Public Key Cryptography

- Public key cryptography is a method of encrypting or signing data with two different keys and making one of the keys, the public key, available for anyone to use.
- The other key is known as the private key. Data encrypted with the public key can only be decrypted with the private key.
- Public key cryptography, also known as asymmetric cryptography, is a fundamental cryptographic technique used for securing communications, digital signatures, and data encryption.
- It relies on the use of a pair of cryptographic keys: a public key and a private key, which are mathematically related but serve different purposes.

Working & Its Key Concept

1. Key Pair Generation:

- Public Key: This key is intended to be shared openly and is used for encryption and verification. It is generated from the private key using a mathematical algorithm. A public key, once generated, can be freely distributed to anyone.
- Private Key: This key must be kept secret and is used for decryption and creating digital signatures. It is generated along with the public key, but its secrecy is crucial to the security of the system.

2. Encryption:

- When someone wants to send a secure message to another person, they use the recipient's public key to encrypt the message. Once encrypted with the public key, the message can only be decrypted using the corresponding private key, which is held only by the intended recipient. This ensures confidentiality because only the recipient can read the message.
- Common encryption algorithms used in public key cryptography include RSA (Rivest-Shamir-Adleman) and ElGamal.

3. Decryption:

The recipient, who possesses the private key corresponding to the public key used for encryption, can decrypt the message.

Er. Harsh Raj
(Assistant Professor, CSE)

The private key is mathematically designed to work in tandem with the public key, allowing the recipient to recover the original message.

4. Digital Signatures:

• In public key cryptography, digital signatures are used to verify the authenticity and integrity of a message or document. To create a digital signature, the sender uses their private key to encrypt a hash (a fixed-size value derived from the content) of the message or document. This creates a unique signature that can only be verified using the sender's public key.

• The recipient of the digitally signed message can use the sender's public key to decrypt the signature and verify that it matches the hash of the received message. If the signature is valid, it confirms that the message has not been tampered with and was indeed signed by the holder of the private key.

5. Applications:

• Public key cryptography plays a crucial role in securing digital communication over the internet. For example, HTTPS (Hypertext Transfer Protocol Secure) uses public key cryptography to encrypt data exchanged between web browsers and servers. • Secure email communication, as implemented in PGP (Pretty Good Privacy) and GPG (GNU Privacy Guard), relies on public key cryptography.

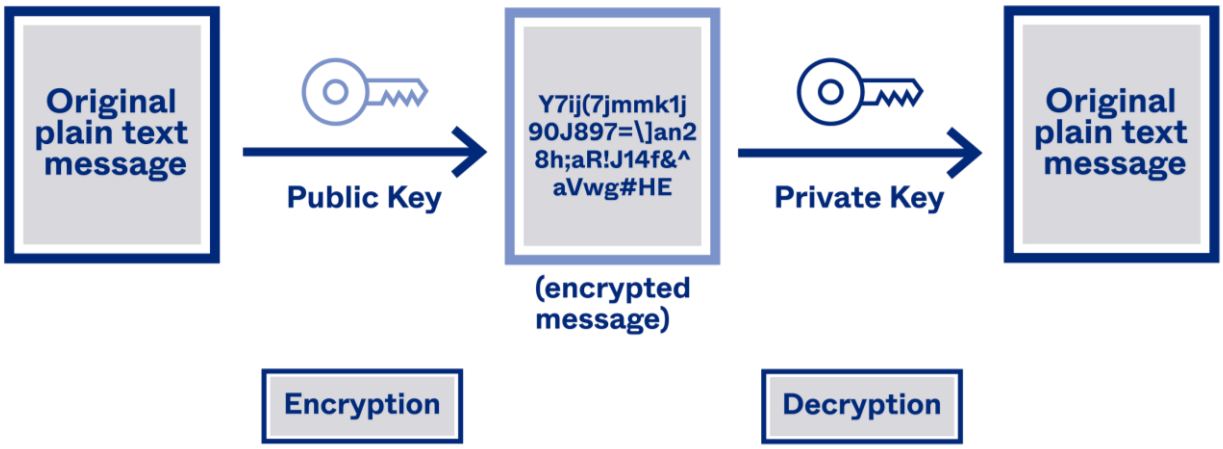
• Digital wallets for cryptocurrencies use public key cryptography to secure transactions. Users have a pair of keys: a public address (used to receive funds) and a private key (used to sign transactions).

• Secure authentication and digital identity management use public key cryptography to verify the identity of individuals and devices.

Note: Public key cryptography is a cornerstone of modern cybersecurity, providing a robust framework for secure communication and authentication in an open and interconnected digital world. Its mathematical foundations ensure that even though the public key is openly shared, the private key remains a well-guarded secret, enabling secure encryption and digital signatures.

Er. Harsh Raj
(Assistant Professor, CSE)

Public Key Encryption



Er. Harsh Raj
(Assistant Professor, CSE)