TEST YOUR KNOWLEDGE WITH TOP MULTIPLE CHOICE QUESTIONS

#1. What is the process of converting ciphertext back into plaintext called in cryptography?

☐
A. Encryption
☐
B. Hashing
☐
C. Decryption
☐
D. Compression
☐
E. Encoding

#2. Which encryption algorithm is known for its use in digital signatures and is considered secure for long-term use?

☐
A. RSA
☐
B. DES
☐
C. AES
☐
D. SHA-256
☐
E. HMAC

#3. What is the purpose of a rainbow table in the context of password security?

☐

A. Data Encryption
☐
B. Data Compression
☐
C. Password Cracking
☐
D. Data Sorting
☐
E. Data Integrity

#4. Which cryptographic hash function is commonly used for password storage and is designed to be slow and computationally intensive?

☐
A. MD5
☐
B. SHA-1
☐
C. SHA-256
☐
D. SHA-512
☐
E. HMAC

#5. Which encryption algorithm operates on blocks of data and is often used in modes like ECB, CBC, and OFB?

☐
A. RSA
☐
B. DES
☐
C. AES
☐

D. HMAC

☐

E. MD5

#6. What is the purpose of a digital certificate in the context of web security?

☐

A. Verify user's identity

☐

B. Encrypt data traffic

☐

C. Provide access control

☐

D. Monitor network traffic

☐

E. Authenticate websites

#7. Which type of cryptography uses the same key for both encryption and decryption?

☐

A. Asymmetric

☐

B. Symmetric

☐

C. Public Key

☐

D. Private Key

☐

E. Hybrid

#8. Which of the following is NOT a symmetric encryption algorithm?

☐

A. DES

☐
B. RSA
☐
C. AES
☐
D. 3DES
☐
E. Blowfish

#9. What is the purpose of key exchange algorithms in cryptography?

☐
A. Encrypt data traffic
☐
B. Generate keys
☐
C. Authenticate users
☐
D. Secure email communication
☐
E. Password hashing

#10. Which encryption algorithm is commonly used for secure communication over the internet and supports key sizes of 128, 192, or 256 bits?

☐
A. AES
☐
B. DES
☐
C. RSA
☐
D. MD5
☐
E. SHA

#11. In the Diffie-Hellman key exchange protocol, what is exchanged between the parties to establish a shared secret key?

☐
A. Private keys
☐
B. Public keys
☐
C. Symmetric keys
☐
D. Session keys
☐
E. Authentication keys

#12. Which type of attack exploits the reuse of initialization vectors (IVs) in encryption algorithms like WEP and TKIP?

☐
A. Brute Force Attack
☐
B. Man-in-the-Middle
☐
C. Replay Attack
☐
D. Birthday Attack
☐
E. Collision Attack

#13. What is the purpose of a nonce in cryptographic protocols?

☐
A. Random number generation
☐
B. Data Encryption

☐
C. Data Compression
☐
D. Data Integrity
☐
E. Data Storage

#14. Which encryption mode ensures that the same plaintext block encrypted multiple times produces different ciphertexts?

☐
A. Electronic Codebook (ECB)
☐
B. Cipher Block Chaining (CBC)
☐
C. Cipher Feedback (CFB)
☐
D. Output Feedback (OFB)
☐
E. Counter (CTR)

#15. Which type of encryption algorithm operates on a continuous stream of data and is commonly used in wireless networks?

☐
A. Symmetric stream cipher
☐
B. Asymmetric stream cipher
☐
C. Symmetric block cipher
☐
D. Asymmetric block cipher
☐
E. Hash function

#16. What is the main advantage of the elliptic curve cryptography (ECC) algorithm over traditional public-key algorithms?

☐
A. Shorter key lengths
☐
B. Faster computation
☐
C. Simplicity of implementation
☐
D. Higher security level
☐
E. Lower memory requirements

#17. Which cryptographic algorithm is commonly used for secure email communication and provides both encryption and authentication?

☐
A. RSA
☐
B. AES
☐
C. DES
☐
D. PGP
☐
E. HMAC

#18. What is the purpose of a Hardware Security Module (HSM) in cryptography?

☐
A. Generate keys
☐
B. Securely store keys

☐
C. Encrypt data traffic
☐
D. Authenticate users
☐
E. Hashing

#19. In the context of public-key cryptography, what is the purpose of the Certificate Authority (CA)?

☐
A. Encrypt data traffic
☐
B. Store public keys
☐
C. Verify user's identity
☐
D. Generate private keys
☐
E. Sign digital certificates

#20. Which type of encryption algorithm uses the same key for both encryption and decryption and is commonly used for securing data transmission?

☐
A. Symmetric
☐
B. Asymmetric
☐
C. Public Key
☐
D. Hybrid
☐
E. Session Key

Next

Results