Register No: | | | | | | | | |

Sri Sivasubramaniya Nadar College of Engineering, Kalavakkam – 603 110

(An Autonomous Institution, Affiliated to Anna University, Chennai)

B.E. / B.Tech. End Semester Theory Examinations, Nov / Dec 2021

Fifth Semester

Computer Science and Engineering

UCS1505 INTRODUCTION TO CRYPTOGRAPHIC TECHNIQUES

(Regulations 2018)

Time: **Three Hours** **Answer ALL Questions** Maximum:**100 Marks**

K1: Remembering K2: Understanding K3: Applying K4 :Analyzing K5: Evaluating

PART – A (10 × 2 = 20 Marks)

01.	K2	List some guarantees the cryptographic expert provide for their security protocols.	CO1
02.	K2	How the utilization of computing power is connected to adversary?	CO1
03.	K2	Summarize the properties of hash function.	CO2
04.	K2	Can Bob construct or choose his tag in verification process of MAC? Justify.	CO2
05.	K1	What is avalanche effect?	CO3
06.	K2	Is one way function, difficult or easy for adversary ? Why?	CO3
07.	K2	List the attacks of Diffie-helman key exchange protocol.	CO4
08.	K2	Alice and bob develop a shared key and use it. Can an adversary access the shared key?	CO4
09.	K2	Illustrate with a diagram to represent the public key usage to communicate message from alice to bob.	CO5
10.	K2	Distinguish between private and public key usage to communicate message from Alice to Bob.	CO5

PART – B (5 × 6 = 30 Marks)

11.	K2	Outline the definition for private key encryption and decryption scheme.	CO1
12.	K2	MAC is uniformly distributed. Apply on 3-bit tag and show the outcomes.	CO2
13.	K2	Classify the advantages of using pseudo random numbers in cryptography.	CO3
14.	K2	Depict the relationship between Alice and Bob, when they apply Dieffie-helman key exchange protocol to exchange the messages between them.	CO4

15.	K2	Outline a definition for public key encryption and decryption scheme.	CO5

PART – C (5 × 10 = 50 Marks)

16.	K3	Show that the shift ciphers are all trivial to break using a chosen-plaintext attack. Determine how much chosen plaintext is needed to recover the key for each of the ciphers?	CO1
		OR	
17.	K3	Prove or refute: An encryption scheme with message space M is perfectly secret if and only if for every probability distribution over M and every c_0, $c_1 \in C$ we have $Pr[C = c_0] = Pr[C = c_1]$.	CO1
18.	K3	Let F be a pseudorandom function. Justify that the following MAC for messages of length $2n$ is insecure: *Gen* outputs a uniform $k \in \{0, 1\}^n$. To authenticate a message $m_1 \parallel m_2$ with $\lvert m_1 \rvert = \lvert m_2 \rvert = n$, compute the tag $F_k(m_1) \parallel F_k(F_k(m_2))$.	CO2
		OR	
19.	K3	Assume collision-resistant hash functions exist and provide the definition of the same. Show a construction of a fixed-length hash function (Gen, *h*) that is not collision resistant.	CO2
20.	K3	Prove that from the output of the SPN and the key, it is possible to recover the input.	CO3
		OR	
21.	K3	Demonstrate the three round feistal network, for *l*-bit input to the network produces l-bit output.	CO3
22.	K3	Apply Euler totient function for the following and state any six reasons why prime numbers play a significant role in cryptography. a. $\phi(29)$ b. $\phi(51)$ c. $\phi(455)$ d. $\phi(616)$	CO4
		OR	
23.	K3	How the Dieffie hellman key exchange protocol generate the shared key between sender and receiver? Interpret how shared key is exchanged, when q=17, g=4(primitive root), with X_A=3, X_B=6.	CO4
24.	K3	Outline the steps used to derive the private and public key in RSA encryption scheme and find the keys when N=33 with e=7 ?	CO5

OR			
25.	K3	Summarize the steps used in RSA digital signature and enumerate at least five applications where this scheme is best suitable. Also, discuss the order of using signature and encryption.	CO5

Course Outcomes:

CO1: Describe and implement classical and symmetric ciphers.
CO2: Describe the authentication schemes and hash algorithms.
CO3: Understand the number theoretic foundations of cryptography.
CO4: Compare and contrast various public key cryptographic techniques.
CO5: Illustrate various public key cryptographic techniques.