

UNIT 1: SECURITY CONCEPTS

1. Computer security deals primarily with protecting data from:

- a) Hardware failure
- b) Unauthorized access, use, disclosure, disruption, modification, or destruction
- c) Power outages
- d) Software bugs only

Answer: b

2. Which of the following is NOT one of the three main goals of security (CIA triad)?

- a) Confidentiality
- b) Integrity
- c) Availability
- d) Authentication

Answer: d (Authentication is a security service, not part of the core CIA triad)

3. The need for security arises mainly because of:

- a) Increasing use of networks and the internet for sensitive transactions
- b) Decreasing computer usage
- c) Lack of computers
- d) None of the above

Answer: a

4. Which security approach builds security into the system from the design phase itself?

- a) Reactive approach
- b) Proactive (security by design) approach
- c) Trial and error approach
- d) Random approach

Answer: b

5. Which of the following is a fundamental principle of security?

- a) Confidentiality
- b) Integrity
- c) Availability
- d) All of the above

Answer: d

CRYPTOGRAPHY AND NETWORK SECURITY

6. Non-repudiation ensures that:

- a) Data cannot be accessed by unauthorized users
- b) A sender cannot deny having sent a message
- c) Data is always available
- d) Data is encrypted

Answer: b

7. Which of the following is an example of a passive attack?

- a) Denial of Service
- b) Masquerading
- c) Traffic analysis
- d) Message modification

Answer: c

8. Which of the following is an example of an active attack?

- a) Eavesdropping
- b) Traffic analysis
- c) Replay attack
- d) Release of message contents

Answer: c

9. An attack that prevents or inhibits normal use of communication facilities is called:

- a) Masquerade
- b) Denial of Service (DoS)
- c) Traffic analysis
- d) Snooping

Answer: b

10. In a replay attack, the attacker:

- a) Creates a fake message from scratch
- b) Captures data and retransmits it later to produce an unauthorized effect
- c) Blocks all communication
- d) Decrypts data instantly

Answer: b

11. Which security service ensures that the sender and receiver of a message are who they claim to be?

- a) Confidentiality
- b) Authentication
- c) Availability
- d) Access control

Answer: b

CRYPTOGRAPHY AND NETWORK SECURITY

12. Which of the following is an access control security mechanism?

- a) Encryption
- b) Digital signature
- c) Password and biometric verification
- d) Notarization

Answer: c

13. Which security mechanism is used to provide proof of the origin and integrity of data using a trusted third party?

- a) Traffic padding
- b) Notarization
- c) Routing control
- d) Access control

Answer: b

14. In the OSI security architecture, security mechanisms are used to implement:

- a) Security attacks
- b) Security services
- c) Security policies
- d) Network topology

Answer: b

15. In the model for network security, the "trusted third party" is responsible for:

- a) Attacking the system
- b) Distributing secret information to both principals while keeping it from any opponent
- c) Monitoring network traffic only
- d) Creating malware

Answer: b

16. Which of the following best defines a security attack?

- a) An action that compromises the security of information owned by an organization
- b) A routine system update
- c) A backup procedure
- d) A firewall configuration

Answer: a

Unit 2: Cryptography Concepts and Techniques

17. The original message before encryption is called:

- a) Cipher text
- b) Plain text
- c) Key text
- d) Hash text

Answer: b

CRYPTOGRAPHY AND NETWORK SECURITY

18. The encrypted, unreadable form of a message is called:

- a) Plain text
- b) Cipher text
- c) Hash value
- d) Digest

Answer: b

19. The process of converting plain text into cipher text is called:

- a) Decryption
- b) Encryption
- c) Steganography
- d) Hashing

Answer: b

20. The process of converting cipher text back into plain text is called:

- a) Encryption
- b) Decryption
- c) Encoding
- d) Compression

Answer: b

21. In the Caesar cipher, each letter in the plain text is:

- a) Replaced by a letter some fixed number of positions down the alphabet
- b) Rearranged in reverse order
- c) Removed entirely
- d) Converted to a number and added

Answer: a

22. Caesar cipher is an example of:

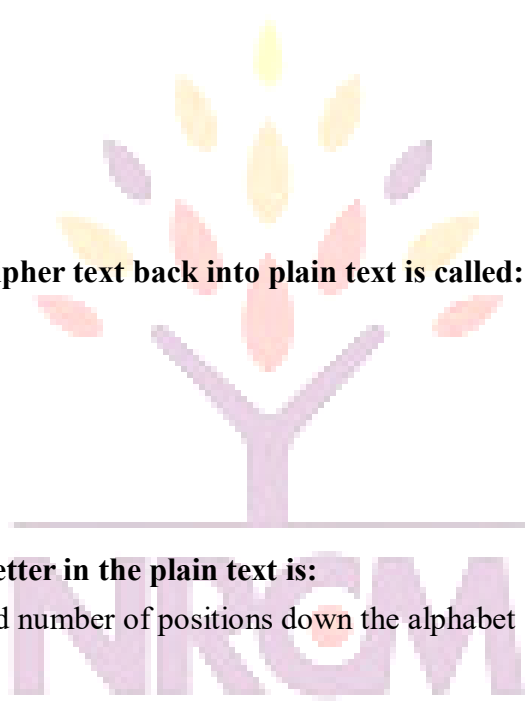
- a) Transposition technique
- b) Substitution technique
- c) Asymmetric encryption
- d) Hashing technique

Answer: b

23. In the Playfair cipher, plain text letters are encrypted in:

- a) Single letters
- b) Pairs (digraphs)
- c) Groups of four
- d) Random order

Answer: b



your roots for success...

NARSIMHA REDDY
ENGINEERING COLLEGE

CRYPTOGRAPHY AND NETWORK SECURITY

24. Which cipher uses a 5x5 matrix of letters constructed using a keyword?

- a) Caesar cipher
- b) Playfair cipher
- c) Rail fence cipher
- d) Vigenère cipher

Answer: b

25. The Vigenère cipher is a type of:

- a) Monoalphabetic substitution cipher
- b) Polyalphabetic substitution cipher
- c) Transposition cipher
- d) Steganographic technique

Answer: b

26. In transposition techniques, the encryption is performed by:

- a) Replacing characters with other characters
- b) Rearranging the order/position of the plain text characters
- c) Hiding data inside images
- d) Generating random keys

Answer: b

27. Which of the following is an example of a transposition technique?

- a) Caesar cipher
- b) Playfair cipher
- c) Rail fence cipher
- d) Vigenère cipher

Answer: c

28. In a rail fence cipher with depth 2, the plain text is written in a:

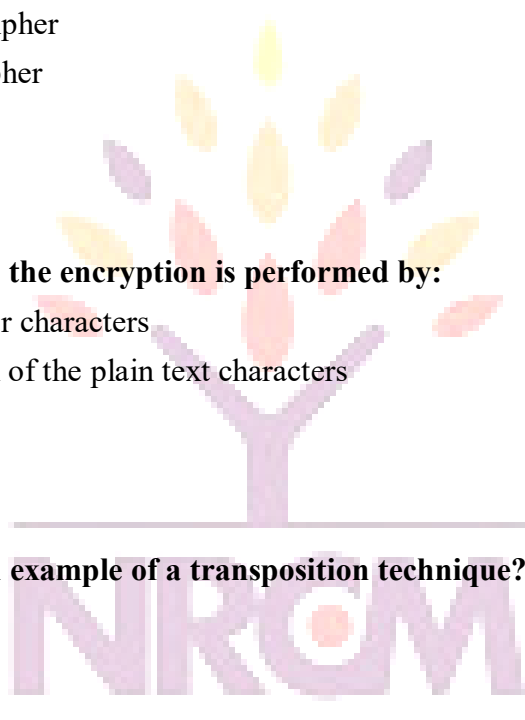
- a) Single straight line
- b) Zigzag pattern across two rows
- c) Circular pattern
- d) Random matrix

Answer: b

29. In symmetric key cryptography, encryption and decryption use:

- a) Two different keys
- b) The same key
- c) No key
- d) A public key only

Answer: b



your tools for success...

NARSIMHA REDDY
ENGINEERING COLLEGE

CRYPTOGRAPHY AND NETWORK SECURITY

30. Which of the following is a symmetric key algorithm?

- a) RSA
- b) DES (Data Encryption Standard)
- c) Diffie-Hellman
- d) Digital Signature Algorithm

Answer: b

31. In asymmetric key cryptography, two different keys used are:

- a) Public key and private key
- b) Primary key and secondary key
- c) Master key and slave key
- d) Session key and shared key

Answer: a

32. Which of the following is an asymmetric key algorithm?

- a) DES
- b) AES
- c) RSA
- d) Triple DES

Answer: c

33. In asymmetric cryptography, the public key is used to:

- a) Decrypt only
- b) Encrypt the message that only the corresponding private key can decrypt
- c) Hide the message permanently
- d) Generate random numbers

Answer: b

34. Steganography is best described as:

- a) The science of breaking codes
- b) The technique of hiding a secret message within another non-secret medium (such as an image)
- c) A symmetric encryption algorithm
- d) A type of transposition cipher

Answer: b

35. The main difference between steganography and cryptography is that:

- a) Cryptography hides the existence of a message, steganography scrambles it
- b) Steganography hides the existence of a message, cryptography scrambles its content
- c) Both are exactly the same
- d) Steganography is faster than cryptography

Answer: b

CRYPTOGRAPHY AND NETWORK SECURITY

36. The "key range" refers to:

- a) The total number of possible keys that can be generated by an algorithm
- b) The physical distance over which a key can be transmitted
- c) The size of the plain text
- d) The number of users in a network

Answer: a

37. The "key size" of an encryption algorithm is generally measured in:

- a) Meters
- b) Bits
- c) Bytes of plain text
- d) Seconds

Answer: b

38. A larger key size generally provides:

- a) Weaker security and slower processing
- b) Stronger security against brute-force attacks
- c) No effect on security
- d) Faster but less secure encryption

Answer: b

39. An attack in which the attacker tries every possible key until the correct one is found is called:

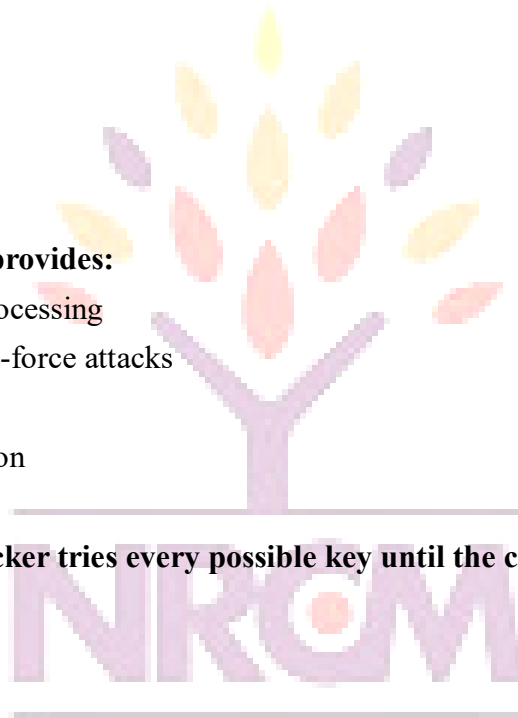
- a) Cipher text-only attack
- b) Brute-force attack
- c) Chosen plaintext attack
- d) Replay attack

Answer: b

40. In a known-plaintext attack, the attacker has access to:

- a) Only the cipher text
- b) Some plain text and its corresponding cipher text
- c) The private key directly
- d) Nothing at all

Answer: b



your roots for success...

NARSIMHA REDDY
ENGINEERING COLLEGE

CRYPTOGRAPHY AND NETWORK SECURITY



your roots for success...

NARSIMHA REDDY ENGINEERING COLLEGE