Total No. of Printed Pages: 2

PRN No.	

PAPER CODE	U314-215-A (ESE)

(AY:2024-25) December 2024 (ENDSEM) EXAM

TY (SEMESTER - I)

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

T.Y PATTERN (2020 R1)

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

(*) Instructions to candidates:

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

Q. No.	Question Description	Max. Marks	CO mapped	BT Level
Q.1	a) Explain any 4 Security Mechanisms in brief.	[4]	CO1	L2 Understand
	b) How would you describe the concept of non-repudiation in the context of information security, and why is it important in digital communication?	[4]	CO3	L3 Applying
	c) Draw the Model of Network Security and give brief explanation.	[4]	CO1	L4 Analysis
Q2	a) i) Evaluate: Ceaser Cipher for plain text "Sun rises in the East". ii) Evaluate: Rail fence for plain text "be careful while chatting".	[4]	CO3	L5 Evaluate
	b) Compare and contrast the substitution and transposition techniques used in symmetric ciphers.	[4]	CO2	L4 Analysis
	c) Sketch and present the internal structure of single round of DES algorithm.	[4]		L2 Understand
Q3	a) Explain why large prime numbers are crucial in the security of the RSA algorithm. OR	[2]	CO5	L3 Apply
	b) Compare the efficiency of elliptic curve cryptography (ECC) with traditional public-key algorithms like RSA in terms of key size and security level.	[2]	CO2	L3 Apply
	c) Evaluate using Diffie-Hellman key exchange process to find a shared secret given the base g=3, prime p=11, and private keys a=2, b=3.	[4]	CO3	L5 Evaluate
Q4	a) Describe how Cipher Block Chaining (CBC) is used to construct a hash function. OR	[2]	CO1	L2 Understand

	b)Distinguish between MD5 and SHA-1 algorithms.(Any 4 Points) c) Draw a detailed block diagram illustrating the key components of the MD5 algorithm.	[2] [4]	CO2 CO1	L2 Understand L6 Design
Q.5	a) How does a Certificate Authority (CA) hierarchy enhance trust in digital certificates within PKI? OR b) Explain how a digital signature provides both authentication in a message. c) Explain how you would integrate the principles of X.509 standard, the concepts of PKIX, and the significance of Public-Key Certificates to ensure secure communication and identity verification across the organization.	[2] [2] [4]	CO6 CO6 CO5	L2 Understand L2 Understand L5 Synthesize
Q.6	a) How do worms differ from viruses in terms of their replication and spread mechanisms? OR b) How would you analyze the effectiveness of signature-based versus anomaly-based intrusion detection systems in identifying new attack vectors? c) Describe a common method to mitigate a DDoS attack in a cloud computing environment.	[2] [2] [4]	CO4 CO2 CO2	L2 Understand L2 Understand L4 Analysis

--All the best--