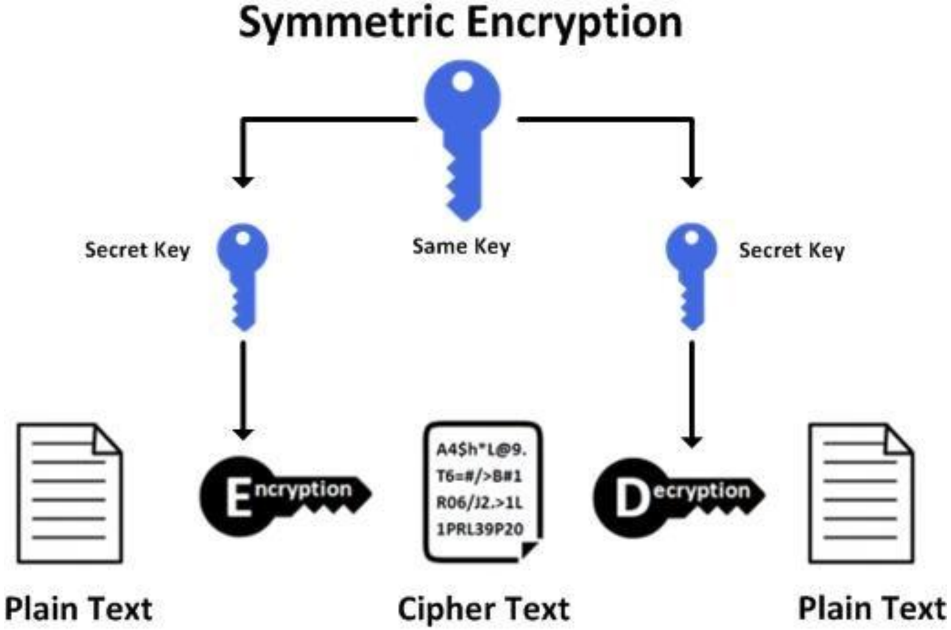
Cryptography in Blockchain

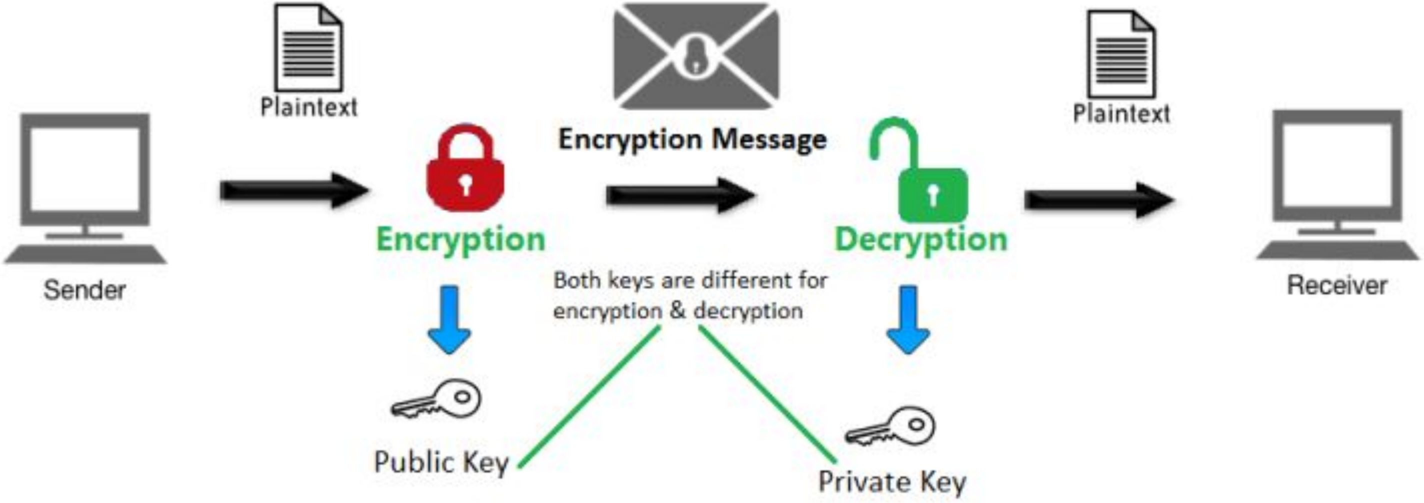
Agenda

1. Private-key cryptography
2. Public-key cryptography
3. Hashing
4. Digital Signature
5. Blockchain security
6. Q&A

1. Private-key cryptography



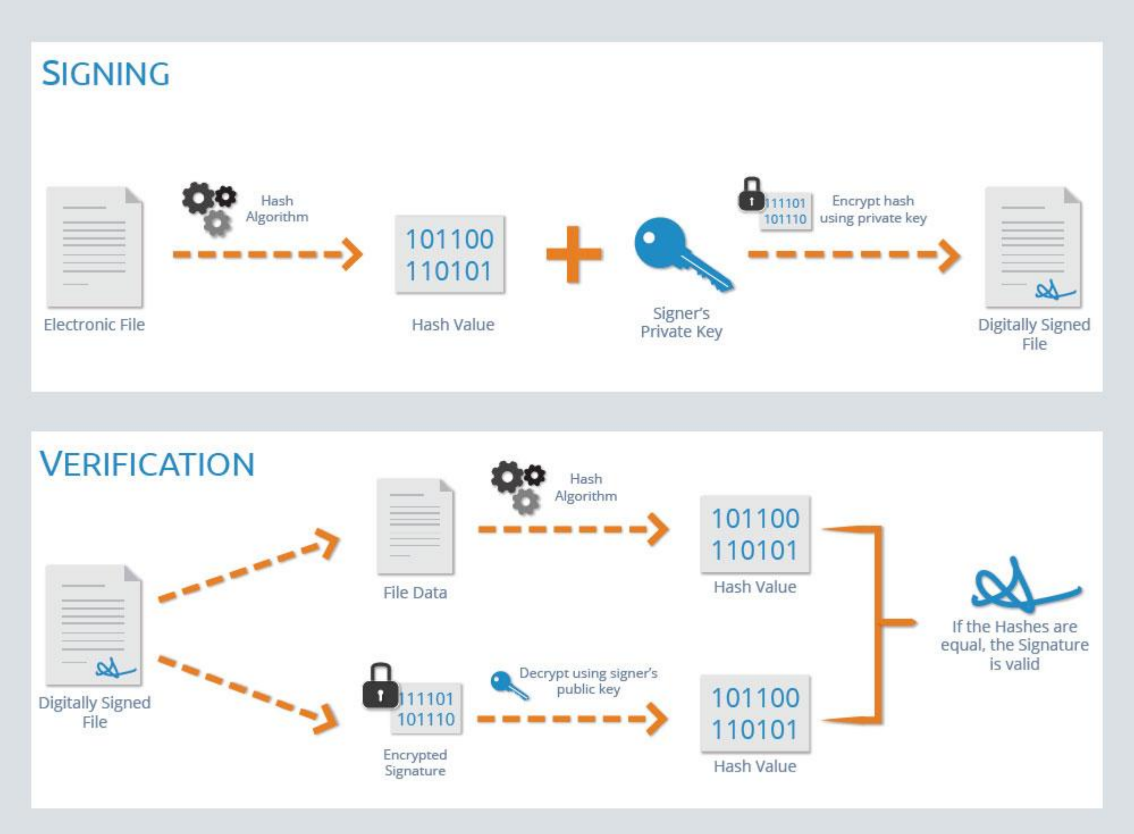
2. Public-key cryptography



3. Hashing

- Hash function
  - Input: An object
  - Output: A fixed-size number
- One way encryption: easily for encrypt and verify and very difficult for decrypt
- Hash collision
- Universal hashing
- Algorithms: MD5, SHA-256, SHA-512

4. Digital signature



Signing

- Signing
  - Input: Message, Signer ‘s private key
  - Output: Signature + Message
- Step
  - Hash Message => A number
  - Encrypt the number with private key => signature

Verifying

- Verifying
  - Input: Message, Signature, Public Key
  - Output: is valid signature
- Step
  - Hash the message => A number (1)
  - Decrypt the signature with the public key (2)
  - Compare (1) and (2)

5. Blockchain security

- An account
  - Private key
  - Public key
  - Address
  - Nonce
- Sign transaction with private key
- Blockchain verify transaction’s signature by using public key
- Avoid double spending
- Verify blockchain data

6. Q&A