In Class Activity 01

1. What is cryptography primarily concerned with?

A. Storing large data efficiently
B. Protecting information from unauthorized access
C. Improving network speed
D. Designing hardware

2. Cryptography mainly helps to protect:

A. Software performance
B. Data, communication, and identity
C. Internet bandwidth
D. Operating systems

3. Which statement best describes cryptography?

A. It prevents all cyber attacks
B. It detects malware automatically
C. It limits the damage when attacks occur
D. It removes vulnerabilities

4. Why is cryptography necessary in modern systems?

A. Data travels only in private networks
B. Data is always encrypted automatically
C. Data travels over untrusted networks
D. Data cannot be intercepted

5. Which of the following is NOT an everyday use of cryptography?

A. WhatsApp messaging
B. Online banking
C. Word document editing
D. HTTPS websites

6. CIA triad stands for:

A. Confidentiality, Integrity, Authorization
B. Control, Integrity, Availability

C. Confidentiality, Integrity, Availability
D. Control, Identity, Access

7. Which security goal ensures that only authorized users can read data?

A. Integrity
B. Availability
C. Confidentiality
D. Authentication

8. Unauthorized modification of data is a violation of:

A. Confidentiality
B. Integrity
C. Availability
D. Authentication

9. Banking mobile app downtime mainly affects:

A. Integrity
B. Confidentiality
C. Availability
D. Authorization

10. Which technique helps preserve confidentiality?

A. Encryption
B. Backup
C. Version control
D. Logging

11. Hashing is mainly used to support:

A. Availability
B. Integrity
C. Authorization
D. Accounting

12. Which security function answers the question: “Who are you?”

A. Authorization
B. Accounting
C. Authentication
D. Integrity

13. Which factor represents “Something you have”?

A. Password
B. Fingerprint
C. Voice
D. Smart card

14. Authorization determines:

A. Who the user is
B. What the user can access
C. How data is encrypted
D. When logs are created

15. A user can authenticate successfully but still be denied access because of:

A. Accounting
B. Encryption
C. Authorization
D. Integrity

16. Which AAA component keeps records of user activity?

A. Authentication
B. Authorization
C. Accounting
D. Availability

17. Non-repudiation ensures that:

A. Messages cannot be modified
B. Sender cannot deny sending a message
C. Systems remain online
D. Passwords are encrypted

18. A weakness in a system that can be exploited is called:

A. Threat
B.Risk
C. Vulnerability
D. Attack

19. A potential danger that may exploit a vulnerability is called:

A. Threat
B. Risk
C. Attack
D. Asset

20. Any action that compromises security is known as:

A. Risk
B. Vulnerability
C. Threat
D. Attack

21. Risk can be expressed as:

A. Threat + Vulnerability
B. Likelihood × Impact
C. Attack – Control
D. Asset ÷ Threat

22. Attacks can be categorized mainly into:

A. Logical and physical
B. Internal and external
C. Passive and active
D. Hardware and software

23. Which of the following is a passive attack?

A. Modifying a database record
B. Stealing network traffic silently
C. Deleting files
D. Blocking a server

24. Which action represents an active attack?

A. Eavesdropping
B. Traffic monitoring
C. Message modification
D. Packet sniffing

25. When one entity pretends to be another, it is called:

A. Replay
B. Masquerade

C. DoS
D. Modification

26. Capturing and retransmitting valid data to gain unauthorized access is called:

A. Modification
B. Masquerade
C. Replay
D. Interception

27. Preventing legitimate users from accessing services is known as:

A. Replay
B. Masquerade
C. Denial of Service
D. Spoofing

28. Which of the following best describes a motive of cyber attacks?

A. Improving system performance
B. Data compression
C. Financial gain
D. Software testing

29. WannaCry is an example of:

A. Hardware failure
B. Natural disaster
C. Cyber attack
D. System update

30. Which statement is TRUE about cryptography?

A. It replaces secure coding
B. It guarantees system availability
C. It supports security objectives
D. It eliminates all vulnerabilities