TEST YOUR KNOWLEDGE WITH TOP MULTIPLE CHOICE QUESTIONS

#1. Which cryptographic algorithm is commonly used for digital signatures and supports both encryption and authentication?

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

#2. What is the primary 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

#3. Which encryption algorithm operates on blocks of data and divides the plaintext into fixed-size blocks during encryption?

☐

A. Stream cipher
☐
B. Block cipher
☐
C. Hybrid cipher
☐
D. Hash function
☐
E. Asymmetric cipher

#4. In Diffie-Hellman key exchange, which of the following is publicly shared between the parties but never transmitted?

☐
A. Private key
☐
B. Public key
☐
C. Session key
☐
D. Initialization vector
☐
E. Authentication key

#5. Which cryptographic algorithm is commonly used for secure email communication and can be used for data encryption and digital signatures?

☐
A. RSA
☐
B. AES
☐
C. DES
☐

D. PGP

☐

E. HMAC

#6. What is the primary purpose of a certificate revocation list (CRL) in public-key infrastructure (PKI)?

☐

A. Authenticate users

☐

B. Encrypt data traffic

☐

C. Verify the integrity of messages

☐

D. Revoke compromised certificates

☐

E. Generate digital signatures

#7. Which encryption algorithm is widely used for securing wireless networks and is part of the WPA2 standard?

☐

A. AES

☐

B. DES

☐

C. RSA

☐

D. 3DES

☐

E. Blowfish

#8. 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

#9. 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)

#10. 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

#11. 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

#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. 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

#14. 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

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

☐
A. Encryption
☐
B. Hashing
☐
C. Decryption

☐
D. Compression
☐
E. Encoding

#16. 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

#17. 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

#18. 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

#19. 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

#20. 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

Next

Results