Security and Encryption

Jane Hsu

 1

The Internet Is An Insecure Place

- Many protocols do not provide any security.
- Viruses, worms, Trojan horses etc.
- Client/server applications often require transmission of user identity/passwords.
- "Crackers" may sniff passwords and other sensitive information off the network.
- Need to restrict control access privileges
- "Crackers" also actively exploit many system vulnerability or "security holes" to inflict damages or to gain access to valuable information.
- *No system is totally immune to security problems.*

 2

Solution?

- There is nothing more secure then a computer which is not connected to the network --- and powered off!
- But…
- These restrictions are simply unrealistic and unacceptable.

 4

Firewalls

Problems

- Firewalls assume that "the bad guys" are on the outside – a bad assumption!
- Firewalls restrict how your users can use the Internet.

 5

Web Security

- Content security
  - Digital rights management (DRM)
  - Encryption
  - Digital watermark
- Network security
  - Encryption
    - Symmetric encryption: DES
    - Asymmetric encryption: RSA
  - IP security
- Digital signature/envelope
- Digital Certificates and certification authorities

 6

Security Threats

- 系統入侵
- 資料竊取
- 資料竄改
- 身份冒用
- 惡意破壞

 7

電子商務安全性的條件

- 存取控制（Access Control）
  - 必須能防止非法使用者或訊息任意進入，同時亦能授權合法登入者，具有特定的使用權限
- 資料保密性（Confidentiality）
  - 必須能防止非法的接收者竊取傳送並發現明文
- 資料完整性（Integrity）
  - 接收方可確認所收到的資訊無被篡改或部分取代之虞
- 資料來源驗證性（Authentication）
  - 可驗證接收到的資訊確實由合法的發送方所傳送，而非別人偽造或利用以前的訊息來傳送
- 不可否認性（Non-Repudiation）
  - 發送方於傳送完資訊後，不可否認其傳送過資訊之事實

 8

網路安全性管理工具

 9

何謂密碼系統？

- 密碼就是發送訊息的一方，秘密地將信息的原文更改成無法輕易辨識的密文，再將密文不做任何特殊保護地傳送。 如此一旦密文一旦落入攻擊者手中時，信息的原文仍然受到保護。當密文傳送到收件者手中，合法的收件者卻能巧 妙地恢復原文。

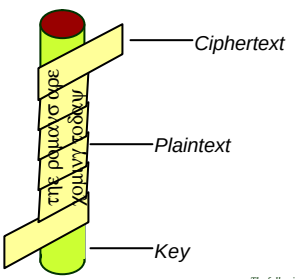
 10

German Enigma Cipher Machine

- In 1918, Arthur Scherbius filed for a patent for Enigma Cipher Machine and offered it to the German Navy.
- In 1926, German navy begins using Enigma Machine, lightly modified from a commercial model.
- In 1930, German armed forces introduced a significantly modified military model.
- In1932, Marian Rejewski, a 27-year-old Cryptanalyst (Cipher Bureau of the Polish Intelligence Service in Warsaw, Poland) mathematically determined the wiring of the Enigma's first rotor. Since 1933 Poland was able to read thousands of German messages encrypted by the Enigma Machine.
- The National Security Agency Museum in Fort George Meade, Maryland has a real WW2 Enigma Cipher Machine on display.

 11

Simple Cryptography



The following slides are adapted from presentations by Lincoln Stein, MIT & KL Lin, NTU

 12

Caesar Cipher

ABCDEFGHIJKLMNOPQRSTUVWXYZ

rotate 13 positions

NOPQRSTUVWXYZABCDEFGHIJKLM

THE GOTHS COMETH — *Plaintext*

13 — *Key*

FUR TAFUE PAYRFU — *Ciphertext*

 13

Rotating Key Cipher

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
BCDEFGHIJKLMNOPQRSTUVWXYZA
CDEFGHIJKLMNOPQRSTUVWXYZAB
DEFGHIJKLMNOPQRSTUVWXYZABC
EFGHIJKLMNOPQRSTUVWXYZABCD
FGHIJKLMNOPQRSTUVWXYZABCDE
GHIJKLMNOPQRSTUVWXYZABCDEF
HIJKLMNOPQRSTUVWXYZABCD...
```

SOUND THE RETREAT — *plaintext*

DEADFED — *key*

VSUPC XKG UEWWEX — *ciphertext*

 14

General Principles

- Longer keys make better ciphers
- Random keys make better ciphers
- Good ciphers produce “random” ciphertext
- Best keys are used once and thrown away

 15

密碼系統的演進

- 早期的密碼系統其關鍵在於所使用的演算法只有發文與收文的兩方知道，如果其他人也知道的話，機密性將不復存在。這種將機密性建立在密碼演算法的密碼系統，只適用於封閉性的環境，但現今網路通訊是開放性的，因此必須使用共通的密碼系統，也就是說密碼演算法必須公開，而任何人都可以使用
- 為了因應這樣的需要，現代的密碼系統使用了鑰匙 (key) 的概念

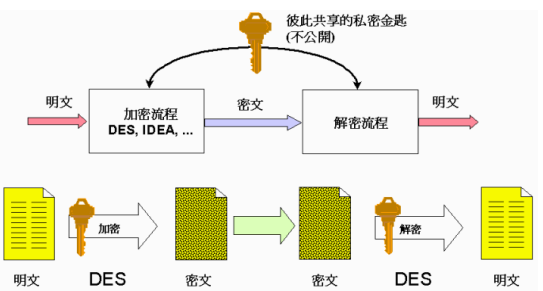
 16

金鑰（Key）

- 所謂「金鑰」實際上僅是一長串難以記憶的 0 與 1 的組合，可以儲存於電腦的硬碟、磁片或 IC 卡片中
- 主要的功能是在文件透過網路傳輸的過程中，由特定的密碼演算法利用金鑰將傳輸文件編碼加密，收件者在接獲文件時，透過金鑰將文件解密還原
- 由於使用的演算法是公開的，因此必須確保演算法本身是安全的、無法破解，並且需要保護鑰匙
- 雖然鑰匙是一連串 0 與 1 的組合，若使用暴力入侵，得嘗試各種不同 0 與 1 的組合。但假設鑰匙的長度為 N 位元，則有 2^N 種不同的鑰匙。因此鑰匙的長度 (位元數) 越長，理論上安全性越佳

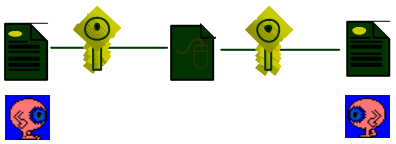
 17

對稱式加密系統流程



 18

Symmetric (Private Key) Cryptography

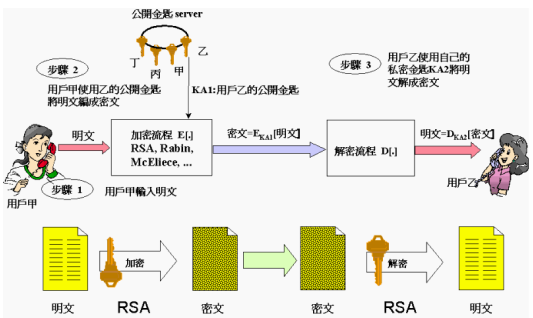


- Examples:
  - DES (Data Encryption Standard) 56-bit key
  - IDEA (International Data Encryption Algorithm) 128-bit key
  - AES (Advanced Encryption Standard)
  - RC4, RC5, Skipjack
- Advantages: fast, ciphertext secure
- Disadvantages: must distribute key in advance, key must not be divulged

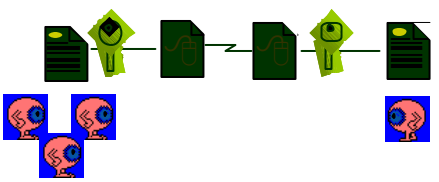
DES: Data Encryption Standard

- Widely published & used - federal standard
- Complex series of bit substitutions, permutations and recombinations
- Basic DES: 56-bit keys
  - Crackable in about a day using specialized hardware
- Triple DES: effective 112-bit key
  - Uncrackable by known techniques

非對稱式加密系統流程



Asymmetric (Public Key) Cryptography



- Examples: *RSA, Diffie-Hellman, ElGamal*
- Advantages: *public key widely distributable, does digital signatures*
- Disadvantages: *slow, key distribution*

RSA

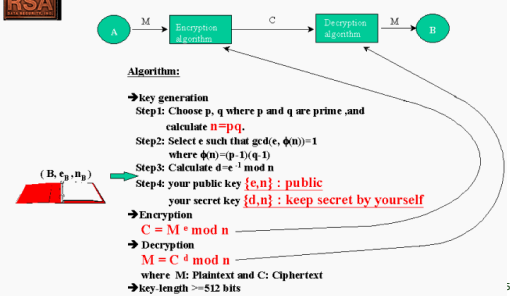
- RSA 是 Rivest、Shamir 和 Adelman 的縮寫，這三位數學家在 1977 年共同發表出特殊加密的演算法
- 這種演算法主要以兩個質數作為加密與解密的兩個鑰匙，這兩個鑰匙分別稱為公開鑰匙和私人鑰匙，鑰匙的長度（位元數）決定了加密編碼的複雜度，只要RSA鑰匙長度增加 (512~1024 bits)，要破解RSA得大費周章，因此它算是相當安全的保密系統

RSA 加解密流程

- 找兩個很大的質數 p,q
- n=pxq z=(p-1)x(q-1)
- 找一個與z互質的整數d
- 找一個整數e使得 (exd) mod z = 1
- Public key: (e,n), Secret key: (d,n)
- 密文: $C=P^e \bmod n$
- 解密: $P=C^d \bmod n$

RSA 加解密流程

☛ Public key encryption algorithm (Asymmetric) ,1977



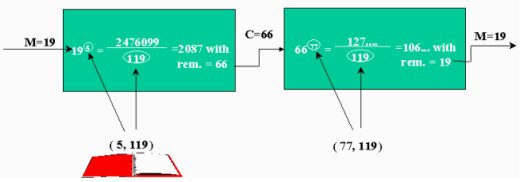
Algorithm:

➔key generation
Step1: Choose p, q where p and q are prime ,and calculate n=pq.
Step2: Select e such that gcd(e, ϕ(n))=1 where ϕ(n)=(p-1)(q-1)
Step3: Calculate $d=e^{-1} \bmod n$
Step4: your public key {e,n} : public
your secret key {d,n} : keep secret by yourself
➔Encryption
$C = M^e \bmod n$
➔ Decryption
$M = C^d \bmod n$
where M: Plaintext and C: Ciphertext
➔key-length >=512 bits

RSA 加解密範例

Example:

1: Choose p=7 and q=17.
2: Calculate n=pq=7x17=119.
3: Calculate ϕ(n)=(p-1)(q-1)=96.
4: Select e=5 (relatively prime to ϕ(n)).
5: Determine d such that de=1 mod 96 and d< 96; d=77. since 77x5=4x96+1.



Public Key Encryption: The Frills

Frills

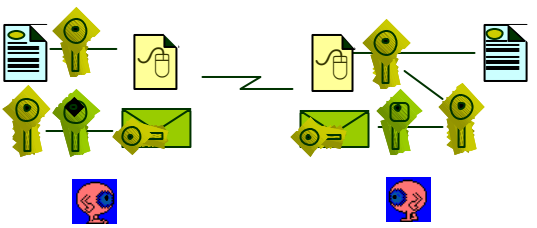
- Fast encryption/decryption
- Authentication of sender
- Verification of message integrity
- Safe distribution of public keys

Technique

- Digital envelopes
- Digital signature
- Message digests
- Certifying authorities

 27

Digital Envelopes



 28

數位簽章

- 數位簽章是以一組公開金鑰與私密金鑰對來驗證個人身分
- 私密金鑰須由客戶妥善保管，不可洩漏他人，而公開金鑰經過CA認證後，可作為驗證私密金鑰的憑據

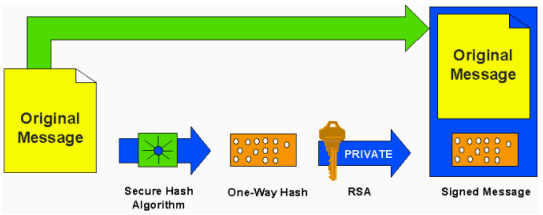
 29

數位簽章的安全保證

- 資料完整性(Integrity)
  - 文件接收者透過數位簽章之核對可確保此文件的完整性，避免被篡改、重送、遺失
- 資料來源辨識(Authentication)
  - 文件接收者可確認此文件之發送者的身分，避免被冒名傳送假資料
- 資料隱密性(Confidentiality)
  - 文件可以金鑰加解密，以達到保密的安全保證
- 不可否認性(Non-repudiation)
  - 因為只有文件發送者知道自己的私密金鑰，而且文件具有發送者之數位簽章，使其無法否認發送此文件的事實

 30

產生數位簽章



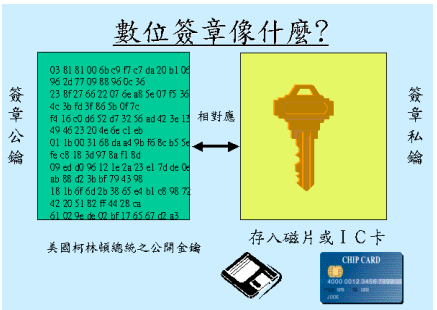
 31

訊息摘要

- 赫序函數(Hash Function)則可將輸入的資料濃縮成較短且為特定長度的結果
- 任意的文件資料經過一個單向赫序函數計算後，可以產生一串固定長度的資料，因為不太可能設計另一份文件資料而在同一函數運算後產生相同的結果，所以該結果可視為原始文件資料的特徵值，稱為數位指紋 (digital fingerprint) 或訊息摘要 (message digest)。

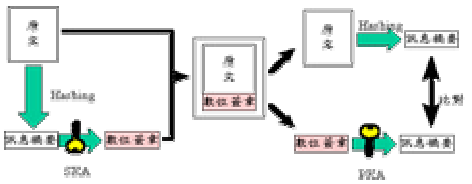
 32

數位簽章像什麼？



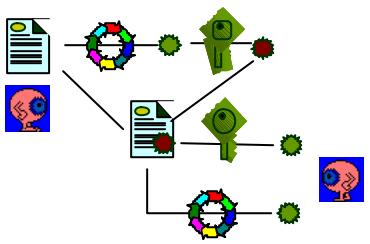
 33

數位簽章運作的基本概念



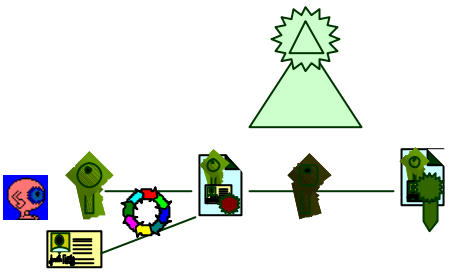
 34

Message Digests



 35

Certifying Authorities



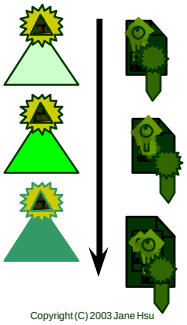
 36

安全認證服務系統

- 交易認證中心
  - 以安控標準提供網路傳輸與系統安全，為網路支付安全把關
- 金鑰認證中心
  - 以認證標準提供私法人憑證、自然人憑證、交易憑證之產製及核發，建立認證機制

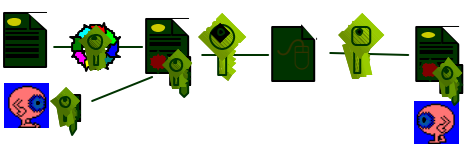
 37

Hierarchy of Trust



 38

Secure, Verifiable Transmission



 39

Public Key Cryptography on the Web

- Secure Socket Layer (SSL)
  - Netscape Communications Corporation
- Secure HTTP (SHTTP)
  - Commerce Net
- SET (Secure Electronic Transaction)

 40

SSL

- SSL(Secure Socket Layer)網路安全協定
- 由Netscape網景公司開發，用來保護網上使用瀏覽器交易安全的規格，因為各家瀏覽器軟體都支援它的功能，因此是目前在網路上最受到廣泛採納的一種
- SSL傳輸的資料也是經過鑰匙加密的處理，雖然有可能被第三者截取，卻很難讀取資料內容，而且經過加密的資料可以保持完整，不會受到竄改或破壞

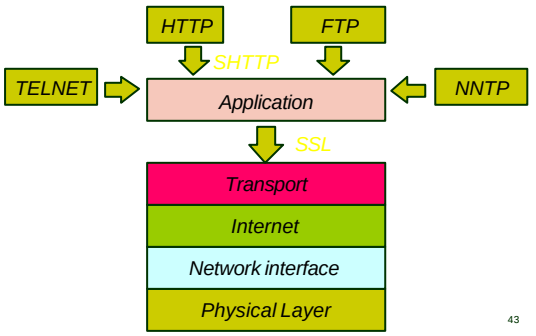
 41

SSL and SHTTP, *similarities*

- RSA public key cryptography
- MD5 message digests
- Variety of private key systems
  - Strong cryptography for use in U.S.
  - Weakened cryptography for export.

 42

SSL and SHTTP, *differences*



43

SET

- SET (Secure Electronic Transaction)安全電子交易
- 一種在網際網路進行付款交易的安全機制
- 其規格採用RSA(1024 bits)非對稱式運算法則（即利用公鑰及私鑰分別加密與解密）結合DES對稱式運算法則(加、解密為相同之基碼)為安全方案，用以保護網路付款交易之安全及隱密性

 44

SET

- SET由萬事達與威士兩個信用卡組織主導，結合IBM、微軟、網景等國際資訊廠商共同推廣的網路電子商務交易安全標準
- 商家可以利用SET確認消費者身分，但不會看見消費者信用卡的號碼，因此消費者在網上沒有被盜刷的危險
- 不過SET的系統太過複雜，建置的成本過高，所以目前電子商務上的保密協定，還是以RSA、SSL系統為主。

 45

Secure Servers

- Netscape Commerce Server
- Microsoft Internet Information Server
- WebSite Professional
- Quarterdeck/WebSTAR Professional
- OpenMarket Secure Server
- Apache SSL
- Many others!

 46

Secure Servers: Costs

- Server software
  - Requires license from RSA Data Security
  - Often free for noncommercial use
  - $200-$1000 for commercial use
  - Export forbidden
- Server certificate
  - $290 for initial certificate
  - $95 each additional servers
  - $75 annual renewal fee

 47

Secure Servers: Set-up

- Install & configure server software
- Create “distinguished name” for your site
- Fill out server certificate application at Verisign’s Web site
  - Pay the piper
- Generate key pair and “certificate request” Mail certificate request to Verisign
- Install signed certificate on your server

 48

Using SSL

 49

SSL Failures

- Two well-publicized incidents in 1995
- 40-bit secret key used in export versions vulnerable to brute force attack
  - Single encrypted message vulnerable to cracking in a few weeks on a network of workstations
  - Specialized hardware (probably) can crack in a matter of hours
- Implementation problem
  - Navigator 2.0 used predictable random number generator to generate secret keys
  - Messages crackable in a few minutes on conventional workstation

 50

Web Encryption Isn't Panacea

- Protect data at browser side & server side
- Server certificates vouchsafe name of server but not honesty of merchant!
- Protect integrity of browser & server software

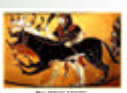
 51

Alternative architectures

- Separate Layer
  - Over TCP: SSL
  - Over IP: IPSec
- Application-Specific
  - SHTTP
- Parallel
  - Kerberos; Kerberos with TLS?

 52

Kerberos



- KERBEROS was the fierce watchdog of Hades. It was depicted as a three-headed dog with a serpent's tail, a mane of snakes, and a lion's claws.
- To provide strong authentication for *client/server applications* by using secret key cryptography.
- A client can prove its identity to a server (and vice versa) across an insecure network connection.
- Client/server can also encrypt all of their communications to assure privacy and data integrity as they go about their business.
- Free implementation available from MIT http://web.mit.edu/kerberos/www/

 53

Reference URLs

- SSL Protocol
  - http://home.netscape.com/newsref/std/SSL.html
- SHTTP Protocol
  - http://www.eit.com/projects/s-http/
- Verisign
  - http://www.verisign.com/
- RSA Data Security
  - http://www.rsa.com/

 54