

Public Key Encryption

1976 saw the introduction of a radical new idea into the field of cryptography. This idea centered around the premise of making the encryption and decryption keys different - where the knowledge of one key would not allow a person to find out the other. Public key encryption algorithms are based on the premise that each sender and recipient has a private key, known only to him/her and a public key, which can be known by anyone. Each encryption/decryption process requires at least one public key and one private key. A key is a randomly generated set of numbers/ characters that is used to encrypt/decrypt information.

A public key encryption scheme has six major parts:

Plaintext - this is the text message to which an algorithm is applied.

Encryption Algorithm - it performs mathematical operations to conduct substitutions and transformations to the plaintext.

Public and Private Keys - these are a pair of keys where one is used for encryption and the other for decryption.

Ciphertext - this is the encrypted or scrambled message produced by applying the algorithm to the plaintext message using key.

Decryption Algorithm - This algorithm generates the ciphertext and the matching key to produce the plaintext.

Selecting the Public and Private Keys

1. Select large prime numbers p and q and form $n = pq$.
2. Select an integer $e > 1$ such that $\text{GCD}(e, (p - 1)(q - 1)) = 1$.
3. Solve the congruence, $ed \equiv 1 \pmod{(p - 1), (q - 1)}$
for an integer d where $1 < d < (p - 1)(q - 1)$.
4. The public encryption key is (e, n) .
5. The private encryption key is (d, n) .

The Encryption Process

- The process of encryption begins by converting the text to a pre hash code. This code is generated using a mathematical formula.
- This pre hash code is encrypted by the software using the senders private key. The private key would be generated using the algorithm used by the software.
- The encrypted pre hash code and the message are encrypted again using the sender's private key.
- The next step is for the sender of the message to retrieve the public key of the person this information is intended for.
- The sender encrypts the secret key with the recipient's public key, so only the recipient can decrypt it with his/her private key, thus concluding the encryption process.

1. Lookup the user's public key (e, n) .
2. Make sure that the message M is an integer such that $0 \leq M \leq n$.
3. Compute, $M^e \pmod n$ where $0 \leq C \leq n$.
4. Transmit the integer C .

The Decryption Process

- The recipient uses his/her private key to decrypt the secret key.
- The recipient uses their private key along with the secret key to decipher the encrypted pre hash code and the encrypted message.
- The recipient then retrieves the sender's public key. This public key is used to decrypt the pre hash code and to verify the sender's identity.
- The recipient generates a post hash code from the message. If the post hash code equals the pre hash code, then this verifies that the message has not been changed en-route.

1. Use your private key (d, n) .
2. Receive the integer C , where $0 \leq C \leq n$.
3. Compute, $C^d \pmod n$ where $0 \leq R \leq n$.
4. R is the original message.

HOW IT WORKS

Public-key infrastructure

Electronic business is picking up, and with it the need for secure electronic credentials is increasing. PKI is a way to prove identity in the online world. It also certifies that documents have not been tampered with.

- 1** A document, such as a check, is digitally signed using hashing technology, the sender's private encryption key and the receiver's public key.



- 2** The scrambled and encrypted document is sent.



- 3** Using rehashing technology, the data from the received document is compared with that of the original document. This way, the document's authenticity can be assured.



- 4** The document is decrypted using the receiver's private key and the sender's public key.