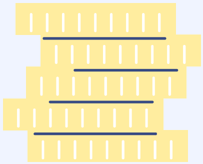
Encryption and BitCoin

“Unlocking the future: Exploring the world of bitcoin & cryptocurrency

Key Takeaways:

- Public-key cryptography VS traditional symmetric-key cryptography.
- Generation of public and private keys. Encryption and decryption of data.
- Digital signatures and authenticity of data.
- Public-private key encryption and Bitcoin wallets for Bitcoin transactions.
- Types of BitCoin Wallets: Hot & Cold Wallets, their advantages and disadvantages
- Securing BitCoin Wallets. Backing up private keys using multi-factor authentication.



01

Asymmetric Cryptography

Alice(sender) and
bob(recipient) possess
two keys: public and
private each

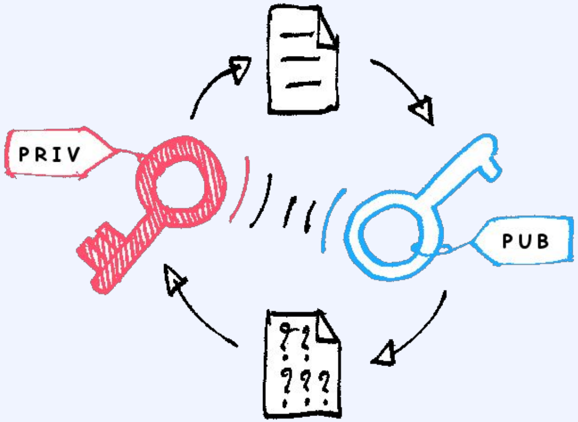
The Key-Pairs

Public Key:

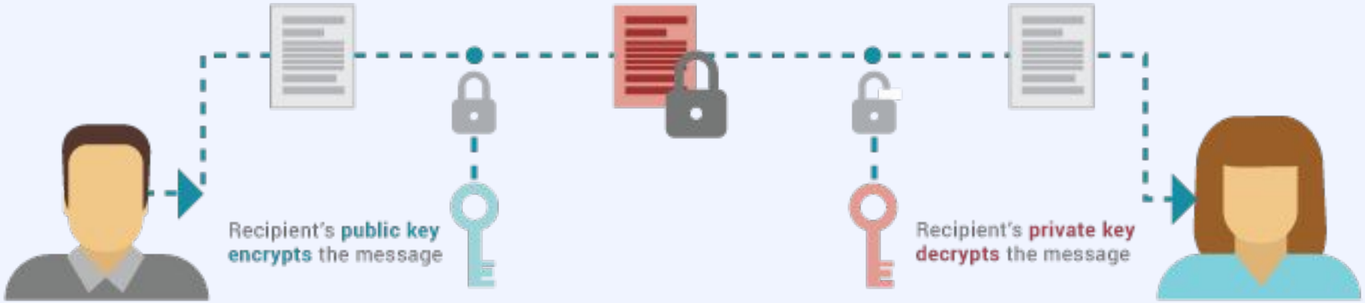
- Unique, openly shared cryptographic key
- Used for encrypting data/messages
- Validates digital signatures
- Generates public addresses in cryptocurrencies

Private Key:

- Secret, known only to owner
- Paired with a public key
- Decrypts data/messages
- Authorizes transactions in cryptocurrencies
- Must be securely stored for asset control

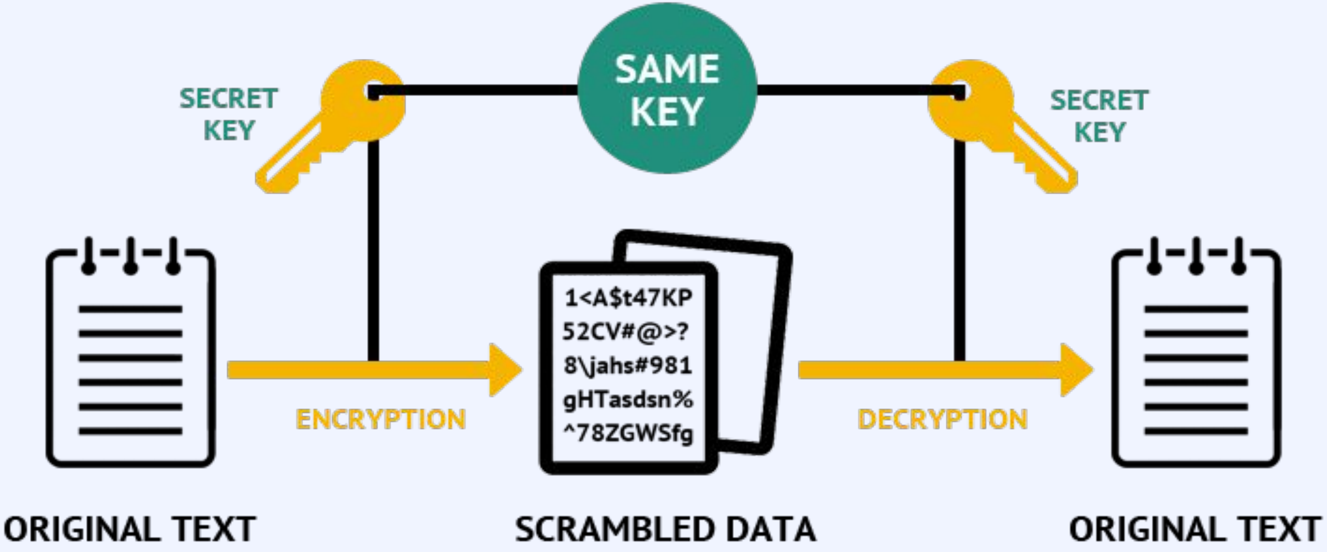


PUBLIC KEY CRYPTOGRAPHY


Recipient's public key encrypts the message
Recipient's private key decrypts the message

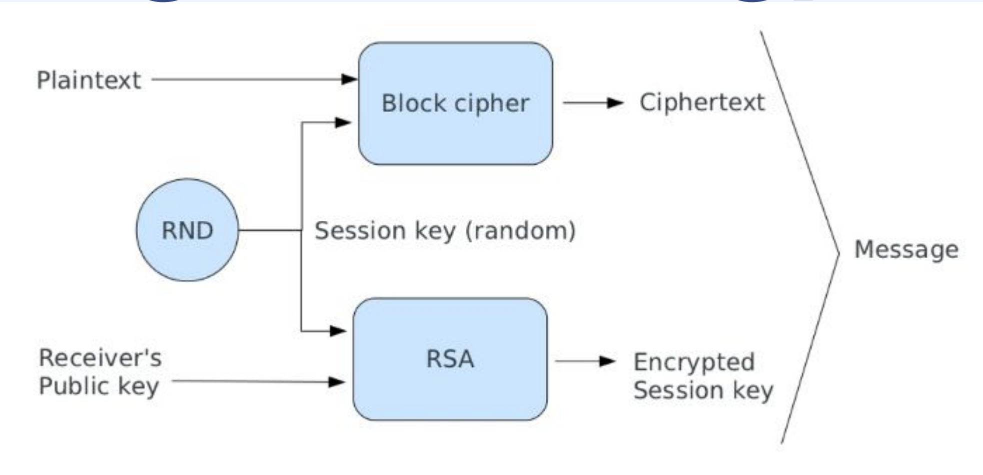
- Uses pairs of keys: public and private keys
- Public key is freely shared, private key is kept secret
- Public key encrypts data, private key decrypts data
- Provides secure communication without needing to share secret keys
- Used for digital signatures, authentication, and encryption in secure communication protocols

Symmetric Encryption



- Utilizes a single shared key for both encryption and decryption
- Key must remain confidential between communicating parties
- Fast and efficient encryption process
- Ideal for encrypting large volumes of data
- Vulnerable to key distribution and management challenges

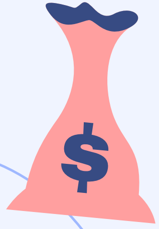
Hybrid Encryption



- Sender creates a random symmetric key to encrypt the message.
- Message is encrypted with the symmetric key.
- Symmetric key is encrypted with receiver's public key.
- Encrypted message and symmetric key are sent to receiver.
- Receiver decrypts symmetric key with private key.
- Message is decrypted with symmetric key, revealing the original content.

The Math: RSA Algorithm

- **RSA Keys:**
  - Public Key: (e, N) - Made public, used for encryption.
  - Private Key: (d, N) - Kept secret, used for decryption.
- **Key Generation:**
  - Choose 2 large, distinct prime numbers (p & q).
  - $N = p \times q$ (modulus for both keys).
  - $\varphi(N) = (p - 1) \times (q - 1)$ (Euler's Totient).
  - Choose public exponent (e): $1 < e < \varphi(N)$, relatively prime to $\varphi(N)$.
  - Find private exponent (d): $e * d \equiv 1 \pmod{\varphi(N)}$ (often using Extended Euclidean Algorithm).
- **Encryption:**
  - $C = m^e \bmod N$ (message raised to public exponent modulo N).
- **Decryption:**
  - $m = C^d \bmod N$ (encrypted message raised to private exponent modulo N).



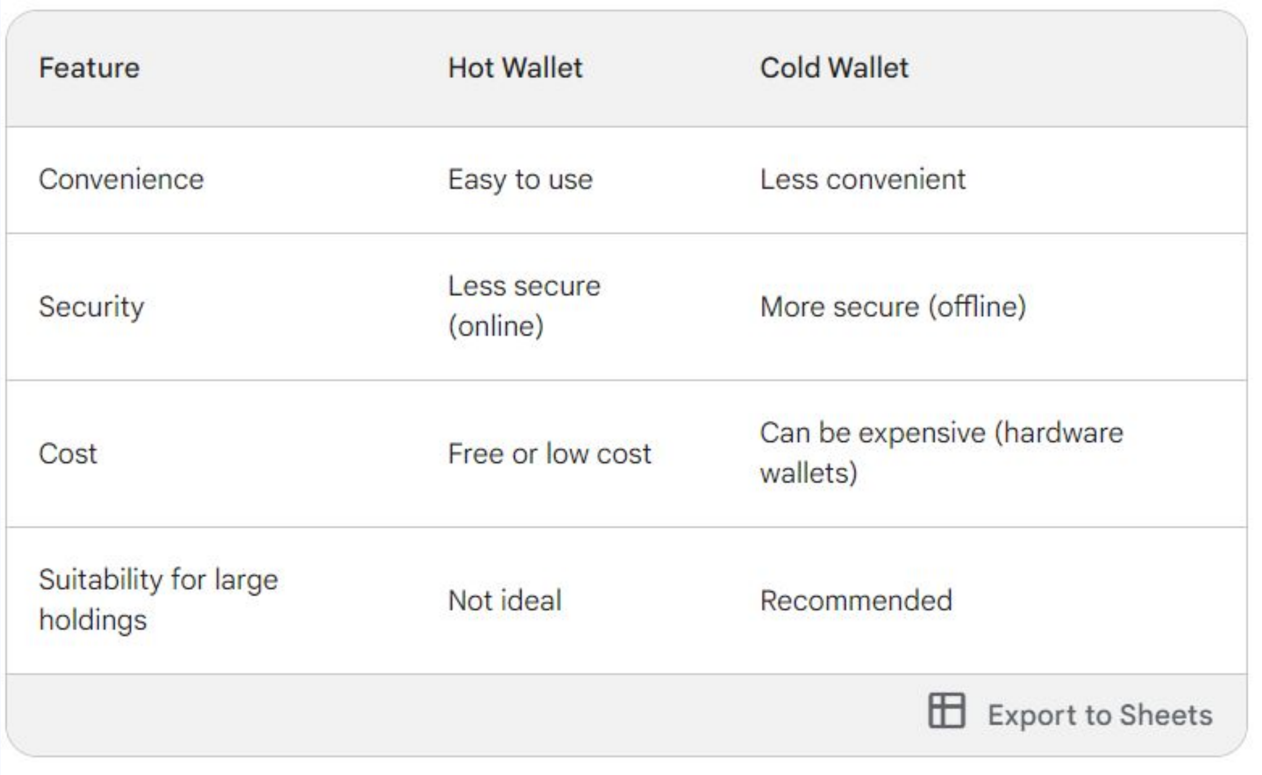
BitCoin & Wallets

THE UNITED STATES OF AMERICA
IN GOD WE TRUST
ONE HUNDRED DOLLARS
100
KB27320920R
INDEPENDENCE HALL

BitCoin

- Each Bitcoin wallet has a unique key pair:
  - Private Key: Secret code for accessing and spending bitcoin.
  - Public Key: Shareable address for receiving bitcoin.
- When sending bitcoin:
  - Specify recipient's public key (Bitcoin address).
  - Sign transaction with your private key.
  - Broadcast transaction to Bitcoin network.
- Miners verify transaction:
  - Use recipient's public key to validate signature.
  - Only owner of private key could authorize transaction.
- Public key encryption:
  - Transaction details visible to all but encrypted.
  - Recipient's private key required to access funds.

- **Bitcoin:**
  - Digital currency, not controlled by any bank or government.
  - Relies on a decentralized network of computers to verify transactions.
  - Units are called bitcoins (BTC) and can be divided into smaller units (mBTC, μBTC).
- **Bitcoin Wallets:**
  - Don't actually store bitcoins, they store cryptographic keys.
  - These keys allow you to:
    - Send and receive bitcoins.
    - Keep track of your bitcoin balance.
  - Different types of wallets offer varying levels of security and functionality:
    - Software(Hot) wallets: Convenient, can be on your phone or computer, but can be vulnerable to hacks.
    - Hardware(Cold) wallets: More secure, store keys offline on a physical device, but less convenient.



Feature	Hot Wallet	Cold Wallet
Convenience	Easy to use	Less convenient
Security	Less secure (online)	More secure (offline)
Cost	Free or low cost	Can be expensive (hardware wallets)
Suitability for large holdings	Not ideal	Recommended

Export to Sheets

- **Backup Private Keys:** This is crucial! Treat them like your bank password and store backups securely offline (consider paper or hardware wallets).
- **Use Multi-Factor Auth (MFA):** Adds an extra verification step for logins and transactions (like a code from your phone).
- **Choose Reputable Wallets:** Research security practices before picking a wallet provider.
- **Update Software:** Keep your wallet app and device firmware up-to-date.
- Beware Phishing: Don't click suspicious links or enter private keys on untrusted websites.
- **Strong Passwords:** Use unique, complex passwords everywhere you access your Bitcoin.
- **Secure Devices:** Keep your devices with antivirus protection and avoid public Wi-Fi for wallet access.

THANK YOU

Do you have any questions?

ALTERNATIVE RESOURCES

Symmetric-Key Cryptography
Basics of Public-Private Key Encryption
RSA (advanced)
Bitcoin Wallet
More on Wallets
Bitcoin Core Github