Computer Science and Information Engineering
National Chi Nan University

The Principle and Application of Secret Sharing

Dr. Justie Su-Tzu Juan

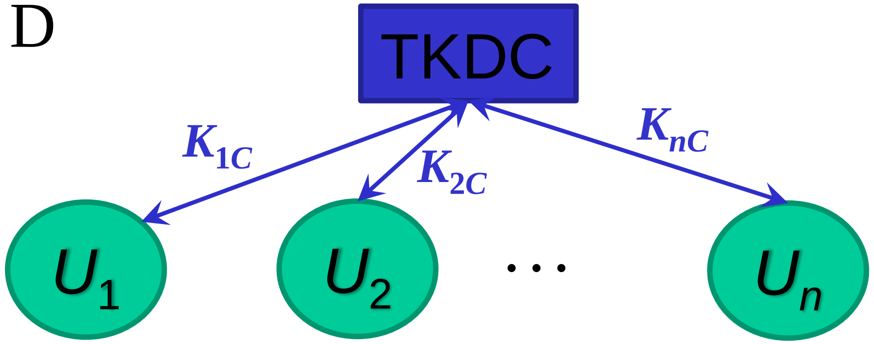
Lecture 1. Overview of Cryptography

§ 1.2 Contemporary Cryptography (2)

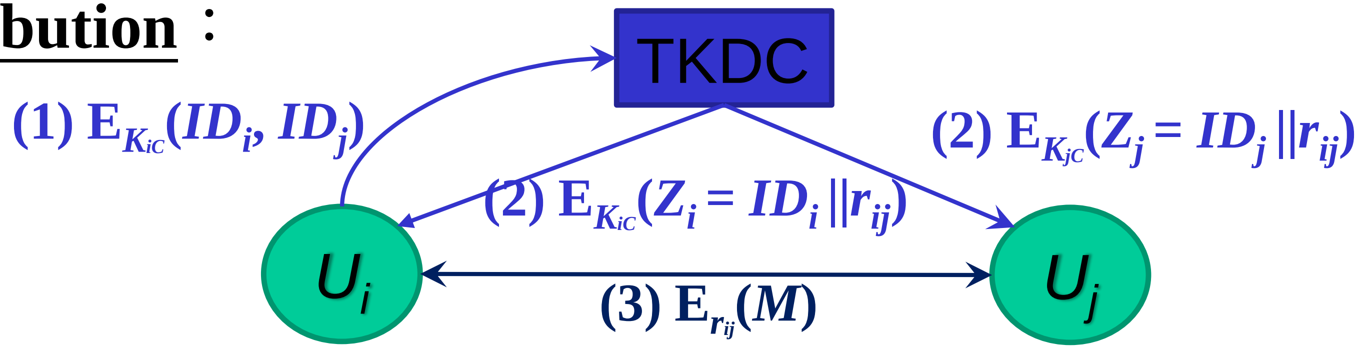
Slides for a Course Based on the Text
近代密碼學及其應用
by 賴溪松、韓亮、張真誠

Key Distribution System

- **Def: Key Distribution System (or Protocol), KDS** (金鑰分配協定)
  - **Conference-Key Distribution System, CKDS (會議金鑰分配系統)**
- **Trusted-Key Distribution Center, TKDC (可信賴的金鑰分配中心)**
  - **<u>Key generation</u>** : E, D



  - **<u>Key distribution</u>** ：

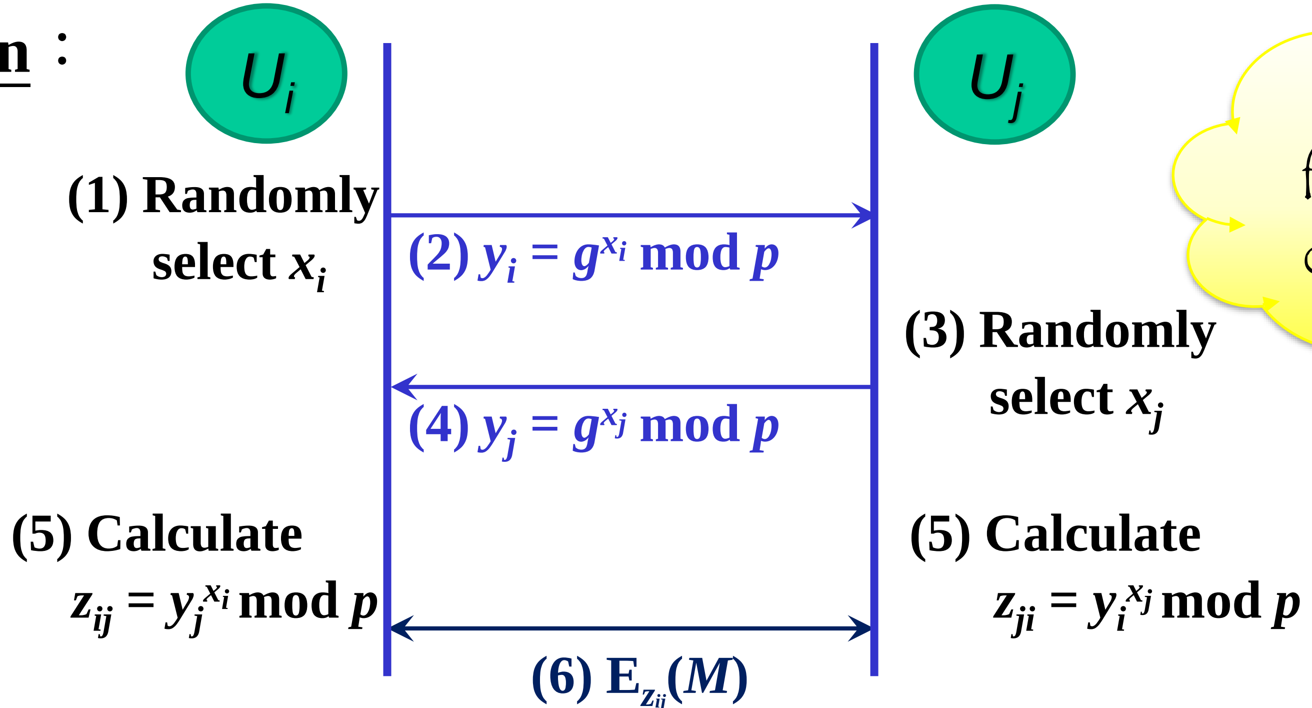


Public-Key Distribution System

- **Public-Key Distribution System, PKDS (公開金鑰分配系統)** for sending messages is a framework which allows one party to securely send a message to a second party without the need to exchange or distribute encryption keys.
  - **Ex**: Using exponentiation function.

Key generation : All participants known big prime p, and primitive root g.

Key distribution :

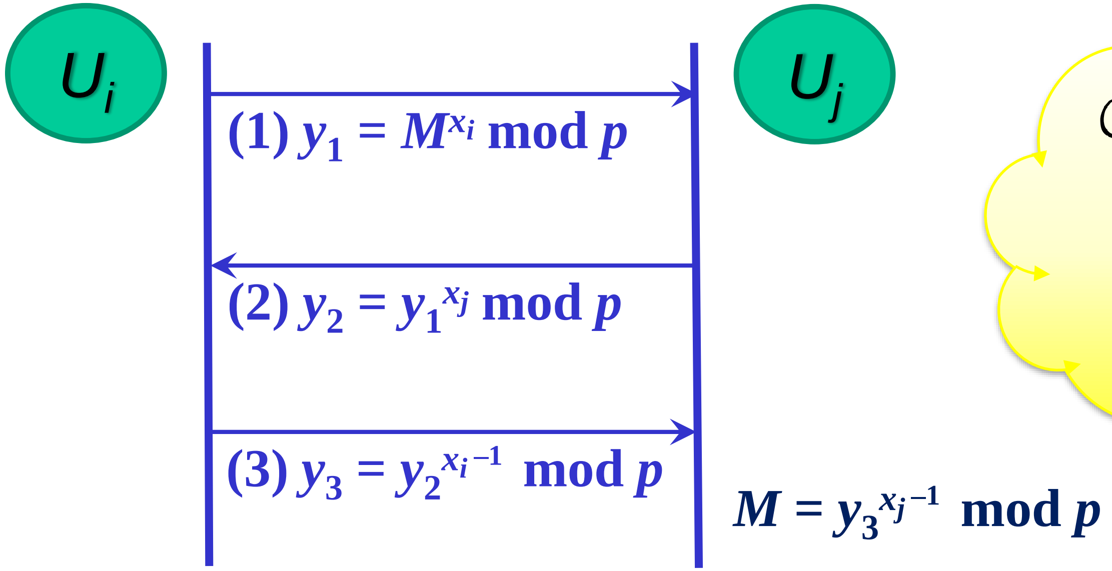


Three-Pass Protocol

- A **three-pass protocol** (三遍通訊協定)
  - **Ex**: Using exponentiation function.

    Key generation : All participants known big prime p, and primitive root g, and each participant U_i has their own secret key x_i and x_i^{-1} (that is, $x_i x_i^{-1} \equiv 1 \bmod (p - 1)$).

    Key distribution ：



OPC (XOR-operation) can not be used here.

ElGamal Encryption System

- The **ElGamal encr** **stem** (ElGamal 公開金鑰密 asymmetric key orithm for public-key cry based on the ey exchange, 1982.
  - **Ex**: Using e on.

    Key genera pants known big prime p, and primitive root g, and each participant U_i secret key x_i and public the **Public-key $y_i = g^{x_i}$ mod p**.

    Key distributio

Cannot use the same r! or Known-Plaintext Attack

One-way function with commutative

U_i U_j

(1) Randomly select r

Find $C_1 = g^r$ mod p,

$C_2 = My_j^r$ mod p

(2) $C = (C_1, C_2)$

(3) $C_1^{-x_j} = (g^r)^{-x_j} = (g^{x_j})^{-r} = y_j^{-r}$ mod p,

$C_2\,(C_1^{-x_j}) = (My_j^r)(y_j^{-r}) = M$ mod p

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

§ 2.1 Introduction to Number Theory

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*** **(5^{th} Edition) by Ralph P. Grimaldi**

Introduction to Number Theory

- **<u>Thm 2.1</u>:** Modular Arithmetic (模數運算)

  (1) $(x + y) \bmod n = [(x \bmod n) + (y \bmod n)] \bmod n$

  (2) $(x - y) \bmod n = [(x \bmod n) - (y \bmod n)] \bmod n$

  (3) $(x \times y) \bmod n = [(x \bmod n) \times (y \bmod n)] \bmod n$

  – **<u>Ex</u>**: $[75 \times (68 + 3)] \bmod 37 = [75 \times 71] \bmod 37 = 5325 \bmod 37 = 34$

    $[(75 \times 68) + (75 \times 3)] \bmod 37 = [(75 \times 68) \bmod 37 + (75 \times 3) \bmod 37] \bmod 37$

    $= [(75 \bmod 37 \times 68 \bmod 37) \bmod 37 + (75 \bmod 37 \times 3 \bmod 37) \bmod 37] \bmod 37$

    $= [(1 \times 31) \bmod 37 + (1 \times 3) \bmod 37] \bmod 37$

    $= (31 + 3) \bmod 37$

    $= 34$

Introduction to Number Theory

Def 14.7: $n \in Z^+$, $n > 1$, $\forall\, a, b \in Z$,

a is **congruent** to (同餘) b **modulo** $n \Leftrightarrow a \equiv b \pmod{n} \Leftrightarrow a \equiv_n b$

if $n|(a - b)$ ($\Leftrightarrow a = b + kn$ for some $k \in Z$)

Ex 14.12: $17 \equiv 2 \pmod{5}$; $-7 \equiv -49 \pmod{6}$; $11 \equiv -5 \pmod{8}$.

Thm 14.11: Congruence modulo n is an equivalence relation on Z.

(reflexive, symmetric, transitive)

Introduction to Number Theory

$[0] = \{\ldots, -2n, -n, 0, n, 2n, \ldots\} = \{0 + nx \mid x \in Z\}$

$[1] = \{\ldots, -2n + 1, -n + 1, 1, n + 1, 2n + 1, \ldots\} = \{1 + nx \mid x \in Z\}$

$[2] = \{\ldots, -2n + 2, -n + 2, 2, n + 2, 2n + 2, \ldots\} = \{2 + nx \mid x \in Z\}$

:

$[n - 1] = \{\ldots, -n - 1, -1, n - 1, 2n - 1, 3n - 1, \ldots\} = \{(n - 1) + nx \mid x \in Z\}$

Def: $Z_n \equiv \{[0], [1], \ldots, [n - 1]\} = \{0, 1, 2, \ldots, n - 1\}$

$[a] + [b] = [a + b]$, $[a] \cdot [b] = [a \cdot b]$

Def: Simplify, say $[a]$ as a.

Introduction to Number Theory

Def 14.1: $(R, \oplus, \odot)$ is a ring, where

R: a nonempty set

$\oplus: R \times R \to R$, $\odot: R \times R \to R$: two closed binary operations

and $\forall\, a, b, c \in R$ satisfied:

a) $a \oplus b = b \oplus a$ — Commutative Law of $\oplus$

b) $a \oplus (b \oplus c) = (a \oplus b) \oplus c$ — Associative Law of $\oplus$

c) $\exists\, z \in R$ s.t. $a \oplus z = z \oplus a = a\ \forall\, a \in R$ — Existence of an identity for $\oplus$

d) $\forall\, a \in R, \exists\, b \in R$ s.t. $a \oplus b = b \oplus a = z$ — Existence of inverses under $\oplus$

e) $a \odot (b \odot c) = (a \odot b) \odot c$ — Associative Law of $\odot$

f) $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$ — Distributive Laws of $\odot$ over $\oplus$

$(b \oplus c) \odot a = (b \odot a) \oplus (c \odot a)$

Introduction to Number Theory

Def 14.2: Let $(R, +, \cdot)$ be a ring:

a) If $ab = ba \ \forall\ a, b \in R$, then R is called a **commutative ring**.

b) If $\forall\ a, b \in R$, $ab = z \Rightarrow a = z$ or $b = z$, then R is said to have no **proper divisors of zero**.

c) If $\exists\ u \in R$ s.t. $u \neq z$ and $au = ua = a \ \forall\ a \in R$, then call u a **unity**, or **multiplicative identity** of R. Here R is called a **ring with unity**.

Ex: In $Z_5 = \{0, 1, 2, 3, 4\}$, define + and · as Table (i), (ii)

(i)

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

(ii)

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Sol.
Step 1: closed
Step 2: (a): (i) is symmetric.
(b), (e): 125 equalities must test.
(c): additive identity = 0
(d): additive inverse: $-0 = 0, -1 = 4, -2 = 3, -3 = 2, -4 = 1$
Step 3: (ii) is symmetric
Step 4: (f): 125 equalities must test.
Step 5: unity = 1

Introduction to Number Theory

Def 14.3: R be a ring with unity u. If for $a \in R$, $\exists\, b \in R$ s.t. $ab = ba = u$, then

① b is called a multiplicative inverse of a, and

② a is called a unit of R.

Note: The multiplicative inverse are unique, say a^{-1} .

Def: Let R be a commutative ring with unity, Then

a) R is called an integral domain if R has no proper divisors of zero.

b) R is called a field if every nonzero element of R is a unit.

Ex: In $Z_5 = \{0, 1, 2, 3, 4\}$, $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$; 1, 2, 3, 4 are units of Z_5.

Z_5 is an integral domain and field.

Introduction to Number Theory

Thm 14.12: $\forall\, n \in \mathbb{Z}^+$, $n > 1$, $(\mathbb{Z}_n, +, \cdot)$ is a commutative ring with unity 1 and additive identity 0.

Thm 14.13: $\mathbb{Z}_n$ is a field. $\Leftrightarrow$ n is a prime.

Thm 14.14: In $\mathbb{Z}_n$, $[a]$ is a unit. $\Leftrightarrow$ $\gcd(n, a) = 1$.

Ex: In $\mathbb{Z}_{10}$, who are units?

Sol. The units are {1, 3, 7, 9}

Ex 14.13: Find $[25]^{-1}$ in Z_{72}.

Sol.

$\because$ gcd(25, 72) = 1 $\Rightarrow$ 72 = 2(25) + 22,

25 = 1(22) + 3,

22 = 7(3) + 1.

$\Rightarrow$ 1 = 22 – 7(3) = 22 – 7(25 – 22) = –7(25)+ 8(22)

= – 7(25) + 8[72 – 2(25)] = 8(72) – 23(25)

$\because$ 1 = 8(72) – 23(25)

$\Rightarrow 1 \equiv (-23)(25) \pmod{72}$

$\Rightarrow 1 \equiv (72 - 23)(25) \pmod{72}$

so [1] = [49][25] and $[25]^{-1}$ = [49] in Z_{72}

Thm 2.2: Euler's totient function (歐拉函數)

For $n \in Z^+$, $n \geq 2$, Let $\phi(n) = |\{m \in Z^+ \mid \gcd(m, n) = 1, 1 \leq m < n\}|$

$$\phi(n) = n \prod_{p|n,\ p \text{ is a prime}} (1 - (1/p))$$

$$(\phi(n) = \prod_{i = 1, t} p_i^{e_i - 1}(p_i - 1), \text{ where } n = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}.)$$

Ex: Let $n = 36 = 2^2 3^2$, find $\phi(n)$.

Sol. $\phi(36) = 2^{(2-1)} \cdot (2 - 1) \cdot 3^{(2-1)} \cdot (3 - 1) = 2 \cdot 1 \cdot 3 \cdot 2 = 12.$

Introduction to Number Theory

Def 16.1:

- **G: a nonempty set; $\circ$: a binary operation of G**
  then $(G, \circ)$ is called a group ≡
  ① $\forall\, a, b \in G, a \circ b \in G$ (Closure of G under $\circ$)
  ② $\forall\, a, b, c \in G, a \circ (b \circ c) = (a \circ b) \circ c$ (The Associative Property)
  ③ $\exists\, e \in G$, s.t. $a \circ e = e \circ a = a, \forall\, a \in G$ (The Existence of an Identity)
  ④ $\forall\, a \in G, \exists\, b \in G$ s.t. $a \circ b = b \circ a = e$ (Existence of Inverses)
- **If ⑤ $\forall\, a, b \in G, a \circ b = b \circ a$ hold, then**
  G is called a commutative (or abelian) group.

Introduction to Number Theory

Note: ① If $(R, +, \cdot)$ is a ring $\Rightarrow$ $(R, +)$ is an abelian group.

② If $(F, +, \cdot)$ is a field

$\Rightarrow$ $(F, +)$ is an abelian group.

$(F^*, \cdot)$ is an abelian group, where $F^* = F - \{0\}$,

0: the zero element of $(F, +, \cdot)$.

$\forall\, a, b, c \in F,\ a \cdot (b + c) = a \cdot b + a \cdot c$

Ex 16.2: ① $\forall\, n \in \mathbb{Z}^+$, $n > 1$, $(\mathbb{Z}_n, +)$ is an abelian group.

② If p is a prime, $(\mathbb{Z}_p^*, \cdot)$ is an abelian group. ($\mathbb{Z}_p^* = \mathbb{Z}_p - \{[0]\}$)

Introduction to Number Theory

Def 16.2: • $\forall$ group G, the number of elements in $G \equiv$ **order** of G, denoted by $|G|$.

Ex 16.3: $\forall\, n \in \mathbb{Z}^+$, $|(\mathbb{Z}_n, +)| = n$, while $|(\mathbb{Z}_p^*, \cdot)| = p - 1$ $\forall$ prime p.

Note: ① $\forall\, n \in \mathbb{Z}^+$, $n > 1$, if $U_n = \{a \in (\mathbb{Z}_n, +, \cdot) \mid a \text{ is a unit}\}$

$$= \{a \in \mathbb{Z}^+ \mid 1 \leq a \leq n - 1 \text{ and } \gcd(a, n) = 1\}$$

then $(U_n, \cdot)$ is an abelian group under the multiplication modulo n.

② $(U_n, \cdot)$ is called the group of unit for the ring $(\mathbb{Z}_n, +, \cdot)$

③ $|U_n| = \phi(n)$ $\left(\begin{array}{l} = |\{a \in \mathbb{Z}^+ \mid 1 \leq a \leq n - 1 \text{ and } \gcd(a, n) = 1\}| \\ = n \cdot \prod_{p|n} (1 - 1/p) \end{array}\right)$

Introduction to Number Theory

Ex 16.4: In $(\mathbb{Z}_9, +, \cdot)$, let $U_9 = \{a \in \mathbb{Z}_9 \mid a \text{ is a unit in } \mathbb{Z}_9\}$

$= \{a \in \mathbb{Z}_9 \mid a^{-1} \text{ exists}\} = \{1, 2, 4, 5, 7, 8\}$

$= \{a \in \mathbb{Z}^+ \mid 1 \le a \le 8 \text{ and } \gcd(a, 9) = 1\}$

$\Rightarrow |U_9| = \phi(9) = 9(1 - 1/3) = 6$

·	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

$\Rightarrow$ ① U_9 is closed under the multiplication modulo 9.

② 1 is the identity element.

③ each element has an inverse in U_9.

④ $\because$ $(\mathbb{Z}_9, +, \cdot)$ is a ring $\Rightarrow$ $(U_9, \cdot)$ is associative under $\cdot$

i.e. $\forall\, a, b, c \in U_9,\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$

$\Rightarrow$ $(U_9, \cdot)$ is an (abelian) group of order 6.

Def 16.4: $(G, \circ)$ and $(H, *)$ are groups, $f: G \to H$ is called a **(group) homomorphism** if $\forall\, a, b \in G$, $f(a \circ b) = f(a) * f(b)$

Def 16.5: If $f: (G, \circ) \to (H, *)$ is a homomorphism,
f is called an **isomorphism** if it is 1-1 and onto,
and G, H are said to be **isomorphic groups**.

Introduction to Number Theory

Def: If every element of G is a power of i, then we say that i generates G. Denoted by $G = \langle i \rangle$.

Def 16.6: A group G is called cyclic if $\exists\, x \in G$ s.t. $G = \langle x \rangle$,
i.e. $\forall\, a \in G$, $a = x^n$ for some $n \in \mathbb{Z}$.

Ex 16.13: (a) $H = (\mathbb{Z}_4, +)$ is cyclic. ($\because$ the operation is addition.)

Sol.

$1 \cdot [3] = [3]$, $2 \cdot [3] = [3] + [3] = [2]$ ($\therefore$ multiples instead of powers)

$3 \cdot [3] = [1]$, $4 \cdot [3] = [0] \Rightarrow H = \langle [3] \rangle \ (= \langle [1] \rangle)$

i.e. [1], [3] generate H.

Ex 16.13: (b) (U_9) = ({1, 2, 4, 5, 7, 8}, ·) in Ex16.4 is cyclic.

Sol.

$2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 7, 2^5 = 5, 2^6 = 1$ $\therefore U_9 = \langle 2\rangle$

$\because 5^1 = 5, 5^2 = 7, 5^3 = 8, 5^4 = 4, 5^5 = 2, 5^6 = 1$ $\therefore U_9 = \langle 5\rangle$

Ex: $T = (Z_5^*, \cdot)$ is cycle:

Sol. $2^1 = 2, 2^2 = 4, 2^3 = 3, 2^4 = 1.$

2 generate T.

Def: Given a group G, let $a \in G$, the set $S = \{a^k \mid k \in Z\}$ is called the subgroup generated by a and is designated by $\langle a\rangle$.

Introduction to Number Theory

Ex 16.14: Define f: $(U_9, \cdot) \to (\mathbb{Z}_6, +)$ $(= (\mathbb{Z}_{\phi(n)}, +))$ as follows:

$f(1) = [0], f(2) = [1], f(4) = [2], f(8) = f(2^3) = [3], f(5) = f(2^5) = [5], f(7) = f(2^4) = [4].$

i.e. $\forall\, a \in U_9 = \langle 2 \rangle$, say $a = 2^k$, for some $0 \le k \le 5$ then define $f(a) = f(2^k) = [k]$

f is isomorphism and $(U_9, \cdot)$ and $(\mathbb{Z}_6, +)$ are isomorphic.

Def 16.7: If G is a group and $a \in G$,

① $\mathcal{O}(a) \equiv |\langle a \rangle|$, the order of $\langle a \rangle$.

② If $|\langle a \rangle|$ is infinite, we say that a has infinite order.

Remark: ① If $|\langle a \rangle| = 1$, then $a = e$.

② If $|\langle a \rangle|$ is finite, and $a \ne e$, then $\langle a \rangle = \{a, a^2, \ldots, a^n\}$, where n be the smallest positive integer s.t. $a^n = e$.

③ $\mathcal{O}(a)$ can also be defined as the smallest positive integer n s.t. $a^n = e$

<u>Thm 16.6</u>: Let $a \in G$ with $o(a) = n$.

If $k \in \mathbb{Z}$ and $a^k = e$, then $n \mid k$.

Proof.

$\forall\, k \in \mathbb{Z}, \exists\, q \in \mathbb{Z}, r \in \mathbb{Z}^+$ where $0 \le r < n$ s.t. $k = qn + r$

$\therefore\ e = a^k = a^{qn+r} = (a^n)^q(a^r) = (e^q)(a^r) = a^r$

If $0 < r < n$, it contradict the definition of $o(a) = n$

$\therefore\ r = 0 \Rightarrow k = qn.$ i.e. $n \mid k$

<u>Thm 16.7</u>: Let G be a cyclic group.

(a) If $|G|$ is infinite, then G is isomorphic to $(\mathbb{Z}, +)$

(b) If $|G| = n$, where $n > 1$, then G is isomorphic to $(\mathbb{Z}_n, +)$

Introduction to Number Theory

Thm 16.9: **Lagrange's Theorem**

If G is a finite group of order n with H a subgroup of order m, then m divides n. ($m|n$)

Corollary 16.1: **If G is finite group and $a \in G$ then $o(a) \mid |G|$.**

Corollary 16.2: **Every group of prime order is cyclic.**

Thm 2.3: **Fermat's Little Theorem (費馬小定理)**

If p is a prime, $a^p \equiv a \pmod{p}$ for each $a \in Z$.

Ex: **In $(Z_5^*, \cdot)$, $2^5 \equiv 2 \pmod{5}$ (and $2^4 \equiv 1 \pmod{5}$).**

Introduction to Number Theory

Thm 2.4: Euler's (Generalization) Theorem (歐拉廣義定理)
Foe each $n \in Z^+$, $n > 1$, and each $a \in Z$, if $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Ex: In $(U_9, \cdot)$, $4 \in U_9$ ($4 \in Z$, and $\gcd(4, 9) = 1$), and $\phi(9) = 6$, then $4^{\phi(n)} = 4^6 \equiv 1 \pmod{9}$.

Method: Check p is **not** a prime: Find integer a with $\gcd(a, p) = 1$, if $a^{p-1} \bmod p \neq 1$, then p is not a prime.

Thm 17.13: A finite field F has order p^t, where p is a prime and $t \in Z^+$. Also called GF(p^t), Galois Field (有限場, 高斯有限場).

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*** **(5^{th} 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)

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

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

Public-Key Cryptosystem - RSA

- **Programming Homework #1**: (3/21) Implement the RSA.

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

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”

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: Varification $M = S^e \bmod n$

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 $s_2 | p_2 + 1$.