Privacy Preserving Digital Signatures
(具隱私保護功能之數位簽章)

左瑞麟

國立政治大學 資訊科學系 副教授

raylin@cs.nccu.edu.tw

Contents

- Information Security
- History of Cryptography
- Digital Signatures
- Privacy Preserving Digital Signatures
- Zero-knowledge Proof

何謂資訊安全

- 資訊對組織而言就是一種資產，和其它重要的營運資產一樣有價值，因此需要持續給予妥善保護。資訊安全可保護資訊不受各種威脅，確保持續營運、將營運損失降到最低、得到最豐厚的投資報酬率及商機。

現實世界中的資產保護

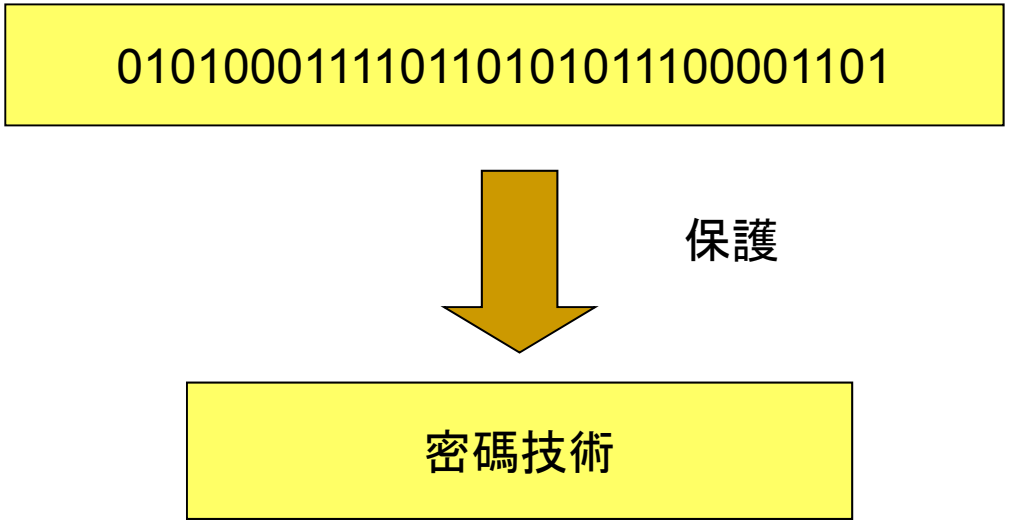
實際的世界

保護

電子方式的資產保護

虛擬的世界

資訊



資訊安全的威脅

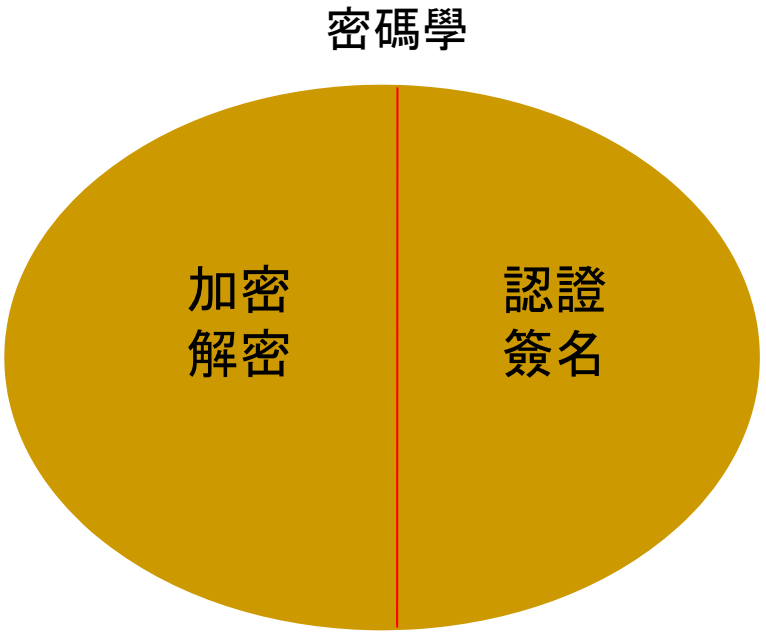
1. 環境的威脅:(15%~17%)
   - 火災、水災、地震等
2. 人的威脅:(83%~85%)
   1）內部人員:(70%~85%)
      - 疏忽、犯錯、惡意行為等
   2）外部人員:(3%~5%)
      - 駭客、病毒、竊聽等

為維護資訊安全 ISO 17799定義

- ISO 17799:**關於資訊安全管理的國際標準**
- a）機密性（ confidentiality）：確保只有經授權（ authorized）的人才能存取資訊。
- b）完整性（ integrity）：保護資訊與處理方法的正確性與完整性。
- c）可用性（ availability）：確保經授權的使用者在需要時可以取得資訊及相關資產。
- More: 不可否認性(non-repudiation)

密碼學

- 密碼學(Cryptography): 包含各種(廣義)加密技術的學科總稱



中國文學的密碼技術

我聞南海大士
為人了卻凡音
秋來明月照柴門
香滿禪堂幽徑
屈指靈山會後
居然紫竹成林
同男童女拜觀音
僕僕和居榮幸


山
姐
秋
天
路
各
夜
心
肝
信
夕
屏
來

鵝飛鳥去永不回

良字去頭雙人陪

雙木非林心相隨

您若無心各自飛

語譯：

我很想你

Classical Cryptography
（古典密碼學）

Caesar Cipher

- earliest known substitution cipher
- by Julius Caesar
- first attested use in military affairs
- replaces each letter by 3rd letter on

Caesar Cipher

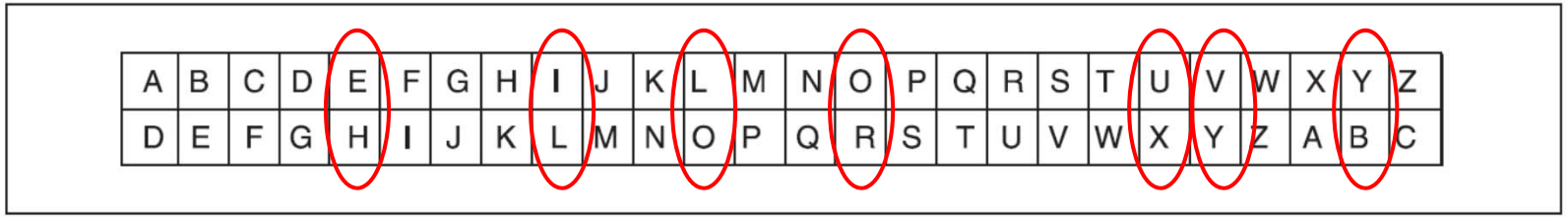
- Example:

```
明文：meet me after the toga party
密文：PHHW Ph DIWHU WKH WRJD SDUWB
```

- Can define transformation as

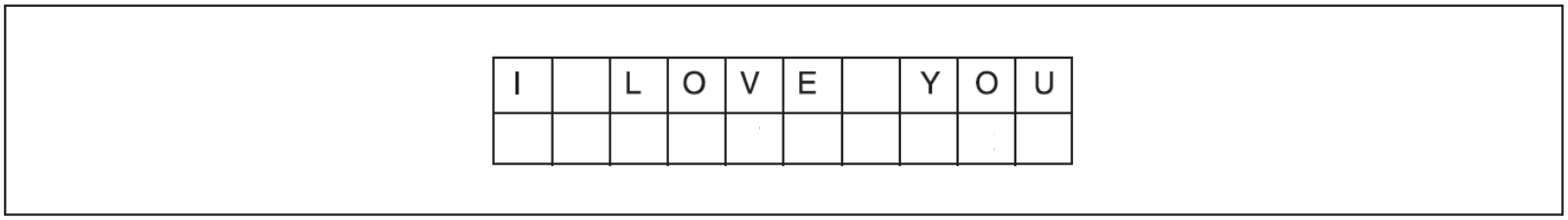
```
明文：a b c d e f g h i j k l m n o p q r s t u v w x y z
密文：D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
```

- 使用適當方法對明文進行編譯所形成的訊息稱為密文。



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
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

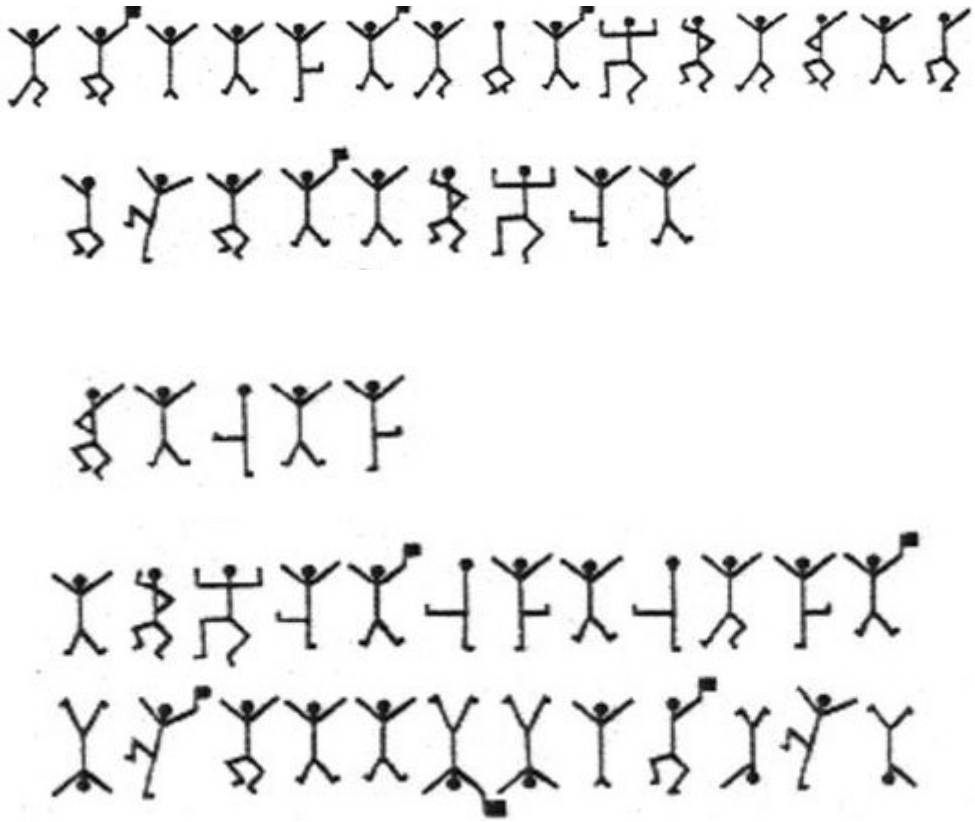
圖 2.2　使用後三位字母替代這一字母的訊息編譯方法



I		L	O	V	E		Y	O	U

圖 2.3　使用字母替代方法的編譯

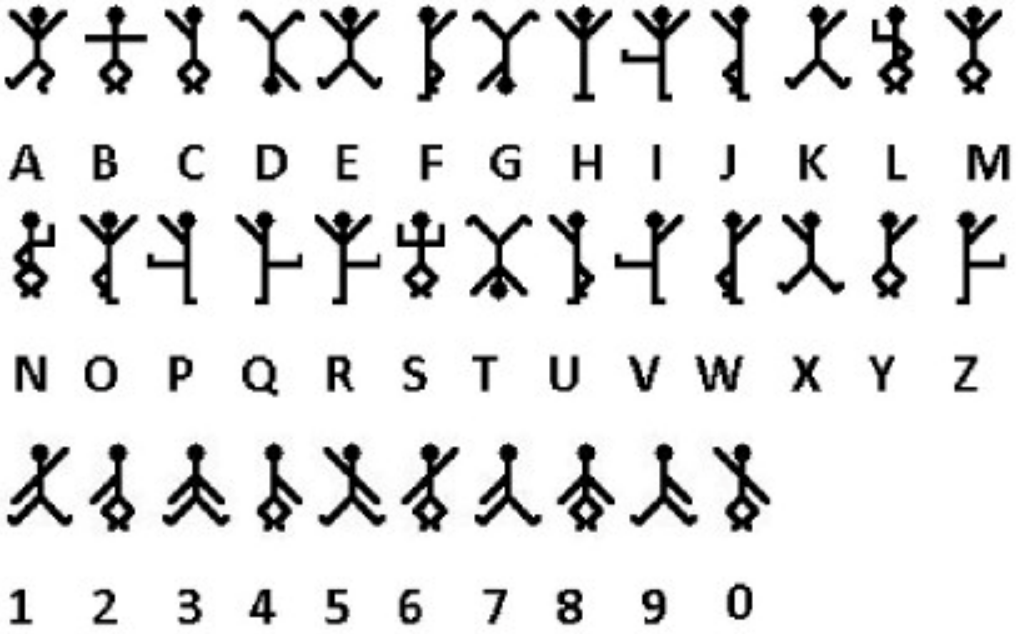
The Adventure of the Dancing Men



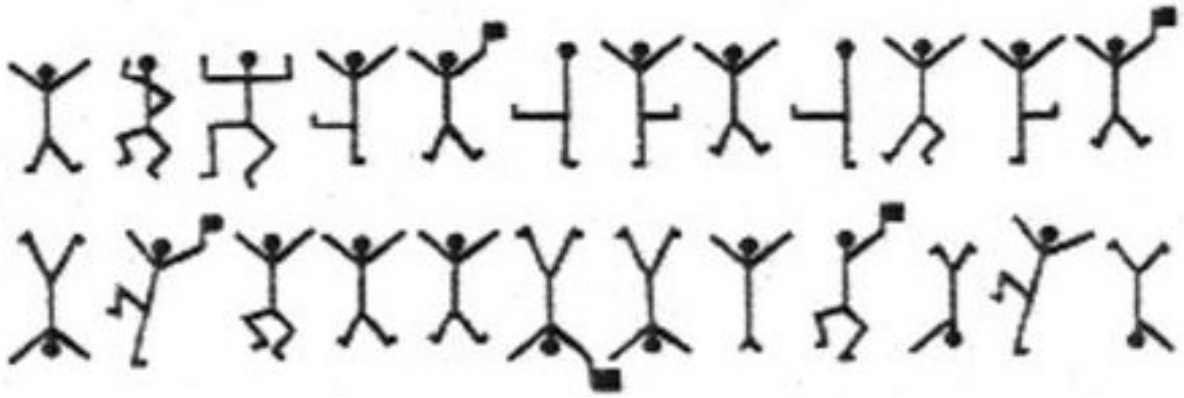
In Sherlock Holmes' story "The Adventure of the Dancing Men", a man reports that his wife, Elsie, became upset when she received several notes with figures of dancing men on them. Holmes went about deciphering the code. He knew that E is the most common letter in the English language and that there was a high probability that the name "Elsie" appeared somewhere in one of the messages. Using this information, can you decipher the messages she received and the one message she sent?

The Adventure of the Dancing Men

Dancing Man Code (Sherlock Holmes)

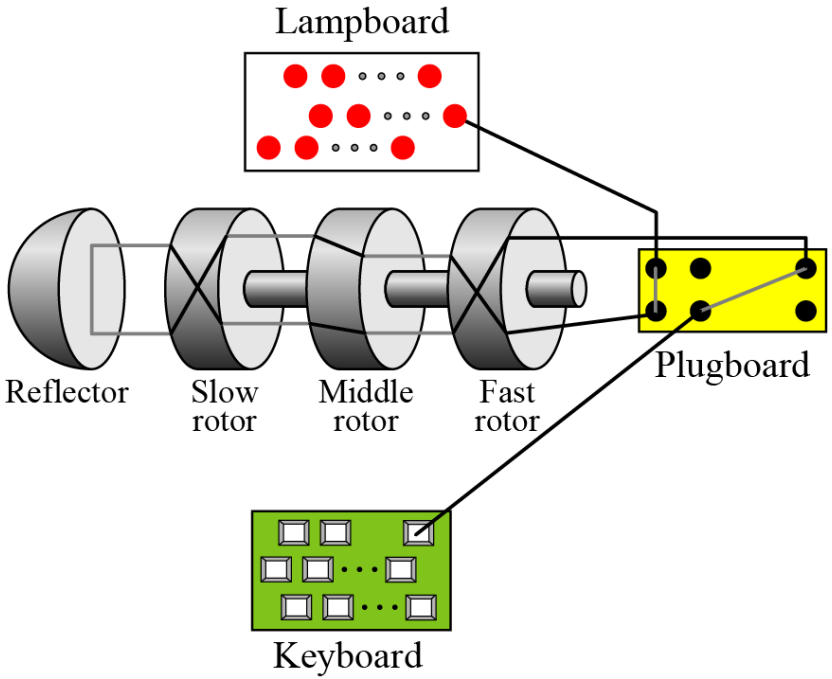


The Adventure of the Dancing Men



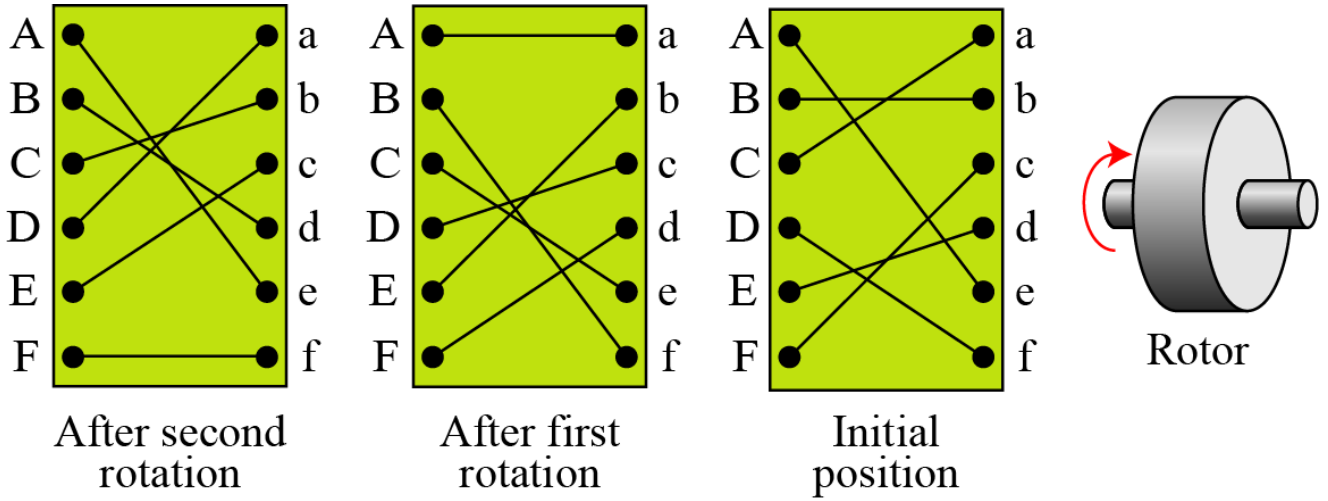
“ELSIE PREPARE TO MEET THY GOD”

Enigma Machine



Rotors of Enigma Machine

- ex:

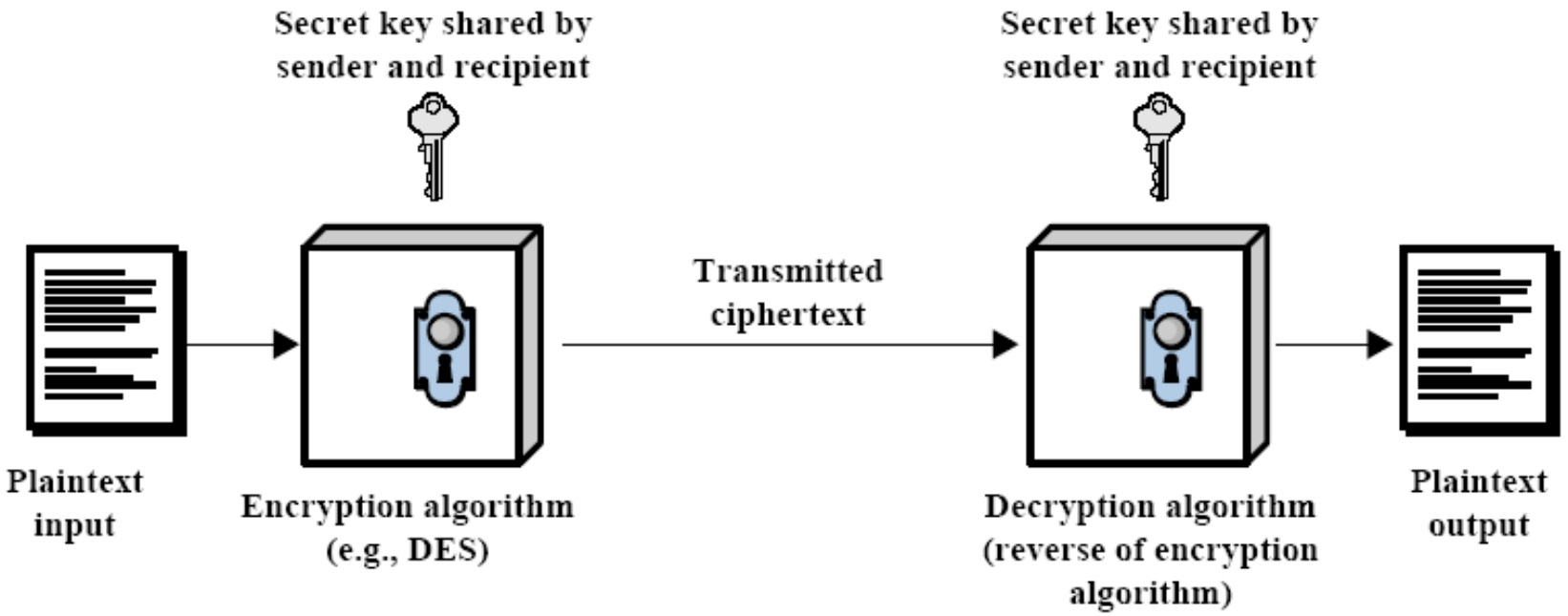


現代密碼
(Contemporary Cryptography)

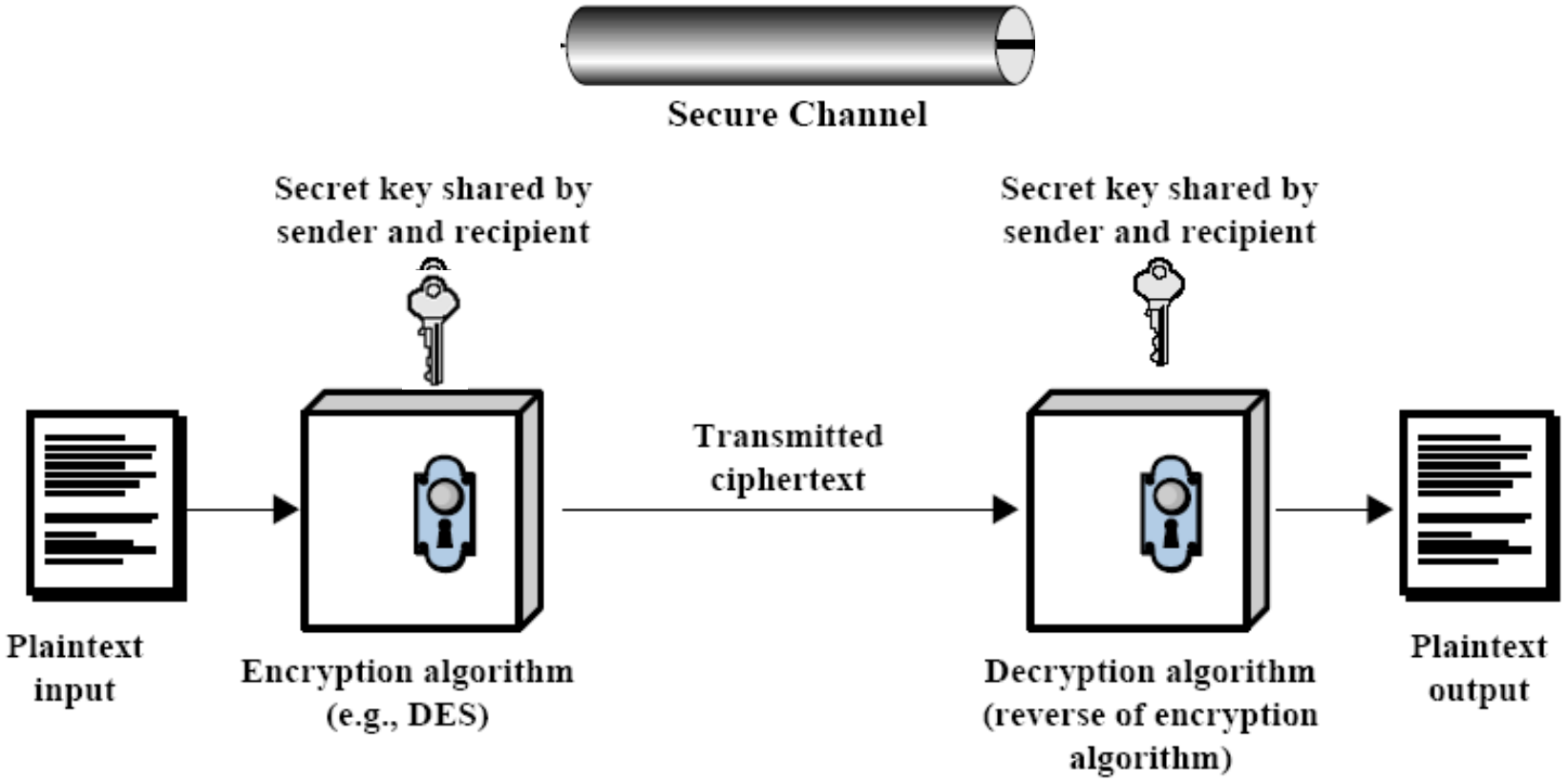
Contemporary Cryptography

- 對稱式密碼（symmetric key cryptography）
- 公開金鑰密碼(public key cryptography)

傳統加密模型

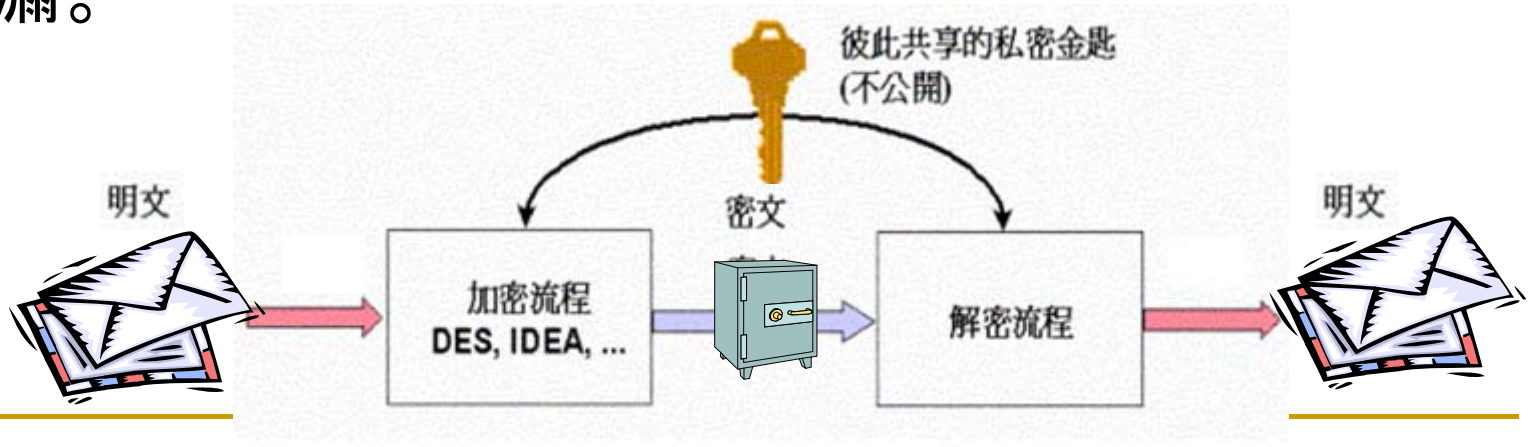

Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

傳統加密技術的問題點


Secure Channel
Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

對稱式密碼系統(Symmetric Cryptography)

- 又稱為傳統或秘密金鑰 (conventional or secret key)密碼系統
- 需要傳送和接收雙方均擁有相同的一把金鑰匙
- 若加密鑰匙不幸外漏，則解密鑰匙等於一併外漏。



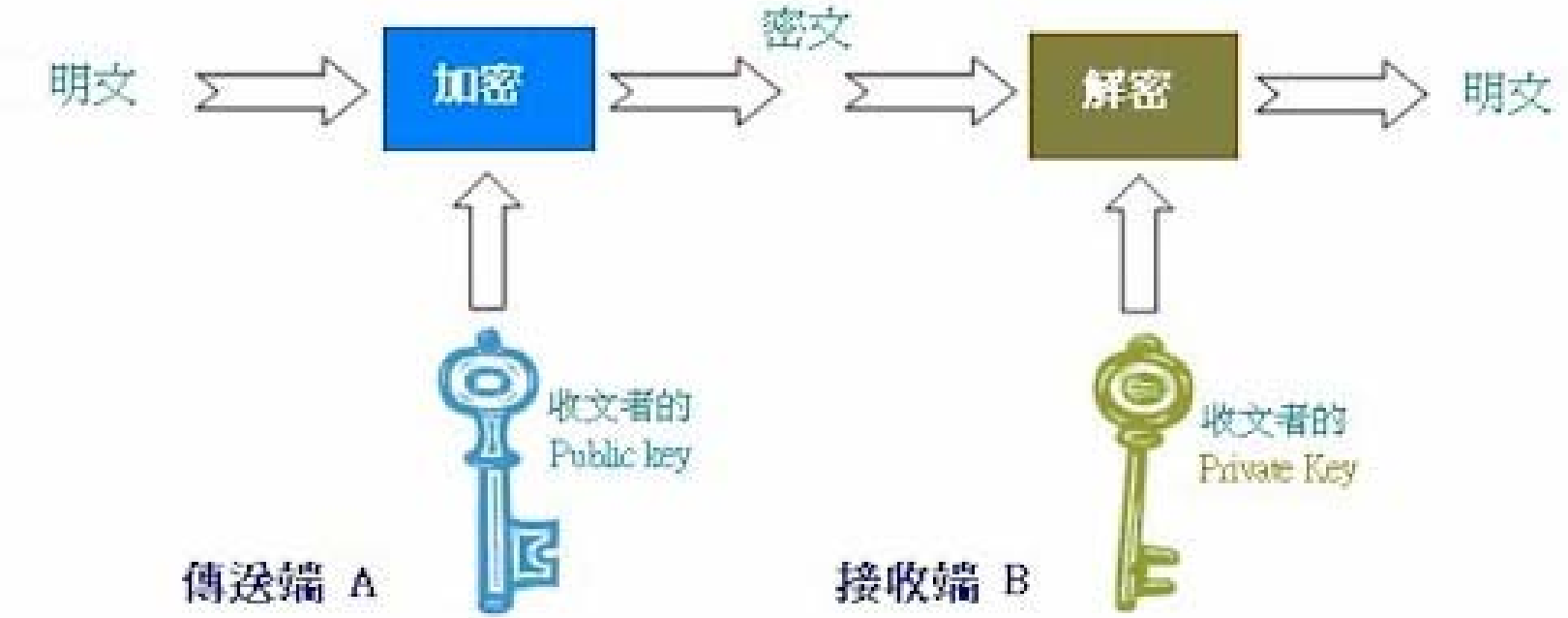
對稱加密技術的優缺點

- 優點:
  - 速度較快
- 缺點:
  - 需要有一個安全性機制將金鑰匙安全性的分送至交易的雙方。
  - 若要秘密通訊，兩兩人之間就需要一把key，n人需要n(n-1)/2把key
  - 兩個人之間共同保有個secret key若其中一方洩漏則相互傳遞的加密訊息無效(等於被攻破了)

著名的對稱性加密演算法

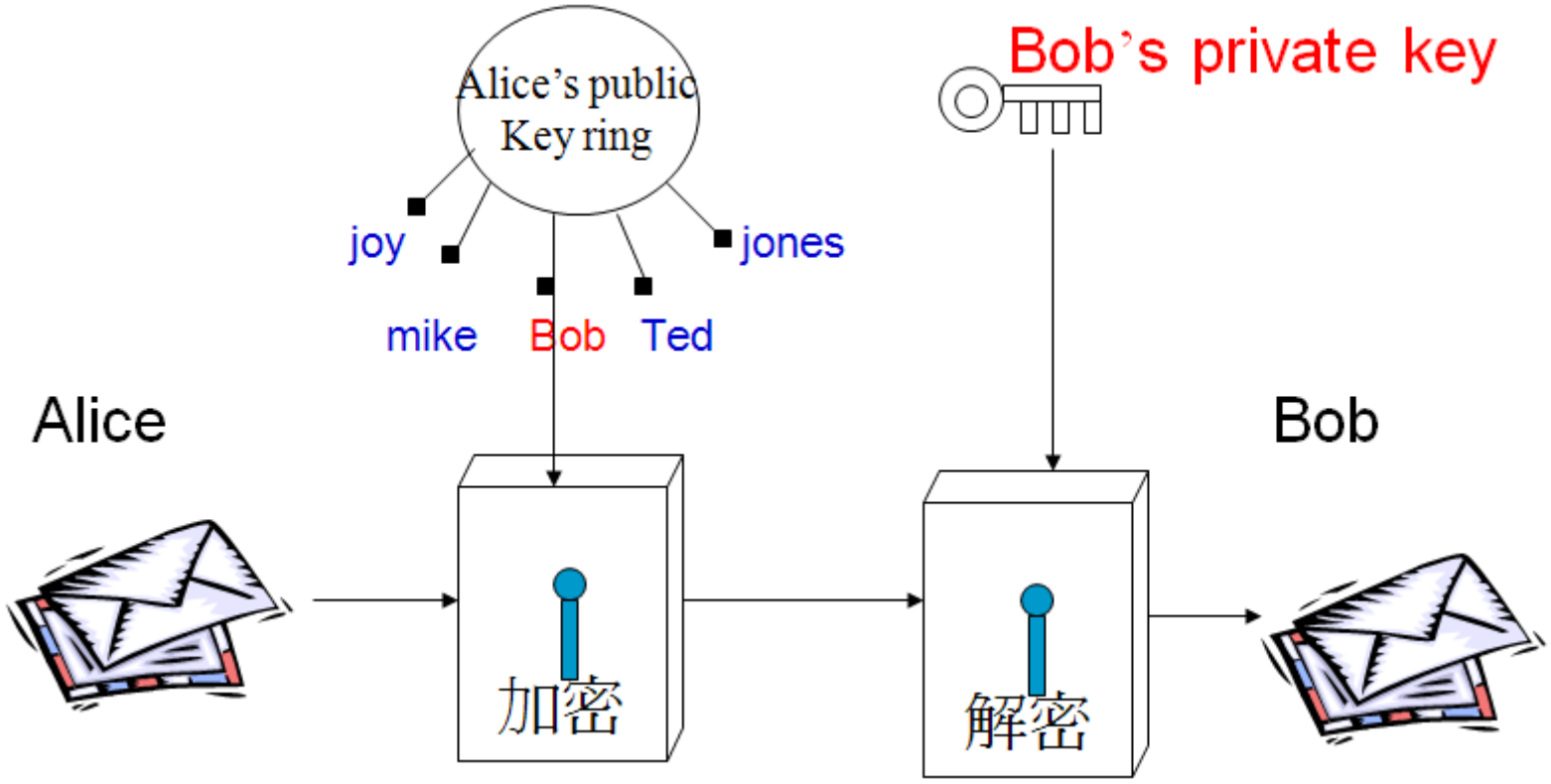
- Data Encryption Standard (DES)
- Triple DES (3DES)
- IDEA
- RC4
- AES

公開金鑰密碼
(Public Key Cryotosystem)

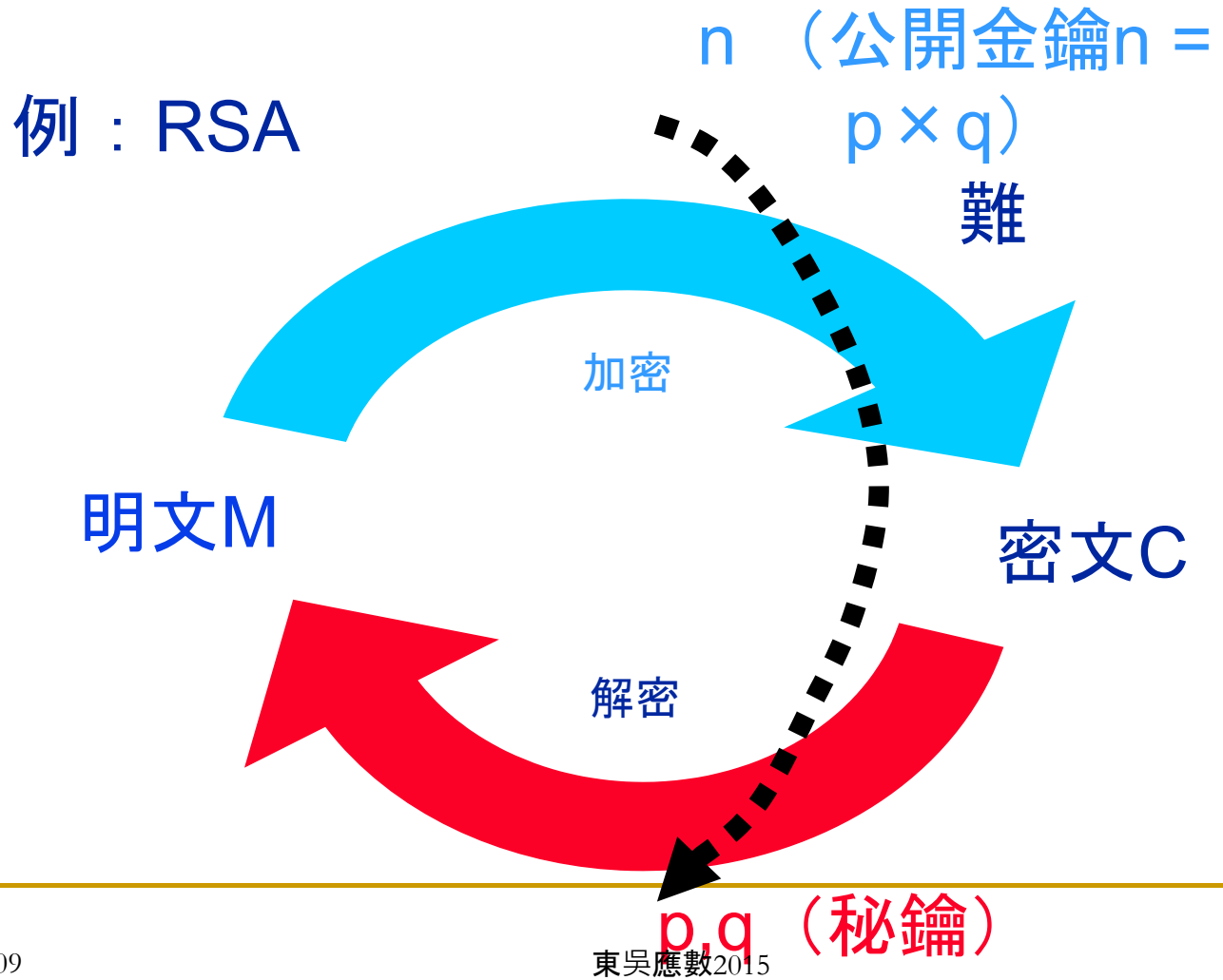


Public key 系統簡介（加解密）

- Alice欲將訊息送給Bob



公開金鑰密碼的原理



公開金鑰密碼的安全性

基於數學上的難問題

- 因數分解問題（Prime Factoring）
- 離散對數問題(Discrete Logarithm)
  - Computational Diffie-Hellman Problem
  - …….

因數分解問題

問題:給一個合成數 n

答: n 的因數 d, $1 < d < n$

因數分解問題(IFP)

問:n=15
答:

問:n=4284179
答:

|n|=768 bits, 2009年破解
實用上,|n|=1024

問:n=247
答:

問:n=83887277
答:

問:|n|=1024bit
答:

US$10,000 — RSA-576

1881988129206079638386972394616504398071635633794173827007633564229888597152346654853190606065047430453173880113033967161996923212057340318795506569962213051687593076502570 59

Solved on Dec. 3, 2003

3980750864240649373971255005503864911990643623425267084063851895759463889572617685833317

4727721461074353025362230719730482246329146953020971164598521711305207112563635903975 27

US$200,000 — RSA-2048

2519590847565789349402718324004839857142928
2126204032027777137836043662020707595556264
0185258807844069182906412495150821892985591
4917618450280848912007284499268739280728777
6735971418347270261896375014971824691165077
6133798590957000973304597488084284017974291
0064245869181719511874612151517265463228221
6869987549182422433637259085141865462043576
7984233871847744479207399342365848238242811
9816381501067481045166037730605620161967625
6133844143603833904414952634432190114657544
4541784240209246165157233507787077498171257
7246796292638635637328991215483143816789988
5040445364023527381951378636564391212010397
12282212072035 7

離散對數問題(Discrete Logarithm Problem)

問題: 質數 p, 整数 g, y

答: 滿足 $y = g^x \bmod p$

的 x

Modular運算 (mod)

- a 及 b 被 n 除後之餘數相等

$$a \equiv b \pmod{n}$$

- 例

$$2 \equiv 7 \pmod{5}$$

Discrete Logarithm Problem

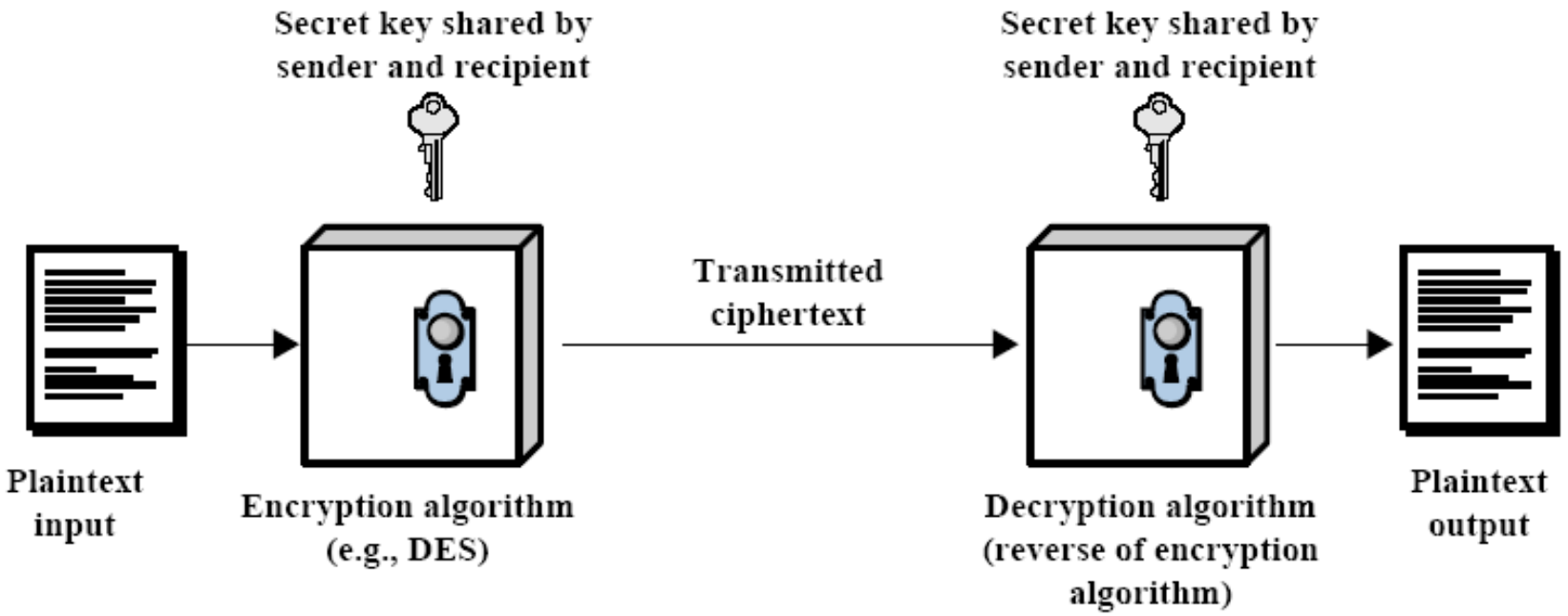
- Ex.

1. $8=2^x \bmod 11$, $x=$
2. $18=2^x \bmod 19$, $x=$
3. $18=3^x \bmod 23$, $x=$
4. $1 = 7^x \bmod 3571$ $x=$

實用上,$|p|=1024$

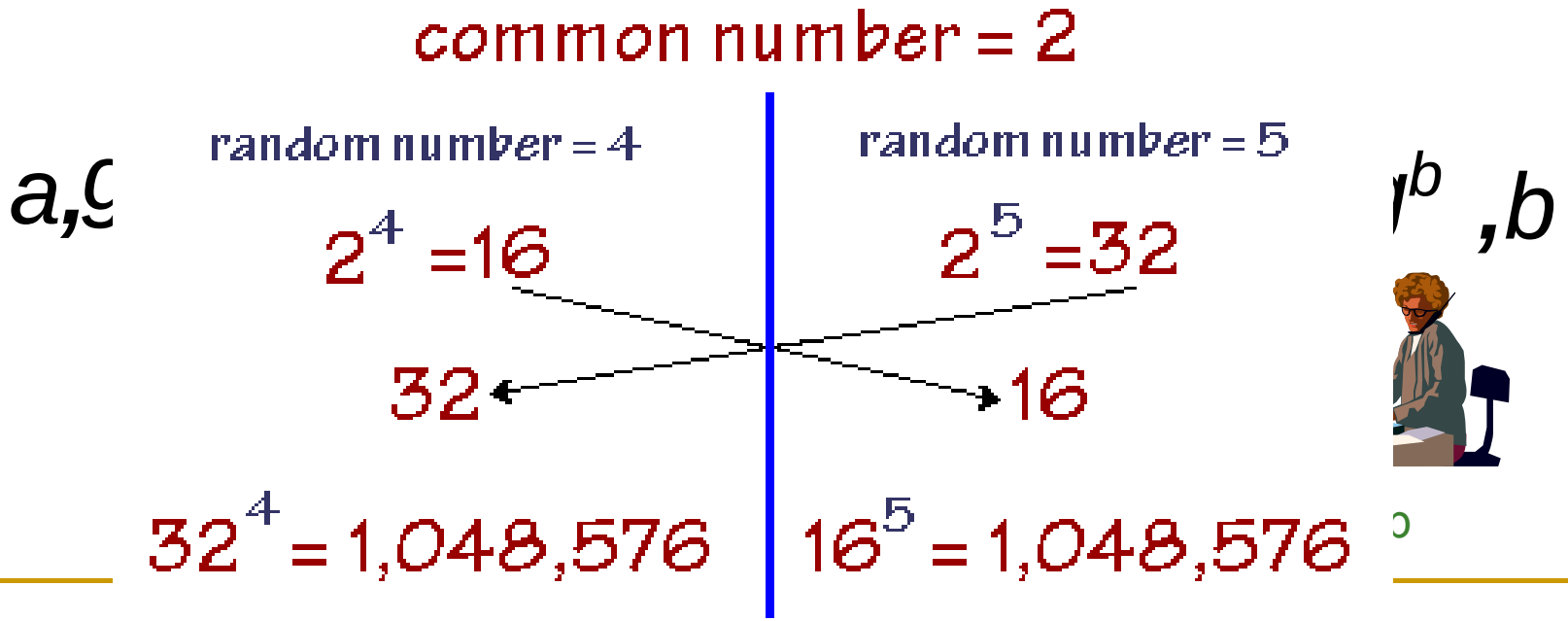
Symmetric Encryption

Symmetric Cryptosystem



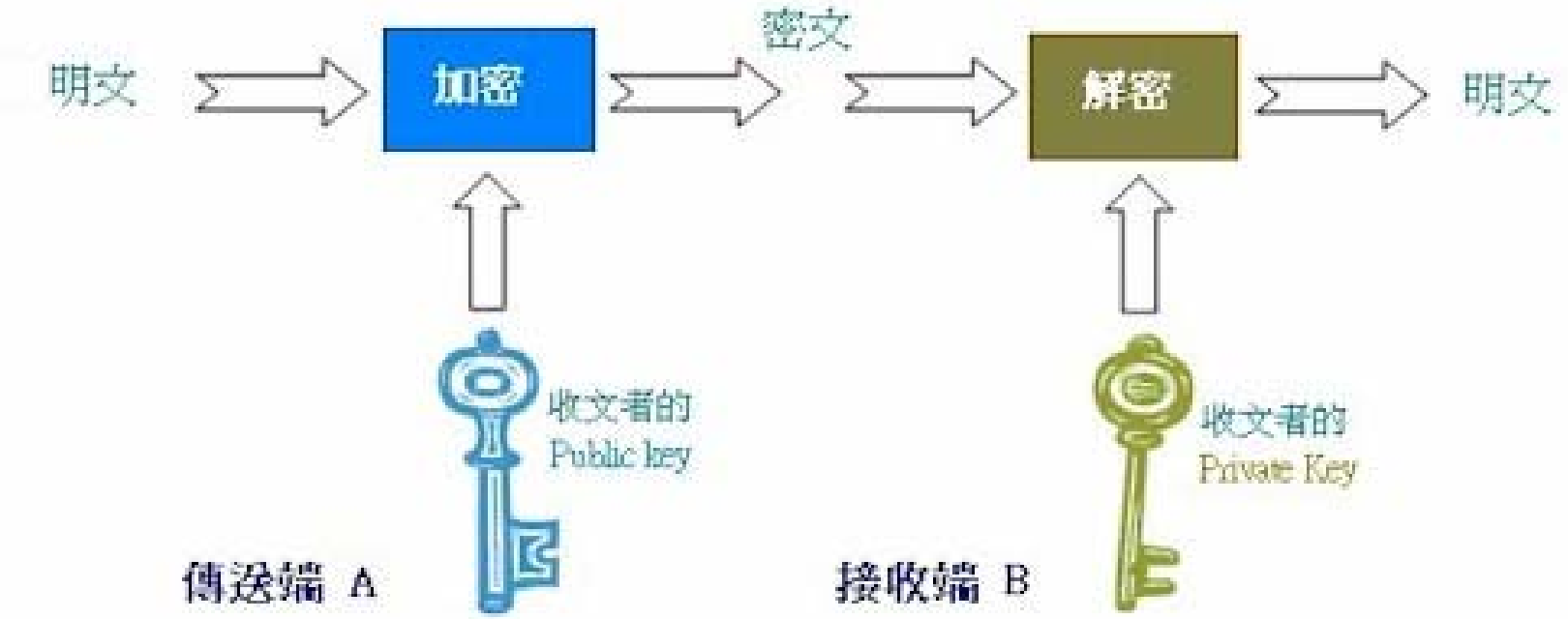
Diffie-Hellman Key Exchange Protocol

- PKC的概念為W. Diffie 和M. E. Hellman在1976年所提出
- 安全性基於離散對數問題



Asymmetric Encryption

Public Key Cryptosystem



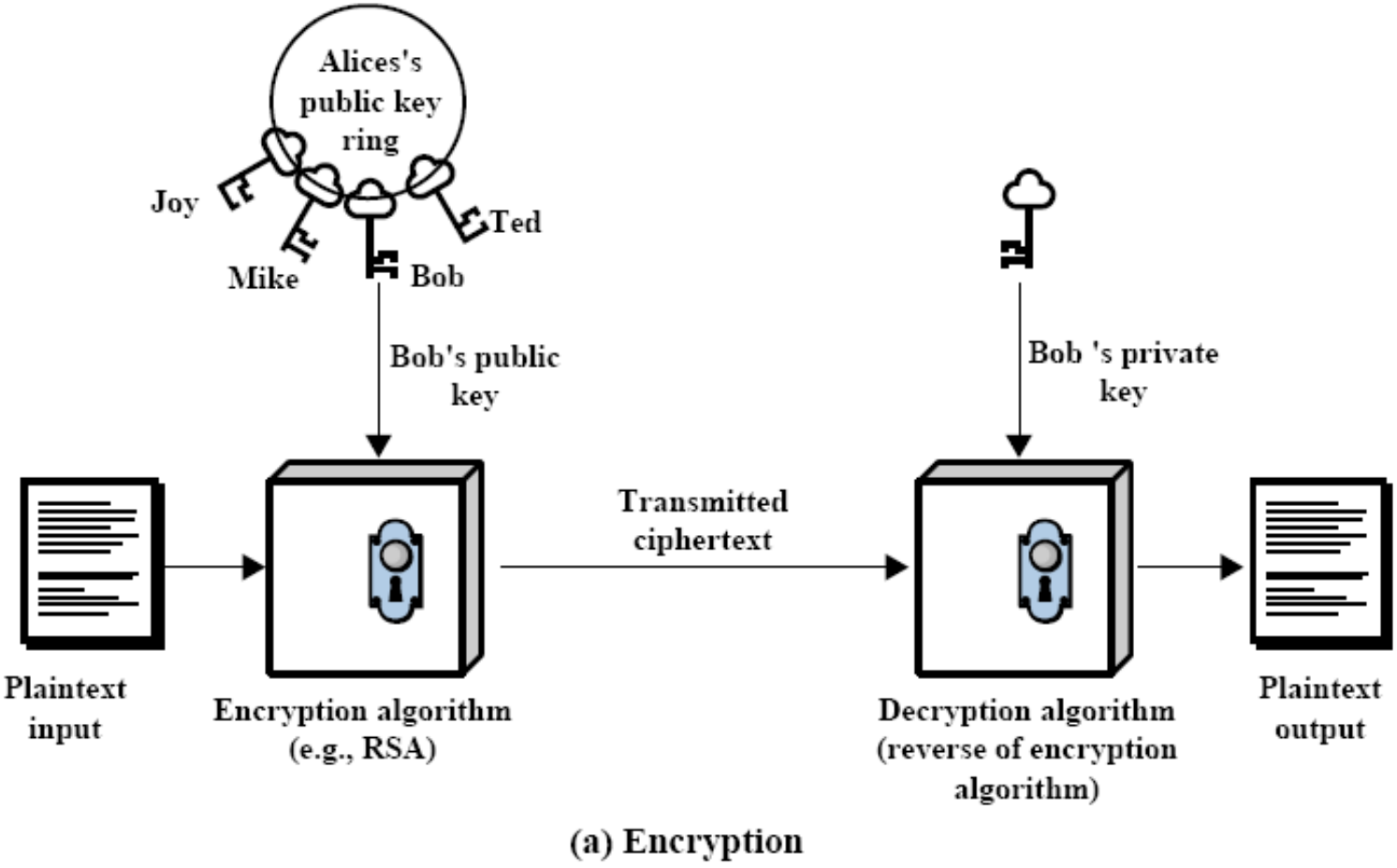
公開金鑰密碼技術的優缺點

- 優點:
  - 加密金鑰公開也不影響系統的安全性
  - 不需要安全通道(Secure channel)來分配鑰匙(因為加密用的鑰匙可以公開發送)
  - 加密者不需要記任何密鑰
  - 解密者只需記一個密鑰
  - 可用在加解密及數位簽章
- 缺點:
  - 效率較差，速度慢

著名的公開金鑰密碼系統

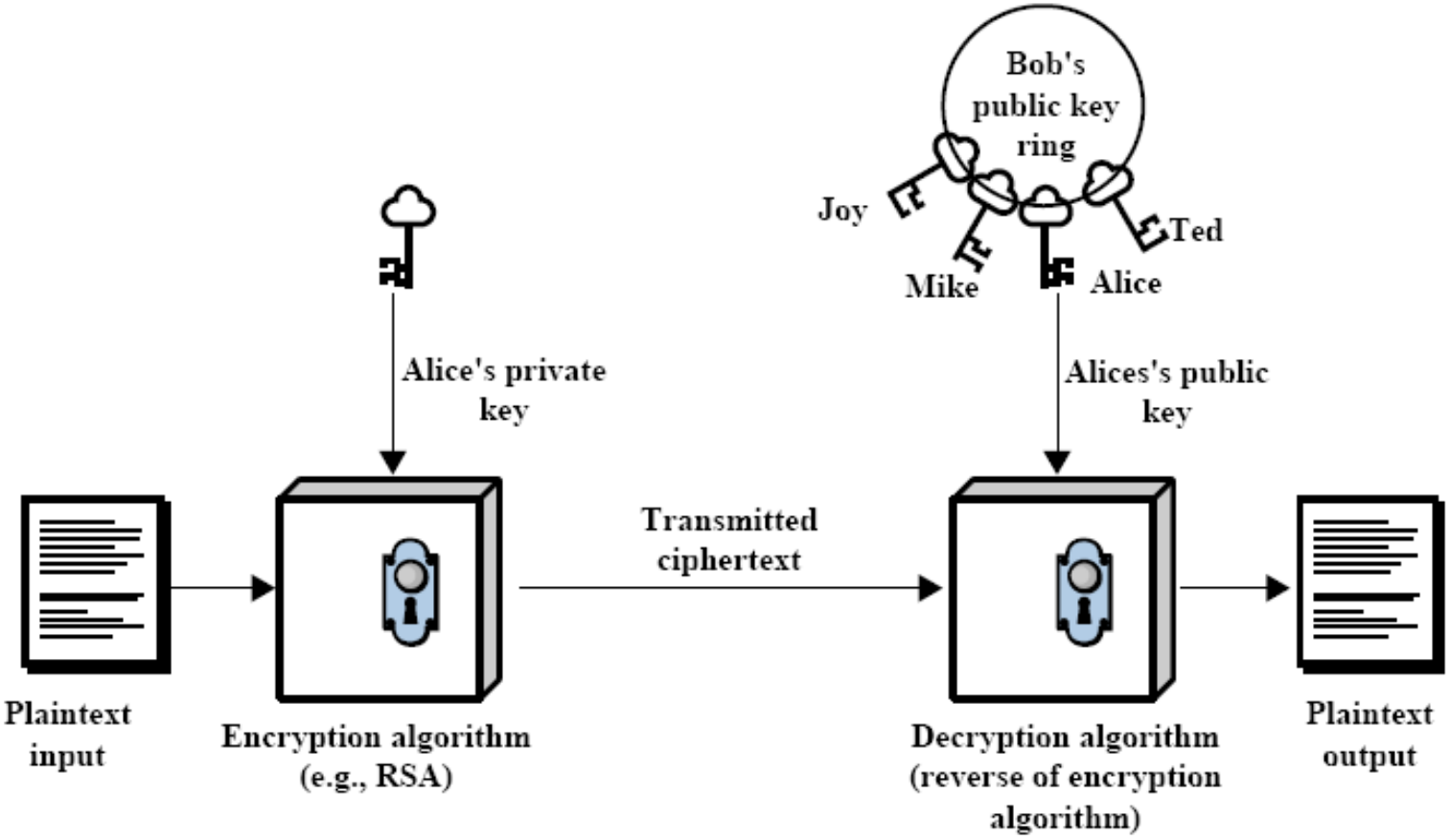
- RSA Cryptosystem
- ElGamal Cryptosystem
- Digital Signature Algorithm (DSA)
- …

公開金鑰加密流程



(a) Encryption

Digital Signature



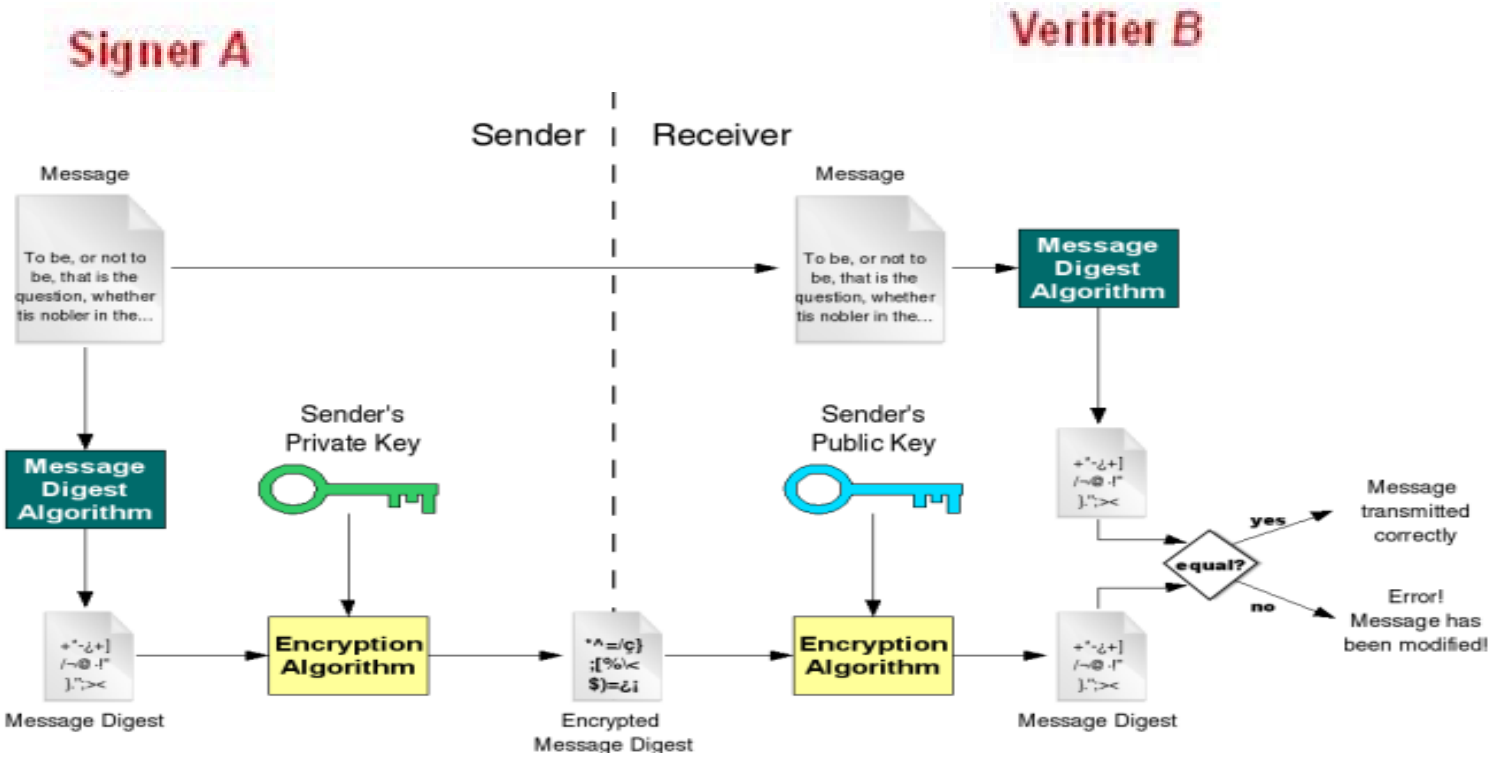
(b) Authentication

Digital Signatures

- A **digital signature** is a type of asymmetric cryptography. For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender

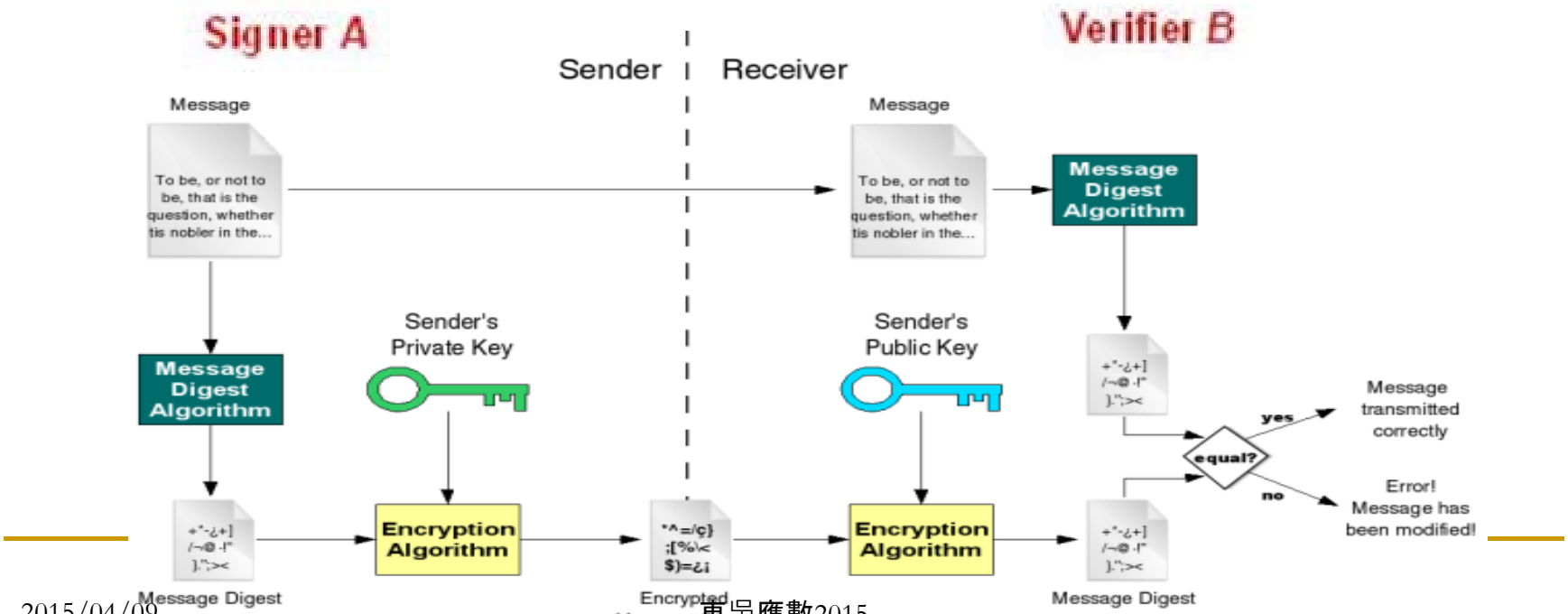
Digital Signatures

- Only A can generate the signature S of a message M
- Anyone can verify the signature S
- It can be fair judged by the third party if A and B dispute on the signature S



Characteristic

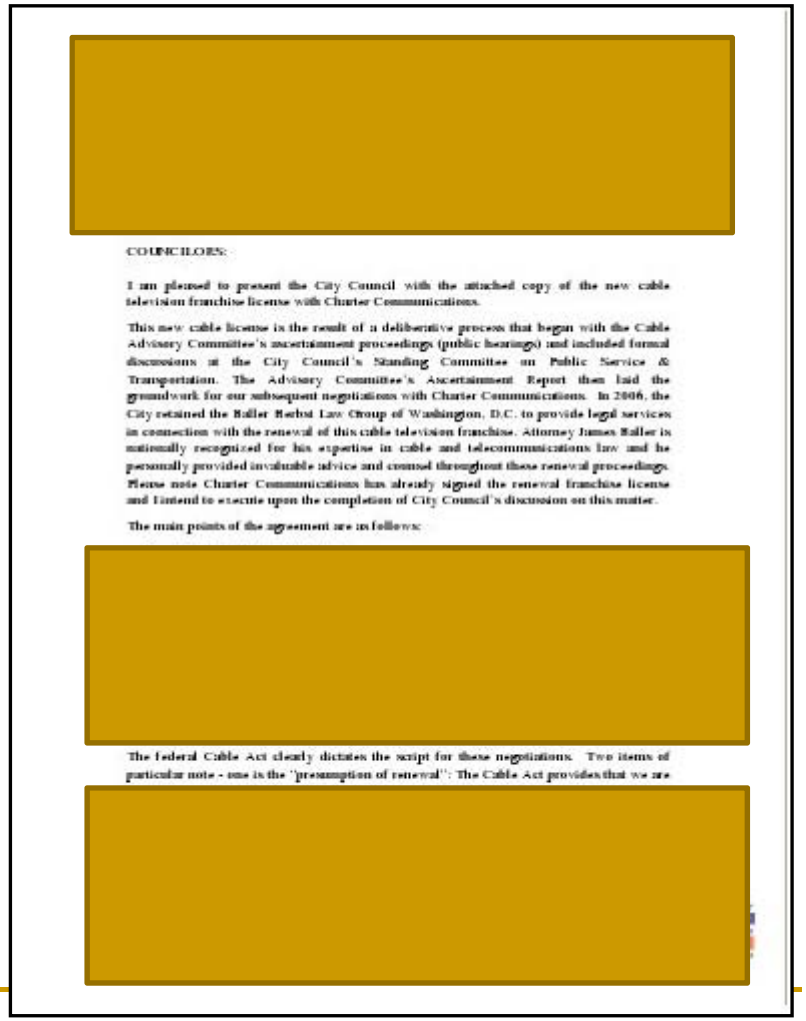
- The signature is authentic
- The signature is unforgeable
- The signature is not reusable
- The signed document is unalterable
- The signature cannot be repudiated



What Digital Signatures Cannot Do

- Hiding information
- Protecting personal privacy

- This is because that a secure digital signature does not allow any alternation on the signed document



COUNCILORS:

I am pleased to present the City Council with the attached copy of the new cable television franchise license with Charter Communications.

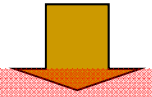
This new cable license is the result of a deliberative process that began with the Cable Advisory Committee's ascertainment proceedings (public hearings) and included formal discussions at the City Council's Standing Committee on Public Service & Transportation. The Advisory Committee's Ascertainment Report then laid the groundwork for our subsequent negotiations with Charter Communications. In 2006, the City retained the Baller Herbst Law Group of Washington, D.C. to provide legal services in connection with the renewal of this cable television franchise. Attorney James Baller is nationally recognized for his expertise in cable and telecommunications law and he personally provided invaluable advice and counsel throughout these renewal proceedings. Please note Charter Communications has already signed the renewal franchise license and I intend to execute upon the completion of City Council's discussion on this matter.

The main points of the agreement are as follows:

The federal Cable Act clearly dictates the script for these negotiations. Two items of particular note - one is the "presumption of renewal": The Cable Act provides that we are

About Privacy Protection

- Traditional digital signatures do not provide any privacy protection for users (signers, receivers)
- Privacy protection has become more and more important
  - Consumers increasingly rely on the internet for shopping, banking and other activities
  - E-voting
- An encryption system is not what we want
  - We want to hide the identity of signers from verifiers
  - We want to hide some information from signers/verifiers
- A secure system to protect personal information is required



Signature schemes providing privacy protection

Privacy Protection Digital Signature

- We already have some digital signatures that providing privacy protection
  - Ring signature
  - Blind signature
  - Designated verifier signature
  - Content extract signature
  - etc.

Story of Ring Signatures : Old

- Once upon a time, there was a signature scheme like a ring signature scheme in Japan.

資料來源:www.iacr.org/conferences/crypto2005/r/38.ppt

In This Talk

- We consider two major paradigms when using digital signatures
  - two-entity case (a signer and a verifier)
  - three-entity case (a signer, a signature holder, and a signature verifier)

Two-Entity Case

Signer

ask a signature on a sensitive message

OK, what protocol can we use

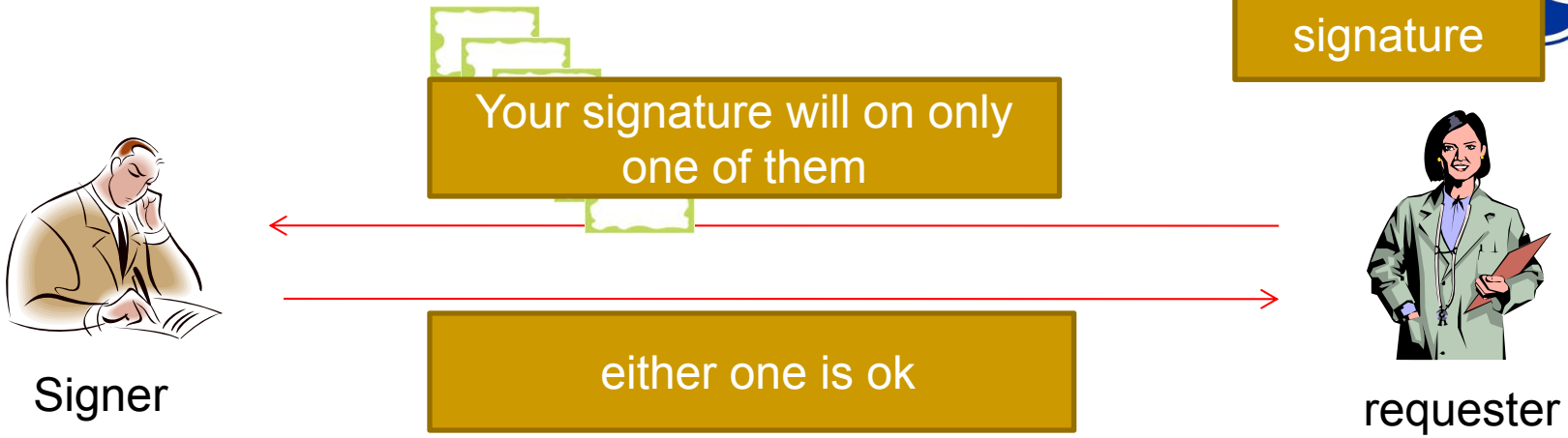
requester

- A very friendly signer that willing to sign any kind of secure signature that protect requester's privacy

Blind Signatures (Shortcoming)

- Signer's view is perfectly shut off from the resulting signatures
- The signer has no control over the message to be signed
- It is a risk for the signer to sign such a blinded message (ie., he must trust the signature requestor)

Two-Entity Case

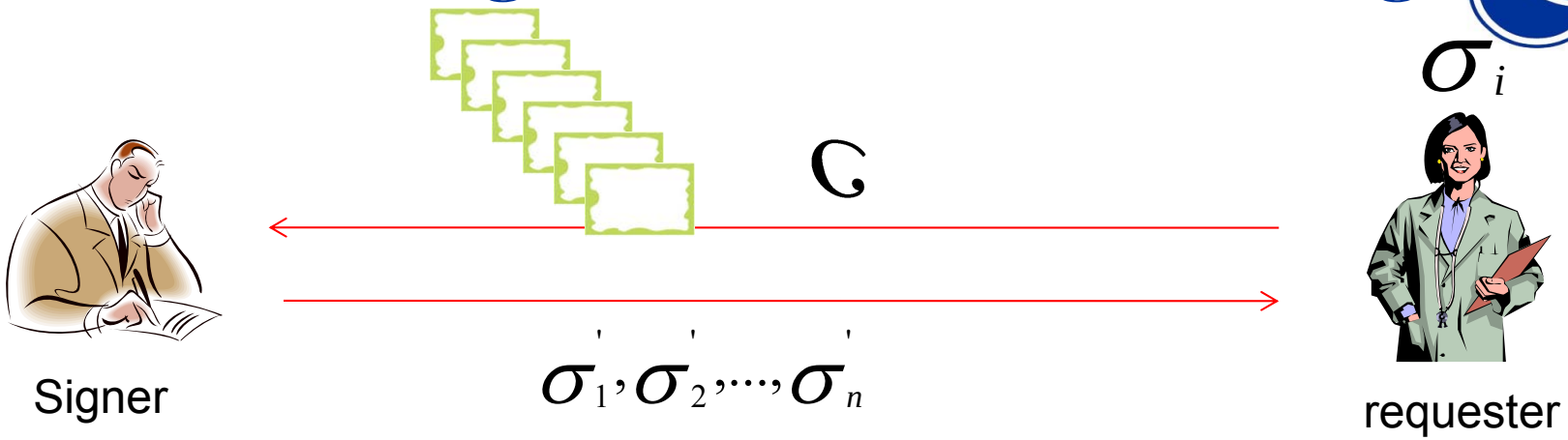


- A very friendly signer that willing to sign any kind of secure signature that protect requester's privacy

Oblivious signatures

- First introduced by L. Chen in 1994
- Two types of oblivious signatures
  - Oblivious signature with *n* messages
  - Oblivious signature with *n* keys

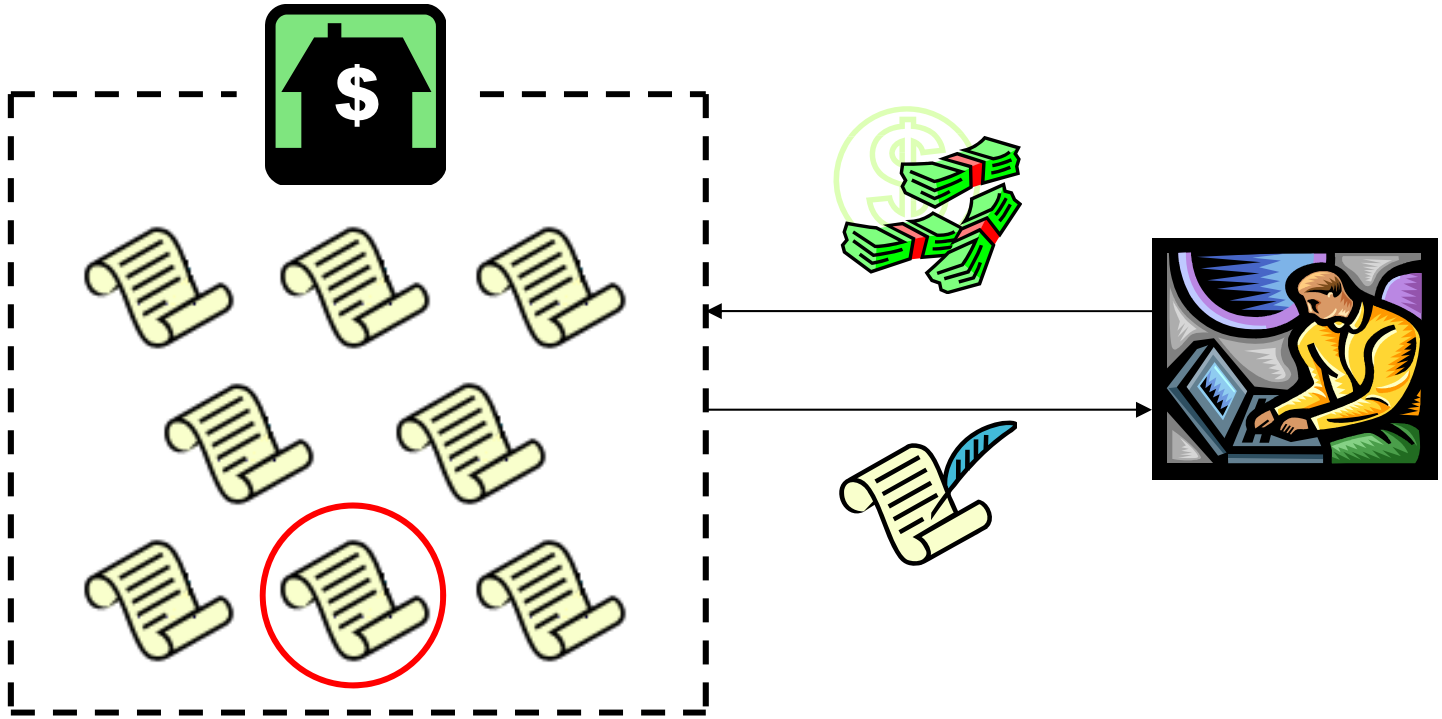
Oblivious Signature with n Message



- By executing the protocol, the recipient R can choose only one of the *n* messages to get signed
- The singer cannot find out on which message the recipient has got the signature

Application to On-line Shopping

- On-line shopping

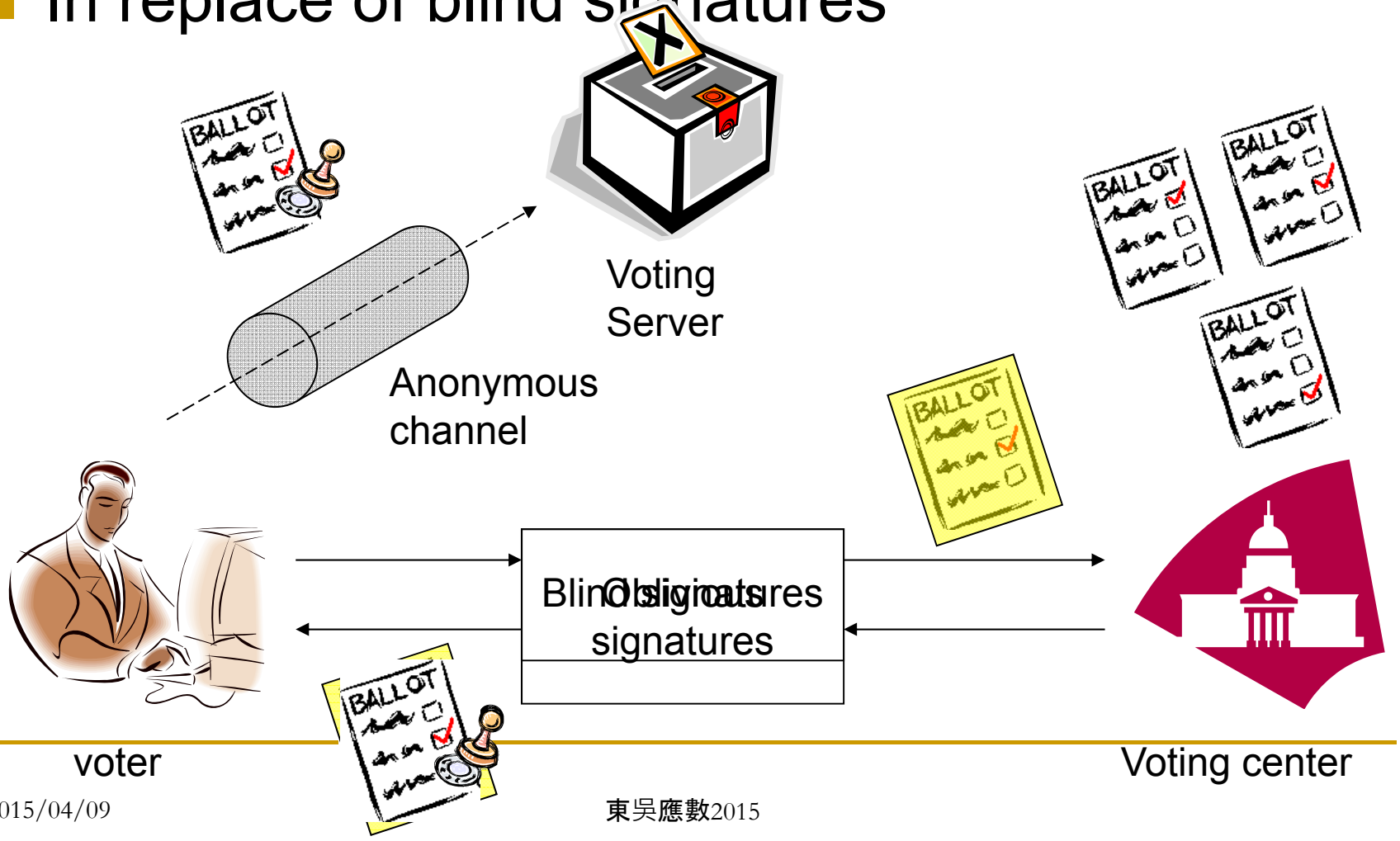


1. Which product interests the user is kept secret to the seller

2. Get receipt from the seller

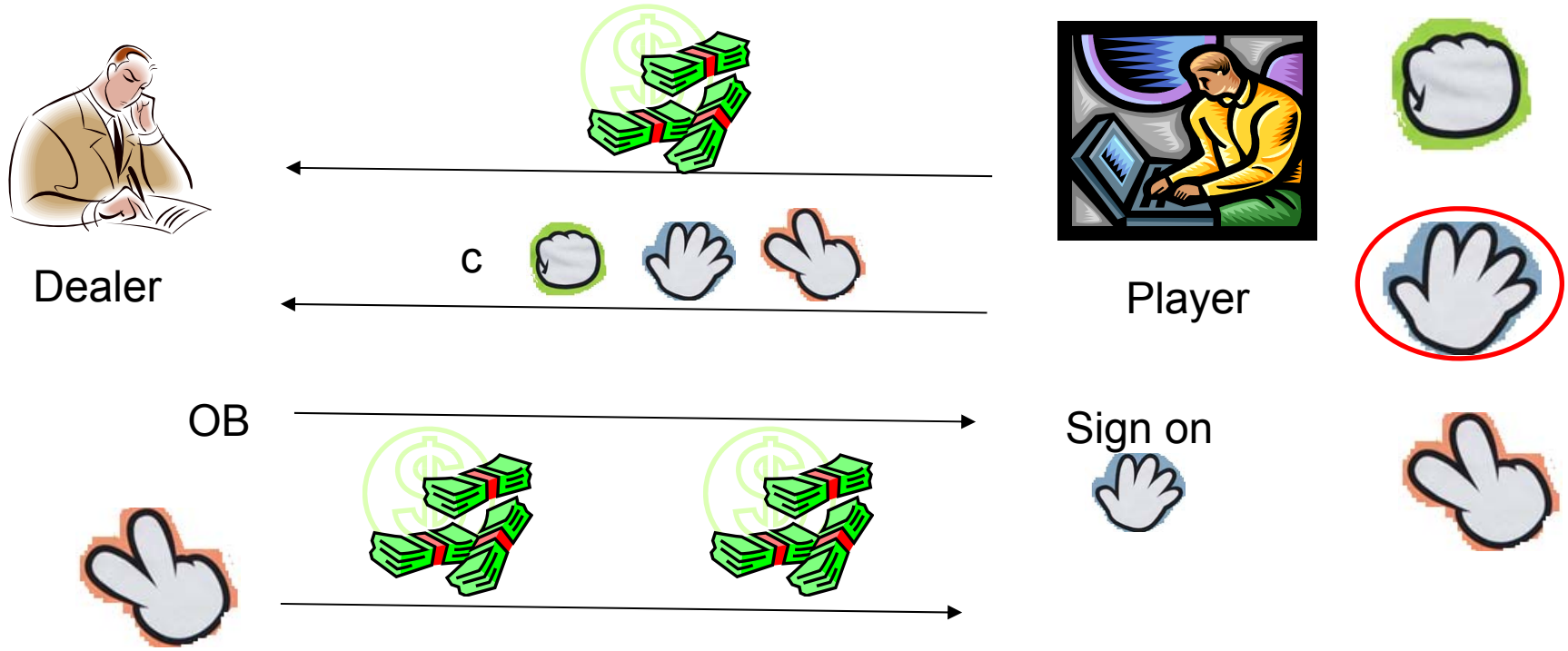
Application to E-voting

- In replace of blind signatures

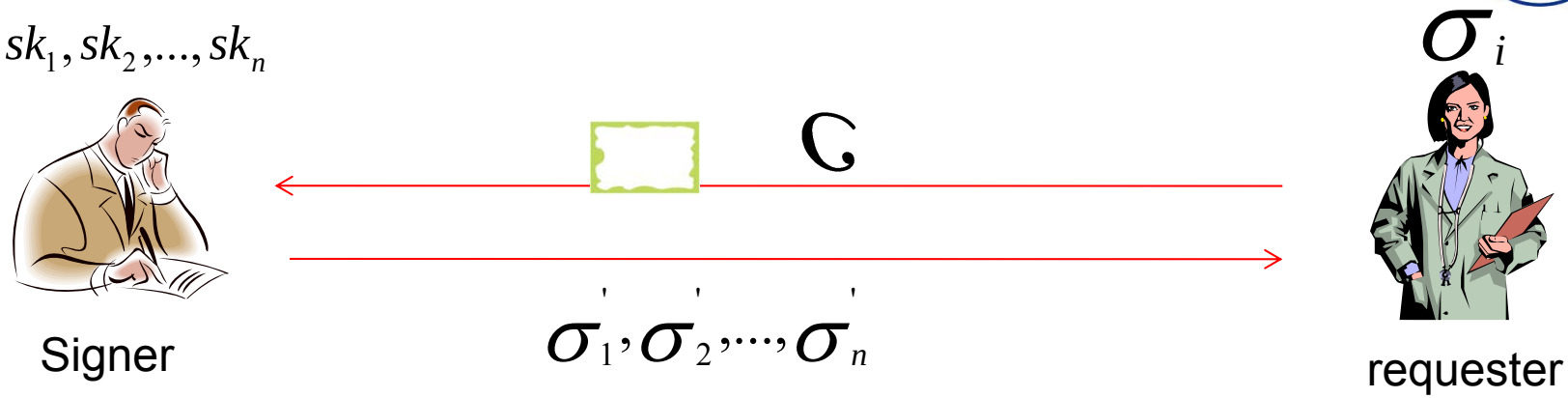


Possible applications

- Fair Games
  - eg., On-line Lottery, finger game, etc.,



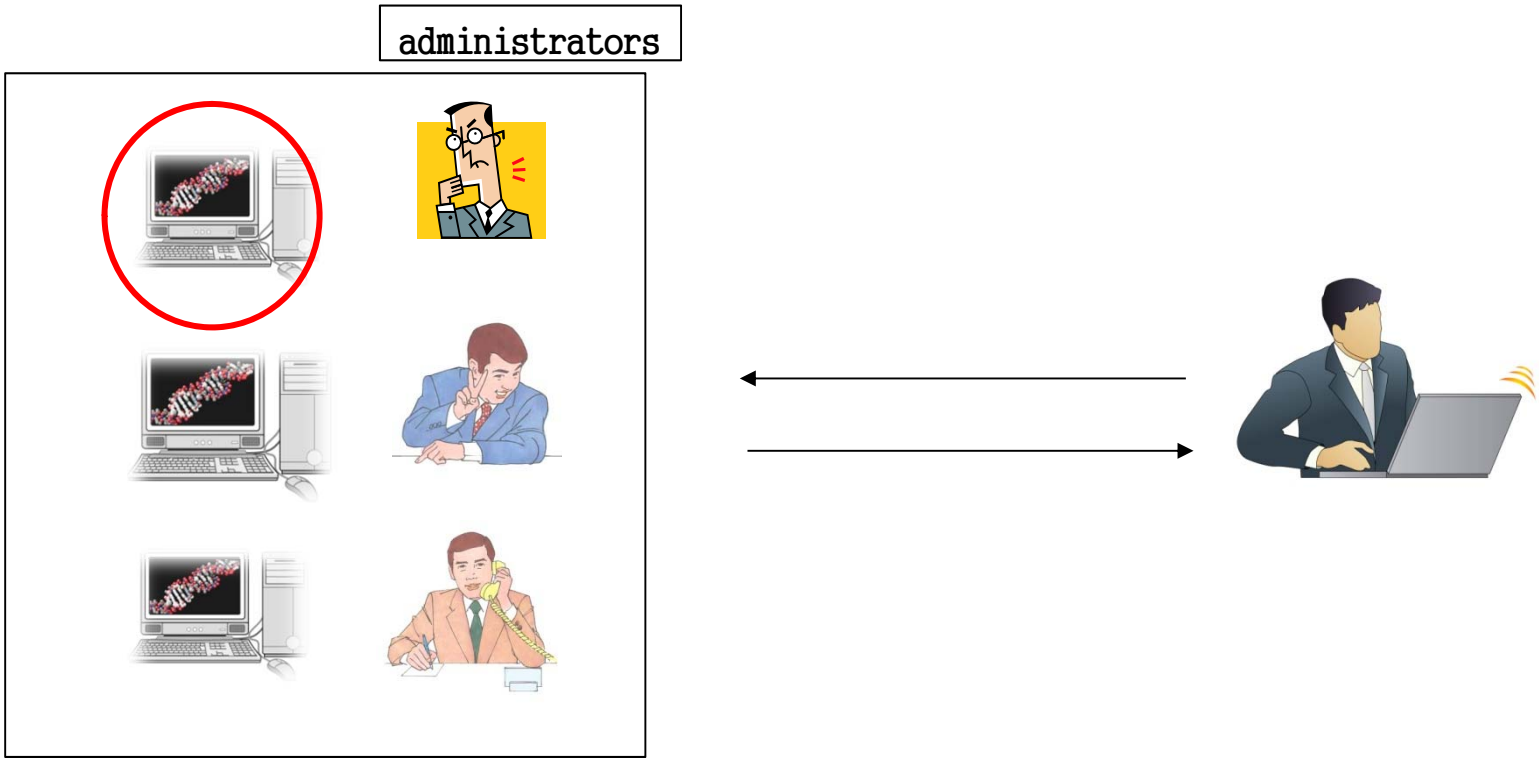
Oblivious Signature with n Keys



- By executing the protocol, the recipient R can get a message signed with one of *n* keys which is chosen by himself
- The possible signers, even the holder of the accepted keys, cannot find out with which key the message is got signed

Possible application

- Access to sensitive databases



1. Which database interests the user is kept secret to the administrators

2. Get permit to access one of the databases from the administrators

Our Contribution

- Previous reference does not crisply formalize
  - The notion of oblivious signatures
  - The model of the schemes
  - The adversary model of the schemes
- We give formal definition of oblivious signatures
- We define the security/adversary model of the schemes
- We propose more efficient oblivious signature schemes

- R. Tso, T. Okamoto, and E. Okamoto, 1-out-of-n oblivious signatures, In proceedings of ISPEC'08, Lecture Notes in Computer Science Vol. 4991, pp.45—55, 2008

Review of Schnorr Signature Scheme

- Setting: $H : \{0,1\}^* \to Z_q^*.$

  p, q : two large primes s.t $q \mid p-1$,

  $g \in Z_p^*$ of order q,

- Signer's Key: $(x_A, y_A) : x_A \in Z_q^*, y_A = g^{x_A} \bmod p.$
- To sign a message $m \in \{0,1\}^*$:

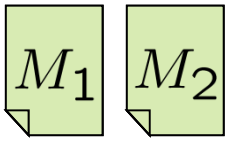
  $k \leftarrow_R Z_q^*, \quad r = H(m, g^k \bmod p), \quad s = k - x_A r \bmod q.$
- The signature is $\sigma = (r, s)$.
- A user *R* accepts the signature if and only if

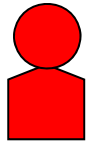
  $r = H(m, y_A^r g^s \bmod p).$

Proposed Scheme (based on Schnorr sig.)

: Signer

Messages





: Recipient

$PK: y = g^x, g, h \in Z_p^*, p, q \in N_{prime}$

$SK: x \in_R Z_q, q|(p-1)$

$\ell \in \{1,2\},\ r \in_R \mathbb{Z}_q$

c ←

$c = g^r h^\ell mod p$

$k_1, k_2 \in_R Z_q^*$

$K_i = g^{k_i} mod p, i = 1,2$

$\hat{e}_i = H(m_i, K_i c/(gh)^i mod p)$

$\hat{s}_i = k_i - x\hat{e}_i mod q$

$(\hat{e}_1, \hat{s}_1)$

$(\hat{e}_2, \hat{s}_2)$ →

$e = \hat{e}_\ell$

$s = r - \ell + \hat{s}_\ell \ (mod q)$

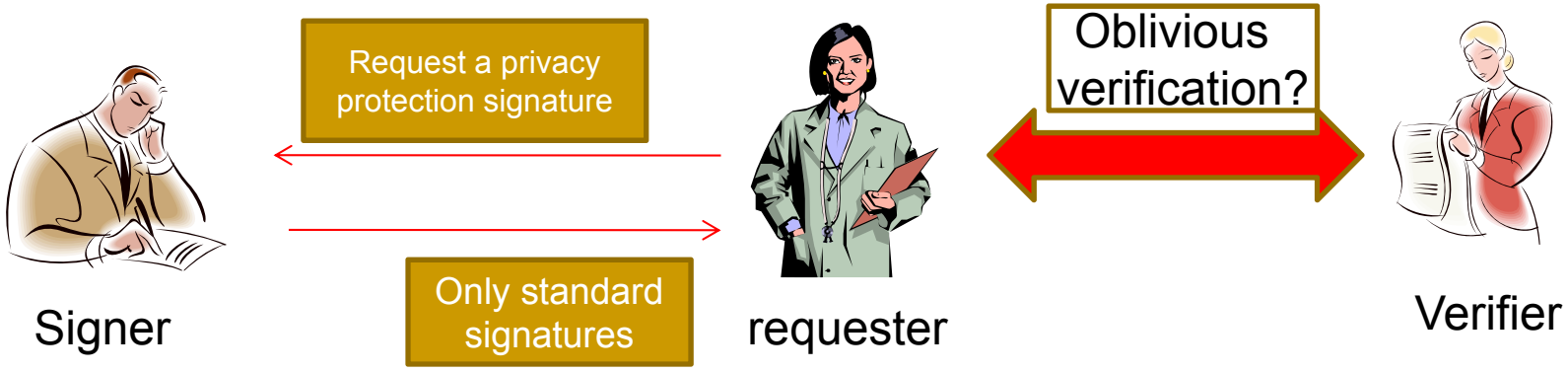
Security

- Security for signers: Unforgeability
  - It is computationally infeasible for any adversary to produce any valid signature without knowing the private key of the original signer (EUF-ACMA secure)
- Security for recipients: Ambiguity in selected message
  - It is unconditionally infeasible for any attacker S to find out which one of the messages is chosen by a recipient R

Performance Comparison

Scheme	Communication Cost (bits)			Computation			Numbers of Communications
	S → R	R → S	R → V	S	R	V	
DSA-OT	2368n	1024	320	5nEx	3Ex	2Ex	2
Chen's scheme	3232n	160	7488	3nEx	(2n+10) Ex	8Ex	3
Proposed scheme	320n	160	320	2nEx	(2n+2) Ex	2Ex	2

Three-Entity Case



- A unfriendly signer who will sign using only conventional digital signatures such as DSA, ElGamal, or Schnorr

Motivation

- During the course of a person's lifetime, one can find many cases in which a formal document /certificate is required to be presented to a third party
- Usually, those certificates contain a lot of personal information
  - Some of them may be necessary to be presented in one case but not in other cases

Motivation

- Due to the increased awareness of privacy issues, an owner of a certificate may wish that
  - Only the limited information which is necessary for that specific case can be verified
  - While other information included in the certificate which is irrelevant to the case cannot be verified by a third party

Solutions to the above Mentioned Problem

- Ask the CA issuing the certificate to issue a copy of the certificate case by case
  - Whether this kind of a friendly CA exists
- The adoption of an anonymous credentials
  - An interactive protocol is required
- The adoption of an sanitizing signature scheme
  - Need the agreement of the original author to perform such an division and extraction processes for the user

Our Solution- Universal 1-out-of-n Signature

- A US$^{(1,n)}$ is a solution to deal with the above mentioned problem without the assistance of the original signer
- In a US$^{(1,n)}$, a signer signed a document m by a standard digital signature and sent to a user
- Without a modification to the signature, anyone can verify the correctness of the signature
- When necessary, the user holding the signature can modify the signature into a US$^{(1,n)}$ in which n different signatures on l (<=n)different messages signed by k (<=n)different signers are involved

Features of a US$^{(1,n)}$

- Message Ambiguous: n different signatures on n different messages (including m) signed by the original signer
- Signer Ambiguous: n different signatures on the same message m signed by n different signers (including the original signer)
- Message and Signer Ambiguous: n different signatures on n different messages (including m) signed by n different signers (including the original signer)
- Set-up-free: the US$^{(1,n)}$ can be made without the knowledge or consent of any users

Universal 1-out-of-n Signatures

Signer

User

Verifier

M_1
Alice

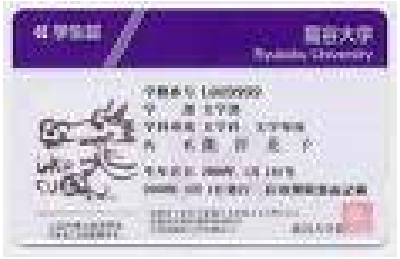
M_1
Alice

M_2
Bob

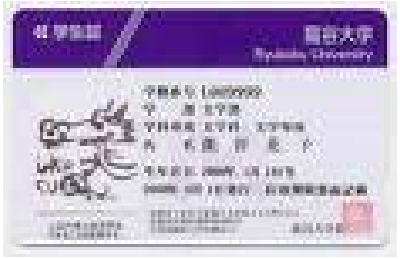
M_3
Cindy

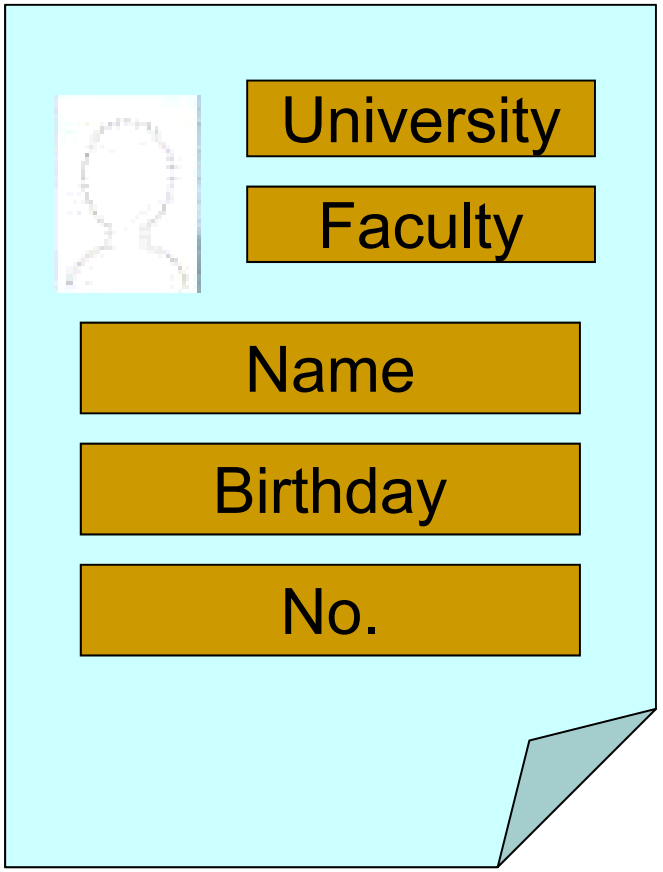
I see. But which one is real?

Possible Applications (1/4)

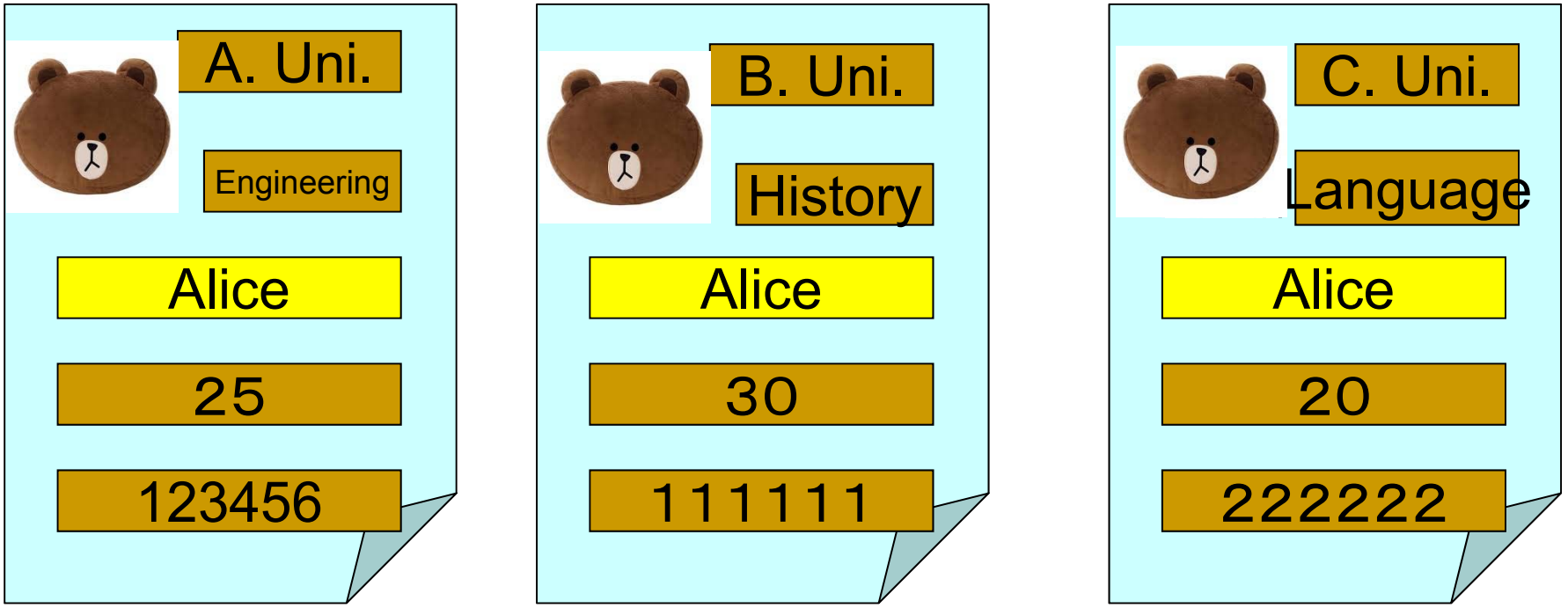


Possible Applications (2/4)



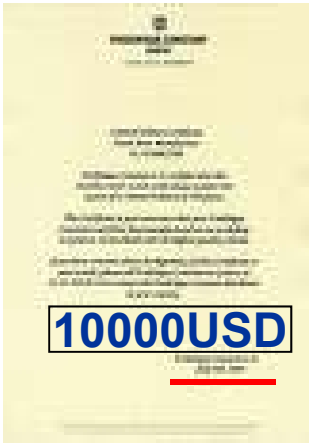


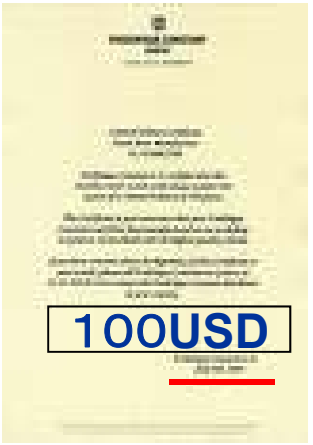
Possible Applications (3/4)



Possible Applications (4/4)

- Show a signed contract but ambiguous some information






娱乐时尚 国际在线
WWW.CRI.CN
gb.chinabroadcast.cn 资料


中華民國國民身分證
姓 名
出生年月日 民國 50 年 7 月 23 日
性別 女
發證日期 民國95年2月3日（南市）換發
統一編號


中華民國國民身分證
姓 名
出生年月日 民國 51 年 7 月 23 日
性別 女
發證日期 民國95年2月3日（南市）換發
統一編號

. . . . . .


中華民國國民身分證
姓 名
出生年月日 民國 75 年 7 月 23 日
性別 女
發證日期 民國95年2月3日（南市）換發
統一編號


中華民國國民身分證
姓 名
出生年月日 民國 76 年 7 月 23 日
性別 女
發證日期 民國95年2月3日（南市）換發
統一編號


TOYOTA
Samaniya


中華民國國民身分證
姓 名
出生年月日 民國 年 7 月 23 日
性別 男
發證日期 民國95年2月3日（南市）換發


中華民國國民身分證
姓 名
出生年月日 民國 年 7 月 23 日
性別 女
發證日期 民國95年2月3日（南市）換發

Proposed Scheme

- System Setting: $H : \{0,1\}^* \rightarrow Z_q^*.$

  p, q : two large primes s.t $q \mid p-1$,

  $g \in Z_p^*$ of order q,

- Signer Key: $(x_A, y_A) : x_A \in Z_q^*, y_A = g^{x_A} \bmod p.$
- To sign a message $m^* \in \{0,1\}^*$:

  $k \leftarrow_R Z_q^*, \quad r^* = H(m^*, g^k \bmod p), \quad s^* = k - x_A r^* \bmod q.$
- The signature is $\sigma^* = (r^*, s^*).$
- A user *R* accepts the signature if and only if

  $r^* = H(m^*, y_A^{r^*} g^{s^*} \bmod p).$

Proposed Scheme

- Conversion: $m^* \in M = \{m_1, \cdots, m_n\}, y_A \in PK = \{y_1, \cdots, y_n\}.$
  - For $m^* : \delta^* \leftarrow g^{s^*} \bmod p.$ $Schnorr$ Sig. $:(r^*, s^*)$
  - For $m_i \in M \setminus \{m^*\}$:

$$\alpha_i \leftarrow_R Z_p^*, \quad r_i \leftarrow H(m_i, \alpha_i), \quad \delta_i \leftarrow \alpha_i \Big/ y_i^{r_i} \bmod p.$$

  - More over, make a witness hiding proof $WHP(s^*)$ for s^*.
  - The *1*-out-of-*n* signature is

$$\left(WHP(s^*), (m_1, r_1, \delta_1), \cdots, (m_i, r_i, \delta_i), \cdots, (m_n, r_n, \delta_n)\right).$$

- Oblivious Verification:
  - Check if $r_i = H(m_i, y_i^{r_i} \delta_i), \qquad 1 \le i \le n.$
  - Check the correctness of $WHP(s^*)$.

Witness Hiding Proof

- The purpose of witness hiding proof WHP(s) is to convince a verifier that the prover knows some witness s for input δ.

What is a Zero Knowledge Proof?

- 1985年Goldwasser, Micali and Rackoff所提出
- 概念
  - 在不洩漏某個特定資訊的情況下，也能證明自己確實知道此特定資訊
- Wikipedia
  - In cryptography, a **zero-knowledge proof** or **zero-knowledge protocol** is an interactive method for one party to prove to another that a (usually mathematical) statement is true, without revealing anything other than the veracity of the statement.

What is a Zero Knowledge Proof?

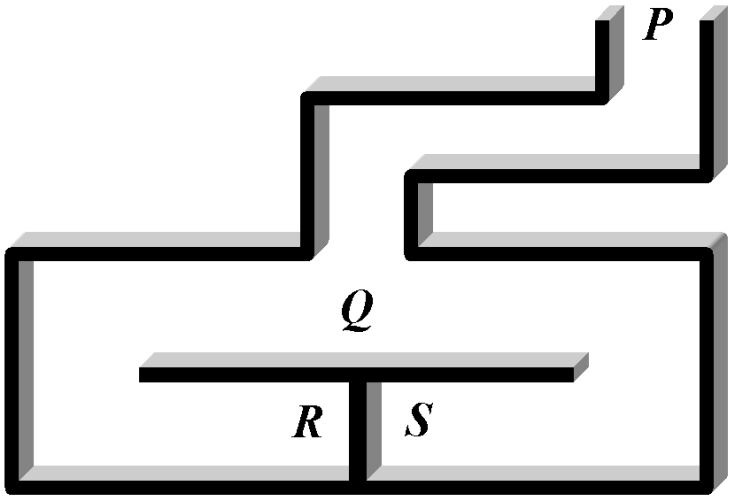


Image from RSA Labs [1]
http://www.rsasecurity.com/rsalabs/node.asp?id=2178

- Classic Example:
  - Ali Baba's Cave (zero-knowledge cave)
- Alice wants to prove to bob that she knows how to open the secret door between R and S.
  - Bob goes to P
  - Alice goes to R or S
  - Bob goes to Q and tells Alice to come from one side or the other of the cave
  - If Alice knows the secret, she can appear from the correct side of the cave every time
- Bob repeats as many times until he believe Alice knows to open the secret door

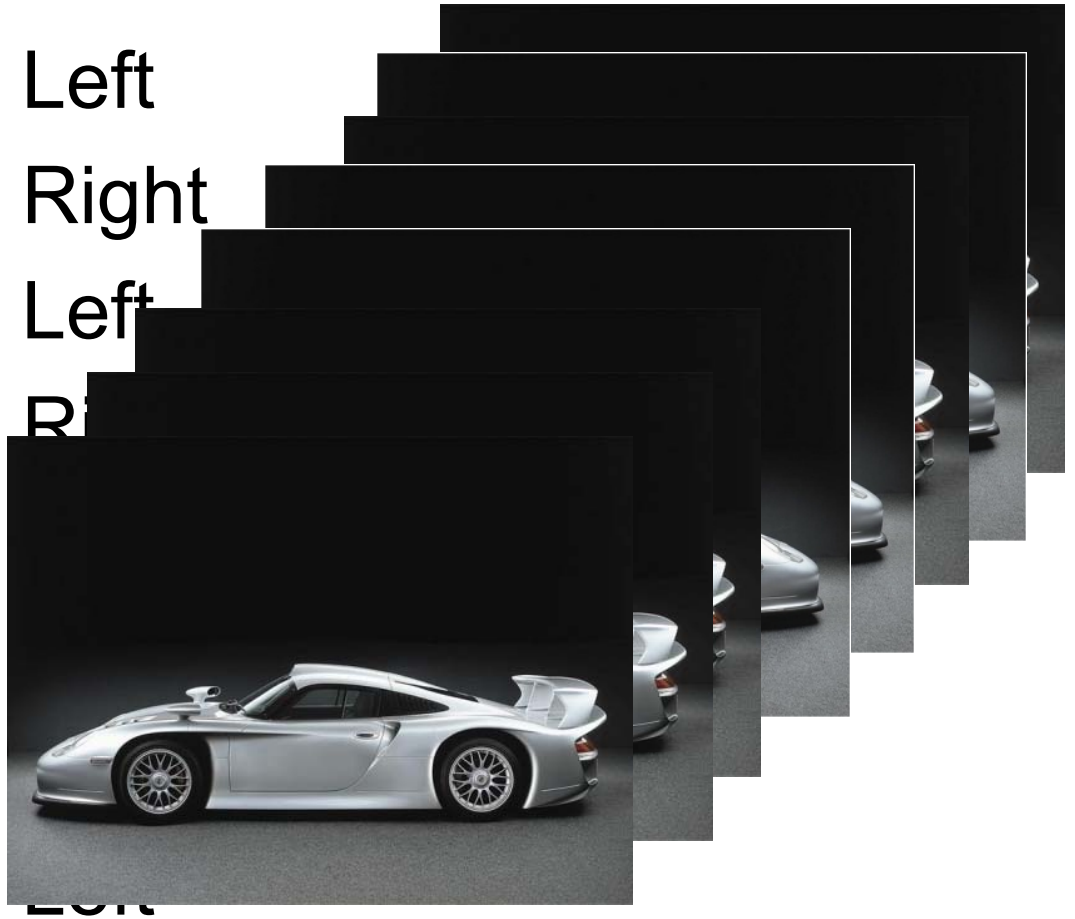
Why called Zero-knowledge

- At the end of the protocol
  - Bob will believe that Alice really knows the secret to open the door
  - Bob cannot transfer this proof to a third party
  - Bob got no information about the secret

Prove of Ownership of a Car

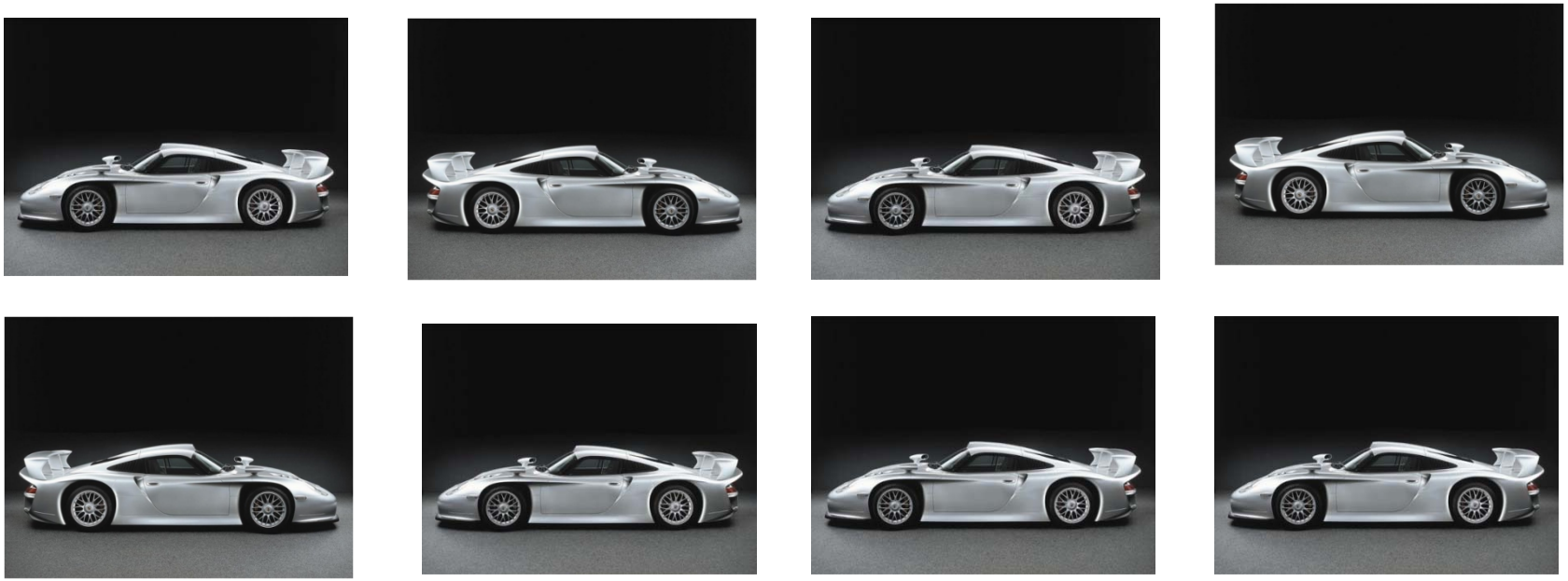
Prove of Ownership of a Car

- Day 1: Head Left
- Day 2: Head Right
- Day 3: Head Left
- Day 4: Head R
- Day 5: Head
- Day 6: Head
- Day 7: Head
- Day 8: Head Left



Prove of Ownership of a Car

- Bob cannot transfer this proof to a third party



Security

- Unforgeability: based on the security of the Schnorr signature and the WHP

- Ambiguity：unconditionally secure

Relation to other Signatures

US$^{(1,n)}$

Signer

User

Verifier

n messages

n keys

Relation to other Signatures

US$^{(1,n)}$

Signer

User

Verifier

1 messages

n keys

universal 1 out of n signature

ring signature

Relation to other Signatures

US$^{(1,n)}$

Signer

User

Verifier

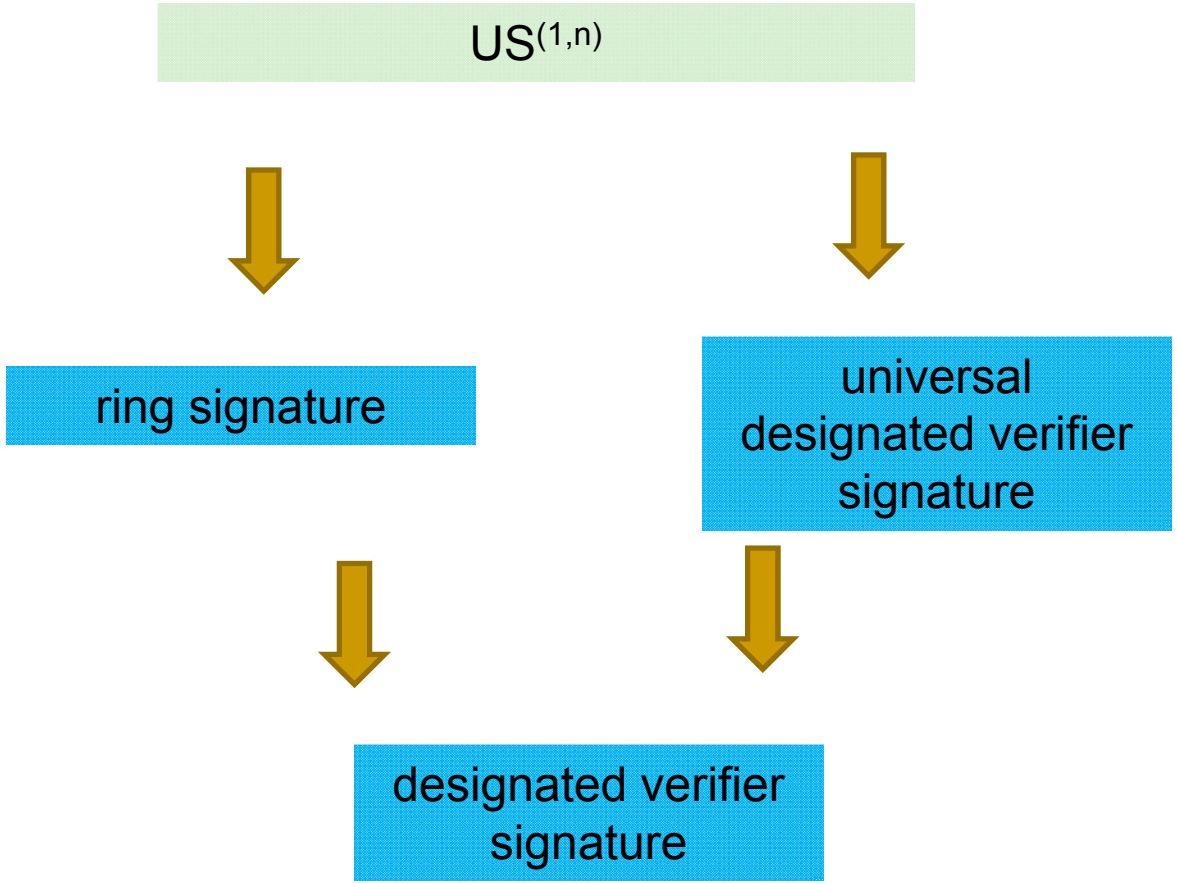
1 messages

2 keys

universal 1 out of n signature

universal designated verifier signature

Relation to other Signatures



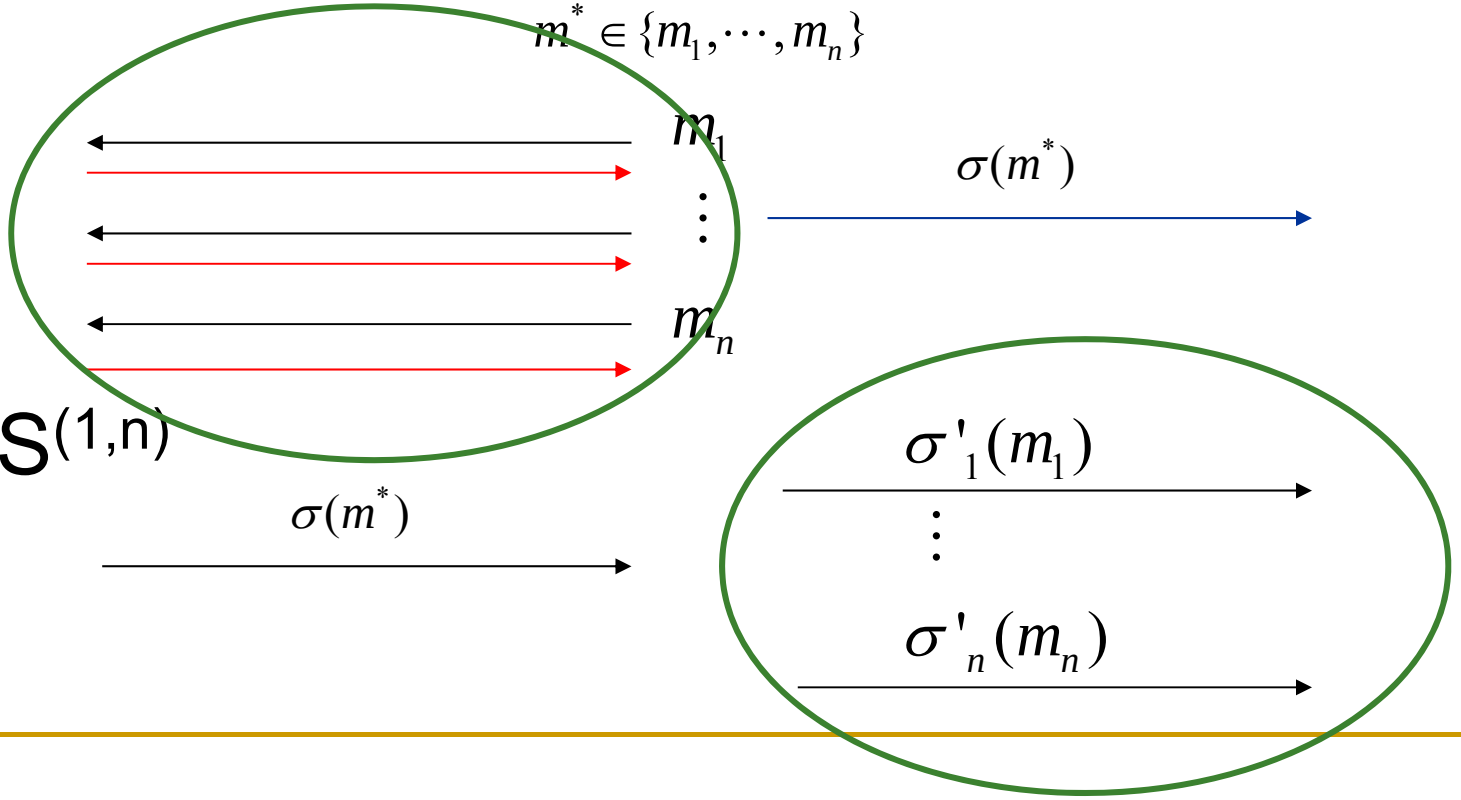
Extensions:
Oblivious Signature +US$^{(1,n)}$

Signer

User

Verifier

- US$^{(1,n)}$



Conclusion

- Many kinds of signature schemes providing privacy protection are introduced
- To protect personal information against signers, we introduced a new oblivious signature
- To protect personal information against verifiers, we introduced a new type of signature scheme called US$^{(1,n)}$
- A secure digital signature does not allow any alternation on the signed document, so we can only ambiguous the contents of a message or ambiguous the real signer
- In this way to prevent or discourage the abuse of personal information by a third party

- Thank you!