DDoS, HTTPS, IDS,

Unitwise Multiple Choice Questions

Select the correct option.

Unit-I

1. **Which of the following is a type of malware that disguises itself as a legitimate file or program?**
   a. Virus b. Worm
   [✓ c. Trojan Horse] d. Spyware

2. **What is a DDoS attack?**
   a. Direct Denial of Service
   [✓ b. Distributed Denial of Service]
   c. Data Disclosure Service
   d. Dangerous Denial of Service

3. **Which of the following is a social engineering attack that involves manipulating individuals to disclose confidential information?**
   [✓ a. Phishing] b. Spoofing
   c. DDoS d. Ransomware

4. **What does the term 'SQL injection' refer to in the context of security attacks?**
   [✓ a. Injecting code to exploit vulnerabilities in a web application's database]
   b. Injecting viruses into the system
   c. Injecting malicious scripts in emails
   d. Injecting malware into the network

5. **What is the purpose of a firewall in network security?**
   a. To detect and remove viruses
   [✓ b. To block unauthorised access and control traffic]
   c. To encrypt communication between devices
   d. To monitor network performance

6. **Which of the following is an example of a passive attack?**
   a. Brute force attack
   b. Denial of Service (DoS) attack
   [✓ c. Eavesdropping]
   d. Spoofing

7. **What does the acronym 'HTTPS' stand for in the context of web security?**
   [✓ a. HyperText Transfer Protocol Secure]
   b. Hyperlink Text Protocol System
   c. High-Efficiency Transfer Protocol for Secure websites
   d. Home Encryption and Transfer Protocol System

8. **Which security measure involves the use of a unique, secret key that only the communicating parties know?**
   [✓ a. Symmetric encryption]
   b. Asymmetric encryption
   c. Hashing
   d. Firewall

9. **What is the main purpose of Intrusion Detection System (IDS)?**
   a. To prevent attacks from occurring
   [✓ b. To monitor and detect suspicious activities in a network]
   c. To encrypt communication between devices
   d. To remove malware from the system

10. **Which of the following is a common authentication factor based on something a user knows?**
    a. Fingerprint b. Retina scan
    [✓ c. Password] d. Smart card

11. **Which security service ensures that information is not disclosed to unauthorised individuals or systems?**
    a. Authentication b. Integrity
    [✓ c. Confidentiality] d. Availability

12. **What security mechanism verifies the identity of a user or system?**
    a. Authorisation [✓ b. Authentication]
    c. Encryption d. Access control

13. **In the context of computer security, what does the term 'integrity' refer to?**
    a. Ensuring that information is not disclosed to unauthorised individuals
    b. Verifying the identity of a user or system
    [✓ c. Protecting information from unauthorised modification]
    d. Ensuring the availability of information

14. **Which security service ensures that information is available when needed and that systems can withstand attacks or failures?**
    a. Authentication b. Integrity
    c. Confidentiality [✓ d. Availability]

15. What security mechanism involves encoding information to make it unintelligible to unauthorised individuals?

a. Hashing

b. Access control

[✓ c. Encryption]

d. Digital signatures

16. Which security service ensures that individuals or systems have the appropriate permissions to access resources?

a. Authentication

[✓ b. Authorisation]

c. Confidentiality

d. Availability

17. What is the purpose of a digital signature in security mechanisms?

a. Encrypting information

[✓ b. Verifying the integrity and authenticity of a message]

c. Controlling access to resources

d. Ensuring the availability of information

18. Which security mechanism involves using a unique identifier to control access to resources?

a. Encryption

[✓ b. Access control]

c. Digital signatures

d. Hashing

19. What security service involves ensuring that information is not altered or tampered with during transmission?

a. Authentication

[✓ b. Integrity]

c. Confidentiality

d. Availability

20. What is the primary purpose of a firewall in the context of security mechanisms?

a. Encryption

[✓ b. Access control]

c. Digital signatures

d. Availability

21. What is plaintext in the context of cryptography?

a. Encrypted data

b. Data that has undergone a hashing process

[✓ c. Original, unencrypted data]

d. Digital signature of data

22. In a cryptographic system, what term is used to refer to the process of converting plaintext into ciphertext?

[✓ a. Encryption]

b. Decryption

c. Hashing

d. Salting

23. Which of the following is an example of plaintext?

a. Cipher

b. Hash

c. Encrypted message

[✓ d. Clear, readable message]

24. What is the main purpose of encrypting plaintext?

a. To compress data

b. To ensure data integrity

[✓ c. To protect data confidentiality]

d. To create digital signatures

25. Which cryptographic term is associated with converting ciphertext back into plaintext?

[✓ a. Decryption]

b. Encryption

c. Hashing

d. Salting

26. What is the relationship between plaintext and ciphertext in a cryptographic process?

a. They are the same

b. Ciphertext is derived from the hash of plaintext

[✓ c. Ciphertext is the result of encrypting plaintext]

d. Plaintext is a type of ciphertext

27. In the context of encryption, what is the importance of the key used in the process?

a. It defines the length of the plaintext

b. It determines the color of the ciphertext

[✓ c. It controls the encryption and decryption process]

d. It is used for data compression

28. Which cryptographic concept involves using the same key for both encryption and decryption?

a. Asymmetric encryption

[✓ b. Symmetric encryption]

c. Hashing

d. Digital signatures

29. What does the term 'clear text' refer to in the context of cryptography?

a. Encrypted data

[✓ b. Data that is readable without decryption]

c. Hashed data

d. Digital signature

30. What type of information is typically not suitable for transmission as plaintext over insecure networks?

a. Public keys

b. Digital signatures

[✓ c. Passwords]

d. Hash values

31. What is the primary purpose of encryption in the context of information security?

a. Compression of data

b. Authentication of users

[✓ c. Protection of data confidentiality]

d. Ensuring data integrity

32. Which type of encryption uses the same key for both encryption and decryption?

a. Asymmetric encryption
[✓ b. Symmetric encryption]
c. Public-key encryption
d. Private-key encryption

33. In public-key cryptography, which key is used for encryption?

a. Private key
[✓ b. Public key]
c. Session key
d. Symmetric key

34. What is the term for the mathematical function that transforms plaintext into ciphertext in encryption?

a. Hash function
[✓ b. Cipher]
c. Key exchange algorithm
d. Digital signature

35. Which encryption algorithm is commonly used for securing internet communication, including HTTPS?

a. DES (Data Encryption Standard)
b. RSA (Rivest-Shamir-Adleman)
[✓ c. AES (Advanced Encryption Standard)]
d. SHA (Secure Hash Algorithm)

36. What does the term 'key length' refer to in encryption algorithms?

a. The size of the plaintext
b. The size of the ciphertext
[✓ c. The length of the encryption key]
d. The length of the decryption key

37. Which of the following is an example of a symmetric encryption algorithm?

a. RSA
b. ECC (Elliptic Curve Cryptography)
[✓ c. Blowfish]
d. Diffie-Hellman

38. In what type of attack does an attacker intercept and alter communication between two parties without their knowledge?

a. Brute force attack
[✓ b. Man-in-the-middle attack]
c. DoS (Denial of Service) attack
d. Phishing attack

39. What is the term for the process of converting ciphertext back into plaintext?

a. Encryption
[✓ b. Decryption]
c. Hashing
d. Key exchange

40. Which encryption technique uses a pair of keys, one for encryption and one for decryption?

a. Symmetric encryption
[✓ b. Asymmetric encryption]
c. Public-key encryption
d. Private-key encryption

41. What is the primary purpose of a cryptographic key in encryption?

a. To compress data
b. To authenticate users
[✓ c. To control the encryption and decryption process]
d. To ensure data integrity

42. In symmetric encryption, what is the relationship between the encryption key and the decryption key?

[✓ a. They are the same key]
b. The encryption key is a public key and the decryption key is private
c. The encryption key is private and the decryption key is public
d. They are unrelated

43. What is the term for the process of converting plaintext into ciphertext using a cryptographic algorithm and a key?

a. Decryption
b. Hashing
[✓ c. Encryption]
d. Salting

44. In asymmetric encryption, which key is kept private by the owner?

a. Public key
b. Session key
[✓ c. Private key]
d. Shared key

45. What does the term 'ciphertext' refer to in the context of cryptography?

[✓ a. Encrypted data]
b. Original, unencrypted data
c. Hashed data
d. Digital signature

46. Which of the following is true regarding the relationship between plaintext and ciphertext?

a. They are always the same
b. Ciphertext is derived from the hash of plaintext
[✓ c. Ciphertext is the result of encrypting plaintext]
d. Plaintext is a type of ciphertext

47. What term is used for the key used in symmetric encryption that must be kept secret and secure between communicating parties?

a. Public key
b. Private key
[✓ c. Shared key]
d. Session key

48. In public-key cryptography, which key is used for encryption?

a. Private key
[✓ b. Public key]
c. Session key
d. Symmetric key

49. What is the term for the process of converting ciphertext back into plaintext?

a. Encryption
[✓ b. Decryption]
c. Hashing
d. Salting

50. What is the significance of key length in encryption algorithms?

a. Determines the color of the ciphertext
b. Affects the size of the plaintext
c. Controls the encryption and decryption process
[✓ d. Influences the security of the encryption]

51. What is the primary purpose of decryption in the context of cryptography?

a. To compress data
b. To authenticate users
[✓ c. To convert ciphertext back into plaintext]
d. To ensure data integrity

52. In symmetric encryption, what key is used for the decryption process?

a. Public key
b. Session key
c. Private key
[✓ d. Shared key]

53. Which term is used for the process of breaking a cryptographic system or code without knowledge of the key?

a. Decryption
b. Encryption
[✓ c. Cryptanalysis]
d. Hashing

54. What does the term 'brute force attack' refer to in the context of decryption and cryptanalysis?

[✓ a. Systematic trial-and-error to find the decryption key]
b. Decrypting data using advanced mathematical algorithms
c. Collaborative effort to break a cryptographic system
d. Using social engineering to obtain the decryption key

55. In asymmetric encryption, which key is used for decryption, and is kept secret by the owner?

a. Public key
b. Session key
[✓ c. Private key]
d. Shared key

56. What is the primary goal of cryptanalysis?

a. To create secure cryptographic algorithms
[✓ b. To break or decipher encrypted messages]
c. To compress data efficiently
d. To authenticate users

57. What is a chosen plaintext attack in cryptanalysis?

[✓ a. Attack where the adversary can choose the plaintexts to be encrypted]
b. Attack where the adversary can choose the ciphertexts to be decrypted
c. Attack where the adversary can modify the encryption algorithm
d. Attack where the adversary can guess the decryption key

58. What is frequency analysis in cryptanalysis?

[✓ a. Analysing the frequency of occurrence of letters or symbols in ciphertext]
b. Analysing the frequency of system updates
c. Counting the frequency of login attempts
d. Measuring the frequency of data backups

59. What is a weakness of the Caesar cipher, making it vulnerable to cryptanalysis?

a. Use of a long key
[✓ b. Use of a short key]
c. Complexity of the encryption algorithm
d. Integration of modern cryptographic techniques

60. What does the term 'known-plaintext attack' refer to in cryptanalysis?

a. Attack where the adversary knows the ciphertext and wants to find the plaintext
[✓ b. Attack where the adversary knows both the plaintext and the ciphertext]
c. Attack where the adversary knows only the ciphertext
d. Attack where the adversary knows the encryption key

61. In public-key encryption, how many keys are used for the encryption and decryption processes?

a. One
[✓ b. Two]
c. Three
d. Four

62. Which key is kept private by the owner in a public-key encryption system?

a. Public key
b. Session key
[✓ c. Private key]
d. Shared key

63. What is the primary advantage of public-key encryption over symmetric encryption?

a. Faster encryption and decryption
b. Simplicity of key management
[✓ c. Ability to securely share information without a shared key]
d. Higher level of encryption security

64. What is the purpose of the public key in public-key encryption?

a. It is used for decryption

[✓ b. It is used for encryption]

c. It is a shared key between parties

d. It is a session key

65. Which algorithm is commonly used in public-key encryption for secure communication on the internet?

a. DES (Data Encryption Standard)

[✓ b. RSA (Rivest-Shamir-Adleman)]

c. AES (Advanced Encryption Standard)

d. Diffie-Hellman

66. In public-key cryptography, what is the purpose of the private key?

a. It is used for encryption

[✓ b. It is used for decryption]

c. It is shared between parties

d. It is used for key exchange

67. What is the term for the process of using one's private key to validate a digital signature?

a. Encryption

b. Decryption

[✓ c. Signing]

d. Hashing

68. Which of the following is a common use case for public-key encryption?

a. Encrypting large files for efficiency

[✓ b. Securely exchanging symmetric keys]

c. Encrypting data for storage

d. Encrypting data for communication with a single party

69. What is a potential drawback of public-key encryption compared to symmetric encryption?

[✓ a. Slower encryption and decryption processes]

b. Complexity of key management

c. Limited security

d. Requirement for a shared key

70. What is the Diffie-Hellman key exchange used for in public-key cryptography?

a. Encrypting data

b. Decrypting data

[✓ c. Securely exchanging symmetric keys]

d. Creating digital signatures