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: 50037

M.E. / M.Tech. DEGREE END-SEMESTER EXAMINATIONS – JAN. 2025
Third Semester
Computer Science and Engineering
P23CSE19 – INFORMATION SECURITY
(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.	List out what are the attacks that can be performed in the network.	2	K1	CO1
2.	Spell the need for CIA triad?	2	K1	CO1
3.	Why do we need Diffie-Hellman algorithm?	2	K2	CO2
4.	Differentiate between symmetric key cryptography and public key cryptography.	2	K2	CO2
5.	Differentiate between IP spoofing and sniffing.	2	K2	CO3
6.	Differentiate between SSL connection and SSL session.	2	K2	CO3
7.	What is OS fingerprinting?	2	K1	CO4
8.	List the various cybercrimes against property and against organization	2	K1	CO4
9.	What is web application security?	2	K1	CO5
10.	How to differentiate privacy and anonymity?	2	K2	CO5

PART – B

(5 x 13 = 65 Marks)

Q.No.		Questions	Marks	KL	CO
11.	a)	Explain various types of security attacks.	13	K1	CO1
		(OR)			
	b)	List the different levels of losses that occur without CIA triad and briefly explain.	13	K1	CO1
12.	a)	AES consists of four functions in three layers. Which of these layers and functions are primarily for confusion and which are primarily for diffusion? Justify your answer.	13	K3	CO2
		(OR)			
	b)	Explain RSA algorithm. Perform encryption and decryption using RSA (p = 3, q = 11, e = 7, M = 5).	5 + 8 = 13	K3	CO2
13.	a)	Describe the differences between a host-based IDS and a network-based IDS. How can their advantages be combined into a single system?	8 + 5 = 13	K3	CO3
		(OR)			
	b)	A PGP user may have multiple public keys so that a recipient knows which public key is being used by a sender. A key ID consisting of the least significant 64 bits of the public key is sent with the message. What is the probability that a user with N public keys will have at least one duplicate key ID?	13	K4	CO3
14.	a)	Describe the classification of Social Engineering with examples.	13	K2	CO4
		(OR)			
	b)	Explain in detail the Digital Forensics lifecycle.	13	K2	CO4
15.	a)	Illustrate the fundamental concepts in privacy policies.	13	K2	CO5
		(OR)			
	b)	Briefly explain privacy in the following domains: • Health care • Finance.	6.5 + 6.5 = 13	K2	CO5

PART – C

(1 x 15 = 15Marks)

Q.No.		Questions	Marks	KL	CO
16.	a)	Explain how does screened host architectures for firewalls differ from screened subnet firewall architectures? Which of these offers more security for the information assets that remain on the entrusted network?	10 + 5 = 15	K2 K4	CO3
		(OR)			
	b)	The IPsec architecture document states that when two transport mode Security Association (SAs) are bundled to allow both AH and ESP protocols on the same end-to-end flow; only one ordering of security protocols seems appropriate: performing the ESP protocol before performing the AH protocol. Why is this approach recommended rather than authentication before encryption?	15	K4	CO3