Total No. of Printed Pages: 2

PRN No.	

PAPER CODE	U315-214B (ESE)

(AY:2025-26) December 2025 (ENDSEM) EXAM

TY (SEMESTER - I)

COURSE NAME: Cyber Security **Branch: AI & DS** **COURSE CODE: AD31234B**

T.Y (Pattern 2023)

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 non-repudiation in information security and why it matters in digital communication.	[4]	CO1	L2 Explain
	b) Analyze the potential risks and vulnerabilities associated with a poorly secured computer network. How might these impact an organization's operations and data integrity?	[4]	CO1	L4 Analyze
	c) Evaluate the effectiveness of an employee security awareness program. What key elements ensure its success, and how can it be improved to strengthen organizational security?	[4]	CO1	L3 Evaluate
Q2	a) A plaintext was encrypted with a Caesar cipher with a shift of 7 (A maps to H). The resulting ciphertext is: **"Kvu'a qbknl h ivvr if paz jvcly".** What was the original plaintext?	[4]	CO2	L3 Evaluate
	b) Compare and contrast the substitution and transposition techniques used in symmetric ciphers. (Any 4 points)	[4]	CO2	L4 Compare
	c) Explain the substitution-permutation structure in DES and its role in ensuring the algorithm's security and efficiency.	[4]	CO2	L3 Apply
Q3	a) How RSA Algorithm is useful for Key management?	[2]	CO3	L2 Explain
	OR			
	b) What are the two key principles underlying a public-key cryptosystem?	[2]	CO3	L2 Explain
	c) Evaluate using Deffie-Hellman: Given- n = 17, a = 5, Private key of Alice = 4, Private key of Bob = 6	[4]	CO3	L3 Evaluate

Q4	a) List any two important applications of cryptographic hash functions. OR	[2]	CO4	L2 Explain
	b) Differentiate between SHA-1 and SHA-2 in terms of output length and security.	[2]	CO4	L4 Compare
	c) Create a detailed block diagram illustrating the key components of the SHA algorithm and provide a step-by-step explanation of the algorithm	[4]	CO4	L4 Analyze
Q.5	a) What is the role of X.509 in PKI? OR	[2]	CO5	L2 Explain
	b) What is meant by a CA hierarchy, and why is it used?	[2]	CO5	L2 Explain
	c) Compare and contrast the key management approach in asymmetric cryptosystems with that of symmetric cryptosystems. (Any 6 points)	[4]	CO5	L4 Compare
Q.6	a) What is a Distributed Denial of Service (DDoS) attack, and why is it difficult to prevent? OR	[2]	CO6	L2 Explain
	b) Define IoT security and state one key vulnerability in IoT devices.	[2]	CO6	L2 Explain
	c) Differentiate between intrusion detection and intrusion prevention systems. (Any 6 points)	[4]	CO6	L4 Compare