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

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

Goals of Cryptography

- **SECRECY** (秘密性) (or CONFIDENTIALITY, or PRIVACY)
  - Keep information secret
- **AUTHENTICATION** (鑑定性)
  - Receiver can verify who sender was
- **INTEGRITY** (完整性)
  - Detect modified messages
- **NON-REPUDIATION** (不可否認性)
  - Sender cannot later falsely deny sending a message. (Receiver cannot falsely deny receiving it.)

Cryptography Systems

Cryptography Systems (密碼系統)

Sender → Plaintext (M) → Encrypt (E) → Ciphertext (C) → Decrypt (D) → Plaintext (M) → Receiver

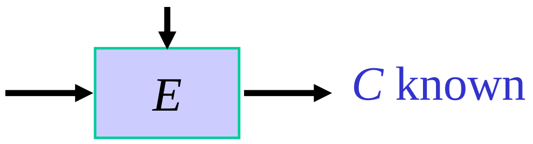
$C = E_{k1}(M)$ $\qquad$ $M = D_{k2}(C)$

$$\boxed{M = D_{k2}(E_{k1}(M))}$$

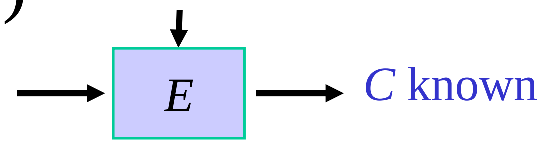
- When $k_1 = k_2$：Symmetric Key Cryptosystem (對稱金鑰密碼系統)、One-key Cryptosystem (單一金鑰密碼系統)、Private Key Cryptosystem (秘密金鑰密碼系統)、Conventional cryptosystem (傳統密碼系統)
- When $k_1 \neq k_2$：Asymmetric Cryptosystem (非對稱密碼系統)、Two Key Cryptosystem (雙金鑰密碼系統)、Public Key Distribution System (公開金鑰分配系統)

Types of Attacks

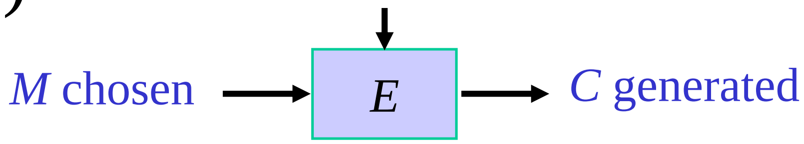
- Ciphertext-Only Attack (密文攻擊法)

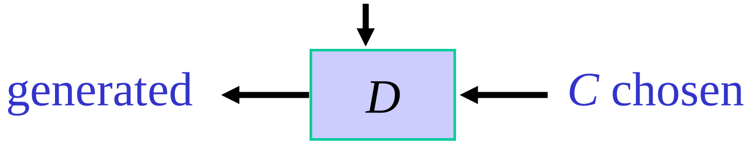


- Known-Plaintext Attack (已知明文攻擊法)



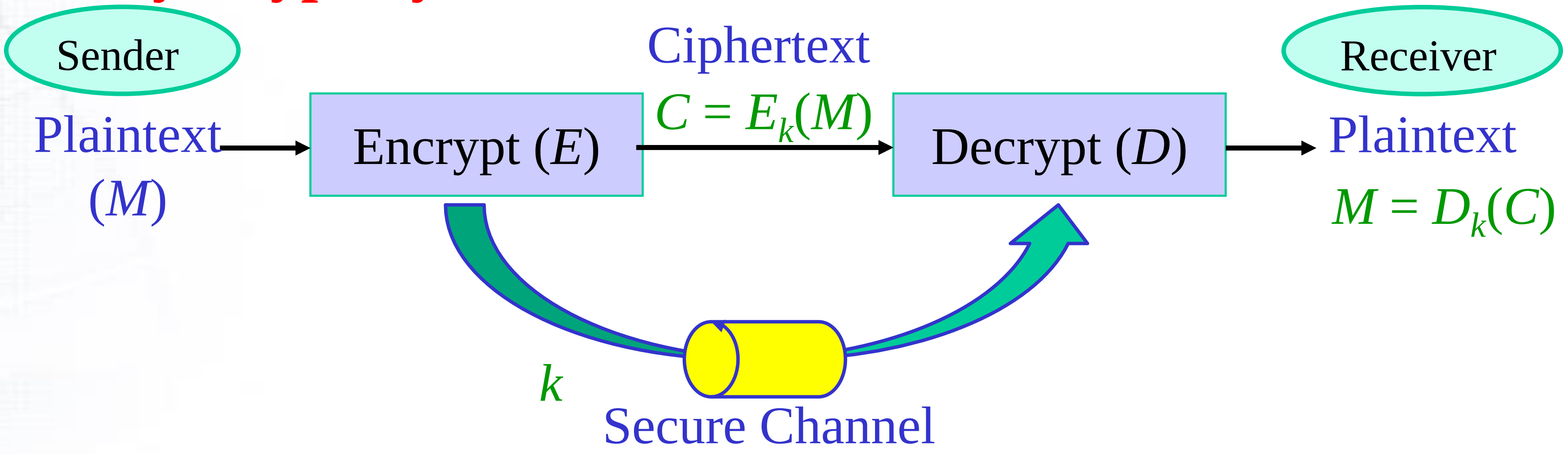
- Chosen-Text Attack (選擇文攻擊法)
  - Chosen-Plaintext Attack
  - Chosen-Ciphertext Attack





Symmetric Key Cryptosystem

Symmetric Key Cryptosystem:



- Advantage: Secrecy, Authentication, Integrity
- Disadvantage: 1. Need secure channel

  2. Too many keys required ($n(n – 1)/2$, for n participants.)

  3. No “Non-repudiation"

Asymmetric Key Cryptosystem

Asymmetric Cryptosystem (1976, Diffie and Hellman):

Sender

Plaintext (M) → Encrypt (E) → Ciphertext $C = E_{k1}(M)$ → Decrypt (D) → Plaintext $M = D_{k2}(C)$

Receiver

Public k_1

- Advantage: Secrecy, Integrity, Non-repudiation, Only one key for each participant.
  - If Commutative ($D_{k2}(E_{k1}(M)) = M = E_{k1}(D_{k2}(M))$): Non-repudiation (Digital Signature, 數位簽章)
- Disadvantage: Calculations are complex and time-consuming

  (RSA takes 1000 times longer than DES)

Security Types

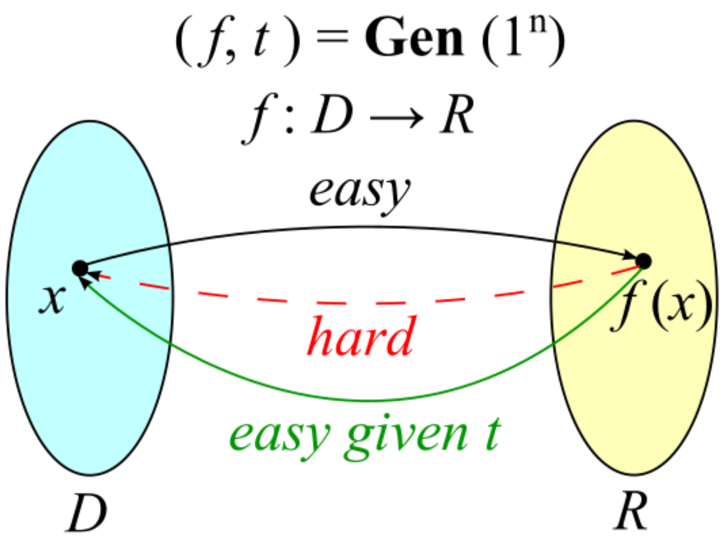
By Shannon, 1949.

- Theoretical Security or Perfect Security (理論安全):
  - – One-Time Pad
  - – Stream Cryptography (not really)
- Practical Security or Computational Security (實際安全):
  - Work Characteristic $W(n) > 10^{30}$
  - Historical Work Characteristic $W_h(n) > 10^{30}$
  - Ex: Each calculate need 10^{-6} second, then

	n^5	2^n	$n!$
$n = 10$	0.1 sec	0.0001 sec	3.6 sec
$n = 100$	10^4 sec $\approx$ 2.8 h	$\approx$1024 sec $\approx 10^{16}$ years	$\approx 10^{186}$ sec $\approx 10^{176}$ years
$n = 1000$	10^9 sec $\approx$ 10 years	$\approx 10^{286}$ years	$\approx 10^{2974}$ centuries

Mathematic Problems

- Def: One-way Function (單向函數)
  - It is easy to compute on every input, but hard to invert given the image of a random input.
  - 逃生門
- Def: One-way Trapdoor Function (單向暗門函數)
  - It is easy to compute in one direction, yet difficult to compute in the opposite direction (finding its inverse) without special information, called the "trapdoor".
  - 有鑰匙的逃生門



By IkamusumeFan - Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=45284265

Mathematic Problems

- **Problem 1: Discrete Logarithm Problem, DLP** (解離散對數問題)
  - **Def:** given a group G, a generator g and an element h of G, to find the discrete logarithm to the base g of h in the group G.
  - Discrete logarithm problem is not always hard. The hardness of finding discrete logarithms depends on the groups.
  - **Ex:** In group $(Z_5, \times)$, $g = 2$, then the discrete logarithm of 1 is 4 because $2^4 \equiv 1 \bmod 5$.
  - The fastest known algorithm for solving DLP is $L(p) = \exp\{(\ln p)^{1/3}(\ln(\ln p))^{2/3}\}$, ex: $L(10^{512}) \geq e^{38.92} \geq 8 \times 10^{16}$; $L(10^{1024}) \geq e^{52.19} \geq 4.6 \times 10^{22}$
- **Representative:** Diffie-Hellman Key Agreement System
  Elgamal Public-key Cryptography
  Digital Signature Algorithm (DSA)
- **Recent Usage:** Widely

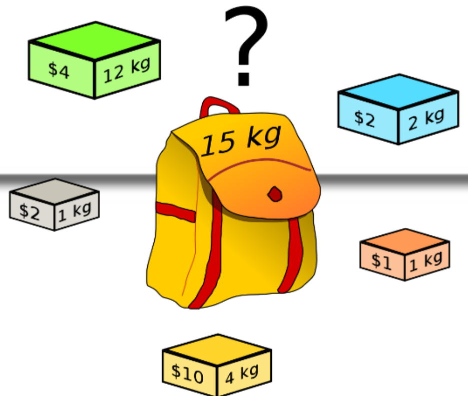
Mathematic Problems

- **Problem 2: Factorization Problem, FAC** (因數分解問題)
  - **Def:** Given n, find p and q for any two big prims p and q, such that $n = pq$.
  - **Ex:** 2851697 (=)
  - The fastest known algorithm for solving FAC is $T(p) = \exp\{C(\ln p)^{1/3}(\ln(\ln p))^{2/3}\}$, C is a constant.
  - DLP is a bit more difficult than FAC.

- **Representative:** RSA Public-key Cryptography

- **Recent Usage:** RSA is still the most widely used system

Mathematic Problems



- **Problem 3: Knapsack Problem** (迷袋問題、背包問題)
  - **Def:** Given a set of items, each with a weight and a value, determine the number of each item to include in a collection so that the total weight is less than or equal to a given limit and the total value is as large as possible.
  - Let $B = \{b_1, b_2, \ldots, b_n\}$, $V = \{v_1, v_2, \ldots, v_n\}$. Given an positive integer S, find $X = \{x_1, x_2, \ldots, x_n\}$ where $x_i \in \{0, 1\}$ for any $1 \le i \le n$, such that $\Sigma_{i=1,n} x_i b_i \le S$, and $\Sigma_{i=1,n} x_i v_i$ as large as possible.
  - **Ex:** $B = \{2, 5, 7, 16, 19, 25, 32, 38, 40, 47\}$, $S = 100$.

- **Representative:** Merkle-Hellman Public-key Cryptosystem

- **Recent Usage:** The Knapsack Problem has largely been cracked and is currently under-appreciated.

Mathematic Problems

- **Problem 4: Elliptic Curve Cryptosystem, ECC** (橢圓曲線密碼系統)
  - **Def:** An approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields.
  - **Def: Elliptic Curves over Z_p:** In $E_p(a, b)$, means $y^2 = x^3 + ax + b$ in Z_p (or say GF(p)) and $(4a^3 + 27b^2) \neq 0 \bmod p$. If $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$, define O is the identity, the invers of $P = -P = (x_P, -y_P)$, and $R = P + Q = (x_R, y_R)$ is determined by the following rules:

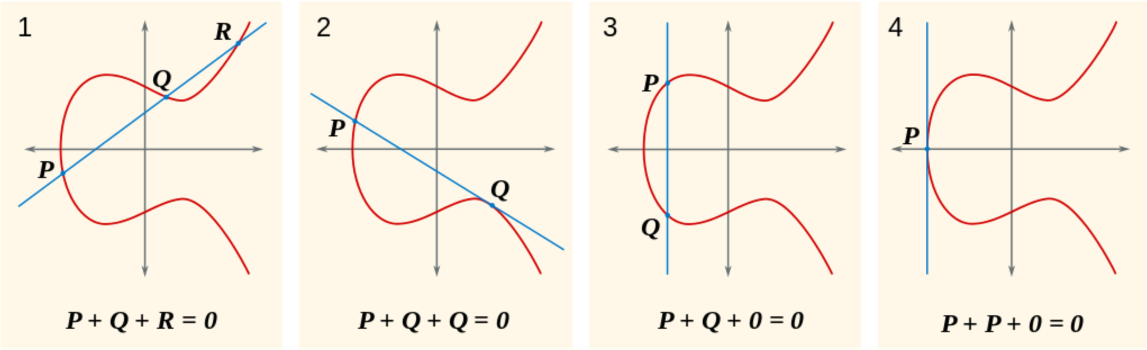
$$x_R \equiv (\lambda^2 - x_P - x_Q) \bmod p$$

$$y_R \equiv (\lambda(x_P - x_R) - y_P) \bmod p$$

where $\lambda \equiv (y_Q - y_P)/(x_Q - x_P) \bmod p$, if $P \neq Q$;

$(2x_P^2 + a)/2y_P \bmod p$, if $P = Q$.

Multiplication is defined as repeated addition.



By SuperManu - Own work based on Image:ECClines.png by en:User:Chas zzz brown, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=2970559

Mathematic Problems

- **Problem 4: Elliptic Curve Cryptosystem, ECC** (橢圓曲線密碼系統)
  - **Ex:** Let p = 211, G = (2, 2) in $E_p(0, -4)$: 240G = O; 121(2, 2) = (115, 48); 203(2,2) = (130, 203). Knowing kG and G, p, it is difficult to get k.
  - ECC allows smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security.

- **Representative:** Analog of Diffie-Hellman Key Exchange
  Elliptic Curve Encryption/Decryption
  IEEE P1363
  Many standards are being developed.

- **Recent Usage:** ECC is considered to have development potential in the future.

Exponentiation function

- **Def:** Let $(G, \cdot)$ is a finite group, and $g \in G$. The exponentiation function (指數函數) $E_x(g)$ is a function in G such that for any x in G, $E_x(g) = g^x \in G$. In $G = Z_p = \{0, 1, 2, \ldots, p - 1\}$, $E_g(x) = g^x \bmod p$. It has the following properties
  - 1. Periodically (週期性): $\langle g \rangle = \{g^0, g^1, g^2, \ldots\} \subseteq Z_p$, must periodically.
  - 2. For any minimum positive integer T such that $g^T = 0$, T is called the order (序) of g.
  - 3. $T \mid p - 1$ by Fermat's Theorem.
  - 4. If $g \in Z_p$ with order $T = p - 1$, g is called the primitive root (原根) of $(Z_p, \cdot)$. If $\gcd(a, p - 1) = 1$, g^a is also a primitive root.
  - 5. The number of the primitive root of $(Z_p, \cdot) = \phi(p - 1)$, Euler Totient Function.
  - 6. Commutative (交換律): $E_x(E_y(g)) = E_x(g^y) = g^{yx} = g^{xy} = E_y(g^x) = E_y(E_x(g))$
  - 7. Asymmetric (非對稱性): $E_x(-g) = (-g)^x = (-1)^x g^x = (-1)^x E_x(g)$

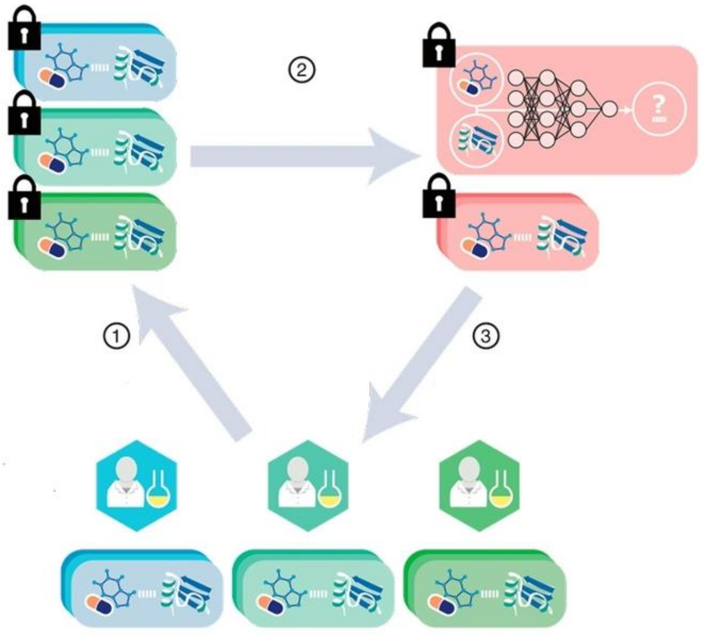
Exponentiation function

- 8. Inverse (乘法反元素): If T is the order of g, then $E_x(g^{-1}) = E_{T-x}(g)$ for any $0 \le x < T$.
- 9. Multiplicity (乘法性): $E_x(g_1)E_x(g_2)) = g_1{}^x g_2{}^x = E_x(g_1 g_2)$.
- 10. Reversibility (可逆性): If T is the order of g, and x^{-1} is the inverse of x in Z_T, that is $x\,x^{-1} \equiv 1 \bmod T$. Then $E_x(E_{x^{-1}}(g)) = E_{x^{-1}}(E_x(g)) = g^{xx^{-1}} = g^{kT+1} = (g^T)^k\, g \equiv g \bmod p$, because $x\,x^{-1} \equiv 1 \bmod T$, so $x\,x^{-1} = kT + 1$ for some integer k.
- 11. Square-multiplication (平方再乘法): Let $(x)_{10} = (b_{n-1}, b_{n-2}, \ldots, b_1, b_0)_2$ is large, then $g^x = (\ldots((1 \cdot g^{b^{n-1}})^2 \cdot g^{b^{n-2}})^2 \cdot g^{b^{n-3}} \ldots)^2 \cdot g^{b^0}$. Take square: $n - 1$, multiply: $\omega(x) - 1$, where $\omega(x) = |\{j \mid b_j = 1 \text{ for } 0 \le j \le n-1\}|$.
- 12. Security (安全性): Given g, y in G, find x such that $y \equiv g^x \bmod p$ is DLP.
- 13. By 11 and 12, exponentiation function is a one-way function with commutative. It is good for designing a Public-Key Distribution System, PKDS).

Cryptographic Protocol

- **Def:** Roughly speaking, a protocol (協定) refers to a multiparty algorithm in which two or more parts cooperate to accomplish some work through a well-defined series of actions.

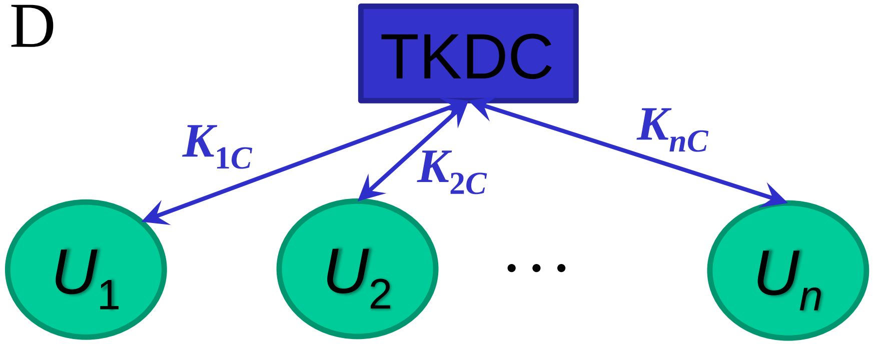
- **Cryptographic Protocol**: On public networks; for secret information exchange, or confirm information integrity.
- Include: cryptosystem, key distribution, digital signatures, authentication systems, secret sharing schemes.



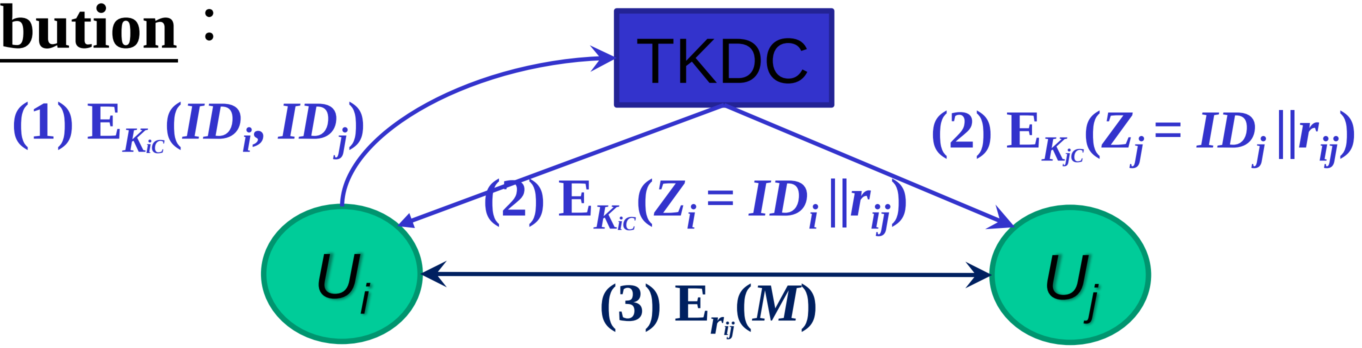
https://news.mit.edu/2018/cryptographic-protocol-collaboration-drug-discovery-1018

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)**
  - **Key generation** : E, D



  - **Key distribution**：



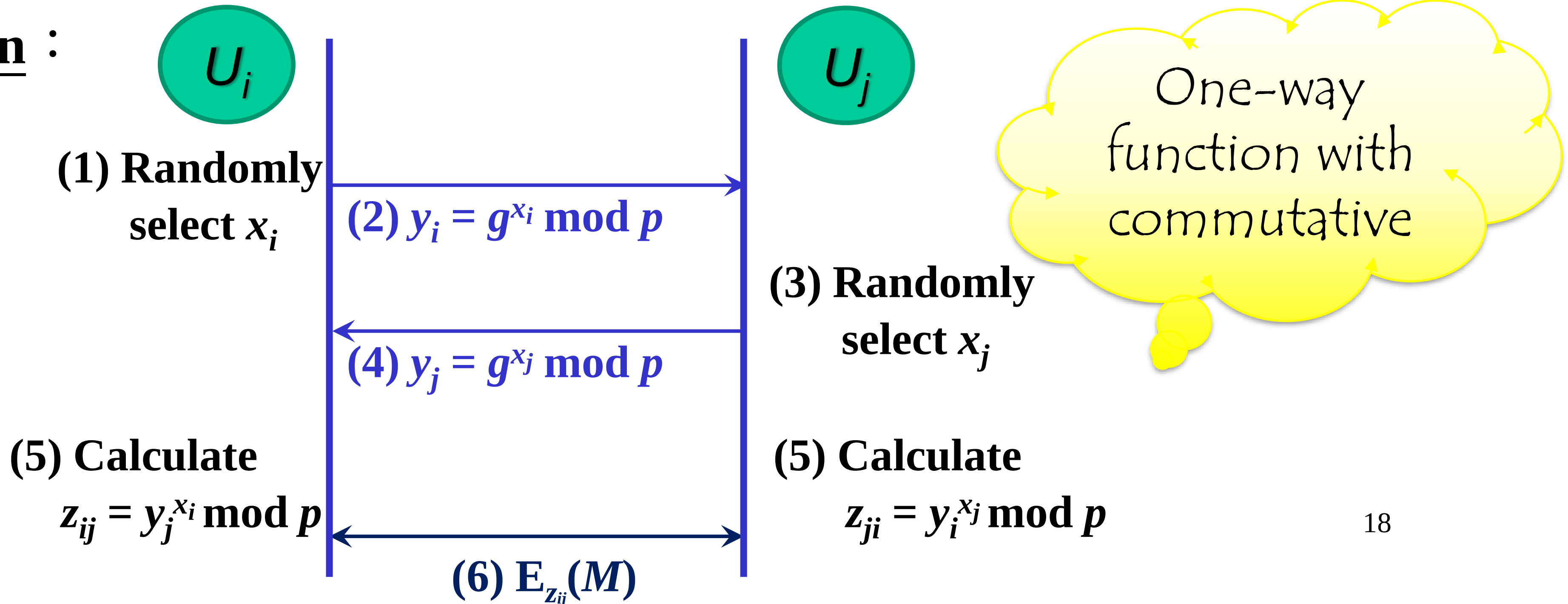
Known-Plaintext Attack

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 :

U_i $\qquad$ U_j

$U_i \rightarrow U_j$: (1) $y_1 = M^{x_i} \bmod p$

$U_i \leftarrow U_j$: (2) $y_2 = y_1^{x_j} \bmod p$

$U_i \rightarrow U_j$: (3) $y_3 = y_2^{x_i^{-1}} \bmod p$

$M = y_3^{x_j^{-1}} \bmod p$

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

ElGamal Encryption System

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

    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,
$C_2 = My_i^r$ mod p

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

(3) $C_1^{x_i} = (g^r)^{x_i} = (g^{x_i})^r = y_i^r$ mod p,
$C_2\,(C_1)^{-1} = (My_i^r)(y_i^r)^{-1} = M$ mod p