RSA Algorithm
A Short Description

Frans (frans@ic.vlsi.itb.ac.id)
Department of Electrical Engineering
Institut Teknologi Bandung
Ganesha 10 Bandung, Indonesia

Abstract

RSA is a widely used cryptosystem in the world. It is a public key cryptosystem which uses two kinds of key, private key and public key. Every user has both of the keys, a private one and a public one. If user A wants to send a message to B, he need B's public key to encrypt the message. After encrypted, the message is received by B, then B uses his private key to decrypt the message.

RSA Algorithm

RSA algorithm can be classified as three algorithms, the key generation algorithm, encryption algorithm, and decryption algorithm.

RSA key generation algorithm can be described as follows [1],

1. Generate two large random and distinct primes P and Q
2. Calculate $N = P.Q$ and $\phi = (P - 1)(Q - 1)$
3. Choose a random integer E, $1 < E < \phi$, such that $\gcd(E,\phi) = 1$
4. Compute the unique integer D, $1 < D < \phi$, such that $ED \equiv 1 \pmod{\phi}$
5. Public key is (N, E) and private key is (N, D)

RSA encryption algorithm can be described as follows,

$$C = M^E \bmod N,$$

RSA decryption algorithm can be described as follows,

$$M = C^D \bmod N,$$

which C represents ciphertext and M represents message.

Reference

[1] A. Menezes, P. van Oorschot, S. Vanstone . Handbook of Applied Cryptography . CRC Press . 1996.