Computer Science and Information Engineering
National Chi Nan University

The Principle and Application of Secret Sharing

Dr. Justie Su-Tzu Juan

Lecture 2. Fundamental and Technology of Cryptography

§ 2.2 Public-Key Cryptosystem - RSA

Slides for a Course Based on the Text

1. *密碼學與網路安全* **by** 王旭正、柯宏叡

2. ***Discrete & Combinatorial Mathematics*** **(5th Edition) by Ralph P. Grimaldi**

Public-Key Cryptosystem - RSA

RSA: developed in the 1970s (and patented in 1983), by
Ronald **R**ivest, Adi **S**hamir, and Leonard **A**dleman

Ex 16.18: Given p, q : larger primes (> 100 digits)
let $n = pq$, $r = (p - 1)(q - 1) = \phi(n)$
choose an invertible element (unit) e in Z_r (= $Z_{\phi(n)}$, is isomorphic to U_n)
(choose e such that $\gcd(e, r) = 1$)
Encryption $E : \mathbb{Z}_n \to \mathbb{Z}_n : E(M) = M^e \bmod n = C$ (Ex 14.16)
Decryption $D : \mathbb{Z}_n \to \mathbb{Z}_n = ?$

Sol.
Let $d = e^{-1}$ in Z_r (use Euclidean algorithm (as in Ex 14.13))
Claim: $D(C) = C^d \bmod n = M$

Public-Key Cryptosystem - RSA

Sol. Let $d = e^{-1}$ in Z_r (use Euclidean algorithm (as in Ex 14.13))

<u>**Claim:**</u> $D(C) = C^d \bmod n = M$

Proof.

Since $d = e^{-1}$ in $Z_r \Rightarrow ed \bmod \phi(n) = 1$

$\Rightarrow ed = k\phi(n) + 1$ for some $k \in \mathbb{Z}$

Since only $p + q - 1$ possibilities for failure, say M is a unit in Z_n

$\because (U_n, \cdot)$ forms an abelian group of order $\phi(n)$ (by Ex 16.4)

$\therefore M^{\phi(n)} = 1$ (by §16.3 ex. 8)

$\Rightarrow C^d = M^{ed} \pmod{n}$, and $M^{ed} = M^{k\phi(n)+1} = (M^{\phi(n)})^k M^1 \equiv M \pmod{n}$

i.e. $M^{ed} \bmod n = M$ (Euler's Thm. as §16.3 ex. 13)

Public-Key Cryptosystem - RSA

Ex 16.18: $p = 61$, $q = 127$, $n = pq = 7747$, $r = (p-1)(q-1) = \phi(n) = 7560$

choose an invertible element $e = 17$ in Z_r ($= Z_{\phi(n)}$)

The plaintext = "INVEST IN BONDS"

1. Encryption :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

I N V E S T I N B O N D S X

⇒ 08 13 21 04 18 19 08 13 01 14 13 03 18 23

$0813^{17} \bmod 7747 = 2169$

$2104^{17} \bmod 7747 = 0628$ $1819^{17} \bmod 7747 = 5540$

$0813^{17} \bmod 7747 = 2169$ $0114^{17} \bmod 7747 = 6560$

$1303^{17} \bmod 7747 = 6401$ $1823^{17} \bmod 7747 = 4829$

⇒ Ciphertext = 2169 0628 5540 2169 6560 6401 4829

Public-Key Cryptosystem - RSA

<u>Ex 16.18</u>: $p = 61$, $q = 127$, $n = pq = 7747$, $r = (p-1)(q-1) = \phi(n) = 7560$

choose an invertible element $e = 17$ in Z_r $(= Z_{\phi(n)})$

The plaintext = "INVEST IN BONDS"

2. Decryption :

let $d = e^{-1}$ in $\mathbb{Z}_{7560} = 3113$

Ciphertext = 2169 0628 5540 2169 6560 6401 4829

$2169^{3113} \bmod 7747 = 0813$ $\quad$ $0628^{3113} \bmod 7747 = 2104$

: $\quad$:

⇒0813 2104 1819 0813 0114 1303 1823

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

08 13 21 04 18 19 08 13 01 14 13 03 18 23

⇒ I N V E S T I N B O N D S X

Public-Key Cryptosystem - RSA

Remark: 1. Public: (n, e), secret: (p, q, r, d)

2. Find $r \Leftrightarrow$ find p, q

3. Find p, q, prime factors of n is hard, and this is what makes this system so much secure than the other.

4. More digits of p, $q \Rightarrow$ more secure.

Sol. (2.)

($\Leftarrow$) trivial

($\Rightarrow$) $p + q = pq - (p - 1)(q - 1) + 1 = n - \phi(n) + 1 = n - r + 1$

$$p - q = \sqrt{(p-q)^2} = \sqrt{(p-q)^2 + 4pq - 4pq} = \sqrt{(p+q)^2 - 4pq}$$

$$= \sqrt{(p+q)^2 - 4n} = \sqrt{(n-r+1)^2 - 4n}.$$

$$p = (1/2)[(n - r + 1) + \sqrt{(n-r+1)^2 - 4n}\ ]$$

$$q = (1/2)[(n - r + 1) - \sqrt{(n-r+1)^2 - 4n}\ ].$$

Public-Key Cryptosystem - RSA

Key Generation:

1. Select p, q (p and q both are prime)
2. Calculate $n = pq$
3. Calculate , $r = \phi(n) = (p - 1)(q - 1)$
4. Select integer e such that $\gcd(e, r) = 1$
5. Calculate $d = e^{-1}$ in Z_r
6. Public $\{e, n\}$
7. Keep key $\{d\}$

Public-Key Cryptosystem - RSA

Encryption:

Input: Plaintext $M < n$

Output: Ciphertext $C = M^e \bmod n$

Decryption:

Input: Ciphertext C

Output: Plaintext $M = C^d \bmod n$

RSA Signature Algorithm

Sign:

Input: Plaintext $M < n$

Output: Signature $S = M^d \bmod n$

Verify:

Input: Signature S

Output: Verification $M = S^e \bmod n$

RSA Encryption + Signature Algorithm

Sign: $S = D_A(M) = M^{d_A} \bmod n_A$

Encryption: $C = E_B(S) = S^{e_B} \bmod n_B$

Decryption: $D_B(C) = C^{d_B} \bmod n_B = S'$

Verify: $E_A(S') = S'^{e_A} \bmod n_A = M'$

How to select the parameters in RSA

How to select *n*:

1. **p and q must be Strong Primes.**
2. **The difference between p and q must be large (more than a few bits).**
3. **$\gcd(p - 1, q - 1)$ must be small.**
4. **p and q should be so large that the decomposition factor N is computationally impossible**

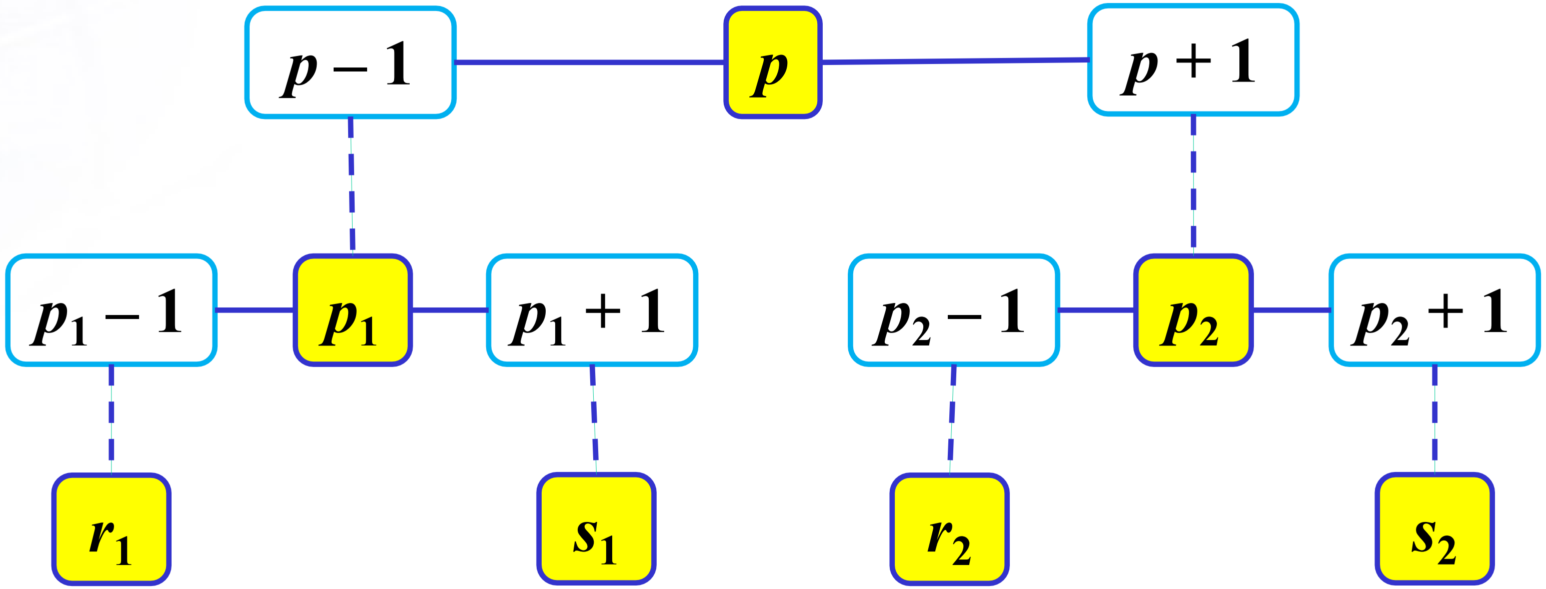
How to select *e*:

1. **Can't be too small.**
2. **[illegible]$(e) = r = \phi(n)$.**
3. **$e^{-1} = d > n^{1/4}$.**

How to select the parameters in RSA

Def: p is called a **Strong Prime** if

1. There are two big primes p_1, p_2 such that $p_1 | p - 1$ and $p_2 | p + 1$.
2. There are four big primes r_1, s_2, r_2, s_2 such that $r_1 | p_1 - 1$, $s_1 | p_1 + 1$, $r_2 | p_2 - 1$ and $s_2 | p_2 + 1$.



Miller–Rabin primality test

How to find a prime:

1. **Lemma:** For any odd integer $n = 2^r d + 1 > 0$ for some odd d and $r > 0$.
   For any integer a in the range $[2, n - 2]$:
   if $a^d \not\equiv 1 \pmod{n}$ and $a^{2^s d} \not\equiv n - 1 \pmod{n}$ for any $0 \le s \le r - 1$,
   then n is composite.

2. **Note:** Find k different a's and repeat the test, if n is not prime, the test fails with probability $(1/4)^k$.

3. **Theorem:** If $n < 2^{32}$, set $a = 2, 7, 61$; if $n < 2^{64}$, set $a = 2, 325, 9375, 28178, 450775, 9780504$. The probability would be 0.

Miller–Rabin primality test

Input: $n > 3$, an odd integer to be tested for primality;
k, a parameter that determines the accuracy of the test.
Output: *Composite* if n is composite, otherwise *probably prime*

Write $n - 1$ as $2^r d$ with d odd by factoring powers of 2 from $n - 1$.
repeat k times:
  pick a random integer a in the range $[2, n - 2]$
  $x = a^d \bmod n$
  if $x \neq 1$ and $x \neq n - 1$ then
    $t = 0$
    repeat
      $x = x^2 \bmod n$
      $t = t + 1$
    Until $x = n - 1$ or $t = r - 1$
    if $(t = r - 1$ and $x \neq n - 1)$ then return *Composite*
return *probably prime*

Public-Key Cryptosystem - RSA

- **Programming Homework #1**: (3/21) Implement the RSA.
- 1. 不要求p, q皆為Strong Prime.
- 2. The difference between p and q must > 1000; one of p, q must > 2^{32}.
- 3. gcd(p – 1, q – 1) must < 1000.
- 4. The test plaintext will > 20 words.