Tejal Saurabhi

KOSS Selection Task

EXPLORING PUBLIC-PRIVATE KEY ENCRYPTION AND BITCOIN WALLETS

CRYPTOGRAPHY IS THE SCIENCE OF ENCRYPTING AND DECRYPTING DATA TO PREVENT UNAUTHORIZED ACCESS.

Encryption is the process of making the message unreadable to any third party.
Decryption is the process of reversing the encrypted text to its original readable format.

The original data is known as the **plaintext.**
The data after encryption is known as the **ciphertext**.

PLAINTEXT + KEY = CIPHERTEXT

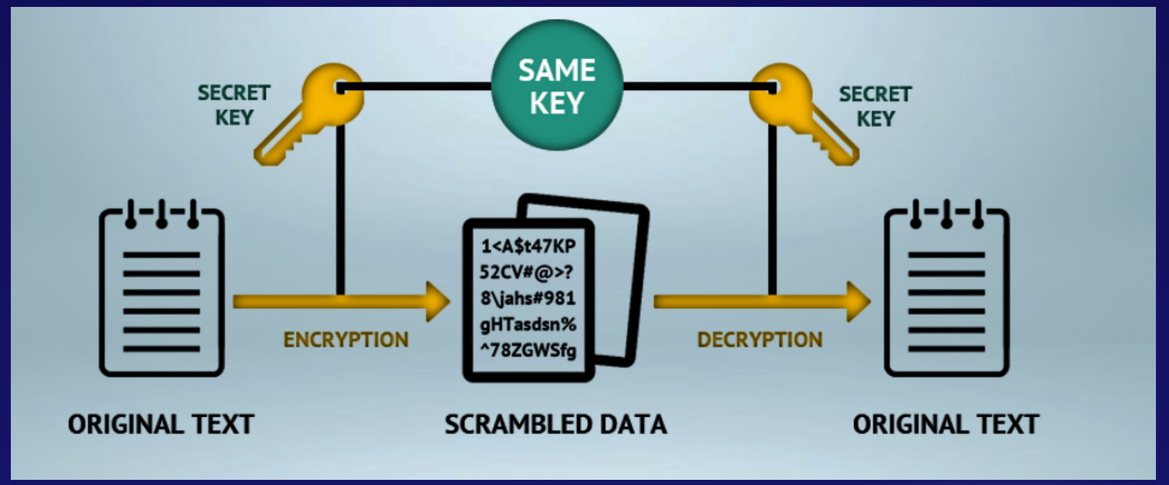
SYMMETRIC KEY ENCRYPTION

Same key used for both encryption and decryption.

1)**Secret key generation:** Generated randomly or through key derivation functions.

2)**Encryption:** To encrypt a message, you take your secret key and combine it with the message using a specific algorithm.

3)**Decryption:** When the encrypted message reaches the intended recipient, they apply the decryption algorithm with the same secret key to reverse the encryption process and reveal the original message.



OPERATION MODE

Stream ciphers: encrypt the digits or letters one at a time.
Block ciphers: encrypt a number of bits as a single unit. Blocks of 64 bits were commonly used. E.g. AES, DES

PROBLEMS

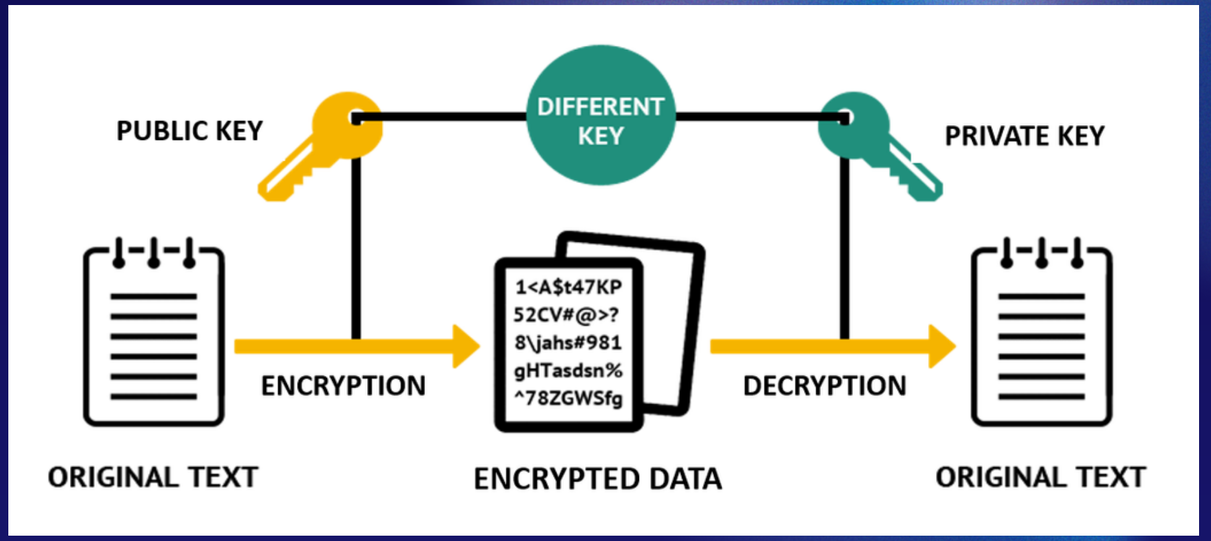
- The key challenge with private key encryption is **securely sharing the secret key** with the intended recipient.
- Not suitable to communicate securely with **multiple parties**, as each pair of communicators needs a unique secret key.

ASYMMETRIC ENCRYPTION

Uses a pair of keys to encrypt and decrypt data

- **Key Generation:** The user generates a **public key** and a corresponding **private key.**
  The public key can be distributed to anyone.
  The private key is kept secret by the owner.
- **Encryption:**
  To encrypt a message or data, the sender uses the recipient's public key.
- **Decryption:**
  The recipient uses their private key to decrypt the ciphertext received from the sender.

EXAMPLE: RSA and ECC



USE

Symmetric-key algorithms are generally fast and **efficient** for encrypting large amounts of data. **Asymmetric cryptography is not efficient** and therefore used only for exchanging a shared key, after which the symmetric key is used to encrypt/decrypt data.

RSA ENCRYPTION

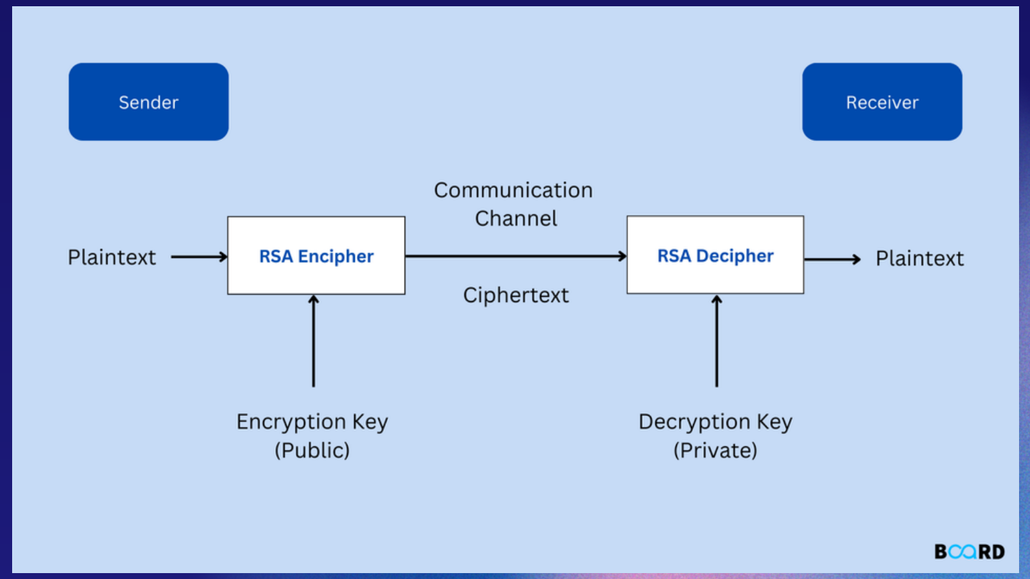
Under RSA encryption, messages are encrypted with a code called public key.

RSA encryption is often used in combination with other encryption schemes, because it is less efficient and more resource-heavy than symmetric-key encryption.

To make things more efficient, a file will generally be encrypted with a symmetric-key algorithm, and then the symmetric key will be encrypted with RSA encryption.

TRAPDOOR FUNCTION

RSA algorithm is based on trapdoor function
It is **easy to compute in one direction** but **computationally difficult to invert** without special knowledge (the trapdoor)



PADDING

The structure of a message can give attackers clues about its content.
Thus randomized data is added to hide the original formatting clues. RSA uses padding schemes like OAEP

WORKING

ALGORITHM TO GENERATE THE KEYS

PUBLIC KEY (n, e):

1) We need two prime numbers (p and q), which are selected with a primality test (E.g.: Rabin Miller Primality test). The prime numbers need to be very large, and also relatively far apart.
2) Find modulus(n) and Carmichael's totient function.
3) Choose a value for e, between 1 and lambda(n)
4) cypher text(c) = message(m)^(e) mod n

PRIVATE KEY (n, d):

1) Calculate d by: d = 1/e mod λ(n) where (1/e mod) symbolizes that we need to calculate the modular inverse of e and λ(n)(by Extended Euclidean Algorithm).
2) Find the original text by: m = c^(d) mod n

RSA is still seen in a range of web browsers, email, VPNs, chat and other communication channels.

EXAMPLE

n = p x q

Where p = 907 and q = 773

=> n = 907 x 773 = 701,111

λ(n) = lcm (p − 1, q − 1)

λ(701,111) = lcm (907 − 1, 773 − 1)

=> λ(701,111) = 349,716

Say we take e = 11 and **m = 4**

c = m^(e) mod n

=> cypher text = 688,749

d =1/e mod λ(n)

d =1/11 mod 349,716 = 254, 339

m = cd mod n

m = 688,749254,339 mod 701,111.

=> m = 4

DIGITAL SIGNATURE

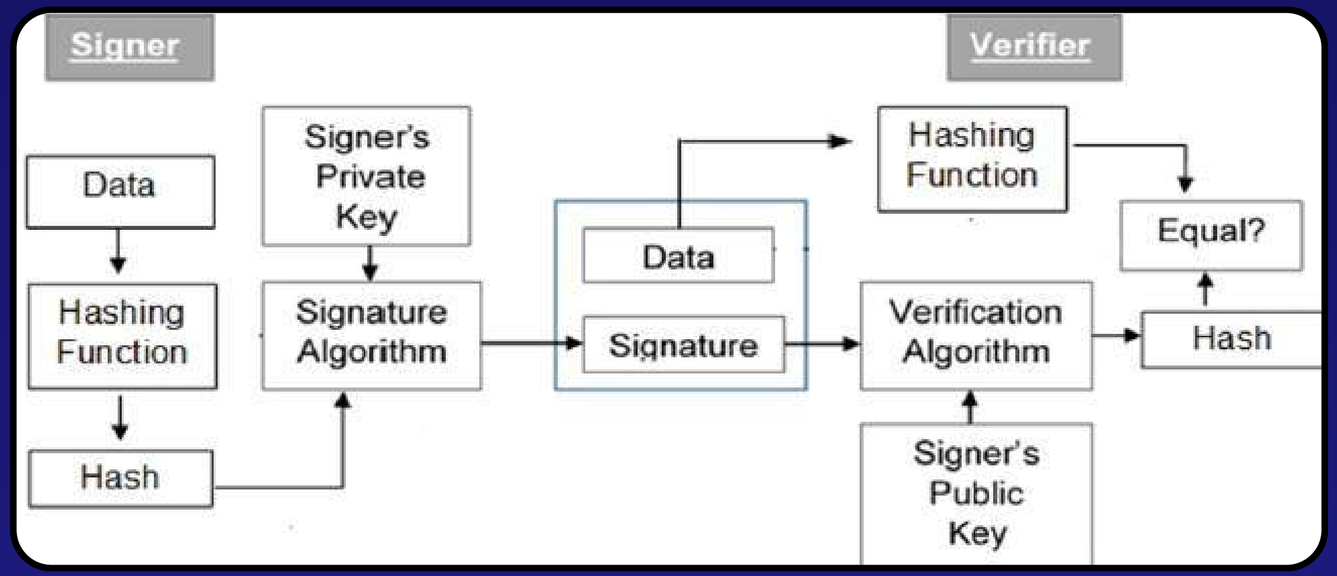
USE

- Verify the **authenticity** and integrity of digital messages or documents.
- Verify the sender (**non-repudiation**)
- Make sure the message has not been **altered** in transit.

THE PRIVATE KEY IS USED TO GENERATE SIGNATURE
THE PUBLIC KEY CAN BE USED TO VERIFY THE SIGNATURE

APPLICATION

Secure email communication, online transactions, software distribution, and legal documents to ensure the authenticity,



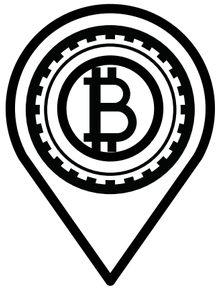
WHAT IS A BITCOIN WALLET?

- It’s most crucial function is to securely **store the private keys** associated with the user's Bitcoin addresses.
- It’s is a software program or a physical device that allows users to store, send, and receive Bitcoin and other cryptocurrency.
- It maintains a records of all incoming and outgoing transactions.
- It implements various security features to protect users' funds and private keys from unauthorized access and theft.

HOW PUBLIC-PRIVATE KEY ENCRYPTION IS USED IN BITCOIN WALLETS

BITCOIN ADDRESSES

- Bitcoin wallets typically generate unique Bitcoin addresses, which are cryptographic identifiers **derived from public keys.**
- Each Bitcoin address corresponds to a unique public key and serves as a **destination for receiving Bitcoin transactions.**



TRANSACTION SIGNING

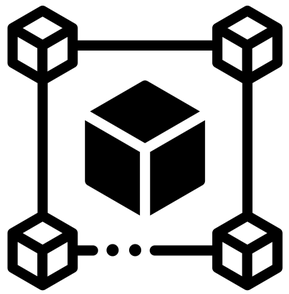
- Users sign their transactions with their private key. This involves **digitally signing** a message that includes transaction details, such as the sender, recipient, and amount.
- The signature provides **proof that the transaction has been authorized by the owner of the private key associated with the sending address.**

OWNERSHIP CONTROL

- Users who possess the private keys associated with specific Bitcoin addresses have control over the funds stored at those addresses.
- By **securely managing their private keys**, users maintain control over their Bitcoin holdings and can authorize transactions as needed

BITCOIN AUTHENTICATION

- Bitcoin transactions are recorded on a public ledger called the blockchain. Each transaction is cryptographically linked to the previous transaction, forming a chain of blocks.
- The **integrity and immutability of the blockchain are maintained through cryptographic hashing and digital signatures.**



TYPES OF BITCOIN WALLETS

Bitcoin wallets come in a range of styles, each offering a tradeoff between convenient access and security against theft.

SOFTWARE WALLETS

1. **Desktop Wallets:**
   - Programs installed on computers to **store coins locally.**
   - Provide full control over the Bitcoin wallet and are typically more secure than other software wallets.
   - Examples: Electrum, Bitcoin Core, Exodus.
2. **Mobile Wallets:**
   - Apps for smartphones and tablets, offering on-the-go access to Bitcoin.
   - Suitable for small transactions and daily use.
   - Examples: Mycelium, Trust Wallet.
3. **Web Wallets:**
   - Accessed via web browsers, storing coins through online third parties.
   - Convenient for multi-device access but may be less secure.
   - Examples: Coinbase, Blockchain.com, BitGo.

HARDWARE WALLETS

- Hardware wallets are **physical devices**, like a **USB drive**, that are **not connected to the web.**
- They offer the **highest level of security for storing large amounts** of Bitcoin.
- There is typically **another password involved** in making the internet connection.
- Examples: Ledger Nano S, Trezor, and KeepKey.

PAPER WALLETS

In a paper wallet, you print off your key, typically a QR code, on a paper document. This makes it impossible for a hacker to access and steal the password online, but then you need to protect the physical document.

COMPARISON

ASPECT	SOFTWARE/HOT WALLETS	HARDWARE & PAPER WALLETS/COLD WALLETS
Security	Lower security due to being connected to the internet and vulnerable to hacking or malware attacks.	Higher security as they are typically offline and not susceptible to online threats.
Convenience	Convenient for quick access and easy management of funds.	Less convenient for immediate access but suitable for long-term storage.
Risk of Loss	Higher risk of loss in case of hacking or other security breaches.	Lower risk of loss as they are offline and not exposed to online threats.
Suitable For	Suitable for frequent trading, spending, or accessing funds on the go.	Suitable for long-term storage or holding large amounts of cryptocurrency.

BEST SECURITY PRACTICES

1. Select a reputable and **secure Bitcoin wallet**

2. **Set a strong and unique password** for your Bitcoin wallet. Consider using a **passphrase** for added security. Use a **password manager** to generate and store strong passwords securely. **Regularly backup your private keys.**

3. Keep your Bitcoin wallet software, operating system, and security software updated with the latest patches and **security updates.**

4. Avoid accessing your Bitcoin wallet from unsecured or **public Wi-Fi networks**

5. **Diversify** your Bitcoin holdings across multiple wallets to minimize risk

6. Consider **using cold storage solutions**, such as hardware wallets or paper wallets, for storing **large amounts** of Bitcoin

Two-factor authentication is the most common form of MFA used in Bitcoin wallets.
It typically involves the combination of two different authentication factors:

- Something you know: A password, PIN, or passphrase.
- Something you have: A second factor, such as a mobile device or hardware token.

When enabled, users are required to provide both factors to access their Bitcoin wallet, adding an extra layer of security beyond just a password.

THANK YOU!