UNLOCKING SECURITY

The Fundamentals of Encryption & Cryptography

PUBLIC KEY CRYPTOGRAPHY

Asymmetric Key Cryptography:

This type of cryptography uses a pair of keys to encrypt data. Each user has a public & private key. Public key is available to everyone. Anyone can use the public key to encrypt the data, however only the recipient who holds the private key can decrypt the data. Public key cryptography works on asymmetric key cryptography.

Public Key Cryptography

- Separate keys for encrypting and decrypting.
- The size of ciphertext is the same or larger than the original plaintext.
- It provides confidentiality, authenticity and non-repudiation.
- The length of key used is 128 or 256 bits.
- It is efficient since it is used for handling large amount of data.
- The mathematical expression :

$$P = D(Kd, E(Ke, P))$$

Ke: encryption key

D: decryption

Kd: decryption key

P: plain text

E(Ke, P) : Encryption of plain text using encryption key Ke.

Symmetric Key Cryptography

- Requires only single key for both encrypting and decrypting.
- The size of ciphertext is the same or smaller than the original plaintext.
- It provides confidentiality.
- The length of key used is 2048 or higher.
- Comparatively less efficient as it can handle small amount of data.
- The mathematical expression :

$$P = D(K, E(K, P))$$

K: encryption key

D: decryption

K: decryption key

P: plain text

E(K, P) : Encryption of plain text using encryption key K.

MATH OF PUBLIC KEY CRYPTOGRAPHY

The maths behind public key cryptography

While the box analogy was something physical, we're going to go back to encrypting messages much like we did with Caeser Cipher.

$$K_b^-(K_b^+(m)) = m$$

When you apply the public key (K^+) to the encrypted message, and the private key (K^-) to the encrypted message you get the plaintext messag are also looking for these attributes:

It is computationally easy to:

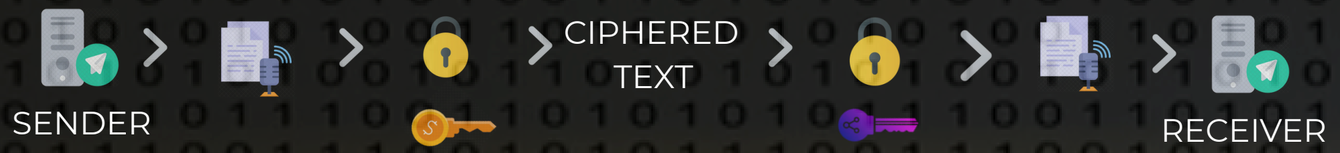
- Generate a set of keys
- Encrypt / Decrypt using these keys

But it is also computationally infeasible to:

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

RSA ALGORITHM

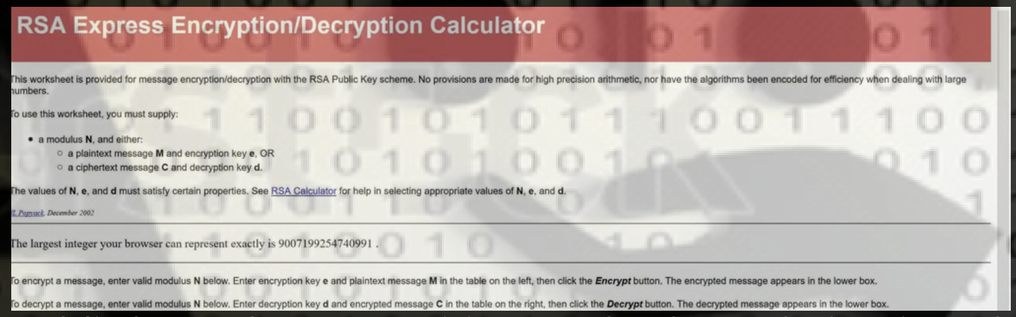
What is RSA Algorithm?



RSA - **R**ivest-**S**hamir-**A**dleman

Under RSA encryption, messages are encrypted with a code called a public key, which can be shared openly. Due to some distinct mathematical properties of the RSA algorithm, once a message has been encrypted with the public key, it can only be decrypted by another key, known as the private key. Each RSA user has a key pair consisting of their public and private keys. As the name suggests, the private key must be kept secret. Uses asymmetric key cryptography.

Working of RSA Algorithm



RSA Express Encryption/Decryption Calculator

This worksheet is provided for message encryption/decryption with the RSA Public Key scheme. No provisions are made for high precision arithmetic, nor have the algorithms been encoded for efficiency when dealing with large numbers.

To use this worksheet, you must supply:

- a modulus **N**, and either:
  - a plaintext message **M** and encryption key **e**, OR
  - a ciphertext message **C** and decryption key **d**.

The values of **N**, **e**, and **d** must satisfy certain properties. See RSA Calculator for help in selecting appropriate values of **N**, **e**, and **d**.

T. Pogrzeb, December 2007

The largest integer your browser can represent exactly is 9007199254740991 .

To encrypt a message, enter valid modulus **N** below. Enter encryption key **e** and plaintext message **M** in the table on the left, then click the ***Encrypt*** button. The encrypted message appears in the lower box.

To decrypt a message, enter valid modulus **N** below. Enter decryption key **d** and encrypted message **C** in the table on the right, then click the ***Decrypt*** button. The decrypted message appears in the lower box.

The two entities first need to set up their key pairs and share their public keys. The two entities need to keep their private keys secret in order for their communications to remain secure. Once the sender has the public key of their recipient, they can use it to encrypt the data that they want to keep secure. Once it has been encrypted with a public key, it can only be decrypted by the private key from the same key pair. When the recipient receives the encrypted message, they use their private key to access the data. In this way, RSA encryption can be used by previously unknown parties to securely send data between themselves.

IDEA : It is difficullt to factorize a large integer. Public key is **(n, e)** and private key is **(n, d)**. **(d * e) = 1 mod (p-1)*(q-1)**. We need to find the values of p and q. RSA Algorithm takes the value of p and q to be very large which in turn makes the value of n extremely large and factorizing such a large value is computationally impossible. Therefore encryption strength lies in the values of p and q. RSA keys can be typically 1024 or 2048 bits long.

CODE FOR RSA

```
def rsa(p, q):
    n = p * q
    z = (p - 1) * (q - 1)

    # calculate e such that e is less than z
    # and e has no common factors with z
    for i in range(1, z - 1):
    if z % i != 0:
        e = i
        break

    d = (filter(lambda x: ((x * 5) - 1) % 24 == 0, range(1, 200)))[0]
    return{"Public key": [n, d], "Private Key": [n, e]}

# change p and q here to any prime numbers of your choice
p = 5
q = 7

print(rsa(p, q))
```

DIGITAL SIGNATURE

Concept

A digital signature is a mathematical scheme that is used to verify the integrity and authenticity of digital messages and documents. The digital signatures use asymmetric cryptography i.e. also known as public key cryptography. Digital signatures prove that the message or document came from the claimed sender and ensures integrity. They provide a way to prove that the sender signed the message, making it difficult for them to deny having done so. Digital signatures rely on Public Key Infrastructure (PKI), which uses a pair of keys: a private key (known only to the signer) and a public key (available to anyone).

How it works?

This is used in conjunction with hashing. The private key of the sender is used to encrypt the hash value generated. The encrypted hash value along with the hash algorithm constitutes the digital signature. The sender will now send the message along with the encrypted hash value to the receiver. The receiver can only decrypt the hash value using the sender’s public key. At the receiver end, there are two steps, to generate the hash of the message and decryption of the signature. By using the sender’s public key, the signature can be decrypted. if the decrypted hash matches the second computed hash value then it proves that the message hasn’t been changed since it was signed. If the two hash values don’t match then it means that the message has been tampered with along its way. Bitcoin signatures have a way of indicating which part of a transaction’s data is included in the hash signed by the private key using a SIGHASH flag. The SIGHASH flag is a single byte that is appended to the signature. Every signature has either an explicit or implicit SIGHASH flag, and the flag can be different from input to input. A transaction with three signed inputs may have three signatures with different SIGHASH flags, each signature signing (committing) to different parts of the transaction.

TYPES OF BITCOIN WALLETS

HOT & COLD WALLETS

- Hot wallets are connected to the internet and thus are less secure and pose more risks. Cold wallets, on the other hand, are stored offline and don't require internet connectivity.
- Hot wallets offer convenience and accessibility, cost-effective and integration with exchanges. Cold wallets offer superior security by keeping private keys completely offline.
- Hot wallets are not Ideal for Large Holdings, lack of control and security risks. being less convenient for frequent transactions, having a learning curve for beginners, and facing potential risks of physical loss or damage.

HARDWARE WALLETS

- Hardware wallets are hardware devices that individually handle public addresses and keys. It looks like a USB with an OLED screen and side buttons.
- The major advantage of hardware wallets is that they do not stay connected to the internet 24/7 and are at the least risk of getting hacked.
- Less convenient for day-to-day transactions. Hardware wallets are the most expensive.

PAPER WALLETS

- A paper wallet is a method of storing cryptocurrency offline by writing (or printing) the personal and public keys onto a piece of paper. Unlike other storage methods, paper wallet does not use any form of digital storage.
- Maximum protection from cyberattacks, hardware failures, operating system errors and breakdowns. Useful for long-term storage of funds. It is easy to generate and print them.
- A major flaw is not being able to send partial funds, therefore, it can't be reused. Also paper can be easily damaged.

DESKTOP WALLETS

- A desktop wallet is a program for your computer that store your private keys on your computer's hard drive. This type of wallet still needs to be connected to the internet should you ever want to buy or use your cryptocurrency.
- The best method for cold storage in a completely clean system. They are easy to use, give privacy and anonymity, and involve no third party.
- Anti-virus is required because a system connected to the Internet poses fundamental security issues. Regular backing up of the computer is needed..

MOBILE WALLETS

- Mobile wallets are just like desktop wallets made for smartphones. They are quite convenient as it uses QR codes for transactions. They are suitable for daily operations but are vulnerable to malware infection.
- These are convenient, accessible with enhanced security features. Comes with backup and recovery options and integration with other apps
- These are vulnerable to Cyber Attacks with potential exposure to data gathered by mobile platforms. Also susceptible to physical loss.

WEB WALLETS

- These wallets are accessed by internet browsers. The private keys are held in some web wallets. Web wallets allow users to access their funds on the go as long as they can connect to the internet, so it can be very convenient.
- These are convinient, have multiple security features like encryption and 2FA. It has cross platform compatibility and efficient with quick transactions.
- It has security issues due to dependence on third-parties. It also has limited control. Posed to risks of phising & malware.

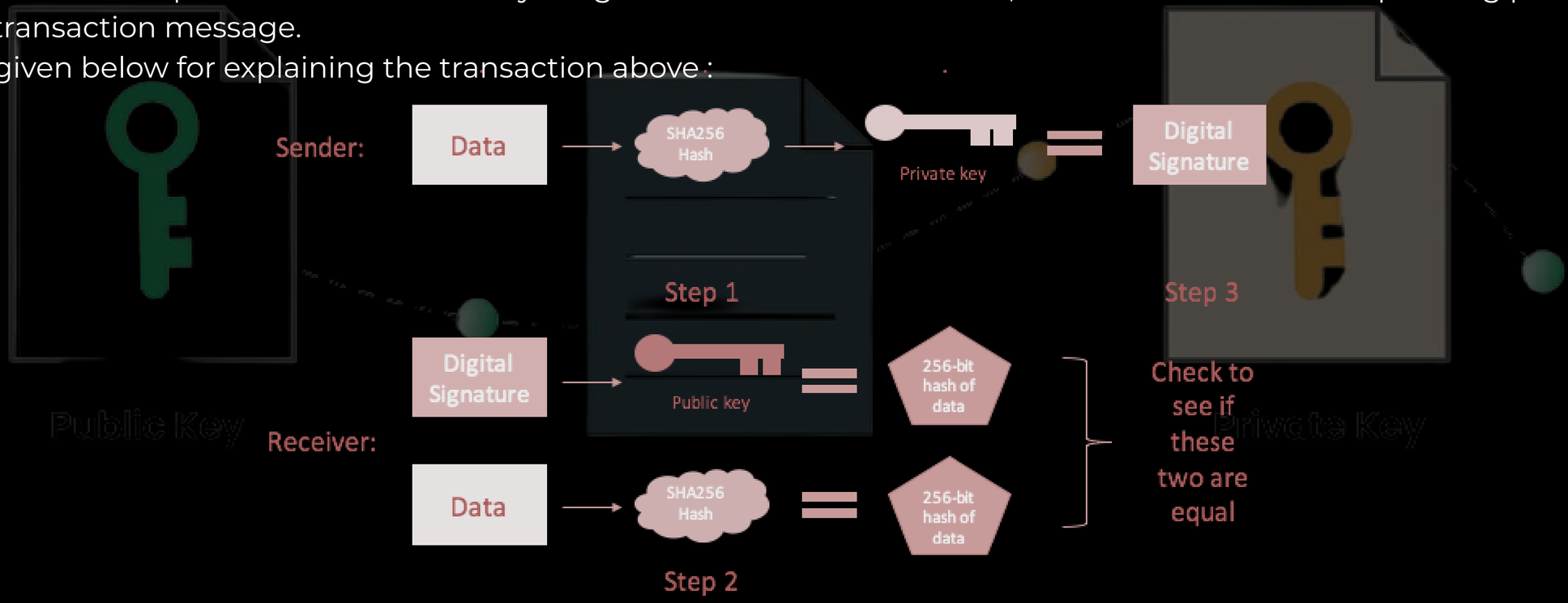
PUBLIC-PRIVATE KEY IN BITCOIN WALLETS

Encryption:

To understand this, let us consider two persons, Alice and Bob.

Bob sends Alice his Bitcoin wallet address to enable the transaction. Next, Alice pastes the address in her wallet and uses her private key to sign the transaction. Note that the seed phrase isn't directly used to sign transactions. However, someone can access Alice's private key if they get her seed phrase. The private key generates a signature containing transaction details. This acts like a digital fingerprint, proving to the blockchain that Alice owns the funds and wants to perform the transaction described in the message. Once Alice has signed the transaction, it is encrypted by Bob's public key and then broadcast to the network for verification. Nodes validate the transaction by checking that the signature corresponds to Alice's public key and that Bob's address exists. The nodes will confirm the transaction and complete the transfer if everything is valid. To access the 1 BTC, Bob must use the corresponding private key to decrypt the transaction message.

An image is given below for explaining the transaction above :



USE OF PUBLIC PRIVATE KEY

How it is generated?

Public and private keys are generated **using cryptographic algorithms like RSA or ECC, where a mathematical relationship links them, allowing the public key to be shared while the private key remains secret**. Some algorithms are :

- **Rivest-Shamir-Adelman (RSA):** Oldest of the public-private key cryptography systems. Frequently used to transmit shared keys for symmetric key cryptography.
- **Digital Signature Standard (DSS):** A Federal Information Processing Standard specifying the algorithms that can be used to generate digital signatures used by NIST.
- **Elliptic curve cryptography (ECC):** As its name implies, ECC relies on elliptic curves to generate keys. It is often used for key agreements and digital signatures.

How it is used for encryption?

Public key encryption uses a pair of mathematically-related keys. A message that is encrypted with the first key must be decrypted with the second key, and a message that is encrypted with the second key must be decrypted with the first key.

Each participant in a public key system has a pair of keys. One key is the private key and is kept secret. The other key is public, this key is the public key. Anyone can encrypt a message by using your public key. When you receive the message, you decrypt it by using your private key. You can then send the message safely over an unsecured connection.

This kind of encryption has characteristics that make it very suitable for general use:

- Public key encryption requires only two keys per participant.
- Only the private key needs to be kept secret, hence it is less vulnerable to theft in transmission than the shared key in a symmetric key system.
- Public keys can be published, which eliminates the need for prior sharing of a secret key before communication. Anyone who knows your public key can use it to send you a message that only you can read.

SECURING BITCOIN WALLETS

How are bitcoin wallets secured?

Private keys are essential because they allow you to access your Bitcoin assets. Anyone with access to the keys can easily access your funds. As such, you should always safeguard your wallet's private keys using the following measures:

- **Back Up Your Seed Phrase :**

Your seed phrase is the gateway to your private keys. If your phone crashes, for example, you can't access your wallet and seed phrase and could lose your assets forever. To avoid this, back up the seed phrase by writing it down on paper. Then, store this paper in a secure home safe. You can access your private keys on any device using your seed phrase.

- **Add an Extra Layer of Security :**

Use your wallet's security features to add an extra layer of security. For instance, rather than relying on biometric authentication, you can improve the security of your wallet by creating a password or PIN. Ensure you save this password or PIN with a reliable password manager to avoid forgetting it.

- **Consider Cold Storage :**

Hardware wallets eliminate the worry of online threats by storing private keys and seed phrases offline. This is a suitable solution if you have accumulated a large amount of bitcoin or other digital assets. Still, you must back up your hardware wallet's seed phrase on paper for easy private key recovery.

- **Use a Reputable and Reliable Wallet Provider :**

A reputed wallet provider gives several security features like 2FA, encryption & access control, multi-signature support and it also has regular maintainance an regulatory updates. Open-source wallets like Electrum allow anyone to audit their code for security and transparency, enhancing trust and security.


THANK YOU!
TANUSH BADONIA