PNS School of Engg. & Tech, Marshaghai, Kendrapara

LESSON PLAN
Session (2024-2025)

Discipline : Computer Science & Engineering	**Semester:**6th	**Name of the Faculty:**Sushree Sangita Tripathy
Subject: Cryptography & Network Security (Th- 1)	**No. Of Days/Week:** 05	**Semester From Date: 04.02.2025** **To Date: 17.05.2025**
Week	**Class Day**	**Theory Topics**
1st	1st	**Unit-1: Possible attacks on computers** Introduction To CNS, The need for security
	2nd	Security approach, Principles of security
	3rd	Types of attacks, Passive Attack
	4th	Active attack
	5th	**Unit-2: Cryptography concepts** Plain text & Cipher Text
2nd	1st	Substitution techniques
	2nd	Poly alphabetic substitution cipher
	3rd	Hill cipher, Play fair cipher
	4th	Transposition techniques
	5th	Doubt Clearing class
3rd	1st	Rail fence technique
	2nd	Simple columnar transposition technique
	3rd	Continue
	4th	Simple columnar transposition technique with multiple Round
	5th	Vernam cipher, Book cipher
4th	1st	Class Test
	2nd	Encryption & Decryption
	3rd	Continue
	4th	Doubt Clearing class
	5th	Encryption & Decryption
5th	1st	**Unit-3: Symmetric & Asymmetric key algorithms**
	2nd	Symmetric key cryptography,Asymmetric key cryptography, Asymmetric key cryptography Example

	3rd	Overview of Symmetric keycryptography Problem about symmetric key cryptography
	4th	Data encryption standards, Initial permutation
	5th	LPT and RPT 16 rounds, Final permutation
6th	1st	Des decryption, Variation of des: Double des, Triple des
	2nd	Triple des with 2 key and 3key
	3rd	Over view of Asymmetric keycryptography Private key and public key
	4th	RSA algorithm
	5th	Example of RSA algorithm
7th	1st	Comparison between symmetric & asymmetric key cryptography
	2nd	Digital envelope, Steps of digital envelope
	3rd	**Unit-4: Digital certificate & Publickey infrastructure** Introduction, Concept of digital certificates
	4th	Certificate authority, Technical details of digital certificate
	5th	Technical details of digital certificate, Steps to digital certificates creation Key generation
8th	1st	Registration, Verification, Certificate creation
	2nd	Certificate hierarchy, Self signed digital certificate Cross certification
	3rd	Certificate revocation and its type, Private key management, Protecting private keys Multiple key pair
	4th	PKIX Model, PKIX services, PKIX architectural model
	5th	Public key cryptography standards
9th	1st	**Unit-5: Internet security protocols**
	2nd	Introduction Static web page, Dynamic web pages and Active web pages ,Protocols
	3rd	Introduction to TCP / IP, Layer of TCP / IP
	4th	Handshake protocol, Establish security capabilities Server authentication, Client authentication, Finish
10th	1st	Record protocol, Fragmentation, Compression Addition of mac, Encryption, Alert protocol
	2nd	Transport layer security
	3rd	Difference between SSL and TLS
	4th	Secure Hyper text transferprotocol(SHTTP)

	5th	Time stamping protocol (TSP), Secure electronic transaction (SET)
11th	1st	**Unit-6: User authentication** Authentication basics, Password
	2nd	Adding randomness to password ,Password encryption
	3rd	6 authentication tokens, Challenge response token, Time-based token
	4th	Certificate based authentication
	5th	Biometric authentication
12th	1st	**Unit-7: Network Security & VPN** Brief introduction of TCP/IP, Firewall, Packet filter
	2nd	Application gateway, Firewall configuration, Overview of IP security
	3rd	Basic concept(AH and ESP), Tunnel mode, Transport mode
	4th	Virtual private network (VPN), Smart card
	5th	Semester regarding Questions & answers discussion

Sushree sangita Tripathy.

SIGNATURE OF LECTURER

Biswaranjan Swain

SIGNATURE OF H.O.D