RSA Encryption

Rivest-Shamir-Adleman

Introduction

The most famous of the public key cryptosystem is RSA which is named after its three developers Ron Rivest, Adi Shamir, and Leonard Adleman. It is a public key asymmetric cryptographic algorithm used to encrypt/decrypt data.

A suite of cryptographic algorithms that are used for specific security services or purposes -- which enables public key encryption and is widely used to secure sensitive data, particularly when it is being sent over an insecure network such as the internet.

Working of RSA Encryption

It works on two keys:

- Public key: It comprises two numbers, in which one number is the result of the product of two large prime numbers. This key is provided to all the users.
- Private key: It is derived from the two prime numbers involved in public key and it always remains private.

- Key Generation:
  a. Select 2 large prime numbers ‘p’ and ‘q’.
  b. Calculate n

$$n = p*q$$

  c. Calculate $\phi(n)$

$$\phi(n) = (p-1)*(q-1) \text{ \{euler's Totient Function\}}$$

  d. Chose value of e, which can be used for decryption.

$$1 < e < \phi(n) \text{ and } \gcd(\phi(n), e) = 1$$

  e. Calculate d

$$d \equiv e^{-1} \bmod \phi(n) \qquad \text{i.e.} \quad ed = 1 \bmod \phi(n)$$

  f. Public key = {e, n}
  g. Private key = {d,n}

- Encryption
  a. Plaintext (M)
  b. ciphertext(C)

$$C = M^e \bmod n$$

- Decryption

$$M = C^d \bmod n$$

The Uses of RSA Encryption

- RSA encryption is often used in combination with other encryption schemes, or for digital signatures which can prove the authenticity and integrity of a message. It isn't generally used to encrypt entire messages or files, because it is less efficient and more resource-heavy than symmetric-key encryption
- A file will generally be encrypted with a symmetric-key algorithm, and then the symmetric key will be encrypted with RSA encryption. Under this process, only an entity that has access to the RSA private key will be able to decrypt the symmetric key.
- RSA encryption can be used in a number of different systems. It can be implemented in OpenSSL, wolfCrypt, cryptlib and a number of other cryptographic libraries.
- One of the first widely used public-key encryption schemes, RSA laid the foundations for much of our secure communications. It was traditionally used in TLS and was also the original algorithm used in PGP encryption. RSA is still seen in a range of web browsers, email, VPNs, chat and other communication channels.
- RSA is also often used to make secure connections between VPN clients and VPN servers. Under protocols like OpenVPN, TLS handshakes can use the RSA algorithm to exchange keys and establish a secure channel.

Advantages of RSA

- It is very easy to implement RSA algorithm.
- RSA algorithm is safe and secure for transmitting confidential data.
- Cracking RSA algorithm is very difficult as it involves complex mathematics.
- Sharing public key to users is easy.

Disadvantages of RSA

- It may fail sometimes because for complete encryption both symmetric and asymmetric encryption is required and RSA uses asymmetric encryption only.
- It has slow data transfer rate due to large numbers involved.
- It requires third party to verify the reliability of public keys sometimes.
- High processing is required at receiver’s end for decryption.
- RSA can’t be used for public data encryption like election voting.