LESSON PLAN 2025-26(SUMMER)

NAME OF THE TEACHER : MAMUNI MAHANANDA,GUEST FACULTY(CSE)

Subject: CRYPTOGRAPHY AND NETWORK SECURITY**(TH1)**
Program: Diploma in Computer Science and Engineering
Semester: 6th
Total Contact Hours: 60
Total Marks: 100
Assessment: Internal Assessment – 20, End Term – 80

Understand the basic concepts that of security approach.
CO1: Learn about different attack on the computer systems.
CO2:Learn about the measures to save computer hardware and software.
CO3: Understand different certification to ensure security.
C04: Learn about basic concepts of firewalls and their use.
CO5: Understand privacy and security.

Lesson No.	UNIT	Topic/Sub-Topic	Learning Objective	Activity	Homework	COURSE OBJECTIVE
UNIT-1-: Overview of Operating System: (5 Hours)						
1	I	Introduction to Computer Security	Students will be able to identify sensitive data types and explain the financial, legal, and personal impact of security failures.	Asset Mapping: In small groups, list all digital assets a typical school might have (student grades, staff payroll, research) and rank them by "Value" vs "Risk."	Find a news article about a recent data breach. Write a one-paragraph summary of what was stolen and what the penalty was for the company.	**CO1**
2	I	Security Approaches	Students will differentiate between proactive and reactive security and understand the "Defense in Depth" (layered) approach.	The "Castle Analogy": How did medieval castles use moats, walls, and gates? Relate this to firewalls, passwords, and encryption.	Audit your own "Security Approach." List 3 layers of security you currently use for your personal social media or gaming accounts.	C01
3	I	Principles of Security - The CIA Triad	Students will define the CIA Triad and identify which principle is violated in various scenarios.	Scenario Sorting: Give students 5 scenarios (e.g., "A hacker deletes a website," "A stranger reads your texts"). Students must categorize which part of the CIA Triad was attacked.	Create a poster or digital slide illustrating the CIA Triad with a real-world example for each pillar.	C01

4	I	Principles of Security - AAA & Non-Repudiation	Students will explain the difference between identifying a user and granting them specific permissions.	Role-Based Access Control (RBAC): Create a table for a "Hospital System." Decide what a Doctor, a Nurse, and a Patient should be allowed to see/edit.	Research "Multi-Factor Authentication" (MFA). List two ways it improves the "Authentication" step of AAA.	CO2
5	I	Types of Attacks	Students will distinguish between passive (eavesdropping) and active (modifying) attacks and identify common malware types.	Attack Roleplay: Students act out "Man-in-the-Middle," "Phishing," and "DDoS" attacks using paper slips to represent data packets and traffic.	"The Threat Glossary": Write a 1-sentence definition for: Virus, Worm, Trojan, Ransomware, and Spyware.	CO2
UNIT-2:- Cryptography Concepts(10 hours)						
7	II	Advanced Cryptography Fundamentals	Students will distinguish between "Cleartext" and "Ciphertext" and understand the goal of obfuscation.	The Scavenger Hunt: Hide clues around the room in simple "Pigpen" cipher. Students must translate them back to plaintext to find the "treasure."	Find a historical example of a "hidden message" used in a war or a famous movie. Identify what the plaintext was.	CO3
8	II	The Cryptographic Process	Students will explain the mathematical relationship: $C = E(P, K)$ and $P = D(C, K)$.	Flowchart Design: Draw a process map showing how a message travels from a Sender (Alice) to a Receiver (Bob) while an Eavesdropper (Eve) watches.	Define the term "Key Space." Explain why a longer key makes decryption harder for an attacker.	CO3
9	II	Substitution I - The Caesar Cipher	Students will manually encrypt/decrypt using the Caesar Shift and identify its weaknesses.	Shift-Key Challenge: In pairs, one student chooses a key (n) and encrypts a sentence. The partner must "Brute Force" the message without knowing the key.	Use the Caesar Cipher to encrypt the phrase "CYBER SECURITY IS COOL" with a shift of 7.	CO3

10	II	Substitution II - Vigenère & Polyalphabetic	Students will understand how polyalphabetic ciphers defeat simple frequency analysis.	Vigenère Square: Use a printed Vigenère table to encrypt a message using the keyword "BOLT." Observe how the same letter in plaintext becomes different letters in ciphertext..	Research "Frequency Analysis." Write 3 sentences on why the Caesar cipher is vulnerable to it, but the Vigenère is more resistant.	CO3
11	II	Transposition I - Rail Fence	Students will perform a "zigzag" transposition and recognize that letter frequency remains unchanged.	The ZigZag Workshop: Encrypt a 20-letter sentence using a 3-rail fence. Swap papers and try to "read the rails" to decrypt.	Explain why a Rail Fence cipher is easier to crack if the attacker knows the length of the message.	CO3
12	II	Transposition II - Columnar Methods	Students will use a keyword to determine the order of column readout in a grid.	Grid Lock: Create a 5×5 grid. Use the word "APPLE" to number the columns and read out the ciphertext vertically.	Create a "Double Transposition" example. (Perform a columnar transposition, then perform a second one on the result).	CO3
13	II	Diffie-Hellman Key Exchange	Students will grasp the concept of "One-Way Functions" through a color-mixing analogy.	The Paint Mix: Use the "Color Mixing" analogy (Yellow + Blue = Green). Demonstrate how Alice and Bob can end up with the same "Secret Color" without sending it directly.	Write a paragraph explaining why Diffie-Hellman is not technically "Encryption" but a "Key Exchange."	CO3
14	II	Asymmetric Key Cryptography	Students will define the roles of the Public Key (Encryption) and Private Key (Decryption).	The Padlock Box: A student puts a lock on a box (Public Key). Only the owner of the key (Private Key) can open it. Demonstrate why the owner never gives away the key.	Explain: "If I want Alice to send me a secret message, whose Public Key does she use? Whose Private Key do I use to read it?"	CO3

15	II	Hybrid Cryptography & Digital Signatures	Students will understand that Asymmetric is used to swap a Symmetric key, which is then used for the actual data.	The Digital Handshake: Roleplay the "SSL/TLS Handshake." Alice sends her Public Key $\rightarrow$ Bob sends an encrypted Symmetric Key $\rightarrow$ Communication is now private.	Look at the "Lock" icon in your browser URL bar. Click it, view the certificate, and list which Asymmetric algorithm (like RSA or ECC) is being used.	CO3
UNIT-3:Symmetric & Asymmetric key algorithms :(15 hours)						
16	III	Advanced Algorithms & Digital Integrity	Students will identify the mathematical components of a symmetric system: Plaintext, Encryption Algorithm, Secret Key, and Ciphertext.	Speed vs. Security: A timed challenge where students compare the time taken to encrypt a long text using a simple shift vs. a complex multi-step rule.	List three real-world scenarios where high-speed encryption is more important than complex key management.	CO3
17	III	Symmetric Key Algorithm Types - Block Ciphers	Students will define "Block Size" and explain how Padding works when data doesn't fit perfectly.	Grid Blocks: Divide a message into 8-character blocks. If the last block is short, students must come up with a "Padding" rule to fill the space.	Research why 64-bit and 128-bit are common block sizes in computing.	CO3
18	III	Symmetric Key Algorithm Types - Stream Ciphers	Students will understand the concept of a "Keystream" and why synchronization is vital.	The XOR Logic: A hands-on exercise using the XOR (Exclusive OR) gate logic to combine a binary message with a binary key.	Compare Block vs. Stream ciphers in a table. Which is better for streaming a live video?	CO3
19	III	Introduction to DES	Students will explain the Feistel Network structure and why 56-bit keys became obsolete.	Students will explain the Feistel Network structure and why 56-bit keys became obsolete.	Find out what year DES was officially "cracked" and how long it took the hackers to do it.	CO3

20	III	The Rise of AES	Students will identify the four stages of an AES round: SubBytes, ShiftRows, MixColumns, and AddRoundKey.	AES Step-by-Step: Use a 4×4 grid of numbers to simulate the "ShiftRows" and "SubBytes" (using a lookup table) transformations.	Research why the US government chose Rijndael as the winner of the AES competition.	CO3
21	III	Comparing DES, 3DES, and AES	Students will evaluate the security-to-performance ratio of different symmetric standards.	Security Audit: Given a list of "Old Systems," students must recommend whether to keep 3DES or upgrade to AES-256 based on security needs.	Explain why "Triple DES" (3DES) is slower than the original DES.	CO3
22	III	Overview of Asymmetric Key Cryptography	Students will explain the mathematical "Trapdoor" concept—easy to do one way, hard to reverse.	Students will explain the mathematical "Trapdoor" concept—easy to do one way, hard to reverse.	Write a definition for a "One-Way Function."	CO3
23	III	The RSA Algorithm	Students will perform simplified RSA calculations using small prime numbers.	Small-Scale RSA: Given $p=3, q=11$, students calculate $n=33$ and find a possible public key e.	Why is it crucial that p and q remain secret in the RSA algorithm?	CO3
24	III	The RSA Algorithm - Encryption & Decryption	Students will apply the formula $C = M^e \pmod{n}$ for encryption.	The Calculator Challenge: Use scientific calculators to encrypt a single digit (e.g., "5") using the RSA keys generated in Lesson 8.	Research what "Modular Arithmetic" is and why it's used in RSA.	CO3
25	III	Asymmetric vs. Symmetric - The Showdown	Students will categorize algorithms into Symmetric (AES, DES) or Asymmetric (RSA, ECC).	The Debate: One side argues for Symmetric (Speed/Efficiency), the other for Asymmetric (Scalability/Key Security).	Create a comparison chart covering: Key Length, Speed, and Primary Use Case.	CO3

26	III	The Concept of Hashing	Students will explain why a hash cannot be reversed and how it detects data tampering.	Fingerprinting Data: Use an online SHA-256 generator. Change one letter in a sentence and observe how the entire hash changes (Avalanche Effect).	Define "Collision" in the context of hashing.	CO3
27	III	Digital Signatures - Authentication	Students will describe the process of signing a message using a Private Key.	The Wax Seal: A roleplay where a "King" signs a scroll. Explain how the Public Key acts as the "Verification Tool" for the public.	List the three things a Digital Signature provides: Authentication, Integrity, and Non-Repudiation.	CO3
28	III	Digital Signatures - Non-Repudiation	Students will explain how digital signatures prevent a sender from claiming they didn't send a message.	Mock Court: A scenario where a student tries to deny sending an email. Classmates use "Digital Evidence" to prove the signature matches their Private Key.	Research the "Digital Signature Act" in your country or region.	CO3
29	III	Digital Certificates & CAs	Students will define a Certificate Authority (CA) and its role in the Public Key Infrastructure (PKI).	Distinguish between Remote Access VPNs and Site-to-Site VPNs.	Find the name of three major Certificate Authorities (e.g., DigiCert, Let's Encrypt).	CO3
30	III	Putting it All Together	Students will synthesize all concepts to explain how a secure web transaction works.	The Secure Web Map: Students draw a complete diagram of a user visiting an online bank, labeling where AES, RSA, Hashing, and Digital Signatures are used.	Final Reflection: Which of the two (Symmetric or Asymmetric) do you think is more vital to the modern internet? Defend your answer.	CO3
UNIT 4:-Digital certificate & Public key infrastructure (10 hours)						

31	IV	Introduction to Digital Certificates	Students will define a Digital Certificate and identify its primary components (Serial Number, Issuer, Validity Period).	Identity Audit: Students open a browser (Chrome/Edge), click the lock icon on a site like Google or their school portal, and list five pieces of information found in the certificate.	Draw a comparison between a physical Driver's License and a Digital Certificate. What features do they share?	CO4
32	IV	The Role of the Certificate Authority	Students will explain the hierarchy of trust, including Root CAs and Intermediate CAs.	The Trust Chain Simulation: A "Root CA" (teacher) authorizes "Intermediate CAs" (selected students), who then issue "ID Cards" to the rest	Research "Self-Signed Certificates." Why are they usually blocked or flagged by browsers?	CO4
33	IV	X.509 Standards	Students will understand the X.509 standard and why formatting consistency is vital for global interoperability.	Standardization Workshop: Students receive "mismatched" identity data and must organize it into a standardized X.509 template provided by the teacher.	Find out the difference between X.509 Version 1 and Version 3.	CO4
34	IV	Private Key Management - Generation & Storage	Students will identify secure methods for generating and storing private keys (HSMs, Token-based storage).	Security Brainstorm: In groups, students brainstorm where a company should hide its master private key. Evaluate "Cloud Storage" vs. "Offline Cold Storage.".	Define an HSM (Hardware Security Module) and explain how it differs from a standard USB drive.	CO4
35	IV	Private Key Lifecycle - Revocation	Students will define Certificate Revocation Lists (CRL) and the Online Certificate Status Protocol (OCSP).	The "Lost Key" Drill: A student "loses" their private key. The class must figure out how to alert everyone else to stop trusting that student's certificate.	Compare CRL and OCSP. Which one is faster for a browser to check?	CO4

36	IV	The PKIX Model - Architecture	Students will identify the five main entities in the PKIX model: End Entity, CA, RA, CRL Issuer, and Repository.	PKIX Mapmaking: Students draw a diagram connecting the five entities and use arrows to show how a certificate request flows through them.	Research the role of the "Registration Authority" (RA). How is it different from a CA?	CO4
37	IV	The PKIX Model - Management Functions	Students will describe the management phases: Initialization, Certification, and Key Pair Update.	Lifecycle Roleplay: Students act out the process from "Initial Request" to "Renewal" and finally "Expiration" of a digital certificate.	Why is it important for certificates to have an expiration date? Why not make them last forever?	CO4
38	IV	Public Key Cryptography Standards	.Students will recognize common PKCS standards (e.g., PKCS #7 for signatures, PKCS #12 for storage).	Discussion: "Why does my computer get slower over time?" Relate to fragmentation.	What is "caching"? How does a disk cache improve performance?	CO4
39	IV	PKI in Practice - HTTPS and Beyond	Students will synthesize all PKI components to explain how a secure SSL/TLS connection is established.	The Ultimate Handshake: A full-class simulation of a computer connecting to a bank. Identify every step from checking the CA to exchanging the symmetric key.	Final Project: Create a "Security Checklist" for a new business setting up its first PKI system.	CO4
40	IV	Trust Models - Hierarchical vs. Web of Trust	Students will compare the centralized PKI (CA-based) with the decentralized Web of Trust (PGP-based).	The Reputation Game: Students vouch for each other's identity without a "Teacher/CA." See how long it takes to establish a "Web of Trust."	Write a paragraph on why the "Web of Trust" is rarely used for commercial websites compared to the PKI model.	CO4
UNIT-5 -:Internet security protocols :(10 hours)						
41	V	5.1 Basic Concepts of Network Security	Define CIA triad (Confidentiality, Integrity, Availability) and the role of protocols.	Case Study: Analyze a famous data breach and identify which security pillar failed.	Write a 300-word reflection on why "Security by Design" is better than "Security as a Patch."	CO4

42	V	Introduction to SSL	Understand the history of Secure Socket Layer and the Handshake process.	Diagram Mapping: Draw the step-by-step interaction between a Client and Server during an SSL handshake.	Research the differences between SSL 2.0, 3.0, and why they are now deprecated.	CO4
43	V	SSL vs. TLS Comparison	Distinguish between the two in terms of cipher suites and alert messages.	Debate: Group A defends SSL's legacy; Group B argues for the necessity of TLS 1.3's speed.	Debate: Group A defends SSL's legacy; Group B argues for the necessity of TLS 1.3's speed.	CO4
44	V	Application Layer & Web Security	Understand document-level security vs. connection-level security.	Roleplay: Simulate a "Request-Response" cycle using S-HTTP headers vs. standard HTTPS.	Compare HTTPS (TLS) with S-HTTP. Why did HTTPS win the "protocol war"?	CO4
45	V	Time Stamping Protocol	Explain the role of TST (Time Stamp Tokens) in non-repudiation.	Activity: "The Document Race." Demonstrate how a timestamp proves a file existed before a certain time.	Research a legal case where "Digital Timestamps" were used as evidence in court.	CO4
46	V	The Future of Security Protocols	Explore Quantum-resistant cryptography and future trends.	Brainstorming: How will security change when Quantum computers can crack RSA encryption?	Final Project: Design a "Security Checklist" for a new e-commerce startup using all protocols learned.	CO4
47	V	Secure Electronic Transaction	Understand the SET architecture involving Merchant, Cardholder, and Issuer.	Scenario Mapping: Map a credit card transaction from the moment "Buy" is clicked to bank approval.	List the advantages of SET over standard SSL for e-commerce (e.g., Dual Signatures).	CO4
48	V	S-HTTP: Secure HTTP	Understand document-level security vs. connection-level security.	Roleplay: Simulate a "Request-Response" cycle using S-HTTP headers vs. standard HTTPS.	Compare HTTPS (TLS) with S-HTTP. Why did HTTPS win the "protocol war"?	CO4

49	V	TLS: The Modern Standard	Explain the evolution from SSL to TLS and the Record Protocol.	Wireshark Demo: Observe (via simulation) how a packet changes from plaintext to ciphertext using TLS.	List three modern browsers and check their current supported TLS versions.	CO4
50	V	TSP Architecture	Identify the roles of the Requester and the TSA (Time Stamping Authority).	Flowchart Design: Create a flow diagram of a request sent to a TSA and the signature returned.	Explain how Hash functions are used within a Time Stamp Token.	CO4
UNIT-6 User authentication(4 Hours)						
51	VI	Authentication Basics & Passwords	Define the "Three Factors of Authentication" and the vulnerabilities of static passwords (hashing, salting).	Password Strength Test: Use a "How secure is my password" simulator to test various strings and discuss entropy.	Research the "Top 10 most common passwords of 2025" and write three rules for a "Strong Password Policy."	CO5
52	VI	Authentication Tokens (OTP & Hardware)	Differentiate between "Something you have" (Tokens) and "Something you know." Explain HMAC-based One-Time Passwords (HOTP).	The MFA Relay: Simulate a login where one student is the "Server" and another must provide a timed code from a "Token" student.	Identify three apps you use that offer 2FA/MFA. Note whether they use SMS, email, or an Authenticator app.	CO5
53	VI	Certificate-Based Authentication	Understand Public Key Infrastructure (PKI) and how digital certificates remove the need for passwords.	Identity Exchange: Use a simplified paper-based "Digital Certificate" exercise to verify a classmate's identity using a "Trusted Third Party."	Compare Password-based vs. Certificate-based login. Which is more secure for a corporate VPN, and why?	CO5
54	VI	Biometric Authentication	Evaluate physiological vs. behavioral biometrics (Fingerprint, Iris, Voice) and the concept of "False Acceptance."	Biometric Audit: List all biometric sensors in the room (phones/laptops). Discuss the privacy risks of storing "identity" in a database	Research the "False Rejection Rate" (FRR). Why is a high FRR annoying but a high "False Acceptance Rate" (FAR) dangerous?	CO5
UNIT-7- (6 hours)						

55	VII	TCP/IP Security Foundations	Understand the 4-layer TCP/IP model and identify vulnerabilities at each layer (e.g., IP spoofing).	Packet Mapping: Trace a "request" from the Application layer down to the Network layer on a whiteboard.	Create a table showing one specific security threat for each of the four TCP/IP layers.	CO5
56	VII	Firewall Basics & Types	Define Packet Filtering, Stateful Inspection, and Application-level gateways.	The Bouncer Game: Students act as a firewall, deciding which "packets" (index cards with IP/Port info) to let into the "club" (classroom).	Draw a diagram showing where a "DMZ" (Demilitarized Zone) sits in relation to an internal firewall.	CO5
57	VII	Next-Gen Firewalls (NGFW)	Explain Deep Packet Inspection (DPI) and Intrusion Prevention Systems (IPS).	Analysis: Compare a standard router's firewall settings with an enterprise-grade NGFW feature list.	Research the difference between an IDS (Detection) and an IPS (Prevention).	CO5
58	VII	IP Security (IPsec) - Part 1	Understand the role of AH (Authentication Header) and ESP (Encapsulating Security Payload).	Encapsulation Demo: Use a "Letter in an Envelope" analogy to show how ESP wraps data for transit.	Explain the difference between Transport Mode and Tunnel Mode in IPsec.	CO5
59	VI	IP Security (IPsec) - Part 2	Learn about IKE (Internet Key Exchange) and Security Associations (SA).	Flowcharting: Diagram the 3-step process of establishing an IPsec connection between two branch offices.	Define a "Security Association" (SA) and list the parameters it must track.	CO5
60	VII	Virtual Private Networks (VPN)	Distinguish between Remote Access VPNs and Site-to-Site VPNs.	Setup Simulation: Use a free VPN tool or browser extension to observe how a public IP address changes.	Write a summary on "Split Tunneling"—what are the benefits and the security risks?	CO5

22/12/25

Signature of Teacher

Deepak M
22.12.2025

Signature of HOD