Estd: 2009 JNTUH College Code: 6C
An ISO 9001:2015 Certified Institution
PRIYADARSHINI INSTITUTE OF SCIENCE AND TECHNOLOGY FOR WOMEN
(Approved by AICTE, New Delhi and Affiliated to JNTUH Hyderabad)
SaiPrabhath Nagar , Khammam Rural -507003, Khammam Dist., Telangana State.
Website: www.priw.ac.in Email Id: jks_edu@yahoo.com Cell: +91-92466 25050.

Network security and Cryptography

Branch: ECE AY:2023-24

Year /sem:IV/I

Lesson-Wise Plan

Lesson No.	Topic	Subtopics	Teaching Aids / Methods	Duration
1	Introduction to Security Concepts	Need for security Goals of security (CIA)	Chalk & board, PPT	1 hour
2	Security Services & Mechanisms	X.800 Security Services Mechanisms: Encipherment, Digital Signature, Access Control, Hashing	PPT, Real-life analogies	1 hour
3	Types of Security Attacks	Passive & Active Attacks Examples: DoS, Masquerade, Traffic Analysis	Diagrams, PPT	1 hour
4	Model for Internetwork Security	Components of model Security transformation Trusted third party	Flow diagrams, Interactive Q&A	1 hour
5	Classical Techniques: Encryption & Steganography	Conventional encryption model Caesar cipher, Monoalphabetic, Vigenère cipher Steganography intro	Hands-on demo, Python tools	1 hour
6	Classical Techniques: Continued	Playfair cipher Transposition ciphers Frequency analysis attacks	Cipher examples on board	1 hour
7	Modern Techniques: Simplified DES (S-DES)	Key generation, encryption/decryption process	Animation / Step-by-step board explanation	1 hour
8	Modern Techniques: Block Cipher & DES	Block cipher principles Structure of DES Initial/Final permutations Round function	PPT with DES structure diagram	1 hour
9	Strength of DES & Design Principles	Avalanche effect Key space Cryptanalysis overview	Case studies	1 hour

PRIYADARSHINI INSTITUTE OF SCIENCE AND TECHNOLOGY FOR WOMEN

(Approved by AICTE, New Delhi and Affiliated to JNTUH Hyderabad)
SaiPrabhath Nagar , Khammam Rural -507003, Khammam Dist., Telangana State.
Website: www.priw.ac.in Email Id: jks_edu@yahoo.com Cell: +91-92466 25050.

		Block cipher design principles		
10	Triple DES (3DES)	Structure of 3DES Encryption/decryption process Modes and security	Diagrams, comparison charts	1 hour
11	International Data Encryption Algorithm (IDEA)	Modular arithmetic Sub-key generation Round structure	Flowchart explanation, PPT	1 hour
12	Blowfish Algorithm	Key setup and subkeys F-function Feistel structure	Diagram-based walkthrough	1 hour
13	RC5 Algorithm	Variable parameters (word size, rounds, key length) Key expansion Encryption process	Examples with steps	1 hour
14	Characteristics of Advanced Symmetric Block Ciphers	Confusion, diffusion Key size, block size, flexibility Speed and complexity	Comparative table	1 hour
15	Placement of Encryption Function & Traffic Confidentiality	Where to place encryption in OSI/TCP stack Protecting message flow patterns	Practical use cases	1 hour
16	Key Distribution	Types: manual, automated, session keys Needham-Schroeder protocol Key distribution centers	Flow diagrams and role-play	1 hour
17	Random Number Generation	Cryptographic randomness PRNG vs TRNG Applications in key generation	Python demo, PPT	1 hour
18	Principles of Public Key Cryptography	- Basic concept - Public vs Private key - Uses of public key cryptography	PPT, Real-life examples	1 hour
19	RSA Algorithm	- Key generation - Encryption & decryption - Mathematical foundation	Step-by-step board explanation, examples	1 hour
20	Key Management	- Key distribution in public key systems	Flow diagrams, case study	1 hour

		- Public Key Infrastructure (PKI) - Certificates and authorities		
21	Diffie-Hellman Key Exchange	- Working of the algorithm - Mathematical example - Security considerations	Example problem, Python demo	1 hour
22	Elliptic Curve Cryptography (ECC)	- Elliptic curves over finite fields - Key generation, encryption, decryption - Advantages over RSA	Diagram, comparison table	1 hour
23	Applications and Summary	- Use in HTTPS, email encryption, digital signatures - Recap and Q&A	Videos, summary slides	1 hour
24	Prime and Relatively Prime Numbers	- Definitions - Properties - Prime factorization	Chalkboard, PPT with examples	1 hour
25	Modular Arithmetic	- Congruence - Modulo operations - Arithmetic properties in Z_n	Hands-on math examples, Number wheel	1 hour
26	Fermat's and Euler's Theorems	- Fermat's Little Theorem - Euler's Theorem - Applications in cryptography	Proofs and application in RSA	1 hour
27	Primality Testing & Euclid's Algorithm	- Trial division - Fermat test - Euclidean Algorithm for GCD	Board examples, code demo (Python)	1 hour
28	Chinese Remainder Theorem (CRT)	- Theorem statement - Applications in modular systems - Solving CRT problems	Problem-solving session	1 hour
29	Discrete Logarithms	- Definition and examples - Applications in cryptography (DH, ECC) - Hardness of DLP	Comparison chart, real-world use	1 hour
30	Authentication Requirements	- Threats to message integrity - Types of attacks - Requirements for secure	Real-life scenarios, PPT	1 hour

		authentication		
31	Authentication Functions	- Message Authentication Codes (MAC) - Basic authentication model - MAC generation & verification	Diagrams, practical flow example	1 hour
32	Hash Functions	- Introduction to cryptographic hash functions - Properties: pre-image, second pre-image, collision resistance	PPT, Hash examples (SHA, MD5)	1 hour
33	Security of Hash Functions	- Birthday attacks - Length extension attacks - Salting and other defense mechanisms	Problem solving, case studies	1 hour
34	Security of MACs and Summary	- Keyed hash functions - HMAC construction - Summary and real-world applications	Code demo (Python/Java), Q&A	1 hour
35	MD5 & Message Digest Algorithm	- Working of MD5 - Step-by-step operation - Use cases	Slides, Code Demo, Whiteboard	1 hour
36	Secure Hash Algorithm (SHA)	- SHA-1, SHA-2 overview - Steps and structure - Differences from MD5	Diagrams, Live Tool Demonstration	1 hour
37	Digital Signatures	- Purpose and features - RSA-based signatures - Signing & verification process	PPT, Animation, RSA flow	1 hour
38	Authentication Protocols	- Threats (e.g., replay attacks) - Protocol types and examples	Real-world protocol analysis	1 hour
39	Digital Signature Standards	- Digital Signature Standard (DSS) - NIST involvement - Comparison with RSA	Slides, Standard Diagrams	1 hour
40	Authentication Applications	- Kerberos: working and architecture - PGP for email - S/MIME for secure mail	Flowcharts, Sample Emails, Video	1 hour

PRIYADARSHINI INSTITUTE OF SCIENCE AND TECHNOLOGY FOR WOMEN
(Approved by AICTE, New Delhi and Affiliated to JNTUH Hyderabad)
SaiPrabhath Nagar , Khammam Rural -507003, Khammam Dist., Telangana State.
Website: www.priw.ac.in Email Id: jks_edu@yahoo.com Cell: +91-92466 25050.

41	IP Security Overview & Architecture	IPSec components Architecture overview Security services	Network diagrams, PPT	1 hour
42	IPSec Authentication & ESP	Authentication Header (AH) Encapsulating Security Payload (ESP)	Packet analysis, flowcharts	1 hour
43	Key Management in IPSec	ISAKMP IKE protocol Key exchange processes	Protocol demos, flow diagrams	1 hour
44	Web Security	SSL/TLS structure Secure Electronic Transaction (SET)	SSL handshake demo, real-site analysis	1 hour
45	Intruders, Viruses and Worms	Types of intruders Viruses and worms Detection & prevention	Case studies, Antivirus demo	1 hour
46	Firewalls and Trusted Systems	Firewall types Design principles Trusted system overview	Firewall setup demo, Q&A	1 hour