LỜI CẢM ƠN

Lời đầu tiên em xin được bày tỏ lòng biết ơn chân thành tới thầy giáo TS. Lê Phê Đô - giảng viên trường ĐH Công Nghệ - ĐHQG Hà Nội, người thầy đã trực tiếp giảng dậy và tận tình giúp đỡ, chỉ bảo em trong suốt thời gian qua. Cảm ơn thầy đã luôn động viên, hướng dẫn, định hướng và truyền thụ cho em những kiến thức vô cùng quý báu để em có thể hoàn thành luận án tốt nghiệp này.

Em xin chân thành cảm ơn các thầy giáo, cô giáo trường ĐHDL Hải Phòng và đặc biệt là các thầy cô trong bộ môn tin học, những người đã không ngừng truyền đạt cho chúng em những kiến thức quý báu trong học tập tập cũng như trong cuộc sống xuốt bốn năm học vừa qua.

Và cuối cùng, hơn hết em muốn được bày tỏ lòng biết ơn sâu sắc tới gia đình, bố mẹ, anh chị em cũng như tất cả bạn bè em, những người luôn ở bên động viên, cổ vũ và giúp đỡ em trong học tập cũng như trong cuộc sống.

Dưới đây là những gì em đã tìm hiểu và nghiên cứu được trong thời gian qua. Do tính thực tế và kiến thức còn hạn chế, vì vậy em rất mong nhận được sự chỉ bảo cảu các thầy cô giáo và sự tham gia đóng góp ý kiến của các bạn để em có thể hoàn thành tốt đề tài của mình

Một lần nữa em xin chân thành cảm ơn !

Hải Phòng, ngày 30 tháng 06 năm 2009

Sinh viên

Trần Thị Thanh Tâm

MỤC LỤC

MỞ ĐẦU

Sự phát triển như vũ bão của khoa học công nghệ, đặc biệt là ngành công nghệ thông tin, đã tác động đến mọi mặt hoạt động của đời sống, kinh tế-xã hội, làm thay đổi nhận thức và phương pháp sản xuất kinh doanh của nhiều lĩnh vực, nhiều ngành kinh tế khác nhau, trong đó có lĩnh vực Ngân hàng. Những khái niệm về Ngân hàng điện tử, giao dịch trực tuyến, thanh toán trên mạng,... đã bắt đầu trở thành xu thế phát triển và cạnh tranh của các Ngân hàng thương mại ở Việt Nam.

Phát triển các dịch vụ Ngân hàng dựa trên nền tảng công nghệ thông tin – Ngân hàng điện tử- là xu hướng tất yếu, mang tính khách quan, trong thời đại hội nhập kinh tế quốc tế. Lợi ích đem lại của Ngân hàng điện tử là rất lớn cho khách hàng, Ngân hàng và cho nền kinh tế, nhờ những tiện ích, sự nhanh chóng, chính xác của các giao dịch.

Nhưng bên cạnh đó vấn đề bảo mật vẫn luôn là vấn đề được .Do đó đề tài này được nghiên cứu nhằm giới thiệu phương pháp mã hoá và bảo mật phổ biến nhất đang được thế giới áp dụng đó là chứng chỉ số. Đồng thời cũng nói lên ứng dụng của nó trong Ngân hàng.

Kết cấu của luận văn: Luận văn gồm 3 chương

Chương 1: Cơ sở toán học của chứng chỉ số

Chương 2: Chứng chỉ số.

Chương 3: Ứng dụng của chứng chỉ số trong lĩnh vực Ngân hàng.

CHƯƠNG 1: CƠ SỞ TOÁN HỌC CỦA CHỨNG CHỈ SỐ

1. SỐ HỌC MODULO

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 có 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 $\{0, 1, 2, \ldots\ldots, n-1\} \equiv Z_n$. Tập Z_n có thể được coi là tập hợp tất cả lớp tương đương 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≡4(mod 25)

Tương tự, 13*16 = 8 trong Z_{25}

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

Ví dụ: $Z_2 = \{ 0,1 \}$

$Z^*_2 = \{1 \mid$ 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 mod n = $a.b^{-1}$ mod 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} mod 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} mod 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 $a^{\phi(n)} \equiv 1 (\text{mod } n)$.

(ii).Nếu n là tích của các số nguyên tố phân biệt và nếu $r \equiv s (\text{mod } \phi(n))$ thì $a^t \equiv a^s (\text{mod } n)$ 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 $a^{p-1} \equiv 1 (\text{mod } p)$

Nếu $r \equiv s (\text{mod } p-1)$ thì $a^t \equiv a^s (\text{mod } p)$ 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, $a^p \equiv a (\text{mod } p)$ với mọi số nguyên a.

1.6. Thặng dư bậc hai theo modulo

Định 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 $x^2 \equiv a \text{ mod } n$, 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 $a = a^i \text{ mod } p$.

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	$a^{-1} \bmod n$	$O((\ln n)^2)$
Phép tính lũy thừa modulo	$a^k \bmod n$, 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:

$$x1 \neq x2 \text{ và } h(x1) = h(x2)$$

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. Giới thiệu một số hàm băm.

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, …, M_N, sử dụng hệ mã thuận tiện như DES để tính mã Hash như sau :

$$H_0 = \text{giá trị ban đầu}$$

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

$$G = H_N$$

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

$h^*: X \to (Z_2)^t$, 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:

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

Trong đó $|x_1| = |x_2| = \ldots = |x_{k-1}| = m - t - 1$ và $|x_k| = m - t - 1 - d$, $0 \leq d \leq m - t - 2$

$$\Rightarrow |x_k| \geq 1 \text{ và } m - t - 1 \geq 1, k \geq 2.$$

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

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 $y(x) \neq y(x')$ nếu $x \neq x'$

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

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

Hệ mật 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 ϵ E

$$e_k : P \rightarrow C$$

và một hàm giải mã d_k ϵ 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.

Và bây giờ chúng ta đi tìm hiểu qua một số hệ 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 $e_k(x) = (x + k) \bmod 26$ $d_k(y) = (y – k) \bmod 26$

$(x, y \text{ є } Z_{26})$

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 địch 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)

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

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 $k = (k_1, k_2,\ldots,k_m)$ є 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 $k = \pi \in S_m$, 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 $\gamma = \alpha^k \bmod p$ và $\delta = x.(\alpha^a)k \bmod p$

e. Nhận được bản mã là (γ, δ)

(ii). Giải mã:

a. Sử dụng khóa bí mật (a) và tính $\gamma^{p-1-a} \bmod p$

b. Lấy bản rõ: $x = \gamma^{p-1-a} .\delta \bmod p$

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 ($p=2357; \alpha=2; \alpha^a=1185$).

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 2: CHỨNG CHỈ SỐ

Ngày nay việc giao tiếp qua mạng Internet đã trở thành một nhu cầu cấp thiết. Các thông tin truyền trên mạng đều rất quan trọng, như mã số tài khoản, thông tin mật … Tuy nhiên với các thủ đoạn tinh vi, nguy cơ bị ăn cắp thông tin qua mạng cũng ngày càng gia tăng. Hiện nay, giao tiếp qua mạng Internet chủ yếu sử dụng giao thức TCP/IP. Đây là giao thức cho phép các thông tin được gửi từ máy tính này tới máy tính khác thông qua một loạt các máy trung gian hoặc các mạng riêng biệt. Chính điều này đã tạo cơ hội cho những "kẻ trộm" công nghệ cao có thể thực hiện các hành vi phi pháp. Các thông tin truyền trên mạng đều có thể bị nghe trộm, giả mạo, mạo danh… Các biện pháp bảo mật hiện nay, chẳng hạn như dùng mật khẩu, đều không được đảm bảo vì có thể bị nghe trộm hoặc dò ra nhanh chóng. Do vậy, để bảo mật, các thông tin truyền trên Internet ngày nay đều có xu hướng được mã hoá. Trước khi truyền đi, người gửi mã hoá thông tin, trong quá trình truyền, dù có "chặn" được các thông tin này, kẻ trộm cũng không thể đọc được vì thông tin đã bị mã hoá. Khi tới đích, người nhận sẽ sử dụng một công cụ đặc biệt để giải mã. Phương pháp mã hoá và bảo mật phổ biến nhất đang được thế giới áp dụng là ***chứng chỉ số (Digital Certificate)***. Dưới đây là một số khái niệm cơ bản về chứng chỉ số.

2.1. Khái niệm

Chứng chỉ số là một tệp tin điện tử dùng để xác minh danh tính một cá nhân, một máy chủ, một công ty… trên Internet. Nó giống như một bằng lái xe, hộ chiếu, chứng minh thư hay những giấy tờ xác minh cá nhân. Để có được chứng minh thư, bạn phải được cơ quan Công an sở tại cấp. Chứng chỉ số cũng vậy, phải do một tổ chức đứng ra chứng nhận những thông tin của bạn là chính xác, được gọi là ***Nhà cung cấp chứng thực số*** (Certificate Authority, ***viết tắt là CA***). CA phải đảm bảo về độ tin cậy, chịu trách nhiệm về độ chính xác của chứng chỉ số mà mình cấp.

Một chứng chỉ số có 3 thành phần chính:

1. Thông tin cá nhân của người được cấp.

2. Khoá công khai (Public key) của người được cấp.
3. Chữ ký số của cơ sở cấp chứng chỉ.

♦ ***Thông tin cá nhân của người được cấp***

Đây là các thông tin của đối tượng được cấp chứng chi số gồm tên, quốc tịch, địa chỉ, điện thoại, email, tên tổ chức … Phần này giống như thông tin trên chưng minh thư của mỗi người.

♦ ***Khoá công khai***

Trong khái niệm mật mã, khoá công khai là một giá trị được nhà cung cấp chứng thực đưa ra như một khoá mã hoá, kết hợp cùng với một khoá cá nhân duy nhất được tạo ra từ khoá công khai để tạo thành cặp khoá bất đối xứng. Nguyên lý hoạt động của khoá công khai trong chứng chie số là hai bên giao dịch phải biết khoá công khai của nhau. Bên A muốn gửi cho bên B thì phải dùng khoá công khai của bên B để mã hoá thông tin. Bên B sẽ dùng khoá cá nhân của mình để mở thông tin đó ra. Tính bất đối xứng trong mã hoá thể hiện ở chỗ khoá cá nhân có thể giải mã dữ liệu được mã hoá bằng khoá công khai (trong cùng một cặp khoá duy nhất mà một cá nhân sở hữu) nhưng khoá công khai không có khả năng giải mã lại thông tin, kể cả những thông tin do chính khoá công khai đó mã hoá. Đây là đặc tính cấn thiết vì có thể có nhiều cá nhân B, C, D… cùng thực hiện giao dịch và có khoá công khai của A, nhưng C, D… không thể giải mã được các thông tin mà B gửi cho A dù cho đã chặn bắt được các gói thông tin gửi đi trên mạng.Một cách hiểu nôm na, nếu chứng chỉ số là một chứng minh thư nhân dân, thì khoá công khai đóng vai trò như danh tính của bạn trên giấy chứng minh thư (gồm tên, địa chỉ, ảnh…) còn khoá cá nhân là đặc điểm nhận dạng và dấu vân tay của bạn.

♦ ***Chữ ký của CA cấp chứng chỉ.***

Còn gọi là chứng chỉ gốc. Đây chính là xác nhận của CA, bảo đảm tính chính xác và hợp lệ của chứng chỉ. Muốn kiểm tra một chứng chỉ số, trước tiên phải kiểm tra chữ ký số của CA có hợp lệ hay không. Trên chứng minh thư, đấy chính là con dấu xác nhận của Công an Tỉnh hoặc Thành phố mà bạn trực thuộc.Về nguyên tắc,

khi kiểm tra chứng minh thư, đúng ra đầu tiên phải xem con dấu này, để biết chứng minh thư có bị làm giả hay không.

♦ ***Cấu trúc của chứng chỉ số***

Cấu trúc của một chứng chỉ số bao gồm:

- ISSuer: Tên của CA tạo ra chứng chỉ
- Period of validity: ngày hết hạn của chứng chỉ số.
- Subject: bao gồm những thông tin về thực thể được chứng nhận.
- Public key: Khóa công khai được chứng nhận.
- Signature: do private key của CA tạo ra và đảm bảo giá trị của chứng nhận.

2.2. Phân loại chứng chỉ số

Chứng chỉ số không mang tính đa năng, cũng tương tư như việc một người có bằng lái xe máy, không đồng nghĩa với việc anh ta có thể lái được xe ô tô. Mỗi chứng chỉ số chỉ có tác dụng trong một phạm vi xác định. Dựa vào mục đích sử dụng người ta chia chứng chỉ số ra làm các loại sau:

♦ Cá nhân: Sử dụng bởi một người cụ thể. Chứng chỉ loại này được sử dụng chủ yếu cho mục đích đảm bảo an toàn trong các kết nối với môi trường Internet như bảo mật email hay các giao dịch web.

♦ Tổ chức: Đây là loại chứng chỉ sử dụng cho mục đích xác thực là chính. Trong các tổ chức, công ty sử dụng công nghệ chứng chỉ số đảm bảo xác thực các nhân viên một cách chính xác là dựa trên yếu tố: các thông tin định danh của người sử dụng được nhà phát hành chứng chỉ xác nhận thông qua chữ ký của mình.

♦ Máy chủ: Chứng minh quyền sở hữu một tên miền, cung cấp một kết nối https an toàn giữa máy chủ và client. Trong mô hình mạng LAN, thì chứng chỉ số đảm bảo việc xác thực và các kết nối an toàn giữa các host.

♦ Người phát triển: Chứng chỉ số còn cung cấp giải pháp chứng minh quyền tác giả, nguồn gốc phần mềm và đảm bảo tính toàn vẹn của chương trình phần mềm được cung cấp trên mạng Internet công khai.

2.3. Lợi ích của chứng chỉ số.

♦ ***Mã hoá***: Lợi ích đầu tiên của chứng chỉ số là tính bảo mật thông tin. Khi người gửi đã mã hoá thông tin bằng khoá công khai của bạn thì chắc chắn rằng chỉ có bạn mới giải mã được thông tin để đọc.

♦ ***Chống giả mạo***: Khi bạn gửi một thông tin, có thể là một dữ liệu hoặc một email, có sử dụng chứng chỉ số, người nhận sẽ kiểm tra được thông tin của bạn có bị thay đổi hay không. Bất kỳ một sự sửa đổi hay thay thế nội dung của thông điệp gốc đều sẽ bị phát hiện, bởi vì địa chỉ email của bạn, tên miền… đều có thể bị kẻ xấu làm giả để đánh lừa người nhận nhằm ăn cắp thông tin hoặc lây lan virus nhưng chứng chỉ số thì không thể làm giả nên việc trao đổi thông tin có kèm theo chứng chỉ số luôn đảm bảo an toàn.

♦ ***Xác thực***: Khi bạn gửi một thông tin kèm chứng chỉ số, người nhận – có thể là một đối tác kinh doanh, tổ chức hoặc cơ quan chính quyền… sẽ xác định được danh tính của bạn. Có nghĩa là dù không nhìn thấy bạn, nhưng qua hệ thống chứng chỉ số mà bạn và người nhận cùng sử dụng, người nhận sẽ biết chắc chắn đó là bạn chứ không phải một ai khác.

♦ ***Chống chối cãi nguồn gốc***: Khi sử dụng chứng chỉ số, bạn phải chịu trách nhiệm hoàn toàn về những thông tin mà chứng chỉ số đi kèm. Vì nếu chối cãi hay phủ nhận một thông tin nào đó không phải do mình gửi thì chứng chỉ số mà người nhận có được sẽ là bằng chứng khẳng định bạn là tác giả của những thông tin đó.

♦ ***Chữ ký điện tử***: Email đóng một vai trò khá quan trọng trong việc trao đổi thông tin hàng ngày của chúng ta vì ưu điểm nhanh, rẻ và dễ sử dụng. Tuy nhiên, email dễ bị tổn thương bởi các hacker. Những thông điệp gửi đi có thể bị đọc hoặc bị giả mạo trước khi đến tay người nhận, bạn sẽ ngăn ngừa được các nguy cơ này

mà vẫn không làm giảm lợi thế của email. Với chứng chỉ số cá nhân, bạn có thể tạo thêm một chữ ký điện tử vào email như một bằng chứng xác nhận của mình.

♦ ***Bảo mật webstie***: Khi website của bạn sử dụng cho mục đích thương mại điện tử hay cho những mục đích quan trọng khác, những thông tin trao đổi giữa bạn và khách hàng có thể bị lộ. Để tránh nguy cơ này, bạn có thể dùng chứng chỉ số SSL Sever để bảo mật cho website của mình. Chứng chỉ số SSL Sever cũng cho phép bạn lập cấu hình website của mình theo giao thức bảo mật SSL (Secure Sockets Layer). Loại chứng chỉ số này sẽ cung cấp cho website của bạn một định danh duy nhất đảm bảo với khách hàng của bạn về tính xác thực và tính hợp pháp của website. Chứng chỉ số SSL Sever cũng cho phép trao đổi thông tin an toàn và bảo mật giữa website với khách hàng, nhân viên và các đối tác của bạn thông qua công nghệ SSL mà nổi bận là các tính năng:

- Thực hiện mua bán bằng thẻ tín dụng.
- Bảo vệ những thông tin cá nhân của khách hàng.
- Đảm bảo hacker không thể dò tìm được mật khẩu.

♦ ***Đảm bảo phần mềm***: Nếu bạn là một nhà sản xuất phần mềm, chắc chắn bạn sẽ cần những "con tem chống hàng giả" cho những sản phẩm của mình. Đây là một công cụ không thể thiếu trong việc áp dụng hình thức sở hữu bản quyền. Chứng chỉ số Nhà phát triển phần mềm sẽ cho phép bạn ký vào các applet, script, Java software, ActiveX control, các file dạng EXE, CAB, DLL… Như vậy, thông qua chứng chỉ số, bạn sẽ đảm bảo tính hợp pháp cũng như nguồn gốc xuất cứ của sản phẩm. Hơn nữa, người dùng sản phẩm có thể xác thực được bạn là nhà cung cấp, phát hiện được sự thay đổi của chương trình (do vô tình hỏng hay do virus phá, bị crack và bán lậu…).

2.4. Nhà phát hành chứng chỉ.

Nhà phát hành chứng chỉ gọi tắt là CA (Certificate Authority) là hạt nhân của hệ thống PKI. Chỉ có CA mới có quyền phát hành chứng chỉ cho một đối tượng sau khi kiểm tra những thông tin về đối tượng đó. Trong hệ thống PKI, CA đóng vai trò

là một bên thứ ba mà các ứng dụng sử dụng chứng chỉ trong hệ thống phải tin tưởng. Muốn kiểm tra chữ ký của CA trên chứng chỉ, hệ thống sử dụng khoá công khai của nhà phát hành CA được CA tự chứng thực hoặc được chứng thực bởi một CA khác mà hệ thống tin tưởng.

Mỗi chứng chỉ có một thời gian sống nhất định. Sau khoảng thời gian này chứng chỉ cần được thu hồi và cấp phát mới cho đối tượng sử dụng. Mặt khác do một điều kiện nào đó việc sử dụng chứng chỉ là không hợp lệ ví dụ như khoá bí mật của chủ thể chứng chỉ bị tiết lộ; chứng chỉ cần được thu hồi. Nhà phát hành chứng chỉ cần quản lý trạng thái thu hồi của chứng chỉ để chương trình sử dụng đầu cuối sử dụng chứng chỉ một cách an toàn.

Như vậy CA không những quản lý chứng chỉ khi nó được khởi tạo mà CA còn phải quản lý cả chứng chỉ trong quá trình sử dụng.

♦ ***Các chức năng của CA:***

▪ ***Xác thực yêu cầu cấp phát chứng chỉ:*** Đây là quá trình kiểm tra thông tin định danh, cũng như cặp khoá mã của đối tượng yêu cầu cấp phát chứng chỉ. Quy trình diễn ra tuỳ thuộc vào hệ thống mà ta xây dựng. Việc xác minh này có thể được thực hiện gián tiếp thông qua một bên trung gian, như các trung tâm đăng ký địa phương, hoặc xác minh trực tiếp thông qua tiếp xúc trực tiếp.

▪ ***Phát hành chứng chỉ:*** Sau khi xác minh thông tin định danh, khoá mã hoá của các đối tượng yêu cầu cấp chứng chỉ, hoặc nhận được các yêu cầu từ một LRA, CA tiến hành cấp phát chứng chỉ cho đối tượng. Tuỳ thuộc vào chính sách của CA mà chứng chỉ sau khi tạo ra sẽ được đưa đến một kho chứa công khai để các ứng dụng lấy chứng chỉ về sử dụng.

▪ ***Phân phối chứng chỉ:*** Nhà phát hành chứng chỉ còn cung cấp các dịch vụ để các hệ thống sử dụng chứng chỉ truy cập và lấy về các chứng chỉ mà nó cần. Các dịch vụ này rất đa dạng nhưng sử dụng phổ biến nhất là dịch vụ email và dịch vụ thư mục LDAP.

▪ ***Thu hồi chứng chỉ:*** Khi một chứng chỉ được yêu cầu huỷ bỏ, hoặc do một nguyên nhân nào đó mà việc sử dụng chứng chỉ không còn an toàn, thì CA phải thu hồi chứng chỉ đó và phải thông báo cho toàn bộ hệ thống biết danh sách các chứng chỉ bị thu hồi thông qua các CRL (Certificate Revocation List - danh sách thu hồi chứng chỉ).

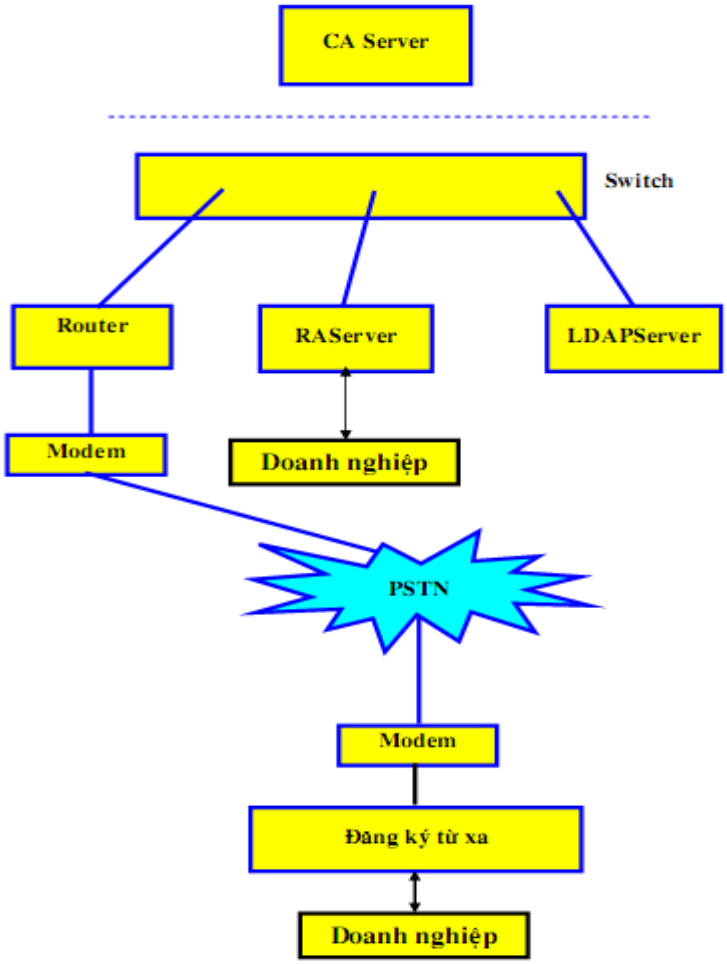
▪ ***Treo chứng chỉ:*** Trong trường hợp CA phát hiện ra các dấu hiệu khả nghi về việc sử dụng chứng chỉ là không còn an toàn nữa thì CA phải treo chứng chỉ, tức là chứng chỉ đó bị thu hồi tạm thời, nhưng nếu CA tìm được thông tin chứng minh rằng việc sử dụng chứng chỉ vẫn đảm bảo an toàn thì chứng chỉ sẽ được thay đổi lại trạng thái bị thu hồi.

▪ ***Gia hạn chứng chỉ:*** Trong trường hợp chứng chỉ hết hạn sử dụng, nhưng chứng chỉ vẫn đảm bảo tính bí mật khi sử dụng, thì nó có thể được cấp phát lại (tuỳ thuộc vào yêu cầu của chủ thể chứng chỉ). Tức là gia hạn thêm thời gian sử dụng cho chứng chỉ. Chứng chỉ được cấp mới không có gì thay đổi, ngoại trừ trường hợp thời gian hết hạn được thay, tất nhiên là kéo theo cả chữ ký của nhà phát hành chứng chỉ cũng thay đổi.

▪ ***Quản lý trạng thái chứng chỉ:*** Thông qua các CRL không những giúp cho các nhà phát hành chứng chỉ quảng bá thông tin về những chứng chỉ bị thu hồi mà còn giúp cho CA quản lý trạng thái thu hồi của chứng chỉ. VIệc quản lý trạng thái thu hồi này rất quan trọng, vì nếu các ứng dụng đầu cuối sử dụng chứng chỉ bị thu hồi thì hệ thống không còn an toàn nữa.

♦ ***Mô hình hoạt động của CA.***

Hệ thống CA hoạt động theo mô hình sau:



Trong đó:

▪ ***CA Sever:*** là thành phần quan trọng nhất trong hệ thống. Nó được cài đạt phần mềm CA và lưu giữ khoá riêng của CA. Chính vì vậy cần phải đảm bảo an toàn tuyệt đối cho CA Sever.

▪ ***RA Sever:*** cài đặt chương trình quản lý các đăng ký và các chứng chỉ. RA Sever thực hiện kiểm tra các yêu cầu đăng ký chứng chỉ, chấp nhận hoặc huỷ bỏ các yêu cầu đăng ký chứng chỉ trước khi chúng được CA ký, đồng thời gửi chứng chỉ đã được CA phát hành xuống các điểm đăng ký từ xa để chuyển cho doanh nghiệp, hoặc cũng có thể chuyển trực tiếp cho doanh nghiệp.

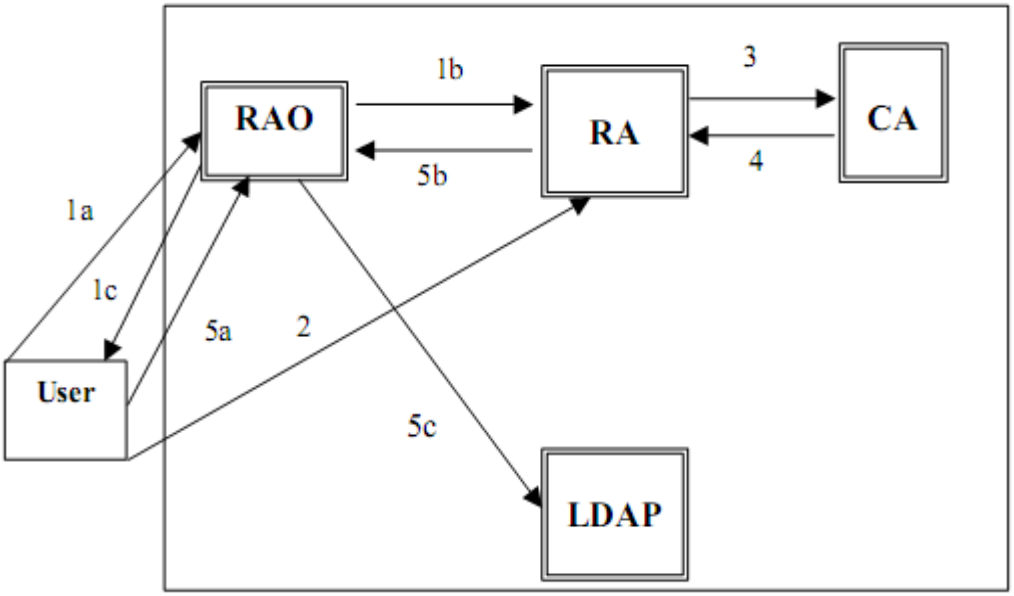
▪ ***LDAP Sever:*** là một máy chủ chứa tất cả các chứng chỉ đã được phát hành, cho phép các doanh nghiệp sử dụng dịch vụ thư mục để tra cứu thông tin về chứng chỉ.

▪ ***Điểm đăng ký từ xa:*** có nhiệm vụ kiểm tra thông tin đăng ký (chẳng hạn như xin cấp mới, huỷ bỏ, hoặc cấp lại chứng chỉ) của doanh nghiệp và ký xác nhận trước khi chuyển cho RA Sever. Tất cả quá trình thruyenf thông giữa RA Sever và điểm đăng ký từ xa được thực hiện thông qua những phiên liên lạc an toàn.

2.5. Quy trình cấp phát và thu hồi chứng chỉ.

2.5.1. Quy trình đăng ký và cấp chứng chỉ.

Người sử dụng có nhu cầu được cấp chứng chỉ đến trung tâm làm thủ tục đăng ký. Khi đến trung tâm người sử dụng cần đem theo những giấy tờ có liên quan đến bản thân (ví dụ như chứng minh thư). Việc thực hiện quá trình đăng ký nhân viên của hệ thống thực hiện qua from RAO.



Hình 1.1. Mô hình đăng ký và cấp chứng chỉ số

Hình 1.1 ở trên là mô hình quy trình đăng ký và cấp chứng chỉ số. Các thủ tục cần thực hiện được mô tả cụ thể như sau:

1a. Cá nhân (hoặc tổ chức) nào đó có nhu cầu sử dụng chứng chỉ số lên trung tâm đăng ký, có đem them một số giấy tờ cần thiết.

1b. Người quản trị máy RAO (nơi đăng ký) đưa thông tin đã đăng ký từ phía người sử dụng lên máy RA thông qua trang putDB (trang này đặt trên máy RA và

được thiết lập https). Sau bước này người sử dụng đã có trình sinh khoá riêng gắn với một IDkey duy nhất.

1c. Người sử dụng đem trình sinh khoá về (bước này có thể có hoặc không). Nếu người sử dụng hoàn toàn tin tưởng vào trung tâm thì có thể sinh khoá luôn tại trung tâm.

2. Người sử dụng sinh khoá (bằng trình sinh khoá đã được cấp) và yêu cầu cấp chứng chỉ. Sau đó gửi yêu cầu này lên trung tâm (máy RA).

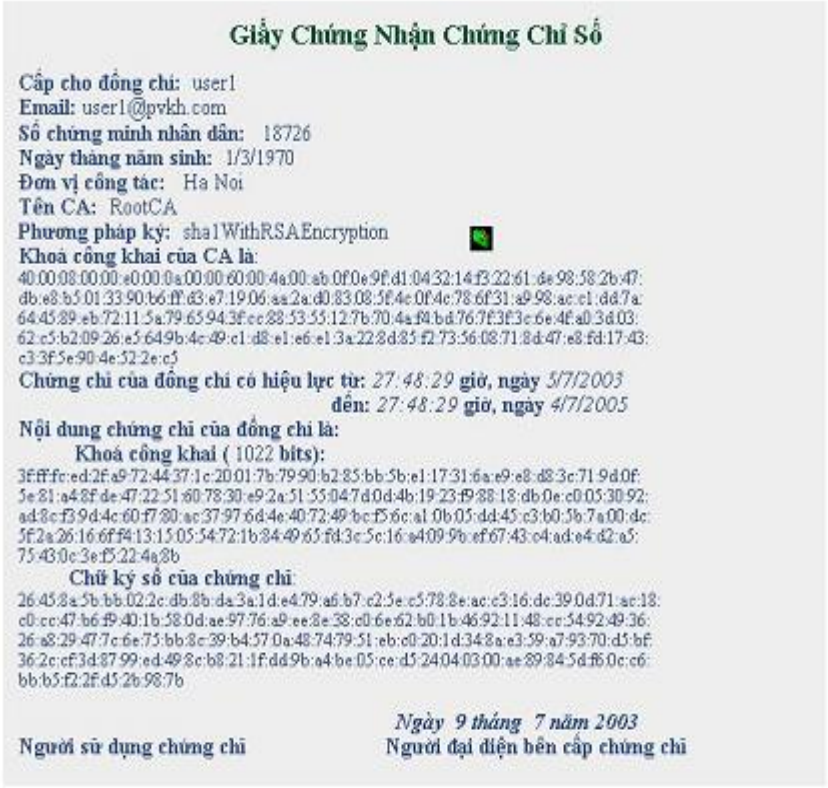
3. Người quản trị máy RA thực hiện so sánh thông tin đã đăng ký với thông tin gửi lên trung tâm qua đường công khai, đồng thời kiểm tra chữ ký của người dùng trong yêu cầu cấp chứng chỉ (bằng khoá công khai được gửi đến). Nếu hoàn toàn hợp lệ thì RA sẽ ký lên yêu cầu cấp chứng chỉ và gửi yêu cầu này sang máy CA.

4. Người quản trị máy CA kiểm tra chữ ký của RA trên yêu cầu cấp chứng chỉ của người sử dụng và IDkey trong cơ sở dữ liệu xem có bị trùng không, nếu hợp lệ thì CA chấp nhận yêu cầu cấp chứng chỉ đó, phát hành chứng chỉ (thực hiện ký trên chứng chỉ) và gửi sang máy RA.

5a. Người sử dụng lên trung tâm đã đăng ký để nhận chứng chỉ số và giấy chứng nhận chứng chỉ số. Để chặt chẽ hơn thì khi lên người sử dụng phải đem theo yêu cầu cấp chứng chỉ (đã có khi sinh yêu cầu cấp chứng chỉ) để trung tâm so sánh thông tin đã đăng ký và khoá công khai tương ứng với chứng chỉ số. Đây là bước đảm bảo cấp chứng chỉ số cho đúng người sử dụng và đảm bảo về mặt pháp lý.

5b. Người quản trị máy RAO lấy chứng chỉ số trên máy RA và cấp chứng chỉ số cùng giấy chứng nhận đã được cấp chứng chỉ cho người dùng.

5c. Chứng chỉ số của người dùng khi đó đã được công nhận trên toàn bộ hệ thống CA, được người quản trị máy RAO đưa công khai lên máy LDAP và người dùng khác có thể truy cập máy này để lấy về.



Giấy Chứng Nhận Chứng Chỉ Số

Cấp cho đồng chí: user1
Email: user1@pvkh.com
Số chứng minh nhân dân: 18726
Ngày tháng năm sinh: 1/3/1970
Đơn vị công tác: Ha Noi
Tên CA: RootCA
Phương pháp ký: sha1WithRSAEncryption
Khoá công khai của CA là:
40:00:08:00:00:e0:00:0a:00:00:60:00:4a:00:ab:0f:0e:9f:d1:04:32:14:f3:22:61:de:98:58:2b:47:
db:e8:b5:01:33:90:b6:ff:d3:e7:19:06:aa:2a:d0:83:08:5f:4c:0f:4c:78:6f:31:a9:98:ac:c1:dd:7a:
64:45:89:eb:72:11:5a:79:65:94:3f:cc:88:53:55:12:7b:70:4a:f4:bd:76:7f:3f:3c:6e:4f:a0:3d:03:
62:c5:b2:09:26:e5:64:9b:4c:49:c1:d8:e1:e6:e1:3a:22:8d:85:f2:73:56:08:71:8d:47:e8:fd:17:43:
c3:3f:5e:90:4e:52:2e:c5
Chứng chỉ của đồng chí có hiệu lực từ: *27:48:29* **giờ, ngày** *5/7/2003*
đến: *27:48:29* **giờ, ngày** *4/7/2005*
Nội dung chứng chỉ của đồng chí là:
Khoá công khai (1022 **bits):**
3f:ff:fc:ed:2f:a9:72:44:37:1c:20:01:7b:79:90:b2:85:bb:5b:e1:17:31:6a:e9:e8:d8:3c:71:9d:0f:
5e:81:a4:8f:de:47:22:51:60:78:30:e9:2a:51:55:04:7d:0d:4b:19:23:f9:88:18:db:0e:c0:05:30:92:
ad:8c:f3:9d:4c:60:f7:80:ac:37:97:6d:4e:40:72:49:bc:f5:6c:a1:0b:05:dd:45:c3:b0:5b:7a:00:dc:
5f:2a:26:16:6f:f4:13:15:05:54:72:1b:84:49:65:fd:3c:5c:16:a4:09:9b:ef:67:43:c4:ad:e4:d2:a5:
75:43:0c:3e:f5:22:4a:8b
Chữ ký số của chứng chỉ:
26:45:8a:5b:bb:02:2c:db:8b:da:3a:1d:e4:79:a6:b7:c2:5e:c5:78:8e:ac:c3:16:dc:39:0d:71:ac:18:
c0:cc:47:b6:f9:40:1b:58:0d:ae:97:76:a9:ee:8e:38:c0:6e:62:b0:1b:46:92:11:48:cc:54:92:49:36:
26:a8:29:47:7c:6e:75:bb:8c:39:b4:57:0a:48:74:79:51:eb:c0:20:1d:34:8a:e3:59:a7:93:70:d5:bf:
36:2c:cf:3d:87:99:ed:49:8c:b8:21:1f:dd:9b:a4:be:05:ce:d5:24:04:03:00:ae:89:84:5d:f6:0c:c6:
bb:b5:f2:2f:d5:2b:98:7b

Ngày 9 tháng 7 năm 2003
Người sử dụng chứng chỉ **Người đại diện bên cấp chứng chỉ**

Hình 1.2. Giấy chứng nhận chứng chỉ số.

2.5.2. Quy trình thu hồi chứng chỉ.

2.5.2.1. Lý do thu hồi chứng chỉ.

Trong vòng đời của chứng chỉ số, mặc dù nó vẫn trong thời gian tin cậy nhưng nó vẫn có thể bị nhà phát hành chứng chỉ thu hồi bởi rất nhiều lý do. Ví dụ như việc thoả hiệp khoá riêng của các đối tượng chứng chỉ hay thoả hiệp khoá riêng của nhà phát hành chứng chỉ, hay việc thay đổi các thông tin định danh của đối tượng.

Khoá riêng của đối tượng sử dụng chứng chỉ bị thoả hiệp dẫn tới việc sử dụng cặp khoá riêng, và công khai của đối tượng là không an toàn, đối tượng cần được thay thế bộ khoá riêng, công khai khác. Như vậy đồng nghĩa với việc cấp lại chứng chỉ cho đối tượng đó. Nhưng các ứng dụng sử dụng chứng chỉ phải biết rằng chứng chỉ cũ không còn hiệu lực, và như vậy chứng chỉ cũ cần được thu hồi.

Nếu khoá riêng của nhà phát hành chứng chỉ bị thoả hiệp, có nghĩa là quá trình kiểm tra chữ ký của nhà phát hành chứng chỉ là không an toàn, mọi chứng chỉ được ký bởi nhà phát hành này đều có nguy cơ bị giả mạo. Như vậy tất cả chứng chỉ được ký bởi nhà phát hành cần được thu hồi lại và tiến hành cấp phát mới.

Bên cạnh đó, lý do chứng chỉ được thu hồi bởi đối tượng sử dụng chứng chỉ thay đổi các thông tin định danh cũng xảy ra thường xuyên (ví dụ như thay đổi tên miền, IP…). Vì các thông tin trên chứng chỉ được ký bởi nhà phát hành chứng chỉ nên khi thay đổi thông tin định danh của đối tượng dẫn tới chữ ký trên chứng chỉ không còn giá trị nữa, như vậy chứng chỉ cũ cần được thu hồi và phát hành chứng chỉ mới.

Hệ thống cần có một kỹ thuật để truyền tải các trạng thái thu hồi chứng chỉ cho các ứng dụng sử dụng chứng chỉ. Trên thực tế các nhà phát hành chứng chỉ tạo ra các danh sách thu hồi chứng chỉ để công bố những chứng chỉ bị thu hồi.

2.5.2.2. Khái niệm danh sách thu hồi chứng chỉ.

Danh sách thu hồi chứng chỉ (Certificate Revocation List - CRL) là một kỹ thuật mà các nhà phát hành chứng chỉ dùng để công bố thông tin về các chứng chỉ được thu hồi cho các ứng dụng sử dụng chứng chỉ.Mỗi CRL là một cấu trúc dữ liệu chứa thông tin về thời điểm phát hành CRL, thông tin định danh của nhà phát CRL, và toàn bộ số serial của các chứng chỉ bị thu hồi cho tới thời điểm phát hành CRL… Toàn bộ các thông tin trên được xác thực bằng chữ ký của nhà phát hành chứng chỉ.

Trong quá trình sử dụng chứng chỉ, các ứng dụng sử dụng chứng chỉ sẽ lấy về CRL ở thời điểm hiện tại và phải đảm bảo rằng số hiệu của chứng chỉ mình sử dụng không có trong danh sách thu hồi chứng chỉ. Nếu số hiệu của chứng chỉ đang sủ dụng tồn tại trong CRL hiện tại đồng nghĩa với việc là chứng chỉ đó bị thu hồi bởi một lý do nào đó. Và việc sử dụng chứng chỉ là không đảm bảo an toàn.

2.5.2.3. Phân loại danh sách thu hồi chứng chỉ.

♦ ***CRL đầy đủ và hoàn chỉnh***: Đây là loại CRL đặ trưng nhất với khái niệm danh sách thu hồi chứng chỉ. Nó chứa thông tin về tất cả chứng chỉ bị thu hồi bởi

nhà phát hành CA. Trên thực tế không phải bao giờ người ta cũng dùng loại CRL này vì kích thước của nó phụ thuộc vào lượng chứng chỉ bị thu hồi, và theo lý thuyết thì đến một lúc nào đó dung lượng của nó lại là một vấn đề cần giải quyết khi nó được lưu trữ, tải về tại nhiều vị trí khác nhau.

♦ ***CRL thực thể cuối đầy dủ và hoàn chỉnh:*** Để giảm tải kích thước của một file chứa CRL đầy đủ ở trên người ta sử dụng loại CRL này. Đây là loại CRL chỉ chứa những chứng chỉ bị thu hồi bởi nhà phát hành chứng chỉ cho các thực thể sử dụng (không bao gồm các chứng chỉ của nhà phát hành chứng chỉ cấp dưới nếu chúng bị thu hồi).

♦ ***CRL nhà phát hành chứng chỉ đầy đủ và hoàn chỉnh:*** Đây là loại CRL chỉ chứa các chứng chỉ của nhà phát hành chứng chỉ cấp dưới bị thu hồi (có ý nghĩa bổ xung cho loại CRL trên).

♦ ***CRL con:*** Là một danh sách chứng chỉ bị thu hồi không đầy đủ, chúng chỉ chứa thông tin về những chứng chỉ bị thu hồi theo một tiêu chí nào đó tuỳ nhà phát hành quy định cho mỗi loại CRL. Ví dụ như CRL chỉ chứa thông tin về những chứng chỉ bị thu hồi do thoả hiệp khoá, hoặc CRL chỉ chứa thông tin về những chứng chỉ thu hồi do thay đổi thông tin định danh của chủ thể.

♦ ***Delta – CRL:*** Là loại CRL chỉ chứa thông tin về những chứng chỉ mới được thu hồi kể từ lần phát hành CRL trước. Như vậy để kiểm tra chính xác chứng chỉ đã bị thu hồi chưa thì hệ thống không những cần bản Delta – CRL này mà còn cả bản CRL toàn bộ và đầy đủ ở lần phát hành CRL trước. Tuy nhiên việc sử dụng bản Delta – CRL sẽ làm giảm tải dung lượng trên đường truyền.

2.5.2.4. Cập nhật danh sách thu hồi chứng chỉ.

Để giúp cho các hệ thống sử dụng chứng chỉ có được thông tin về những chứng chỉ bị thu hồi, CRL cần được thường xuyên cập nhật, có thể theo chu kỳ hàng giờ, hàng ngày, hàng tuần hay lâu hơn. Điều này phụ thuộc vào hệ thống mà ta xây dựng. Nếu như chu kỳ cập nhật CRL quá dài sẽ dẫn đến trường hợp các chương trình sử dụng chứng chỉ sẽ sử dụng những chứng chỉ bị thu hồi và như thế làm cho

quá trình kết nối không đảm bảo an toàn. Còn nếu chu kỳ cập nhật CRL ngắn, sẽ dẫn tới việc các chương trình sử dụng chứng chỉ mỗi khi đến chu kỳ cập nhật CRL lại yêu cầu hệ thống (hoặc tự thực hiện) kiểm tra xem chứng chỉ mà nó sử dụng có bị thu hồi hay không. Do chu kỳ ngắn nên mật độ các yêu cầu này đối với hệ thống là lớn, điều này có thể gây ra nhiều rắc rối bởi cơ sở hạ tầng vật lý, dung lượng đường truyền không cho phép thực hiện nhiều yêu cầu cùng một lúc.

2.5.2.5. Quản bá CRL.

Các chương trình sử dụng chứng chỉ muốn có được thông tin về trạng thái thu hồi của chứng chỉ mà nó sử dụng**.** Nó hoàn toàn có thể sử dụng một trong ba phương thức quản bá thông tin CRL mà hệ thống cấp phát chứng chỉ cung cấp**.** Dưới đây sẽ phân tích qua về ba phương thức đó:

♦ ***Bỏ phiếu danh sách thu hồi chứng chỉ:*** Trong phương thức bỏ phiếu chứng chỉ, chương trình sử dụng chứng chỉ chủ động truy cập vào kho CRL và lấy về bản CRL mới nhất. Các bản CRL có thể được lưu trữ và được lấy về trên các kênh truyền không an toàn, nhưng do được ký bởi nhà phát hành chứng chỉ nên mọi thay đổi thông tin trên CRL đều được phát hành thông qua việc kiểm tra tính toàn vẹn của CRL.

Với phương thức này hệ thống sử dụng chứng chỉ cần được biết thời điểm tiếp theo mà CRL được cập nhật. Thời điểm cập nhật tiếp theo phải được xác nhận trong mỗi bản CRL hiện thời để các chương trình có thể cập nhật thông tin chính xác về trạng thái thu hồi của chứng chỉ mà nó đang sử dụng.

Phương thức bỏ phiếu CRL bộc lộ một vài nhược điểm. Đó là nếu trong chu kỳ cập nhật CRL, chứng chỉ bị thu hồi thì trạng thái thu hồi của nó chỉ được ghi nhận ở lần công bố CRL tiếp theo. Như thế các hệ thống sử dụng chứng chỉ hoàn toàn không biết về trạng thái bị thu hồi thực sự của chứng chỉ, làm cho hệ thống sử dụng chứng chỉ không an toàn mà vẫn nhầm tưởng rằng chúng còn giá trị. Một giải pháp làm giảm bớt thời gian của chu kỳ cập nhật, tuy nhiên cũng chỉ đến một mức

nào đó. Bởi đến một giới hạn, thì chương trình sử dụng chứng chỉ không thể thực hiện được việc cập nhật vì chu kỳ của nó quá ngắn.

♦ ***Đẩy các CRL cho ứng dụng đầu cuối:*** CA có thể đẩy CRL xuống cho từng ứng dụng như là quá trình nó thu hồi chứng chỉ vậy. Mỗi khi có sự thay đổi trong CRL là hệ thống CA sẽ sử dụng phương pháp broadcast gửi phiên bản CRL mới nhất đến cho tất cả các ứng dụng sử dụng chứng chỉ. Và quá trình gửi này hoàn toàn không có chu kỳ như phương pháp bỏ phiếu bởi nó phụ thuộc vào quá trình chứng chỉ bị thu hồi, do đó giải quyết được nhược điểm của phương pháp bỏ phiếu CRL.

Tuy nhiên phương pháp này cũng có rất nhiều hạn chế. Thứ nhất việc gửi tin Broadcast phải đảm bảo rằng các CRL phải đến được đúng đích, nếu, nếu một ứng dụng trong hệ thống không có được phiên bản CRL mới nhất thì nó có thể thực hiện các giao dịch không đảm bảo. Thứ hai việc gửi CRL broadcast tới nhiều đích có thể làm mạng quá tải đường truyền. Cuối cùng và quan trọng hơn là làm thế nào để có thể broadcast tới tất cả các ứng dụng khác nhau, mà mỗi ứng dụng khác nhau chưa chắc đã có cùng giao thức kết nối. Việc quản lý các chương trình đầu cuối là cực kỳ khó khăn. Và điều này là tất yếu trong thực tế.

♦ ***Kiểm tra trạng thái thu hồi trực tuyến:*** Các ứng dụng có thể thực hiện một yêu cầu trực tuyến tới CA để kiểm tra trạng thái thu hồi của chứng chỉ mà nó đang sử dụng. Phương thức này tỏ ra ưu điểm hơn so với hai phương thức kia. Thứ nhất chúng loại bỏ bớt thời gian chết gây ra bởi chu kỳ cập nhật chứng chỉ. Thứ hai chúng hoàn toàn không gây quá tải đường truyền, bởi dữ liệu truyền trên mạng chỉ là các truy vấn. Và điều quan trọng hơn là không cần thêm hệ thống xác định, quản lý các ứng dụng chứng chỉ, bởi các yêu cầu kiểm tra trạng thái chứng chỉ là theo chuẩn và hệ thống CA không cần quan tâm tới cơ chế làm việc của từng ứng dụng một.

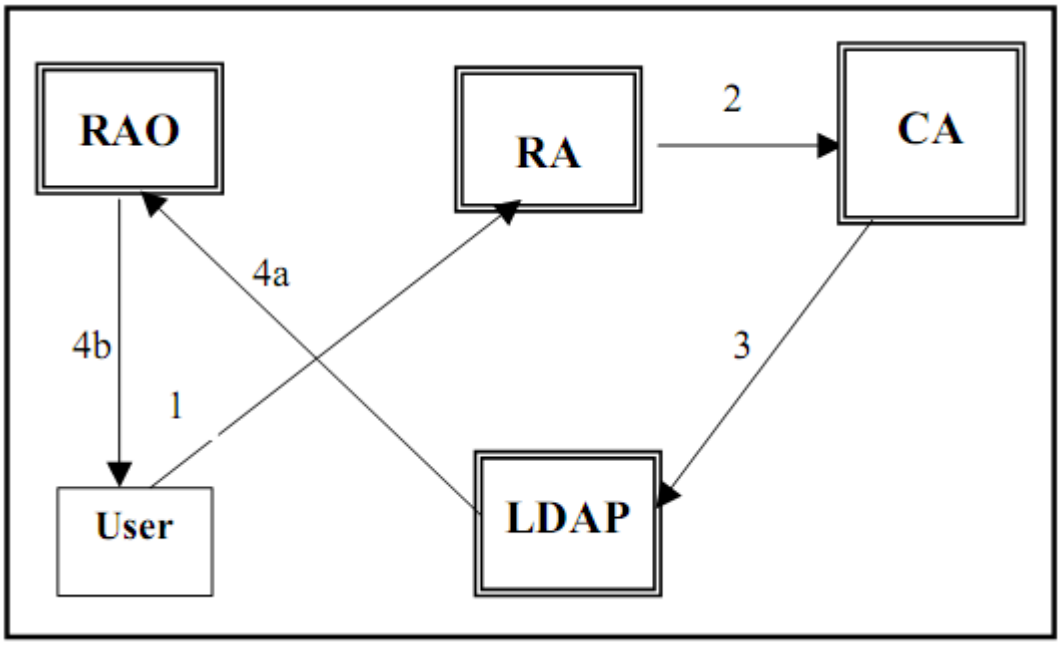
Tuy nhiên hệ thống CA phải đảm bảo luôn sẵn sàng khi có yêu cầu từ ứng dụng bất kỳ. Hơn thế nữa hệ thống CA còn phải thực hiện rất nhiều thao tác số học

phức tạp với các con số lớn do đó yêu cầu về nền tảng vật lý của CA là cao hơn rất nhiều so với hai phương pháp ban đầu.

2.5.3. Quy trình huỷ bỏ chứng chỉ.

Trong quá trình sử dụng chứng chỉ khi chưa hết hạn sử dụng người dùng có thể yêu cầu huỷ bỏ chứng chỉ với nhiều lý do: chuyển công tác, thay đổi địa chỉ e-mail, nghi ngờ lộ khoá bí mật…

Quy trình huỷ bỏ chứng chỉ được mô tả trong hình 1.3.



Hình 1.3: Mô hình huỷ bỏ chứng chỉ

1. Người sử dụng gửi yêu cầu huỷ bỏ chứng chỉ lên máy RA.
2. RA kiểm tra chữ ký trên yêu cầu huỷ bỏ chứng chỉ, nếu đúng thì ký sau đó chuyển sang máy CA.
3. CA kiểm tra chữ ký của RA trên yêu cầu huỷ bỏ chứng chỉ, nếu đúng thì ký sau đó chuyển sang máy LDAP

4a. Người quản trị cập nhật danh sách các chứng chỉ bị huỷ bỏ.

4b. Người dùng được cấp giấy chứng nhận huỷ bỏ chứng chỉ.

CHƯƠNG 3: ỨNG DỤNG CỦA CHỨNG CHỈ SỐ.

Do tính xác thực, tính bảo mật, tính toàn vẹn dữ liệu và tính không chối bỏ, chứng chỉ số được sử dụng trong khá nhiều các ứng dụng như: ký vào tài liệu điện tử, thư điện tử bảo đảm, thương mại điện tử, bảo vệ mạng WLAN (Wireless Lan Area Network), mạng riêng ảo (VPN).

Các nhu cầu đối với dịch vụ chứng thực điện tử khá đa dạng và bao quát nhiều lĩnh vực khác nhau. Trong thương mại điện tử, chứng chì số có thể được sử dụng nhằm chứng thực người tham gia vào giao dịch, xác thực tính toàn vẹn của giao dịch trên Internet, chứng thực tính toàn vẹn của hợp đồng, ...

Trong thực tế, hình thức các chứng chỉ số được sử dụng nhiều nhất trong các giao dịch thương mại điện tử, các giao dịch trong các cơ quan nhà nước, đặc biệt là các hoạt động thanh toán trực tuyến của ngân hàng.

3.1.Giao dịch ngân hàng online – Ngân hàng điện tử.

3.1.1. Khái niệm Ngân hàng điện tử.

Mạng Internet, mạng viễn thông và các mạng thông tin khác giúp con người thực hiện toàn bộ hoặc một phần các giao dịck qua mạng một cách thuận tiện và nhanh chóng, vì nó khắc phục được trở ngại về khoảng cách địa lý giữa các bên tham gia giao dịch.

Sự xuất hiện của các dịch vụ mới tại các ngân hàng như Home banking hay Phone banking đã mang lại nhiều tiện ích và sự hài lòng cho các ngân hàng cũng như khách hàng của họ. Tuy nhiên trên thực tế nó vẫn chưa có được sự ưu việt để đáp ứng các nhu cầu của khách hàng về thời gian và địa điểm. Vì vậy đã có sự ra đời của một mô hình cao hơn đó là Online banking.

Dịch vụ ngân hàng trực tuyến là sự kết nối trực tiếp giữa hệ thống phần mềm thanh toán của ngân hàng với hệ thống của các nhà cung cấp dịch vụ để thực hiện thanh toán giữa khách hàng vói nhà cung cấp dịch vụ. Bắt nguồn từ thực tế, điều mà doanh nghiệp cần hiện nay là một ngân hàng trực tuyến để ngồi ở bất cứ đâu,

truy cập mạng là có thể ra lệnh chuyển tiền dễ dàng và an toàn. Các ngân hàng trong nước đua nhau giới thiệu về dịch vụ Online Banking.

Với dịch vụ ngân hàng điện tử, khách hàng có khả năng truy nhập từ xa nhằm: thu thập thông tin, thực hiện các giao dịch thanh toán, tài chính dựa trên các tài khoản lưu ký tại ngân hàng, và đăng ký sử dụng các dịch vụ mới.

Dịch vụ ngân hàng điện tử là một hệ thống phần mềm vi tính cho phép khách hàng tìm hiểu hay mua dịch vụ Ngân hàng thông qua việc nối mạng máy vi tính của mình với ngân hàng.

Các khái niệm trên đều khái niệm Ngân hàng điện tử thông qua các dịch vụ cung cấp hoặc qua các kênh phân phối điện tử. Khái niệm này có thể đúng ở từng thời điểm nhưng không thể khái quát hết được cả quá trình lịch sử phát triển cũng như tương lai phát triển của Ngân hàng điện tử. Do vậy, nếu coi ngân hàng cũng như một thành phần của nền kinh tế điện tử, một khái niệm tổng quát nhất về Ngân hàng điện tử có thể được diễn đạt như sau: "*Ngân hàng điện tử là Ngân hàng mà tất cả các giao dịch giữa Ngân hàng và khách hàng (cá nhân và tổ chức) dựa trên quá trình xử lý và chuyển giao dữ liệu số hoá nhằm cung cấp sản phẩm dịch vụ Ngân hàng.*"

3.1.2. Sự phát triển Ngân hàng điện tử tại Việt Nam.

Trong thời gian vừa qua, hệ thống ngân hàng thương mại Việt Nam đã có những bước chuyển biến mạnh mẽ về quy mô cũng như chất lượng dịch vụ ngân hàng. Đặc biệt, đã có một số ngân hàng mạnh dạn thử nghiệm và cung cấp các dịch vụ ngân hàng điện tử cho khách hàng, mang lại dự thuận tiện, hiệu quả rất lớn cho khách hàng, ngân hàng và xã hội. Tuy nhiên phần lớn khách hàng còn dè dặt, thăm dò và sử dụng còn hạn chế vì hình như những khái niệm như Home-banking, Phone-banking, Mobile-banking, Internet-banking … còn tương đối mới mẻ và lạ lẫm. Do nhiều nguyên nhân(tài chính, con người, công nghệ…) nên một số ngân hàng cũng chưa có website và dịch vụ ngân hàng điện tử vẫn còn bỏ ngỏ.

Hiện nay, Ngân hàng điện tử tồn tại dưới hai hình thức: hình thức Ngân hàng trực tuyến, chỉ tồn tại dựa trên môi trường Internet, cung cấp dịch vụ 100% thông qua môi trường mạng; và mô hình kết hợp giữa hệ thống Ngân hàng thương mại truyền thống và điện tử hoá cá dịch vụ truyền thống, tức là phân phối những sản phẩm dịch vụ cũ trên kênh phân phối mới. Ngân hàng điện tử tại Việt Nam chủ yếu phát triển theo mô hình này.

Về nguyên tắc, thực chất dịch vụ của ngân hàng điện tử là việc thiết lập một kênh trao đổi thông tin tài chính giữa khách hàng và ngân hàng nhằm phục vụ nhu cầu sử dụng dịch vụ Ngân hàng của khách hàng một cách thực sự nhanh chóng, an toàn và thuận tiện. Sau rất nhiều tìm tòi, thử nghiệm và ứng dụng, hiện nay dịch vụ Ngân hàng điện tử được các Ngân hàng thương mại Việt Nam cung cấp qua các kênh chính sau đây: Ngân hàng trên mạng Internet (Internet-banking), Ngân hàng tại nhà (Home-banking), Ngân hàng tự động qua điện thoại (Phone-banking), Ngân hàng qua mạng thông tin di động (Mobile-banking)…

Một số dịch vụ ngân hàng điện tử ở Việt Nam:

♦ ***Internet Banking(Ngân hàng trên mạng Internet).***

Internet-banking là dịch vụ cung cấp tự động các thông tin sản phẩm và dịch vụ NH thông qua đường truyền Internet. Đây là một kênh phân phối rộng các sản phẩm và dịch vụ NH tới khách hàng ở bất cứ nơi đâu và bất cứ thời gian nào. Với máy tính kết nối Internet, khách hàng có thể truy cập vào website của ngân hàng để được cung cấp các thông tin, hướng dẫn đầy đủ các sản phẩm, dịch vụ của Ngân hàng. Bên cạnh đó, với mã số truy cập và mật khẩu được cấp, khách hàng cũng có thể xem số dư tài khoản, in sao kê…Internet-banking còn là một kênh phản hồi thông tin hiệu quả giữa khách hàng và Ngân hàng.

Các dịch vụ Internet-banking cung cấp:

- Xem số dư tài khoản tại thời điểm hiện tại.
- Vấn tin lịch sử giao dịch
- Xem thông tin tỷ giá, lãi suất tiền gửi tiết kiệm

- Thanh toán hóa đơn điện, nước, điện thoại.

- Khách hàng có thể gửi tất cả các thắc mắc, góp ý về sản phẩm, dịch vụ của Ngân hàng và được giải quyết nhanh chóng.

♦ ***Home Banking(Ngân hàng tại nhà).***

Ứng dụng và phát triển Home-banking là một bước phát triển chiến lược của các NHTM Việt Nam trước sức ép rất lớn của tiến trình hội nhập toàn cầu về dịch vụ NH. Đứng về phía khách hàng, Home-banking đã mang lại những lợi ích thiết thực như tiết kiệm chi phí, thời gian. Và khẩu hiệu "Dịch vụ Ngân hàng 24 giờ mỗi ngày, bảy ngày mỗi tuần" chính là ưu thế lớn nhất mà mô hình Ngân hàng "hành chính" truyền thống không thể nào sánh được. Hiện nay, dịch vụ Home-banking tại Việt Nam đã được nhiều NH tại Việt Nam ứng dụng và triển khai rộng rãi như: NH Á Châu, NH Ngoại thương Việt Nam, NH Kỹ thương….

Dịch vụ Ngân hàng tại nhà được xây dựng trên một trong hai nền tảng: hệ thống các phần mềm ứng dụng (Software Base) và nền tảng công nghệ Web (Web Base), thông qua hệ thống máy chủ, mạng Internet và máy tính con của khách hàng, thông tin tài chính sẽ được thiết lập, mã hóa, trao đổi và xác nhận yêu cầu sử dụng dịch vụ. Mặc dù có một số điểm khác biệt, nhưng nhìn chung, chu trình sử dụng dịch vụ Ngân hàng tại nhà bao gồm các bước cơ bản sau:

- Bước 1: Thiết lập kết nối (khách hàng kết nối máy tính của mình với hệ thống máy tính của Ngân hàng qua mạng Internet (dial-up, Direct-cable, LAN, WAN…), sau đó truy cập vào trang Web của Ngân hàng phục vụ mình (hoặc giao diện người sử dụng của phần mềm). Sau khi kiểm tra và xác nhận khách hàng, khách hàng sẽ được thiết lập một đường truyền bảo mật (https) và đăng

nhập (login) vào mạng máy tính của Ngân hàng.

- Bước 2: Thực hiện yêu cầu dịch vụ (khách hàng có thể sử dụng rất nhiều dịch vụ Ngân hàng điện tử phong phú và đa dạng như truy vấn thông tin tài khoản, chuyển tiền, hủy bỏ việc chi trả séc, thanh toán điện tử… và rất nhiều dịch vụ trực tuyến khác).

- Bước 3: Xác nhận giao dịch, kiểm tra thông tin, và thoát khỏi mạng (thông qua chữ ký điện tử, xác nhận điện tử, chứng từ điện tử…); khi giao dịch được hoàn tất, khách hàng kiểm tra lại giao dịch và thoát khỏi mạng, những thông tin chứng từ cần thiết sẽ được quản lý, lưu trữ và gửi tới khách hàng khi có yêu cầu.

Đối với các Ngân hàng khác nhau, quy trình nghiệp vụ cũng tương tự cùng với một vài đặc trưng riêng của mỗi Ngân hàng.

♦ ***Phone Banking (Ngân hàng qua điện thoại)***

Cũng như PC-banking, dịch vụ NH được cung cấp qua một hệ thống máy chủ và phần mềm quản lý đặt tại NH, liên kết với khách hàng thông qua tổng đài của dịch vụ. Thông qua các phím chức năng được khái niệm trước, khách hàng sẽ được phục vụ một cách tự động hoặc thông qua nhân viên tổng đài. Khi đăng ký sử dụng dịch vụ Phone-banking, khách hàng sẽ được cung cấp một mã khách hàng, hoặc mã tài khoản, tùy theo dịch vụ đăng ký, khách hàng có thể sử dụng nhiều dịch vụ khác nhau.

♦ ***Mobile Banking(Ngân hàng qua mạng di động).***

Cùng với sự phát triển của mạng thông tin di động, các Ngân hàng thương mại Việt Nam cũng đã nhanh chóng ứng dụng những công nghệ mới này vào các dịch vụ Ngân hàng. Về nguyên tắc, thông tin bảo mật được mã hóa và trao đổi giữa trung tâm xử lý của Ngân hàng và thiết bị di động của khách hàng (điện thoại di động, Pocket PC Palm…). Dịch vụ này đã được Ngân hàng Á Châu và Ngân hàng Kỹ thương triển khai từ lâu và các NH khác cũng đã và đang bắt đầu xây dựng hệ thống và cung ứng dịch vụ Mobile-banking do tính chất thuận tiện và nhanh chóng đặc trưng của nó.

♦ ***Kiosk Ngân hàng***

Là sự phát triển của dịch vụ Ngân hàng hướng tới việc phục vụ khách hàng với chất lượng cao nhất và thuận tiện nhất. Trên đường phố sẽ đặt các trạm làm việc với đường kết nối Internet tốc độ cao. Khi khách hàng cần thực hiện giao dịch hoặc yêu cầu dịch vụ, họ chỉ cần truy cập, cung cấp số chứng nhận cá nhân và mật khẩu

để sử dụng dịch vụ của hệ thống Ngân hàng phục vụ mình. Đây cũng là một hướng phát triển đáng lưu tâm cho các nhà lãnh đạo của các Ngân hàng thương mại Việt Nam. Hiện nay, Ngân hàng Kỹ thương đã thử nghiệm dịch vụ này tại hội sở Ngân hàng.

3.1.3. Tính ưu việt của dịch vụ Ngân hàng điện tử.

- Nhanh chóng, thuận tiện: Ngân hàng điện tử giúp khách hàng có thể liên lạc với Ngân hàng một cách nhanh chóng, thuận tiện để có thể thực hiện một số nghiệp vụ Ngân hàng tại bất kỳ thời điểm nào và bất cứ nơi đâu.

- Mở rộng phạm vi hoạt động, tăng khả năng cạnh tranh: Ngân hàng điện tử là một giải pháp của ngân hàng thương mại để nâng cao chất lượng dịch vụ và hiệu quả hoạt động, qua đó nâng cao khả năng cạnh tranh của các ngân hàng thương mại.

- Nâng cao hiệu quả sử dụng vốn: Thông qua các dịch vụ của Ngân hàng điện tử, các lệnh chi tra của khách hàng được thực hiện nhanh chóng, tạo điều kiện chu chuyển nhanh vốn tiền tệ, trao đổi tiền – hàng. Qua đó đẩy nhanh tốc độ lưu thông hàng hoá, tiền tệ, nâng cao hiệu quả sử dụng vốn.

- Tăng khả năng chăm sóc và thu hút khách hàng: Chính từ tiện ích công nghệ ứng dụng, từ phần mềm, từ nhà cung cấp dịch vụ mạng, dịch vụ Internet đã thu hút và giữ khách hàng sử dụng, quan hệ giao dịch với Ngân hàng. Với mô hình Ngân hàng hiện đại, kinh doanh đa năng nên khả năng phát triển, cung ứng các dịch vụ cho nhiều đối tượng khách hàng, nhiều lĩnh vực kinh doanh của Ngân hàng điện tử là rất cao.

- Cung ứng dịch vụ trọn gói: Điểm đặc biệt của dịch vụ Ngân hàng điện tử là có thể cung cấp các dịch vụ trọn gói. Theo đó các Ngân hàng có thể liên kết với các công ty bảo hiểm, công ty chứng khoán, công ty tài chính khác để đưa ra các sản phẩm tiện ích đồng bộ nhằm đáp ứng căn bản các nhu cầu của một khách hàng hoặc một nhóm khách hàng về các dịch vụ liên quan tới Ngân hàng, bảo hiểm, đầu tư, chứng khoán…

3.2. Điều kiện phát triển dịch vụ Ngân hàng điện tử.

3.2.1. Điều kiện pháp lý.

Dịch vụ Ngân hàng điện tử với việc sử dụng công nghệ mới đòi hỏi khuôn khổ pháp lý mới. Các dịch vụ Ngân hàng điện tử chỉ có thể triển khai được hiệu quả và an toàn khi các dịch vụ này được công nhận về mặt pháp lý.

Ngày 29/11/2005, Quốc hội nước Cộng Hoà Xã Hội Chủ Nghĩa Việt Nam đã thông qua Luật giao dịch điện tử số 51/2005/QH11. Luật này chính thức được áp dụng vào ngày 1/3/2006, tiếp đó, Chính phủ cũng đã ban hành một số Nghị định nhằm hướng dẫn chi tiết việc thi hành Luật giao dịch điện tủ:

- Ngày 09/06/2006: ban hành Nghị định số 57/2006/NĐ-CP hướng dẫn thi hành Luật giao dịch điện tử.
- Ngày 15/02/2007: ban hành Nghị định số 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.
- Ngày 23/02/2007: ban hành Nghị định số 27/2007/NĐ-CP quy định chi tiết thi hành luật giao dịch điện tử trong hoạt đọng tài chính.
- Ngày 08/03/2007: ban hành Nghị định số 35/2007/NĐ-CP quy định về giao dịch điện tử trong Ngân hàng.

3.2.2. Điều kiện về công nghệ.

An ninh bảo mật đã trở thành vấn đề sống còn của nghành Ngân hàng trong thời điện tử hoá. An ninh bảo mật cũng là mối quan tâm hàng đầu của khách hàng khi quyết định lựa chọn hình thức thanh toán phi tiền mặt. Vì vậy nếu thiếu những biện pháp an toàn bảo mật thì việc phát triển dịch vụ Ngân hàng điện tử không thể thực hiện được.

Để giữ bí mật khi truyền tải thông tin giữa hai thực thể nào đó người ta tiến hành mã hoá chúng. Có hai thuật toán mã hoá là thuật toán mã hoá đối xứng và thuật toán mã hoá bất đối xứng (thuật toán mã hoá khoá công khai). Và một trong các phương pháp dựa trên thuật toán mã hoá khoá công khai được ứng dụng nhều

nhất hiện nay và đặc biệt sử dụng trong giao dịch Ngân hàng điện tử là Chứng chỉ số. Đây là công nghệ cấp mã bất đối xứng mã hoá dữ liệu trên đường truyền và xác định rằng: về phía khách hàng được xác nhận là đang giao dịch, về phía ngân hàng được xác nhận là đang thực hiện giao dịch với khách hàng.

3.2.3. Điều kiện về con người.

Phụ thuộc vào ba yếu tố:

- ***Mức sống của người dân***: là một nhân tố quan trọng để phát triển dịch vụ thanh toán điện tử. Khi người dân phải sống với mức thu nhập thấp, hay nói cách khác có ít tiền thì có lẽ họ sẽ không quan tâm đến các dịch vụ Ngân hàng. Họ sẽ dùng tiền mặt thay vì các dịch vụ thanh toán điện tử.
- ***Sự hiểu biết và chấp nhận các dịch vụ Ngân hàng điện tử***: Thói quen và sự yêu thích dùng tiền mặt, tính "ì" của khách hàng trước các dịch vụ mới có thể là trở ngại chính cho việc phát triển Ngân hàng điện tử.
- ***Nguồn nhân lực của Ngân hàng***: Các hệ thống thanh toán điện tử đòi hỏi một lực lượng lớn lao động được đào tạo tốt về CNTT và truyền thông để cung cấp các ứng dụng cần thiết, đáp ứng yêu cầu hỗ trợ và chuyển giao các tri thức kỹ thuật thích hợp.

3.4. Giới thiệu một số Ngân hàng điện tử có ứng dụng Chứng chỉ số.

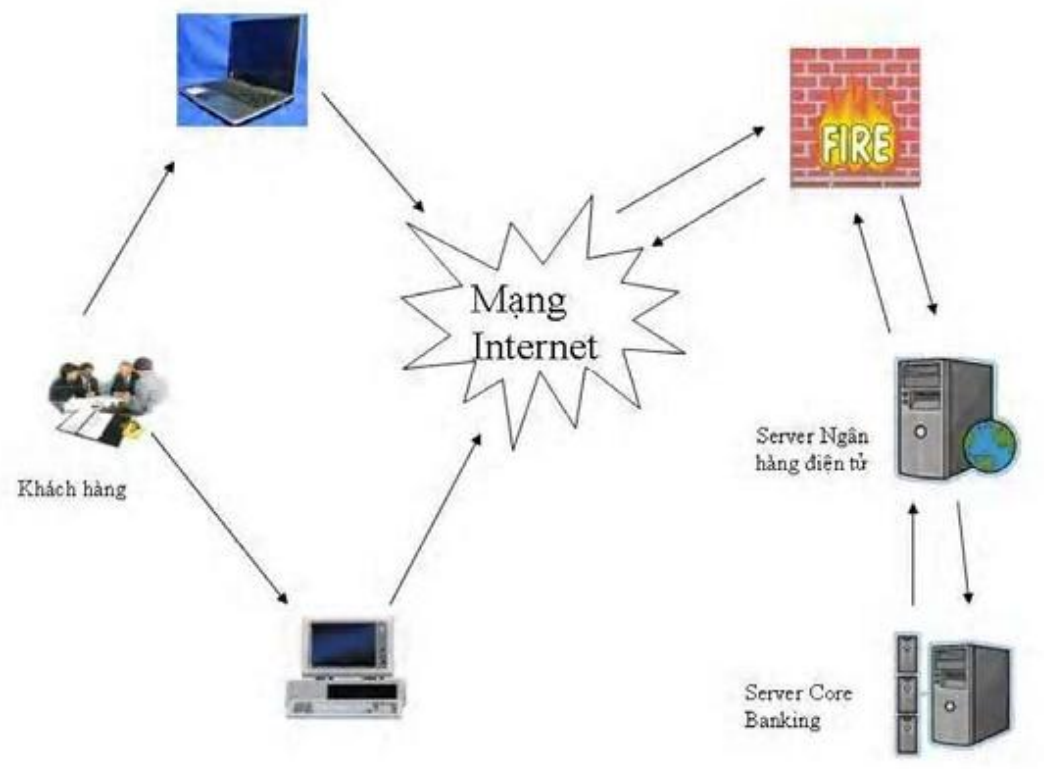
3.4.1. Ngân hàng Á Châu (ACB)Việt Nam.

Trong quá trình phát triển, Ngân hàng Á Châu không ngừng nâng cao chất lượng dịch vụ sẵn có và cung cấp dịch vụ mới nhằm phục vụ tốt hơn cho khách hàng. Vì thế, Ngân hàng Á Châu đã đưa vào sử dụng dịch vụ Ngân hàng điện tử với nhiều lợi ích và thuận tiện cho khách hàng, cùng với sự kiện này là việc thành lập phòng Ngân hàng điện tử vào năm 2003.

3.4.1.1. Hệ thống Ngân hàng điện tử tại ACB.

a) Phần cứng : sơ đồ mạng Ngân hàng

Nhằm đảm bảo sự giao dịch thuận tiện và chất lượng tốt, vừa an toàn cho hoạt động của Ngân hàng, vừa có thể xử lý được các giao dịch của Ngân hàng điện tử, Ngân hàng Á Châu đã bố trí hai máy chủ liên kết chạy song song với nhau: Sever Ngân hàng điện tử và Sever CoreBanking theo mô hình dưới đây:



Theo mô hình này, các giao dịch trên web sẽ được xử lý tại Sever Ngân hàng điện tử, sau đó định kỳ sẽ được cập nhật sang Sever CoreBanking và ngược lại.

b) Phần mềm:

♦***Phần mềm bảo mật:*** Chứng chỉ số (CA)

Ngày 30/09/2003, ABC đã chính thức ký hợp đồng "ứng dụng chứng chỉ số trong giao dịch Ngân hàng điện tử" với Công ty Phần mềm và Truyền thông VASC – nhà cung cấp chứng thực số (Certification Authorities - CA). Nhà cung cấp CA sẽ có trách nhiệm đảm bảo ba vấn đề cở bản: Chứng thực nguyên gốc dữ liệu, chống xem trộm, và toàn vẹn dữ liệu.

♦ ***Phần mềm sử dụng lưu trữ dữ liệu (Oracle Database).***

Oracle Database hỗ trợ việc lưu trữ khối lượng dữ liệu lớn lên đến hàng terabytes của Ngân hàng, Oracle cho phép quản lý và cấp phát các không gian lưu trữ một cách mềm dẻo và đầy đủ nhất. Đồng thời, nó hỗ trợ một số lượng lớn người sử dụng truy cập và thao tác đồng thời trên cùng một dữ liệu. Tuy nhiên, trong môi trường nhiều người sử dụng với các thao tác khác nhau, Oracle vẫn đảm bảo được hiệu suất tối ưu của toàn bộ hệ thống, đảm bảo được tính toàn vẹn của dữ liệu và giảm thiểu xung đột giữa những người sử dụng khác nhau.

♦ ***Công nghệ core-banking:***

Core-banking là công nghệ phần mềm lõi để xử lý đa dịch vụ với cơ sở dữliệu tập trung. ACB đã ứng dụng core-banking từ năm 2001 và hiện nay đang triển khai rất tốt, phục vụ cho việc giao dịch, quản lý cơ sở dữ liệu của khách hàng, hoạt động của các sản phẩm e-banking, sàn giao dịch vàng.

♦ ***Phần mềm hệ thống "Giải pháp Ngân hàng toàn diện".***

Giải pháp này được cung cấp bởi OSI (Open Solutions Incorporation) có trụ sở chính tại Hoa Kỳ. Hệ thống được triển khai tại ACB thông qua đối tác phân phối là công ty Thiên Nam. Giải pháp TCBS có thiết kế mềm dẻo, độ số hóa cao cho phép ACB cung cấp cho khách hàng nhiều sản phẩm đặc thù, có hàm lượng công nghệ cao như: quản lý tiền mặt, sản phẩm bao thanh toán, quản lý số liệu gửi vàng và ngoại tệ, dự thưởng – xổ số, và gần đây nhất là sàn giaodịch vàng…, góp phần giữ vững vị trí hàng đầu của ACB trong khối các Ngânhàng thương mại cổ phần tại Việt Nam.

♦ ***Mạng riêng ảo của Ngân hàng.***

Mạng riêng ảo hay VPN (viết tắt cho Virtual Bí mật Network) là một mạng dành riêng để kết nối mạng LAN của Ngân hàng dựa trên một đường truyền internet do Ngân hàng thuê riêng. Mạng VPN (Virtual Bí mật Network) là một

mạng riêng được xây dựng trên một nền tảng hạ tầng mạng công cộng như mạng Internet, sử dụng cho việc truyền thông riêng tư. Giải pháp VPN cho phép khách hàng có thể truy cập tại nhà hoặc khi đi công tác xa vẫn có thể truy cập được vào mạng Ngân hàng để kiểm tra và giao dịch bằng việc sử dụng hạ tầng mạng kết nối nội hạt tới một ISP. Trong quá trình thực hiện, VPN kết nối và thiết lập đường truyền giữa khách hàng với mạng Ngân hàng. Từ đây khách hàng sử dụng có thể thực hiện các công việc như đang ngồi ở công ty thay vì đến Ngân hàng. Kết nối VPN cũng cho phép các tổ chức kết nối liên mạng giữa các địa điểm đến ISP. Kết nối trực tiếp có thể giảm chi phí gọi đường dài qua dial-up và chi phí thuê đường leased line đường dài. Mọi dữ liệu, gói truyền thông chuyển đi đều được mã hoá đảm bảo an toàn nhất.

3.4.1.2. Các dịch vụ Ngân hàng điện tử được triển khai tại ACB

♦ ***Internet-banking.***

Đây là dịch vụ Ngân hàng quảng bá hoạt động và cung cấp thông tin đến khách hàng thông qua website được ACB xây dựng và cập nhật thường xuyên. Truy cập vào website http://www.acb.com.vn, khách hàng có thể nhận được những thông tin liên quan đến hoạt động của Ngân hàng, các thông tin về sản phẩm, dịch vụ mới. Khách hàng cũng có thể tham khảo biểu phí dịch vụ, lãi suất, tỷ giá, tham khảo các chỉ dẫn khi muốn đăng ký, sử dụng dịch vụ.

a. Tiện ích của sản phẩm:

- Thông qua trang web www.acb.com.vn, khách hàng có thể biết được:

+ Thông tin sản phẩm, dịch vụ mới của Ngân hàng một các nhanh chóng (sản phẩm tiền gửi thanh toán, sản phẩm tiền gửi tiết kiệm, sản phẩm tín dụng, sản phẩm Ngân hàng điện tử, thanh toán quốc tế, các dịch vụ thẻ…), các thông tin của công ty địa ốc, chứng khoán, sàn giao dịch vàng…

+ Thông tin về biểu phí, lãi suất tiết kiệm, tỷ giá hối đoái

+ Thông tin về giá chứng khoán.

+ Bảng giá vàng trực tuyến của sàn giao dịch vàng.

- Đăng ký thẻ trên mạng.

- Đăng ký vay trên mạng.

- Xem và in giao dịch từng tháng

- Kiểm tra số dư tài khoản, số dư thẻ

b. Đối tượng khách hàng: tất cả các khách hàng

c. Nguyên tắc hoạt động:

Mỗi khách hàng đến giao dịch tại ACB lần đầu tiên sẽ được cấp ngay mã số truy cập và mật khẩu để truy cập vào website của ACB và sử dụng dịch vụ.

Tất cả các tiện ích nêu trên được mỗi khách hàng kiểm tra và giao dịch một cách độc lập và bảo mật.

d. Cơ chế bảo mật:

Hệ thống Internet-banking được bảo mật dựa trên:

- Xác thực người sử dụng bằng mã số truy cập, mật khẩu.

- Khi nhập sai mật khẩu 5 lần, hệ thống sẽ khóa lại.

- Công nghệ mã hóa dữ liệu trên đường truyền SSL (Secure Sock

- Firewall

♦ ***Phone-banking.***

Đây là dịch vụ truy vấn thông tin cơ bản do Ngân hàng cung cấp cho khách hàng của mình thông qua điện thoại.

a. Tiện ích của sản phẩm:

- Kiểm tra số dư tài khoản tiền gửi thanh toán

- Nghe 5 giao dịch phát sinh mới nhất

- Kiểm tra các thông tin về lãi suất, tỷ giá hối đoái

- Kiểm tra các thông tin chứng khoán (kết quả khớp lệnh, kết quả 5 giao dịch đặt mua, đặt bán)

- Yêu cầu Ngân hàng fax bảng liệt kê giao dịch, lãi suất tiết kiệm, tỷ giá hối đoái .

- Yêu cầu Ngân hàng fax bản giá chứng khoán, liệt kê giao dịch chứng khoán

b. Đối tượng khách hàng: tất cả các khách hàng

c. Nguyên tắc hoạt động:

Khách hàng khi cần biết thông tin sẽ gọi đến số điện thoại cố định do Ngân hàng quy định trước và thực hiện tuần tự các bước theo hướng dẫn tự động bằng cách sử dụng các phím số và phím chức năng của điện thoại, khách hàng sẽ nhận được các thông tin phản hồi dựa trên phần mềm đã được cập nhật thông tin và cài đặt sẵn.

d. Cơ chế bảo mật:

Hệ thống Phone-banking được bảo mật dựa trên:

- Xác thực người sử dụng bằng mã số truy cập, mật khẩu.

- Khi nhập sai mật khẩu 5 lần, hệ thống sẽ khóa lại.

♦ ***Mobile-banking.***

Đây là kênh phân phối của dịch vụ Ngân hàng điện tử của ACB cho phép khách hàng (có tài khoản hay chưa có tài khoản tại ACB) dùng điện thoại di động nhắn tin theo mẫu quy định của Ngân hàng đến tổng đài 997 yêu cầu Ngân hàng cung cấp các dịch vụ: thông tin về tài khoản tiền gửi thanh toán, thông tin thẻ, thông tin về tỷ giá, chứng khoán… và thanh toán các hoá đơn, chuyển tiền từ tài khoản tiền gửi thanh toán qua thẻ bằng tin nhắn điện thoại di động.

a. Đối tượng khách hàng: tất cả các khách hàng

b. Nguyên tắc hoạt động:

Tùy theo nhu cầu, với chiếc điện thoại di động, khách hàng soạn tin nhắn theo cú pháp được quy ước cho từng dịch vụ, sau đó nhắn tin đến tổng đài 997 sẽ được Ngân hàng cung cấp các thông tin cần thiết hoặc được Ngân hàng thực hiện lệnh theo yêu cầu. Đối với dịch vụ thanh toán tiền hàng hóa, dịch vụ cho đơn vị chấp nhận, với yêu cầu bảo mật và đảm bảo tính chính xác của thông tin, một số câu lệnh đề nghị xác nhận giao dịch thể hiện dưới dạng tin nhắn sẽ được lưu chuyển giữa người sử dụng và trung tâm xử lý đặt tại Ngân hàng khi thực hiện giao dịch.

c. Cơ chế bảo mật:

Hệ thống Mobile-banking được bảo mật dựa trên:

- Xác thực người sử dụng bằng mã số truy cập, mật khẩu.
- Khi nhập sai mật khẩu 5 lần, hệ thống sẽ khóa lại.
- Xác thực số điện thoại di động đăng ký của khách hàng
- Xác thực một ký tự mật mã trong chiều dài mật mã, hạn mức khi khách hàng nhắn tin thanh toán
- Khách hàng muốn thanh toán phải đăng ký trước với Ngân hàng.

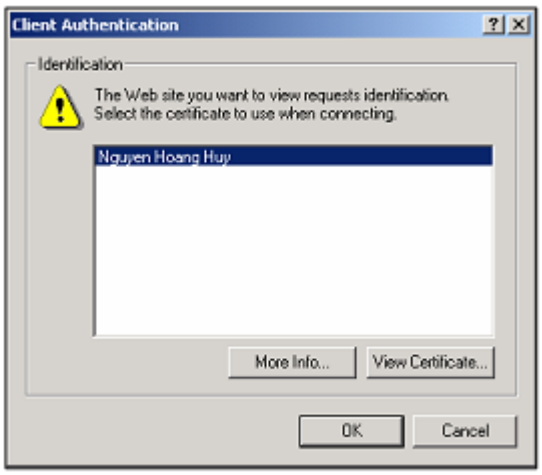
♦ ***Home-banking***

♦ ***Call-center.***

3.4.1.3. Hướng dẫn sử dụng dịch vụ Internet-banking.

- Truy cập vào website http:// www.internetbanking.acb.com.vn

- Màn hình yêu cầu chọn Chứng chỉ số để truy cập vào website, người dùng click chọn Chứng chỉ số với tên mình, sau đó chọn OK



- Màn hình đăng nhập vào hệ thống Internetbanking xuất hiện.

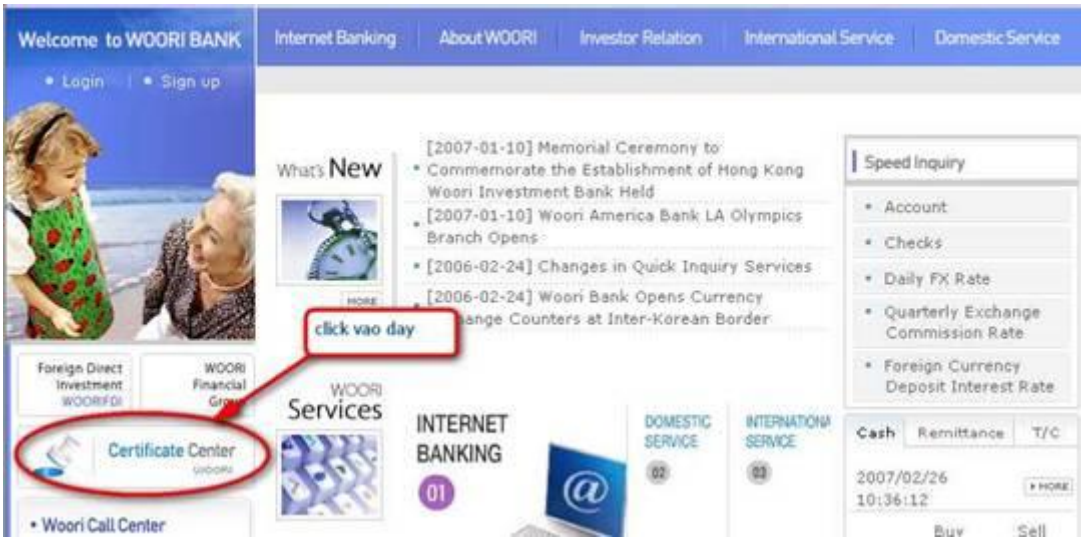
Quý khách nhập mã số truy cập và mật khẩu được ACB cung cấp khi khách hàng đăng ký sử dụng InternetBanking.

Đăng nhập thành công màn hình xuất hiện:

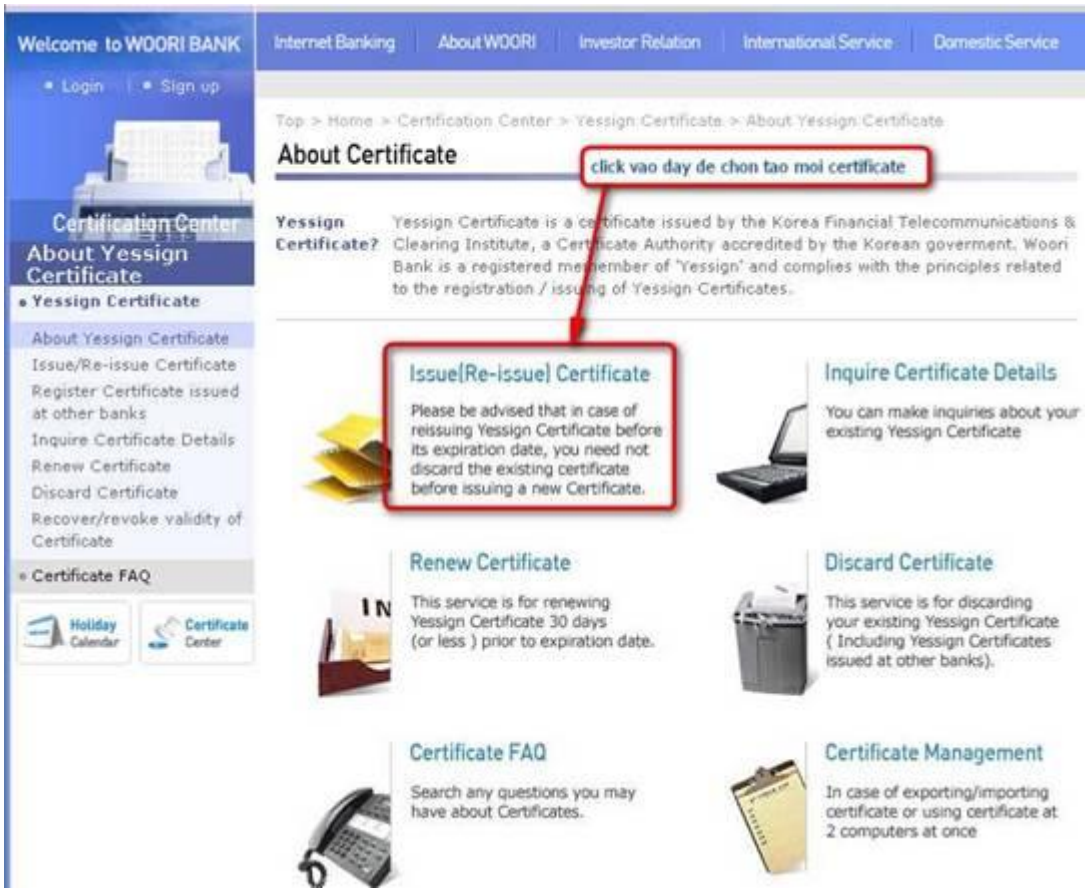
3.4.2. Ngân hàng Woori (Hàn Quốc).

1. Đăng nhập vào website http://www.wooribank.com sau đó chọn ngôn ngữ tiếng Anh (English) như hình dưới đây:

2.Chọn mục "Certificate center"



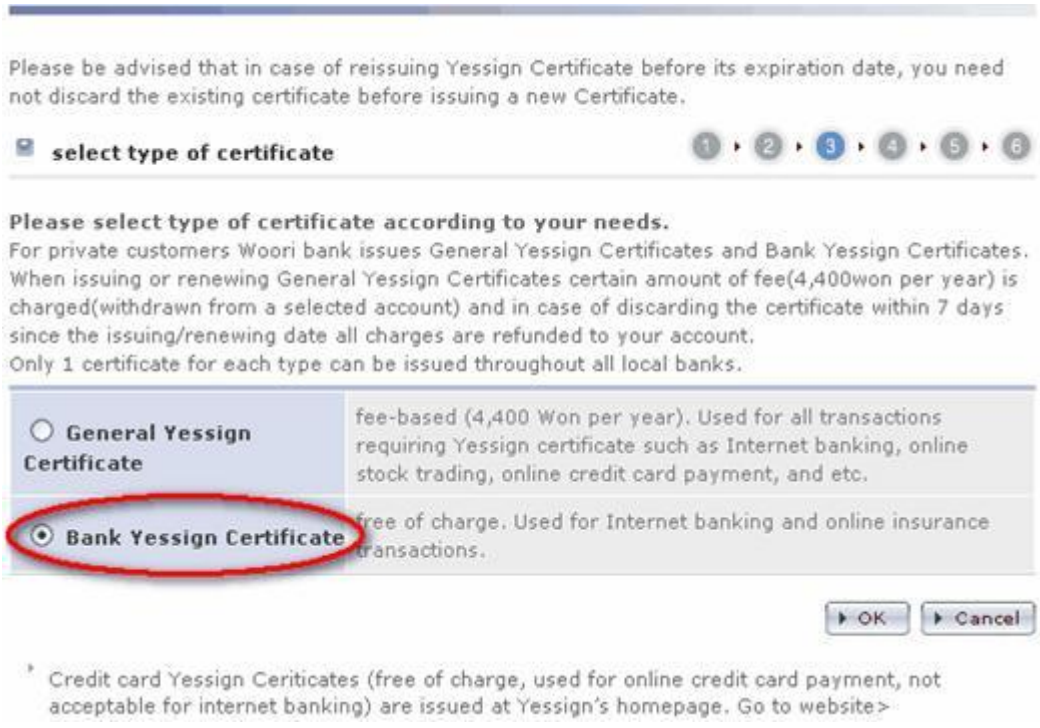
3. Chọn Issue (Re-issue) Certificate.



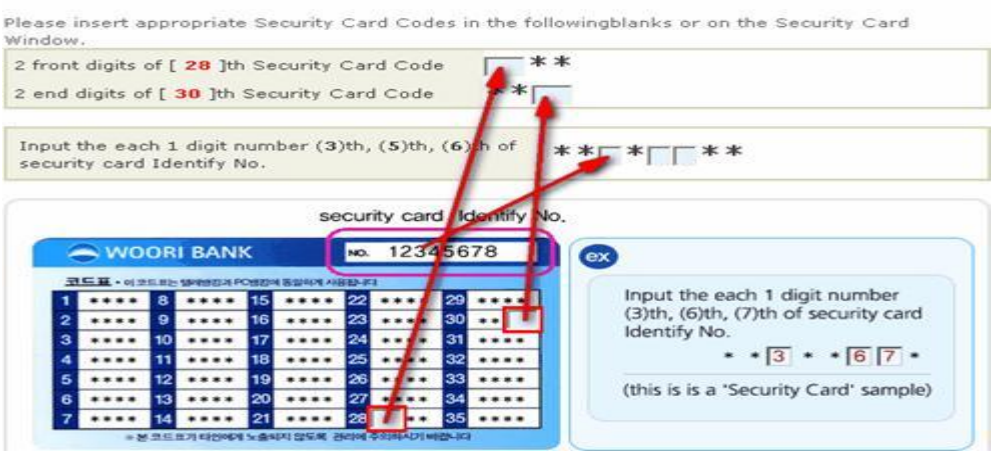
4. Đồng ý với thỏa thuận sử dụng dịch vụ.

5. Nhập tài khoản (account) Internet Banking mà ngân hàng cấp cho bạn và nhập số thẻ di trú (Alien card) sau đó chọn "OK".

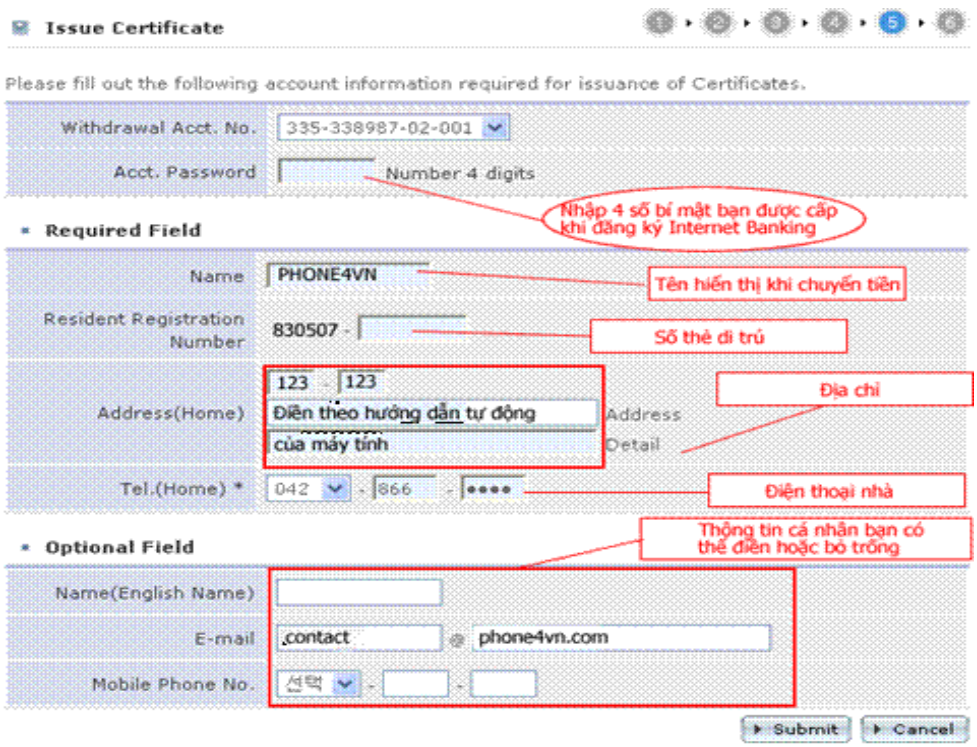
6. Chọn loại certificate như hình vẽ:



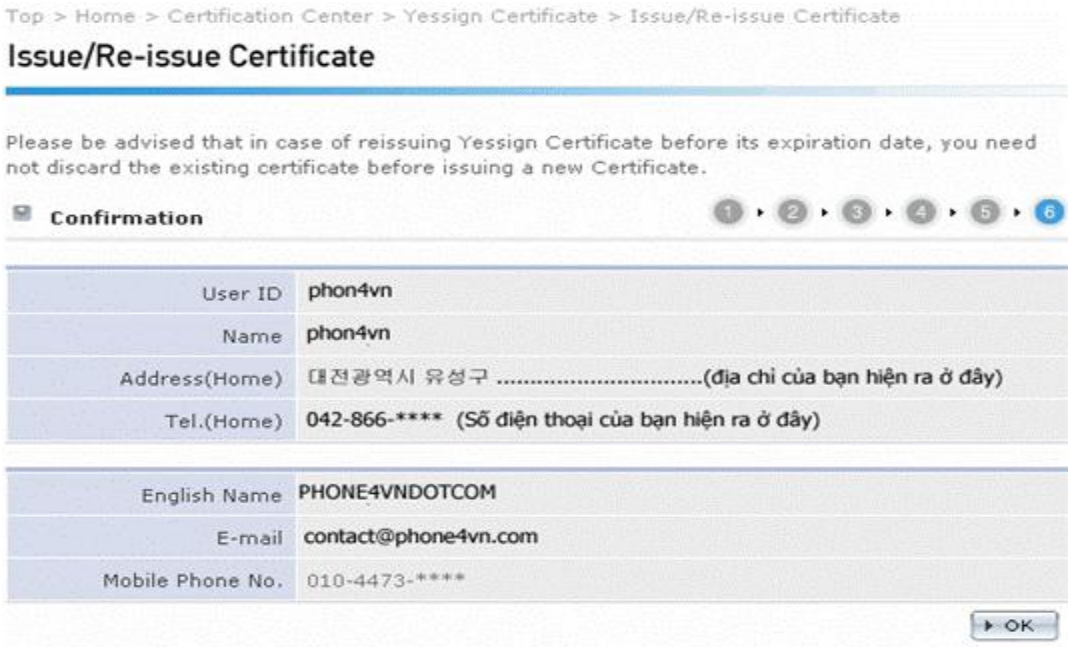
7. Điền các con số từ trong bảng vào các vị trí ngẫu nhiên do máy tính tạo ra (các bạn chú ý, một ô số gồm 4 con số, bạn cần điền 2 con số, 2 con số còn lại đánh dấu "*" trên màn ình thì bạn không cần điền).



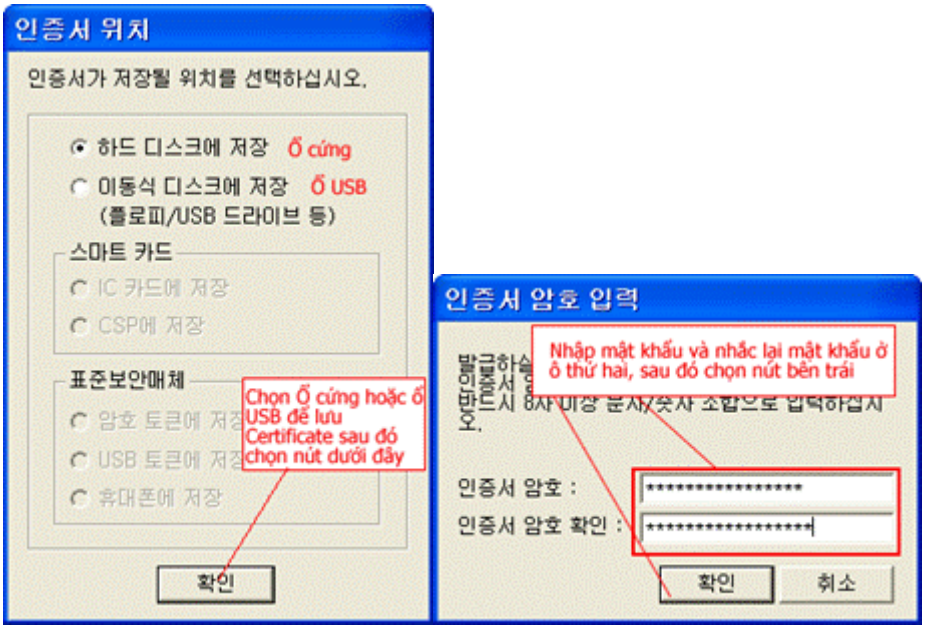
8. Điền thông tin theo hướng dẫn như hình vẽ.



9. Chọn OK để đồng ý tạo Certificte.



10. Chọn vị trí lưu Certificate (trên ổ cứng hoặc trên USB) và tạo password để truy nhập.



11. Hoàn thành quá trình tạo Certificate.

KẾT LUẬN

Ngày nay, những khái niệm về Ngân hàng điện tử, giao dịch trực tuyến, thanh toán trên mạng,... đã bắt đầu trở thành xu thế phát triển và cạnh tranh của các Ngân hàng thương mại ở Việt Nam. Phát triển các dịch vụ Ngân hàng dựa trên nền tảng công nghệ thông tin - Ngân hàng điện tử- là xu hướng tất yếu, mang tính khách quan, trong thời đại hội nhập kinh tế quốc tế.

Nhưng cùng với sự phát triển đó thì vấn đề bảo mật cũng là vấn đề được quan tâm hàng đầu. Do đó đề tài này được đưa ra và nghiên cứu nhằm mục đích:

- Tìm hiểu và nghiên cứu về lý thuyết mật mã và chứng chỉ số
- Tìm hiểu vấn đề an toàn thông tin nói chung và vấn đề an toàn thông tin trong lĩnh vực ngân hàng nói riêng.
- Tìm hiểu ứng dụng CNTT và đảm bảo an toàn trong lĩnh vực Internet – Banking.

TÀI LIỆU THAM KHẢO

1. Phan Đình Diệu, *Lý thuyết mật mã và an toàn thông tin*, NXB Đại Học Quốc gia Hà Nội, 2002

2. CHARLES P. PFLEEGER, *An toàn tính toán*, Học viện mật mã

3. Luận văn Phát triển dịch vụ Ngân hàng điện tử tại ngân hàng Thương mại Cổ phần Á Châu - LƯU THANH THẢO