Department of CSE

Details of Lesson Plan

S.No.	Particulars	Details
1.	Course Name	**Cryptography and Computer Security**
2.	Course Code	MCSE21B
3.	Academic Year	2024-2025
4.	Semester	2ND
5.	Number of Lesson plans	30
6.	Faculty Assigned	Ms. Vani Malagar

Faculty Signature

Lesson Plan No. 1	Course Name: Cryptography and Computer Security	Course No.: MCSE21B

Objectives	At the end of the lesson, the student shall be able to: a. Understand the security mindset and its importance in computing. b. Explain the fundamental concepts of computer security (Confidentiality, Integrity, and Availability - CIA Triad). c. Identify various threats, attacks, and assets in the domain of computer security.
Teaching Aids (if any)	a. PowerPoint Presentation b. Short Video/Animated presentation.
Teaching Development	1. **Introduction** (10 minutes) Discussion starts with real-life examples of different systems (Facebook) | Introduction Video (8:20): https://www.youtube.com/watch?v=_r97qdyQtIk - Organizations are using which techniques for data storage and why? (MAANG companies) 2. **Development** (30 minutes) Career & Job Perspective (Database Administrator, Data Analyst, Market Research Analyst) - Discussion on Coursera Certification by IBM - Oracle Database 12c Administrator Certified Associate - Microsoft Certified: Azure Database Administrator Associate - For More Oracle Certification :(Oracle University) - Introduction of Course (RDBMS) 3. **Examples of DBMS** (10 minutes) - Real-world examples. (Banking Management System, Pi360) - IT Industry (Meta) - Online Bookings (E-Ticketing)
Closure	Summarize the Lesson correlation with Learning Outcomes

Lesson Plan	Course Name: Cryptography and Computer Security	Course No.: MCSE21B

Objectives	At the end of the lesson, the student shall be able to: a. Understand the security mindset and its importance in computing. b. Explain the fundamental concepts of computer security (Confidentiality, Integrity, and Availability - CIA Triad). c. Identify various threats, attacks, and assets in the domain of computer security.
Teaching Aids (if any)	a. PowerPoint Presentation b. Animated Video Resources
Teaching Development	**Introduction (5 minutes)** **Pre-Discussion Questions:** 1. Have you ever heard of a major cybersecurity breach (e.g., Facebook, LinkedIn)? 2. Why do you think companies invest so much in cybersecurity? 3. What could be the consequences of a cyber-attack? **Engagement Activity:** • Show a short **introductory video** on cybersecurity threats. *Link: Cybersecurity Threats Explained* • Ask students to discuss their experiences or knowledge of cyber threats. --- **Development (30 minutes)** **1. Security Mindset (10 minutes)** • Definition and importance of cybersecurity. • **Case Study:** Discussion on a real-world security breach (e.g., Facebook data leak). • Interactive discussion on how security failures impact businesses and individuals. **2. Computer Security Concepts – CIA Triad (10 minutes)** • Define **Confidentiality, Integrity, and Availability (CIA Triad)**. • **Activity:** Divide students into three groups and assign each group one aspect of the CIA Triad. They will discuss and present their findings with real-life examples. • **Visual Aid:** Use a diagram to illustrate the CIA triad. **3. Threats, Attacks, and Assets (10 minutes)** • **Threats:** Differentiate between natural, human, and environmental threats. • **Attacks:** Explain Passive vs. Active attacks with examples. • **Assets:** Identify key assets in an IT environment and discuss how they can be protected. • **Live Demonstration:** Ethical hacking demo using a basic password-cracking tool (legal and educational purpose).

Lesson Plan	Course Name: Cryptography and Computer Security	Course No.: MCSE21B

Closure	• The importance of a **security-first mindset** in computing. • **CIA Triad** as the foundation of security principles. • **Threats and Attacks**: Understanding and mitigating cybersecurity risks. "Cryptography and Network Security" by William Stallings, Chapter 1. "Computer Security: Principles and Practice" by William Stallings and Lawrie Brown, Chapter 1. Spend 5 minutes to wrap up and consolidate the leanings.
Evaluation	• How does understanding security concepts help in preventing cyber-attacks? • Can you identify a security threat in your daily life? Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan	Course Name: Cryptography and Computer Security	Course No.: MCSE21B

Objectives	At the end of the lesson, the student shall be able to: • Understand the need for cryptography in computer security. • Explain different cryptographic techniques (symmetric, asymmetric, hashing). • Implement basic cryptographic methods.
Teaching Aids (if any)	a. PowerPoint Presentation b. Animated Video Resources : https://youtu.be/5jpgMXt1Z9Y
Teaching Development	1. **Introduction (5 minutes)** ○ Discussion on how encryption is used in daily life. ○ Short video on cryptographic applications. 2. **Development (30 minutes)** ○ Explanation of symmetric vs. asymmetric encryption. ○ Demonstration of encryption using OpenSSL. ○ Group activity: Encrypt and decrypt messages.
Closure	**Exercise (5 minutes)** • Hands-on encryption task. "Cryptography and Network Security" by William Stallings, Chapter 1. "Computer Security: Principles and Practice" by William Stallings and Lawrie Brown, Chapter 1. Spend 5 minutes to wrap up and consolidate the leanings.
Evaluation	Recap of cryptographic techniques and short assessment.

Lesson Plan	Course Name: Cryptography and Computer Security	Course No.: MCSE21B

Objectives	**Understanding Threats in Cybersecurity** At the end of the lesson, the student shall be able to: • Identify different types of cybersecurity threats. • Understand real-world cybersecurity incidents. • Analyze how threats impact individuals and organ
Teaching Aids (if any)	a. PowerPoint Presentation b. Animated Video Resources: Short video on encryption techniques: Introduction to Cryptography : https://youtu.be/5jpgMXt1Z9Y
Teaching Development	1. **Introduction (5 minutes)** o Ask students: "Have you ever received a suspicious email or message? What did you do?" o Show a video on major cyber threats. 2. **Development (30 minutes)** o Discuss types of threats: Malware, Phishing, Social Engineering, Insider Threats, etc. o Real-life case study: Analyzing the Equifax Data Breach. o Interactive role-play: Students act as cybersecurity experts responding to a security threat. 3. **Exercise (5 minutes)** o Quiz: Identify different threats based on given scenarios.
Closure	• Summary discussion and Q&A. "Cryptography and Network Security" by William Stallings, Chapter 1. "Computer Security: Principles and Practice" by William Stallings and Lawrie Brown, Chapter 1. Spend 5 minutes to wrap up and consolidate the leanings.
Evaluation	• Assignment: Research and present a recent cyber threat.

Lesson Plan	Course Name: Cryptography and Computer Security	Course No.: MCSE21B

Objectives	**Cyber Attacks – Methods and Mitigation** At the end of the lesson, the student shall be able to: • Understand different types of cyber-attacks. • Analyze attack techniques and their impact. • Learn mitigation strategies for cyber-attacks.
Teaching Aids (if any)	a. PowerPoint Presentation b. Animated Video Resources
Teaching Development	1. **Introduction (5 minutes)** o Discussion: "Have you ever heard of hacking? What do you think hackers do?" o Show a video demonstrating major cyber-attacks. 2. **Development (30 minutes)** o Explain attack types: DDoS, Man-in-the-Middle, Ransomware, Zero-day Exploits. o Live demonstration of packet sniffing using Wireshark. o Group discussion: How can organizations prevent attacks?
Closure	• Summary discussion. • Assignment: Write a report on a famous cyber-attack and its mitigation. "Cryptography and Network Security" by William Stallings, Chapter 1. "Computer Security: Principles and Practice" by William Stallings and Lawrie Brown, Chapter 1. Spend 5 minutes to wrap up and consolidate the leanings.
Evaluation	Cybersecurity challenge: Identify vulnerabilities in a mock scenario.

Lesson Plan	Course Name: Cryptography and Computer Security	Course No.: MCSE21B

Objectives	**Assets in Cybersecurity – Protection and Risk Management** At the end of the lesson, the student shall be able to: • Define assets in cybersecurity. • Understand asset classification and protection. • Conduct risk assessments for cybersecurity assets.
Teaching Aids (if any)	a. PowerPoint Presentation b. Animated Video Resources c. Case Study: How Companies Secure Their Digital Assets
Teaching Development	1. **Introduction (5 minutes)** ○ Ask students: "What do you consider valuable in a digital system?" ○ Show a video on asset protection. 2. **Development (30 minutes)** ○ Explain assets: Data, Software, Hardware, Networks, Human Resources. ○ Discuss asset protection strategies: Encryption, Firewalls, Access Controls.
Closure	Students categorize assets and propose security measures. "Cryptography and Network Security" by William Stallings, Chapter 1. "Computer Security: Principles and Practice" by William Stallings and Lawrie Brown, Chapter 1. Spend 5 minutes to wrap up and consolidate the leanings.
Evaluation	Recap of asset management and risk mitigation.

Lesson Plan	Course Name: Cryptography and Computer Security	Course No.: MCSE21B

Objectives	**Introduction to Protocols in Cryptography** At the end of the lesson, the student shall be able to: • Understand the role of protocols in cryptography. • Explain different cryptographic protocols (SSL, TLS, IPSec). • Analyze real-world applications of cryptographic protocols.
Teaching Aids (if any)	a. PowerPoint Presentation b. Video Resources : Introduction to Cryptographic Protocols
Teaching Development	1. **Introduction (5 minutes)** o Ask students: "How does HTTPS secure a website?" o Show a video on cryptographic protocols. 2. **Development (30 minutes)** o Discuss cryptographic protocols and their importance. o Demonstrate SSL/TLS handshake using a browser inspection tool. o Group discussion: Compare TLS vs. IPSec.
Closure	Students analyze HTTPS traffic using Wireshark. "Cryptography and Network Security" by William Stallings. "Computer Security: Principles and Practice" by William Stallings and Lawrie Brown. Spend 5 minutes to wrap up and consolidate the leanings.
Evaluation	• Summary discussion and Q&A. • Assignment: Research and explain a cryptographic protocol.

Lesson Plan	Course Name: Cryptography and Computer Security	Course No.: MCSE21B

Objectives	**Communications using Symmetric Cryptography** At the end of the lesson, the student shall be able to: • Understand symmetric encryption and its applications. • Explain key exchange in symmetric cryptography. • Implement basic symmetric encryption using OpenSSL.
Teaching Aids (if any)	a. PowerPoint Presentation b. Video Resources: How Symmetric Encryption Works
Teaching Development	**1. Introduction (5 minutes)** o Ask students: "Why do we need encryption for communication?" o Show a video explaining symmetric encryption. 2. **Development (30 minutes)** o Explain AES, DES, and 3DES algorithms. o Live demo: Encrypting and decrypting messages using OpenSSL. o Discussion: Strengths and weaknesses of symmetric encryption.
Closure	• Summary discussion. • Assignment: Compare AES and DES encryption techniques. "Cryptography and Network Security" by William Stallings, Chapter 1. "Computer Security: Principles and Practice" by William Stallings and Lawrie Brown, Chapter 1. Spend 5 minutes to wrap up and consolidate the leanings.
Evaluation	• **Basic Questions:** What is the major drawback of symmetric encryption? How do we securely exchange keys?

Lesson Plan	Course Name: Cryptography and Computer Security	Course No.: MCSE21B

Objectives	**Substitution and Transposition Ciphers** At the end of the lesson, the student shall be able to: • Differentiate between substitution and transposition ciphers. • Implement basic ciphers (Caesar, Vigenère, Rail Fence). • Analyze the security of classical encryption methods.
Teaching Aids (if any)	a. PowerPoint Presentation b. Video Resources: Substitution vs. Transposition Ciphers
Teaching Development	1. **Introduction (5 minutes)** o Ask students: "Can you create a secret message using simple letter shifts?" o Show a video on substitution and transposition ciphers. 2. **Development (30 minutes)** o Explain and demonstrate different ciphers. o Hands-on activity: Encrypting messages using Python. o Discussion: Why are classical ciphers insecure today?
Closure	Assignment: Research how Enigma worked and why it was broken. • **Basic Questions:** What are the limitations of classical ciphers? How do modern cryptographic methods improve security? "Cryptography and Network Security" by William Stallings. "Computer Security: Principles and Practice" by William Stallings and Lawrie Brown. Spend 5 minutes to wrap up and consolidate the leanings.
Evaluation	Encrypt and decrypt messages using different ciphers.

Lesson Plan	Course Name: Cryptography and Computer Security	Course No.: MCSE21B

Objectives	**Block Cipher – Principles and Examples** At the end of the lesson, the student shall be able to: • Understand block cipher principles. • Explain DES and AES encryption. • Implement block ciphers using Python.
Teaching Aids (if any)	a. PowerPoint Presentation b. Video Resources : How AES Works
Teaching Development	1. **Introduction (5 minutes)** o Ask students: "What makes AES secure compared to older encryption methods?" o Show a video explaining AES encryption. 2. **Development (30 minutes)** o Discuss block cipher principles. o Demonstrate encryption and decryption using AES. o Group discussion: Why is AES preferred over DES?
Closure	Encrypt and decrypt text using AES in Python. Cryptography and Network Security" by William Stallings. "Computer Security: Principles and Practice" by William Stallings and Lawrie Brown.
Evaluation	• Assignment: Compare AES and DES security. • **Basic Questions:** How does AES improve upon DES? Why is padding important in block ciphers?

Lesson Plan	Course Name: Cryptography and Computer Security	Course No.: MCSE21B

Objectives	**Stream Cipher – Design and Security** At the end of the lesson, the student shall be able to: • Understand stream cipher principles. • Compare stream and block ciphers. • Implement RC4 encryption.
Teaching Aids (if any)	a. PowerPoint Presentation b. Video Resources : Stream vs Block Ciphers
Teaching Development	1. **Introduction (5 minutes)** o Ask students: "Where is stream cipher used in real life?" o Show a video explaining stream ciphers. 2. **Development (30 minutes)** o Explain stream cipher working principles. o Demonstrate RC4 encryption. o Discussion: When to use stream vs. block ciphers?
Closure	Implement RC4 encryption in Python. Cryptography and Network Security" by William Stallings. "Computer Security: Principles and Practice" by William Stallings and Lawrie Brown.
Evaluation	• Assignment: Compare AES and RC4 encryption. • **Basic Questions:** What are the advantages of stream ciphers? Why is RC4 considered weak today?

Lesson Plan	Course Name: Cryptography and Computer Security	Course No.: MCSE21B

Objectives	**Cryptographic Techniques – Classical Ciphers (Caesar, Hill, Vigenère)** At the end of the lesson, the student shall be able to: • Understand the working of classical ciphers: Caesar, Hill, and Vigenère. • Implement and analyze the security of these ciphers. • Compare classical ciphers to modern encryption techniques.
Teaching Aids (if any)	a. PowerPoint Presentation b. Video Resources : Caesar and Vigenère Cipher Explained
Teaching Development	1. **Introduction (5 minutes)** ○ Ask students: "How did ancient civilizations keep messages secret?" ○ Show a video explaining classical ciphers. 2. **Development (30 minutes)** ○ Demonstrate encryption and decryption using Caesar, Hill, and Vigenère ciphers. ○ Hands-on activity: Students encrypt and decrypt messages using online tools. ○ Discussion: Why are classical ciphers not secure today?
Closure	Implement a Vigenère cipher in Python. Cryptography and Network Security" by William Stallings. "Computer Security: Principles and Practice" by William Stallings and Lawrie Brown.
Evaluation	• Assignment: Compare the Hill cipher with modern cryptographic algorithms. • **Basic Questions:** What are the weaknesses of classical ciphers? How do they influence modern cryptography?

Lesson Plan	Course Name: Cryptography and Computer Security	Course No.: MCSE21B

Objectives	**Key Length & Management in Cryptography** At the end of the lesson, the student shall be able to: • Understand the importance of key length in encryption. • Differentiate between symmetric and public-key key length. • Analyze key management strategies.
Teaching Aids (if any)	a. PowerPoint Presentation b. Video Resources : Key Management in Cryptography
Teaching Development	1. **Introduction (5 minutes)** ○ Ask students: "Does increasing key length always improve security?" ○ Show a video on key length and security. 2. **Development (30 minutes)** ○ Explain symmetric vs. public-key encryption key lengths. ○ Discuss key management techniques and secure key exchange. ○ Group discussion: Why are longer keys used in public-key cryptography?
Closure	Generate symmetric and asymmetric keys using OpenSSL. Cryptography and Network Security" by William Stallings. "Computer Security: Principles and Practice" by William Stallings and Lawrie Brown.
Evaluation	• Assignment: Compare the security of 128-bit and 256-bit encryption. • **Basic Questions:** Why does public-key cryptography require longer key lengths? What are the challenges in key management?

Lesson Plan	Course Name: Cryptography and Computer Security	Course No.: MCSE21B

Objectives	**Cryptographic Algorithms – Diffie-Hellman & RSA** At the end of the lesson, the student shall be able to: • Understand how Diffie-Hellman and RSA work. • Analyze the role of these algorithms in secure communications. • Implement basic RSA encryption.
Teaching Aids (if any)	a. PowerPoint Presentation b. Video Resources : How Diffie-Hellman and RSA Work
Teaching Development	1. **Introduction (5 minutes)** o Ask students: "How do two strangers securely exchange keys over an insecure channel?" o Show a video explaining Diffie-Hellman and RSA. 2. **Development (30 minutes)** o Explain the mathematical principles behind Diffie-Hellman and RSA. o Demonstrate a live key exchange using Diffie-Hellman. o Hands-on RSA encryption and decryption using Python.
Closure	Students encrypt and decrypt messages using RSA keys. Cryptography and Network Security" by William Stallings. "Computer Security: Principles and Practice" by William Stallings and Lawrie Brown.
Evaluation	• Assignment: Compare Diffie-Hellman and RSA security. • **Basic Questions:** Why is RSA widely used in secure communications? How does Diffie-Hellman facilitate secure key exchange?

Lesson Plan	Course Name: Cryptography and Computer Security	Course No.: MCSE21B

Objectives	**DES – Data Encryption Standard** At the end of the lesson, the student shall be able to: • Understand the working of the DES algorithm. • Analyze the weaknesses of DES and why it was replaced by AES. • Implement DES encryption using Python.
Teaching Aids (if any)	a. PowerPoint Presentation b. Video Resources : DES Encryption Explained
Teaching Development	1. **Introduction (5 minutes)** ○ Ask students: "Why was DES used as the encryption standard for decades?" ○ Show a video on DES encryption. 2. **Development (30 minutes)** ○ Explain the DES algorithm and its structure. ○ Discuss the vulnerabilities of DES and why AES replaced it. ○ Live demonstration of DES encryption using Python
Closure	Hands-on: Encrypt and decrypt a message using DES Cryptography and Network Security" by William Stallings. "Computer Security: Principles and Practice" by William Stallings and Lawrie Brown.
Evaluation	• Assignment: Compare DES and AES encryption strength. • **Basic Questions:** Why was DES replaced by AES? What are the major weaknesses of DES?

Lesson Plan	Course Name: Cryptography and Computer Security	Course No.: MCSE21B

Objectives	**Encryption in Practical Cryptography** At the end of the lesson, the student shall be able to: • Understand encryption concepts in practical applications. • Implement encryption using modern cryptographic tools. • Compare encryption methods for different use cases.
Teaching Aids (if any)	a. PowerPoint Presentation b. Video Resources : Understanding Encryption
Teaching Development	1. **Introduction (5 minutes)** ○ Ask students: "Where do we use encryption in daily life?" ○ Show a video explaining encryption techniques. 2. **Development (30 minutes)** ○ Explain encryption concepts (symmetric vs asymmetric). ○ Demonstrate AES encryption using OpenSSL. ○ Discuss encryption in cloud storage & messaging apps.
Closure	Hands-on: Encrypt & decrypt a file using AES. Cryptography and Network Security" by William Stallings. "Computer Security: Principles and Practice" by William Stallings and Lawrie Brown.
Evaluation	• Assignment: Compare file encryption in different applications. • **Basic Questions:** Why is encryption necessary? How do modern systems implement encryption?

Lesson Plan	Course Name: Cryptography and Computer Security	Course No.: MCSE21B

Objectives	**Authentication in Practical Cryptography** At the end of the lesson, the student shall be able to: • Understand authentication techniques in cryptography. • Analyze multi-factor authentication (MFA) and its role. • Implement basic authentication protocols.
Teaching Aids (if any)	a. PowerPoint Presentation b. Video Resources: How Authentication Works
Teaching Development	1. **Introduction (5 minutes)** o Ask students: "Have you used 2FA before? How does it improve security?" o Show a video on authentication methods. 2. **Development (30 minutes)** o Explain authentication techniques (passwords, biometrics, 2FA). o Discuss real-world authentication failures. o Hands-on: Setting up a 2FA system.
Closure	Students enable 2FA on a service & discuss their experience. Cryptography and Network Security" by William Stallings. "Computer Security: Principles and Practice" by William Stallings and Lawrie Brown.
Evaluation	• **Basic Questions:** Why is authentication important? How does MFA improve security?

Lesson Plan	Course Name: Cryptography and Computer Security	Course No.: MCSE21B

Objectives	**Hashing in Practical Cryptography** Objectives At the end of the lesson, the student shall be able to: • Explain hashing and its cryptographic importance. • Implement hashing algorithms using Python. • Differentiate between secure and insecure hash functions
Teaching Aids (if any)	a. PowerPoint Presentation b. Video Resources: How Hashing Works
Teaching Development	1. **Introduction (5 minutes)** ○ Ask students: "How does hashing secure passwords?" ○ Show a video on hashing techniques. 2. **Development (30 minutes)** ○ Explain how hashing ensures data integrity. ○ Demonstrate SHA-256 hashing using Python. ○ Discuss password storage & salting in databases.
Closure	• Students hash a file and verify integrity. Cryptography and Network Security" by William Stallings. "Computer Security: Principles and Practice" by William Stallings and Lawrie Brown.
Evaluation	• Assignment: Compare MD5, SHA-1, and SHA-256 security. • **Basic Questions:** How is hashing used in authentication? Why are some hash functions weak?

Lesson Plan	Course Name: Cryptography and Computer Security	Course No.: MCSE21B

Objectives	**Symmetric & Asymmetric Cryptography** At the end of the lesson, the student shall be able to: • Differentiate between symmetric and asymmetric encryption. • Implement RSA encryption using Python. • Compare performance and security of both cryptographic methods.
Teaching Aids (if any)	a. PowerPoint Presentation
Teaching Development	1. **Introduction (5 minutes)** o Ask students: "Why do we use two different encryption methods?" o Show a video on symmetric vs asymmetric encryption. 2. **Development (30 minutes)** o Explain the strengths and weaknesses of each method. o Demonstrate RSA key generation and encryption. o Discussion: Why is asymmetric encryption slower?
Closure	Encrypt & decrypt a message using RSA. Cryptography and Network Security" by William Stallings. "Computer Security: Principles and Practice" by William Stallings and Lawrie Brown.
Evaluation	o Assignment: Compare AES and RSA for secure communication. o **Basic Questions:** Why do we need asymmetric encryption? How is RSA used in digital signatures?