Register Number

Sri Sivasubramaniya Nadar College of Engineering, Kalavakkam – 603 110

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

Department of Computer Science and Engineering

Continuous Assessment Test – I

Question Paper

Degree & Branch	B.E CSE				**Semester**	V
Subject Code & Name	UCS1505 & INTRODUCTION TO CRYPTOGRAPHIC TECHNIQUES				**Regulation: 2018**	
Academic Year	2022-23 ODD	**Batch**	2020-24	**Date**	**21.09.2022**	**FN**
Time: 8.15 – 9.45 AM (90 Minutes)	**Answer All Questions**				**Maximum: 50 Marks**	

Part – A (6×2 = 12Marks)

K2	1. Outline the formal definition of the Gen, Enc, and Dec algorithms for the mono-alphabetic substitution cipher.	CO1	1.4.1
K2	2. Show how many keys are required for two people to communicate via symmetric and asymmetric ciphers?	CO1	1.3.1
K3	3. Apply the Vigenère cipher and decrypt the ciphertext VEQPJIREDOZXOE with the key café.	CO1	1.4.1
K2	4. Outline Kerchoff's principle and justify it.	CO1	1.3.1 1.4.1
K3	5. Compare and contrast the encryption, MAC and Hash functions	CO2	1.3.1 2.4.3
K2	6. Summarize the properties of hash function.	CO2	1.4.1

Part – B (3×6 = 18 Marks)

K3	7. Caesar wants to arrange a secret meeting with Marc Antony, either at the Tiber (the river) or at the Coliseum (the arena). He sends the shift cipher text EVIRE. However, Antony does not know the key, so he tries all possibilities. Apply the appropriate decryption algorithm and deduce where he will meet Caesar?	CO1	1.4.1 13.3.1
K3	8. Assume an attacker knows that a user's password is either $abcd$ or $bedg$. Say the user encrypts his password using the shift cipher, and the attacker sees the resulting ciphertext. Apply the appropriate decryption algorithm and show how the attacker can determine the user's password or explain why this is not possible.	CO1	1.4.1 13.3.1
K2	9. Outline the formal definition for the construction of CBC MAC with proper illustration.	CO2	1.4.1 13.3.1

Part – C (2×10 = 20 Marks)

K3	10. Let (E, D) be a semantically secure cipher with key space $K = \{0,1\}^l$. A bank wishes to split a decryption key $k \in \{0,1\}^l$ into two pieces p_1 and p_2 so that both are needed for decryption. The piece p_1 can be given to one executive and p_2 to another so that both must contribute their pieces for decryption to proceed. The bank generates random k_1 in $\{0,1\}^l$ and sets $k_1' \leftarrow k \oplus k_1$.	CO1	1.4.1 13.3.1

Note that $k_1 \oplus k_1' \rightarrow k$. The bank can give k_1 to one executive and k_1' to another. Both must be present for decryption to proceed since, by itself, each piece contains no information about the secret key k (note that each piece is a one-time pad encryption of k).
Now, suppose the bank wants to split k into three pieces p_1, p_2, p_3 so that any two of the pieces enable decryption using k. This ensures that even if one executive is out sick, decryption can still succeed. To do so the bank generates two random pairs (k_1, k_1') and (k_2, k_2') as in the previous paragraph so that $k_1 \oplus k_1' = k_2 \oplus k_2' = k$.
Solve the given problem and show how the bank assign pieces, so that any two pieces enable decryption using k, but no single piece can decrypt?
Check whether this combination of the keys $p_1 = (k_1, k_2), p_2 = (k_1'), p_3 = (k_2')$works, if not provide the correct combination.

OR

K3

11. Apply the concept of perfect secrecy and prove that the cryptosystem built is perfectly secure?

$$P(X=a) = \frac{1}{2}, P(X=b) = \frac{1}{3}, P(X=c) = \frac{1}{6},$$

$$P(K=k_1) = P(K=k_2) = P(K=k_3) = \frac{1}{3}$$

Plaint text $P = \{a, b, c\}$, Cipher text $C = \{1,2,3,4\}$

Encryption Matrix

	a	b	c
k1	1	2	3
k2	2	3	4
k3	3	4	1

CO1

1.4.1
13.3.1

K3

12. Consider the shift cipher, but with the following distribution over M:

$$\Pr[M = kim] = 0.5, \Pr[M = ann] = 0.2, \Pr[M = boo] = 0.3$$

Solve the problem and compute the probability for $C = DQQ$?
Also prove or Refute: For every encryption scheme that is perfectly secret it holds that for every distribution over the message space M, every $m, m^1 \in M$and every $c \in C$: $\Pr[M = m | C = c] = \Pr[M = m' | C = c]$.

CO2

1.3.1
13.3.1

OR

K3

13. Alice wants to send a message M with a message authentication code MAC(M) to Bob. Alice and Bob share a secret key k and have agreed on using a specific algorithm MAC function which takes input parameters M and k to produce MAC(M).
a. Apply the MAC algorithm and outline the steps that Alice must follow for sending M and the steps that recipient Bob must follow for verifying the authenticity of M.
b. Make of use the principle of MAC and explain why the MAC proves to Bob that a received message is authentic, and why Bob is unable to prove to a third party that the message is authentic.

CO2

1.3.1
13.3.1

Prepared By	Reviewed By	Approved By
V. M 13/9/22	13/9/22	13/9/22
Course Coordinator	PAC Team	HOD