LESSON PLAN
(PVPSIT/ACD/01)

Academic Year	**: 2025-26**
Year/Semester/Section	**: III B. Tech II SEM/G1**
Branch	**: Computer Science and Engineering (CSE)**
Subject Code & Name	**: Cryptograph and Network Security**
Name of Faculty	**: Dr S Phani Praveen**

COs	Course Outcomes	Cognitive Level
CO1	Understand core cryptography and network security principles for building secure systems.	L2
CO2	Apply hashing, digital signatures, and key management techniques to ensure message integrity, authentication, and secure key distribution.	L3
CO3	Apply network security protocols and system security mechanisms to secure communication and networks.	L3
CO4	Analyze symmetric and asymmetric encryption algorithms for data confidentiality, secure key exchange, and authentication.	L4

Unit No	**Topic**	**Learning Outcomes**	**Teaching Mode BB / LCD/ LCD**	**Hours Required**		**Total no. of Hours (Cumulative)**	**Expected date of completion**	**Review / Remarks (By HOD)**
				L	**T**			
1	Introduction: Security Goals	Able to understand about security goals (CO1-L2)	**BB/LCD**	**1**		**1**		
1	Cryptographic Attacks	Able to outline the cryptographic attacks (CO1-L1)	**BB/LCD**	**1**		**2**		
1	Security Services	Able to classify security services (CO1-L2)	**BB/LCD**	**1**		**3**		
1	Security Mechanisms	Able to explain about security mechanisms (CO1-L2)	**BB/LCD**	**1**		**4**		
1	A model for Internetwork security	Able to explain the model of internetwork security (CO1-L2)	**BB/LCD**	**1**		**5**		

1	Internet Standards and RFCs	Able to explain about internet standards and RFCs (CO1-L2)	**BB/LCD**	**1**		**6**		
2	**Symmetric Encryption:** Introduction to Modern Symmetric-Key Ciphers	Able to explain about Modern Symmetric-Key Ciphers.(CO1-L4)	**BB/LCD**	**1**		**7**		
2	Modern Block Ciphers	Able to explain about the operations of Block Ciphers (CO1-L4)	**BB/LCD**	**2**		**9**		
2	Data Encryption Standard (DES)	Able to analyze the DES Encryption Algorithm (CO4-L4)	**BB/LCD**	**4**		**13**		
2	Advanced Encryption Standard (AES)	Able to analyze the AES Encryption Algorithm (CO4-L4)	**BB/LCD**	**3**		**16**		
3	**Asymmetric Encryption:** Public key cryptography principles	Able to explain about public key cryptography principles (CO4-L4)	**BB/LCD**	**1**		**17**		
3	RSA Crypto Systems	Able to Apply RSA Crypto Systems (CO4-L4)	**BB/LCD**	**2**		**19**		
3	Rabin Crypto Systems	Able to Apply RSA Crypto Systems (CO4-L4)	**BB/LCD**	**2**		**21**		
3	Elgamal Crypto Systems	Able to Apply RSA Crypto Systems (CO4-L4)	**BB/LCD**	**2**		**23**		
3	Diffie-Hellmen key exchange algorithms	Able to Apply Diffie-Hellman key exchange algorithm (CO4-L4)	**BB/LCD**	**2**		**25**		
4	**Message Integrity and Message Authentication:** Introduction:	Able to explain about Message Integrity and Message Authentication (CO2-L3)	**BB/LCD**	**2**		**27**		
4	Random Oracle Model	Able to explain about Random Oracle Model (CO2-L3)	**BB/LCD**	**1**		**28**		
4	Message Authentication	Able to explain about Message Authentication (CO2-L3)	**BB/LCD**	**2**		**30**		

4	**Cryptographic Hash Functions:** SHA-512 and Whirlpool	Able to explain about Cryptographic Hash Functions (CO2-L3)	**BB/LCD**	**3**		**32**		
4	**Digital Signatures:** Process, Services & Attacks	Able to explain about Digital Signatures (CO2-L3)	**BB/LCD**	**3**		**36**		
4	**Key Management:** Symmetric Key Distribution and Kerberos	Able to explain Various Key Management Techniques (CO2-L3)	**BB/LCD**	**2**		**38**		
5	**Security at the Application Layer:** PGP	Able to explain about PGP (CO3-L2)	**BB/LCD**	**1**		**39**		
5	S/MIME	Able to explain about S/MIME (CO3-L2)	**BB/LCD**	**1**		**40**		
5	**Security at the Transport Layer: SSL and TLS**	Able to explain about SSL and TLS (CO3-L2)	**BB/LCD**	**2**		**42**		
5	**Security at the Network Layer:** IPSec	Able to explain about IP Security (CO3-L2)	**BB/LCD**	**1**		**43**		
5	**Internet Key Exchange and ISAKMP**	Able to explain about Internet Key Exchange and ISAKMP (CO3-L2)	**BB/LCD**	**1**		**44**		
5		Industry Institution Interaction	**LCD**	**1**		**45**		

Legend: Teaching Mode

BB: Black Board / LCD: Power Point Presentation/MOOCS: Massive Open Online Courses

Signature of the Faculty **Signature of the HOD**