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: 50012

B.E. / B.Tech. DEGREE END-SEMESTER EXAMINATIONS – NOV. / DEC. 2024
Seventh Semester
Computer Science and Engineering
U19CSV23 – CRYPTOGRAPHY AND NETWORK SECURITY
(Regulation 2019)

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 the categories of passive and active security attacks.	2	K3	CO1
2.	Identify the difference between a block cipher and a stream cipher.	2	K3	CO1
3.	Contrast between diffusion and confusion.	2	K3	CO2
4.	Infer the purpose of the State array.	2	K2	CO2
5.	List types of attacks addressed by message authentication.	2	K1	CO3
6.	State the difference between direct and arbitrated digital signatures.	2	K2	CO3
7.	Outline the major issue in end-to-end key distribution.	2	K2	CO4
8.	What is a suppress-replay attack?	2	K2	CO4
9.	Find the protocols comprise TLS.	2	K1	CO5
10.	List the key characteristics of firewalls.	2	K1	CO5

PART – B

(5 x 13 = 65 Marks)

Q.No.			Questions	Marks	KL	CO
11.	a)	i.	Consider an automated cash deposit machine in which users provide a card or an account number to deposit cash. Give examples of confidentiality, integrity, and availability requirements associated with the system, and, in each case, indicate the degree of importance of the requirement.	8	K3	CO1
		ii.	Repeat the above problem for a payment gateway system where a user pays for an item using their account via the payment gateway.	5		
			(OR)			
	b)	i.	What is the encryption algorithm?	3	K2	CO1
		ii.	How secure is it?	4		
		iii.	To make the key distribution problem simple, both parties can agree to use the first or last sentence of a book as the key. To change the key, they simply need to agree on a new book. The use of the first sentence would be preferable to the use of the last. Why?	6		
12.	a)		Explain simplified DES with an example.	13	K2	CO2
			(OR)			
	b)		Compare AES to DES. For each of the following elements of DES, indicate the comparable element in AES or explain why it is not needed in AES.		K3	CO2
		i.	XOR of subkey material with the input to the f function	3		
		ii.	XOR of the f function output with the left half of the block	3		
		iii.	f function	3		
		iv.	permutation P	4		
13.	a)		Alice wants to send a single bit of information (a yes or a no) to Bob by means of a word of length 2. Alice and Bob have four possible keys available to perform message authentication. The following matrix shows the 2-bit word sent for each message under each key:		K3	CO3

	Message	
Key	0	1
1	00	11
2	01	10
3	10	01
4	11	00

i. The preceding matrix is in a useful form for Alice. Construct a matrix with the same information that would be more useful for Bob. 7

ii. What is the probability that someone else can successfully impersonate Alice? 3

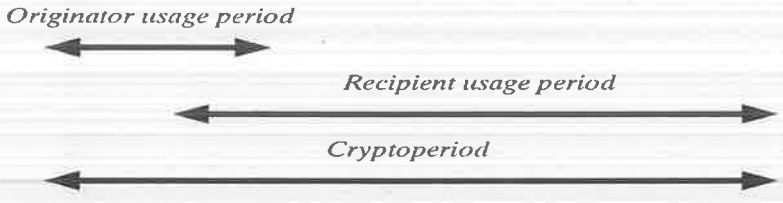
iii. What is the probability that someone can replace an intercepted message with another message successfully? 3

(OR)

b) DSA specifies that if the signature generation process results in a value of s = 0, a new value of k should be generated and the signature should be recalculated. Why? 7 K3 CO3

What happens if a k value used in creating a DSA signature is compromised? 6

14. a) NIST defines the term cryptoperiod as the time span during which a specific key is authorized for use or in which the keys for a given system or application may remain in effect. One document on key management uses the following time diagram for a shared secret key. 13 K3 CO4



Explain the overlap by giving an example application in which the originator's usage period for the shared secret key begins before the recipient's usage period and also ends before the recipients usage period.

(OR)

b) i. Explain remote user authentication principles. 7 K2 CO4

ii. Write a note on Kerberos. 6

15. a) Explain the key features of intrusion detection systems. 8 K2 CO5

Explain the role of firewalls as part of a computer and network security strategy 5

(OR)

b)	Is SSL or TLS more secure to a man-in-the-middle attack? Can an intruder create key material between the client and herself and between the server and herself?	13	K3	CO5

PART – C

(1 x 15 = 15 Marks)

Q.No.		Questions	Marks	KL	CO
16.	a)	List threats to Web security and describe how each is countered by a particular feature of TLS.	15	K3	CO5

(OR)

	b)	Explain, How to handle social engineering attacks with managing password? i. Users Alice and Bob use the Diffie-Hellman key exchange technique with a common prime q = 83 and a primitive root $\alpha = 5$. If Alice has a private key $X_A = 6$, what is Alice's public key Y_A? ii. If Bob has a private key $X_B = 10$, what is Bob's public key Y_B? iii. Construct the shared secret key.	15	K3	CO5