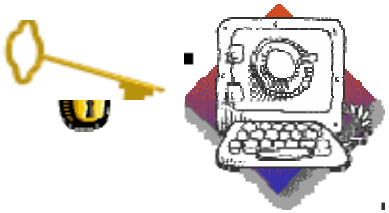


Introduction to Cryptography and Information Security

Sung-Ming Yen

Lcls, CSIE, NCU

目錄

- 網路安全與資訊安全之重要性
- 秘密金鑰加密器 (SKC)
- 公開金鑰加密器 (PKC) 與數位簽章
- 金鑰管理
- 系統安全性相關事項之探討
- A Cryptographic Game

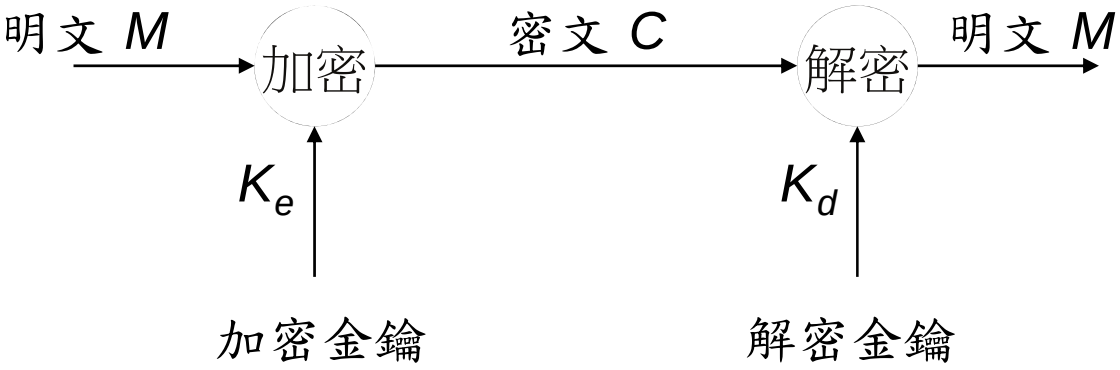
網路安全與資訊安全之重要性

- 重要性
  - 隨資訊與電腦網路工業發展而日益重要
  - 隨全面性商務資訊化及網路化(EDI)而日益重要
  - 因NII之推動而日益重要
  - 雖然近年來資訊與網路安全之技術與產品已絕大多數用於民生用品與商業途徑但仍有些國家將其列為出國管制產品(例如:美國)

- 基本認知
  - 資訊與網路系統的安全性與其它因素，諸如:效率性、可靠性等有絕對的不同。安全性分類基本上只有:安全與不安全兩種!
  - 系統設計方法:公開。 系統運作金鑰:保密
  - 資訊安全之科技極需本土化與自主化。唯有如此才能達到徹底的安全之保障。

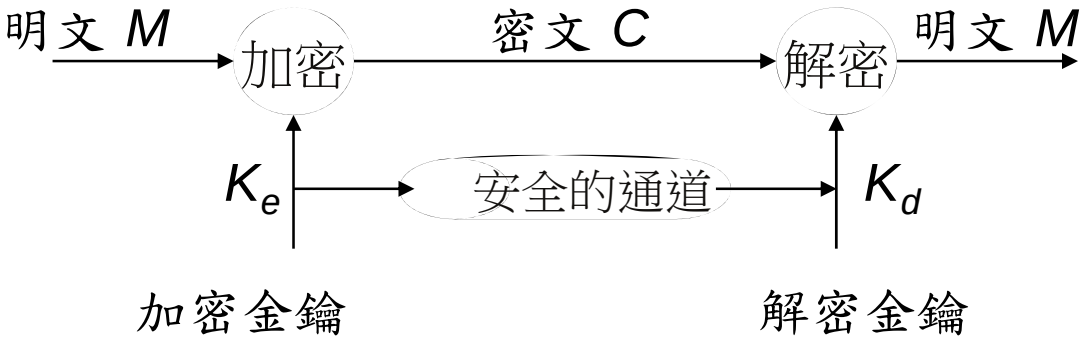
加解密基本模式

- 加密(encryption)與解密(decryption)之基本模式
  - 明文(plaintext); 密文(ciphertext)
  - 加密金鑰(encryption key); 解密金鑰(decryption key)

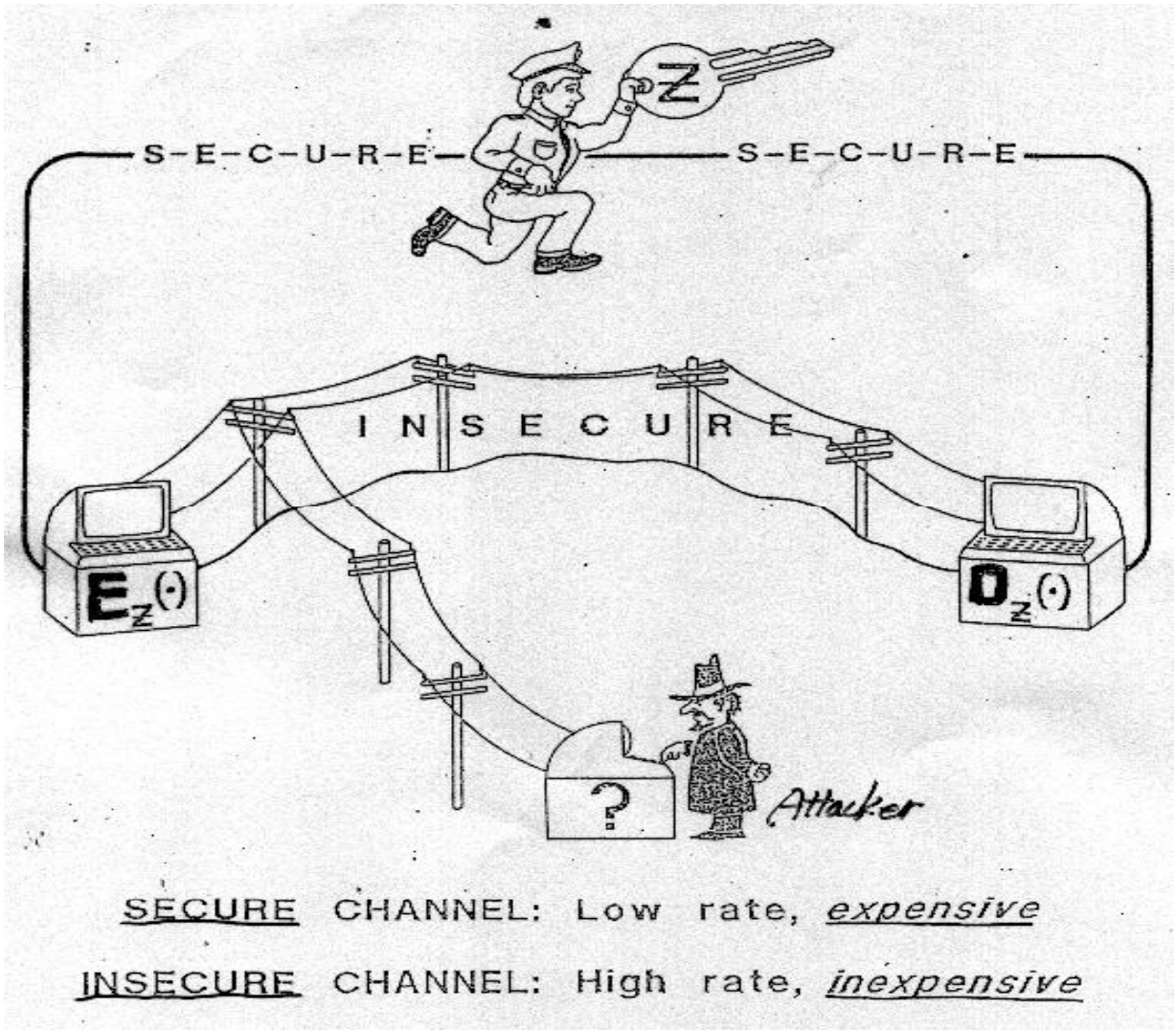


祕密金鑰加密器 (SKC)

- 秘密金鑰(secret-key)系統:
  - 對稱金鑰系統; 單金鑰系統
  - $K_e = K_d$
  - K_e及K_d: 皆需保密; K_e及K_d由雙方共同選擇或由一方選擇



Secure Channel?

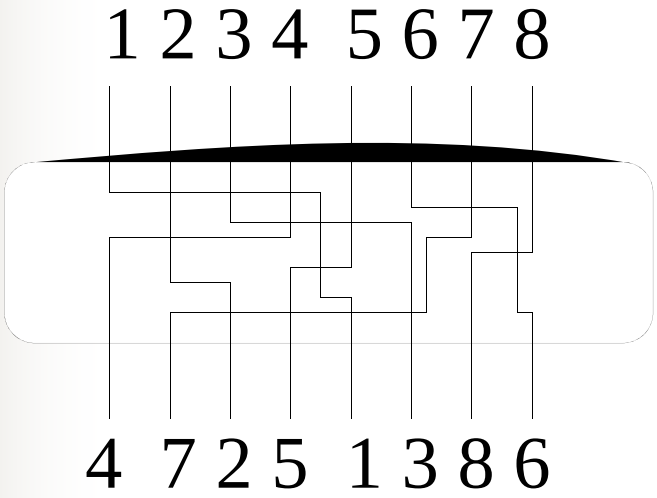


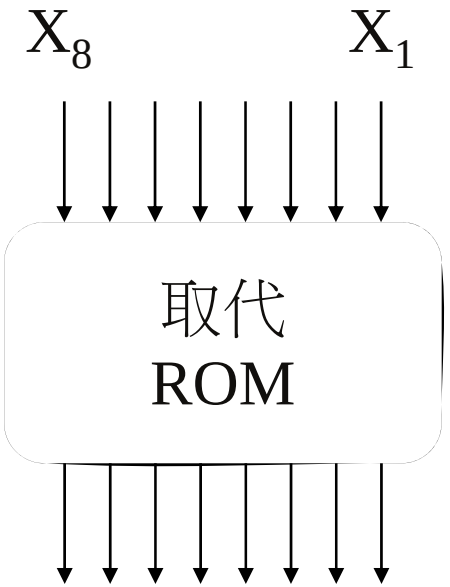
SECURE CHANNEL: Low rate, *expensive*

INSECURE CHANNEL: High rate, *inexpensive*

祕密金鑰加密器-- Basic Idea

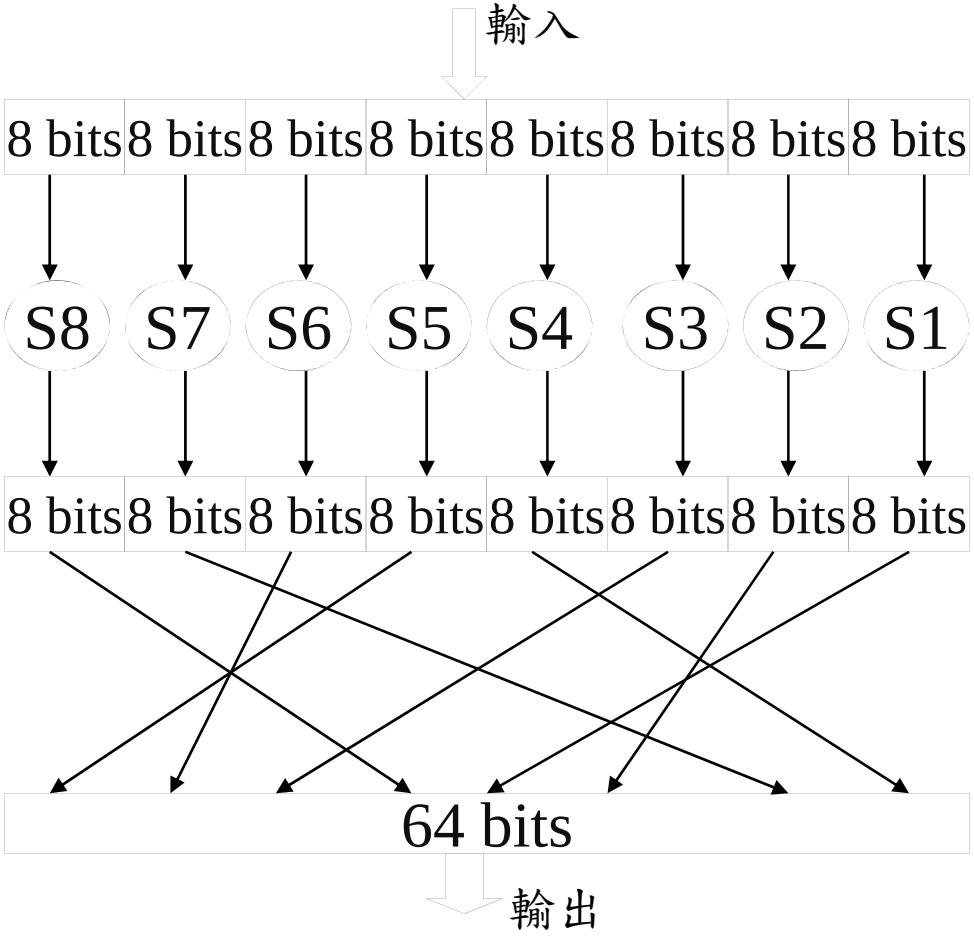
- 兩種基本加密功能
  - 重排法與取代法





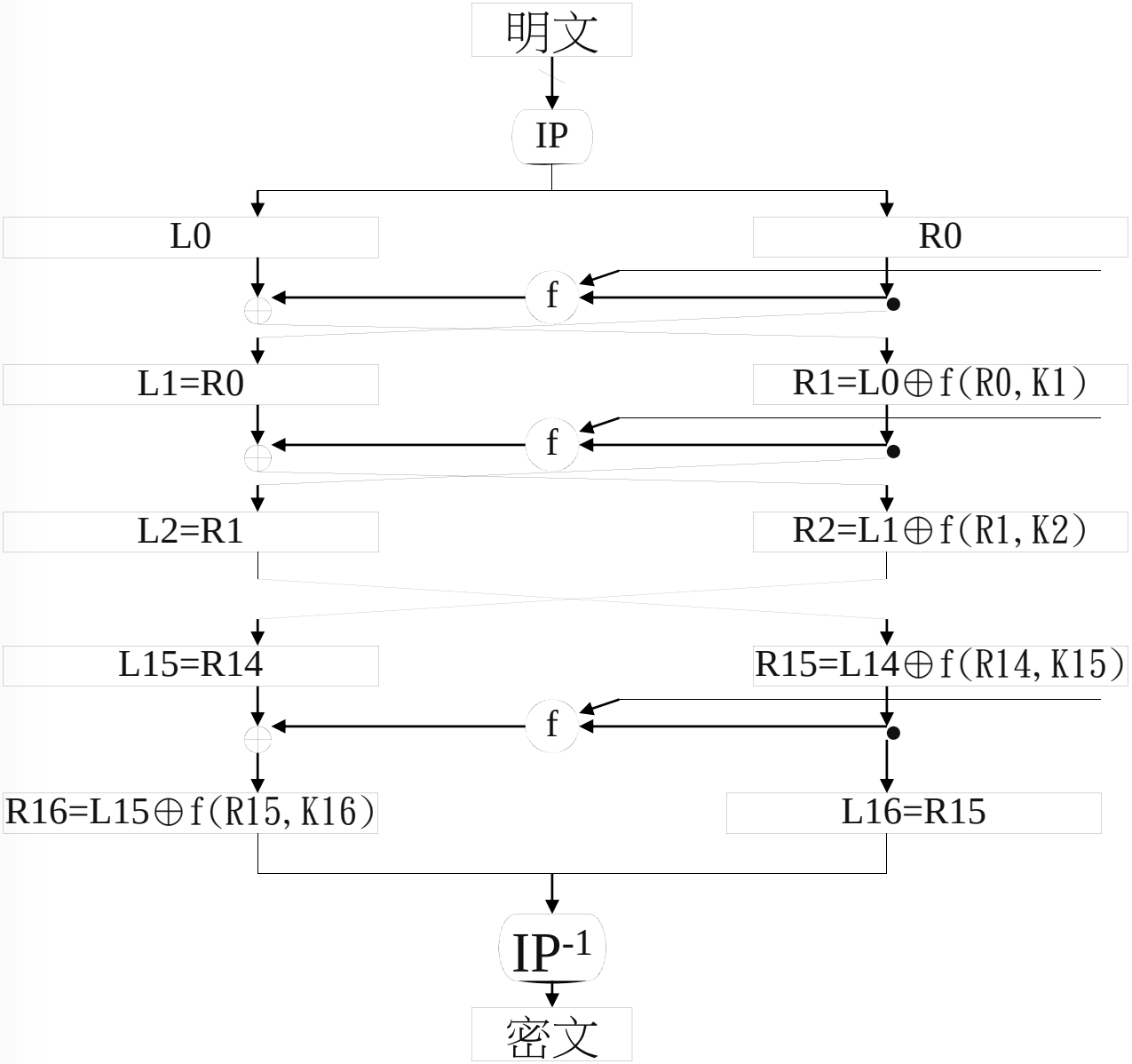
祕密金鑰加密器--Enhancement

- 實際加密系統觀念



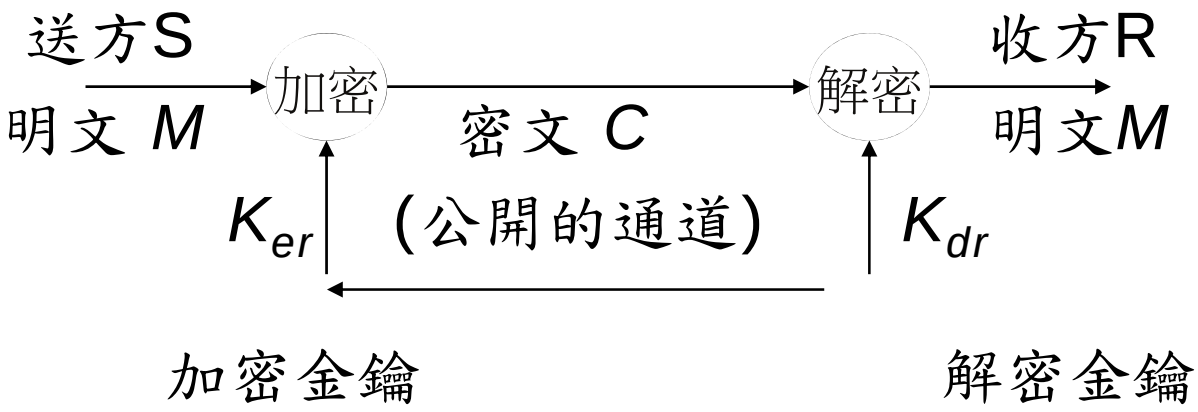
祕密金鑰加密器-- Example

- DES (Data Encryption Standard)資料加密標準
  - 1977年由IBM公司發展完成且被美國國家標準局公佈為資料加密標準
  - DES的區塊大小為64 bits，金鑰(key)長度為56 bits
  - 加解密速度非常快，以80486(33MHz)為例，其處理速度可高達每秒40600個區塊，相當於2.5Mbps


明文
IP
L0
R0
f
L1=R0
R1=L0⊕f(R0, K1)
f
L2=R1
R2=L1⊕f(R1, K2)
L15=R14
R15=L14⊕f(R14, K15)
f
R16=L15⊕f(R15, K16)
L16=R15
IP-1
密文

公開金鑰加密器 (PKC)

- 公開金鑰(public-key)系統
  - 非對稱金鑰系統; 雙金鑰系統
  - $K_{er} \neq K_{dr}$
  - K_{er}:須公開 ; K_{dr}需保密 ; K_{er}及K_{dr}由收方選擇



公開金鑰加密器 -- Basic Idea

- 計算困難問題
  - 質因數分解問題

    $21 = ? \times ?$

    $391 = ? \times ?$

    $4119223 = ? \times ?$

    $609660055686445307994220 3 = ? \times ?$
  - 離散對數問題

    $a = b^c \bmod d$: 給定a, b, d, 求解c

公開金鑰加密器 -- Example

- RSA公開金鑰密碼系統
  - 於1977年由R. Rivest, A. Shamir, 及L. Adleman三位於麻省理工學院所發展出來
  - 可用於資料加密及數位簽章

$$21 = 3 \times 7$$

$$391 = 17 \times 23$$

$$4119223 = 1933 \times 2131$$

$$609660055686445307994220 3 = 1331677695151 \times 4578135219253$$

RSA系統設計

收方選取兩個大質數1933和2131，算出兩個的乘積

$$n = p \times q = 1933 \times 2131 = 4119223$$

選取一數e當作加密金匙K_{er} (公開金鑰)

$$K_{er} : e = 11$$

計算e之乘法反元素d，作為解密金匙K_{dr} (私密金鑰)，使得 $e \times d = 1 \bmod 1932 \times 2130$

$$K_{dr} : d = 748211$$

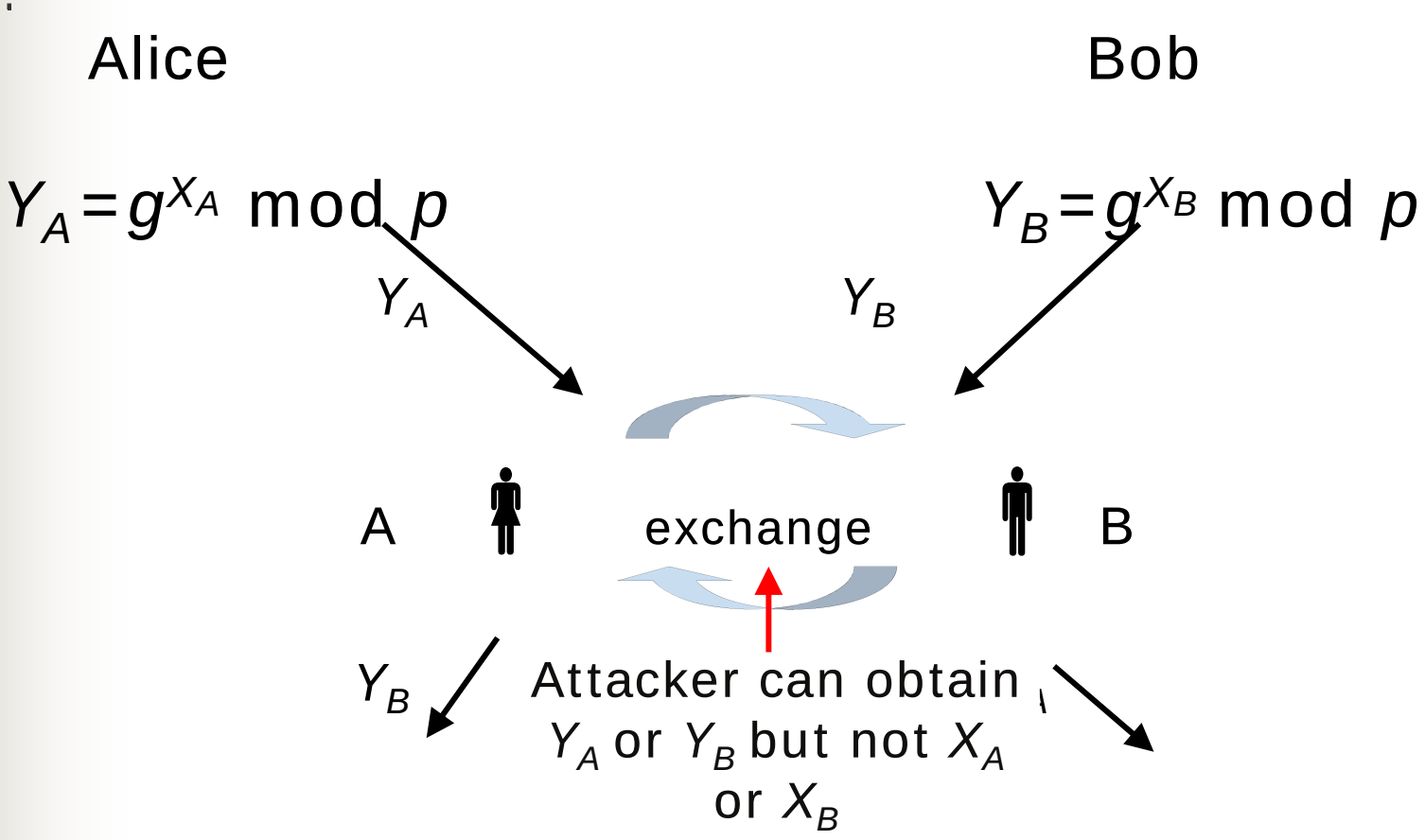
加密時將明文$M = 2245613$ 轉換成密文 C

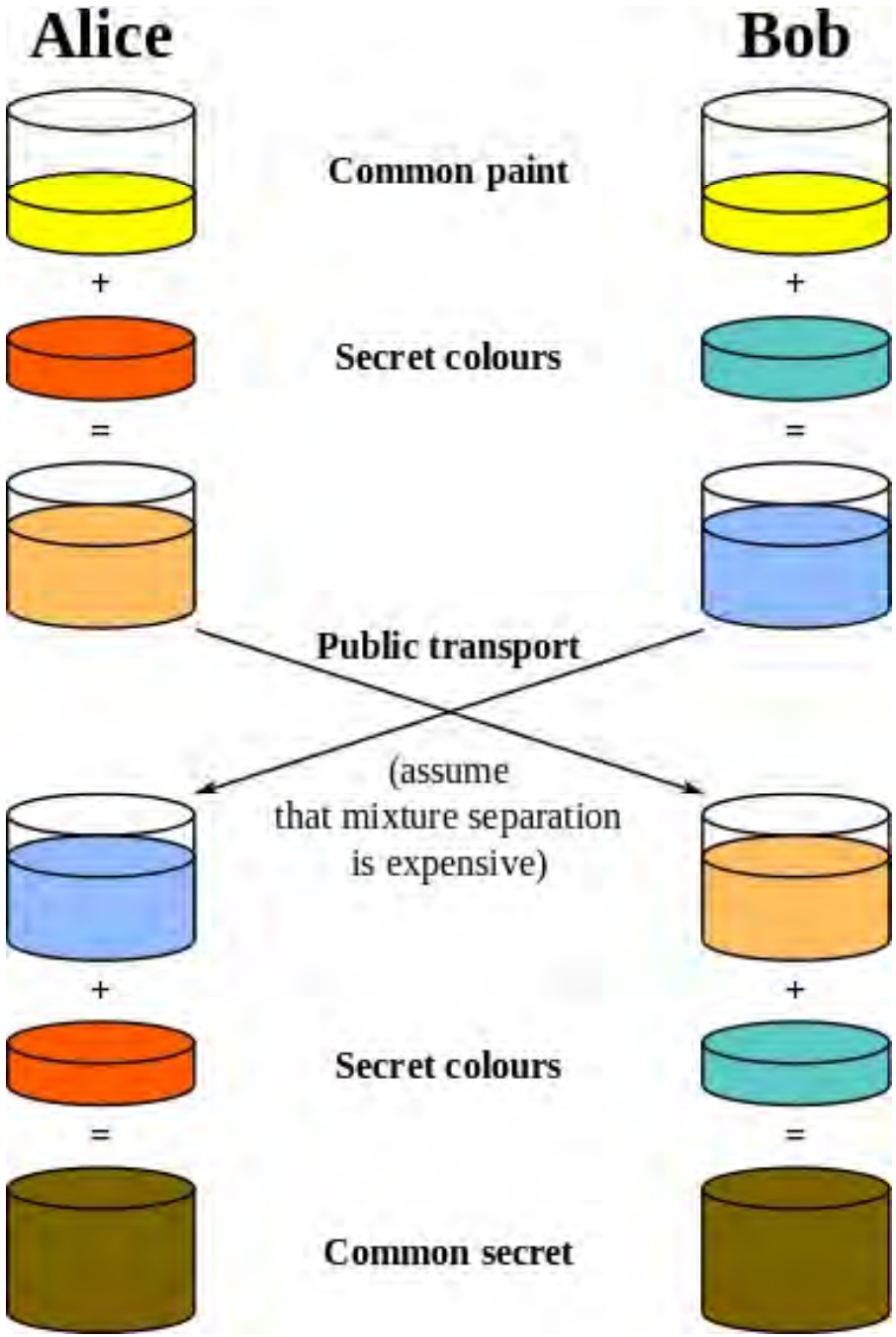
$$C = 2245613^{11} \bmod 4119223 = 771889$$

解密時將密文C轉換回明文

$$M = 771889^{748211} \bmod 4119223 = 2245613$$

Diffie-Hellman Public Key Exchange




Alice
Bob
Common paint
+
Secret colours
=
Public transport
(assume
that mixture separation
is expensive)
+
Secret colours
=
Common secret

公開金鑰加密器 -- Comparison

- 公開金鑰與秘密金鑰密碼系統比較
  - 秘密金鑰系統

    送方必須經由一個安全通道傳送金鑰給接收方解密，當雙方互不認識時，則問題相當嚴重
  - 公開金鑰系統

    (a)雙方不需要再傳送解密金鑰，故使用上較秘密金鑰系統方便許多

    (b)在軟體上，DES是RSA的100倍，在特製的晶片上更高達1000倍

- 混合式密碼系統 (Hybrid Cryptosystem)

  現行之方式一般採用公開金鑰系統來實現:

  (1)秘密金鑰交換; (2)數位簽章.

  採用秘密金鑰系統於大量資料加解密之運作

公開金鑰數位簽章

- 數位簽章
  - 在數位資訊處理的環境下，如何取得確切之證據以茲證明對某份數位文件之所有權以及簽署者對此文件之確實簽署效力，顯得格外重要與實用
  - 數位簽章之發明實現了以上之需求並且更提供了諸多手寫簽章所不具有之功能或特性
  - RSA數位簽章(簽署金鑰d為簽署者之私密金鑰)

    簽署時將明文$M=2245613$ 轉換成簽章 S

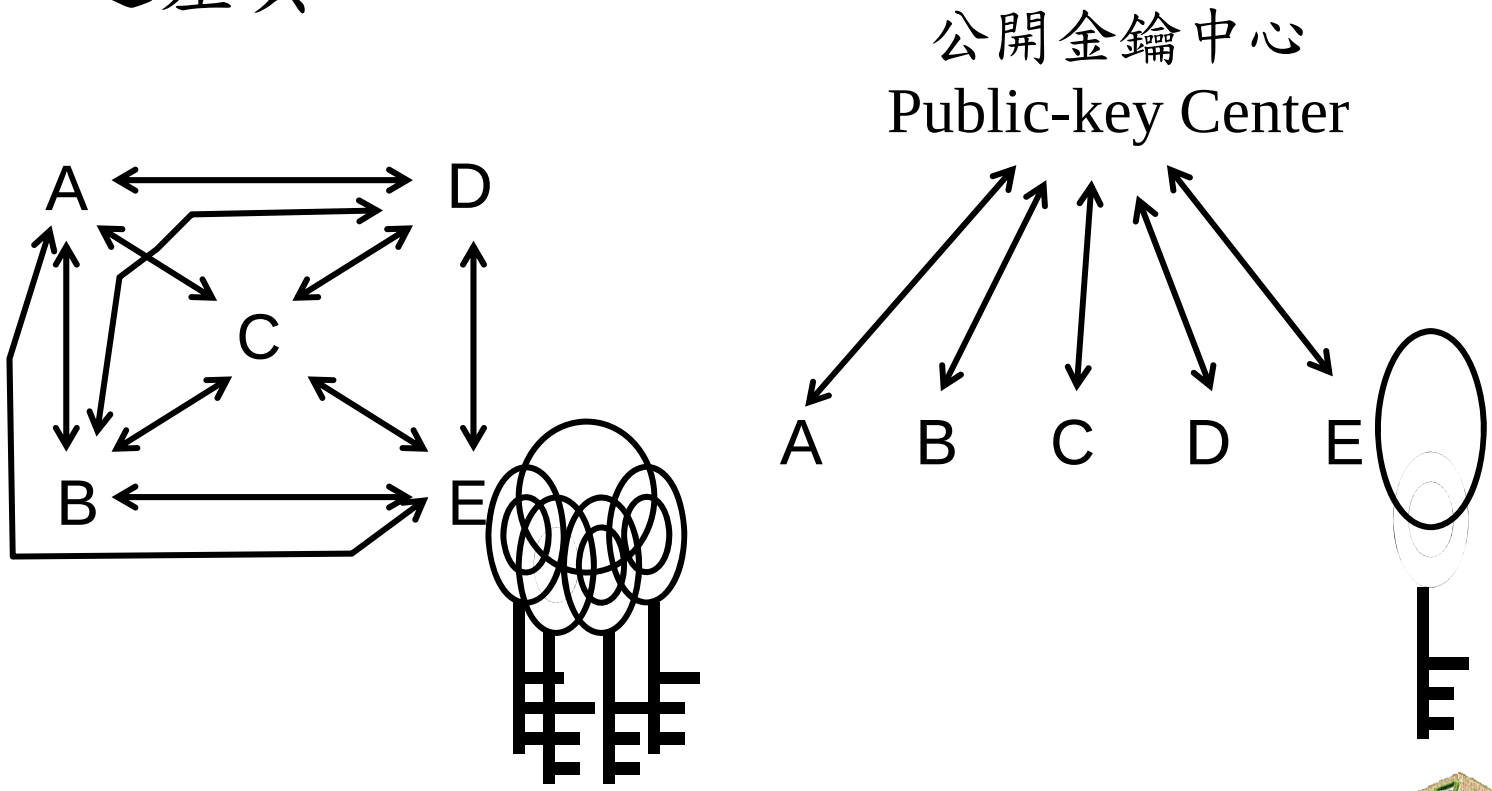
    $$S = 2245613^{748211} \bmod 4119223$$

    驗證簽章時將簽章 S 轉換回明文

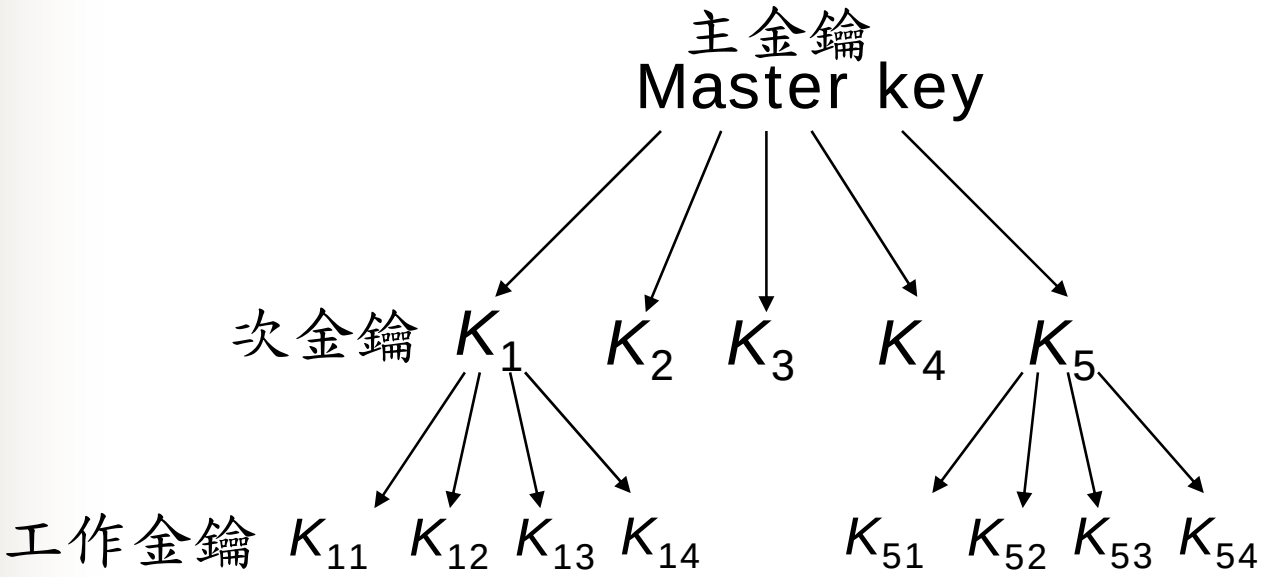
    $$M = S^{11} = 2245613 \bmod 4119223$$

金鑰管理 (Key Management)

- (1)秘密金鑰與公開金鑰系統於“金鑰管理”之差異



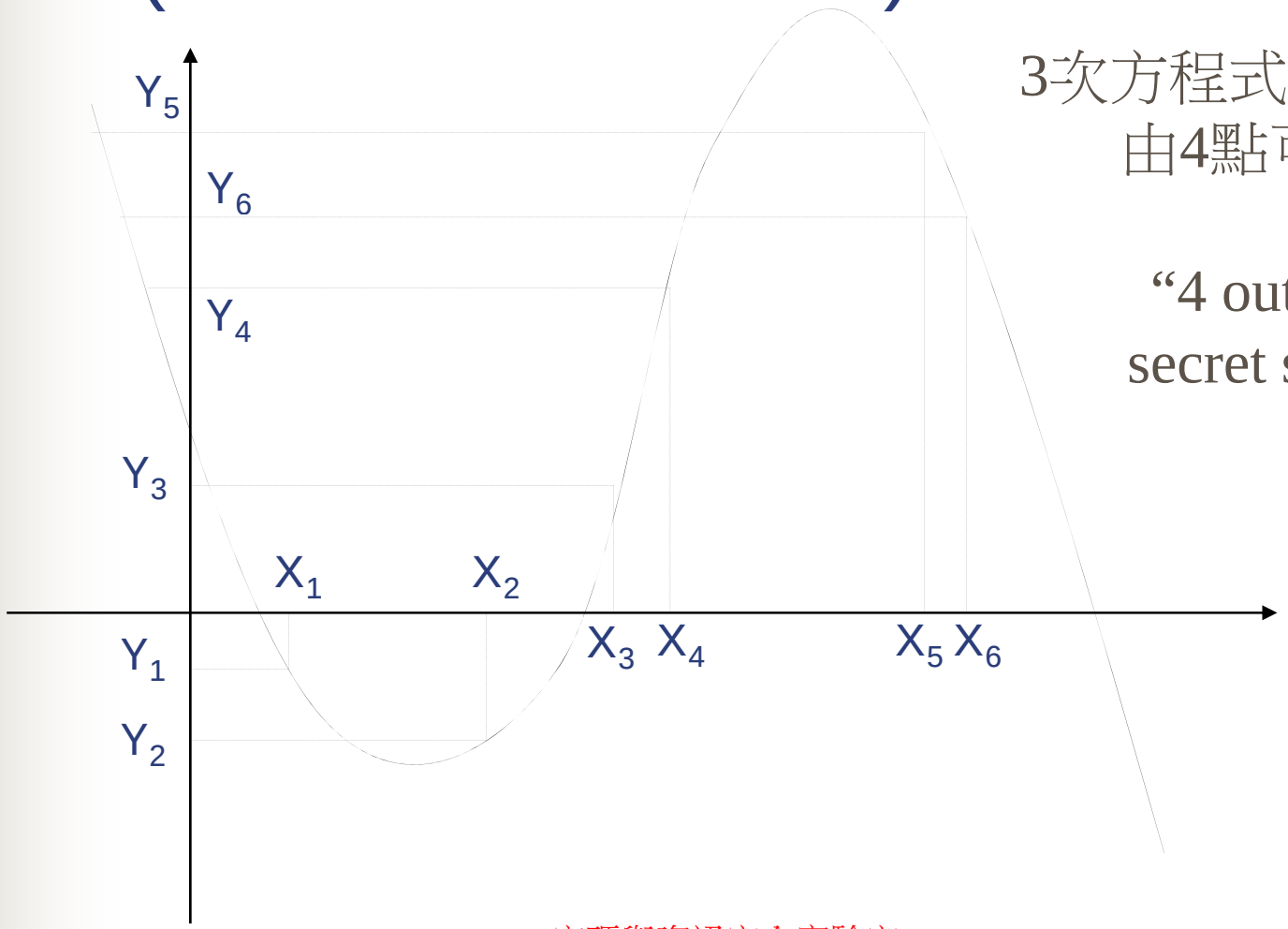
(2) 階層式金鑰管理系統:



(3) 如何保護主金鑰 (安全性 & 可使用性):

交專人負責? 備份多個主金鑰分散儲存?

秘密分享 (secret sharing) 或稱門檻方案 (threshold scheme)



3次方程式 $y=f(x)$ 軌跡由4點可決定:

"4 out of 6" secret sharing

Lagrange polynomial interpolation

- from Wiki

  https://en.wikipedia.org/wiki/Lagrange_polynomial

- To interpolate $f(x) = x^2$ given three points

$$x_0 = 1 \qquad f(x_0) = 1$$
$$x_1 = 2 \qquad f(x_1) = 4$$
$$x_2 = 3 \qquad f(x_2) = 9.$$

The interpolating polynomial is:

$$L(x) = 1 \cdot \frac{x-2}{1-2} \cdot \frac{x-3}{1-3} + 4 \cdot \frac{x-1}{2-1} \cdot \frac{x-3}{2-3} + 9 \cdot \frac{x-1}{3-1} \cdot \frac{x-2}{3-2}$$

$$= x^2.$$

系統安全性相關事項之探討

(1) 系統參數選取與系統生命週期之關連性(適當金鑰長度之選取)

- 四個角度去探討適合的金鑰長度之選取:
  (a)演算法之進展; (b)系統安全性之需求;
  (c)系統/金鑰生命週期; (d)科技進展速度
- 系統安全需求與其面對之**破密者**所擁有之計算能力之不同而有大幅之差異。
- 系統/金鑰生命週期則由國際標準協定所需的大約20年小至個人使用的1至5年不等。

(2) 科技成長與系統安全之相關性

- 有人預估其成長率約為: 每年以20%-40%不等之成長加速中。
- 有人宣稱其假說為: 平均每1.5年加倍成長且已符合實際紀錄約達10年之久。
- 計算能力的提昇對**破密者**與**加密者**(系統使用者)之相關性為何?
  計算能力的成長**對何者較有利**?

(3) 可靠之金鑰長度選取

- 公開金鑰加密器

Rivest 對安全金鑰長度之建議

年代	金鑰長度 (bit)		
	樂觀值	平均值	保守值
1990	398	515	1289
1995	405	542	1399
2000	422	572	1512
2005	439	602	1628
2010	455	631	1754
2015	472	661	1884
2020	489	677	2017

秘密金鑰加密器

Diffie, Rivest, Schneier等人對安全金鑰長度之建議

金鑰長度(bit)	安全程度
40	完全不保密
56	逐漸不保密
75	現今而言足以提供安全需求
90	足夠提供未來近20年內之安全需求

A Cryptographic Game

- PKC or SKC or Hybrid? Or, something?