

TEST YOUR KNOWLEDGE WITH TOP MULTIPLE CHOICE QUESTIONS

#1. Which encryption algorithm is commonly used for securing wireless networks and is part of the WPA3 standard?

☐

A. AES

☐

B. DES

☐

C. RSA

☐

D. ChaCha20

☐

E. Blowfish

#2. What is the purpose of a salt in password hashing?

☐

A. Encrypt data traffic

☐

B. Data Integrity

☐

C. Secure password storage

☐

D. Random number generation

☐

E. Authenticate users

#3. Which encryption algorithm is widely used for securing web traffic and is supported by most web browsers?

☐

A. AES

☐

B. DES

☐

C. RSA

☐

D. ECC

☐

E. SSL/TLS

#4. What is the purpose of key stretching in password hashing algorithms?

☐

A. Increase key length

☐

B. Generate random keys

☐

C. Slow down brute force attacks

☐

D. Simplify key management

☐

E. Enhance encryption strength

#5. Which cryptographic algorithm is commonly used for secure email communication and provides both encryption and digital signatures?

☐

A. RSA

☐

B. AES

☐

C. DES

☐

D. PGP

☐

E. HMAC

#6. In public-key cryptography, what is the purpose of a digital certificate?

☐

A. Encrypt data traffic

☐

B. Sign public keys

☐

C. Authenticate users

☐

D. Store private keys

☐

E. Generate session keys

#7. What is the main advantage of using elliptic curve cryptography (ECC) over RSA in terms of key size?

☐

A. ECC keys are shorter

☐

B. ECC keys are longer

☐

C. ECC keys are faster to generate

☐

D. ECC keys are more secure

☐

E. ECC keys are easier to manage

#8. Which cryptographic hash function is known for its collision resistance and is commonly used in digital signatures and certificates?

☐

A. MD5

☐

B. SHA-1

☐

C. SHA-256

☐

D. SHA-512

☐

E. RIPEMD-160

#9. What is the purpose of a digital envelope in public-key cryptography?

☐

A. Encrypt data traffic

☐

B. Decrypt data traffic

☐

C. Sign digital certificates

☐

D. Generate session keys

☐

E. Authenticate users

#10. 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)

#11. What is the primary purpose of the Certificate Revocation List (CRL) in public-key infrastructure (PKI)?

☐

A. Encrypt data traffic

☐

B. Authenticate users

☐

C. Verify the integrity of messages

☐

D. Revoke compromised certificates

☐

E. Generate digital signatures

#12. 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

#13. 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

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

☐

A. Encryption

☐

B. Hashing

☐

C. Decryption

☐

D. Compression

☐

E. Encoding

#15. 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

#16. 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

#17. 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

#18. 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 Attack

☐

C. Replay Attack

☐

D. Birthday Attack

☐

E. Collision Attack

#19. 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

#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

