PNS School of Engg. & Tech, Marshaghai, Kendrapara

LESSON PLAN

Session (2025-2026)

Discipline: CSE	**Semester: 6th**	**Name of the faculty:** Biswaranjan Swain
Subject: Cryptography and Network Security (Th1)	**No. of Days/Week: 5**	**Start Date: 22/12/2025 End Date: 18/04/2026**

Week	**Class Day**	**Theory Topics**
1st	1st	**1. Possible attacks on Computers:** The need for security
	2nd	Security approach
	3rd	Principles of security
	4th	Types of attacks : Passive attacks
	5th	Active attacks, Computer Security
2nd	1st	**2. Cryptography Concepts** : Plain text & Cipher Text
	2nd	Substitution-cipher technique: Caesar Cipher, Modified Version of Caesar Cipher, Mono-alphabetic Cipher
	3rd	Homophonic Substitution Cipher, Polygram substitution, Poly-alphabetic Substitution Cipher
	4th	Transposition techniques : Rail fence Technique, Simple columnar transposition technique,
	5th	Simple columnar transposition technique with multiple rounds,Vernam Cipher
3rd	1st	Encryption & Decryption
	2nd	Symmetric & Asymmetric key cryptography
	3rd	**3. Symmetric & Asymmetric key algorithms:** ALGORITHM TYPES, ALGORITHM MODES
	4th	OVERVIEW OF SYMMETRIC KEY CRYPTOGRAPHY
	5th	Diffie-Hellman Key Exchange/Agreement Algorithm
4th	1st	Asymmetric Key Operation
	2nd	Data encryption standards, Initial permutation
	3rd	LPT and RPT 16 rounds, Final permutation
	4th	Des decryption, Variation of des: Double des, Triple des
	5th	Triple des with 2 key and 3key
5th	1st	Overview of asymmetric key cryptography
	2nd	RSA algorithm
	3rd	Example of RSA algorithm
	4th	Difference between symmetric and asymmetric key cryptography
	5th	Digital envelope, Steps of digital envelope
6th	1st	Chapter review, Question discussion
	2nd	**4. Digital certificate & Public key infrastructure :** Introduction
	3rd	Concept of digital certificates, Technical details of digital certificate
	4th	Steps for digital certificates creation, Key generation

	5th	Registration, Verification, Certificate creation
7th	1st	Mechanisms for protecting private keys
	2nd	Private key management
	3rd	Key update, Key Archival
	4th	PKIX Model
	5th	Public key cryptography standards
8th	1st	Chapter review, Question discussion
	2nd	**5. Internet security protocols** Basic concepts: Static and dynamic webpage, Active webpage
	3rd	TCP/IP protocol suite
	4th	Secure socket layer
	5th	Hand-shake Protocol, Establish security capabilities Server authentication, Client authentication, Finish
9th	1st	Record protocol, Fragmentation, CompressionAddition of mac, Encryption, Alert protocol
	2nd	Transport layer security
	3rd	Difference between SSL and TLS
	4th	Secure Hyper text transfer protocol(SHTTP)
	5th	Time stamping protocol (TSP)
10th	1st	Secure electronic transaction (SET)
	2nd	SET Process
	3rd	**6. User authentication :** Authentication basics, Password
	4th	Authentication Tokens
	5th	Time based tokens
11th	1st	Certificate based authentication
	2nd	Biometiric Authentication
	3rd	Behavioural Biometrics, Applications
	4th	**7. Network Security & VPN :** Brief introduction of TCP/IP
	5th	Firewall, Limitations of firewall
12th	1st	Types of Firewall
	2nd	Application Gateways
	3rd	VPN
	4th	IP Sec protocols
	5th	Applications of IP Sec