Total No. of Printed Pages: 02

PRN No.	

PAPER CODE	U315-284B (CESE)

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

TY/ (SEMESTER -I)

COURSE NAME: Information Security

Branch: CE (Software Engineering)

COURSE CODE: SE31234B

(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) What is cryptology? List and briefly types of attacks	[4]	CO1	BT2
	b) What is the need of authorization and authentication	[4]	CO1	BT2
	c) What is the main purpose of Access Control in networks?	[4]	CO1	BT1
Q2	a) Explain Double DES with diagram.	[4]	CO2	BT2
	b) Briefly define the Caesar cipher and limitation of this type.	[4]	CO2	BT1
	c) Explain Advance Encryption Standard (AES).	[4]	CO2	BT2
=Q3	a) What is RSA? Assume prime number p=? and q=? perform encryption and decryption in RSA.	[2]	CO3	BT1
	OR	[2]	CO3	BT2
	b) Write a short note on key management		CO3	BT2
	c) How is key distribution implemented in public key cryptography ?	[4]		
Q4	a) Describe SSL handshake protocol.	[2]	CO4	BT2
	OR			
	b)write HTTPS with header format.	[2]	CO4	BT2
	c)compare SSL with TLS.	[4]	CO4	BT2

Q.5	a) Differentiate MAC and Hash function.	[2]	CO5	BT1
	OR			
	b) What is need of VPN? How it can be implemented.	[2]	CO5	BT2
	c) What is message authentication code? Explain how MAC ensures the integrity of message	[4]	CO5	BT3
Q.6	a) Define XSS attack and give one example for it.	[2]	CO6	BT2
	OR			
	b) What is CSRF?	[2]	CO6	BT2
	c) Explain any two example Data tampering and phishing techniques.	[4]	CO6	BT3