SNS COLLEGE OF ENGINEERING
Kurumbapalayam (Po), Coimbatore – 641 107
AN AUTONOMOUS INSTITUTION
Accredited by NAAC-UGC with 'A' Grade, Accredited by NBA
Approved by AICTE & Affiliated to Anna University, Chennai.

Introduction to Public-Key Cryptography

Public-key cryptography, also known as asymmetric cryptography, is a cryptographic system that uses a pair of keys: a public key and a private key. This system enables secure communication and data exchange over insecure channels without the need to share secret keys beforehand. Here's a comprehensive overview of public-key cryptography:

Key Concepts

1. **Public Key**:
   - This key can be shared openly with anyone. It is used to encrypt data or verify a digital signature.
2. **Private Key**:
   - This key is kept secret and is used to decrypt data encrypted with the corresponding public key or to create a digital signature.
3. **Asymmetry**:
   - The key pair is mathematically related, but it is computationally infeasible to derive the private key from the public key.

How Public-Key Cryptography Works

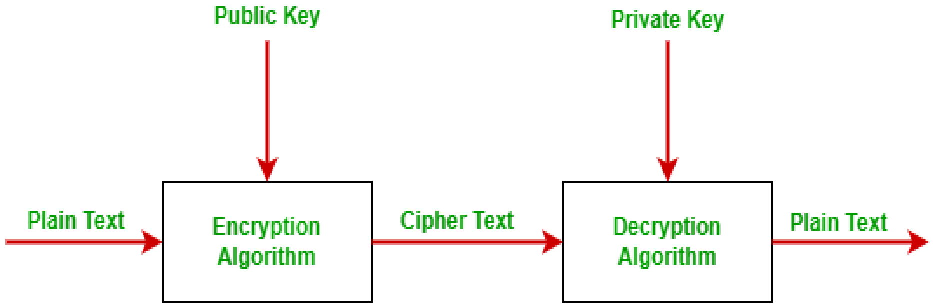
1. **Encryption**:
   - When someone wants to send a confidential message, they encrypt the message using the recipient's public key. Only the recipient, who possesses the corresponding private key, can decrypt the message.
2. **Digital Signatures**:
   - The sender can create a digital signature for a message using their private key. The recipient can verify the authenticity of the message by using the sender's public key. This process ensures the message's integrity and authenticity.
3. **Key Exchange**:

- Public-key cryptography can be used to securely exchange symmetric keys, which can then be used for faster encryption of messages using symmetric encryption algorithms.

Applications of Public-Key Cryptography

- **Secure Communication**: Encrypted email, instant messaging, and secure file transfer.
- **Digital Signatures**: Used in software distribution, contracts, and legal documents to verify authenticity and integrity.
- **SSL/TLS**: Public-key cryptography is foundational to secure web communications, enabling HTTPS.
- **Cryptocurrencies**: Used in blockchain technology for transaction verification and user authentication.

Most of the time blockchain uses public-key cryptography, also known as asymmetric-key cryptography. Public key cryptography uses both public key and private key in order to encrypt and decrypt data. The public key can be distributed commonly but the private key can not be shared with anyone. It is commonly used for two users or two servers in a secure way.



Public Key: Public keys are designed to be public. They can be freely given to everyone or posted on the internet. By using the public key, one can encrypt the plain text message into the cipher text. It is also used to verify the sender authentication. In simple words, one can say that a public key is used for closing the lock.

Private Key: The private key is totally opposite of the public key. The private key is always kept secret and never shared. Using this key we decrypt cipher text messages into plain text. In simple words, one can say that the private key is used for opening the lock.

Why Do We Need Public-Key Cryptography?

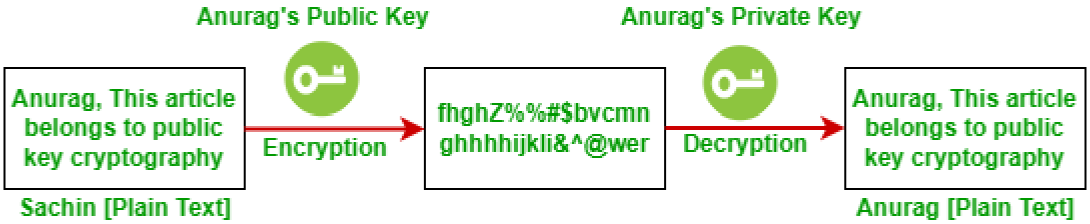
- In symmetric-key cryptography, a single key is used to encrypt and decrypt the message. Here, the possibility of data loss or unauthorized access to data is high. To overcome the unauthorized access of data and data sent securely without any loss, we use public-key cryptography.
- Public-key cryptography is more secure than symmetric-key cryptography because the public key uses two keys to encrypt and decrypt the data
- Public-key cryptography allows users to hide the data that they want to send. The sender encrypts the data and the receiver decrypts the data. The encrypted message is not understood by unauthorized users.

Working On Public-Key Cryptography

Suppose, the sender wants to send some important message to the receiver.

- The sender first creates a message in the form of plain text which is in a readable format.
- The sender knows the public key of the receiver but doesn't know the private key of the receiver because the receiver keeps secret his private key. With the help of the public key of the receiver and the private key of the sender, the sender generates the encrypted message i.e. called cipher text. Cipher text is in an unreadable format. In this step, plain text converts into cipher text.
- Now, cipher text reaches the receiver end. The receiver knows its own private key, and with the help of the private key receiver converts the cipher text into readable format i.e. plain text.

The below example shows the working of public-key cryptography.


Anurag's Public Key
Anurag's Private Key
Anurag, This article belongs to public key cryptography
Sachin [Plain Text]
Encryption
fhghZ%%#$bvcmn ghhhhijkli&^@wer
Decryption
Anurag, This article belongs to public key cryptography
Anurag [Plain Text]

Let us try to under the working of public-key cryptography with an example. Suppose Sachin is the sender who wants to send a message to Anurag. Here Anurag is the receiver.

- Sachin uses Anurag's public key to encrypt the message and Anurag uses his own private key to decrypt the message.
- First Sachin creates plain text. Sachin has access to Anurag's private key and cipher text. Using Anurag's public key and his own public key,
- Sachin will generate an encrypted message i.e. cipher text which is in an unreadable format. After applying the encryption process plain text converts into cipher text.
- Now, Anurag receives a cipher text. First Anurag will decrypt the cipher text message into a readable format. For decrypting Anurag will use the private key. Now cipher text converts into plain text and is readable by the receiver. Because Sachin keeps his private key, Anurag knows that this message couldn't have come from anyone else. This is also called a digital signature.

Benefits of Public-key Cryptography

- **Authentication:** It ensures to the receiver that the data received has been sent by the only verified sender.
- **Data integrity:** It ensures that the information and program are changed only in a specific and authorized manner.

- **Data confidentiality:** It ensures that private message is not made available to an unauthorized user. It is referred to as privacy or secrecy.
- **Non-repudiation:** It is an assurance that the original creator of the data cannot deny the transmission of the said data to a third party.
- **Key management:** Public-key cryptography allows for secure key management, as the private keys are never transmitted or shared. This eliminates the need for a secure channel to transmit the private key, as is required in symmetric key cryptography.
- **Digital signatures:** Public-key cryptography allows for the creation of digital signatures, which provide non-repudiation and can be used to verify the authenticity and integrity of data.
- **Key exchange:** Public-key cryptography enables secure key exchange between two parties, without the need for a pre-shared secret key. This allows for secure communication even if the parties have never communicated before.
- **Secure communication:** Public-key cryptography enables secure communication over an insecure channel, such as the internet, by encrypting the data with the public key of the recipient, which can only be decrypted by the recipient's private key.
- **Versatility:** Public-key cryptography can be used for a variety of purposes, such as secure communication, digital signatures, and authentication, making it a versatile tool for securing data and communications.

Limitation of Public-Key Cryptography

- One can encrypt and decrypt the fixed size of messages or data. If there is an attempt to encrypt or decrypt a large size of the message then the algorithm demands high computational power.
- The main disadvantage of this algorithm is that if the receiver losses its private key then data/message will be lost forever.
- If someone has access private key then all data will be in the wrong hand.
- There are many secret-key which is faster than public-key cryptography.

- **Key distribution:** The process of securely distributing public keys to all authorized parties can be difficult and time-consuming, especially in large networks.
- **Performance:** Public-key cryptography is generally slower than symmetric-key cryptography due to its more complex algorithms, making it less suitable for applications that require fast processing speeds.
- **Security assumptions:** Public-key cryptography relies on mathematical assumptions about the difficulty of certain problems, such as factoring large numbers, which may not hold true in the future. As a result, public-key cryptography is vulnerable to future advancements in computing power and algorithmic breakthroughs.
- **Susceptibility to man-in-the-middle attacks:** Public-key cryptography is vulnerable to man-in-the-middle attacks where an attacker intercepts and alters the public key before it reaches the intended recipient. This can result in the attacker being able to decrypt the message or impersonate the sender.
- **Complexity:** Public-key cryptography can be more complex to understand and implement than symmetric-key cryptography, requiring specialized knowledge and expertise.