Total No. of Printed Pages: 2

PRN No.	

PAPER CODE	U313-215-A-ESE

December 2023 (ENDSEM) EXAM

TY (SEMESTER - I)

COURSE NAME: CYBER SECURITY **Branch: AI&DS** **COURSE CODE: ADUA31205 (A)**

(PATTERN 2020)

Time: [1Hr. 30 Min] **[Max. Marks: 40**

(*) Instructions to candidates:

1) **Figures to the right indicate full marks.**
2) **Use of scientific calculator is allowed**
3) **Use suitable data wherever required**
4) **All questions are compulsory. Solve any one sub question from Question 3 and any tw sub questions each from Questions 4,5 and 6 respectively.**

Q. No.	Question Description	Max. Marks	CO mapped	BT Level
Q.1	a) Can you explain what authorization means in the context of computer security and access control?	[2]	CO1	L2 Explain
Q2	a) Evaluate: Ceaser Cipher for plain text "Sun rises in the East"	[2]	CO3	L3 Evaluate
Q3.	a) Solve using Diffie-Hellman Algorithm p=353, q=3, a=97 and b=233.	[6]	CO3	L3 Evaluate
	b) Calculate Cipher text using RSA algorithm: Prime numbers p=13 and q= 17 and plain text to be send is 12. Public key e is 19.	[6]	CO3	L3 Evaluate
Q.4	a) Create a detailed block diagram illustrating the key components of the MD5 algorithm. Provide a step-by-step explanation of the MD5 algorithm, referring to your block diagram.	[5]	CO2	L4 Analyse
	b) Create a detailed block diagram illustrating the key components of the SHA algorithm. Provide a step-by-step explanation of the SHA algorithm, referring to your block diagram.	[5]	CO5	L4 Analyse
	c) Describe the basic idea behind Cipher Block Chaining and justify how it is employed in hash functions.	[5]	CO6	L2 Understand
Q.5	a) Describe the concept of digital signatures, Public-Key Infrastructure (PKI) and its significance in facilitating secure communication over untrusted networks.	[5]	CO5	L3 Apply
	b) Compare and contrast the key management approach in asymmetric cryptosystems with that of symmetric cryptosystems.	[5]	CO2	L4 Compare
	c) Imagine you are leading a team of researchers in the			

	field of quantum information science. Your goal is to pioneer a groundbreaking advancement in quantum key cryptography and dynamic key management. Propose a revolutionary advancement in quantum key cryptography that goes beyond current paradigms.	[5]	CO5	L6 Develop
Q.6)	a) Differentiate between intrusion detection and intrusion prevention systems. Evaluate the importance of effective password management in securing digital systems.	[5]	CO2	L3 Execute
	b) Discuss how viruses and worms typically exploit vulnerabilities in systems and the potential impact on infected devices. Justify by Providing examples of real-world incidents where each type of malware has been particularly problematic.	[5]	CO3	L5 Justify
	c) Analyze the strategies and technologies commonly employed to mitigate the impact of DDoS attacks. Discuss the role of network infrastructure, traffic analysis, and mitigation techniques in preventing or minimizing the effects of DDoS incidents.	[5]	CO4	L4 Examine