AHMEDABAD UNIVERSITY
School of Engineering and Applied Science
2025-2026 Winter

CSE212 Cyber Security
Mid-Term Examination
Sunday 22 February 2026, 05:00 – 05:45

Name:	Roll no.	A	U	2							Marks /30

Instructions: This is an online examination conducted on a Learning Management System (LMS). Duration of the exam: 45 minutes; Total marks: 30; Total questions: 30. It is a closed-book examination. Therefore, you are not allowed to exchange or refer to any online or printed material/book during the examination.

1. A system administrator claims that installing a firewall eliminates vulnerabilities. Which statement correctly evaluates this claim?
   A. Correct, because threats are removed by firewalls
   B. Incorrect, because vulnerabilities are weaknesses that may still exist internally
   C. Correct, because firewalls prevent all active attacks
   D. Incorrect, because threats and vulnerabilities are identical

2. The sender encrypts a message using the recipient's public key. The recipient decrypts the message using their private key. Identify the category of cryptographic implementation in this situation.
   A. Symmetric key cryptographic implementation
   B. Asymmetric key cryptographic implementation
   C. Single key cryptographic implementation
   D. Hash key cryptographic implementation
   E. none of these

3. What does the term "Phishing" refer to?
   A. Sending fraudulent emails to trick users into revealing sensitive information
   B. Installing a firewall for protection
   C. Encrypting data for security
   D. Preventing malware attacks

4. Which of the following is relatively more strong password compare to others?
   A. pass123word
   B. 1234567890
   C. Passw0r$26
   D. USERpassword
   E. YourPassword

5. What does Two-Factor Authentication (2FA) provide?
   A. A single method to log in securely
   B. Additional security by requiring two forms of verification
   C. Additional security by requiring use of two public keys
   D. A way to bypass security settings

6. An attacker intercepts network traffic and reads sensitive customer data without modifying it. Which cybersecurity principle has been violated?
   A. Integrity
   B. Availability
   C. Confidentiality
   D. Authentication
   E. Source Authentication

7. A company database was accessed by an unauthorized employee who modified several financial records. The system continued functioning normally without downtime. Which key aspect of cybersecurity is primarily affected?
   A. Availability only
   B. Integrity only
   C. Confidentiality and Availability
   D. Availability and Authentication
   E. DDos only

8. A cloud service provider experiences a temporary outage due to poor server maintenance. During the outage, no data is leaked or altered. Which statement best describes the security impact?
   A. Only Confidentiality is compromised
   B. Only Integrity is compromised
   C. Only Availability is compromised
   D. Confidentiality and Integrity are compromised

9. A ransomware attack encrypts all company files, preventing employees from accessing them. Before encryption, the attacker also copied sensitive data to an external server. Which combination of cybersecurity principles has been violated?
   A. Integrity and Availability
   B. Confidentiality and Availability
   C. Confidentiality and Integrity
   D. Integrity and Authentication only

10. In X.800, which security service ensures that only authorized users can access specific resources?
   A. Non-repudiation
   B. Access Control
   C. Data Confidentiality
   D. Data Integrity

11. A primary school server is running an outdated content management system. An attacker scans the server, finds the outdated version, and uses a known exploit to gain unauthorized administrative access. In this scenario, what is the vulnerability?
   A. The attacker scanning the server
   B. The outdated content management system
   C. The exploit script used
   D. The unauthorized access gained

12. An attacker intercepts a valid authentication message between a user and a banking server. Later, the attacker retransmits the exact same message to gain unauthorized access without modifying its contents. This attack is classified as _____ .
   A. Masquerade
   B. Fabrication
   C. Replay
   D. Passive eavesdropping

13. An organization enforces Multi-Factor Authentication (MFA). Even after passwords are stolen via a keylogger, attackers cannot access accounts. Why?
   A. MFA blocks malware installation
   B. MFA requires an additional authentication factor
   C. MFA encrypts all keystrokes
   D. MFA disables remote access

14. An attacker deploys malicious software on a victim's system. The malware is delivered through a phishing attachment, silently records all keystrokes, stores captured credentials, forwards them to a remote command-and-control server, and later uses the stolen information to perform fraudulent transactions. Which of the following activities is NOT directly related to the functional operation of a keylogger in this scenario?
    A. Installation
    B. Keystroke Logging
    C. Data Transmission
    D. Encryption of victim files for ransom
    E. Exploitation of stolen credentials

15. Identify the Threat Category for the Following Statement: "Cybercriminals utilize stolen personal information to engage in fraud or impersonate individuals."
    A. Identity Theft
    B. Ransomware
    C. DDos
    D. Virus-Worm
    E. Social Engineering

16. Which of the following does not qualify as a best practice for social media cybersecurity?
    A. Avoid sharing sensitive data such as your address, phone number, or financial details.
    B. Do not click on unknown links or attachments
    C. Limit the visibility of personal information on your social media profiles.
    D. Monitor account activity regularly to stay informed about any unauthorized access.
    E. Disable two-factor authentication for smooth operations

17. Identify the proper order of the Ransomware attack lifecycle:
    A. Infection -> Encryption -> Ransom demand -> Payment -> Decryption
    B. Encryption -> Infection -> Ransom demand -> Payment -> Decryption
    C. Infection -> Compression -> Encryption -> Ransom demand -> Decryption -> Payment
    D. Infection -> Decryption -> Ransom demand -> Encryption -> Payment
    E. Infection -> Encryption -> Ransom demand -> Decryption -> Payment

18. A hospital's computers are locked, and staff cannot access the operating system at all. No files appear encrypted, but users cannot log in. What type of ransomware is most likely involved?
    A. Crypto Ransomware
    B. Scareware
    C. Locker Ransomware
    D. Doxware

19. Which security service ensures that a sender cannot deny sending a message?
    A. Access Control
    B. Non-repudiation
    C. Data Confidentiality
    D. Authentication

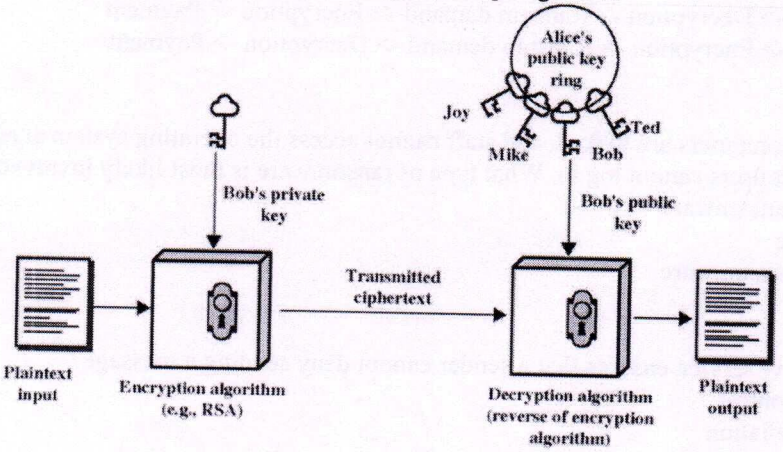
20. What does Data Integrity service in X.800 security ensure?
    A. Protection of data from unauthorized modification
    B. Protection against denial-of-service attacks
    C. Ensuring only authorized users can access the data
    D. Encrypting data for confidentiality

21. A sender is using Monoalphabetic encryption algorithm to encrypt a plaintext message using a key: "DKVQFIBJWPESCXHTMYAUOLRGZN". What will be the cipher text for a plaintext message "HELLOSTUDENTS" in this case? [0.25% negative marks for wrong answer].
    A. JFSSHAUOQFXUA
    B. JFSASHOUQFXUA
    C. JFSAAAUOQFXUA
    D. JFSSLLUOQFXUA
    E. None of these

22. If the plaintext is "PUNECOLLEGE" and the ciphertext is "EJCTRDAATVT", what is the shift value used during this encryption? [0.25% negative marks for wrong answer].
    A. 15
    B. 12
    C. 13
    D. 14
    E. 16
    F. 17

23. If the ciphertext is "DLIAOEHKLL" and you know it is encrypted using Rail Fence encryption technique with 2 rails setup, what is the plaintext? [0.25% negative marks for wrong answer].
    A. DELHIKALOL
    B. KALOLDELHI
    C. DELKALOLHI
    D. DELHIKALLO
    E. none of these

24. Following image shows implementation of one of the security service. Identify which of the following is achieved in this setup? [0.25% negative marks for wrong answer]. Figure9.1



    A. Authentication
    B. Integrity
    C. Availability
    D. Secret-key cryptography
    E. none of these

25. What is the encryption of "HAPPY" using following playfair key matrix? Type your answer in the given textbox. Image:Playfair-matrix

K	E	Y	W	O
R	D	A	B	C
F	G	H	I	L
M	N	P	Q	S
T	U	V	X	Z

Correct answer: _____

26. A sender is encrypting the plaintext message "HELLOAHMEDABADUNIVERSITY" using the Vigenère cipher. The sender chooses the word "SECRET" as the basis for generating the encryption key. What is the complete key used in this encryption process?
ANSWER: _____

27. Given that the ciphertext is "HDGJWXJHZYNYD" and it was encrypted using the Caesar cipher with a shift of 5, what would the plaintext be? Write your answer in the provided space.
ANSWER: _____

28. Match the following:
Use of Virtual Keyboards : Prevents keystroke logging.
Antivirus and Anti-Malware Tools : Detect and remove keyloggers.
Regular Software Updates : Patching vulnerabilities prevents infections.
Multi-Factor Authentication (MFA) : Adds an extra security layer.
Network Monitoring : Identifies unusual data transmission activities.

29. Match the following:
Malware : Malicious software like viruses, worms, and ransomware.
Phishing : Fraudulent attempts to obtain sensitive information through fake emails or websites.
Denial of Service (DoS) Attacks : Overloading systems to make them unavailable.
Man-in-the-Middle (MITM) Attacks : Intercepting communications between two parties.

30. Which of the following is not a substitution type of cipher? [0.25% negative marks for each wrong selection]
A. Monoalphabetic
B. Polyalphabetic
C. Vigenère Cipher
D. Caesar Cipher
E. Columnar
F. Rail Fence Cipher
ANSWER: _____