# PUBLIC-PRIVATE KEY ENCRYPTION AND BITCOIN WALLETS

BY : TARANISEN NAIK

# SYMMETRIC VS. PUBLIC-KEY CRYPTOGRAPHY

## Symmetric Key Cryptograpy

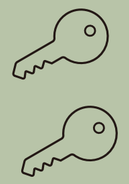
With symmetric cryptography, we use one key to unlock and lock.

Only people with the key or a copy of the key can unlock the lock.

Key distribution is problematic—if intercepted, security is breached.

Quicker because of easy arithmetic operations.

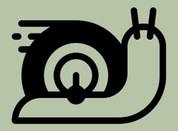
## Public Key Cryptography



With public-key cryptography, a public key is used for encryption, and a private key is used for decryption.

The sender encrypts the message with the recipient's public key, and only the recipient can decrypt it using their private key.

Safer, since the private key is never transmitted.

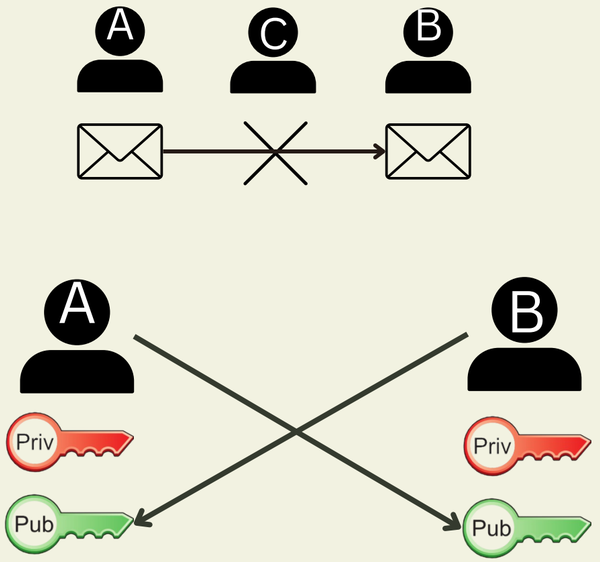


Slower because of complicated mathematical calculations.

# ENCRYPTION & DECRYPTION IN ACTION

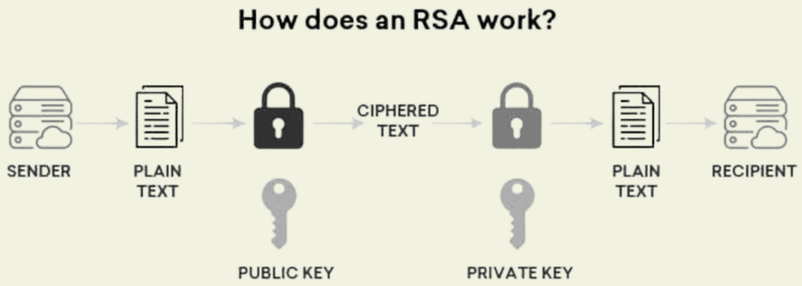
## Situation

Person A wants to transfer a message to person B such that no other person can read it. A has B's public key and his own private key, while B has A's public key and his own private key.



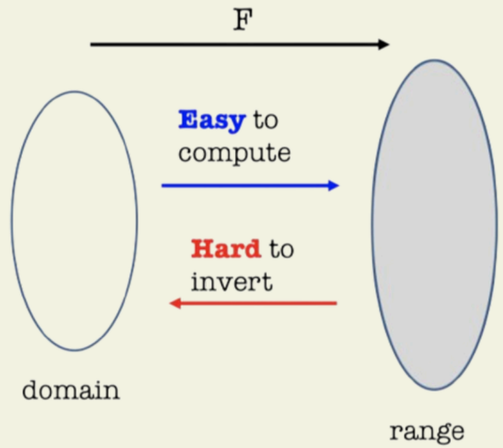

## Process

A will encrypt the message using B's public key and share it publicly. B will retrieve the encrypted message and decrypt it using their private key.




## Mechanism

It uses a one-way function, which is easy to compute but hard to reverse. First, two keys are generated. The message is then encrypted using one key and can only be decrypted using the other.



# HOW KEYS ARE GENERATED

## Characteristics of Function

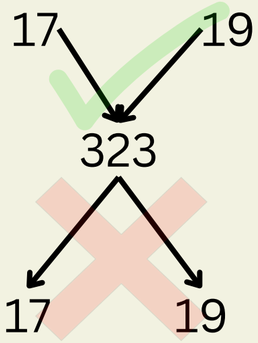
It is computationally easy to:

- Generate a set of keys
- Encrypt / Decrypt using these keys

computationally infeasible to:

- Determine the private key from the public key
- Bruteforce the private key from the public key and bruteforce the ciphertext

## Mathemathical concept




It is based on the fact that multiplying two prime numbers is easy, but factoring the product back into those primes is extremely difficult. This one-way function is the foundation of RSA encryption, which ensures secure communication by leveraging this mathematical complexity.

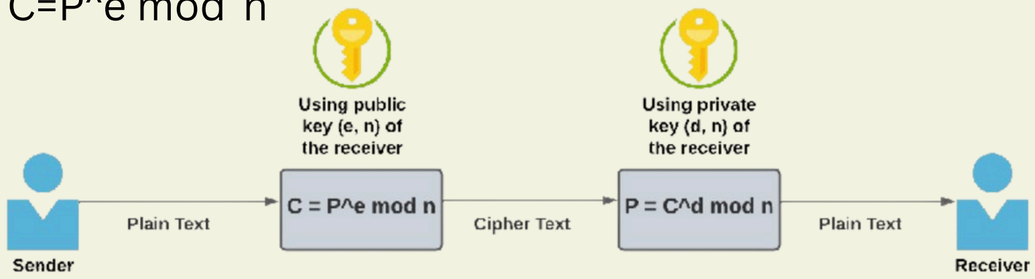
## RSA Algorithm

**A→65**


- Each character is converted to its ASCII or Unicode value.
- Select two large prime numbers, p and q.
- Compute n=p×q , Calculate ϕ(n)=(p−1)×(q−1)
- Choose an encryption exponent e (public key) such that 1<e<ϕ(n) and gcd(e, ϕ(n)) = 1.
- Compute the decryption exponent d (private key) as d=e^−1(mod) ϕ(n)

## Encryption & Decryption

- Convert the message into a number P.
- Compute the ciphertext: C=P^e mod n
- Compute the original message: P=C^d mod n

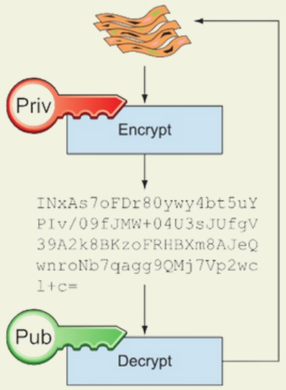


# DIGITAL SIGNATURE

## Defination


A Digital signature is a cryptographic method that verifies the authenticity and integrity of digital documents or messages. It uses complex mathematical algorithms and encryption techniques to create a virtual “fingerprint” that uniquely identifies the signer and the document’s contents.

## Mechanism




The signer uses their private key to electronically sign documents, while the public key is available for anyone who needs to verify the signature's authenticity.

## Technology Framework

- Creating Keys: A unique pair of keys is generated:
  Private key (used for signing).
  Public key (used for verification).
- Signing a Document – The document is converted into a hash (a unique digital fingerprint), which is then encrypted using the private key to create the signature.
- Verifying the Signature – The recipient generates a hash from the document and decrypts the signature using the public key. If both hashes match, the document is authentic.
- Trust & Security – Certificate Authorities (CAs) issue digital certificates to confirm the signer’s identity, making signatures legally valid.

```
if public==private:
    print("Approved")
else:
    print("Rejected")
```

# BITCOIN WALLET

## Bitcoin Wallet vs. Traditional Wallet

A Bitcoin wallet stores the private key, not actual Bitcoin, whereas a traditional wallet holds physical currency. This key allows users to access and manage their Bitcoin securely, unlike cash, which is directly stored in a physical wallet.

## Mechanism

- Creating Keys: A Bitcoin wallet generates a public key and a private key.
- Receiving Bitcoin: our public address, created from our public key, acts as our user ID, allowing anyone to send Bitcoin to us.
- Sending Bitcoin: We sign the transaction with our private key when we send Bitcoin. Others can verify the signature using our public key to ensure authenticity.

## Different Types Of Bitcoin Wallets

### Hot wallet

**Definition**:
A hot wallet is connected to the internet and stores the private key on a server.

**Pros**:
- Easy to use
- Accessible from multiple devices.
- Ideal for traders.

**Cons**:
- It is prone to hackers as it is exposed to the internet.
- So, storing a large amount of assets in it is not advisable.

### Cold wallet

**Definition**:
A cold wallet is a physical device or paper that stores the private key and kept disconnected from the internet.

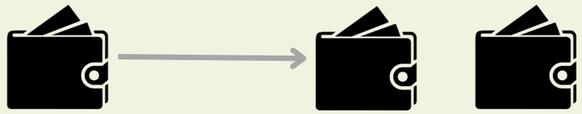
**Pros**:
- Stealing from it is difficult as it requires physical possession.
- It is more secure since it is encrypted with an additional PIN.

**Cons**:
- It is less convenient
- Not ideal for regular trading.
- Over time, you may even forget where you stored your wallet.

# ENCRYPTION & DECRYPTION IN ACTION

## Backup your wallet

We should make a copy of our wallet so that if we lose our original wallet or if our laptop or mobile is stolen, we can still recover our Bitcoin.



## Encrypt your wallet

Setting a password for our devices as well as our wallet can reduce the risk of Bitcoin being stolen. We should use a strong password and ensure that we do not forget it.

## Multi-signature to protect

It is a method in which multiple signatures or private keys are required for a transaction. We can also create a system where 3 out of 5 keys are required at a time to open the wallet or make a transaction.

## Offline wallet for savings


Since offline wallets are more secure, we should use them for saving, while online wallets should be used for day-to-day transactions.

## software up to date


We should update our wallet software regularly, as it includes new security features and improved versions that fix past loopholes.

## Be careful with online services

Many exchanges and online wallets have suffered from security breaches in the past, so we should be careful when choosing a wallet platform.

# USING BITCOIN-CLI FOR REGTEST WALLET

## start the regset

```
PS C:\Program Files\Bitcoin\daemon> .\bitcoind -regtest
2025-03-26T16:55:41Z Bitcoin Core version v27.0.0 (release build)
2025-03-26T16:55:41Z Script verification uses 15 additional threads
2025-03-26T16:55:41Z Using the 'x86_shani(1way,2way)' SHA256 impleme
```

## Veryfing if local regtest is active

```
PS C:\Program Files\Bitcoin\daemon> .\bitcoin-cli -regtest getblockcount
0
```

## Creat the wallet

```
PS C:\Program Files\Bitcoin\daemon>
                                > .\bitcoin-cli -regtest createwallet
"testwallet"
{
  "name": "testwallet"
}
```

## Mine 101 blocks to get spendable BTC:

```
PS C:\Program Files\Bitcoin\daemon> .\bitcoin-cli -regtest generatetoadd
ress 101 $(.\bitcoin-cli -regtest getnewaddress)
[
  "639fd25f77cd7604b531bec2aac934577ec6e2d0991212a5363e99b6e7e90e17",
  "5bbdb9219381885d19e7cdb3804f949fe84cbf00d35c865ab91802f94b059e15",
```

## Checking balange

```
PS C:\Program Files\Bitcoin\daemon> .\bitcoin-cli -regtest getbalance
50.00000000
```

## Generating new address

```
PS C:\Program Files\Bitcoin\daemon> .\bitcoin-cli -regtest getnewaddress

bcrt1qkh0puuhnuducqwl6hqq939anmjekwygfra4wsz
```

## Transiction

```
PS C:\Program Files\Bitcoin\daemon> .\bitcoin-cli -regtest sendtoaddress
 "bcrt1qxe3qdzmc5hl9mfwqc9z2hlxwsxm4s4km8ghzpt" 5 "" "" false
b8927ed4e445f936eeaa2de712b36df532446e217756185b93bbf1251148593f
```

## Balance after transiction

```
PS C:\Program Files\Bitcoin\daemon> .\bitcoin-cli -regtest getbalance
44.99998590
```

Thank you!