

Total No. of Printed Pages: 02

PRN No.	
---------	--

PAPER	AI → U315-244A (ESE)
CODE	AIML → U315-254A (ESE)

(AY:2025-26) December 2025 (ENDSEM) EXAM
TY (SEMESTER - I)

COURSE NAME:
INFORMATION SECURITY

Branch: CSE-AIML and CSE-AI COURSE CM31234A,
CODE: CA31234A
(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) Determine how security mechanism incorporated with OSI security services.	[4]	1	2
	b) Elaborate important considerations for developing Information security policy.	[4]	1	2
	c) Ensure how security goal is maintained with Information security policy	[4]	1	2
Q2	a) Design and explain biometric system architecture with suitable example.	[4]	2	2
	b) Analyze how an attacker might exploit piggybacking, and suggest preventive mechanisms.	[4]	2	2
	c) Explain how Shoulder Surfing exploits personal data and suggest preventive mechanisms.	[4]	2	2
Q3	a) Demonstrate Playfair cipher for the encryption of 'SECRET' using key "KEYWORD".	[2]	3	3
	OR b) Generalize the steganography with suitable example	[2]	3	3
	c) Construct the counter mode from block cipher modes of operation.	[4]	3	3
Q4	a) Compute key exchange algorithm for $p = 23$, $g = 5$ and $a = 6$ to obtain shared secret key.	[2]	4	3
	OR b) Differentiate between AES and DES in cryptography	[2]	4	3
	c) Validate how the authenticity and integrity of a message or document in cryptographic hash function.	[4]	4	3

Q.5	a) Explain SSL Record Protocol from SSL protocols. OR	[2]	5	2
	b) Differentiate between packet-filter firewalls and stateful firewalls.	[2]	5	2
	c) Ensure how an email message is encrypted using public key cryptography in S/MIME.	[4]	5	2
Q.6	a) Explain the cyberstalking with suitable examples. OR	[2]	6	2
	b) Mention two major challenges faced by the Indian IT Act in addressing cybercrime.	[2]	6	2
	c) A company suspects that an employee is involved in cyber defamation and unauthorized data access. Suggest suitable cyber law provisions and preventive measures that can be applied to handle this situation.	[4]	6	2

Note: 1 - Remember, 2 - Understanding, 3 - Apply, 4 - Analyze, 5 - Evaluate, 6 - Create