Reg.No.:												

VIVEKANANDHA COLLEGE OF ENGINEERING FOR WOMEN
[AUTONOMOUS INSTITUTION AFFILIATED TO ANNA UNIVERSITY, CHENNAI]
Elayampalayam – 637 205, Tiruchengode, Namakkal Dt., Tamil Nadu.

Question Paper Code: 50054

M.E. / M.Tech. DEGREE END-SEMESTER EXAMINATIONS – FEB. 2025
First Semester
Computer Science and Engineering
P23CSE27 – SECURITY PRINCIPLES AND PRACTICES
(Regulation 2023)

Time: Three Hours | Maximum: 100 Marks

Answer ALL the questions

Knowledge Levels (KL)	K1 – Remembering	K3 – Applying	K5 - Evaluating
	K2 – Understanding	K4 – Analyzing	K6 - Creating

PART – A

(10 x 2 = 20 Marks)

Q.No.	Questions	Marks	KL	CO
1.	Explain modular arithmetic and its application in cryptography.	2	K3	CO1
2.	Explain the difference between cryptography and cryptanalysis.	2	K2	CO1
3.	Write the differences between substitution and transposition ciphers.	2	K2	CO2
4.	What are the modes of operation for block ciphers?	2	K1	CO2
5.	State the principle behind public-key cryptography.	2	K1	CO3
6.	Discuss the significance of the modulus function in RSA cryptography.	2	K2	CO3
7.	How does TLS ensure data integrity during transmission?	2	K1	CO4
8.	Elaborate the role of a Certificate Authority (CA) in authentication.	2	K1	CO4
9.	Explain the role of incident response in computer security.	2	K1	CO5
10.	Define intellectual property in the context of software security.	2	K2	CO5

PART – B

(5 x 13 = 65 Marks)

Q.No.		Questions	Marks	KL	CO
11.	a)	Discuss the significance of probability in information security. Explain addition rules conditional probability, independent events with appropriate examples.	13	K2	CO1
		(OR)			
	b)	Elaborate the application of number theory in cryptographic algorithms. Illustrate with examples how prime numbers are utilized in public key cryptography.	13	K3	CO1
12.	a)	Discuss in detail the functioning of the AES algorithm. Explain its key features and how it improves over DES. Provide examples of how the modes of operation impact the encryption process.	13	K2	CO2
		(OR)			
	b)	Compare and contrast substitution and transposition ciphers by discussing their advantages and disadvantages. i. Encrypt the message "SECURITY" using a Caesar cipher with a shift of 3 (substitution cipher). ii. Encrypt the message "INFORMATION" using a columnar transposition cipher with 4 columns.	13	K3	CO2
13.	a)	Explain the Diffie-Hellman Key Exchange Protocol in detail. Discuss the mathematical foundations of the protocol and provide a step-by-step example, where two users (Alice and Bob) agree upon a shared secret using a prime number p=23 and a primitive root g=5. Demonstrate how the shared secret is computed.	13	K3	CO3
		(OR)			
	b)	Explain the combination of asymmetric and symmetric cryptography in secure communication systems, such as in hybrid cryptosystems. Describe how asymmetric cryptography can be used for key exchange, followed by symmetric encryption for actual data transmission using an example.	13	K2	CO3
14.	a)	Explain the Kerberos Authentication Protocol in detail and its working including the key components involved (Authentication Server, Ticket Granting Server, Client, and Service). Provide a step-by-step process of authentication, illustrating how tickets are used for secure communication.	13	K1	CO4
		(OR)			

	b)	Compare the Directory-Based Authentication Framework and the Non-Directory Based Public-Key Authentication Framework with the help of examples where each framework is used in real-world applications, such as in LDAP-based systems for the directory-based framework and SSH for non-directory-based authentication.	13	K3	CO4
15.	a)	Describe the computer crime and its impact on modern society including the different types of computer crimes, such as hacking, identity theft, and DDoS attacks. Provide real-world examples of significant cybercrimes, and analyze the steps organizations and governments take to mitigate such risks. Discuss the importance of incident response and the role of cybersecurity professionals in combating computer crime.	13	K1	CO5
		(OR)			
	b)	Discuss the ethical and legal challenges faced by organizations when balancing employee privacy and security monitoring. How should organizations handle these issues?	13	K2	CO5

PART – C

(1 x 15 = 15 Marks)

Q.No.		Questions	Marks	KL	CO
16.	a)	In an RSA cryptosystem, let the public key (e, n) be e=7 and n=55. i. Compute the private key d if $d \times e \equiv 1 \, mod \, \phi(n)$, where $\phi(n) = (p-1)(q-1)$. ii. Encrypt the message m=9 and compute the ciphertext using $c = m^e \, mod \, n$.	15	K5	CO1
		(OR)			
	b)	A major financial institution experienced a data breach where sensitive customer information was stolen. After an investigation, it was revealed that the attackers exploited weaknesses in the bank's asymmetric encryption system, particularly focusing on the RSA key management process. i. Analyze the possible causes of the breach related to RSA and asymmetric cryptography. Discuss the vulnerabilities that might have led to this incident. ii. Propose a comprehensive security framework to mitigate such vulnerabilities in the future, focusing on key management, encryption protocols, and user training.	15	K4	CO3