietary software had been stolen and pirated by a competitor. The competitor reverse-engineered the software and sold it under a different name, causing significant financial losses and damaging the company's intellectual property rights. Identify the type of attack and explain how reverse engineering can be used to steal software. Analyze the case from a legal and ethical perspective, discussing the impact on the company's revenue and reputation. Suggest measures to protect such valuable data in the cyberspace. | 10 | L3 | CO4 |
| | b. | An online gambling site operating illegally in India was found to be using the dark web to attract users and evade detection by law enforcement. The site exploited the lack of clear regulations in India concerning online gambling and facilitated money laundering through cryptocurrency transactions, causing financial and social harm. Identify the type of cybercrime involved and explain how the dark web and cryptocurrency were used in this case. Analyze the broader implications of this crime for Indian society and propose regulatory and technological measures to prevent the growth of illegal online gambling operations. | 10 | L3 | CO4 |
| **OR** | | | | | |
| Q10 | a. | Several Indian banks recently reported a massive cyber theft where hackers stole millions of rupees by exploiting weaknesses in the banks' digital payment systems. Identify the type of techniques used by the attackers to obtain employee credentials and deployed malware to manipulate banking transactions and divert funds to foreign accounts. Analyze the case, highlighting the financial and reputational damage faced by the banks, and suggest measures that banks should take to prevent such attacks in the future. | 10 | L3 | CO4 |
| | b. | The official website of the Government was defaced by hackers who replaced the homepage with malicious content. Upon investigation, it was found that the attackers exploited vulnerabilities in the website's outdated content management system (CMS). The defacement embarrassed the government and undermined public trust in the security of official digital infrastructure. Identify the type of attack that occurred in this case and explain how such vulnerabilities are exploited. Analyze the potential impact of this attack on government credibility and propose security measures to prevent such defacements in the future. | 10 | L3 | CO4 |

*****