MỤC LỤC

LỜI CẢM ƠN.

Em xin chân thành cám ơn Ts. Lê Phê Đô – người luôn chỉ bảo, hướng dẫn, cung cấp những tài liệu quý báu trong quá trình học và hoàn thành đồ án này.

Em xin cám ơn các thầy cô giáo trong khoa công nghệ thông tin – trường DHDL Hải Phòng và gia đình đã tạo điều kiện giúp đỡ về vật chất cũng như tinh thần để em có thể học tập tốt và hoàn thành đồ án này

Sinh viên

Hà Thị Hồng Gấm

MỞ ĐẦU

Hàng ngày chúng ta vẫn hay dùng chữ ký để xác minh một vấn đề, hay để xác nhận quyền của mình đối với một vật thông qua những giấy tờ hoặc là một hợp đồng nào đó. Chẳng hạn như trên một bức thư nhận tiền từ ngân hàng, hay những hợp đồng ký kết mua bán, chuyển nhượng. Những chữ ký như vậy còn gọi là chữ ký viết tay, bởi nó được viết bởi chính tay người ký không thể sao chụp được. Thông thường chữ ký viết tay trên các văn bản, trên các tài liệu hay trên các hợp đồng kinh tế ...v.v ... thì được dùng để xác nhận người ký nó.

Ngày nay khi sự phát triển của internet và công nghệ thông tin ngày càng cao. Đã cho phép chúng ta thực hiện những giao dịch điện tử thông qua internet,nhưng tính linh hoạt của internet cũng tạo cơ hội cho "bên thứ ba" có thể thực hiện các hành động bất hợp pháp như: nghe trộm,giả mạo,mạo danh. Do vậy để đảm bảo an toàn trong các thương mại điện tử và các giao dịch điện tử cần có các hình thức bảo mật có hiệu quả nhất công nghệ phổ biến hiện nay được sử dụng là chữ ký số.

Từ những vấn đề an toàn về giao dịch và tính tương đồng và hợp lý của chữ ký bằng tay thì chữ ký điện tử ra đời co những nét đặc trưng của chữ ký bằng tay. Nhưng thông tin trên máy tính luôn được sao chép một cách dễ dàng việc thay đổi hoặc đánh cắp thông tin của một văn bản là rất đơn giản, cách sử dụng hình ảnh của chữ ký bằng tay không thể áp dụng vào được do vậy tạo ra một chữ ký số người ta phải áp dụng những công nghệ như mã hóa,chứng thực…

Đồ án này đề cập tới vấn đề chữ ký số và dịch vụ chứng thực chữ ký số.

Đồ án gồm 3 chương :

Chương I: Cơ sở toán học của chữ ký số.

Trong chương này đề cập tới các khái niệm toán học và cơ sở toán của chữ ký điện tử.

Chương II: Chữ ký số

Trong chương này ta tìm hiểu chi tiết về chữ ký số và một vài phương pháp ký

Chương III: Dịch vụ chứng thực chữ ký số.

Tìm hiểu về dịch vụ chứng thực chữ ký số và tình hình triển khai dịch vụ này trên thế giới và ở Việt Nam.

VÍ DỤ: Chứng thực macro trong Word và Excel

CHƯƠNG 1: CƠ SỞ TOÁN HỌC CỦA CHỮ KÝ SỐ

1 SỐ HỌC MODUL

1.1. Số nguyên tố

Định nghĩa:

Số nguyên tố là số nguyên dương chỉ chia hết cho 1 và chính nó

Tính chất:

- Giả sử p là số nguyên tố và p|a.b thì p|a hoặc p|b hoặc cả hai đều chia hết cho p.
- Có vô số số nguyên tố.

1.2. Đồng dư

Định nghĩa:

Nếu a và b là hai số nguyên, khi đó a được gọi là đồng dư với b theo modulo n, được viết $a \equiv b \pmod n$ nếu (a - b)chia hết cho n, và n được gọi là modulus của đồng dư.

Ví dụ :

$24 \equiv 9 \pmod 5$ vì 24 – 9 = 3 * 5.

$-11 \equiv 17 \pmod 7$ vì -11 – 17 = -4 * 7.

Tính chất

- $a \equiv b \pmod n$, nếu và chỉ nếu a và b đều trả số dư như nhau khi đem chia chúng cho n
- $a \equiv a \pmod n$ Tính phản xạ
- Nếu $a \equiv b \pmod n$ thì $b \equiv a \pmod n$ Tính đối xứng
- Nếu $a \equiv b \pmod n$ và $b \equiv c \pmod n$ thì $a \equiv c \pmod n$ Tính bắc cầu
- Nếu $a \equiv a_1 \pmod n$ và $b \equiv b_1 \pmod n$ thì $a + b \equiv a_1 + b_1 \pmod n$
- Nếu $a \equiv a_1 \pmod n$ và $b \equiv b_1 \pmod n$ thì $a * b \equiv a_1 * b_1 \pmod n$

1.3 Trong tập hợp Z_n và Z^*_n

Ta kí hiệu{0, 1, 2, ……., n-1} ≡ Z_n. Tập Z_n có thể được coi là tập hợp tất cả lớp tương đương trên Z_n theo modulo n. Trên tập Z_n các phép toán cộng, trừ, nhân được thực hiện theo modulo n.

Ví dụ: Z_{25} ={0,1,2,...,24}. Trong Z_{25} : 13+16 =4 bởi vì :$13+16=29 \equiv 4 \pmod{25}$

Tương tự, 13*16 = 8 trong Z_{25}

$Z^*_n = \{ p \in Z_n \mid UCLN(n,p) = 1 \}$

Ví dụ: $Z_2 = \{ 0,1 \}$

$Z^*_n = \{1 \}$ vì UCLN(1,2)=1

1.4. Phần tử nghịch đảo trong Z_n

Cho $a \in Z_n$. Nghịch đảo nhân của a theo modulo n là một số nguyên $x \in Z_n$ sao cho $a*x \equiv 1 \pmod n$. Nếu tồn tại thì đó là giá trị duy nhất và a gọi là khả đảo, nghịch đảo của a ký hiệu là a^{-1}.

Tính chất

Cho a, $b \in Z_n$, $a/b \bmod n = a.b^{-1} \bmod n$ được xác định khi và chỉ khi b là khả nghịch theo modulo n với $a \in Z_n$, phần tử a là khả nghịch khi và chỉ khi gcd(a,n) =1.

Hệ quả

Cho d=gcd(a,n). Khi đó phương trình đồng dư có dạng $a.x \equiv b \bmod n$ sẽ có nghiệm x khi và chỉ khi b chia hết cho d.

Thuật toán: Tính phần tử nghịch đảo trên Z_n

INPUT: $a \in Z_n$

OUTPUT: $a^{-1} \bmod n$, nếu tồn tại.

Sử dụng thuật toán Euclide mở rộng, tìm x và y để ax+ny=d, trong đó gcd(a,n)

Nếu d>1, thì $a^{-1} \bmod n$ không tồn tại, ngược lại kết quả x

1.5. Nhóm nhân Z^*_n

Định nghĩa:

Nhóm nhân của Z_n ký hiệu là $Z^*_n = \{ a \in Z_n \mid \gcd(a,n)=1 \}$. Đặc biệt, nếu n là số nguyên tố thì $Z^*_n = \{ a \mid 1 \le a \le n-1 \}$.

Tập Z^* lập thành một nhóm con đối với phép nhân của Z_n vì trong Z^*_n phép chia theo modulo n bao giờ cũng thực hiện được.

Tính chất 1

Cho $n \ge 2$ là số nguyên

(i).Định lý Euler: Nếu $a \in Z^*_n$ thì $a^{\phi(n)} \equiv 1 \pmod n$.

(ii).Nếu n là tích của các số nguyên tố phân biệt và nếu $r \equiv s \pmod{\phi(n)}$ thì $a^t \equiv a^s \pmod n$ với mọi số nguyên a. Nói cách khác, làm việc với các số theo modulo nguyên tố p thì số mũ có thể giảm theo modulo $\phi(n)$.

Tính chất 2

Cho số nguyên tố p

Định lý Fermat: Nếu gcd(a,p)=1 thì $a^{p-1} \equiv 1 \pmod p$

Nếu $r \equiv s \pmod{p-1}$ thì $a^t \equiv a^s \pmod{p}$ với mọi số nguyên a. Nói cách khác, làm việc với các số theo modulo nguyên tố p thì số mũ có thể giảm theo modulo p-1.

Đặc biệt, $a^p \equiv a \pmod{p}$ với mọi số nguyên a.

1.6. Thặng dư bậc hai theo modulo

Đinh nghĩa:

Cho $a \in Z^*_n$, a được gọi là thặng dư bậc hai theo modulo n, nếu tồn tại một $x \in Z^*_n$, sao cho $x^2 \equiv a \bmod n$, và nếu không tồn tại x như vậy thì a được gọi là bất thặng dư bậc hai theo modulo n, Tập các thặng dư bậc hai ký hiệu là Q_n và tập các bất thặng dư bậc hai ký hiệu là $\overline{Q_n}$.

Tính chất:

Cho p là nguyên tố lẻ và α là phần tử sinh của Z^*_p, thì $a \in Z^*_p$ là thặng dư bậc hai modulo p khi và $a = a^i \bmod p$.

Thuật toán: Tính luỹ thừa theo modulo n trong Z_n

INPUT: $a \in Z_n$, số nguyên $0 \le k \le n$ trong đó k biểu diễn dạng nhị phân. $k = \sum_{i=0}^{t} k_i 2^i$

OUTPUT: $a^k \bmod n$

1. Đặt $b \leftarrow 1$, nếu k=0 thì kết quả b
2. Đặt $A \leftarrow a$.
3. Nếu k_0=1, thì đặt $b \leftarrow a$.
4. Với mỗi I từ 1 đến t, thực hiện như sau:
   4.1 Đặt $A \leftarrow A^2 \bmod n$.
   4.2 Nếu k_i=1, thì $b \leftarrow A.b \bmod n$
5. Kết quả b

Ví dụ: Bảng dưới đây mô tả các bước thực hiện để tính luỹ thừa theo *modulo 1234*. của phép tính $5^{596} \bmod 1234 = 1013$.

i	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
k_i	*0*	*0*	*1*	*0*	*1*	*0*	*1*	*0*	*0*	*1*
A	*5*	*25*	*625*	*681*	*1011*	*369*	*421*	*779*	*947*	*925*
b	*1*	*1*	*625*	*625*	*67*	*67*	*1059*	*1059*	*1059*	*1013*

Phép toán	Độ phức tạp

Phép cộng modulo	(a+b)mod n	O(ln n)
Phép trừ modulo	(a-b)mod n	O(ln n)
Phép nhân modulo	(a.b)mod n	$O((\ln n)^2)$
Phép lấy nghịch đảo	a^{-1} mod n	$O((\ln n)^2)$
Phép tính lũy thừa modulo	a^k mod n, k<n	$O((\ln n)^3)$

2. Hàm băm

2.1. Giới thiệu

Theo các sơ đồ chữ ký thì chữ ký của thông điệp cũng có độ dài bằng độ dài của thông điệp, đó là một điều bất tiện. Ta mong muốn như trong trường hợp chữ ký viết tay, chữ ký có độ dài ngắn và hạn chế cho dù văn bản có độ dài bằng bao nhiêu. Vì chữ ký số được ký cho từng bit của thông điệp, nếu muốn chữ ký có độ dài hạn chế trên thông điệp có độ dài tùy ý thì ta phải tìm cách rút gọn độ dài thông điệp. Nhưng bản thân thông điệp không thể rút ngắn được, nên chỉ còn cách là tìm cho mỗi thông điệp một thông điệp thu gọn có độ dài hạn chế và thay việc ký trên thông điệp, ta ký trên thông điệp thu gọn.

Để giải quyết vấn đề này ta sử dụng hàm băm, chấp nhận một thông điệp có độ dài tuỳ ý làm đầu vào. Hàm băm sẽ biến đổi thông điệp này thành một thông điệp rút gọn và sau đó sẽ dùng lược đồ ký để ký lên thông điệp rút gọn đó.

2.2. Định nghĩa

Hàm Hash là hàm tính toán có hiệu quả khi ánh xạ các dòng nhị phân có độ dài tùy ý thành những dòng nhị phân có độ dài cố định nào đó.

- Hàm Hash yếu: hàm Hash gọi là yếu nếu cho một thông báo x thì về mặt tính toán không tìm ra được thông báo x’ khác x sao cho:

$h(x') = h(x)$

- Hàm Hash mạnh: hàm Hash được gọi là mạnh nếu về mặt tính toán không tìm ra được hai thông báo x và x’ sao cho:

$x_1 \neq x_2$ và $h(x_1) = h(x_2)$

Nói cách khác, tìm hai văn bản khác nhau có cùng một đại diện là cực kỳ khó

Hàm Hash phải là hàm một phía, nghĩa là cho x tính z = h(x) thì dễ, nhưng ngược lại, biết z tính x là công việc cực khó.

Hàm Hash yếu làm cho chữ ký trở lên tin cậy giống như việc ký trên toàn thông báo.

Hàm Hash mạnh có tác dụng chống lại kẻ giả mạo tạo ra hai bản thông báo có nội dung khác nhau, sau đó thu nhận chữ ký hợp pháp cho một bản thông báo dễ được xác nhận rồi lấy nó giả mạo làm chữ ký của thông báo thứ 2 hay nói cách khác tìm 2 văn bản khác nhau có cùng một đại diện là cực kỳ khó.

Một hàm băm tốt phải thỏa mãn các điều kiện sau:

- Tính toán nhanh.
- Các khoá được phân bố đều trong bảng.
- Ít xảy ra đụng độ.
- Xử lý được các loại khóa có kiểu dữ liệu khác nhau.

2.3 Ứng dụng

Các hàm băm được ứng dụng trong nhiều lĩnh vực, chúng thường được thiết kế phù hợp với từng ứng dụng. Ví dụ, các hàm băm mật mã học giả thiết sự tồn tại của một đối phương - người có thể cố tình tìm các dữ liệu vào với cùng một giá trị băm. Một hàm băm tốt là một phép biến đổi "một chiều", nghĩa là không có một phương pháp thực tiễn để tính toán được dữ liệu vào nào đó tương ứng với giá trị băm mong muốn, khi đó việc giả mạo sẽ rất khó khăn. Một hàm một chiều mật mã học điển hình không có tính chất hàm đơn ánh và tạo nên một hàm băm hiệu quả; một hàm trapdoor mật mã học điển hình là hàm đơn ánh và tạo nên một hàm ngẫu nhiên hiệu quả.

Bảng băm, một ứng dụng quan trọng của các hàm băm, cho phép tra cứu nhanh một bản ghi dữ liệu nếu cho trước khóa của bản ghi đó (Lưu ý: các khóa này thường không bí mật như trong mật mã học, nhưng cả hai đều được dùng để "mở khóa" hoặc để truy nhập thông tin.) Ví dụ, các khóa trong một từ điển điện tử Anh-Anh có thể là các từ tiếng Anh, các bản ghi tương ứng với chúng chứa các định nghĩa. Trong trường hợp này, hàm băm phải ánh xạ các xâu chữ cái tới các chỉ mục của mảng nội bộ của bảng băm.

Các hàm băm dành cho việc phát hiện và sửa lỗi tập trung phân biệt các trường hợp mà dữ liệu đã bị làm nhiễu bởi các quá trình ngẫu nhiên. Khi các hàm băm được dùng cho các giá trị tổng kiểm, giá trị băm tương đối nhỏ có thể được dùng để kiểm chứng rằng một file dữ liệu có kích thước tùy ý chưa bị sửa đổi. Hàm băm được dùng để phát hiện lỗi truyền dữ liệu. Tại nơi gửi, hàm băm được tính cho dữ liệu được gửi, giá trị băm này được gửi cùng dữ liệu. Tại đầu nhận, hàm băm lại được tính lần nữa, nếu các giá trị băm không trùng nhau

thì lỗi đã xảy ra ở đâu đó trong quá trình truyền. Việc này được gọi là kiểm tra dư (redundancy check).

Các hàm băm còn được ứng dụng trong việc nhận dạng âm thanh, chẳng hạn như xác định xem một file MP3 có khớp với một file trong danh sách một loại các file khác hay không.

Thuật toán tìm kiếm xâu Rabin-Karp là một thuật toán tìm kiếm xâu kí tự tương đối nhanh, với thời gian chạy trung bình O(n). Thuật toán này dựa trên việc sử dụng băm để so sánh xâu.

2.4. Một số hàm Hash sử dụng trong chữ ký số

2.4.1. Các hàm Hash đơn giản:

Tất cả các hàm Hash đều được thực hiện theo quy tắc chung là: Đầu vào được biểu diễn dưới dạng một dãy các khối n bit, các khối n bit này được xử lý theo cùng một kiểu và lặp đi lặp lại để cuối cùng cho đầu ra có số bit cố định.

Hàm Hash đơn giản nhất là thực hiện phép toán XOR từng bit một của mỗi khối. Nó được biểu diễn như sau:

$C_i = b_{1i} \oplus b_{2i} \oplus \ldots \oplus b_{mi}$

Trong đó :

C_i : là bit thứ i của mã Hash, i = $\overline{1,n}$

m : là số các khối đầu vào

b_{ji} : là bit thứ i trong khối thứ j

$\oplus$: là phép cộng modulo 2

Sơ đồ hàm Hash sử dụng phép XOR.

Khối 1:	b_{11}	b_{12}	…	b_{1n}
Khối 2:	b_{21}	b_{22}	…	b_{2n}
…	…	…	…	…
Khối m:	b_{m1}	b_{m2}	…	b_{mn}
Mã Hash:	C_1	C_2	…	C_n

C_i là bit kiểm tra tính chẵn lẻ cho vị trí thứ i khi ta chia tệp dữ liệu thành từng khối, mỗi khối con vị trí. Nó có tác dụng như sự kiểm tra tổng thể tính toàn vẹn của dữ liệu.

Khi mã hóa một thông báo dài thì ta sử dụng mode CBC (The Cipher Block Chaining), thực hiện như sau:

Giả sử thông báo X được chia thành các khối 64 bit liên tiếp

$X= X_1X_2 \dots X_n$

Khi đó mã Hash C sẽ là:

$C = X_{NH} = X_1 \oplus X_2 \oplus \dots \oplus X_n$

Sau đó mã hóa toàn bộ thông báo nối với mã Hash theo mode CBC sản sinh ra bản mã.

$Y_1Y_2 \dots Y_{N+1}$

2.4.2. Kỹ thuật khối xích :

Người ta đầu tiên đề xuất kỹ thuật mật mã xích chuỗi nhưng không có khóa bí mật là Rabin.

Kỹ thuật này được thực hiện như sau :

Chia thông báo M thành các khối có cỡ cố định là $M_1, M_2, \dots, M_N$, sử dụng hệ mã thuận tiện như DES để tính mã Hash như sau :

H_0 = giá trị ban đầu

$H_i = E_{Mi}(H_{i-1})$, $i = \overline{1, N}$

$G = H_N$

2.5. Các hàm Hash mở rộng:

Ở trên, ta đề cập đến hàm Hash có nhiều đầu vào hữu hạn. Tiếp theo ta sẽ đề cập tới loại hàm Hash mạnh với đầu vào vô hạn thu được do mở rộng một hàm Hash mạnh có đầu vào độ dài hữu hạn. Hàm này sẽ cho phép ký các thông báo có độ dài tùy ý.

Giả sử $h: (Z_2)^m \rightarrow (Z_2)^t$ là một hàm Hash mạnh, trong đó $m \geq t + 1$ ta sẽ xây dựng một hàm Hash mạnh :

$h^*: X \rightarrow (Z_2)^t$, trong đó $\overset{\infty}{\underset{i=m}{X}} = \cup(Z_2)^i$

❖ Xét trường hợp $m \geq t + 2$

Giả sử $x \in X$, vậy thì tồn tại n để $x \in (Z_2)^n$, $n \geq m$.

Ký hiệu : $|x|$ là độ dài của x tính theo bit. Khi đó, $|x| = n$.

Ký hiệu : $x \,||\, y$ là dãy bit thu được do nối x với y.

Giả sử $|x| = n \geq m$. Ta có thể biểu diễn x như sau:

$x = x_1 \,||\, x_2 \,||\, \dots \,||\, x_k$

Trong đó $|x_1| = |x_2| = \ldots = |x_{k-1}| = m - t - 1$ và $|x_k| = m - t - 1 - d$,

$0 \le d \le m - t - 2$

$\Rightarrow |x_k| \ge 1$ và $m - t - 1 \ge 1$, $k \ge 2$.

Khi đó: $k = \left\lfloor \frac{n}{m-t-1} \right\rfloor + 1$

Thuật toán xây dựng h thành h* được mô tả như sau :

1. Cho i = 1 tới k-1 gán $y_i = x_i$;
2. $y_k = x_k \,||\, 0^d$ (0^d là dãy có d số 0. Khi đó y_k dài m-t-1)
3. y_{k+1} là biểu diễn nhị phân của d ($|y_{k+1}| = m-t-1$)
4. $g_1 = h(0^{t+1} || y_1)$ ($|g_1| = t$, $0^{t+1} || y_1$ dài m)
5. Cho i=1 tới k thực hiện

   $g_{i+1} = h(g_i || 1 || y_{i+1})$

   a. $h^*(x) = g_{k+1}$

Ký hiệu $y(x) = y_1 \,||\, y_2 \,||\ldots||\, y_{k+1}$

Ta thấy rằng $y(x) \ne y(x')$ nếu $x \ne x'$

❖ Xét trường hợp m=t+1

Cũng như trên, ta giả sử |x| = n >m

Ta xác định f như sau:

f(0) = 0;

f(1) = 01;

Thuật toán xây dựng h* khi m=t+1 như sau :

1. Cho $y= y_1,y_2, \ldots, y_k =11 \,||\, f(x_1) \,||\, f(x_2) \ldots f(x_n)$ (x_1 là một bit)
2. $g_1 = h(0^t || y_1)$ ($|y_1| = m - t$)
3. Cho i=1 tới k -1 thực hiện

   $g_{i+1} = h(g_i || y_{i+1})$ ($|y_i| = m - t - 1$)
4. $h^*(x) = g_{k^*s}$

Ngoài ra còn có một số hàm Hash khác như hàm Hash MD4 và hàm Hash MD5.

3.Hệ mật mã

3.1 Giới thiệu về hệ mật mã

Mật mã đã được sử dụng từ rất sớm, khi con người biết trao đổi thông tin cho nhau và trải qua bao nhiêu năm nó đã được phát triển từ những hình thức sơ khai cho đến hiện đại và tinh vi. Mật mã được sử dụng trong rất nhiều lĩnh vực của con người và các quốc gia, đặc biệt trong các lĩnh vực quân sự, chính trị, ngoại giao và thương mại. Mục đích của mật mã là tạo ra khả năng trao đổi thông tin trên một kênh thông tin chung cho những đối tượng cùng tham gia trao đổi thông tin và không muốn một đối tượng thứ ba khác biết được những thông tin mà họ trao đổi.

Khi một đối tượng A muốn gửi một thông điệp cho những người nhận, A sẽ phải mã hóa thông điệp và gửi đi, những người nhận được thông điệp mã hóa muốn biết được nội dung thì phải giải mã thông điệp mã hóa. Các đối tượng trao đổi thông tin cho nhau phải thỏa thuận với nhau về cách thức mã hóa và giải mã, quan trọng hơn là khóa mật mã đã sử dụng trong quá trình mã hóa và giải mã, nó phải tuyệt đối được giữ bí mật. Một đối tượng thứ ba mặc dù có biết được nhưng sẽ không biết được nội dung thông điệp đã mã hóa.

Có hai phương pháp mã hóa dữ liệu là Mã hóa khóa đối xứng và Mã hóa khóa công khai.

3.2. Sơ đồ hệ thống mật mã

Là một bộ năm (P, C, K, E, D) trong đó:

+ P là một tập hữu hạn các bản rõ.

+ C là một tập hữu hạn các bản mã.

+ K là một tập hữu hạn các khoá.

+ Với mỗi k ϵ K, có một hàm lập mã $e_k \epsilon E$

$$e_k : P \rightarrow C$$

và một hàm giải mã $d_k \epsilon D$

$$d_k : C \rightarrow P \text{ sao cho } d_k(e_k(x)) = x \text{ với mọi } x \epsilon P$$

3.3. Mật mã khóa đối xứng

Phương pháp mã hóa đối xứng (symmetric cryptography) còn được gọi là mã hóa khóa bí mật (secret key cryptography). Với phương pháp này, người gửi và người nhận sẽ dùng chung một khóa để mã hóa và giải mã thông điệp. Trước khi mã hóa thông điệp gửi

đi, hai bên gửi và nhận phải có khóa chung và phải thống nhất thuật toán dùng để mã hóa và giải mã. Có nhiều thuật toán ứng dụng cho mã hóa khóa bí mật DES - Data Encrytion Standard, 3DES - triple-strength DES, RC2 - Rons Cipher 2 và RC4, v.v... và sơ khai nhất là các hệ mật mã cổ điển.

Nhược điểm chính của phương pháp này là khóa được truyền trên kênh an toàn nên chi phí tốn kém và không kip thời. Ưu điểm là tốc độ mã hóa và giải mã rất nhanh.

❖ **Một số hệ mật mã cổ điển**

3.3.1. Mã dịch chuyển:

Định nghĩa: Mã dịch chuyển: (P, C, K, E, D)

P = C = K = Z_{26} với k є K, định nghĩa $e_k(x) = (x + k) \bmod 26$ $d_k(y) = (y – k) \bmod 26$

(x, y є Z_{26})

Ví dụ: Dùng khoá k = 9 để mã hoá dòng thư: “toinaydichoi” dòng thư đó tương ứng với dòng số

t	o	i	n	a	y	d	i	c	h	o	i
19	14	8	12	0	24	3	8	2	7	14	8

qua phép mã hoá e_9 sẽ được:

2	23	17	22	9	7	12	17	11	16	23	17
c	x	r	w	j	h	m	r	l	q	x	r

bản mã sẽ là:

“qnwcxrcqdkjh”

Nhận được bản mã đó, dùng d_9 để nhận được bản rõ.

Cách đây 2000 năm mã dịch chuyển đã được Julius Ceasar sử dụng, với khoá k=3 mã đích chuyển được gọi là mã Ceasar.

Tập khoá phụ thuộc vào Z_m với m là số khoá có thể.

Trong tiếng Anh tập khoá chỉ có 26 khoá có thể, việc thám mã có thể được thực hiện bằng cách duyệt tuần tự 26 khoá đó, vì vậy độ an toàn của mã dịch chuyển rất thấp.

3.3.2. Mã thay thế:

Định nghĩa Mã thay thế: (P, C, K, E, D)

$P = C = Z_{26}$, $K = S(Z_{26})$ Với mỗi $\pi \in K$, tức là một hoán vị trên Z_{26}, ta xác định

$$e_\pi(x) = \pi(x)$$

$$d_\pi(y) = \pi^{-1}(y)$$

với $x, y \in Z_{26}$, π^{-1} là nghịch đảo của л

Ví dụ: π được cho bởi (ở đây ta viết chữ cái thay cho các con số thuộc Z_{26}):

a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*
x	*n*	*y*	*a*	*h*	*p*	*o*	*g*	*z*	*q*	*w*	*b*	*t*	*s*

o	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*
f	*l*	*r*	*c*	*v*	*m*	*u*	*e*	*k*	*j*	*d*	*i*

bản rõ:

"toinaydichoi"

sẽ được mã hoá thành bản mã (với khoá π):

"mfzsxdazygfz"

Dễ xác định được π^{-1}, và do đó từ bản mã ta tìm được bản rõ.

Mã thay thế có tập hợp khoá khá lớn - bằng số các hoán vị trên bảng chữ cái, tức số các hoán vị trên Z_{26}, hay là $26! > 4.10^{26}$. Việc duyệt toàn bộ các hoán vị để thám mã là rất khó, ngay cả đối với máy tính. Tuy nhiên, bằng phương pháp thống kê, ta có thể dễ dàng thám được các bản mã loại này, và do đó mã thay thế cũng không thể được xem là an toàn.

3.3.3. Mã Anffine:

Định nghĩa Mã Anffine: (P, C, K, E, D)

$$P = C = Z_{26}, K = \{ (a, b) \epsilon Z_{26} x Z_{26} : (a, 26) = 1 \}$$

với mỗi k = (a, b) ϵ K ta định nghĩa:

$$e_k(x) = ax + b \bmod 26$$

$$d_k(y) = a^{-1}(y - b) \bmod 26$$

trong đó x, y ϵ Z_{26}

Ví dụ: Lấy k = (5, 6).

Bản rõ:

"toinaydichoi"

	t	o	i	n	a	y	d	i	c	h	o	i
x	19	14	8	13	0	14	3	8	2	7	14	8

y=5x + 6 mod 26

y	23	24	20	19	6	24	21	20	16	15	24	20
	x	y	u	t	g	y	v	u	q	p	y	u

Bản mã:

"xyutgyvuqpyu"

Thuật toán giải mã trong trường hợp này có dạng:

$$d_k(y) = 21(y - 6) \bmod 26$$

Với mã Apphin, số các khoá có thể có bằng (số các số ≤ 26 và nguyên tố với 26) × 26, tức là 12 × 26 = 312. Việc thử tất cả các khoá để thám mã trong trường hợp này tuy khá mất thì giờ nếu tính bằng tay, nhưng không khó khăn gì nếu dùng máy tính. Do vậy, mã Apphin cũng không phải là mã an toàn.

3.3.4. Mã Vigenère:

Định nghĩa Mã Vigenere: (P, C, K, E, D)

Cho m là số nguyên dương.

$$P = C = K = Z_{26}^{m}$$

với mỗi khoá $k = (k_1, k_2,\ldots,k_m) \epsilon K$ có:

$$e_k(x_1, x_2,\ldots, x_m) = (x_1 + k_1, x_2 + k_2,\ldots, x_m + k_m)$$

$$d_k(y_1, y_2,\ldots, y_m) = (y_1 - k_1, y_2 - k_2,\ldots, y_m - k_m)$$

các phép cộng phép trừ đều lấy theo modulo 26

Ví dụ: Giả sử m = 6 và khoá k là từ CIPHER - tức k=(2, 8, 15, 7, 4, 17).

Bản rõ:

"toinaydichoi"

	t	o	i	n	a	y	d	i	c	h	o	i
x	19	14	8	13	0	24	3	8	2	7	14	8
k	2	8	15	7	4	17	2	8	15	7	4	17
y	21	22	23	20	4	15	5	16	17	14	18	25
	v	w	x	u	e	p	f	q	r	o	s	z

Bản mã

"vwxuepfqrosz"

Từ bản mã đó, dùng phép giải mã d_k tương ứng, ta lại thu được bản rõ.

Chú ý: Mã Vigenere với m = 1 sẽ trở thành mã Dịch chuyển.

Tập hợp các khoá trong mã Vigenere mới $m \geq 1$ có tất cả là 26^m khoá có thể có. Với m = 6, số khoá đó là 308.915.776, duyệt toàn bộ chừng ấy khoá để thám mã bằng tính tay thì khó, nhưng với máy tính thì vẫn là điều dễ dàng.

3.3.5. Mã Hill:

Định nghĩa Mã Hill: (P, C, K, E, D)

Cho m là số nguyên dương.

$$P = C = Z_{26}^{m}$$

$K = \{ k \in Z_{26}^{mxm} : (\det(k), 26) = 1 \}$

với mỗi $k \in K$ định nghĩa:

$$e_k(x_1, x_2,\ldots, x_m) = (x_1, x_2,\ldots, x_m).k$$

$$d_k(y_1, y_2,\ldots, y_m) = (y_1, y_2,\ldots,y_m).k^{-1}$$

Ví dụ: Lấy m = 2, và $k = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$

Với bộ 2 ký tự (x_1, x_2), ta có mã là $(y_1, y_2) = (x_1, x_2)$. k được tính bởi

$$y_1 = 11.x_1 + 3.x_2$$

$$y_2 = 8.x_1 + 7.x_2$$

Giả sử ta có bản rõ: "**tudo**", tách thành từng bộ 2 ký tự, và viết dưới dạng số ta được

19 20 | 03 14 , lập bản mã theo quy tắc trên, ta được bản mã dưới dạng số là: 09 06 | 23 18, và dưới dạng chữ là "**fgxs**".

Chú ý:

Để đơn giản cho việc tính toán, thông thường chọn ma trận vuông 2×2. Khi đó có thể tính ma trận nghịch đảo theo cách sau :

Giả sử ta có

$$k = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Ta có ma trận nghịch đảo

$$k^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$$

Và được tính như sau

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}$$

Một chú ý là để phép chia luôn thực hiện được trên tập Z_{26} thì nhất thiết định thức của k : det(k) = (ad – bc) phải có phần tử nghịch đảo trên Z_{26}, nghĩa là (ad – bc) phải là một trong các giá trị : 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, hoặc 25. Đây cũng là điều kiện để ma trận k tồn tại ma trận nghịch đảo.

Khi đó: $k^{-1}.k = I$ là ma trận đơn vị (đường chéo chính bằng 1)

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Định thức của $\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$

Là 11*7 – 8*3 = 1 ≡ 1 mod 26

Khi đó

$$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}^{-1} = \begin{pmatrix} 7 & -8 \\ -3 & 11 \end{pmatrix} \equiv \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \ mod\ 26$$

3.3.6. Mã hoán vị:

Định nghĩa Mã hoán vị: (P, C, K, E, D)

Cho m là số nguyên dương.

$P = C = Z_{26}$, $K = S_m$

với mỗi k = π є S_m, ta có

$$e_k(x_1, x_2, \ldots, x_m) = (x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(m)})$$

$$d_k(y_1, y_2, \ldots, y_m) = (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)}, \ldots, y_{\pi^{-1}(m)})$$

trong đó π^{-1} là hoán vị nghịch đảo của π

Ví dụ: Giả sử m = 6, và khoá k được cho bởi phép hoán vị π

1	2	3	4	5	6
3	5	1	6	4	2

Khi đó phép hoán vị nghịch đảo π^{-1} là:

1	2	3	4	5	6
3	6	1	5	2	4

Bản rõ:

"toinaydichoi"

	t	o	i	n	a	y	d	i	c	h	o	i
vt	1	2	3	4	5	6	1	2	3	4	5	6
π	1->3	2->5	3->1	4->6	5->4	6->2	1->3	2->5	3->1	4->6	5->4	6->2
vt	3	5	1	6	4	2	3	5	1	6	4	2
	i	a	t	y	n	o	c	o	d	i	h	i

Bản mã:

"iatynocodihi"

Dùng hoán vị nghịch đảo, từ bản mật mã ta lại thu được bản rõ.

Chú ý:

Mã hoán vị là một trường hợp riêng của mã Hill. Thực vậy, cho phép hoán vị π của {1, 2,…, m}, ta có thể xác định ma trận $K_\pi=(k_{ij})$, với

$$k_{ij}=\begin{cases}1 & \text{nếu } \quad i=\pi(j)\\ 0 & \text{nếu ngược lại}\end{cases}$$

Thì dễ thấy rằng mã Hill với khoá K_π trùng với mã hoán vị với khoá π.

Với m cho trước, số các khoá có thể có của mã hoán vị là m!

Dễ nhận thấy với m = 26 ta có số khóa 26! (mã Thay thế).

3.4. Mã khóa công khai:

Phương pháp mã hóa khóa công khai (*public key cryptography*) còn được gọi là mã hóa bất đối xứng (*asymmetric cryptography*) đã giải quyết được vấn đề của phương pháp mã hóa khóa bí mật (*đối xứng*) là sử dụng hai khóa: khóa bí mật (*private key*) và (*public key*). Khóa bí mật được giữ kín, trong khi đó được gửi công khai bởi vì tính chất khó tính được khóa bí mật từ khóa công khai. Khóa công khai và khóa bí mật có vai trò trái ngược nhau, một khóa dùng để mã hóa và khóa kia sẽ dùng để giải mã.

Hiện nay các hệ mật mã khóa công khai đều dựa trên hai bài toán "khó" là bài toán logarith rời rạc trên trường hữu hạn và bài toán tìm ước số nguyên tố.

Phương pháp cho phép trao đổi khóa một cách dễ dàng và tiện lợi. Nhưng tốc độ mã hóa khá chậm hơn rất nhiều so với phương pháp mã hóa khóa đối xứng rất nhiều, Tuy nhiên, hệ mật mã khóa công khai có một ưu điểm nổi bật là cho phép tạo chữ ký điện tử.

❖ Một số hệ mật mã khóa công khai

3.4.1 Hệ mật mã RSA

Trong mật mã học, RSA là một thuật toán mật mã hóa khóa công khai. Đây là thuật toán đầu tiên phù hợp với việc tạo ra chữ ký điện tử đồng thời với việc mã hóa. Nó đánh dấu một sự tiến bộ vượt bậc của lĩnh vực mật mã học trong việc sử dụng khóa công cộng. RSA đang được sử dụng phổ biến trong thương mại điện tử và được cho là đảm bảo an toàn với điều kiện độ dài khóa đủ lớn.Thuật toán được Ron Rivest, Adi Shamir và Len Adleman mô tả lần đầu tiên vào năm 1977 tại Học viện Công nghệ Massachusetts (MIT). Tên của thuật toán lấy từ 3 chữ cái đầu của tên 3 tác giả.Trước đó, vào năm 1973, Clifford Cocks, một nhà toán học người Anh làm việc tại GCHQ, đã mô tả một thuật toán tương tự. Với

khả năng tính toán tại thời điểm đó thì thuật toán này không khả thi và chưa bao giờ được thực nghiệm. Tuy nhiên, phát minh này chỉ được công bố vào năm 1997 vì được xếp vào loại tuyệt mật.Thuật toán RSA được MIT đăng ký bằng sáng chế tại Hoa Kỳ vào năm 1983 (Số đăng ký 4.405.829). Bằng sáng chế này hết hạn vào ngày 21 tháng 9 năm 2000. Tuy nhiên, do thuật toán đã được công bố trước khi có đăng ký bảo hộ nên sự bảo hộ hầu như không có giá trị bên ngoài Hoa Kỳ. Ngoài ra, nếu như công trình của Clifford Cocks đã được công bố trước đó thì bằng sáng chế RSA đã không thể được đăng ký.

Hệ mật mã khóa công khai RSA được đưa ra năm 1977, là công trình nghiên cứu của ba đồng tác giả Ronald Linn Revest, Adi Shamir, Leonard Aldeman. Hệ mật mã được xây dựng dựa trên tính khó giải của bài toán phân tích thừa số nguyên tố hay còn gọi là bài toán RSA

Định nghĩa: Bài toán RSA

Cho một số nguyên dương n là tích của hai số nguyên tố lẻ p và q. Một số nguyên dương b sao cho gcd(b, (p-1) *(q-1)) =1 và một số nguyên c. Bài toán đặt ra là phải tìm số nguyên x sao cho $x^b \equiv c(\text{mod } n)$

Thuật toán: Sinh khóa cho mã khóa công khai RSA

Sinh hai số nguyên tố lớn p và q có giá trị xấp xỉ nhau.

Tính n=p*q, và $\phi(n) = (p-1)(q-1)$, sao cho gcd(b, $\phi(n)$) =1

Chọn một số ngẫu nhiên b, $1 < b < \varphi(n)$, sao cho gcd(b, $\varphi(n)$) = 1

Sử dụng thuật toán Euclide để tính số a, $1<a<\phi(n)$, sao cho $a*b \equiv 1(\text{mod } \phi(n))$

Khóa công khai là (n, b). Khóa bí mật là a

Thuật toán: Mã hóa RSA

(i). Lập mã :

a. Lấy khóa công khai (n, b) theo thuật toán trên

b. Chọn một bản rõ x, trong khoảng [1, n-1]

c. Tính : $y = x^b \bmod n$

d. Nhận được bản mã y

(ii). Giải mã :

Sử dụng khóa bí mật a để giải mã : $x = y^a \bmod n$

Ví dụ

Sau đây là một ví dụ với những số cụ thể. Ở đây chúng ta sử dụng những số nhỏ để tiện tính toán còn trong thực tế phải dùng các số có giá trị đủ lớn.

Lấy:

p=61: Số nguyên tố thứ nhất (giữ bí mật sau hoặc huỷ sau khi tạo khoá)

q=53: Số nguyên tố thứ hai (giữ bí mật sau hoặc huỷ sau khi tạo khoá)

n=pq=3233: Môđun (công bố công khai)

b=17: Số mũ công khai

a=2753: Số mũ bí mật

Khóa công khai là cặp (b, *n*). Khóa bí mật là a. Hàm mã hóa là:

$$y = x^b \bmod n = y^{17} \bmod 3233$$

với *x* là văn bản rõ. Hàm giải mã là:

$$x = y^a \bmod n = y^{2753} \bmod 3233$$

với y là văn bản mã.

Để mã hóa văn bản có giá trị 123, ta thực hiện phép tính:

$$y = 123^{17} \bmod 3233 = 855$$

Để giải mã văn bản có giá trị 855, ta thực hiện phép tính:

$$x = 855^{2753} \bmod 3233 = 123$$

Cả hai phép tính trên đều có thể được thực hiện hiệu quả nhờ giải thuật bình phương và nhân.

Hệ mã khóa công khai RSA đươc gọi là an toàn nếu ta chọn số nguyên tố p, q đủ lớn để việc phân tích phần khóa công khai n thành tích 2 thừa số nguyên tố là khó có thể thực hiện trong thời gian thực.

Tuy nhiên việc sinh một số nguyên tố được coi là lớn lại là việc rất khó, vấn đề này thường được giải quyết bằng cách sinh ra các số lớn (khoảng 100 chữ số) sau đó tìm cách kiểm tra tính nguyên tố của nó.

Một vấn đề đặt ra là phải kiểm tra bao nhiêu số nguyên tố ngẫu nhiên (với kích thước xác định) cho tới khi tìm được một số nguyên tố. Một kết quả nổi tiếng trong lý thuyết số (Định lý số nguyên tố) phát biểu rằng: "Số các số nguyên tố không lớn hơn N xấp xỉ bằngN/lnN". Vậy nếu P là một số nguyên tố ngẫu nhiên thì sắc xuất để P là số nguyên tố là 1/lnP. Nói chung vấn đề cố lõi của hệ mã RSA đó là việc chọn được số nguyên tố p, q đủ lớn để đảm bảo an toàn cho bản mã. Như đã biết nếu kẻ thám mã mà biết được số nguyên tố q, p thì dễ dàng tính được khóa bí mật (a) từ khóa công khai (b, n) do đó bản mã sẽ bị lộ.

4.Hệ mật mã Elgamma

Hệ mật mã khóa công khai ElGamal được đưa ra năm 1978. Hệ mật mã này được xây dựng dựa trên tính khó giải của Bài toán logarit rời rạc phần tử sinh α của tập Z*. Bài toán đặt ra: tìm một số nguyên x, $0 \le x \le$ p-2, sao cho $\alpha^x \equiv \beta \mod p$

Thuật toán: Sinh khóa cho mã hóa công khai Elgamal

1. Sinh ngẫu nhiên một số nguyên tố lớn p và α là phần tử sinh của Z^*_p
2. Chọn ngẫu nhiên một số nguyên a, $1 \le a \le p-2$, tính $\alpha^a \mod p$
3. Khóa công khai la (p, α, α^a). Khóa bí mật (a)

Thuật toán Mã hóa ElGamal

(i). Lập mã:

a. Lấy khóa công khai (p, α, α^a) theo thuật toán trên
b. Chọn một bản mã x, trong khoảng [0, p−1]
c. Chọn ngẫu nhiên một số nguyên k, $1 \le k \le p-2$
d. Tính $\gamma = \alpha^k \mod p$ và $\delta = x.(\alpha^a)k \mod p$
e. Nhận được bản mã là (γ, δ)

(ii). Giải mã:

a. Sử dụng khóa bí mật (a) và tính $\gamma^{p-1-a} \mod p$
b. Lấy bản rõ: $x = \gamma^{p-1-a} .\delta \mod p$

Thuật toán ElGamal lấy được bản rõ vì: $(\gamma^{-a}).\delta \equiv (\alpha^{-ak}).x.(\alpha^{ak}) \equiv x \pmod p$.

Ví dụ:

Sinh khóa: Đối tượng A chọn một số nguyên p = 2357 và một phần tử sinh $\alpha = 2$ của tập Z^*_{2357}. A chọn một khóa bí mật a = 1751

Và tính: $\alpha^a \bmod p = 2^{1751} \bmod 2357 = 1185$.

Khóa công khai của A (p=2357; α=2; α^a=1185).

Lập mã: Mã hóa bản rõ x = 2035, B chọn một số nguyên k = 1520 và tính:

$\gamma = 21520 \bmod 2357 = 1430$.

và

$\delta = 2035.11851520 \bmod 2357 = 697$.

B gửi $\gamma = 1430$ và $\delta = 697$ cho A.

Giải mã: Để giải mã A tính:

$\gamma^{p-1-a} = 1430605 \bmod 2357 = 872$.

và lấy lại được bản rõ khi tính

$x = 872.697 \bmod 2357 = 2035$.

CHƯƠNG II. CHỮ KÝ SỐ

2.1. Chữ ký số.

2.1.1. Giới thiệu về chữ ký số

Trong cuộc sống hàng ngày, ta cần dùng chữ ký để xác nhận các văn bản tài liệu nào đó và có thể dùng con dấu với giá trị pháp lý cao hơn đi kèm với chữ ký.

Cùng với sự phát triển nhanh chóng của công nghệ thông tin, các văn bản tài liệu dưới dạng số, dễ dàng được sao chép, sửa đổi. Nếu ta sử dụng hình thức chữ ký truyền thống như trên sẽ rất dễ dàng bị giả mạo chữ ký. Vậy làm sao để có thể ký vào văn bản, tài liệu số như vậy ?

Câu trả lời đó là sử dụng chữ ký điện tử. Chữ ký điện tử đi kèm với các thông tin chủ sở hữu và một số thông tin cần thiết khác sẽ trở thành chứng chỉ điện tử. Chữ ký điện tử hoạt động dựa trên hệ thống mã khoá công khai. Hệ thống mã khoá gồm hai khoá: khoá bí mật và khoá công khai. Mỗi chủ thể có một cặp khoá như vậy, chủ thể đó sẽ giữ khoá bí mật, còn khoá công khai sẽ được đưa ra công cộng để bất kỳ ai cũng có thể biết. Nguyên tắc của hệ thống mã khoá công khai đó là, nếu ta mã hoá bằng khoá bí mật thì chỉ khoá công khai mới giải mã được, và ngược lại thì nếu mã hoá bằng khoá công khai thì khoá bí mật mới giải mã được.

2.1.2. Định nghĩa chữ ký số

Chữ ký số (digital signature) là đoạn dữ liệu ngắn đính kèm với văn bản gốc để chứng thực tác giả (người ký văn bản) của văn bản và giúp người nhận kiểm tra tính toàn vẹn của nội dung văn bản gốc.

2.1.3. Các ưu điểm của chữ ký số

Việc sử dụng chữ ký số mang lại một số lợi điểm sau:

Khả năng nhận thực:

Các hệ thống mật mã hóa khóa công khai cho phép mật mã hóa văn bản với khóa bí mật mà chỉ có người chủ của khóa biết. Để sử dụng chữ ký số thì văn bản không cần phải được mã hóa mà chỉ cần mã hóa hàm băm của văn bản đó (thường có độ dài cố định và ngắn hơn văn bản). Khi cần kiểm tra, bên nhận giải mã (với khóa công khai) để lấy lại hàm băm và kiểm tra với hàm băm của văn bản nhận được. Nếu 2 giá trị này khớp nhau thì bên nhận có thể tin tưởng rằng văn bản xuất phát từ người sở hữu khóa bí mật. Tất nhiên là chúng ta không thể đảm bảo 100% là văn bản không bị giả mạo vì hệ thống vẫn có thể bị phá vỡ.

Vấn đề nhận thực đặc biệt quan trọng đối với các giao dịch tài chính. Chẳng hạn một chi nhánh ngân hàng gửi một gói tin về trung tâm dưới dạng *(a,b)*, trong đó *a* là số tài khoản và *b* là số tiền chuyển vào tài khoản đó. Một kẻ lừa đảo có thể gửi một số tiền nào đó để lấy nội dung gói tin và truyền lại gói tin thu được nhiều lần để thu lợi (tấn công truyền lại gói tin).

Tính toàn vẹn

Cả hai bên tham gia vào quá trình thông tin đều có thể tin tưởng là văn bản không bị sửa đổi trong khi truyền vì nếu văn bản bị thay đổi thì hàm băm cũng sẽ thay đổi và lập tức bị phát hiện. Quá trình mã hóa sẽ ẩn nội dung của gói tin đối với bên thứ 3 nhưng không ngăn cản được việc thay đổi nội dung của nó. Một ví dụ cho trường hợp này là tấn công đồng hình (homomorphism attack): tiếp tục ví dụ như ở trên, một kẻ lừa đảo gửi 1.000.000 đồng vào tài khoản của a, chặn gói tin *(a,b)* mà chi nhánh gửi về trung tâm rồi gửi gói tin (a,b^3) thay thế để lập tức trở thành triệu phú!

Tính không thể phủ nhận

Trong giao dịch, một bên có thể từ chối nhận một văn bản nào đó là do mình gửi. Để ngăn ngừa khả năng này, bên nhận có thể yêu cầu bên gửi phải gửi kèm chữ ký số với văn bản. Khi có tranh chấp, bên nhận sẽ dùng chữ ký này như một chứng cứ để bên thứ ba giải quyết. Tuy nhiên, khóa bí mật vẫn có thể bị lộ và tính không thể phủ nhận cũng không thể đạt được hoàn toàn.

2.1.4 Tình trạng hiện tại - luật pháp và thực tế

Tất cả các mô hình chữ ký số cần phải đạt được một số yêu cầu để có thể được chấp nhận trong thực tế:

- Chất lượng của thuật toán: một số thuật toán không đảm bảo an toàn;
- Chất lượng của phần mềm/phần cứng thực hiện thuật toán;
- Khóa bí mật phải được giữ an toàn;
- Quá trình phân phối khóa công cộng phải đảm bảo mối liên hệ giữa khóa và thực thể sở hữu khóa là chính xác. Việc này thường được thực hiện bởi hạ tầng khóa công cộng (PKI) và mối liên hệ khóa $\leftrightarrow$ người sở hữu được chứng thực bởi những người điều hành PKI. Đối với hệ thống PKI *mở*, nơi mà tất cả mọi người đều có thể yêu cầu sự chứng thực trên thì khả năng sai sót là rất thấp. Tuy nhiên các PKI thương mại cũng đã gặp phải nhiều vấn đề có thể dẫn đến những văn bản bị ký sai.

- Những người sử dụng (và phần mềm) phải thực hiện các quá trình đúng thủ tục (giao thức).

Chỉ khi tất cả các điều kiện trên được thỏa mãn thì chữ ký số mới là bằng chứng xác định người chủ (hoặc người có thẩm quyền) của văn bản.

Một số cơ quan lập pháp, dưới sự tác động của các doanh nghiệp hy vọng thu lợi từ PKI hoặc với mong muốn là người đi tiên phong trong lĩnh vực mới, đã ban hành các điều luật cho phép, xác nhận hay khuyến khích việc sử dụng chữ ký số. Nơi đầu tiên thực hiện việc này là bang Utah (Hoa kỳ). Tiếp theo sau là các bang Massachusetts và California. Các nước khác cũng thông qua những đạo luật và quy định và cả Liên hợp quốc cũng có những dự án đưa ra những bộ luật mẫu trong vấn đề này. Tuy nhiên, các quy định này lại thay đổi theo từng nước tùy theo điều kiện về trình độ khoa học (mật mã học). Chính sự khác nhau này làm bối rối những người sử dụng tiềm năng, gây khó khăn cho việc kết nối giữa các quốc gia và do đó làm

chậm lại tiến trình phổ biến chữ ký số.

2.1.5.Quy trình tạo ra và kiểm tra chữ ký điện tử:

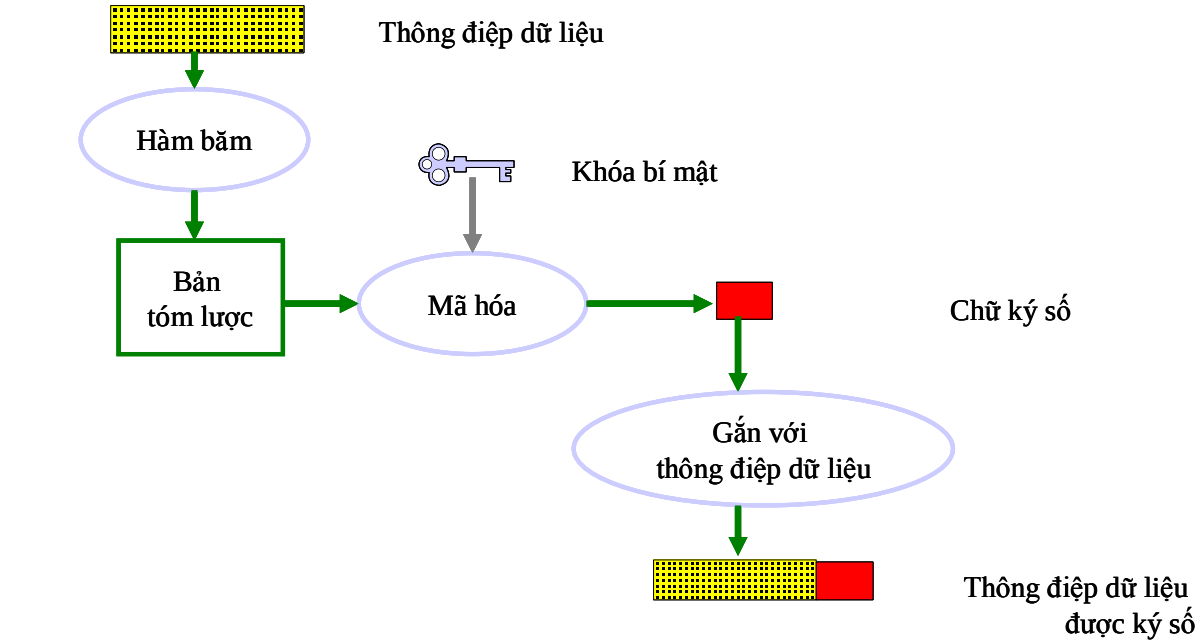
Quy trình tạo

- Dùng giải thuật băm để thay đổi thông điệp cần truyền đi,kết quả ta được một message diget,dùng giải thuật md5 ta được digest có chiều dài 128 bit,dùng giải thuật sha ta có chiều dài 160bit.
- Sử dụng khóa private key của người để mã hóa message digest thu được ở bước 1,thông thường ở bướb này ta dùng giải thuật RSA,kết quả thu được

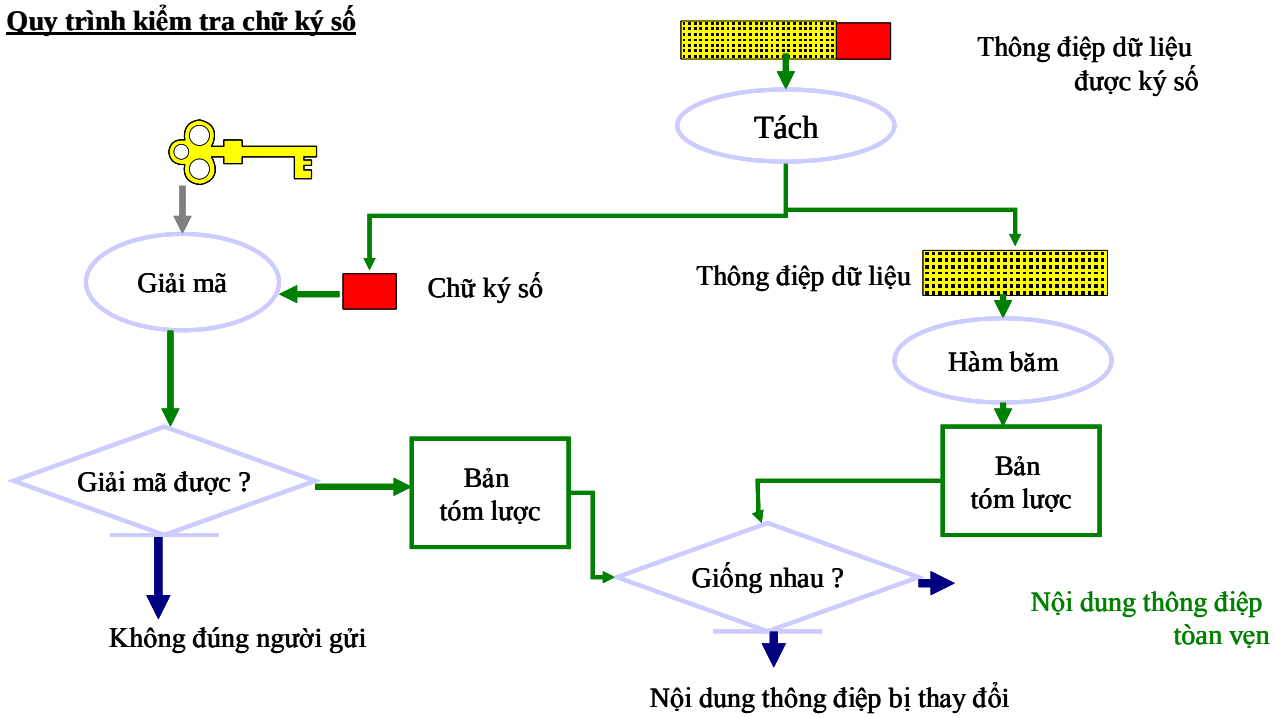
Các bước kiểm tra

- Dùng public key của người gửi (khóa này được thông báo đến mọi người) để giải mã chữ ký số của message.
- Dùng giải thuật md5 hoặc sha băm message đính kèm.
- So sánh kết quả thu được ở các bước trên.Nếu trgùng nhau,ta kết luận message này không bị thay đổi trong quá trình truyền và message này là của người gửi

Quy trình tạo chữ ký số



Quy trình kiểm tra chữ ký số



2.2. Sơ đồ chữ ký

2.2.1 Định nghĩa sơ đồ chữ ký

Một sơ đồ chữ ký số là bộ 5 (P, A, K, S, V) thoả mãn các điều kiện sau :

- P: là tập hữu hạn các bức điện có thể.
- A: là tập hữu hạn các chữ ký có thể.
- K: không gian khoá, là tập hữu hạn các khoá có thể.
- Với mỗi $K \in$ K tồn tại một thuật toán ký $Sig_k \in$ S và một thuật toán xác minh $Ver_k \in$ V.

Mỗi Sig_k: P->A và Ver_k: P $_x$A -> {TRUE, FALSE} là những hàm sao cho mỗi bức điện x thuộc P và mỗi bức điện y $\in$ A thoả mãn phương trình sau đây :

$$Ver(x,y) = \begin{cases} \text{TRUE nếu } y = Sig(x) \\ \text{FALSE nếu } y \# Sig(x) \end{cases}$$

Với mỗi $K \in$ K hàm Sig_K và Ver_K là các hàm thời gian đa thức. Ver_K sẽ là hàm công khai còn Sig_K là hàm bí mật. Ta gọi Alice là người gửi còn Bob là người nhận. Không thể dễ dàng tính toán để giả mạo chữ ký của Bob trên bức điện x. Nghĩa là với x cho trước, chỉ có Bob mới có thể tính được chữ ký y để Ver(x,y) =True. Một sơ đồ chữ kí không thể an toàn vô điều kiện vì một người tò mò nào đó có thể kiểm tra tất cả các chữ số y có thể trên bức điện x nhờ dùng thuật toán Ver công khai cho đến khi anh ta có thể tìm thấy một chữ ký đúng. Vì thế, nếu có đủ thời gian anh ta luôn luôn có thể giả mạo chữ ký của Bob. Như vậy, giống như trường hợp hệ thống mã hoá công khai, mục đích của chúng ta là tìm các sơ đồ chữ ký số an toàn về mặt tính toán.

2.2.2 Chữ ký số RSA.

Lược đồ chữ ký RSA được định nghĩa như sau:

- ***Tạo khóa***:

  Sơ đồ chữ ký cho bởi bộ năm (P,A,K,S,V)

Cho n=p.q; với mỗi p,q là các số nguyên tố lớn khác nhau $\phi(n) = (p - 1)(q - 1)$.

Cho P = A = Z_n và định nghĩa:

K là tập các khóa, K=(K',K''); với K'=a; K''=(n,b)

a,b $\in Z_n^*$, thỏa mãn ab $\equiv$ 1mod ϕ(n).

Các giá trị n,b là công khai, các giá trị p,q,a là các giá trị bí mật.

- ***Tạo chữ ký:***

Với mỗi K=(n.p,q,a,b) xác định:

$Sig_{K'}(x)= x^a \bmod n$

- ***Kiểm tra chữ ký:***

$Ver_{K''}(x,y)$= true $\Leftrightarrow x \equiv y^b \bmod n$; x, y $\in Z_n$.

Giả sử A muốn gửi thông báo x, A sẽ tính chữ ký y bằng cách :

$y=sig_{K'}(x)= x^a \bmod n$ (a là tham số bí mật của A)

A gửi cặp (x,y) cho B. Nhận được thông báo x, chữ ký số y, B bắt đầu tiến hành kiểm tra đẳng thức

$x= y^b \bmod(n)$ (b là khóa công khai A)

Nếu đúng, B công nhận y là chữ ký trên x của A. Ngược lại, B sẽ coi x không phải của A gửi cho mình (chữ ký không tin cậy).

Người ta có thể giả mạo chữ ký của A như sau: chọn y sau đó tính

$x= ver_{K''}(y)$, khi đó $y= sig_{K'}(x)$. Một cách khắc phục khó khăn này là việc yêu cầu x phải có nghĩa. Do đó chữ ký giả mạo thành công với xác suất rất nhỏ. Ta có thể kết hợp chữ ký với mã hóa làm cho độ an toàn tăng thêm.

Giả sử trên mạng truyền tin công cộng, ta có hai hệ mật mã khóa công khai δ_1 và hệ xác nhận chữ ký δ_2. Giả sử B có bộ khóa mật mã K=(K',K'') với K'=(n,e) và K''=d trong hệ δ_1, và A có bộ khóa chữ ký $K_s=(K_s',K_s'')$ với K_s'= a và K_s''=(n,b) trong hệ δ_2. A có thể gửi đến B một thông báo vừa bảo mật vừa có chữ ký xác nhận như sau: A tính chữ ký của mình là: $y= sig_A(x)$, và sau đó mã hóa cả x và y bằng cách sử dụng mật mã công khai e_B của B, khi đó A nhận được $z= e_B(x,y)$, bản mã z sẽ được gửi tới B. khi nhận được z việc trước tiên B phải

giải mã bằng hàm d_B để nhận được (x,y). Sau đó B sử dụng hàm kiểm tra công khai của A để kiểm tra xem $ver_A(x,y)$= true? Tức là kiểm tra xem chữ ký đó có đúng là của A?.

Ví dụ:

A dùng lược đồ chữ ký số RSA với n=247,(p=13,q=19);

$\phi(n) = 12.18 = 216$. Khóa công khai của A là b=7.

$\Rightarrow a = 7^{-1} \bmod 216 = 31$.

A công khai (n,b) = (247,7)

A ký trên thông báo x=100 với chữ ký:

$$y = x^a \bmod n = 100^{31} \bmod 247 = 74.$$

A gửi cặp (x,y) = (100,74) cho B, B kiểm tra bằng cách sử dụng khóa công khai của A như sau:

$x = y^b \bmod n = 74^7 \bmod 247 = 100 = x$.

B chấp nhận y=74 là chữ ký tin cậy.

2.2.3 Chữ ký Elgamal.

Lược đồ chữ ký ElGamal được giới thiệu năm 1985 và được Viện tiêu chuẩn và Công nghệ quốc gia Mỹ sửa đổi thành chuẩn chữ ký số. Lược đồ chữ ký ElGammal không tất định cũng giống như hệ mã hóa ElGamal. Điều này có nghĩa là có nhiều chữ ký hợp lệ cho một thông báo bất kỳ. Thuật toán kiểm tra phải có khả năng khả năng chấp nhận bất kỳ chữ ký hợp lệ nào khi xác minh.

Lược đồ chữ ký ElGamal được định nghĩa như sau:

- ***Tạo khóa:***

  Cho p là số nguyên tố sao cho bài toán logarit rời rạc trong Z_p là khó và giả sử $\alpha \in \mathbf{Z}_p^*$ là phần tử nguyên thủy

  Cho $P = Z_p^*$, $A = Z_p^* \times Z_{p-1}$ và định nghĩa

  - $K = \{(p, a, \alpha, \beta): \beta = \alpha^a \bmod p\}$.

  Các giá trị p, α, β là công khai, a là bí mật.

- ***Tạo chữ ký***

  Với K = (p, a, α, β) và với số ngẫu nhiên $k \in Z_{p-1}^*$,

định nghĩa $sig_k(\gamma, \delta)$, trong đó:

- $= \alpha^k \text{ mod} p$ và $\delta = (x - a\gamma)\, k^{-1} \text{mod}(p - 1)$.

- ***Kiểm tra chữ ký số***

Với $x, \gamma \in Z_p^*$ và $\delta \in Z_{p-1}$, ta định nghĩa :

$$\text{Ver}(x, \gamma, \delta) = \text{True} \Leftrightarrow \beta^{\gamma}. \gamma^{\delta} \equiv \alpha^x \text{ mod} p.$$

Chứng minh:

Nếu chữ ký được thiết lập đúng thì hàm kiểm tra sẽ thành công vì:

$$\Rightarrow \beta^{\gamma} \gamma^{\delta} \equiv \alpha^{a.\gamma} \alpha^{r.\delta} \text{ mod} p$$

$$\equiv \alpha^x \text{ mod} p \text{ (vì } a\gamma + r\delta \equiv x \text{ mod}(p - 1)).$$

A tính chữ ký bằng cách dùng cả giá trị bí mật a(là một phần của khóa) lẫn số ngẫu nhiên bí mật k (dùng để ký trên x). Việc kiểm tra có thể thực hiện duy nhất bằng thông tin công khai.

Ví dụ: Giả sử p=467, $\alpha = 2$, a = 127

Khi đó: $\beta = \alpha^a \text{ mod} p = 2^{127} \text{mod} 467 = 132$

Giả sử A có thông báo x=100 và A chọn ngẫu nhiên k=213 vì (213,466)=1 và 213^{-1} mod466 = 431, A ký trên x như sau:

$\gamma = \alpha^k \text{ mod} p = 2^{213} \text{mod} 467 = 29$

Và $\delta = (x - a\gamma)k^{-1} \text{ mod}(p - 1) = (100 - 127.\ 29).431 \text{ mod} 466 = 51.$

Chữ ký của A trên x= 100 là (29,51).

Bất kỳ người nào đó cũng có thể kiểm tra chữ ký bằng cách:

$132^{29} . 29^{51} \equiv 189 \text{ mod } 467$

$2^{100} \equiv 189 \text{ mod } 467$

Do đó, chữ ký là tin cậy.

2.2.4 Chữ ký không chối bỏ.

Chữ ký không chối bỏ được công bố bởi Chaum và Van Antverpen vào năm 1989. Nó có một nét riêng mới lạ và thú vị. Quan trọng nhất trong số đó là chữ ký không thể kiểm tra khi không có sự cộng tác của người ký, A(giả sử người ký là A).

Sự bảo vệ này của A đề phòng khả năng chữ ký trong tài liệu của anh ta bị sao chép và phân bố bởi thiết bị điện tử mà không có sự đồng ý của anh ta.

Ví dụ: A có một phần mềm và chữ ký kèm theo được tạo ra nhờ thuật toán của chữ ký số thông thường. Như vậy, sẽ không tránh khỏi trường hợp phần mềm đó bị sao chép mà B không biết. Người mua sẽ kiểm tra chữ ký kèm theo nhờ thuật toán kiểm tra công khai Ver và công nhận chữ ký đó là đúng. Vì như chúng ta đã biết bản sao của chữ ký số đồng nhất với bản gốc. Đương nhiên như vậy A sẽ bị mất bản quyền. Để tránh điều bất tiện đó A đã dùng chữ ký không chối bỏ. Sự kiểm tra sẽ thành công khi thực hiện giao thức hỏi - đáp.

Lược đồ chữ ký chống chối bỏ gồm 3 phần: thuật toán ký, giao thức kiểm tra, giao thức chối bỏ.

Thuật toán ký:

* Tạo khóa:

Cho p,q là các số nguyên tố lẻ sao cho p=2q+1 và bài toán rời rạc trên Z_p là khó. Lấy $\alpha \in Z_p^*$ là một phần tử bậc q(Nếu α_0 là phần tử nguyên thủy của Z_p thì $\alpha = \alpha_0^{(p-1)/q}$ modp) lấy $1 \le a \le q-1$ và xác định: $\beta = \alpha^a$ modp.

Lấy G là phân nhóm nhân của Z^*_p bậc q (G bao gồm các thặng dư bậc hai theo modun p).

Lấy P=A=G, xác định:

$K = \{ (p, \alpha, a, \beta): \beta = \alpha^a \text{ modp}\}$

Các giá trị p, α, β là công khai, a là bí mật.

* Tạo chữ ký:

Với K= (p, α, a, β) và $x \in G$, xác định chữ ký y trên thông báo x:

$y = sig_k(x) = x^a$ modp

Giao thức kiểm tra :

Với $x, y \in G$, sự kiểm tra được tiến hành theo giao thức sau :

1. A chọn e_1,e_2 ngẫu nhiên, $e_1, e_2 \in Z_p^*$.
2. A tính $c = y^{e_1} \beta^{e_2}$ modp gửi nó cho B.
3. B tính $d= c^{a^{-1} \bmod q}$ modp và gửi nó cho A.
4. A chấp nhận chữ đúng khi và chỉ khi :

$d \equiv x^{e_1} \alpha^{e_2}$ modp. (*)

* Vai trò của p, q trong lược đồ:

Lược đồ nằm trong Z_p; tuy nhiên chúng ta cần tính toán trong phân nhóm nhân G của Z_p^* của bậc nguyên tố lẻ. Đặc biệt, chúng ta cần tính phần tử nghịch đảo theo modun |G|, điều này lý giải tại sao |G| nên là nguyên tố lẻ. Nó thuận tiện lấy p=2q+1 với q là số nguyên tố lẻ. Trong trường hợp này, phân nhóm G tồn tại.

Ví dụ: giả sử ta lấy p = 467, từ 2 là căn nguyên thủy => $2^2 = 4$ là thặng dư bậc hai theo modun 267 và 4 là phần tử sinh của G, lấy $\alpha = 4$. Giả sử a=101, ta có:

$\beta = \alpha^a \text{mod} p = 4^{101} \text{ mod} 467 = 449$

A sẽ ký thông báo x=119 với chữ ký:

$y = x^a \text{ mod} p = 119^{101} \text{ mod} 467 = 129$

Giả sử B muốn kiểm tra chữ ký y, B chọn ngẫu nhiên $e_1 = 38, e_2 = 397$.

Ta có: $c = y^{e_1} \beta^{e_2} \text{ mod} p = 129^{38} 449^{397} \text{ mod} 467 = 13$

B gửi c=13 cho A và A tính d theo:

$d = c^{a^{-1} \bmod q} \text{ mod} p$

$\Rightarrow d = 13^{101^{-1} \bmod 233} \text{ mod} 467$ $(q = (p - 1)/2 = (467 - 1)/2 = 233)$

$\Rightarrow d = 9$

B muốn kiểm tra chữ ký y theo bước 4. Có:

$x^{e_1} \alpha^{e_2} \text{ mod} p = 119^{38} 4^{397} \text{ mod} 467 = 9$

$\Rightarrow d \equiv x^{e_1} \alpha^{e_2} \text{ mod} p$

=> B chấp nhận chữ ký là đúng

Giao thức chối bỏ

Một vấn đề đặt ra, nếu sự cộng tác của chủ thể ký là cần thiết trong việc kiểm tra chữ ký thì điều gì đã ngăn cản anh ta trong việc từ chối chữ ký do anh ta tạo ra. Tất nhiên, anh ta có thể cho rằng chữ ký đúng đó là giả mạo và từ chối kiểm tra nó hoặc anh ta thực hiện một giao thức mà theo đó chữ ký sẽ không được kiểm tra. Vì vậy, một lược đồ chữ ký chống chối bỏ được kết hợp chặt chẽ với một giao thức chối bỏ và nhờ điều đó chủ thể ký có thể chứng minh được chữ ký đó là giả mạo. (Nếu anh ta từ chối thực hiện 1 phần trong

giao thức chối bỏ, điều đó đồng nghĩa với dấu hiệu chứng minh chữ ký đó là của anh ta và anh ta đang cố gắng từ chối chữ ký của mình).

Giao thức chối bỏ gồm hai tiến trình của giao thức kiểm tra và có các bước sau:

1. B chọn e_1, e_2 ngẫu nhiên, $e_1, e_2 \in Z_q^*$.
2. B tính $c = y^{e_1} \beta^{e_2}$ modp và gửi nó cho A
3. A tính $d = c^{a^{-1} \bmod q}$ modp và gửi nó cho B
4. B kiểm tra $d \neq x^{e_1} \alpha^{e_2}$ modp.
5. B chọn f_1,f_2 ngẫu nhiên, $f_1, f_2 \in Z_q^*$.
6. B tính $C = y^{f_1} \beta^{f_2}$ modp và gửi nó cho A
7. A tính $D = c^{a^{-1} \bmod q}$ modp và gửi nó cho B
8. B kiểm tra $D \neq x^{f_1} \alpha^{f_2}$ modp
9. B kết luận rằng y là chữ ký giả mạo khi và chỉ khi

$$(d\alpha^{-e_2})^{f_1} \equiv (D\alpha^{-f_2})^{e_1} \text{ modp}$$

Ví dụ: Lấy p=467, α = 4, a = 101, β = 449. Ký trên thông báo x=286 với chữ ký y= 83 (là giả mạo). A muốn thuyết phục B rằng chữ ký đó là không đúng. Vậy phải thực hiện như sau:

Chọn ngẫu nhiên e_1 = 45, e_2 = 237. B tính c=305 và A trả lời với d= 109. B tính $286^{45}. 4^{237} \bmod 467 = 149$.

Vì 149 ≠ 109 nên ta phải thực hiện giao thức chối bỏ

B chọn tiếp f_1 = 125, f_2 = 9, ngẫu nhiên, B tính C=270 và A trả lời với D=68. B tính: $286^{125}.4^{9} \bmod 467 = 25$.

Vì 25 ≠ 68 nên B thực hiện tiếp bước cuối cùng của giao thức là thực hiện kiểm tra tính chính xác.

Ta có: $109.4^{-237})^{125} \equiv 188 \bmod 467$

và $(68.4^{-9})^{45} \equiv 188 \bmod 467$; $\Rightarrow (d\alpha^{-e_2})^{f_1} \equiv (D\alpha^{-f_2})^{e_1}$ modp

⇨ Vậy B tin chắc rằng đó là chữ ký không đúng

Bây giờ vấn đề đặt ra là:

- A có thuyết phục được B rằng chữ ký không đúng đó là giả mạo

- A không thể làm cho B bị thuyết phục rằng chữ kí đó đúng là giả mạo ngoại trừ xác suất rất nhỏ.

CHƯƠNG 3: DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ

3.1 Tổ chức chứng thực là gì ?.

Tổ chức chứng thực điện tử(CA) là một bên thứ 3 được cả hai bên gửi và nhận tin cậy đứng ra chứng nhận public key là đảm bảo.

Chức năng của của tổ chức chứng thực điện tử là chứng thực nhận dạng người ký thông qua hình thức cấp chứng chỉ số chứa khóa công khai của người ký, và duy trì cơ sở dữ liệu về chứng chỉ số.

Khi chứng chỉ số được CA cung cấp thì nó được tin tưởng trong khi sử dụng

Hiện nay trên thế giới có nhiều tổ chức chứng thực điện tử tin cậy như VeriSign, Entrust, CyberTrust...

Còn ở Việt Nam có một vài tổ chức chứng thực điện tử như VASC, DES...

3.2 Giới thiệu về một số tổ chức chứng thực.

Tổ chức Entrust -một trong những hãng đi đầu về phát triển PKI

Entrust là một tổ chức chứng thực điện tử tin cậy trên thế giới được các công ty thuộc lĩnh vực thương mại điện tử trên thế giới tin cậy.

Misof cũng là nhà phân phối sản phẩm về hệ thống cấp phát chứng chỉ của Entrust tại Việt Nam.

Giải pháp của Entrust không những đáp ứng đầy đủ các yêu cầu về hệ thống CA mà còn cung cấp thêm nhiều ứng dụng của chứng chỉ số, tích hợp chúng trong các ứng dụng khác như email, mã hóa file thư mục....

Các sản phẩm của Entrust cho việc nhận dạng và quản lý truy cập tuân theo chuẩn X509 V3, ngoài ra còn tuân theo các chuẩn quốc tế về mã hóa như PKCS, RFC.

Tổ chức chứng thực điện tử tại Việt Nam_VASC

Công ty VASC đã được xây dựng thành công hệ thống quản lý và cung cấp chứng chỉ số của mình từ tháng 4/2002 và từ tháng 8/2002 đã chính thức phục vụ khách hàng.

Chứng chỉ số VASC CA được dùng trong các giao dịch trên môi trường mạng hoặc Internet để :

- Chứng thực các đối tượng sử dụng.
- Đảm bảo an toàn và bảo mật thông tin
- Cung cấp bằng chứng pháp lý nếu xảy ra tranh chấp

VASC-CA hiện nay cung cấp với cac giải pháp :

- Chứng chỉ số cá nhân VASC-CA : Giúp mã hóa thông tin, bảo mật e-mail, sử dụng chữ ký điện tử cá nhân, chứng thực với một web server thông qua giao thức bảo mật SSL.
- Chứng chỉ số SSL Server VASC-CA: Giúp bảo mật hoạt động trao đổi thông tin trên website, xác thực người dùng bằng SSL, xác minh tính chính thống, chống giả mạo, cho phép thanh toán bằng thẻ tín dụng, ngăn chặn hacker dò mật khẩu.
- Chứng chỉ số nhà phát triển phần mềm VASC-CA: Cho phép nhà phát triển phần mềm ký vào các chương trình applet, script, Java software, ActiveX control, EXE, CAB và DLL, đảm bảo tính hợp pháp của sản phẩm, cho phép người sử dụng nhận diện được nhà cung cấp, phát hiện được sự thay đổi của chương trình (do hỏng, bị hacker hay virus phá hoại).

Tương tự như vậy, số lượng đơn vị cung cấp giải pháp ứng dụng có dùng CKS ở Việt Nam hiện nay cũng chưa nhiều. Các công ty như Giải Pháp Thẻ Minh Thông (www.tomica.vn), MI-SOFT(www.misoft.com.vn)... là những công ty cung cấp tích hợp giải pháp chữ ký số HSM (Hardware Security Module) vào thẻ thông minh và USB Token vào các ứng dụng và giao dịch cần bảo mật như: Internet Banking, Money Tranfer, VPN hay e-Signing.

3.3 Dịch vụ chứng thực chữ ký số.

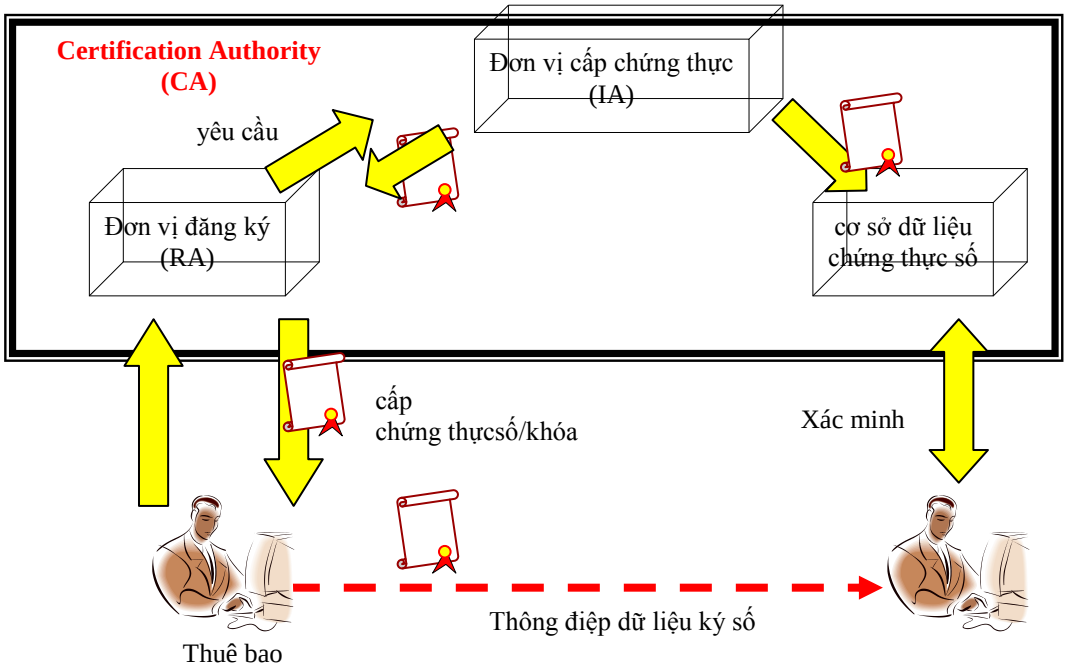
Cung cấp bởi Tổ chức cung cấp dịch vụ chứng thực Chữ ký số (Certification Authority - CA) - Người thứ ba đáng tin cậy bao gồm:

- kiểm tra, xác minh một chủ thể
- cấp cặp khóa
- cấp chứng thư số (chứng minh thư ++)
- bao gồm cả khóa công khai
- duy trì trực tuyến CSDL Chứng thư số
- khác

Bản chất dịch vụ

- Tương tự như cấp chứng minh thư nhân dân hay các giấy tờ tùy thân khác
- Áp dụng cho môi trường mạng

Cung cấp và sử dụng dịch vụ



3.4 Tình hình phát triển dịch vụ chứng thực chữ ký số trên thế giới và ở VIệt Nam.

3.4.1 Tình hình triển khai trên thế giới

Đây là dịch vụ mới, xuất hiện vào khoảng cuối 1990s. Hiện đã được triển khai ở Mỹ, EU, Nhật, Hàn Quốc, Trung Quốc

VD:Hàn Quốc: 9 triệu thuê bao (20% dân số)

Được ứng dụng trong các lĩnh vực:

- Internet banking (chuyển tiền qua mạng)
- hành chính công (khai sinh, khai tử, nộp thuế, cấp các loại giấy tờ và chứng chỉ, ...)
- mua bán, đấu thầu qua mạng
- Y tế, giáo dục, ...

Đây là một vài ví dụ về việc triển khai dịch vụ chứng thực chữ ký số trên thế giới :

"Hệ thống nộp hồ sơ xin phép xây dựng " – Singapore

Việc xây dựng các công trình phải có ý kiến của rất nhiều cơ quan có thẩm quyền (>10). Phê duyệt nhiều loại hồ sơ (đề án, dự án, …).Việc nộp hồ sơ mất rất nhiều thời gian, công sức (nhiều cửa). Chính vì vậy nên họ đã đưa ra một giải pháp kỹ thuật là:

- Hệ thống CORENET e-Submission, tích hợp nhiều ứng dụng phê duyệt

- Hồ sơ nộp có chữ ký số
    - Phê chuẩn dùng chữ ký số

Sử dụng bắt buộc từ năm 2002 và đã mang lại hiệu quả đáng kể :

- Tiện lợi, tiết kiệm thời gian, công sức
- Cải cách hành chính
    - "One stop"
    - Có thể kiểm tra trạng thái phê chuẩn online

"Phê chuẩn của cha mẹ " - Hàn Quốc

- Vấn đề:
    - Tranh cãi giữa cha mẹ và doanh nghiệp nội dung về việc chơi online game và tải nội dung thông tin di động của trẻ em
- Sở cứ pháp lý:
    - Đạo luật khai thác và bảo vệ thông tin

    các doanh nghiệp chỉ được cung cấp dịch vụ cho trẻ em khi có sự phê chuẩn của bố mẹ
- MIC:
    - Các doanh nghiệp không tuân thủ sẽ bị phạt
    - 4/2006: 13 cổng thông tin và online game website đã bị phạt 68,000 USD
- Giải pháp kỹ thuật
    - Thông báo có chữ ký số của cha mẹ
- Hiệu quả
    - Giảm đáng kể đơn từ và tranh cãi
    - Bảo vệ trẻ em khỏi việc sử dụng các nội dung và game không phù hợp

"Mạng chăm sóc sức khỏe và thuốc" – Nhật Bản

- Vấn đề
    - chữa bệnh lâu dài, chữa bệnh từ xa

      $\Rightarrow$ Cần cơ sở dữ liệu về quá trình điều trị, lịch sử bệnh tật, tình trạng sức khỏe ....,
    - Thông tin nhạy cảm, mang tính riêng tư

- Chỉ truy nhập được bởi những người có trách nhiệm và thẩm quyền, cần xác thực đúng người (bác sĩ ?)

- Đối tượng phục vụ
  - bệnh viện, trung tâm sức khỏe, bác sĩ, hộ lý, dược sĩ, bệnh nhân
  - dịch vụ: cấp hồ sơ, kê đơn thuốc, trả tiền chữa bệnh, trả tiền thuốc, ...
- Thời gian: 1995-2004
- Hiệu quả
  - Hơn 80,000 người
  - Giảm chi phí khám, chữa bệnh, điều trị
  - Nâng cao hiệu quả chữa bệnh và điều trị

3.4.2 Chữ ký số ở Việt Nam

Khái niệm "chứng thực số" và "chữ ký số" còn tương đối mới đối với người sử dụng tại VN. Để hiểu được vai trò của nó trong giao dịch điện tử, người dùng đòi hỏi phải có một kiến thức nhất định về CNTT (mã hóa bất đối xứng, public key, private key…). Vì vậy một phần khách hàng vẫn chưa hưởng ứng dịch vụ này vì "không tin" vào chứng thực số và chữ ký số. Hiện nay đã có một số đơn vị cung cấp dịch vụ phục vụ nhu cầu giao dịch nội bộ (ngân hàng công thương) và một số các đơn vị đã cung cấp thử nghiệm cho công cộng: VASC

Sau thời gian dài chuẩn bị soạn thảo, lấy ý kiến các chuyên gia và người dân, Nghị định 26 về chữ ký số và dịch vụ chứng thực chữ ký số đã được Thủ tướng Chính phủ ban hành ngày 15/2/2007, công nhận chữ ký số và chứng thực số có giá trị pháp lý trong giao dịch điện tử, bước đầu thúc đẩy sự phát triển của thương mại điện tử tại Việt Nam

Ngày 31/12/2008, Bộ TT-TT ban hành 6 loại tiêu chuẩn trong giao dịch điện tử được quy định buộc phải áp dụng chữ ký số và chứng thực số, bao gồm: Chuẩn bảo mật cho HSM, Chuẩn mã hóa, Chuẩn tạo yêu cầu và trao đổi chứng thư số, Chuẩn về chính sách và quy chế chứng thực chữ ký số, Chuẩn về lưu trữ và truy xuất chứng thư số và Chuẩn về kiểm tra trạng thái chứng thư số.

Theo Bộ TT-TT, danh mục các tiêu chuẩn này sẽ còn được định kỳ xem xét cập nhật, sửa đổi, bổ sung phù hợp với điều kiện thực tế của Việt Nam.

Các tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia, tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng, tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên

dùng được Bộ Thông tin và Truyền thông cấp giấy chứng nhận đủ điều kiện đảm bảo an toàn cho chữ ký số, tổ chức cung cấp dịch vụ chứng thực chữ ký số nước ngoài được Chính phủ Việt Nam công nhận sẽ dựa trên danh mục ban hành này để áp dụng chứng thực.

Ứng dụng "Chữ ký số" tại Việt Nam

Khả năng ứng dụng của CKS khá lớn, do có tác dụng tương tự như chữ ký tay, nhưng dùng cho môi trường điện tử. Thường CKS được sử dụng trong giao dịch cần an toàn qua mạng Internet, như giao dịch thương mại điện tử, tài chính, ngân hàng. Thứ 2 là dùng để ký lên eMail, văn bản tài liệu Soft-Copy, phần mềm... module phần mềm và việc chuyển chúng thông qua Internet hay mạng công cộng. Tuy nhiên, sử dụng hay không sử dụng CKS vẫn còn tùy vào sự lựa chọn của người dùng.

Hiện nay nhiều ngân hàng Việt Nam đã ứng dụng CKS trong các hệ thống như Internet Banking, Home Banking hay hệ thống bảo mật nội bộ. Ngoài ra các website của các ngân hàng, công ty cần bảo mật giao dịch trên đường truyền, mạng riêng ảo VPN đã áp dụng CKS. Có thể nói, càng ngày càng nhiều sự hiện diện của CKS trong các hệ thống, ứng dụng CNTT bảo mật của DN, tổ chức ở Việt Nam.

Chữ ký số đem lại lợi ích gì?

Ứng dụng CKS giúp giải quyết tốt hơn các giải pháp xác thực và bảo mật. CKS giải quyết vấn đề toàn vẹn dữ liệu và là bằng chứng chống chối bỏ trách nhiệm trên nội dung đã ký, giúp cho các tổ chức, cá nhân yên tâm với các giao dịch điện tử của mình trong môi trường Internet.

Đối với lĩnh vực trao đổi thông tin, với sự phổ biến hiện nay của e-mail nhờ tính nhanh chóng linh hoạt, việc sử dụng CKS sẽ giúp cho việc trao đổi văn bản nội dung trở nên dễ dàng và đảm bảo. Ví dụ: Hệ thống quản lý văn bản, hợp đồng số sẽ được lưu trữ, tìm kiếm bằng hệ thống máy tính. Các giao dịch, trao đổi văn bản giữa cá nhân - tổ chức nhà nước (C2G), DN - Nhà Nước(B-G), DN-DN(B2B) hay giữa các tổ chức cơ quan nhà nước với nhau sẽ nhanh chóng và đảm bảo tính pháp lý, tiết kiệm rất nhiều thời gian, chi phí giấy tờ và vận chuyển, đi lại.

Đặc biệt, tăng cường ứng dụng CKS sẽ thúc đẩy việc ứng dụng thương mại điện tử, chính phủ điện tử, hành chính điện tử và kinh doanh điện tử, đồng thời cũng bảo vệ bản quyền các tài sản số hóa.

Sở TTTT TP.HCM là đơn vị đi tiên phong trong việc triển khai ứng dụng chữ ký số trong hoạt động giao dịch điện tử phục vụ công tác quản lý nhà nước tại địa phương. Hiện sở cũng đã có trung tâm Chứng Thực Chuyên Dùng, được bộ TTTT và Ban Cơ Yếu chính phủ (đơn vị chứng thực điện tử chuyên dùng chính phủ (G-CA), cung cấp và quản lý chứng chỉ điện tử phục vụ các cơ quan trong hệ thống chính trị thực hiện các yêu cầu xác thực thông tin và bảo mật thông tin thuộc phạm vi bí mật nhà nước trên các hệ thống tác nghiệp, điều hành điện tử) đồng ý. Với trung tâm này sở TTTT đã và đang triển khai chứng thực CKS miễn phí cho khối quản lý đô thị như: Sở Tài Nguyên Môi Trường, sở Kiến Trúc, sở Tài Chính, trung tâm Tài Nguyên Môi Trường và Đăng Ký Nhà Đất…Trong năm 2009, sở TTTT TP.HCM sẽ tiếp tục nâng cấp trung tâm này và mở rộng chứng thực cho các sở, ngành khác. Đầu tháng 3/2009, sở TTTT đã có buổi làm việc với 2 cơ quan thuế và hải quan TP.HCM về việc chứng thực chữ ký số cho 2 đơn vị này để tiến tới thực hiện cơ chế "một cửa" và kê khai thuế qua mạng

Ngoài trung tâm Chứng Thực Chuyên Dùng, sở TTTT TP.HCM hiện đang chờ UBND TP.HCM phê duyệt cho phép thành lập trung tâm Chứng Thực Công Cộng. Với trung tâm này, sở TTTT sẽ chứng thực cho mọi đối tượng: DN, người dân, tổ chức...Trung tâm sẽ phục vụ theo loại hình dịch vụ".

3.5 Hành lang pháp lý.

Ngày 23/2, Chính phủ đã ban hành Nghị định 27/2007/NĐ-CP về giao dịch điện tử trong hoạt động tài chính.

Trước đó, ngày 15/2/2007, Chính phủ đã ban hành Nghị định 26/2007/NĐ-CP quy định chi tiết thi hành Luật Giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số. Theo đó, trong trường hợp pháp luật quy định văn bản cần có chữ ký thì yêu cầu đối với một thông điệp dữ liệu được xem là đáp ứng nếu thông điệp dữ liệu đó được ký bằng chữ ký số.

Sau khi nghị định của Thủ tướng được ban hành, Bộ TT-TT và các bộ, ngành liên quan cũng đã ra nhiều văn bản liên quan hướng dẫn thực hiện chữ ký số và dịch vụ chứng thực chữ ký số.

Ngày 31/12/2008, Bộ TT-TT ban hành 6 loại tiêu chuẩn trong giao dịch điện tử được quy định buộc phải áp dụng chữ ký số và chứng thực số, bao gồm: Chuẩn bảo mật cho HSM, Chuẩn mã hóa, Chuẩn tạo yêu cầu và trao đổi chứng thư số, Chuẩn về chính sách và

quy chế chứng thực chữ ký số, Chuẩn về lưu trữ và truy xuất chứng thư số và chuẩn về kiểm tra trạng thái chứng thư số.

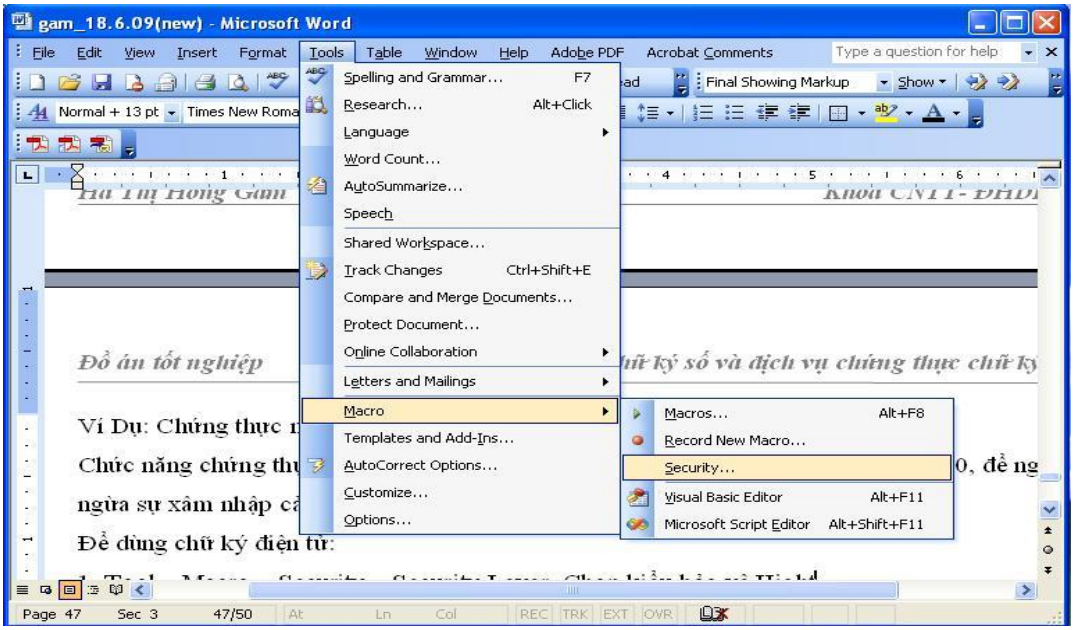
Theo Bộ TT-TT, danh mục các tiêu chuẩn này sẽ còn được định kỳ xem xét cập nhật, sửa đổi, bổ sung phù hợp với điều kiện thực tế của Việt Nam.Các tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia, tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng, tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng được Bộ Thông tin và Truyền thông cấp giấy chứng nhận đủ điều kiện đảm bảo an toàn cho chữ ký số, tổ chức cung cấp dịch vụ chứng thực chữ ký số nước ngoài được Chính phủ Việt Nam công nhận sẽ dựa trên danh mục ban hành này để áp dụng chứng thực.

Ví Dụ: Chứng thực macro trong Word và Excel bằng chữ ký điện tử

Chức năng chứng thực bằng chữ ký điện tử bắt đầu được bổ sung từ bộ Office 2000, để ngăn ngừa sự xâm nhập cảu virut macro.

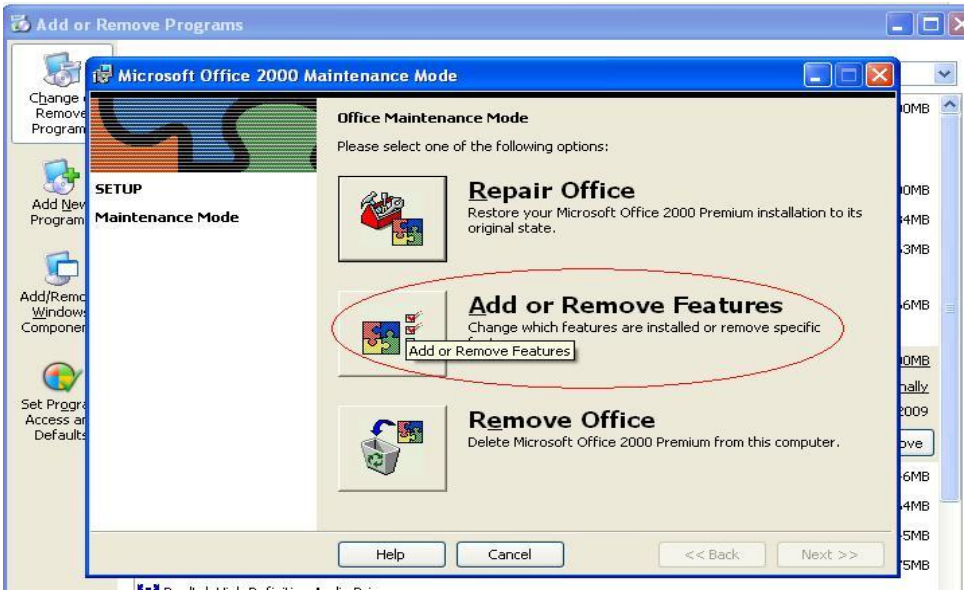
Để dùng chữ ký điện tử:

1.Tool – Macro – Security – Security Lever. Chọn kiểu bảo vệ Hight

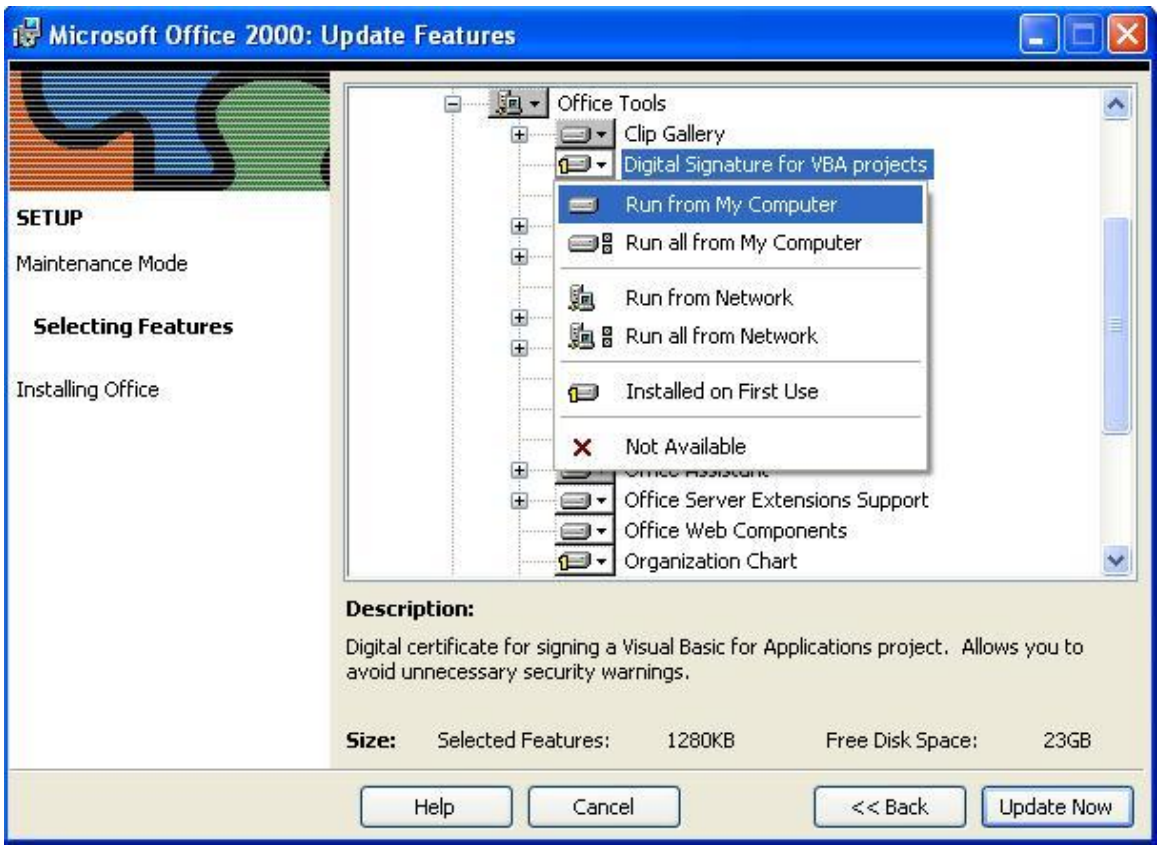


2. Nếu chưa có chương trình tạo chữ ký điện tử của VBA thì bạn cần cài đặt bổ sung :

Control Panel – Add/Remove Progams – Microsoft Office 2000 Premium – nhấn Add/Remove – Add or Remove Features

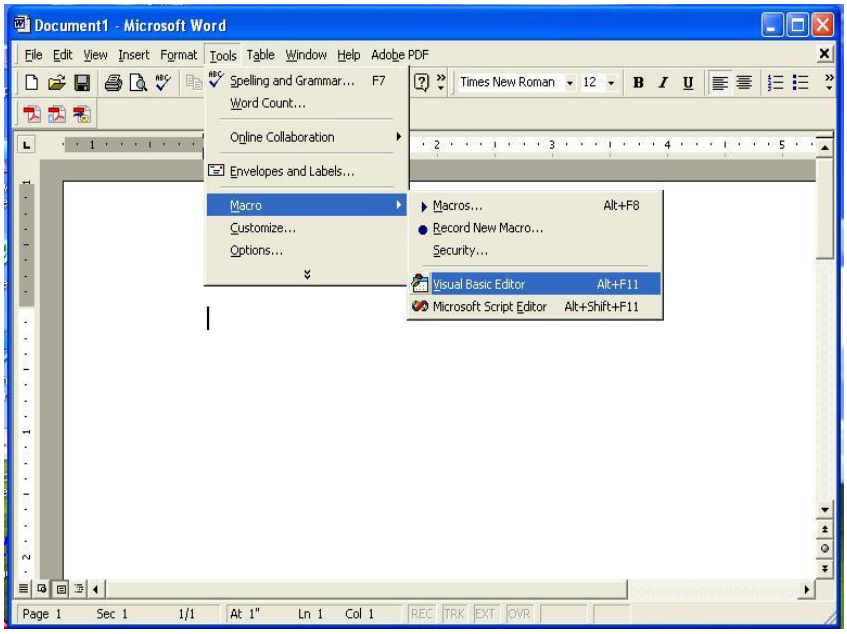


Bấm dấu cộng bên cạnh Office Tool, nhấn vào Digital Signature for VBA project và chọn Run from My Computer, xong bấm Update now. File Selfcert.exe đã được bổ xung vào tại đường dẫn C:ProgamFile/Microsoft Office/ Office

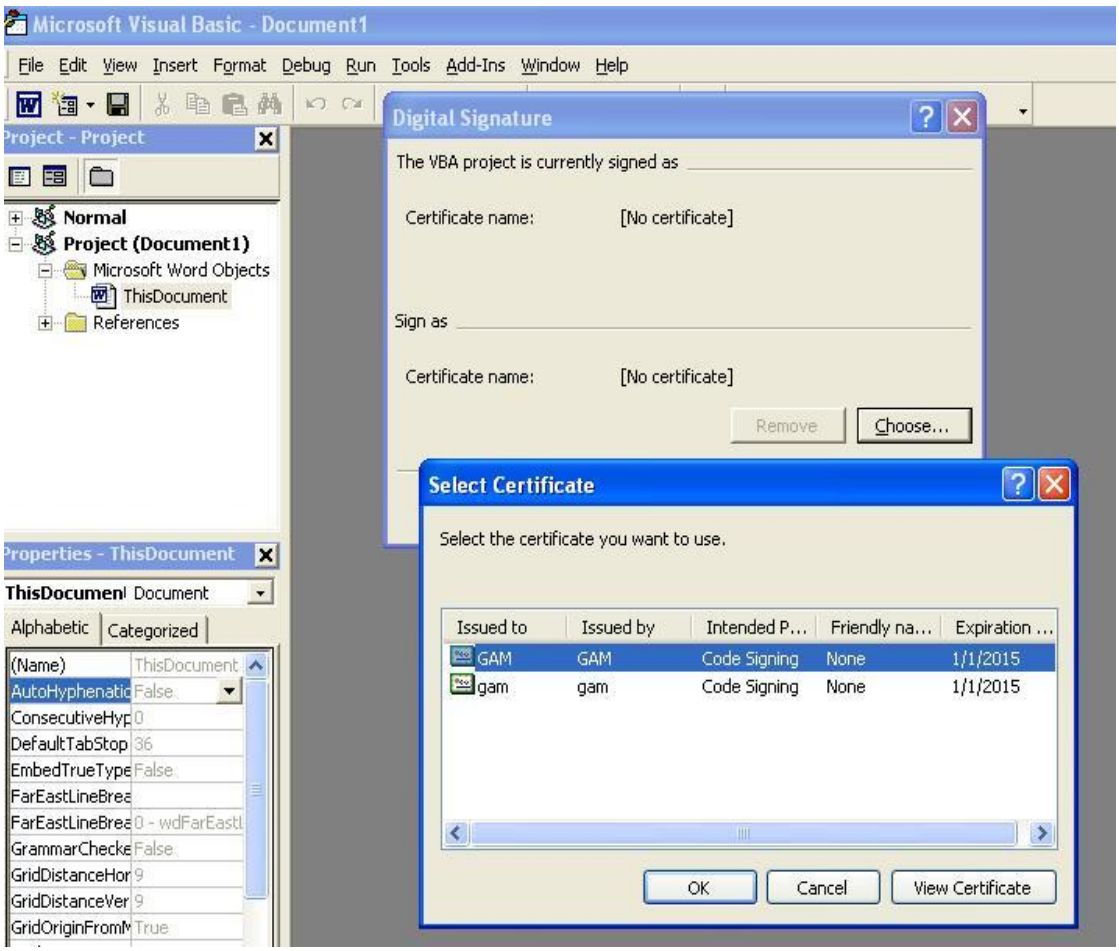


3.Để tạo chữ ký, chạy file Selfcert.exe, gõ tên vào hộp Your name – OK

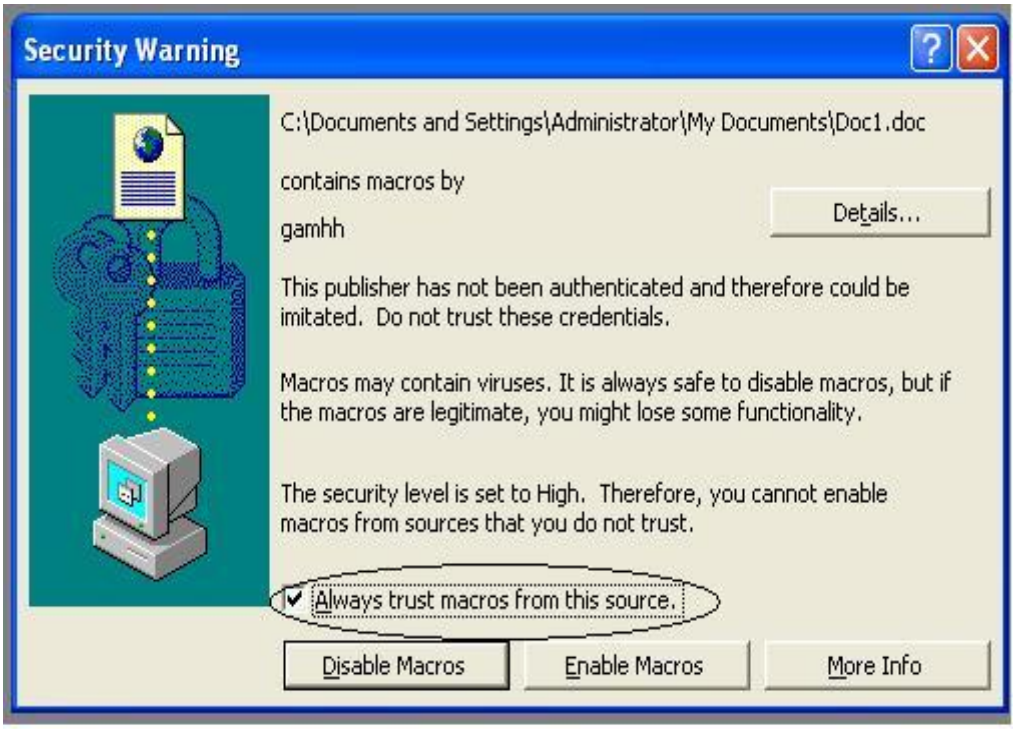
Sau đó chọn macro cần bảo vệ trong cửa sổ Visual Basic Editor,



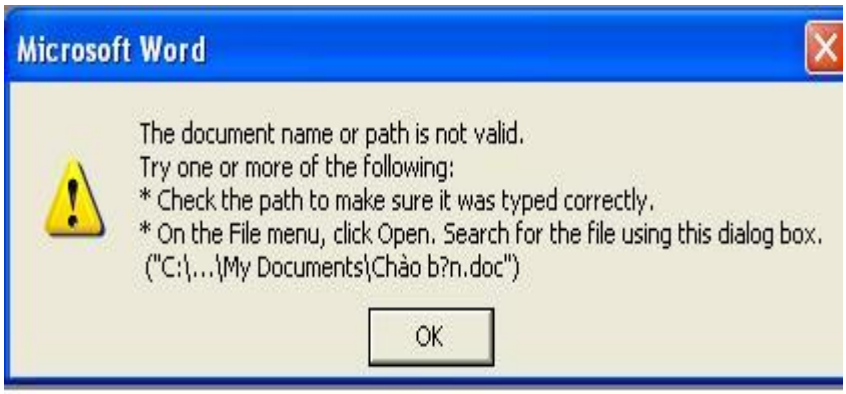
Tool – Digital Signature – nhấn Choose rồi chọn chữ ký điện tử vừa mới được tạo trong danh sách Select Certificate.



4.Lần đầu tiên mở tập tin có chứa macro, hộp thoại Security Warning xuất hiện, yêu cầu bạn xác định đúng là macro và chữ ký của mình không, nếu đúng bạn đánh dấu vào hộp kiểm Always trust macro from this source. Macro của bạn bây giờ đã được chứng thực bằng chữ ký điện tử nên chương trình sẽ không hỏi mỗi khi bạn chạy macro.



Nhưng khi chạy một macro do bạn tạo ra mà chưa được chứng thực hoặc có một virut macro khởi chạy thì chương trình lập tức cảnh báo, khi đó bạn nhấn OK để vô hiệu hóa nó.



KẾT LUẬN

Việc nghiên cứu và tìm hiểu về chữ ký số và dịch vụ chứng thực chữ ký số để đáp ứng nhu cầu xác thực thông tin và người dùng hiện này là rất cần thiết đặc biệt là trong các giao dịch điện tử. Đồ án đã đạt được những kết quả chính sau:

Nghiên cứu và tìm hiểu trong tài liệu để hệ thống lại các vấn đề:

- Các khái niệm về toán học được sử dụng trong mật mã học.
- Các kiến thức chữ ký số.
- Tìm hiểu về dịch vụ chứng thực chữ ký số.

Ví dụ : Chứng thực macro trong Word và Excel bằng chữ ký điện tử.

Mặc dù có nhiều cố gắng, nhưng trong đồ án vẫn có một số vấn đề chưa thật sự hoàn thiện,chưa thực hiện được mô phỏng chương trình cấp chứng chỉ số để ký.

Xin các thầy cô giáo góp ý đề em có thể tiếp tục nghiên cứu đề tài này được tốt hơn.

TÀI LIỆU THAM KHẢO

1. Lý thuyết mật mã và an toàn thông tin_ Phan Đình Diệu(NXB ĐHQG)
2. An toàn tính toán_Charles P.pheeger(Học Viện Kỹ Thuật Mật Mã)
3. Báo cáo: Vai trò của chữ ký điện tử trong TMĐT_Lê Thị Ngọc Mơ
4. http://vi.wikipedia.org/wiki/chữ_ký_số.
5. http://vi.wikipedia.org/wiki/Hàm_băm.
6. http://www.3c.com.vn/Story/vn/hotrokhachhang/thuongmaidientu/ekienthuccoban
7. http://www.ddth.com