Basics of the RSA Cipher System

MIZOGUCHI Koki[1)]

Kochi University of Technology

June 15, 2022

KOCHI UNIVERSITY OF TECHNOLOGY

[1)] Information Security System Laboratory

Table of Contents

1. What's the RSA
2. A type of algorithm for public key cryptography
3. Encryption and decryption
4. Make keys
   - N is obtained
   - L is obtained
   - E is obtained
   - D is obtained

What's the RSA

Prime factorization of large number is difficult.This is because there is no other way to find prime factors except by round-robin.
Therefore, even if one tries to factorize a large number using a computer, it will take an enormous amount of time.
The RSA cipher users this mechanism.

This is named after the three inventors, R.L.Rivest, A.Shamir, and L.Adleman.

A type of algorithm for public key cryptography

RSA cipher is a type of algorithm for public key cryptography.
Public key cryptography is an encryption scheme in which the encroption key and decryption key are separete.
With RSA, the plaintext, key, and ciphertext are number.
Denote the ciphertext as C, plaintext as P.

Encryption and decryption

Encryption by RSA

$$C = P^E \bmod N \tag{1}$$

$\{E, N\}$ is the public key.

RSA decryption

$$P = C^D \bmod N \tag{2}$$

$\{D, N\}$ is the private key.

Make keys

How to prepare the E, D, N?

1. N is obtained.
2. L is obtained. (L appears only when making the keys.)
3. E is obtained.
4. D is obtained.

N is obtained

The first step is to prepare two large prime numbers.Denote the prime numbers as p, q respectively.

L is obtained

L is the least common multiple of $p-1$ and $q-1$

$$L = \mathrm{lcm}(p-1, q-1) \tag{3}$$

L that appears only when creating a key pair.

E is obtained

D is obtained

The first step is to prepare two large prime numbers.Denote the prime numbers as p, q respectively.