


Name:			
Enrolment No:			
UPES End Semester Examination, Dec 2024			
Course: Cyber Security Program: MCA Course Code: CSCS8009P		Semester: III Time : 03 hrs. Max. Marks: 100	
Instructions:			
SECTION A (5Qx4M=20Marks)			
S. No.		Marks	CO
Q 1	Discuss the importance of the Confidentiality, Integrity, and Availability (CIA) triad in the design of a security system.	4	CO1
Q 2	Explain the concept of non-repudiation. Why is it critical in secure communication and digital transactions?	4	CO1
Q 3	Explain the concept of a social engineering attack. How do attackers exploit human psychology to breach security?	4	CO2
Q 4	Encrypt the plaintext "MEETMEAFTERNOON" using a Rail Fence cipher with 2 and 3 rails.	4	CO3
Q 5	Analyse the potential weaknesses in a network that lacks a firewall.	4	CO4
SECTION B (4Qx10M= 40 Marks)			
Q 6	Classify cyber-attacks into categories such as malware, phishing, denial of service (DoS), and advanced persistent threats (APTs). Explain each with examples.	10	CO1
Q 7	How do threats from viruses, worms, and Trojans differ? Provide examples to highlight their unique behaviors and impact.	10	CO2
Q 8	Differentiate between snooping, spoofing, and sniffing attacks. Provide examples of each and their implications on cybersecurity.	10	CO2
Q 9	Describe RSA Cryptosystem. Using RSA, encrypt the message $M = 3$, assuming the two primes chosen to generate the keys are $p = 13$ and $q = 7$. You should choose a value $e < 10$. Show your calculations and assumptions.	10	CO3

SECTION-C
(2Qx20M=40 Marks)

Q 10	Explain the working principle of public key cryptography and how it ensures both confidentiality and authentication. Compare it with symmetric key cryptography, focusing on security, key management, and computational overhead.	20	CO3, CO4
Q 11	<p>Explain the fiestal function F in the DES encryption process, detailing how it combines the subkey and plaintext block to ensure security. Additionally, describe the key generation process in DES, including how the 2 subkeys are derived from the initial key and the roles of permutation and compression. Use a detailed example to illustrate your explanation. (You can take your own value to demonstrate the explanation)</p> <p>OR</p> <p>Compare and contrast direct and arbitrated digital signatures, focusing on their working mechanisms, strengths, and limitations in ensuring secure communications. Discuss the role of a trusted third party in enhancing the security of arbitrated digital signatures and illustrate this with a detailed practical example. Include scenarios where each type is best suited.</p>	20	CO3, CO4