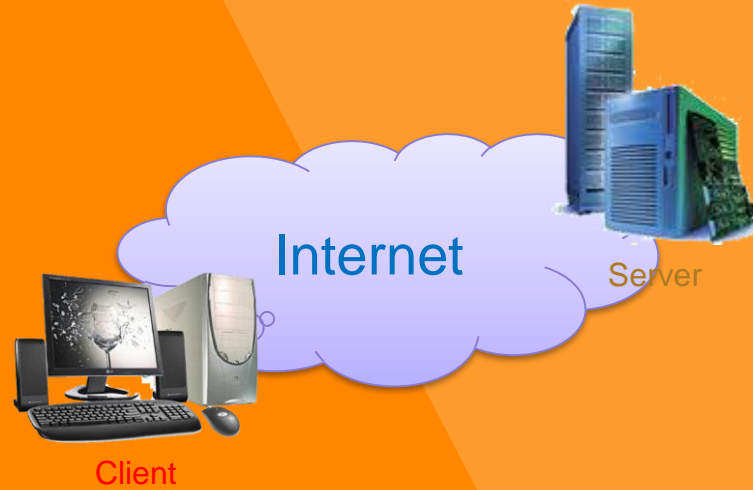


EC Security

KHOA CÔNG NGHỆ THÔNG TIN
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN



- ▶ Giới thiệu
- ▶ Các vấn đề bảo mật trong EC
- ▶ Các loại hình tấn công
- ▶ Một số mối đe dọa đến hệ thống EC
- ▶ Chính sách bảo vệ hệ thống



Một số mối đe dọa đến hệ thống EC
Bảo mật trong EC

▶ Trang web

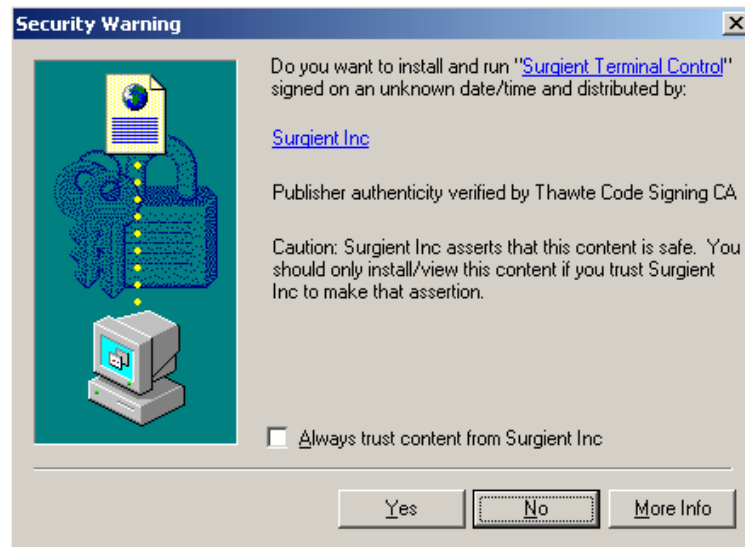
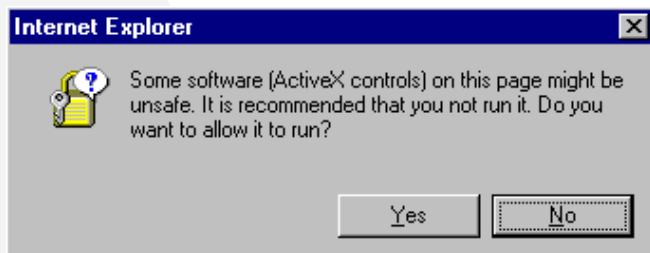
- ▶ Hiển thị **nội dung**
- ▶ Cung cấp các liên kết (**link**)

▶ Active content

- ▶ Đoạn chương trình được nhúng vào trang web và **tự động thực hiện**
 - ▶ Tự động tải về và mở file
- ▶ Cookie, java applet, java script, activeX control
- ▶ Tùy vào mức độ bảo mật tại Client, trình duyệt hiện thị hộp thoại cảnh báo

Mối đe dọa – Client

1/9/2019



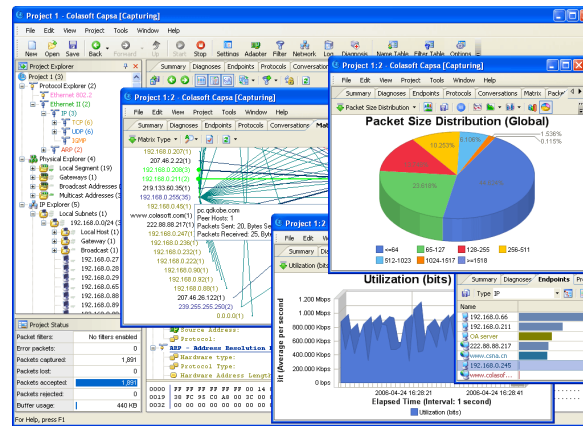
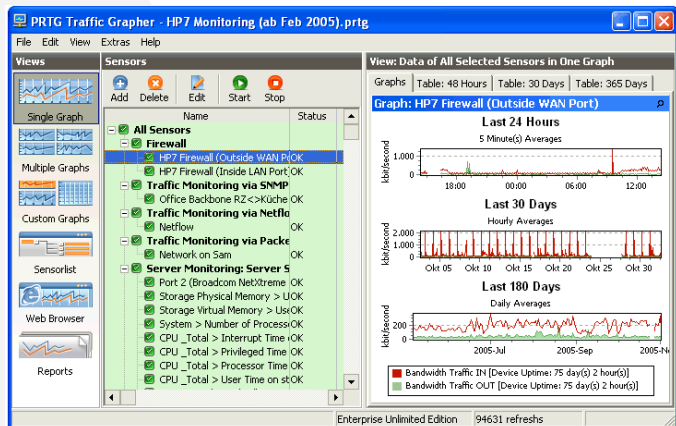
- ▶ **Plug-in**
 - ▶ Chương trình làm tăng khả năng trình bày của các trình duyệt (browser)
 - ▶ Mở nhạc, phim, animation
 - ▶ QuickTime, RealPlayer, FlashPlayer
 - ▶ Có thể nhúng các lệnh với mục đích xấu làm hư hại máy tính

- ▶ **Tập tin đính kèm** theo thư điện tử (e-mail)

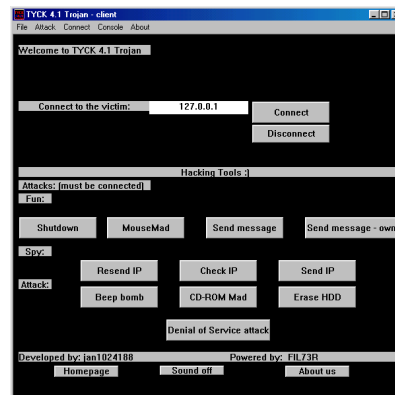
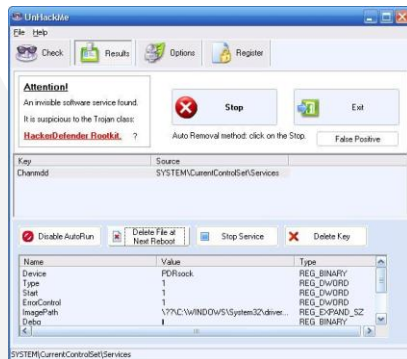
Mối đe dọa – Internet

1/9/2019

- ▶ Các gói tin di chuyển trên Internet theo một con đường không dự kiến trước
 - ▶ Người dùng không biết gói tin sẽ lưu lại ở nơi nào
 - Gói tin bị đọc trộm, sửa đổi, xóa
 - ▶ “*sniffer program*” được sử dụng để bắt gói tin



- ▶ Một số các phần mềm EC vẫn còn nhiều lỗ hổng (*backdoor*)
 - ▶ Lỗi lập trình ngẫu nhiên hay cố ý của người phát triển phần mềm
 - ▶ Nếu có kiến thức và phát hiện được *backdoor*, kẻ xấu có thể quan sát các giao dịch, xóa hay đánh cắp dữ liệu



▶ Web Server

- ▶ Có thể được cấu hình chạy ở **nhiều cấp độ quyền**
 - ▶ **Quyền cao nhất** – cho phép thực thi các lệnh cấp thấp, truy xuất bất kỳ thành phần nào trong hệ thống
 - ▶ **Quyền thấp nhất** – chỉ có thể thực thi chương trình, không cho phép truy xuất nhiều các thành phần trong hệ thống
 - **Quyền càng cao, web server càng bị nguy hiểm**
- ▶ **Nội dung của các thư mục** có thể thấy được từ browser
 - ▶ Trang web mặc định không được cấu hình chính xác
 - ▶ Index.html, Index.htm
- ▶ Yêu cầu người dùng nhập tên và mật mã ở một số trang
 - ▶ Sử dụng **cookie**

▶ Database Server

- ▶ Tập tin chứa dữ liệu có thể được truy xuất bằng quyền hệ thống
 - ▶ **Quyền quản trị** của HĐH
- ▶ Dữ liệu trong CSDL có thể bị lộ nếu **không được mã hóa**

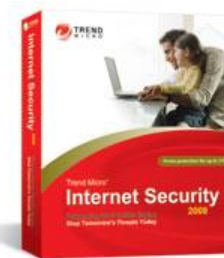
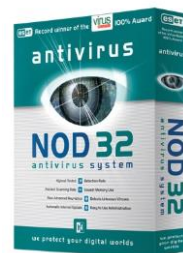
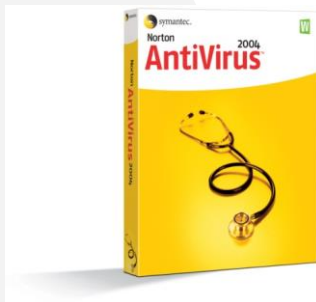




Chính sách bảo vệ

Bảo mật trong EC

- ▶ Trình duyệt có khả năng nhận ra các trang web có chứa *active content*
 - ▶ Cho phép người dùng xác nhận *active content* có đáng tin cậy hay không
 - ▶ Chứng nhận số (Digital Certificate)
- ▶ Phần mềm chống virus



- ▶ Là một thông điệp đính kèm theo thư điện tử hay *active content* nhằm mục tiêu cho biết người gửi thư hoặc trang web đó là ai
 - ▶ Chứng nhận **không nói lên** được chương trình cần cài đặt là chất lượng hay có ích
 - ▶ Chứng nhận cho biết một điều chắc chắn **chương trình là thật**
- Nếu người sử dụng tin tưởng vào các nhà phát triển phần mềm, thì sản phẩm của họ cũng có thể được tin tưởng



Welcome to Gmail



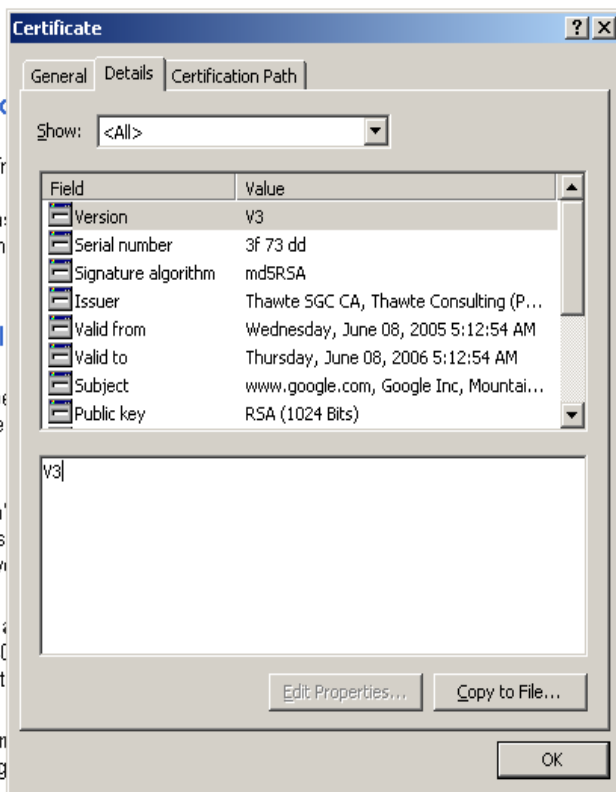
New! Gmail

Chat with your friends
program or look for
already email, as
save and search

About Gmail

Gmail is an experience
never have to delete
want.

- **Search, don't delete**
Use Google search to find
sent or received messages
- **Don't throw away**
Over 2718.940 million messages
to delete another
- **Keep it all in**
Each message is saved



Sign in to Gmail with your

Google Account

Username:

Password:

☐ Remember me on this computer.

[Forgot your username or password?](#)

Learn more [about Gmail](#).

Check out our [new features!](#)

A few words about [Gmail and privacy](#).

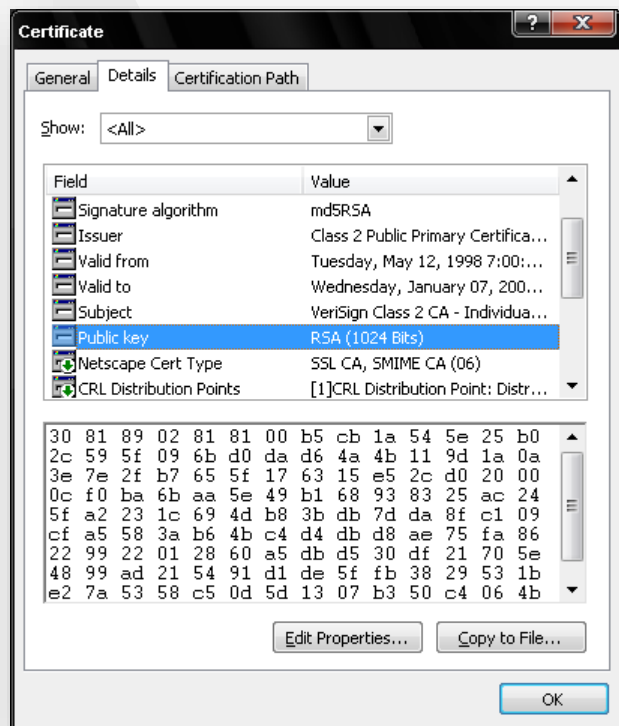
©2006 Google - [Privacy Policy](#) - [Program Policies](#) - [Terms of Use](#)

- ▶ Chứng nhận phải do một đơn vị có uy tín cấp
 - ▶ Certification Authority (CA)
 - ▶ VeriSign
- ▶ **Gồm các thông tin**
 - ▶ Tên, địa chỉ của nhà phát triển phần mềm
 - ▶ Public key của nhà phát triển phần mềm
 - ▶ Thời gian hợp lệ của chứng nhận
 - ▶ Số chứng nhận
 - ▶ Tên người / tổ chức cấp chứng nhận
 - ▶ Chữ ký điện tử của người / tổ chức cấp chứng nhận



Bảo vệ Client – Chứng nhận số

1/9/2019

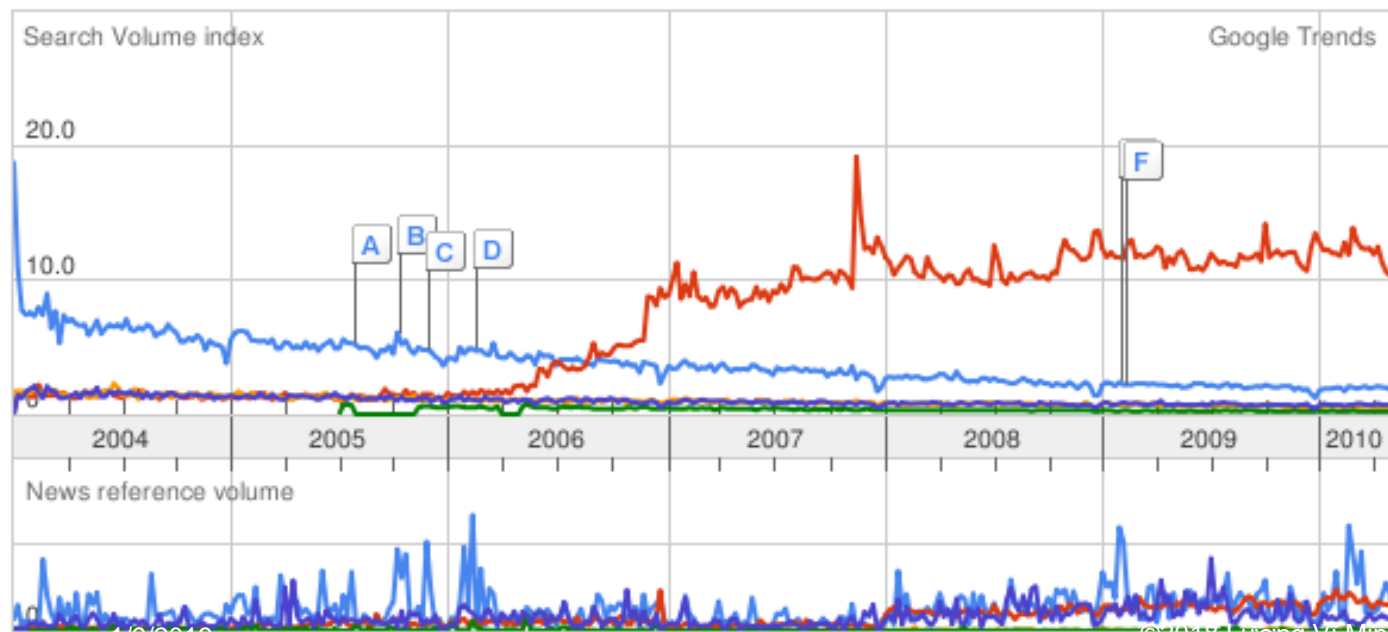


```
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number: 1 (0x1)
  Signature Algorithm: md5WithRSAEncryption
  Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
  OU=Certification Services Division,
  CN=Thawte Server CA/emailAddress=server-certs@thawte.com
  Validity
    Not Before: Aug 1 00:00:00 1996 GMT
    Not After : Dec 31 23:59:59 2020 GMT
  Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
  OU=Certification Services Division,
  CN=Thawte Server CA/emailAddress=server-certs@thawte.com
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
    Modulus (1024 bit):
      00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:
      68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:
      85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:
      6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:
      6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:
      29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:
      6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
      5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
      3a:c2:b5:66:22:12:d6:87:0d
    Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 Basic Constraints: critical
    CA:TRUE
  Signature Algorithm: md5WithRSAEncryption
  07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:
  a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:ca:c8:48:
  3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:
  4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:
  8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:
  e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
  b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:
  70:47
```


Searches Websites

Scale is based on the average worldwide traffic of **entrust** in all years. [Learn more](#)

verisign 3.90 **comodo** 6.80 **thawte** 1.00 **geotrust** 0.20
entrust 1.00



Certification Practice Statement

- ▶ Mỗi CA cấp giấy chứng nhận dựa trên các chính sách và quy trình do CA đó đưa ra.
- ▶ Private keys của CA được lưu trữ trên phần cứng an toàn (hardware cryptomodules)
- ▶ View Verisign [Certification Practice Statement](#)
- ▶ INFN (Istituto Nazionale di Fisica Nucleare) [CPS](#)



[CHRYSLIS LUNA CA3](#)
[TRUSTED ROOT KEY SYSTEM](#)



IBM S/390 SECURE
CRYPTOGRAPHIC MODULE



[LITRONIC 440](#)
[CIPHERACCELERATOR](#)

- ▶ Sử dụng kỹ thuật **Authenticode** để nhận diện các active content
 - ▶ Ai ký xác nhận cho chứng nhận
 - ▶ Danh sách các CA và public key của CA được **lưu trữ trong IE**
 - ▶ Chứng nhận có bị thay đổi gì từ lúc được ký xác nhận không
 - ▶ Sử dụng **public key của CA** để mở chứng nhận
 - ▶ Nếu thông tin trong chứng nhận chứng minh được nhà phát triển phần mềm đã ký cho active content thì chứng nhận là hợp lệ



- ▶ Mã hóa (Encryption)
- ▶ Nghi thức SSL (Secure Sockets Layer)
- ▶ Chữ ký điện tử

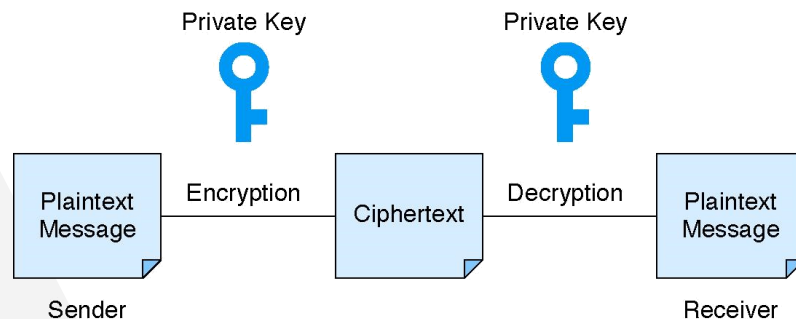
- ▶ Mã hóa – Encryption
- ▶ Chuyển dữ liệu sang dạng thể hiện khác
 - ▶ Thuật toán
 - ▶ Khóa
- ▶ Có 3 kỹ thuật
 - ▶ Mã hóa Hash
 - ▶ Mã hóa không đối xứng (public key)
 - ▶ Mã hóa đối xứng (secret key)



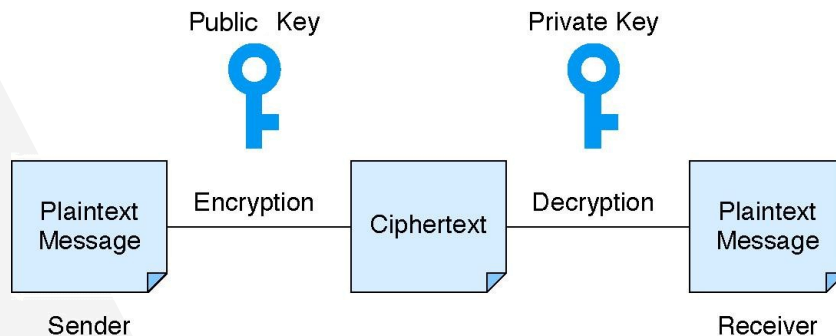
- ▶ Sử dụng thuật toán Hash để đưa ra một con số từ một thông điệp có độ dài bất kỳ
 - ▶ **Xung đột giá trị** hiếm rất hiếm xảy ra
 - ▶ **Không** sử dụng khóa
 - ▶ Chuỗi được mã hóa **không thể giải mã** thành chuỗi ban đầu
- ▶ Thuật toán MD5, SHA-1, SHA256, SHA512, ...



- ▶ Mã hóa chỉ sử dụng 1 loại khóa
 - ▶ **Secret key** – mã hóa và giải mã thông điệp
- ▶ Thuật toán 3DES, Rijndael (AES), blowfish, idea,...



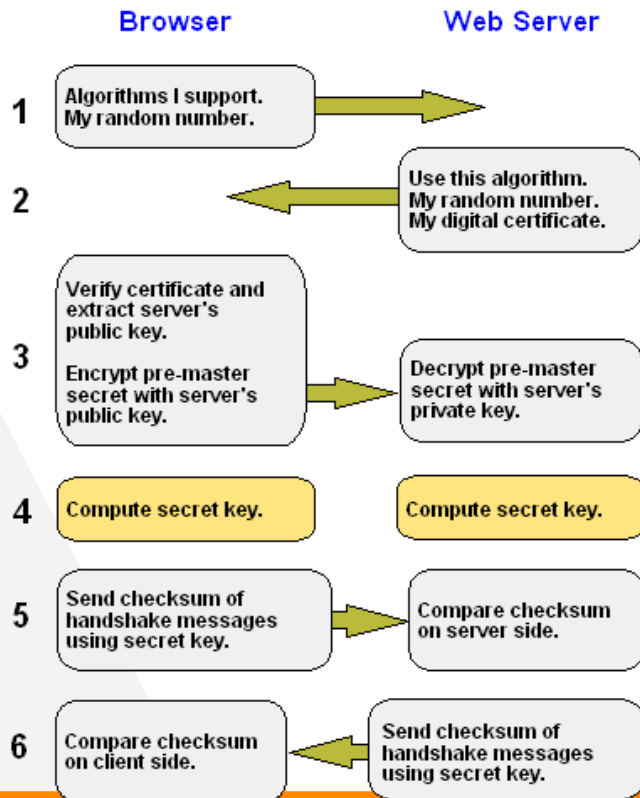
- ▶ Mã hóa dựa vào 1 cặp khóa
 - ▶ **Public key** – mã hóa thông điệp
 - ▶ **Private key** – giải mã thông điệp
- ▶ Thuật toán RSA, DSA,...



Bảo vệ Internet – Nghi thức SSL

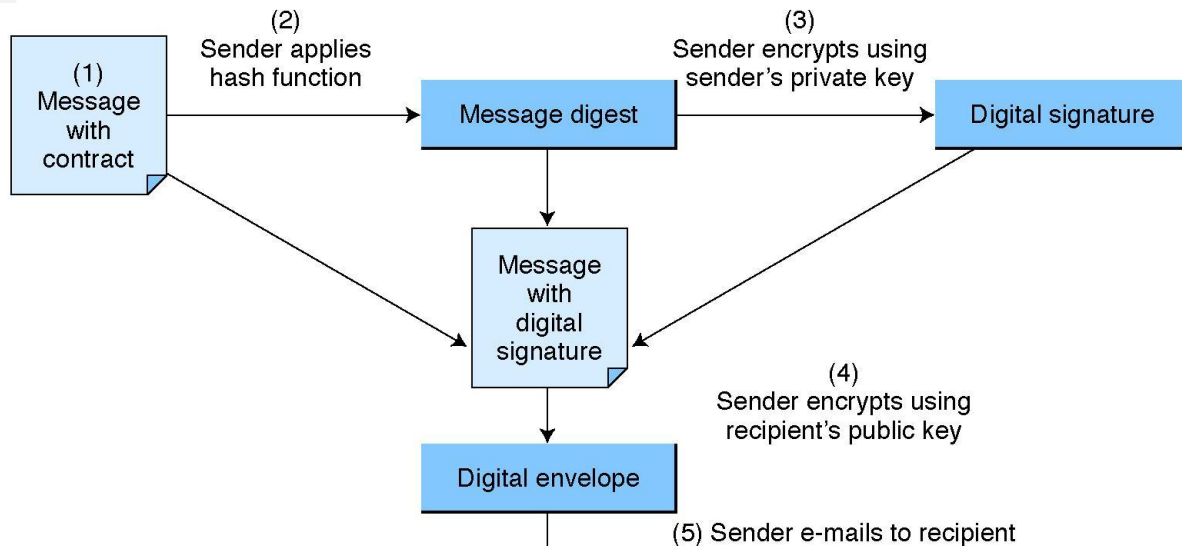
From Computer Desktop Encyclopedia
© 2005 The Computer Language Co., Inc.

1/9/2019

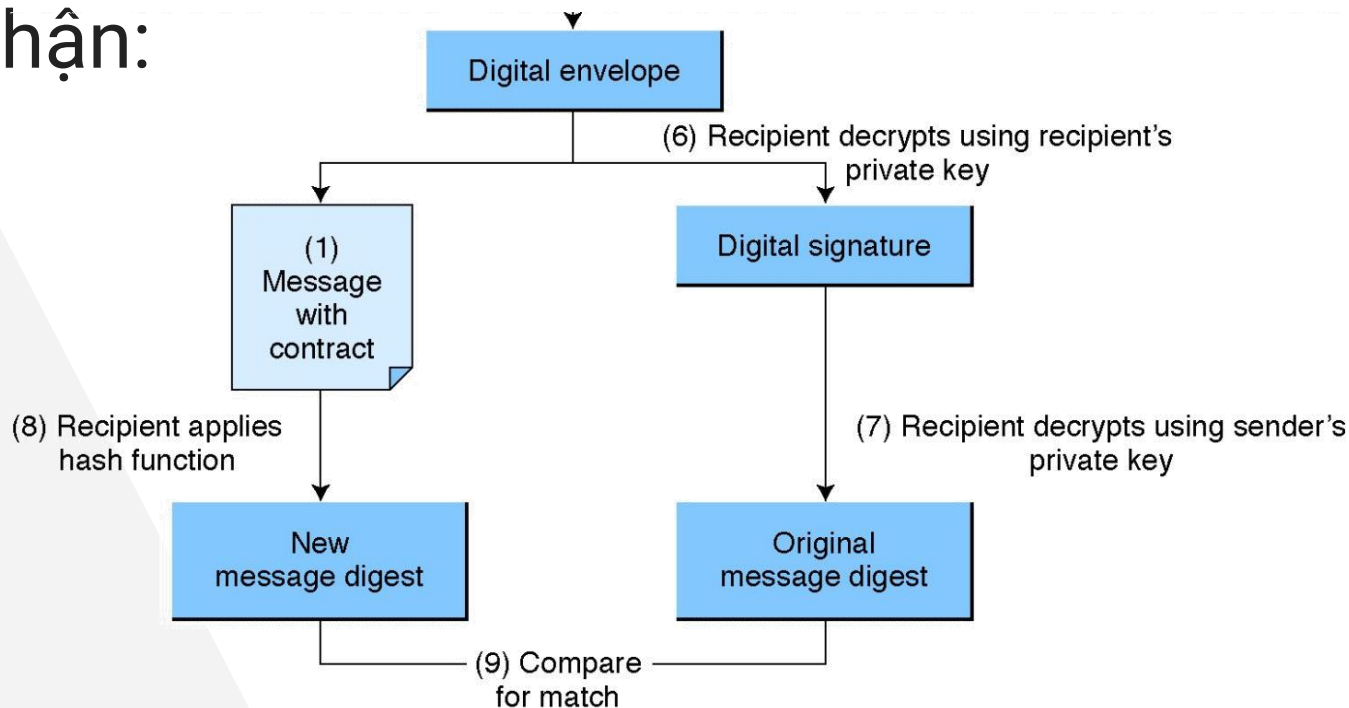


- Nghi thức bảo mật kết nối giữa **client** và **server**

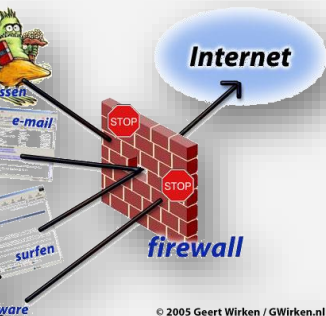
- ▶ Ứng dụng Mã hóa bất đối xứng
- ▶ Sử dụng khóa Private để ký nhận thông tin;
- ▶ Sử dụng khóa Public trong Chữ ký điện tử để xác thực thông tin



► Nhận:



- ▶ Điều khiển truy cập và xác thực người dùng
 - ▶ Ai đang truy cập vào server
 - ▶ Truy cập những gì
- ▶ Bức tường lửa (firewall)
 - ▶ Giải pháp gồm máy tính và phần mềm
 - ▶ Điểm đi ra ngoài Internet của hệ thống mạng
 - ▶ Ngăn chặn các tấn công từ Internet hay từ các mạng khác



Các lời khuyên có ích

1/9/2019

Always update your anti-virus software at least weekly

Back up your important files and ensure that they can be restored.

Change the computer's boot sequence to always start the PC from its hard drive

Don't share Drive C: without a password and without read-only restrictions.

Empy floppy drives of diskettes before turning on computers, especially laptops.

Forget opening unexpected e-mail attachments, even if they're from friends

Get trained on your computer's anti-virus software and use it.

Have multiple backups of important files. This lowers the chance that all are infected.

Install security updates for your operating system and programs as soon as possible.

<http://www.securitystats.com/tools/password.php>

Password Security

A good password is one that cannot be easily guessed.

Enter a password, click submit, then we'll score it against best practices!

DO'S

- DO use a password with mixed-case letters. Use uppercase letters throughout the password.
- DO use a password that contains alphanumeric characters and include punctuation, where supported by the operating system.
- DO use a password with mixed-case letters. Do not just capitalize the first letter, but add uppercase letters throughout the password.
- DO use at least six characters, eight characters for Windows NT.
- DO use a seemingly random selection of letters and numbers.

DONT'S

- DO NOT use a network login ID in any form (reversed, capitalized, or doubled as a password).
- DO NOT use your first, middle or last name or anyone else's in any form. Do not use your initials or any nicknames you may have or anyone else's.
- DO NOT use a word contained in English or foreign dictionaries, spelling lists, or other word lists and abbreviations.
- DO NOT use other information easily obtained about you. This includes pet names, license plate numbers, telephone numbers, identification numbers, the brand of your automobile, the name of the street you live on, and so on. Such passwords are very easily guessed by someone who knows the user.
- DO NOT use a password of all numbers, or a password composed of alphabet characters. Mix numbers and letters.

Online Secure Hash Algorithm Calculator

Hash algorithms are fundamental to many cryptographic applications. Although widely associated with digital signature technology, the hash algorithm has a range of other uses. SHA-1 and MD5 are amongst the most widely known, trusted and used. When utilised with a password (the HMAC version), the potential uses of these algorithms extends further.

Enter a string in the box below and select the hash algorithm.

Dictionary Based Hash Cracker

The "Golden Rule" of password security is **NOT** to choose a password that is easily guessable, or one that might be found in a dictionary. The reason for this is that many hacker tools can crack dictionary-based passwords in mere seconds.

This web based demonstration shows how truly easy it is to break dictionary based passwords, regardless of the type of encryption algorithm used to encrypt them. Simply paste in an encrypted password value, and then count the seconds it takes to return the password associated with that encrypted value (won't be long.....)

Here is an example:

LANMAN HASH: FDA95FBCEA288D44AAD3B435B51404EE

-OR-

NTLM HASH: 066DDFD4EF0E9CD7C256FE77191EF43C

Will return a value of "hello", within about 5 seconds (even using this crude web interface.)