Mini Topics
On RSA and Discrete Logarithm Problem

賴奕甫

Contents

自我介紹

- 賴奕甫 (男)
- 82 (1993) 年生
- 台大數學所碩二 (已通過口試)
- 興趣:半夜慢跑, 摺紙

Chinese Remainder Theorem

中國南北朝時期（公元5世紀）的數學著作《孫子算經》卷下第二十六題，

叫做「物不知數」問題，原文如下：

有物不知其數，三三數之剩二，五五數之剩三，七七數之剩二。問物幾何？

$$\begin{cases} x = 2 \; mod \; 3 \\ x = 3 \; mod \; 5 \\ x = 2 \; mod \; 7 \end{cases}$$

Chinese Remainder Theorem

Chinese Remainder Theorem:

Given n, m with $gcd(n, m) = 1$.

Then the natural homomorphism $\phi : \mathbb{Z}_{n*m} \to \mathbb{Z}_n \times \mathbb{Z}_m$ is an isomorphism.

For $x \in \mathbb{Z}_{n*m}$,
$\phi(x) = (x \ (mod\ n), x \ (mod\ m) \ )$

<sketch>

"Well-defined"

"hom"

"surjective"

RSA Encryption (Notation)

- Public Key :($N = p * q, e$) (p, q: distinct primes, $gcd(e, \phi(N)) = 1$)
- Private Key: d ($de = 1 \pmod{\phi(N)}$)

$\xrightarrow{(N, e)}$

$\xleftarrow{c}$

Message: $m \in \mathbb{Z}_N$

Decryption:

$c^d = m \in \mathbb{Z}_N$

Encryption:

$c = m^e \ (mod\ N)$

Mini Topics on RSA encryption.

- The following content is not about the factoring algorithms but about some little topics in usage or on parameter settings in the RSA encryption.

RSA

- Can $\phi(N)$ be leaked?
- d can be chosen to be $de = 1 \pmod{lcm(p-1, q-1)}$
- What if e is chosen too small ($e = 3$)?
- $\begin{cases} \text{Can N be a domain parameter?} \\ \text{Can we only choose new } d \text{ if the old one is exposed} \end{cases}$
- Can d chosen to be small? (for speeding up decryption)
- Is the least significant bit encryption of RSA as secure as the whole?

Can $\phi(N)$ be leaked?

Solve q by the following steps:

- Assume $\phi(N) = (p-1)(q-1)$ is given
- Public Key $N = pq$

- Write

$$p = N/q$$

- Then

$$\phi(N) = \left({}^{N}/_{q} - 1\right)(q-1)$$
$$\Rightarrow \phi(N)q = (N-q)(q-1)$$

- $\Rightarrow$?

d can be chosen to be $de = 1 \ \left(mod\ lcm(p-1, q-1)\right)$

- Show the **correctness**:

$$m^{de} = m \ (mod\ N) \quad for\ any\ m \in \mathbb{Z}_N$$

<proof>:

Consider Chinese remainder theorem, it suffices to proof

$$m^{de} = m \ (mod\ p)$$
$$m^{de} = m \ (mod\ q)$$

<case:$p|m$ or $q|m$>: HOLDS!

<case:$p \nmid m$ and $q \nmid m$>:

It suffices to show

$$m^{de-1} = 1 \ (mod\ p)$$

Show the correctness:

$$m^{de} = m \pmod N \quad for\ any\ m \in \mathbb{Z}_N$$

<proof>(continued)

<case: $p \nmid m$ and $q \nmid m$>:

Since

$$lcm(p-1, q-1) \mid de - 1,$$

$$p - 1 \mid lcm(p-1, q-1), \text{ and}$$

$$m^{p-1} = 1 \pmod p \qquad \text{(Fermat's little theorem)}$$

$$m^{lcm(p-1,q-1)} = 1 \pmod p,$$

so

$$m^{de-1} = 1 \pmod p$$

What if e is chosen too small?

-Hastad's Broadcast Attack

- Take $e = 3$ for example
- Assumption:
  - There are 3 people use RSA encryption with public key $(N_1, e), (N_2, e), (N_3, e)$ (relatively prime N_1, N_2, N_3)
  - They receive a cipher c_i from the same message m with their own public keys. ($m < N_i$ for all i)

- Oscar collects $(N_i, e = 3)$, and c_i. By CRT, $\exists!\ c \in \mathbb{Z}_{N_1 N_2 N_3}$ satisfies

$$\begin{cases} c = c_1 \quad mod\ N_1 \\ c = c_2 \quad mod\ N_2 \\ c = c_3 \quad mod\ N_3 \end{cases}$$

What if e is chosen too small?

-Hastad's Broadcast Attack

- Oscar collects $(N_i, e = 3)$, and c_i. By CRT, $\exists!\ c \in \mathbb{Z}_{N_1 N_2 N_3}$ satisfies

$$\begin{cases} c = c_1 = m^3 \quad mod\ N_1 \\ c = c_2 = m^3 \quad mod\ N_2 \\ c = c_3 = m^3 \quad mod\ N_3 \end{cases}$$

- Hence, $c = m^3 \quad mod\ N_1 N_2 N_3$
- Notice that $m^3 < N_1 N_2 N_3$
- $\Rightarrow$?

Example

- (See)

If $e = 3$, then half of bits of d are exposed (roughly).

Assume primes $p, q > 5$ and $d < \phi(N)$.

Claim: $e = 3 \Rightarrow ed = 1 + 2\phi(N)$

<proof>

Write $ed = 1 + k\phi(N) = 1 + k(p-1)(q-1)$

Known $0 < k \leq e = 3$

Calculate $(p - 1\, mod\, 3)$

$\because$ $gcd(p, 3) = 1$ and $gcd(p-1, 3) = 1$

$\therefore$ $p - 1 = 1\, mod\, 3$

Similarly, $q - 1 = 1\, mod\, 3.$

Hence, $k = 2\, mod\, 3$, so $k = 2$

■

If $e = 3$, then half of bits of d are exposed (roughly).

- Let $d' = \left\lfloor \frac{1}{e}(1 + kN) \right\rfloor = \left\lfloor \frac{1}{e}(1 + 2N) \right\rfloor$.
- Claim $|d' - d| < p + q$

<Proof>

Write $d' = \left\lfloor \frac{1}{e}(1 + 2N) \right\rfloor = \frac{1}{e}(1 + 2N) + \epsilon$ for some $\epsilon, |\epsilon| < 0.5$

Then $|d' - d| =?$

If $e = 3$, then the linear relation of messages can not be known.

- Assumption:
  - Alice uses RSA encryption with her public key $(N, e = 3)$
  - Encrypting m_1 and m_2 with a linear relation $m_2 = am_1 + b$
  - Given two ciphertexts c_1, c_2 and the coefficients a and b

- Oscar calculates

$$\frac{b(c_2 + 2a^3c_1 - b^3)}{a(c_2 - a^3c_1 + 2b^3)} \ mod\ N$$

$$\frac{b(c_2 + 2a^3c_1 - b^3)}{a(c_2 - a^3c_1 + 2b^3)} =?\ mod\ N$$

Example

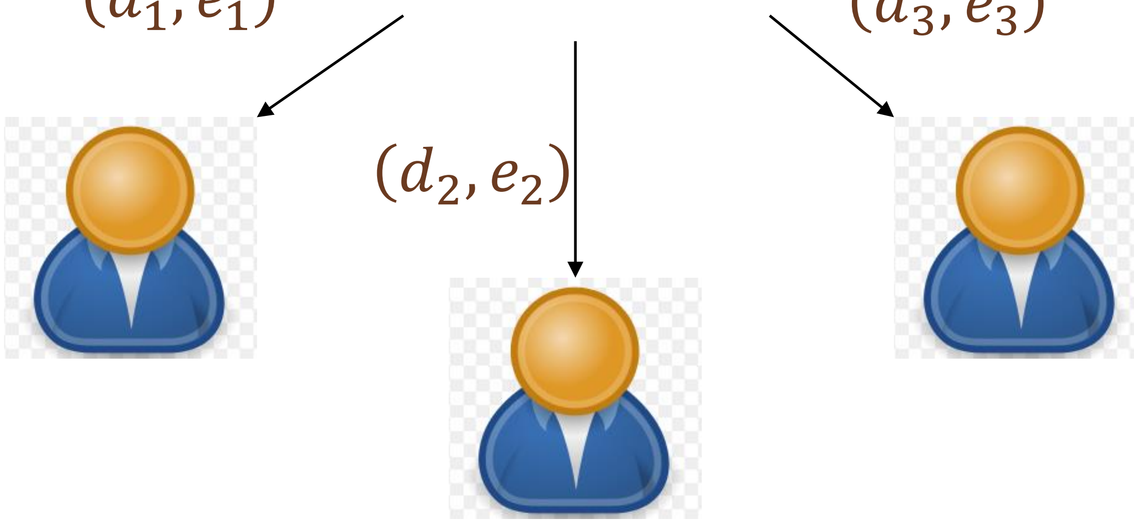
- (See)

Can N be a domain parameter?

$N = pq$

Compute

$$d_i e_i = 1 \; mod \; N$$



Can we only choose new d (and e) if the old one is exposed? (With the same N)

- Claim: Given e. "Knowing $d \Leftrightarrow$ Factoring N"
- "$\Leftarrow$": Obviously, "Factoring N"⇒"Obtain $\phi(N)$" ⇒"Getcha d"
- "$\Rightarrow$": The proof is an algorithm:

Main idea: find x, $x^2 = 1 \pmod N$

Since $N = pq \mid (x+1)(x-1)$,

if $x \neq \pm 1 \pmod N$,

then $\gcd(x \pm 1, N)$ will factor N.

Intuition: $m^{de-1} = 1 \quad (mod\ N)\ if\ gcd(m, N) = 1$

$m^{2^t r} = 1 \quad (mod\ N)\ if\ gcd(m, N) = 1$

Remark: You can further prove that the algorithm is able to factor N with probability greater than ½ for each choice of m

Can we only … if the old one is exposed? (With the same N)

- Claim: Given e. "Knowing $d \Leftrightarrow$ Factoring N"
- "⇒" : **Main idea:** find x, $x^2 = 1 \quad (mod\ N)$

  Write $k = de - 1 = 2^t r$, where r is odd

  1. **Choose** $m \in \{2, \dots, N-1\}$ at random

     Say $gcd(N, m) = 1$ **(why)**

  2. **If** $m^r = 1\ (mod\ N)$ **then** back to 1.
  3. **Compute** $2^1 r, 2^2 r, 2^3 r, \dots$ until $2^{t'} r = 1 \quad (mod\ N)$ first occurs.
  4. **If** $\mathrm{m}^{2^{t'-1} r} = \pm 1 \quad (mod\ N)$ **then** back to 1.
  5. **Else** factor N by $gcd(m^{2^{t'-1} r} \pm 1, N)$

Can N be a domain parameter?

- Given e. "Knowing $d \Leftrightarrow$ Factoring N"

- Hence,

  it's insecure that a group uses the same composite N

  with different e_i, d_i

Question:

Dose the other choice of d $\left(de = 1 \quad mod\ lcm(p-1, q-1)\right)$ alter the result?

- Given e. "Knowing $d \Leftrightarrow$ Factoring N"

- $de = 1 \quad (mod\ N)$
- $de = 1 \quad \left(mod\ lcm(p-1, q-1)\right)$

Example

- (See)

This is a Kitten Licking Its Paw!

Can d be chosen to be small ? (for speeding up decryption)

- Wiener's Attack:

  Given N, e. Assume $q < p < 2q$ and $d < \frac{1}{3}N^{\frac{1}{4}}$

  Then there is an efficient way of factoring N.

- Goal: $de = 1 \quad \left(mod\ \phi(N)\right)$

  $\Leftrightarrow \quad de - k\phi(N) = 1$

  Find k/d

Continued Fraction

- $x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$ where a_0 is an integer and a_i is non-negative integer for $i \geq 0$

is said to be a continued fraction expression of x, denoted $[a_0; a_1, a_2, \dots]$.

- Any rational number can be written as a continued fraction form

Ex. $\frac{44}{7} = 6 + \frac{2}{7} = 6 + \cfrac{1}{\frac{7}{2}} = 6 + \cfrac{1}{3 + \frac{1}{2}} = [6; 3,2]$

$= 6 + \cfrac{1}{3 + \cfrac{1}{1 + \frac{1}{1}}} = [6; 3,1,1]$

Convergents

- You can also use the Euclidean algorithm to compute a continued fraction expression

$1234 = 567 * 2 + 100$

$567 = 100 * 5 + 67$

$100 = 67 * 1 + 33$

$67 = 33 * 2 + 1$

$$\frac{1234}{567} = 2 + \cfrac{1}{5 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{33}}}}$$

- Let $x = [a_0; a_1, a_2, \dots]$, y is said to be the i^{th} convergent of x if

$$y = [a_0; a_1, a_2, \dots, a_i]$$

Origin :

Rational Approximation by Continued Fraction

Theorem. Let x be irrational, and let k/d be a rational number in lowest terms with $d > 0$. Suppose that

$$\left| x - \frac{k}{d} \right| < \frac{1}{2d^2}.$$

Then k/d is a convergent in the continued fraction expansion for x

Origin :

Rational Approximation by Continued Fraction

Theorem. $\boxed{e/N}$ ~~be irrational~~, and let k/d be a rational number in lowest terms with $d > 0$. Suppose that

$$\left|\boxed{e/N} - \frac{k}{d}\right| < \frac{1}{2d^2}.$$

Then k/d is a convergent in the continued fraction expansion for x $\boxed{e/N}$

$$de = 1 \quad \big(mod\ \phi(N)\big)$$

$$\Leftrightarrow \qquad de - k\phi(N) = 1$$

Wiener’ s Attack:

Given N, e. Assume $q < p < 2q$ and $d < \frac{1}{3}N^{\frac{1}{4}}$
Then there is an efficient way of factoring N.

- Wiener’ s Lemma.

  Given N, e, where $N = pq$ and $de - k\phi(N) = 1$

  Assume $q < p < 2q$ and $d < \frac{1}{3}N^{\frac{1}{4}}$

  Then

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}.$$

- Corollary.

  Using the condition above.

  Then k/d is a convergent in the continued fraction expansion for e/N

Wiener’ s Lemma.

$N = pq$

$de - k\phi(N) = 1.$

$q < p < 2q$

$d < \frac{1}{3} N^{\frac{1}{4}}$

Then,

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}.$$

<Proof>

$$\left|\frac{e}{N} - \frac{k}{d}\right| = \left|\frac{1 + k\phi(N) - Nk}{dN}\right|$$

$$< \left|\frac{3k\sqrt{N}}{dN}\right| < \left|\frac{3k}{d\sqrt{N}}\right|$$

$$< \left|\frac{1}{dN^{\frac{1}{4}}}\right| < \left|\frac{1}{3d^2}\right|$$

$$\begin{aligned} \phi(N) - N &= (pq - p - q + 1) - pq \\ &= -(p + q - 1) \\ &> -3q \\ &> -3\sqrt{N} \end{aligned}$$

$$\begin{gathered} d\phi(N) \geq de > k\phi(N) \\ \Rightarrow d > k \end{gathered}$$

Example : Wiener's Attack

- (see)

Take a look at SP800-56B

- (See)

Bit Security of RSA Problem

Is the least significant bit in the encryption of RSA as secure as the whole?

賴奕甫

RSA Problem

- RSA Problem :

  Given (N, e) and $c = m^e \ (mod\ N)$,

  where $N = pq$, p, q: distinct odd primes

  $de = 1 \ \left(mod\ \phi(N)\right)$

  Find $(m \ \ (mod\ N))$

A Fact:

$$Factoring\ Problem\ \geq\ \mathrm{RSA}\ problem$$

is known

$$Factoring\ Problem\ \ngeq\ \mathrm{RSA}\ problem$$

or

$$Factoring\ Problem = \mathrm{RSA}\ problem$$

is **unknown**

RSA Problem

- RSA Problem：

  Given (N, e), where $N = pq$,

  p, q: distinct odd primes

  $de = 1 \ \left(mod\ \phi(N)\right)$

$f(x) = x^e \ \ mod\ N$ is a *one-way* function

- RSA Problem：

  $f(x) = x^e \ mod\ N$ is a *one-way* function

- Even though RSA problem may be hard,

  that does NOT mean we can know nothing from it.
- For example, given $c = f(m) = m^e \ mod\ N$, we can know its

  Jacobi symbol value $\left(\frac{m}{N}\right)$, since e is odd. $\left(\left(\frac{m}{N}\right) = \left(\frac{m}{N}\right)^e = \left(\frac{c}{N}\right)\right)$

The least significant bit secure of RSA

Even though I accept

$f(x) = x^m \ mod\ N$ is a $one\text{-}way$ function,

it only means I accept it' s hard to find the **whole** inverse element.

Is it still hard to find out the parity (lsb) of the inverse element?

In a Simple Usage

ALICE

RSA-3072
(Asymmetric)

AES-128
with key ***k***
(Symmetric)

$$\big((information) \,\|\, \boldsymbol{k} \,\|\, (information)\big)^e \ mod\ N$$

BOB

RSA-3072
(Asymmetric)

AES-128
with key ***k***
(Symmetric)

We don' t have to invert whole m^e but recover some bits from m^e

Is RSA remain secure in this way?

Inverting the LSB ⇔ Solving RSA Problem

- Let $N = pq$, e , d represent the RSA parameter
- The following calculation is under $\mathbb{Z}_N$
- $c = m^e$,define

$$Parity(c) \coloneqq \begin{cases} 1 & if\ lsb\ of\ m\ is\ 1 \\ 0 & if\ lsb\ of\ m\ is\ 0 \end{cases}$$

$$Half(c) \coloneqq \begin{cases} 1 & if\ m \in [0, \frac{1}{2}N) \\ 0 & o.w \end{cases}$$

Inverting the LSB ⇔ Solving RSA Problem

$$Parity(c) \coloneqq \begin{cases} 1 & if\ lsb\ of\ m\ is\ 1 \\ 0 & if\ lsb\ of\ m\ is\ 0 \end{cases} \qquad Half(c) \coloneqq \begin{cases} 0 & if\ m \in [0, \frac{1}{2}N) \\ 1 & o.w \end{cases}$$

Having an oracle of $Half(c)$ ⇔ Having an oracle of $Parity(c)$

(Why?)

Inverting the LSB $\Leftrightarrow$ Solving RSA Problem

- For $c = m^e$, we have

$$Half(c) = 0 \Leftrightarrow m \in [0, \frac{1}{2}N)$$
$$Half(2^e c) = 0 \Leftrightarrow m \in [0, \frac{1}{4}N) \cup [\frac{2}{4}N, \frac{3}{4}N)$$
$$\vdots$$

- It follows that

Having an oracle of $Half(c)$ $\Leftrightarrow$ Solving RSA Problem.

- Since

Having an oracle of $Half(c)$ $\Leftrightarrow$ Having an oracle of $Parity(c)$,

- We know

Inverting the LSB $\Leftrightarrow$ Solving RSA Problem.