CHƯƠNG 9
BẢO MẬT AN NINH TRONG TMĐT

Nội dung

1. Rủi ro mất an toàn dữ liệu
2. Giải pháp bảo vệ dữ liệu
3. Các kỹ thuật mã hóa
4. Chữ ký số - Chứng thư số

Rủi ro mất an toàn dữ liệu

- Các dạng rủi ro:
  - Dữ liệu cá nhân được số hóa và lưu trữ trong máy tính bị lộ ra ngoài (do mất máy tính, thẻ nhớ,…)
  - Nhiễm virus máy tính
  - Tin tặc tấn công
    - Tấn công từ chối dịch vụ (DoS)
    - Trình theo dõi nghe lén (sniffer)
    - Phishing
  - ...

Rủi ro mất an toàn dữ liệu

- Virus máy tính là những chương trình hay đoạn mã được thiết kế để tự nhân bản và sao chép chính nó tạo ra các file bị nhiễm trên các thiết bị lưu trữ.
- **Các hình thức lây nhiễm virus:**
  - Lây qua các thiết bị lưu trữ
  - Lây qua email
  - Lây qua internet

Rủi ro mất an toàn dữ liệu

- **Các phương thức virus lây nhiễm qua email:**
  - Lây nhiễm vào các file đính kèm (attached mail) → máy tính người dùng sẽ không bị nhiễm virus cho tới khi file đính kèm bị nhiễm virus được kích hoạt
  - Lây nhiễm do mở một liên kết trong email → dẫn đến một trang web được cài sẵn virus, do khai thác các lỗ hổng của trình duyệt và hệ điều hành
  - Lây nhiễm ngay khi mở để xem email → chưa cần kích hoạt các file hoặc mở các liên kết, máy tính đã có thể bị lây nhiễm virus, do khai thác các lỗi của hệ điều hành.

Rủi ro mất an toàn dữ liệu

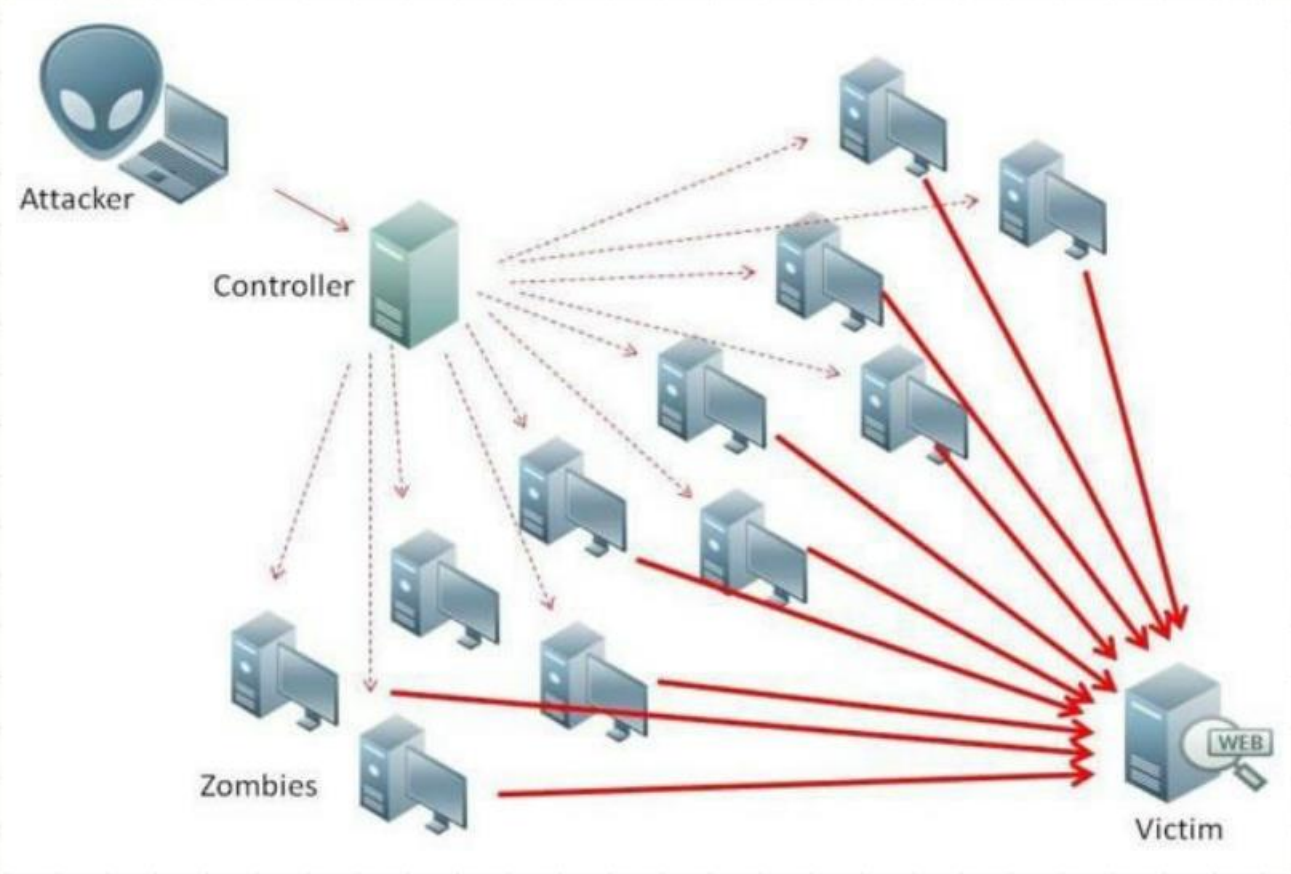
- **Các phương thức virus lây nhiễm qua internet:**
  - Lây nhiễm qua các file tài liệu, phần mềm khi tải từ Internet,...
  - Lây nhiễm khi đang truy cập các trang web được cài đặt mã độc gây lây nhiễm virus và phần mềm độc hại vào máy tính.
  - Lây nhiễm virus hoặc chiếm quyền điều khiển máy tính thông qua các lỗi bảo mật hệ điều hành, ứng dụng sẵn có trên hệ điều hành hoặc phần mềm của hãng thứ ba …

Rủi ro mất an toàn dữ liệu

- Tấn công từ chối dịch vụ (Denial of Service) →kiểu tấn công khiến một hệ thống máy tính hoặc một mạng bị quá tải, dẫn tới không thể cung cấp dịch vụ hoặc phải dừng hoạt động.
- Các dạng DoS khác:
  - DDoS (Distributed Denial of Service) → tấn công từ chối dịch vụ phân tán
  - DRDoS (Distributed Reflection Denial of Service) → tấn công theo phương pháp phản xạ phân tán.

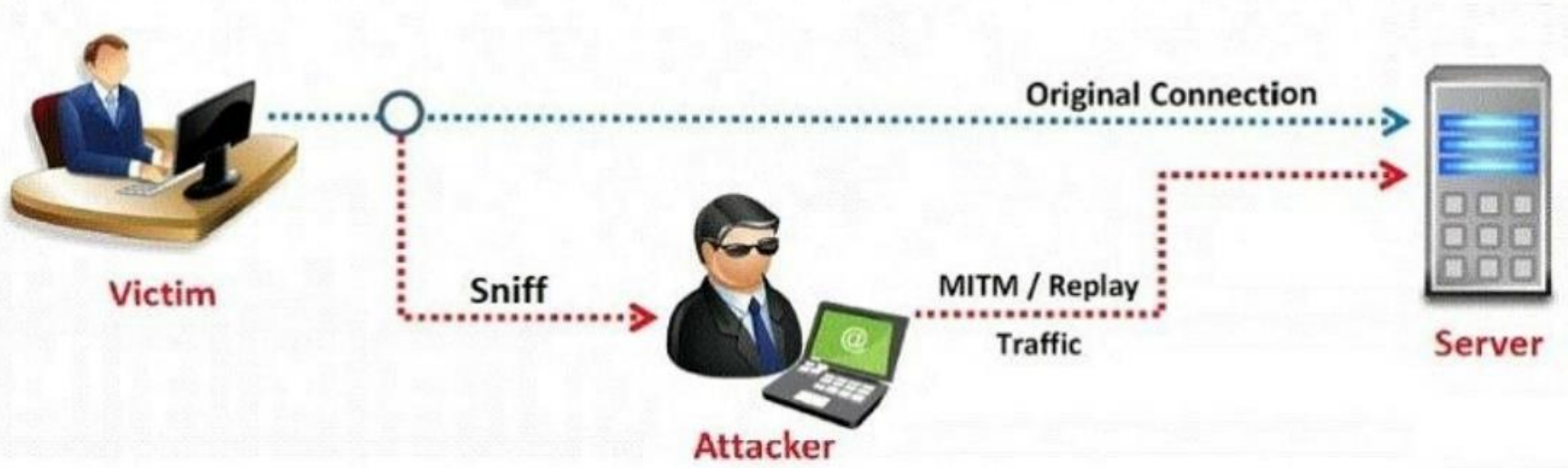
Rủi ro mất an toàn dữ liệu

- Minh họa một kiểu tấn công DoS



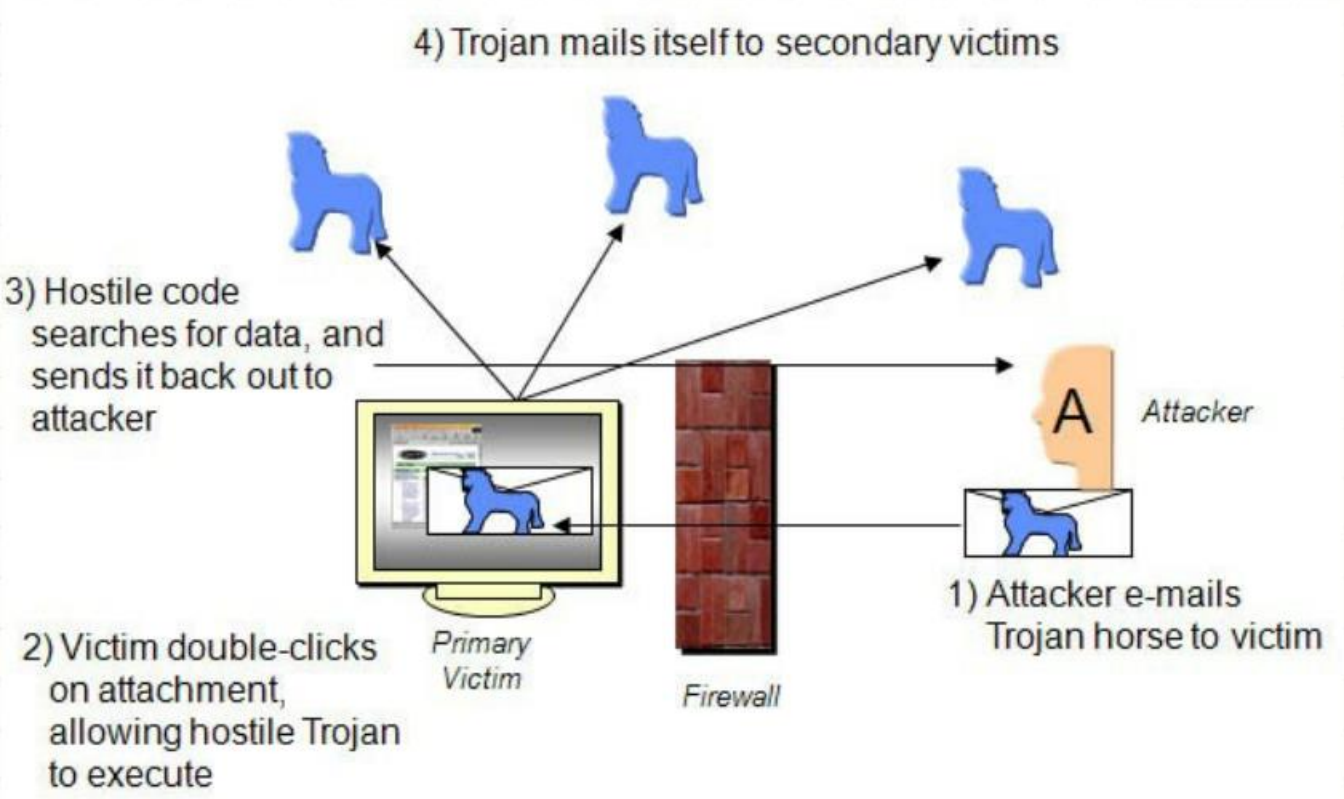
Rủi ro mất an toàn dữ liệu

- Tấn công Sniffer → chương trình theo dõi, nghe trộm, giám sát sự di chuyển của thông tin trên mạng.



Rủi ro mất an toàn dữ liệu

- Minh họa một kiểu phishing bằng cách gửi email có đính Trojan



Giải pháp bảo vệ dữ liệu

- **Các giải pháp:**
  - Phòng chống virus
  - Thiết lập xác minh 2 bước đối với các tài khoản truy cập trực tuyến trên internet
  - Mã hóa các dữ liệu quan trọng lưu trên máy tính và trao đổi trên mạng → sử dụng các kỹ thuật mã hóa
  - Các giải pháp bảo vệ khác …

Giải pháp bảo vệ dữ liệu

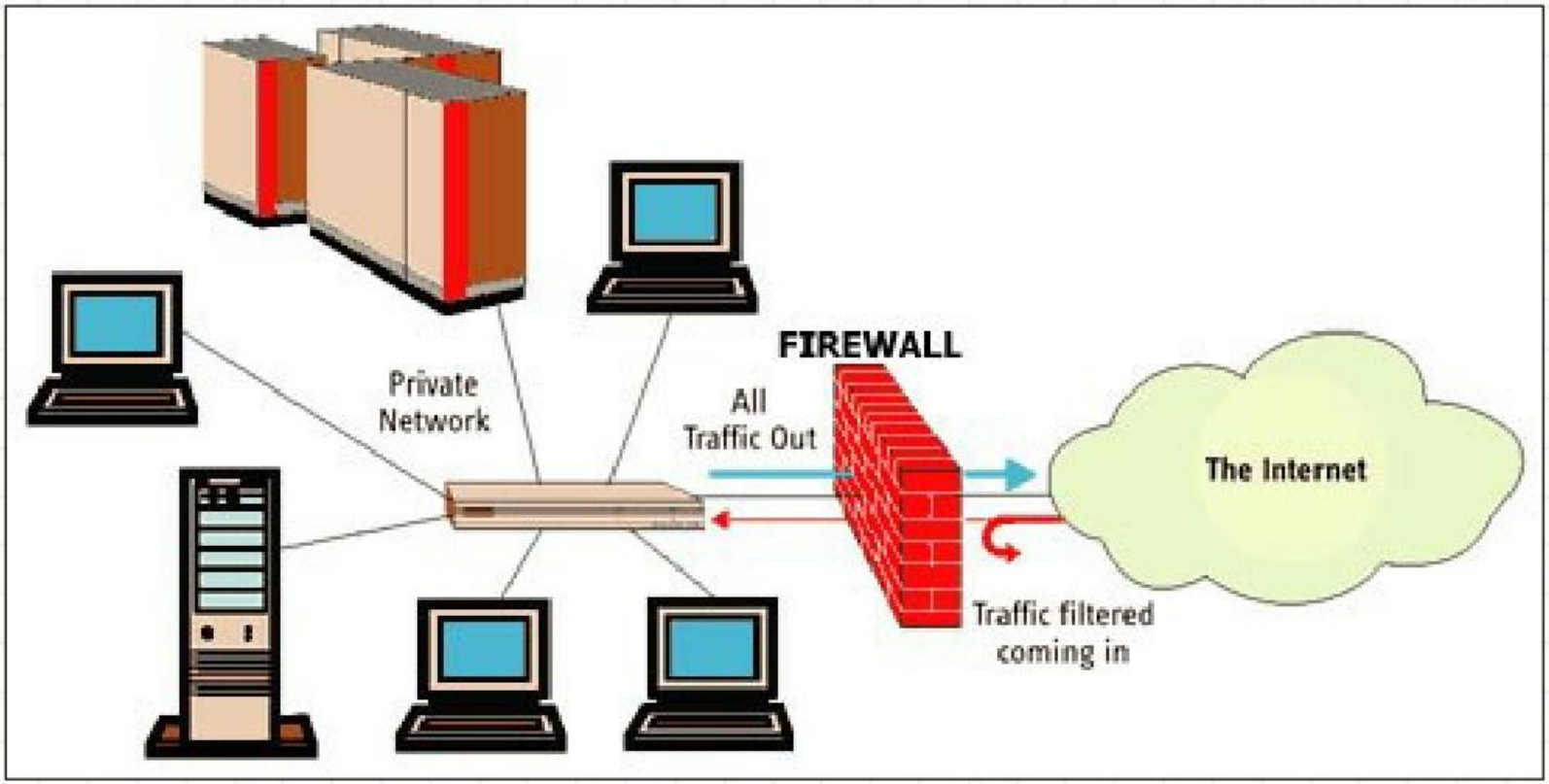
- **Cách phòng chống virus:**
  - Sử dụng phần mềm diệt virus: Microsoft Security Essentials, Norton Symantec, Kaspersky, ...
  - Sử dụng tường lửa bằng phần cứng: cấu hình trên các thiết bị wireless router/access point, …
  - Sử dụng tường lửa bằng phần mềm: chức năng tường lửa có sẵn của HĐH Windows, hoặc của hãng khác như ZoneAlarm Security Suite, …

Giải pháp bảo vệ dữ liệu

- **Thiết lập tường lửa Firewall**
  - Mọi dữ liệu lưu thông từ bên trong hoặc bên ngoài đều bị kiểm soát tại tường lửa và chỉ các dữ liệu được phép mới đi qua tường lửa.
  - Cài Firewall trong HĐH Windows 7: Control Panel → System and Security → Windows Firewall

Giải pháp bảo vệ dữ liệu

- Tường lửa được đặt giữa mạng nội bộ với internet

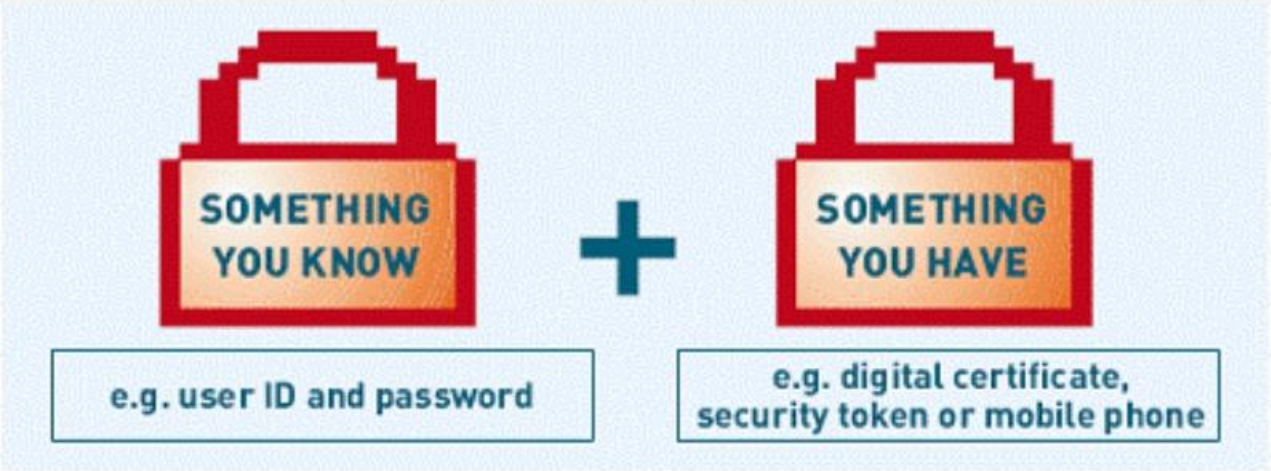


Giải pháp bảo vệ dữ liệu

- **Xác minh 2 bước (two-step verification)**
  → xác thực 2 yếu tố (two-factor authentication)

Giải pháp bảo vệ dữ liệu

- Xác thực 2 yếu tố:
  - Phương pháp xác thực người dùng dựa vào yếu tố người dùng biết (knowledge factor) và yếu tố người dùng sở hữu (possession factor)



Các kỹ thuật mã hóa

- **Mục đích**
  - Đảm bảo an toàn cho các thông tin được lưu giữ, và đảm bảo an toàn cho thông tin khi truyền phát trên mạng.
- **Các kỹ thuật mã hoá cơ bản**
  - Thuật toán băm - hàm băm (Hash function)
  - Mã hoá đối xứng – mã hóa khoá bí mật
  - Mã hoá bất đối xứng – mã hóa khoá công khai

Thuật toán băm

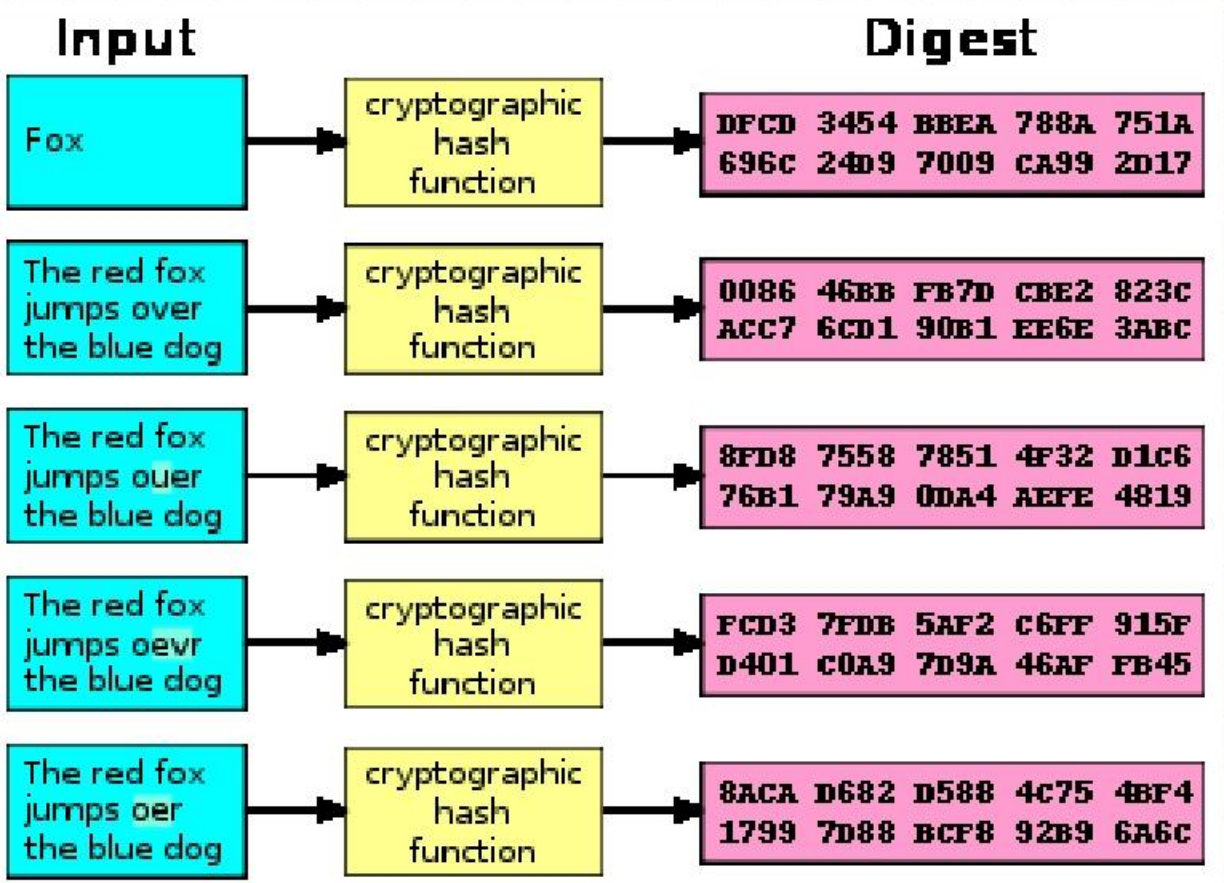
- Thuật toán băm tạo ra mã băm (hash code) từ một khối dữ liệu, có các đặc tính:
  1. Độ dài đầu ra cố định với mỗi thuật toán
  2. Khối dữ liệu đầu vào giống nhau thì mã băm giống nhau
  3. Khi biết mã băm rất khó tìm ra được khối dữ liệu ban đầu
  4. Hai khối dữ liệu gần giống nhau thì tạo ra 2 mã băm tương đối khác nhau

Thuật toán băm

- Khối dữ liệu ban đầu → Hàm băm → Mã băm

Thuật toán băm

- Minh họa thuật toán băm:



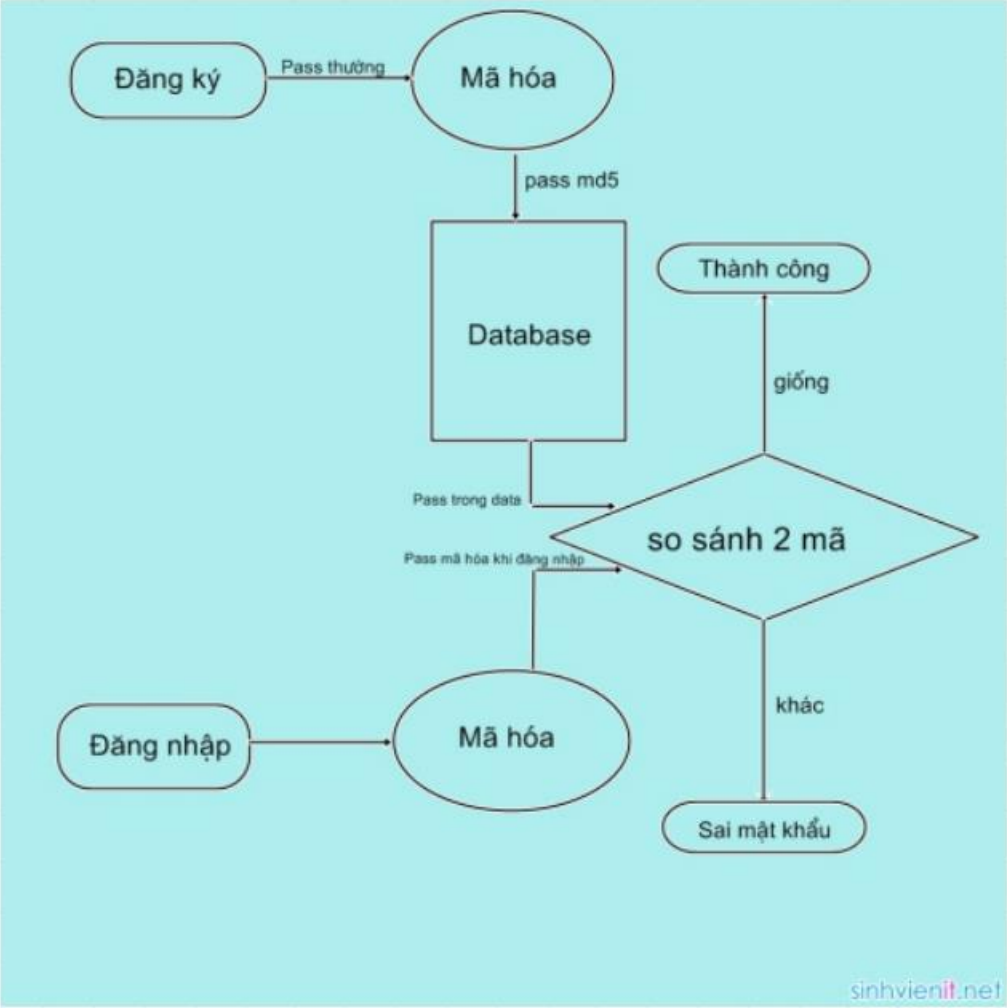
Thuật toán băm

- Các giải thuật phổ biến:
  - CRC32 (Cyclic Redundancy Check): mã băm dài 32 bit
  - MD5 (Message Digest algorithm 5): mã băm dài 128 bit
  - SHA1 (Secure Hashing Algorithm): mã băm dài 160 bit
  - SHA256 (Secure Hashing Algorithm): mã băm dài 256 bit
  - SHA384 (Secure Hashing Algorithm): mã băm dài 384 bit
  - SHA512 (Secure Hashing Algorithm): mã băm dài 512 bit

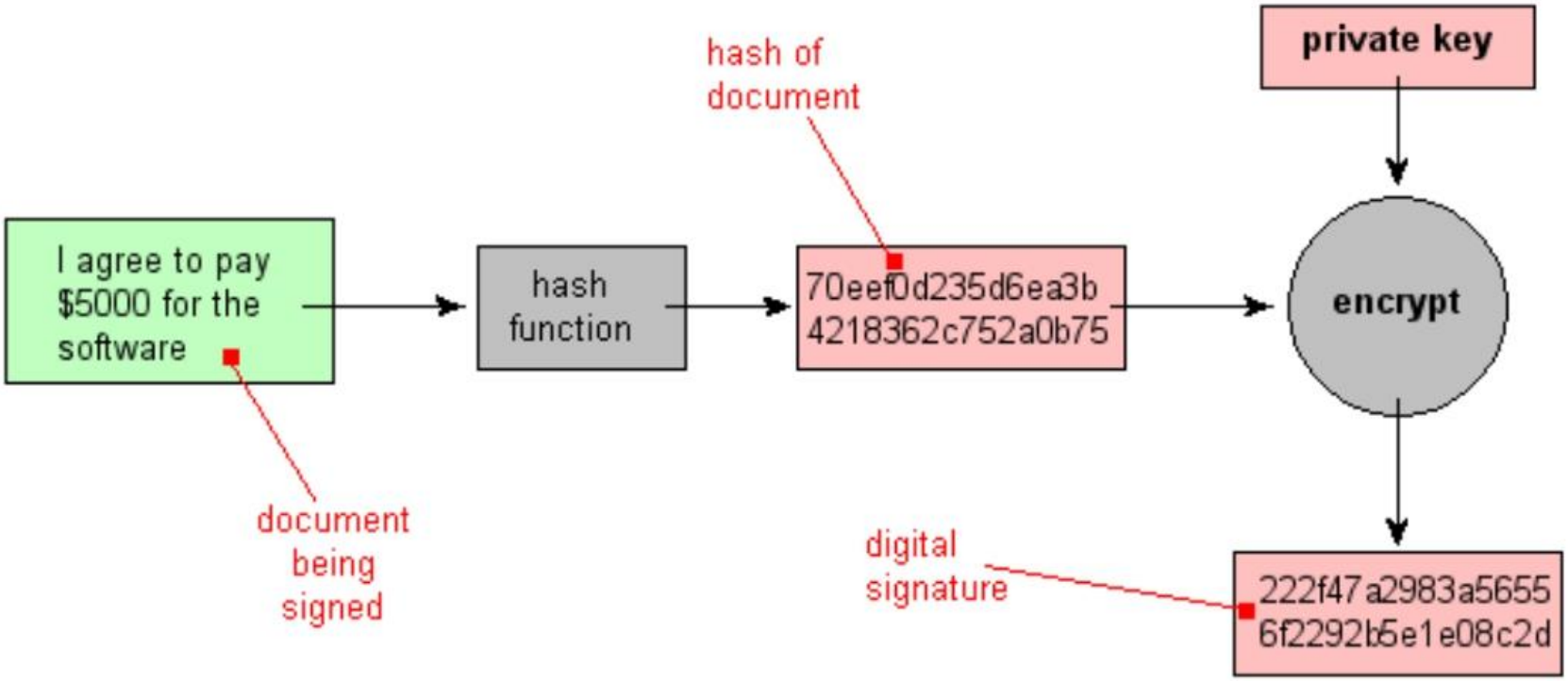
Thuật toán băm

- Ứng dụng của hàm băm:
  - Chống và phát hiện xâm nhập → so sánh giá trị hash của một file/mẫu dữ liệu với giá trị trước đó để kiểm tra file/mẫu dữ liệu đó có bị thay đổi hay không
  - Tạo chìa khóa từ mật khẩu → lưu giá trị mật khẩu dưới dạng mã băm
  - Phối hợp với mã hóa khóa công cộng để tạo chữ ký số.

Ứng dụng của hàm băm: lưu mật khẩu

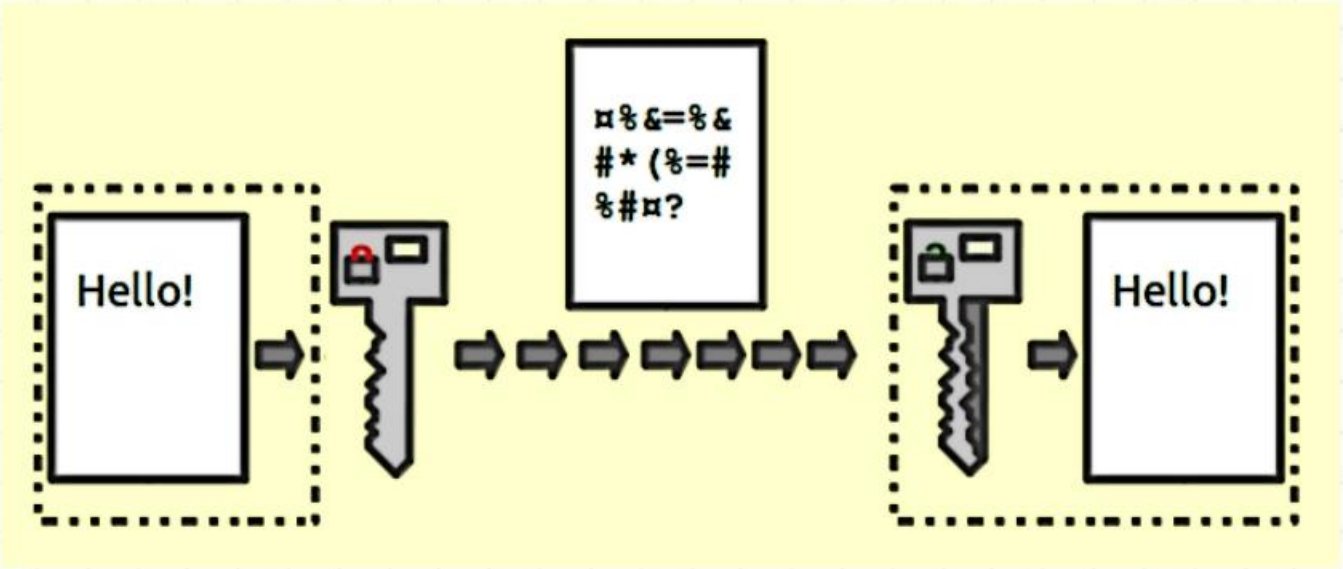


Ứng dụng của hàm băm: tạo chữ ký số



Mã hóa khóa bí mật

- *Mã hoá khoá bí mật →mã hoá đối xứng*
  - Phương pháp mã hóa sử dụng một khoá cho cả quá trình mã hoá (*thực hiện bởi người gửi*) và quá trình giải mã (*thực hiện bởi người nhận*)



Mã hóa khóa bí mật

- Các phương pháp phổ biến:
  - **Ceasar**: quay vòng bộ ký tự
  - **DES (Data Encryption Standard)**: hỗ trợ với khóa dài 64 bit
  - **RC2 (Rivest Cipher 2)**: hỗ trợ với khóa dài từ 40 đến 128 bit
  - **AES (Advanced Encryption Standard)**: hỗ trợ với khóa dài 128, 192 hoặc 256 bit. Còn được gọi với tên là Rijndael
  - **TripleDES**: hỗ trợ khóa dài 128 hoặc 192 bit. Còn được gọi là 3DES

Mã hóa khóa bí mật

- Mã hóa Ceasar:
  - Mật mã thay thế $\rightarrow$ mỗi ký tự trong văn bản được thay thế bằng một ký tự cách nó một đoạn k trong bảng chữ cái để tạo thành bản mã.
  - Mã hóa $E_k(x) = (x+k) \bmod 26$
  - Giải mã $D_k(x) = (x-k) \bmod 26$

Mã hóa khóa bí mật

- Ví trí các ký tự trong bảng chữ cái tiếng Anh

A	B	C	D	E	F	G	H	I	J
00	01	02	03	04	05	06	07	08	09
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z	A	B	C	D
20	21	22	23	24	25	00	01	02	03

Mã hóa khóa bí mật

- **Phép toán modulo:**
  - Cho số nguyên dương n, hai số nguyên a, b được gọi là đồng dư theo modulo n nếu chúng có cùng số dư khi chia cho n.
  - Tương đương (a - b) chia hết cho n.
  - Ký hiệu: $a \equiv b \pmod{n}$
  - Nếu $a \equiv b \pmod{n}$ thì $a + z \equiv b + z \pmod{n}$
  - Ví dụ: $26 \equiv 0 \pmod{26}$ thì $26-15 \equiv 0-15 \pmod{26}$, tức $11 \equiv -15 \pmod{26}$

Mã hóa khóa bí mật

- Ví dụ mã hóa Ceasar: mã hóa chuỗi ATTACK với k=23
  - $E_{23}(A) = (00+23) \bmod 26 = 23 \rightarrow X$
  - $E_{23}(T) = (19+23) \bmod 26 = 16 \rightarrow Q$
  - $E_{23}(T) = (19+23) \bmod 26 = 16 \rightarrow Q$
  - $E_{23}(A) = (00+23) \bmod 26 = 23 \rightarrow X$
  - $E_{23}(C) = (02+23) \bmod 26 = 25 \rightarrow Z$
  - $E_{23}(K) = (10+23) \bmod 26 = 07 \rightarrow H$

Mã hóa khóa bí mật

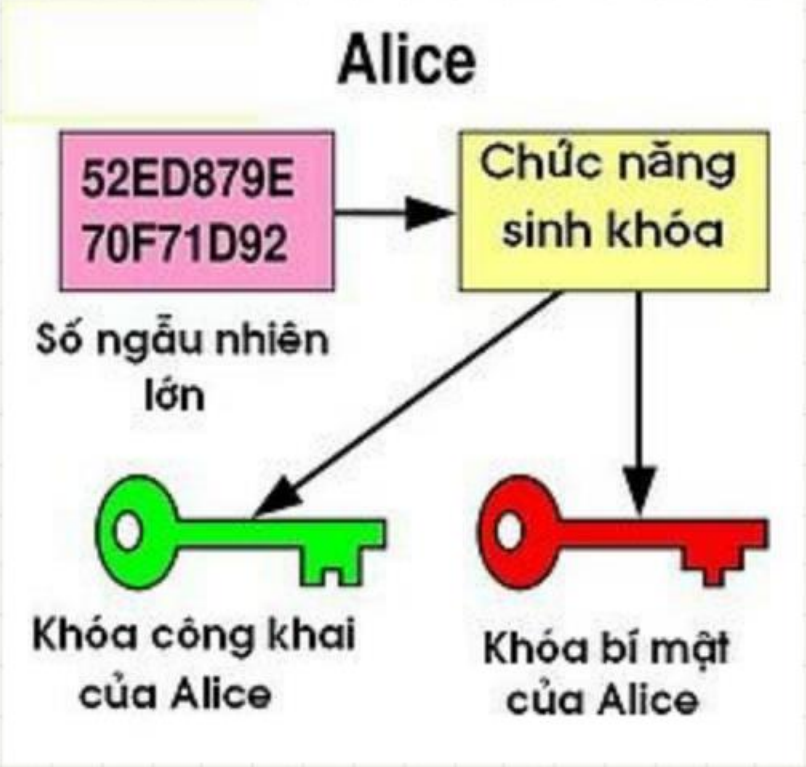
- Bài tập mã hóa Ceasar :
  - Giải mã chuỗi YVCCFNFICU, biết k=17 ?
  - Giải mã chuỗi JHMGSDCNHMFNZH, biết k=25 ?
  - Giải mã chuỗi BFLYECTOZLYSYRSTPA, biết k=11 ?
  - Giải mã chuỗi ETYSZNGLYASZYR, biết k=-15 ?

Mã hóa khóa công khai

- *Mã hoá khoá công khai →mã hoá bất đối xứng*
  - Phương pháp mã hóa sử dụng cặp khoá, một khoá (*khóa public của người gửi*) để mã hoá thông điệp và một khoá khác (*khóa private của người nhận*) để giải mã

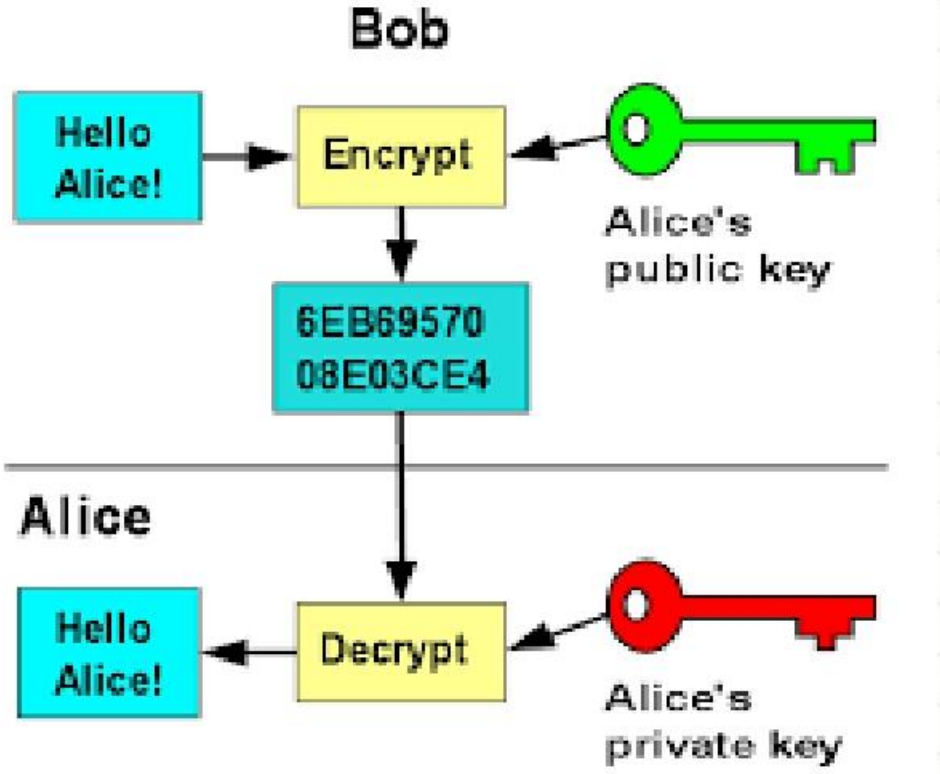
Mã hóa khóa công khai

- Chọn một số ngẫu nhiên lớn để sinh cặp khóa



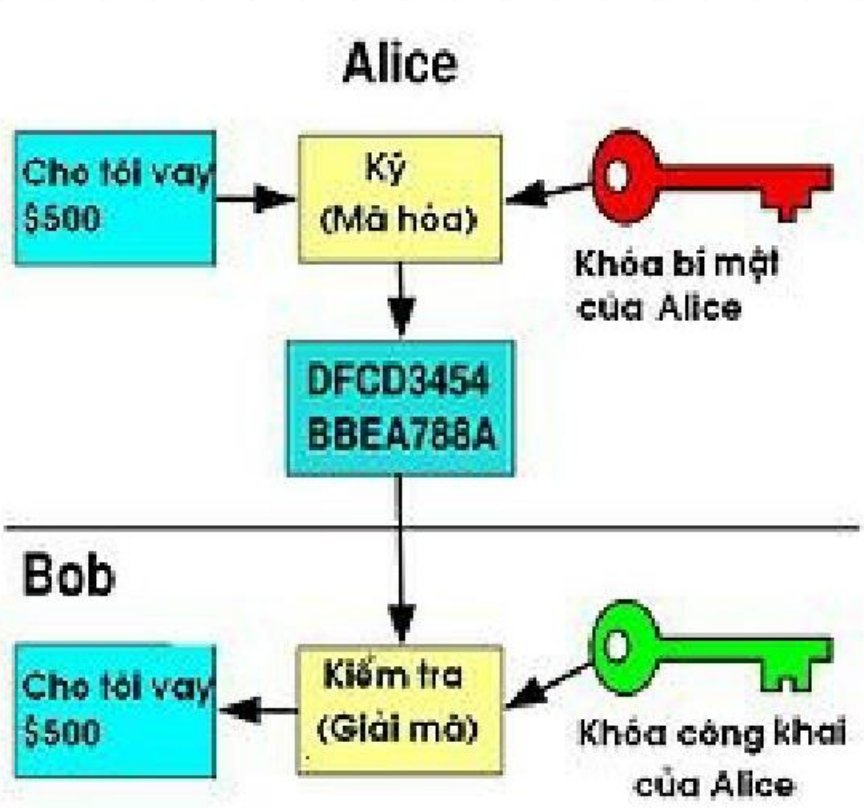
Mã hóa khóa công khai

- Dùng khoá công khai để mã hóa, nhưng dùng khoá bí mật để giải mã



Mã hóa khóa công khai

- Dùng khoá bí mật để ký một thông báo;dùng khoá công khai để xác minh chữ ký



Mã hóa khóa công khai

- Các giải thuật phổ biến:
  - Diffie-Hellman
  - DSS
  - RSA

Giải thuật mã hóa khóa công khai RSA

- Giải thuật RSA:
  - tác giả Ron Rivest, Adi Shamir và Len Adleman phát minh vào năm 1977
  - Ý tưởng: nếu biết trước một số nguyên lớn n, rất khó để tìm ra 2 số nguyên tố p và q mà tích của nó: p*q = n
    (*bài toán phân tích n ra thừa số nguyên tố*)
  - Nếu n đủ lớn (chiều dài 1024 đến 2048 bit) $\rightarrow$ khả năng phá mã gần như không thể !

Giải thuật mã hóa khóa công khai RSA

- Các bước tạo cặp khóa của giải thuật RSA:
  1. Chọn 2 số nguyên tố lớn p và q với $p \neq q$
  2. Tính $n = p*q$
  3. Tính giá trị hàm số Euler $\varphi(n)=(p-1)*(q-1)$
  4. Chọn một số tự nhiên e sao cho $1 < e < \varphi(n)$ và $UCLN(e, \varphi(n)) = 1$
  5. Tính d sao cho $d*e \bmod \varphi(n) = 1$
- Khóa công khai: (e,n)
- Khóa bí mật: (d,n)

Giải thuật mã hóa khóa công khai RSA

- **Mã hóa:**
  - Giả sử Bob muốn gửi thông điệp m cho Alice. Lúc này Bob có m và biết (e,n) do Alice gửi. Bob sẽ tính c là bản mã hóa của m theo công thức:

$$c = m^e \bmod n$$

- **Giải mã:**
  - Alice nhận c từ Bob và biết khóa bí mật d. Alice có thể tìm được m từ c theo công thức sau:

$$m = c^d \bmod n$$

Giải thuật mã hóa khóa công khai RSA

- Ví dụ chọn p = 3 và q = 11
- Tính n = p * q = 3 * 11 = 33
- Tính ϕ(n) = (p - 1) * (q - 1) = 2 * 10 = 20
- Chọn e sao cho 1 < e < ϕ(n) và UCLN(e, ϕ(n)) = 1. Lấy e = 7
- Tính d sao cho (d * e) mod ϕ(n) = 1. Giải pháp là d = 3, vì (3 * 7) mod 20 = 1
- Khóa công khai là (e, n) => (7, 33)
- Khóa bí mật là (d, n) => (3, 33)
- Mã hóa thông điệp *m = 2* thành $c = 2^7 \bmod 33 = 29$
- Từ *c = 29*, giải mã ra $m = 29^3 \bmod 33 = 2$

Giải thuật mã hóa khóa công khai RSA

- Bài tập:
  - Cho 2 số nguyên tố p = 11 và q = 13
  - Tìm public key và private key
  - Mã hóa thông điệp m = 2

Chữ ký số

- Trong giao dịch điện tử, việc sử dụng chứng từ điện tử (thông điệp dữ liệu) còn gặp một số cản trở:
  - Xác thực các bên trong giao dịch (identification);
  - Bảo mật và phân quyền truy cập các thông điệp dữ liệu (entitlements),
  - Xác định trách nhiệm các bên trong giao dịch điện tử (digital accountability).

Chữ ký số

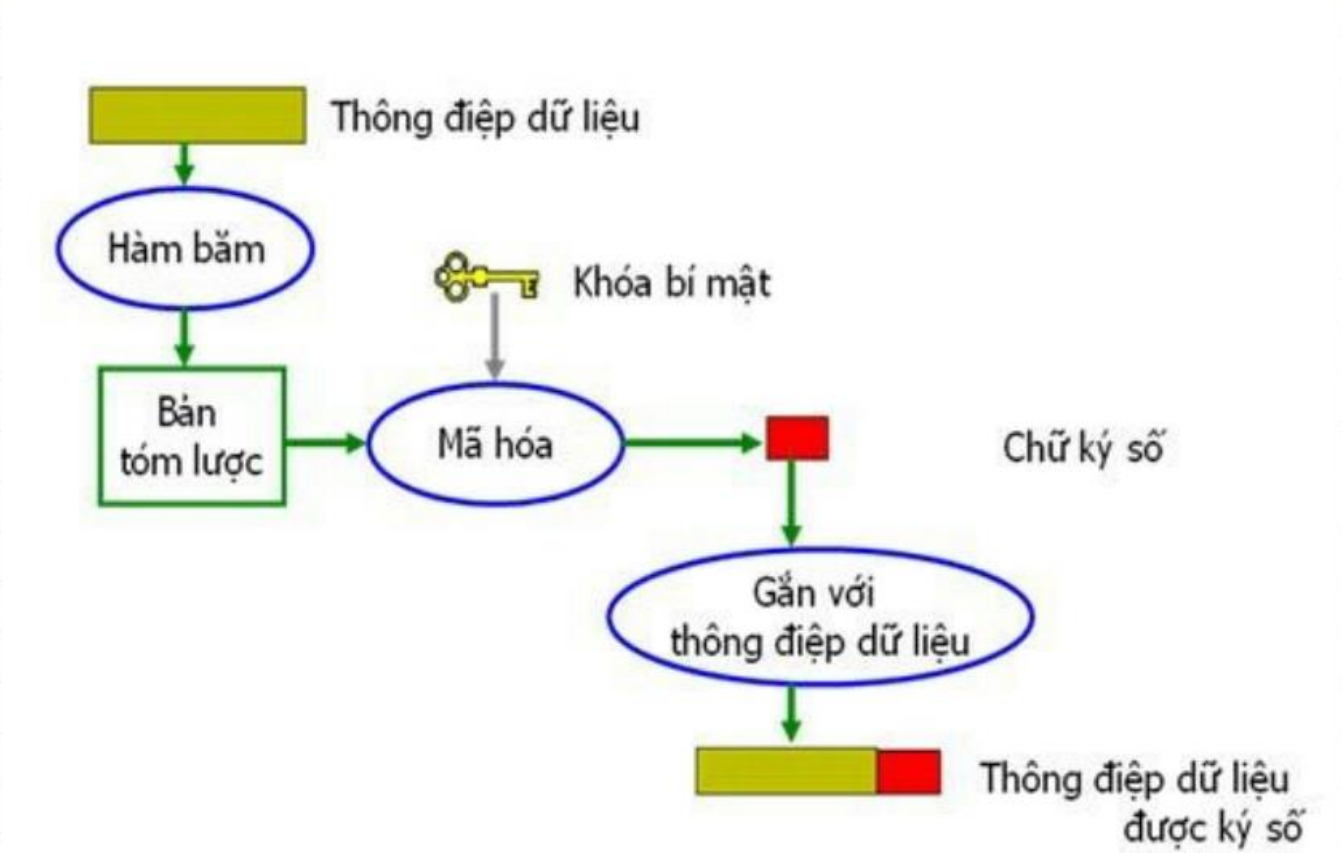
- Chữ ký điện tử (chữ ký số) sử dụng nền tảng hạ tầng mã hóa khóa công cộng (*PKI – public key infrastructure*) có khả năng khắc phục các vấn đề trên trong giao dịch điện tử.

Chữ ký số

- Công thức để sinh ra chữ ký số phụ thuộc vào ba yếu tố đầu vào:
  1. bản thân văn bản điện tử cần ký
  2. khóa bí mật (private key) và
  3. phần mềm để ký số.

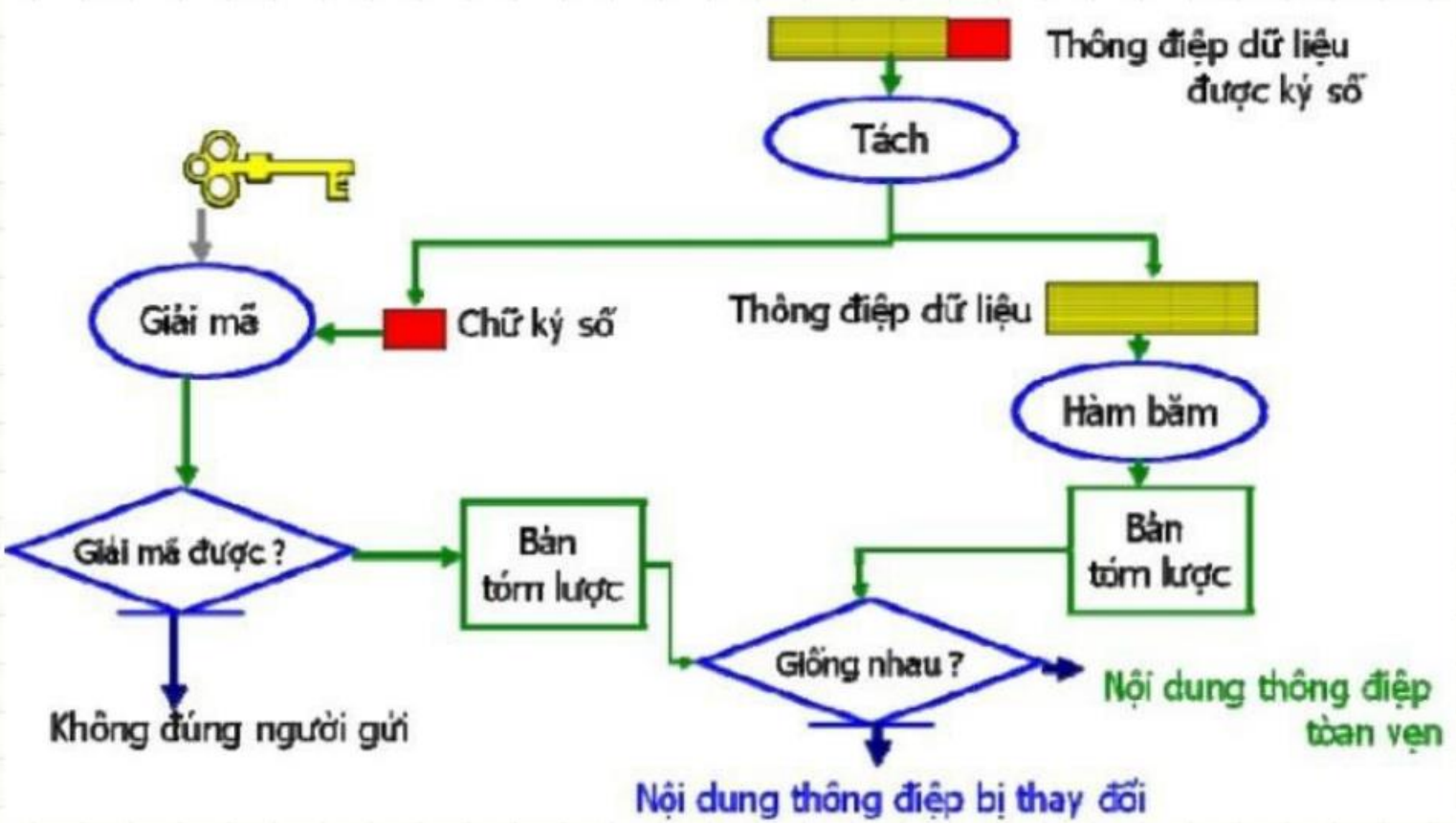
Quy trình tạo và xác thực chữ ký số

- Sơ đồ tạo chữ ký số

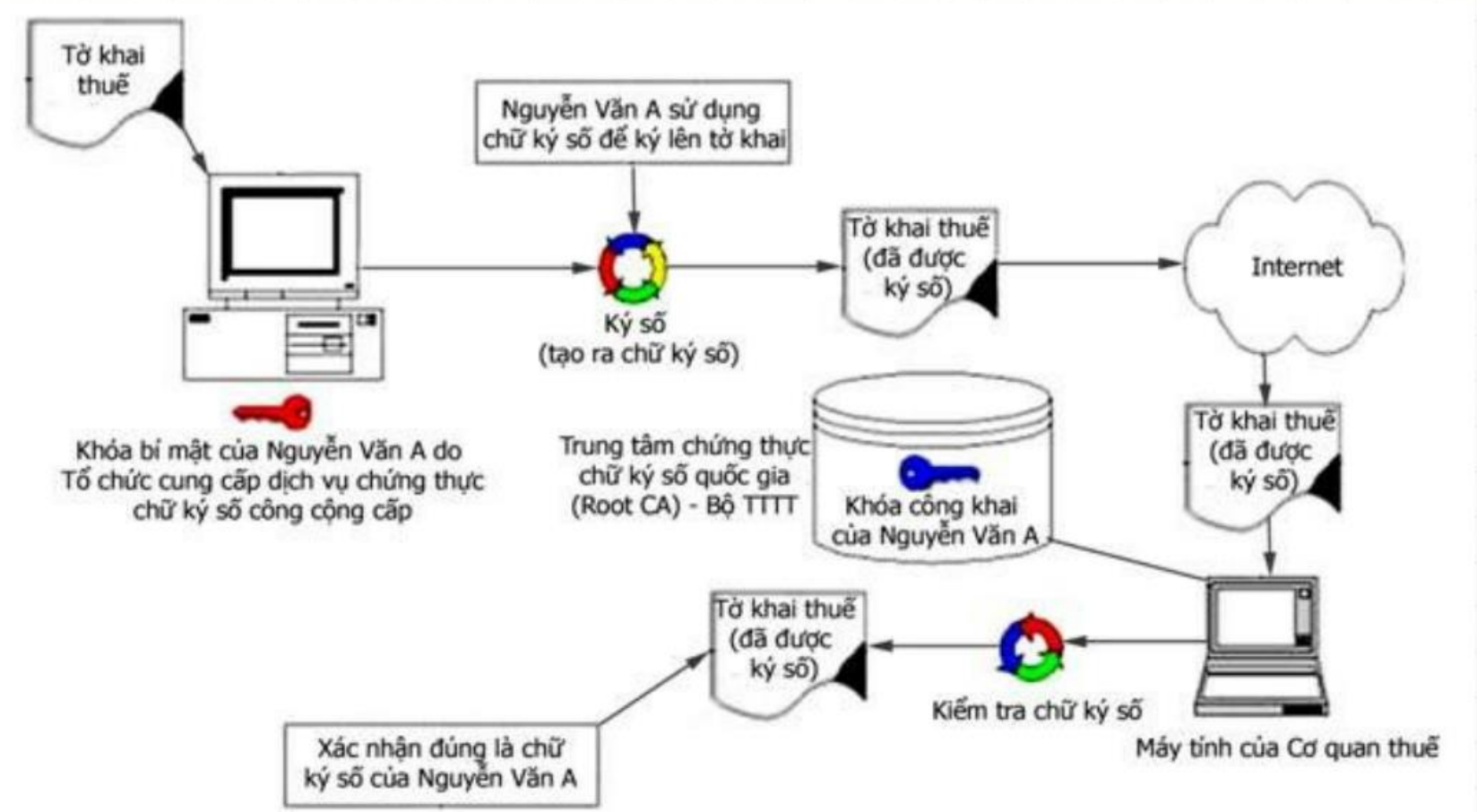


Quy trình tạo và xác thực chữ ký số

- Sơ kiểm tra và xác thực chữ ký số



Ví dụ ứng dụng chữ ký số



Đặc trưng của chữ ký số

- Là điều kiện cần và đủ để quy định tính duy nhất của văn bản điện tử cụ thể;
- Xác định rõ người chịu trách nhiệm trong việc tạo ra văn bản đó;
- Thể hiện sự tán thành đối với nội dung văn bản và trách nhiệm của người ký;
- Bất kỳ thay đổi nào (về nội dung, hình thức...) của văn bản trong quá trình lưu chuyển đều làm thay đổi tương quan giữa phần bị thay đổi với chữ ký.

Ưu điểm của chữ ký số

- Tính bảo mật an toàn thông tin tuyệt đối;
- Xác định được danh tính người dùng rõ ràng;
- Ký mọi lúc mọi nơi, bất kỳ đâu, tiết kiệm được nhiều thời gian chi phí đi lại, lưu giữ giấy tờ;
- Không thể phủ nhận nếu như đã ký;
- Tăng thêm uy tín doanh nghiệp trong mắt khách hàng, bảo mật tốt thông tin cần thiết.

Các lĩnh vực ứng dụng của chữ ký số

- Các hoạt động giao dịch trong ngân hàng, giải pháp Internet Banking;
- Giao dịch chứng khoán;
- Khai báo thuế điện tử trực tuyến;
- Khai báo hải quan trực tuyến;
- Khai báo BHXH, BHYT;
- Các thủ tục ký kết tại tổ chức, doanh nghiệp, …

Chứng thư điện tử

- Chứng thư điện tử (*chứng thư số/chứng chỉ số*) là một loại chứng nhận do các cơ quan chứng nhận CA (*Certification Authority)* cấp;
- CA thường là các cơ quan quản lý nhà nước, hoặc các tổ chức uy tín;
- Là căn cứ để xác thực các bên tham gia giao dịch;
- Là cơ sở đảm bảo tin cậy đối với các giao dịch thương mại điện tử.

Chứng thư điện tử

- Các CA quốc tế tiêu biểu:
  - www.thawte.com
  - www.globalsign.com
  - www.symantec.com
  - www.digicert.com
- Các CA ở Việt Nam tiểu biểu:
  - www.vnpt-ca.vn
  - www.viettel-ca.vn
  - www.fptca.net

Chứng thư điện tử

Nội dung của chứng thư điện tử

- Thông tin về tổ chức cung cấp dịch vụ chứng thực chữ ký điện tử;
- Thông tin về cơ quan, tổ chức, cá nhân được cấp chứng thư điện tử;
- Số hiệu của chứng thư điện tử;
- Thời hạn hiệu lực của chứng thư điện tử;
- Dữ liệu kiểm tra chữ ký điện tử của người được cấp chứng thư điện tử;

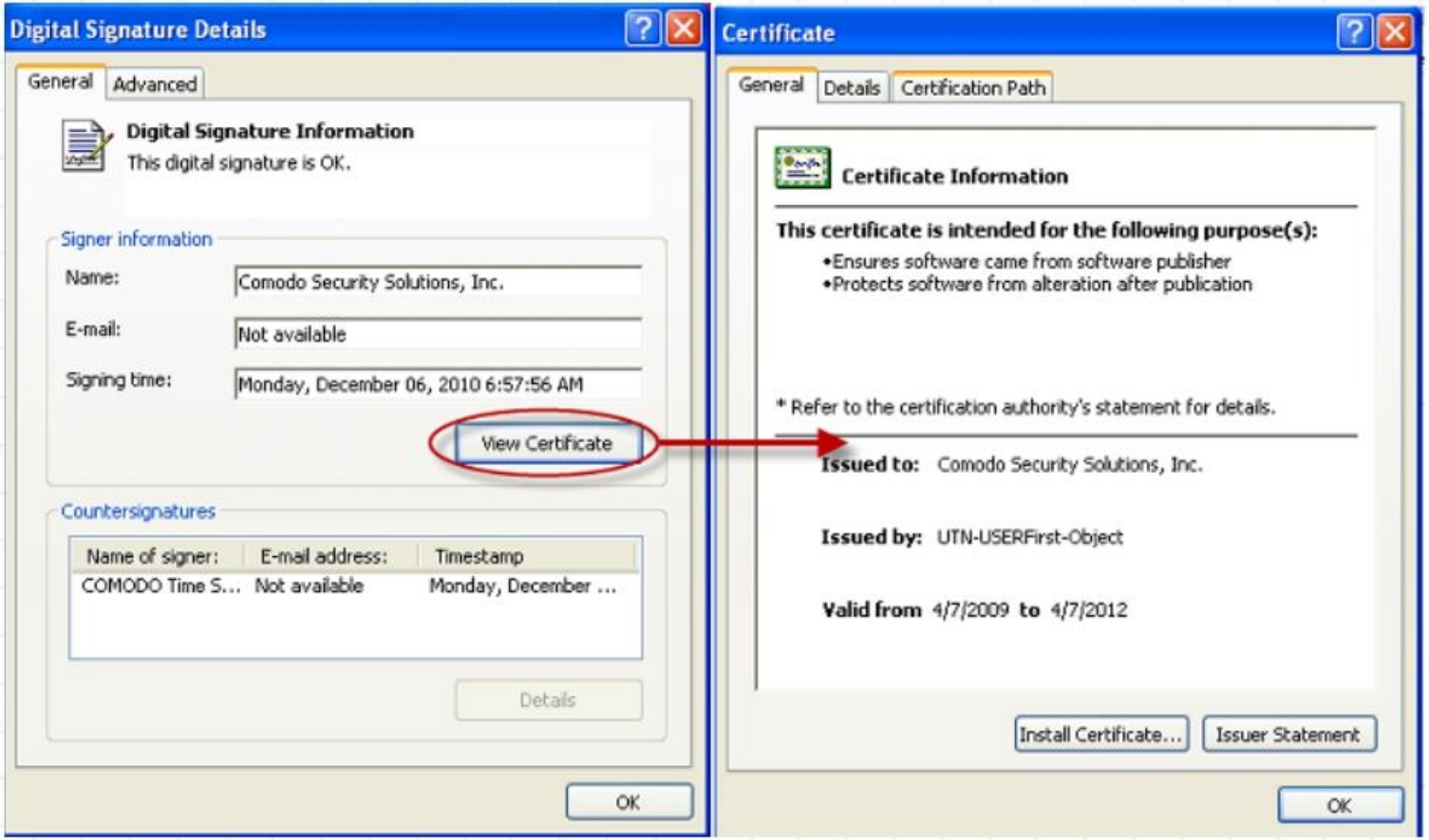
Chứng thư điện tử

Nội dung của chứng thư điện tử

- Chữ ký điện tử của tổ chức cung cấp dịch vụ chứng thực chữ ký điện tử;
- Các hạn chế về mục đích, phạm vi sử dụng của chứng thư điện tử;
- Các hạn chế về trách nhiệm pháp lý của tổ chức cung cấp dịch vụ chứng thực chữ ký điện tử;
- Các nội dung khác theo quy định của Chính phủ.

Chứng thư điện tử

- Ví dụ thông tin của một chứng thư số



Sự khác nhau giữa chữ ký số và chứng thư số

- ***Chứng thư số*** được sử dụng để các đối tác của doanh nghiệp biết và xác định được chữ ký của doanh nghiệp là đúng;
- ***Chữ ký số*** do người sử dụng tạo ra sau khi được CA cung cấp chứng thư số;
- Nếu chữ ký số được xem như "*chữ ký tay*" của mọi người thì chứng thư số của doanh nghiệp tượng trưng cho "*dấu mộc*" và được dùng trong việc ký số các thông điệp dữ liệu trong môi trường điện tử.

Sự khác nhau giữa chữ ký số và chứng thư số

- Ký số là việc đưa khóa bí mật vào một chương trình phần mềm để tự động tạo và gắn chữ ký số vào thông điệp dữ liệu.
- Chữ ký số được xem là an toàn *nếu chữ ký số được tạo ra trong* ***thời gian chứng thư số có hiệu lực*** *và* ***kiểm tra được bằng khóa công khai*** *ghi trên chứng thư số có hiệu lực đó.*


Time for Q&A