Quiz: Public Key Cryptography

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the primary advantage of asymmetric over symmetric cryptography for blockchains?
A) Faster encryption B) Smaller keys C) No key distribution problem D) Lower cost

Quiz (1–5)

Q1. What is the primary advantage of asymmetric over symmetric cryptography for blockchains?
A) Faster encryption B) Smaller keys C) No key distribution problem D) Lower cost
Answer: C – No need to securely share keys between parties.

Q2. In ECC, how is the public key derived from the private key?
A) Hash function B) $Q = k \cdot G$ C) Random generation D) Encryption

Quiz (1–5)

Q1. What is the primary advantage of asymmetric over symmetric cryptography for blockchains?
A) Faster encryption B) Smaller keys C) No key distribution problem D) Lower cost
Answer: C – No need to securely share keys between parties.

Q2. In ECC, how is the public key derived from the private key?
A) Hash function B) $Q = k \cdot G$ C) Random generation D) Encryption
Answer: B – Public key Q = private key k multiplied by generator point G.

Q3. Which elliptic curve does Bitcoin use?
A) secp192k1 B) secp256k1 C) NIST P-256 D) Ed25519

Quiz (1–5)

Q1. What is the primary advantage of asymmetric over symmetric cryptography for blockchains?
A) Faster encryption B) Smaller keys C) No key distribution problem D) Lower cost
Answer: C – No need to securely share keys between parties.

Q2. In ECC, how is the public key derived from the private key?
A) Hash function B) $Q = k \cdot G$ C) Random generation D) Encryption
Answer: B – Public key Q = private key k multiplied by generator point G.

Q3. Which elliptic curve does Bitcoin use?
A) secp192k1 B) secp256k1 C) NIST P-256 D) Ed25519
Answer: B – Bitcoin uses secp256k1 with equation $y^2 = x^3 + 7$.

Q4. What security level does a 256-bit ECC key provide?
A) 64-bit B) 128-bit C) 256-bit D) 512-bit

Quiz (1–5)

Q1. What is the primary advantage of asymmetric over symmetric cryptography for blockchains?
A) Faster encryption B) Smaller keys C) No key distribution problem D) Lower cost
Answer: C – No need to securely share keys between parties.

Q2. In ECC, how is the public key derived from the private key?
A) Hash function B) $Q = k \cdot G$ C) Random generation D) Encryption
Answer: B – Public key Q = private key k multiplied by generator point G.

Q3. Which elliptic curve does Bitcoin use?
A) secp192k1 B) secp256k1 C) NIST P-256 D) Ed25519
Answer: B – Bitcoin uses secp256k1 with equation $y^2 = x^3 + 7$.

Q4. What security level does a 256-bit ECC key provide?
A) 64-bit B) 128-bit C) 256-bit D) 512-bit
Answer: B – 256-bit ECC provides 128-bit security, equivalent to 3072-bit RSA.

Q5. What must be unique for every ECDSA signature to prevent key leakage?
A) Message hash B) Private key C) Nonce D) Public key

Quiz (1–5)

Q1. What is the primary advantage of asymmetric over symmetric cryptography for blockchains?
A) Faster encryption B) Smaller keys C) No key distribution problem D) Lower cost
Answer: C – No need to securely share keys between parties.

Q2. In ECC, how is the public key derived from the private key?
A) Hash function B) $Q = k \cdot G$ C) Random generation D) Encryption
Answer: B – Public key Q = private key k multiplied by generator point G.

Q3. Which elliptic curve does Bitcoin use?
A) secp192k1 B) secp256k1 C) NIST P-256 D) Ed25519
Answer: B – Bitcoin uses secp256k1 with equation $y^2 = x^3 + 7$.

Q4. What security level does a 256-bit ECC key provide?
A) 64-bit B) 128-bit C) 256-bit D) 512-bit
Answer: B – 256-bit ECC provides 128-bit security, equivalent to 3072-bit RSA.

Q5. What must be unique for every ECDSA signature to prevent key leakage?
A) Message hash B) Private key C) Nonce D) Public key
Answer: C – Reusing a nonce allows recovery of the private key.

Quiz (6–10)

Q6. Which hash functions does Bitcoin address derivation use?
A) MD5 + SHA1 B) SHA-256 + RIPEMD-160 C) Keccak-256 D) Blake2b

Quiz (6–10)

Q6. Which hash functions does Bitcoin address derivation use?
A) MD5 + SHA1 B) SHA-256 + RIPEMD-160 C) Keccak-256 D) Blake2b
Answer: B – SHA-256 for security, RIPEMD-160 to reduce address size.

Q7. How long is an Ethereum address (excluding 0x prefix)?
A) 20 chars B) 32 chars C) 40 chars D) 64 chars

Quiz (6–10)

Q6. Which hash functions does Bitcoin address derivation use?
A) MD5 + SHA1 B) SHA-256 + RIPEMD-160 C) Keccak-256 D) Blake2b
Answer: B – SHA-256 for security, RIPEMD-160 to reduce address size.

Q7. How long is an Ethereum address (excluding 0x prefix)?
A) 20 chars B) 32 chars C) 40 chars D) 64 chars
Answer: C – 20 bytes = 40 hexadecimal characters.

Q8. What is the main benefit of HD wallets?
A) Faster transactions B) Lower fees C) Single backup for all keys D) Stronger encryption

Quiz (6–10)

Q6. Which hash functions does Bitcoin address derivation use?
A) MD5 + SHA1 B) SHA-256 + RIPEMD-160 C) Keccak-256 D) Blake2b
Answer: B – SHA-256 for security, RIPEMD-160 to reduce address size.

Q7. How long is an Ethereum address (excluding 0x prefix)?
A) 20 chars B) 32 chars C) 40 chars D) 64 chars
Answer: C – 20 bytes = 40 hexadecimal characters.

Q8. What is the main benefit of HD wallets?
A) Faster transactions B) Lower fees C) Single backup for all keys D) Stronger encryption
Answer: C – Backing up seed phrase once recovers all derived addresses.

Q9. In a 2-of-3 multisig, how many signatures authorize a transaction?
A) 1 B) 2 C) 3 D) All

Quiz (6–10)

Q6. Which hash functions does Bitcoin address derivation use?
A) MD5 + SHA1 B) SHA-256 + RIPEMD-160 C) Keccak-256 D) Blake2b
Answer: B – SHA-256 for security, RIPEMD-160 to reduce address size.

Q7. How long is an Ethereum address (excluding 0x prefix)?
A) 20 chars B) 32 chars C) 40 chars D) 64 chars
Answer: C – 20 bytes = 40 hexadecimal characters.

Q8. What is the main benefit of HD wallets?
A) Faster transactions B) Lower fees C) Single backup for all keys D) Stronger encryption
Answer: C – Backing up seed phrase once recovers all derived addresses.

Q9. In a 2-of-3 multisig, how many signatures authorize a transaction?
A) 1 B) 2 C) 3 D) All
Answer: B – Any 2 of 3 possible signatures required.

Q10. What does "Not your keys, not your coins" mean?
A) Print keys physically B) Control private keys to own crypto C) Share keys D) Public keys = ownership

Quiz (6–10)

Q6. Which hash functions does Bitcoin address derivation use?
A) MD5 + SHA1 B) SHA-256 + RIPEMD-160 C) Keccak-256 D) Blake2b
Answer: B – SHA-256 for security, RIPEMD-160 to reduce address size.

Q7. How long is an Ethereum address (excluding 0x prefix)?
A) 20 chars B) 32 chars C) 40 chars D) 64 chars
Answer: C – 20 bytes = 40 hexadecimal characters.

Q8. What is the main benefit of HD wallets?
A) Faster transactions B) Lower fees C) Single backup for all keys D) Stronger encryption
Answer: C – Backing up seed phrase once recovers all derived addresses.

Q9. In a 2-of-3 multisig, how many signatures authorize a transaction?
A) 1 B) 2 C) 3 D) All
Answer: B – Any 2 of 3 possible signatures required.

Q10. What does "Not your keys, not your coins" mean?
A) Print keys physically B) Control private keys to own crypto C) Share keys D) Public keys = ownership
Answer: B – Without private key control, you depend on third-party custody.