LỜI CẢM ƠN

Em xin chân thành cảm ơn toàn thể các thầy cô giáo trong khoa Công Nghệ Thông Tin Trường Đại Học Dân Lập Hảo Phòng đã rất nhiệt tình dạy dỗ, chỉ bảo, tạo điều kiện tốt nhất cho em trong quá trình học tập cũng như thực tập và trong toàn bộ quá trình làm đò án tốt nghiệp này.

Đặc biệt em gửi lời cảm ơn chân thành và sâu sắc tới ThS Trần Ngọc Thái giáo viên khoa Công Nghệ Thông Tin Trường Đại Học Dân Lập Hải Phòng, người đã trực tiếp quan tâm,tận tình hướng dẫn, giúp đỡ và tạo điều kiện tốt nhất cho em trong quá trình thực hiện đồ án.

Tuy em đã có nhiều cố gắng trong quá trình học tập, thực tập cũng như trong thời gian làm đồ án nhưng không thể tránh khỏi những thiếu sót, em rất mong được sự góp ý quý báu cảu các thầy cô giáo cũng như tất cả các bạn để kiến thức của em được hoàn thiện hơn.

Em xin chân thành cảm ơn!

Hải Phòng ngày tháng năm 2010

Sinh Viên

Nguyễn Hồng Chính

MỤC LỤC

DANH MỤC CÁC TỪ VIẾT TẮT

Gcd (Greatest Common Divisor)	Ước số chung lớn nhất
Ord (Order)	Cấp
Pc (Personal Computer)	Máy tính cá nhân
TMĐT	Thương mại điện tử
TTĐT	Thanh toán điện tử
Smart Card	Thẻ thông minh
Pkl (Public Key infrastructure)	Cơ sở hạ tầng khóa công khai
Online	Trục tuyến
Offline	Ngoại tuyến
Gredit card	Thẻ tín dụng
Anonymaus	Ẩn danh
Identified	Định danh

DANH MỤC CÁC HÌNH VẼ

MỞ ĐẦU

Sự phát triển nhanh chóng của công nghệ thông tin và sự bùng nổ của internet đã mang lại những thay đổi chưa từng thấy trong thương mại điện tử, nó tác động mạnh mẽ đến lĩnh vực ngân hàng truyền thống, thúc đẩy sự phát triển của thương mại điện tử và làm xuất hiện hàng ngày các sản phẩm mới có liên quan đến ngân hàng như thẻ tín dụng, giao dịch ngân hàng qua điện thoại di động…và **tiền điện tử** hay ví điện tử cũng đang trở thành hiện thực. Trên thế giới tiền điện tử đã và đang được ứng dụng thành công, nhưng khái niệm "tiền điện tử" vẫn còn khá mới mẻ ở Việt Nam. Tuy nhiên với xu thế hôi nhập vào nền kinh tế thế giới, phát triển các dịch vụ thương mại điện tử là xu hướng tất yếu, chúng ta phải tìm hiểu và ứng dụng những dịch vụ mới trên thế giới. Chính vì thế khóa luận tìm hiểu và nghiên cứu một loại hình thanh toán điện tử mới, đã được ứng dụng thành công trên thế giới, đó là "**tiền điện tử**".

Khóa luận đề cập đến giải pháp và công nghệ sử dụng tiền điện tử, dựa trên việc tìm hiểu một số lược đồ, những hệ thống tiền điện tử điển hình và những lý thuyết mật mã được áp dụng trong giải pháp tiền điện tử.

Khóa luận gồm ba chương

Chương 1: Các khái niệm cơ bản

Trong chương này sẽ trình bày một số khái niệm toán học, vấn đề mã hóa, ký số, chữ ký mù, vấn đề xưng danh được áp dụng trong giải pháp tiền điện tử.

Chương 2: Thanh toán trong thương mại điện tử

Trong chương này sẽ trình bày mô hình thanh toán trong thương mại điện tử.

Chương 3: Thanh toán bằng tiền điện tử

Trong chương này sẽ tìm hiểu chi tiết về tiền điện tử, khái niệm, đặc điểm, phân loại. Tìm hiểu phân tích lược đồ CHAUM-FIAT-NAOR. Xây dựng chương trình mô phỏng tiền điện tử.

CHƯƠNG 1: CÁC KHÁI NIỆM CƠ BẢN

1.1 MỘT SỐ KHÁI NIỆM TOÁN HỌC

1.1.1 Số nguyên tố và nguyên tố cùng nhau

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

Ví dụ: 2, 3, 5, 7, 17,….. là những số nguyên tố.

Hệ mật mã thường sử dụng các số nguyên tố ít nhất là lớn hơn 10^{150}.

Hai số *m* và *n* được gọi là **nguyên tố cùng nhau** nếu ước số chung lớn nhất của chúng bằng 1. Ký hiệu gcd(*m*,*n*)=1.

Ví dụ: 9 và 14 là nguyên tố cùng nhau.

1.1.2 Đồng dư thức

Cho a và b là các số nguyên tố, n là số nguyên dương thì a được gọi là đồng dư với b theo modulo n nếu n|a-b (tức a-b chia hết cho n hay khi chia a và b cho n được cùng một số dư như nhau). Số nguyên n được gọi là modulo của đồng dư.

Ký hiệu: $a \equiv b \pmod n$

Ví dụ:

$67 \equiv 11 \pmod 7$, bởi $67 \pmod 7 = 4$ và $11 \pmod 7 = 4$

Tính chất đồng dư

Cho $a, a_1, b, b_1, c \in Z$ ta có các tính chất:

- $a \equiv b \bmod n$ nếu và chỉ nếu a và b có cùng số dư khi chia cho n.
- Tính phản xạ: $a \equiv a \bmod n$.
- Tính đối sứng: Nếu $a \equiv b \bmod n$ thì $b \equiv a \bmod n$.
- Tính giao hoán: Nếu $a \equiv b \bmod n$ và $b \equiv c \bmod n$ thì $a \equiv c \bmod n$.
- Nếu $a \equiv a_1 \bmod n$ và $b \equiv b_1 \bmod n$ thì $a + b = a_1 + b_1 \bmod n$ và $a.b = a_1.b_1 \bmod n$.

Lớp tương đương

Lớp tương đương của một số nguyên a là tập hợp các số nguyên đồng dư với a theo modulo n.

Cho n cố định đồng dư với n trong không gian Z vào các lớp tương đương. Nếu a = qn + r, trong đó $0 \leq r \leq n$ thì $a \equiv r \bmod n$. Vì vậy mỗi số nguyên a đồng dư theo modulo n với duy nhất một số nguyên trong khoảng từ 0 đến n-1 và được gọi là thạng dư nhỏ nhất của a theo modulo n. Cũng vì vậy, a và r cùng thuộc một lớp tương đương. Do đó r có thể đơn giản được sử dụng để thể hiện lớp tương đương.

1.1.3 Không gian Z_n và Z_n^*

Không gian Z_n (Các số nguyên theo modulo n) là tập hợp các số nguyên {0,1,2….n-1}. Các phép toán trong Z_n như cộng, trừ, nhân, chia đều được thực hiện theo modulo n.

Ví dụ:

Z_{11} = {0, 1, 2,….10}.

Trong Z_{11}: 6 + 7 = 2 vì $6 + 7 = 13 \equiv 2 \pmod{11}$.

Không gian Z_n^* là tập hợp các số nguyên $p \in Z_n$, nguyên tố cùng n. Tức là: $Z_n^* = \{p \in Z_n \mid \gcd(n,p) = 1\}$.

$\Phi_{(n)}$ là số phần tử của Z_n^*.

Nếu n là một số nguyên thì: $Z_n^* = \{p \in Z_n \mid 1 \leq p \leq n-1\}$.

Ví dụ:

$Z_2 = \{0,1\}$ thì $Z_2^* = 1$ vì gcd(1,2) = 1.

1.1.4 Phần tử nghịch đảo

Định nghĩa:

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

Tính chất:

- Cho a, b $\in Z_n$. Phép chia của a cho b theo modulo n là tích của a và b^{-1} theo modulo n. Và chỉ được xác định khi b có nghịch đảo theo modulo n.
- Cho a $\in Z_n$ a nghịch đảo khi và chỉ khi gcd(a,n) = 1.
- Giả sử a = gcd(a,n). Phương trình đồng dư ax ≡ b mod n có nghiệm x nếu và chỉ nếu d chia hết cho b. Trong trường hợp các nghiệm d nằm trong khoảng từ 0 đến n-1 thì các nghiệm đồng dư theo modulo n/d.

  Ví dụ:

  $4^{-1} = 7(\text{mod } 9)$ vì $4.7 = 1(\text{mod } 9)$.

1.1.5 Khái niệm nhóm, nhóm con, nhóm Cyclic

Nhóm là bộ các phần tử (G,*) thỏa mãn các tính chất:

- Kết hợp: (x*y)*z = x*(y*z).
- Tồn tại phần tử trung lập e ∈ G: e*x = x*e = x với $\forall x \in G$.
- Tồn tại phần tử nghịch đảo: $x' \in G : x' * x = x*x' = e$.

Nhóm con của nhóm (G,*) là bộ các phần tử (S,*) thỏa mãn các tính chất:

- S ⊂ G phần tử trung lập e ∈ S.
- x, y ∈ S =>x*y ∈ S.

Nhóm Cyclic: là nhóm mà mọi phần tử được sinh ra từ một phần tử đặc biệt g ∈ G. Phần tử này được gọi là phần tử sinh (nguyên thủy), tức là:

Với $\forall x \in G: \exists n \in N$ mà $g^n = x$.

Ví dụ: $(Z^+,*)$ là nhóm nhóm Cyclic có phần tử sinh là 1.

Định nghĩa:

Ta gọi cấp của nhóm là số các phần tử trong nhóm đó. Như vậy nhóm Z_n^* có cấp là $\Phi(n)$. Nếu p là số nguyên tố thì Z_p^* có cấp p- 1.

Định nghĩa:

Cho a $\in Z_n^*$, cấp của a (ord(a)) được định nghĩa là số nguyên dương nhỏ nhất t thỏa mãn $a^t \equiv 1 (\text{mod } n)$.

Ví dụ:

$Z_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$, $\Phi(21) = 12 = |Z_{21}^*|$.

Và cấp của từng thành phần trong Z_{21}^* là:

$A \in Z_{21}^*$	1	2	4	5	8	10	11	13	16	17	19	20
Cấp của a	1	6	3	6	2	6	6	2	3	6	6	2

1.1.6 Bộ phần tử sinh (Generator-tuple)

$\{g_1, \ldots\ldots g_k\}$ được gọi là bộ phần tử sinh nếu mỗi g_i là một phần tử sinh và những phần tử này khác nhau ($g_i \neq g_j$ nếu $I \neq j$).

Ví dụ: {3, 5} là bộ phần tử sinh của Z_7^*, bởi vì:

$1 = 3^6 \bmod 7 = 5^6 \bmod 7$

$2 = 3^2 \bmod 7 = 5^4 \bmod 7$

$3 = 3^1 \bmod 7 = 5^5 \bmod 7$

$4 = 3^4 \bmod 7 = 5^2 \bmod 7$

$5 = 3^5 \bmod 7 = 5^1 \bmod 7$

$6 = 3^3 \bmod 7 = 5^3 \bmod 7$

2 không phải là phần tử sinh của Z_7^* bởi vì:

$\{2^1, 2^2, 2^3, 2^4, 2^5, 2^6\} = \{2, 4, 1, 2, 4, 1\} \Leftrightarrow \{1, 2, 4\}$

Tuy nhiên {1, 2, 4} là tập con của {1, 2, 3, 4, 5, 6} = Z_7^*, do đó số 2 được gọi là phần tử sinh của nhóm G(3)", G(3) nghĩa là nhóm có 3 thành phần {1, 2, 4}.

1.1.7 Bài toán đại diện (Presentation problem)

Gọi g là phần tử sinh của nhóm G(q) thuộc Z_n^*. Bài toán logarit rời rạc liên quan đến việc tìm số mũ a, sao cho:

$a = \log_g h \bmod n$ (với $h \in G(q)$)

Cho k >=2, 1<=a_i<=q, I = 1……k.

Bài toán đại diện là: cho h thuộc G(q), tìm {a_1,……,a_k} của bộ phần tử sinh {g_1,…..,g_k}, sao cho:

h = g_1^{a1}*g_2^{a2}*…….*g_k^{ak} mod n

{a_1,……a_k} được gọi là đại diện (representation).

Ví dụ:

Cho Z_{23}^* thì ta có thể tìm được:

Nhóm con G(11) = {1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18} với những phần tử sinh g_i là: 2, 3, 4, 6, 8, 9, 12, 13, 16, 18.

{2, 3} là 2 phần tử sinh của nhóm con G(11) trong Z_{23}^*.

Bài toán đại diện với h = 13 ∈ G(11), tìm {a_1,a_2} sao cho

$$13 = 2^{a1}*3^{a2} \bmod 23$$

Logarit hai vế có a_1*log(2) + a_2*log(3) = log(13) mod 23

Kết quả là: a_1 = 2 và a_2 = 2 vì $2^2*2^3 = 4*9 = 36 = 13 \bmod 23$

Hay: a_1 = 7 và a_2 = 11 vì $2^7*2^{11} = 128*177147 = 13 \bmod 23$

1.1.8 Hàm băm

Hàm băm h là hàm một chiều (one-way hash) với các đặc tính sau:

- Với thông điệp đầu vào x thu được bản băm z = h(x) là duy nhất.
- Nếu dữ liệu trong thông điệp x thay đổi hay bị xóa để thành thông điệp x’ thì h(x) ≠ h(x’). Cho dù chỉ là sự thay đổi nhỏ hay chỉ là xóa đi 1 bit dữ liệu của thông điệp thì giá trị băm cũng vẫn thay đổi. Điều này có nghĩa là: hai thông điệp hoàn toàn khác nhau thì giá trị băm cũng khác nhau.
- Nội dung của thông điệp gốc không thể bị suy ra từ giá trị hàm băm nghĩa là: với thông điệp x thì dễ dàng tìm được z = h(x). Nhưng lại không thể (thực chất là khó) suy ngược lại được x nếu chỉ biết giá trị hàm băm h(x).

Tính chất:

Hàm băm h là không va chạm yếu:

Nếu cho trước một bức điện x, thì không thể tiến hành về mặt tính toán để tìm ra một bức điện x’ ≠ x mà h(x’) = h(x).

Hàm băm h là không va chạm mạnh:

Nếu không có khả năng tính toán để tìm ra hai bức thông điệp x và x’ mà x ≠ x’ và h(x) = h(x’).

1.2 VẤN ĐỀ MÃ HÓA

1.2.1 Khái niệm mã hóa

Mã hóa là phương pháp để biến thông tin (phim ảnh, văn bản, hình ảnh…) từ dạng bình thường sang dạng thông tin "khó" thể hiện được, nếu không có phương tiện giải mã. Giải mã là phương pháp để chuyển thông tin đã được mã hóa về dạng thông tin ban đầu (quá trình ngược của mã hóa).

Ví dụ:

Thông điệp cần mã hóa là chuỗi nhị phân M = 1011, hàm mã hóa và hàm giải mã là hàm XOR với k = 1010.

Mã hóa:

M	1011
K	1010
C	0001

Giải mã:

M	0001
K	1010
C	1011

Việc giao dịch thông tin trên mạng ngày càng trở lên phổ biến, vấn đề an toàn thông tin được đặt ra, làm thế nào để thông tin không bị đánh cắp. Nếu kẻ cắp lấy được dữ liệu nhưng khó lấy được thông tin thực sự. Điều này có thể thực hiện bằng cách mã hóa, nghĩa là trước khi gửi thông điệp, thông điệp được chuyển từ bản rõ sang bản mã, rồi mới gửi đi.Kẻ cắp có thể lấy được bản mã nhưng khó có thể lấy được bản rõ (nghĩa là không lấy được nội dung thông điệp).

Mã hóa tuân theo quy tắc nhất định gọi là Hệ mã hóa. Hiện nay có hai loại mã hóa:

- Mã hóa khóa đối xứng
- Mã hóa khóa công khai (phi đối xứng)

Hệ mã hóa được định nghĩa là bộ năm (P,C,K,E,D) trong đó:

P: là tập hữu hạn các bản rõ có thể.

C: là tập hữu hạn các bản mã có thể.

K: là tập hữu hạn cá khóa có thể.

E: là tập các hàm lập mã.

D: là tập các hàm giải mã d_k: C –> P sao cho $d_k(e_k(x)) = x$ với $\forall x \in P$.

Hệ mã hóa khóa công khai sử dụng một cặp khóa. Một trong hai khóa được gọi là khóa riêng (privete key) và phải được giữ bí mật bởi người sở hữu. Khóa còn lại được gọi là khóa công khai (public key), nó được phổ biến cho tất cả những ai muốn giao dịch với người giữ khóa giêng tương ứng. Cặp khóa này có liên quan về mặt toán học, và không thể sử dụng các thông tin của khóa công khai để tìm ra khóa riêng. Theo lý thuyết bất kỳ ai cũng có thể gửi cho người giữ khóa riêng một thông điệp được mã hóa bằng khóa công khai, và như vậy chỉ có người nào sở hữu khóa riêng mới có thể giải mã được. Đồng thời người sở hữu khóa riêng cũng chứng minh được tính toàn vẹn của giữ liệu mà anh ta gửi cho người khác bằng chữ ký điện tử thông qua việc sử dụng khóa riêng để mã hóa. Bất kỳ ai nhận được giữ liệu đó đều có thể sử dụng khóa công khai tương ứng để kiểm tra xem nó do ai gửi và có còn toàn vẹn hay không.

1.2.2 Hệ mã hóa khóa công khai

RSA là hệ mã hóa khóa công khai và độ an toàn của hệ dựa vào bài toán khó "phân tích số nguyên thành thừa số nguyên tố", sau đây là chi tiết về hệ mã hóa RSA.

Sơ đồ:

- Chọn p, q là số nguên tố lớn.
- Tính $n = p*q$,$\Phi(n) = (p-1)*(q-1)$.
- Chọn b là số nguyên tố với $\Phi(n)$ để tồn tại phần tử nghịch đảo b^{-1} nghĩa là $gcd(b,\Phi(n))=1$.
- Chọn a là nghịch đảo của b: $a*b=1 \bmod \Phi(n)$ (nghịch đảo theo modulo $\Phi(n)$).

  + b là khóa lập mã công khai.

  + a là khóa giải mã giữ bí mật.

Lập mã:

- Chọn P=C=Z_n với n=p*q,Z_n = {0,1,2,….,n-1}

  $x \in Z_n \rightarrow y=x^b \bmod n \in Z_n$.

Giải mã:

$y \in Z_n \rightarrow x \equiv y^a \bmod n \in Z_n$.

Ví dụ:

Giả sử ông B cần gửi cho ông A một thông điệp x = 8 trên kênh truyền công công. A và B muốn giữ bí mật tài liệu hai bên thống nhất sử dụng hệ mã hóa RSA.

Sau đây là các bước thực hiện A và B trao đổi thông điệp:

Chuẩn bị:

Lấy p = 3, q = 5.

→ n = p*q = 3*5 = 15; $\Phi(n) = (p-1)*(q-1) = 2*4 = 8$.

Chọn b = 7 (thỏa mãn gcd(7,8) = 1).

→ $a = b^{-1} \bmod \Phi(n) = 7$(thỏa mãn 7*7 = 1 mod 8).

→ khóa công khai b = 7; n = 15.

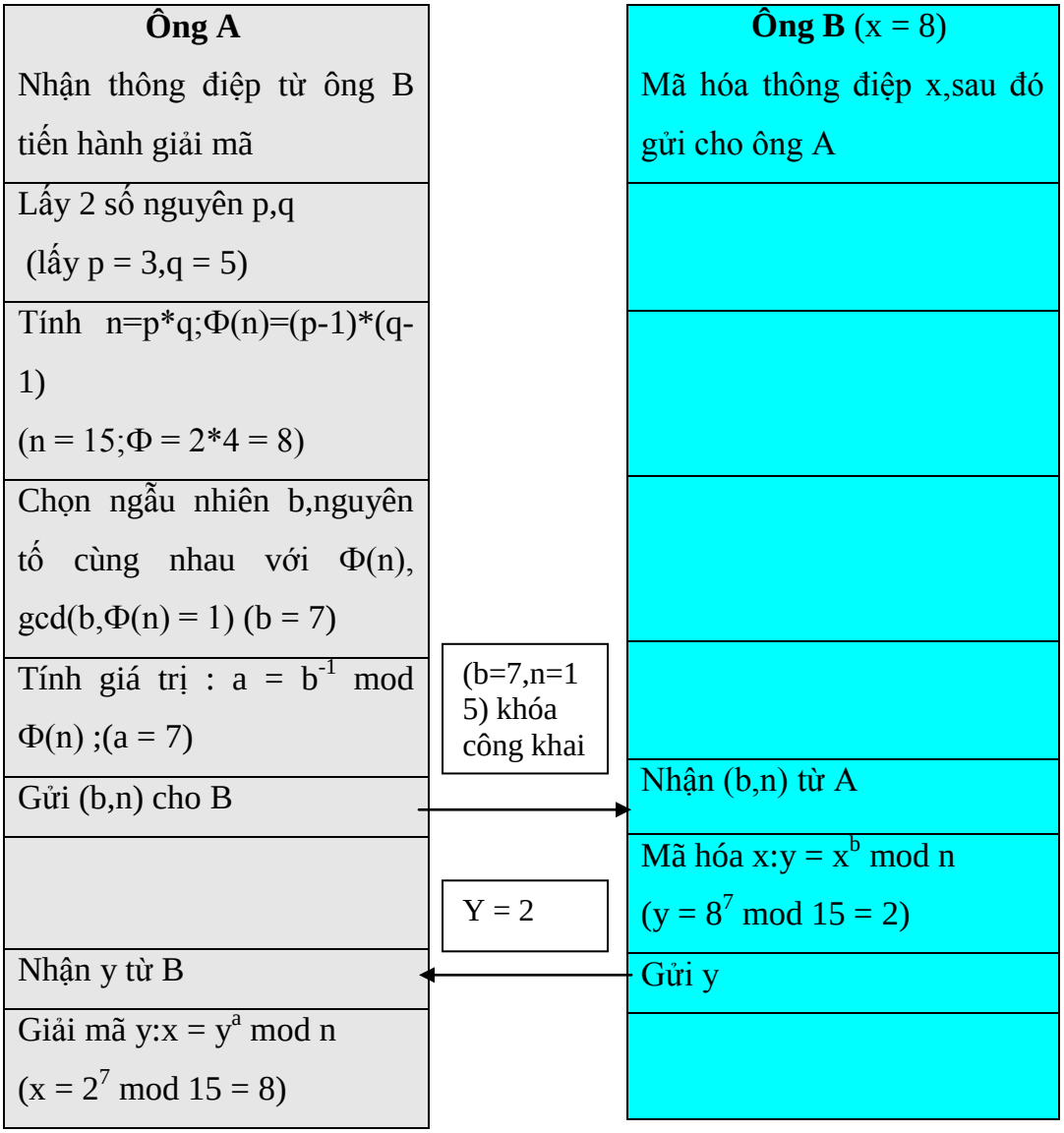
→ khóa bí mật a = 7.

Quá trình mã hóa:

Cho x = 8; mã hóa: $y = x^b \bmod n = 8^7 \bmod 15 = 2097152 \bmod 15 = 2$.

Quá trình giải mã:

Nhận y = 2; giải mã: $x = y^a \bmod n = 2^7 \bmod 15 = 128 \bmod 15 = 8$.



Hình 1 : minh họa hệ mã hóa RSA

1.3 VẤN ĐỀ KÝ SỐ

1.3.1 Khái niệm ký số:

Sơ đồ chữ ký số là phương pháp ký một thông điệp lưu dưới dạng điện tử. Thông điệp được ký và chữ ký có thể được truyền trên mạng. Với chữ ký trên giấy khi ký tên một tài liệu thì chữ ký là bộ phận vật lý của tài liệu được ký. Tuy nhiên chữ ký số không được gắn vật lý với thông điệp được ký.

Đối với chữ ký trên giấy, việc kiểm tra nó bằng cách so sánh nó với chữ ký gốc đã đăng ký. Tất nhiên phương pháp này không an toàn nắm vì có thể bị đánh lừa bởi chữ ký của người khác. Chữ ký số được kiểm tra bằng thuật toán kiểm tra công khai, như vậy người bất kỳ có thể kiểm tra chữ ký số. Việc sử dụng lược đồ an toàn sẽ ngăn chặn khả năng đánh lừa (giả mạo chữ ký).

Sơ đồ chữ ký số là bộ năm (**P,A,K,S,V**) thỏa mãn các điều kiện dưới đây:

- P: tập hữu hạn các thông điệp.
- A: tập hữu hạn các chữ ký.
- K: tập hữu hạn các khóa(không gian khóa).

Với mỗi k thuôc K, tồn tại thuật toán ký $sig_k \in S$ và thuật toán sác minh $verK \in V$

Mỗi sig_k: P→A và ver_k PxA→{true,false} là những hàm sao cho mỗi thông điệp x ∈P và mỗi chữ ký y ∈ A thỏa mãn phương trình dưới đây:

Ver(x,y) → True: nếu y = sig(x)

Ver(x,y) → False: nếu y ≠ sing(x)

1.3.2 Sơ đồ chữ ký RSA

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

Trong đó:

- P = A = Z_n, với n= p*q là tích của hai số nguyên tố lớn p,q Φ(n)=(p-1)*(q-1).
- K: là tập các cặp khóa K = (K^1,K^n), với K^1 = a,K^n = (n,b).

  b: là số nguyên tố cùng Φ(n).

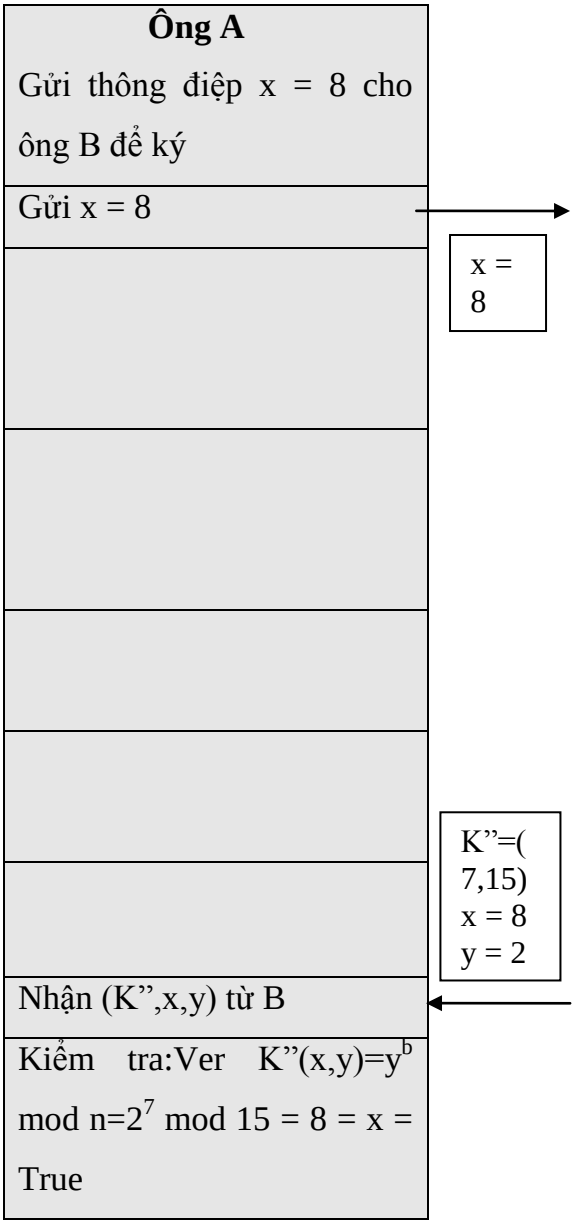
  a: thỏa mãn a.b ≡ 1(mod Φ(n)), (a là phần tử nghịc đảo của b).
- Các hàm $sig_{k'}$ và $ver_{k''}$ được xác định như sau:

  $sig_{k'}(x) = x^a \bmod n$.

  $ver_{k''}(x,y)$ = đúng ⇔ $x \equiv y^b \bmod n$.

Ví dụ:

Giả sử ông B sẽ ký lên thông điệp x = 8 do ông A gửi, thông điệp được ký sẽ gửi lại cho ông A và ông A tiến hành kiểm tra chữ ký.



Ông B
Ký thông điệp x = 8 và gửi lai cho ông A
Nhận x
Lấy hai số nguyên tố lớn p,q (p = 3,q = 5)
Tính n=p*q;Φ(n) = (p-1)*(q-1) (n = 15;Φ(n) = 2*4 = 8)
Chọn b là số nguyên tố cùng nhau với Φ(n) (b = 7)
Tính giá trị $a = b^{-1} \bmod \Phi(n) =$ K' (K' = a = 7)
Ký $sig(x) = x^a \bmod n = y$ $(y = 8^7 \bmod 15 = 2)$
Gửi K" = (b,n),x,y cho A

Hình 2: Minh họa sơ đồ chữ ký RSA

1.3.3 Sơ đồ chữ ký Schnorr

Chuẩn bị:

Lấy G là nhóm con cấp q của Z_n^*, với q là số nguyên tố.

Chọn phần tử sinh g thuộc G sao cho bài toán logrit trên G là khó giải.

Chọn $x \neq 0$ làm khóa bí mật ,$x \in Z_q$.

Tính $y = g^x$ làm khóa công khai.

Lấy H là hàm băm không va chạm.

Ký trên thông điệp m:

Chọn r ngẫu nhiên thuộc Z_q.

Tính c = H(m,g).

Tính s = (r – c x)mod q.

Chữ ký Schnorr là cặp (c,s).

Kiểm tra chữ ký:

Với một văn bản m cho trước,một cặp (c,s) được gọi là một chữ ký Schnorr hợp lệ nếu thỏa mãn phương trình:

$$\mathbf{c = H(m, g^s * y^c)}$$

Để ý rằng ở đây c xuất hiện ở cả 2 vế của phương trình.

1.3.4 Khái niệm chữ ký mù

Chữ ký mù được Chaum giới thiệu vào năm 1983. Mục đích của chữ ký mù là làm sao người ký lên văn bản lại không biết nội dung văn bản. Nghĩa là có được chữ ký trên $x \in P$, mà không cho người ký biết giá trị x.

Để hiểu rõ được ứng dụng của chữ ký mù ,chúng ta sẽ tìm hiểu bài toán trong thực tế: Hệ thống tiền điện tử ẩn danh.

Trong hệ thống tiền điện tử ẩn danh, người mua hàng trước khi giao dịch, họ phải sinh ra đồng tiền điện tử (là dãy số) nhưng vẫn ở dạng "thô", nghĩa là vẫn chưa có giá trị giao dịch. Để đồng tiền này có giá trị giao dịch thực sự, thì cần phải có chữ ký của tổ chức phát hành trên đồng tiền này.

Người mua hàng phải gửi đồng tiền này đến tổ chức phát hành để ký. Nhưng người mua hàng không muốn tổ chức phát hành có thể xác lập được thông tin liên hệ giữa đồng tiền với họ để tránh rắc rối sau này. Để che dấu được thông tin này, người mua hàng "làm mù" đồng tiền, rồi mới gửi cho tổ chức phát hành ký.

Người mua hàng nhận được đồng tiền từ tổ chức phát hành, họ "xóa mù" và thu được đồng tiền có chữ ký. Lúc này đồng tiền mới có giá trị giao dịch thực sự.

Lược đồ chữ ký mù như sau:

- Bước 1: A làm mù x bằng một hàm: z=Blind(x), và gửi z cho B.
- Bước 2: B ký trên z bằng hàm y = Sign(z) = Sign(Blind(x)), và gửi lại y cho A.
- Bước 3: A xóa mù trên y bằng hàm.
  Sign(x) = UnBlind(y) = UnBlind(Sign(Blind(x))).

1.3.5 Chữ ký mù theo sơ đồ chữ ký RSA

Bài toán đặt ra là giả sử A muốn lấy chữ ký của B trên x, nhưng không muốn cho B biết x.Quá trình thực hiện như sau

- Lấy p,q là các số nguyên tố lớn, n = p*q.
- $\Phi(n) = (p-1)*(q-1)$.
- Chọn khóa công khai $b \in Z_n$.
- Chọn khóa bí mật $a \in Z_n$ sao cho $a.b = 1 \bmod \Phi(n)$.
- r là số ngẫu nhiên thuộc Z_n (r được chọn sao cho tồn tại phần tử nghịch đảo $r^{-1}(\text{mod } n)$).

Bước 1: A làm mù x bằng hàm $Blind(x) = x*r^b \bmod n = z$, và gửi z cho B.

Bước 2: B ký trên z bằng hàm $Sign(z) = Sign(Blind(x)) = z^a \bmod n = y$.

Bước 3: A tiến hành xóa mù y bằng thuật toán:

UnBlind(y) = UnBlind(Sign(Blind(x))) = y/r mod n = sign(x).

Ví dụ:

Giả sử ông B ký lên thông điệp đã được làm mù do ông A gửi. Thông điệp ban đầu là x = 8.

Khi ký trên x = 8 thì chữ ký theo sơ đồ RSA(trong ví dụ trước) là:

Sign(x=8) = x^a mod n = 8^7 mod 15 = 2 = y.

Bước 1: làm mù x = 8

Blind(x) = x*r^b (mod n) = 8*11^7(mod 15) = 8*19487171(mod 15) = 155897368 mod 15 = 3 =z

Với r = 11 là số ngẫu nhiên thuộc Z_{15} (thỏa mãn gcd(11,15) = 1).

Bước 2: ký trên z:

Y = Sign(z) = z^a mod n = 13^7(mod 15) = 62748517 mod 15 = 7

Bước 3: xóa mù y = 7:

UnBlind(y) = y/r(mod n) = 7/11(mod 15) = 7*11^{-1}(mod 15) = 7*11(mod 15) = 77(mod 15) = 2.

*(11^{-1} = 11 trong mod 15).

1.4 CHỨNG CHỈ SỐ

Chứng chỉ số là một trong các công cụ để thực hiện an toàn và bảo mật trong hệ thống thông tin

Như đã trình bày, việc dử dụng hệ mã hóa khóa công khai trong bảo mật thông tin là rất quan trọng. Tuy nhiên có vấn đề nảy sinh là nếu hai người không biết nhau, nhưng muốn tiến hành giao dịch thì làm sao họ có thể có khóa công khai của nhau. Giả sử ông A muốn giao tiếp với ông B. Ông ta vào website của ông B để lấy khóa công khai. Ông A gõ địa chit URL của ông B lên trình duyệt tìm DNS của trang web và gửi yêu cầu của ông A. Nhưng không may kẻ giả mạo B' lại nhận yêu cầu củ A và trả về trang web của B' là bản sao của B, hoàn toàn giống trang web của B khiến cho A không thể phát hiện được. Lúc này A có khóa công khai của B'chứ không phải là của B. Ông A mã hóa thông điệp bằng khóa công khai của B'. Kẻ gian B' mã hóa thông điệp, đọc thông tin, mã hóa lại bằng khóa công khai của B và gửi thông điệp cho B. Như vậy cả A và B đều hoàn toàn không biết có kẻ thứ ba là B' đã đọc được nội dung của thông điệp. Trường hợp sấu hơn B' sẽ thay đổi nội dung thông điệp của A trước khi gửi cho B.

Bài toán đặt ra là phải có một kỹ thuật để đảm bảo khóa công khai được trao đổi an toàn không có giả mạo.

Để giải quyết vấn đề này cần có một tổ chức cung cấp chứng nhận, nó xác nhận khóa công khai này thuộc về một người, công ty hay tổ chức nào đó. Tổ chức cung cấp các chứng nhận khóa công khai được gọi là **CA** (Certificate Authority), và chứng nhận này gọi là **chứng chỉ số.**

Với bài toán trên.Ông B muốn cho phép ông A và những người khác giao dịch với mình, Ông ta phải đến một tổ chức **CA** để xin giấy chứng nhận khóa công khai của ông ta. Nhà cung cấp sẽ phat hành chứng nhận và chữ ký số của nhà cung cấp. Nhiệm vụ chính của nhà cung cấp **CA** là gắn kết khóa công khai với tên của người đăng ký (cá nhân, công ty hay tổ chức) sở hữu khóa đó.

Chứng chỉ số là tệp tin điện tử, dùng để xác minh danh tính một cá nhân một công ty….cùng với khóa công khai của họ trên internet. Nó giống như bằng lái xe, hộ chiếu, chứng minh thư hay những giấy tờ xác minh cá nhân. Để có chứng minh thư ta phải được cơ quan Công an sở tại cấp. Chứng chỉ số cũng vậy, phải do một tổ chức đứng da chứng nhận những thông tin của ta là chính xác được gọi là Nhà cung cấp chứng chỉ 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 họ cấp.

Trong chứng chỉ số có ba thành phần chính:

- Thông tin cá nhân

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

- Khóa công khai:

Trong mật mã khóa công khai là một giá trị được CA chứng thực, đó là khóa mã hóa, kết hợp với khóa bí mật duy nhất được tạo ra từ khóa công khai, để tạo thành cặp khóa mật mã đối xứng.

- Chữ ký số của CA cấp chứng chỉ:

Đây chính là sự xác nhận của CA, đảm bảo 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.

Trong cơ sở hạ tầng mật mã khóa công khai (Public key infrastructure), CA sẽ kiểm soát cùng với nhà quản lý đăng ký (Registration authority-RA) để xác minh thông tin về chứng chỉ số mà người ta yêu cầu xác thực. RA xác nhận thông tin của người cần xác thực, CA sau đó sẽ cấp chứng chỉ.

1.5 VẤN ĐỀ XƯNG DANH

Trong thực tế cuộc sống việc xưng danh thường gặp trong mọi hoạt động thông tin, đặc biệt những ứng dung trên mạng, chẳng hạn trong những tình huống sau:

- Để rút tền trên máy rút tiền tự động (ATM), người sử dụng xưng danh bằng cách dùng thẻ rút tiền cùng với số PIN.
- Để truy nhập vào một máy tính trên mạng, người sử dụng cần phải khai báo tên truy cập và mật khẩu.

Việc xung danh theo thông thường là không an toàn, chẳng hạn như ví dụ trên, không có gì đảm bảo là số PIN và mật khẩu được gữi kín, người ngoài không biết được. Tuy nhiên với sự phát triển của những ứng dụng, nhu cầu đặt ra là việc xưng danh phải đảm bảo an toàn hơn.

Mục tiêu an toàn của việc xưng danh là đảm bảo khi "nghe" chủ thể A xưng danh với chủ thể B, bất kỳ một ai khác A cũng không thể mạo nhận mình là A, chính B cũng không thể mạo xưng mình là A, sau khi được A xưng danh với mình.

Nói cách khác, A muốn chứng minh để đối tác xác nhận danh tính của mình, mà không tiết lộ bất cứ thông tin nào về danh tính đó.

Việc xưng danh thường phải thông qua một giao thức hỏi-đáp(request-response). Qua giao thức đó B có thể xác nhận danh tính của A. Đầu tiên B đặt cho A một câu hỏi, A phải trả lời. Trong câu trả lời, A phải chứng tỏ cho B biết rằng A sở hữu một bí mật riêng. Điều đó thuyết phục B tin rằng người trả lời đúng là A, và do đó xác nhận danh tính A.

Vấn đề khó ở đây là A phải làm cho B biết là có sở hữu một bí mật riêng A, nhưng lại không tiết lộ cho B biết điều bí mật này.

CHƯƠNG 2: THANH TOÁN TRONG THƯƠNG MẠI ĐIỆN TỬ

2.1 TỔNG QUAN VỀ THƯƠNG MẠI ĐIỆN TỬ

2.1.1 Khái niệm thương mại điện tử

Hiên nay có nhiều quan niệm khác nhau về "thương mại điện tử" (TMDT), nhưng nhìn chung có hai quan niệm chính trên thế giới được nêu ra dưới đây.

Thương mại điện tử theo nghĩa rộng được định nghĩa trong Luật mẫu về thương mại điện tử của Ủy ban Liên Hợp Quốc về Luật Thương mại Quốc Tế (ULCITRAL): Thuật ngữ Thương mại cần được diễn giải theo nghĩa rộng để bao quát các vấn đề phát sinh từ mọi quan hệ mang tính chất thương mại dù có hay không có hợp đồng. Các quan hệ mang tính thương mại bao gồm các giao dịch sau đây: Bất cứ giao dịch nào về thương mại nào về cung cấp hoặc trao đổi hàng hóa hoặc dịch vụ; thỏa thuận phân phối; đại diện hoặc đại lý thương mại; ủy thác hoa hồng;cho thuê dài hạn; xây dựng các công trinh; tư vấn; kỹ thuật công trình; đầu tư; cấp vốn; ngân hàng; bảo hiểm; liên doanh các hình thức khác về hợp tác công nghiệp hoặc kinh doanh; chuyên chở hàng hóa hay hành khách bằng đường biển, đường không, đường săt hoặc đường bộ. Như vậy thấy rằng phạn vi hoạt động của thương mại điện tử rất rộng, bao quát hầu hết các lĩnh vực hoạt đông kinh tế, việc mua bán hàng hóa và dịch vụ chỉ là một trong hàng ngàn lĩnh vực áp dụng của Thương mại điện tử.

Uỷ ban Châu Âu đưa ra nghị định về Thương mại điện tử như sau: Thương mại điện tử được hiểu là việc thực hiện hoạt động kinh doanh qua các phương tiện điện tử. Nó dựa trên việc xử lý và truyền dữ liệu điện tử dưới dạng text ,âm thanh và hình ảnh. Thương mại điện tử gồm nhiều hành vi trong đó hoạt động mua bán hàng hóa và dịch vụ qua phương tiện điện tử,giao nhận các nội dung kỹ thuật số trên mạng,chuyển tiền điện tử, mua bán cổ phiếu điện tử, vận đơn điện tử, đấu giá thương mại, hợp tác quốc tế , tài nguyên mạng, mua sắm công cộng,tiếp thị trực tiếp với người tiêu dùng, và các dịch vụ sau bán hàng.

Thương mại điện tử được thực hiện đối với cả thương mại hàng hóa(ví dụ như hàng tiêu dùng,các thiết bị y tế chuyên dụng) và thương mại dịch vụ (ví dụ như dịch vụ cung cấp thông tin,dịch vụ pháp lý, tài chính); các hoạt động truyền thống (như chăm sóc sức khỏe,giáo dục) và các hoạt động mới (như siêu thị ảo).

Tóm lại theo nghĩa rộng thì thương mại điện tử có thể được hiểu là các dịch vụ tài chính và thương mại bằng phương pháp điện tử như: trao đổi dữ liệu điện tử, chuyển tiền điện tử và các hoạt động gửi, rút tiền bằng thẻ tín dụng.

Thương mại điện tử theo nghĩa hẹp bao gồm các hoạt động thương mại được thược hiện thông qua mạng internet. Các tổ chức như: Tổ chức thương mại thế giới WTO, tổ chức hợp tác phát triển kinh tế đưa ra các khái niệm về thương mại điện tử theo hướng này. Thương mại điện tử được nói đến ở đây là hình thức mua bán hàng hóa được bày tại các trang Web trên innternet với phương thức thanh toán bằng thẻ tín dụng. Có thể nói Thương mại điện tử đã trở thành một cuộc cách mạng làm thay đổi cách thức mua sắm của con người.

Theo tổ chức thương mại thế giới: Thương mại điện tử bao gồm việc sản xuất, quảng cáo, bán hàng và phân phối sản phẩm được mua bán và thanh toán trên mạng internet, nhưng được giao nhận một cách hữu hình cả các sản phẩm được giao nhận cũng như thông tin số hóa thông qua mạng internet.

Với quan niệm trên theo nghĩa hẹp. Thương mại điện tử chỉ bao gồm các hoạt động thương mại được thực hiện thông qua mạng internet mà không tính đến các phương tiện điện tử khác như điện thoại, fax…vv

Theo nghĩa rộng thì hoạt động thương mại điện tử được thực hiện thông qua các phương tiện thông tin liên lạc đã tồn tại hàng chục năm nay và đạt tới doanh số hàng tỷ đô mỗi ngày. Theo nghĩa hẹp thì thương mại điện tử mới chỉ tồn tại được vài năm nay, nhưng đã đạt được những kết quả rất đáng quan tâm. Trên thực tế chính các hoạt đông thương mại thông qua internet đã làm phát sinh thuật ngữ Thương mại điện tử.

2.1.2 Các đặc trưng của thương mại điện tử

So với các hoạt động thương mại truyền thống, thương mại điện tử có một số điểm khác biệt sau:

- Các bên tiến hành giao dịch trong thương mại điện tử không tiếp xúc trực tiếp với nhau và không đòi hỏi phải biết nhau từ trước.
- Các giao dịch thương mại truyền thống được thực hiện với sự tồn tại của khái niệm biên giới quốc gia, còn thương mại điện tử được thực hiên trên thị trường không có biên giới (thị trường thống nhất toàn cầu). Thương mại điện tử tác động trực tiếp đến môi trường cạnh tranh toàn cầu.
- Trong hoạt động giao dịch thương mại điện tử đều có sự tham gia của ít nhất ba chủ thể, một bên không thể thiếu được là người cung cấp dịch vụ mạng và các cơ quan chứng thực.
- Đối với thương mại truyền thống thì mạng lưới thông tin chỉ là phương tiện để trao đổi dữ liệu. Đối với thương mại điện tử thì mạng lưới thông tin chính là thị trường.

2.1.3 Các mô hình thương mại điện tử

Dựa trên việc phân loại các đối tượng tương tác mua và bán, người ta phân chia các mô hình giao dich trong TMDT theo các khái niệm B2B, B2C, P2P….

Mô hình B2C (Business-To-Customer: nhà cung cấp tới khách hàng**):**

B2C là hình thức giao dịch giữa một doanh nghiệp và người tiêu dùng tại các của hàng trên internet thường là các Website trên internet, bao gồm việc hỗ trợ khách hàng trực tuyến và bán lẻ hàng trực tuyến. Hoạt động bán lẻ hàng hóa trực tuyến thường không đòi hỏi hóa đơn chứng từ. Mô hình này còn gọi là mô hình buôn bán điện tử(E-Business).

Mô hình B2B(Business-To-Business: nhà cung cấp tới nhà cũng cấp):

B2B loại hình cho phép thực hiện giao dịch giữa các doanh nghiệp với nhau hay giữa các chi nhánh với tổng công ty, và khách hàng-người dùng

cuối(end user) của doang nghiệp đó. Các hoạt động có thể gồm đàm phán ký kết hợp đồng, đặt hàng qua hệ thống catalog trực tuyến, quản lý điều phối hàng hóa giữa các chi nhánh, tìm kiếm đối tác đấu giá gọi thầu và bao gồm cả việc bán lẻ hàng hóa trực tuyến. Giao dich B2C không cần hóa đơn chứng từ, giao dịch B2B phải có hóa đơn chứng từ đầy đủ giá trị pháp lý. Mô hình này còn gọi là mô hình thương mại điện tử.

Mô hình P2P (Peer-To-Peer: người tiêu dùng tới người tiêu dùng**):**

P2P là việc kinh doanh thương mại điện tử giữa người tiêu dùng và người tiêu dùng (hai nhóm đối tượng trong đó người bán và người mua đều là cá nhân). Ví dụ Website giao vặt, Website đấu giá trực tuyến www.ebay.com (cho phép khách hàng bán đấu giá các mặt hàng của họ cho khách hàng khác) là lơi mà người mua và người bán đều là cá nhân.

2.2 CÁC PHƯƠNG THỨC THANH TOÁN

2.2.1 Khái niệm thanh toán điện tử

Khâu quan trọng nhất của thương mại điện tử là việc thanh toán, bởi vì mục tiêu cuối cùng của cuộc chao đổi thương mại là người mua nhận được những cái gì cần mua và người bán nhận được số tiền thanh toán. Thanh toán là một trong những vấn đề phức tạp nhất đối với các hoạt đông thương mại điện tử. Hoạt đông thương mại điện tử chỉ phát huy được tính ưu việt của nó khi giao dịch thương mại điện tử được thực hiện với đúng nghĩa của nó, tức là áp dụng được hình thức thanh toán điện tử(TTĐT).

Thanh toán điện tử là việc thanh toán tiền qua các thông điệp điện tử thay cho việc thanh toán bằng tiền mặt. Về mục đich TMĐT là hệ thống cho phép các bên tham gia có thể tiến hành mua bán được. Tuy nhiên cách giao dịch thì hoàn toàn mới, Người thực hiện giao dịch xử lý thanh toán bằng phương pháp thông qua các khâu được thực hiện trên máy tính. Bản chất của mô hình TMĐT cũng là mô phỏng lại những mô hình mua bán truyền thống nhưng từ các thủ tục giao dịch, các thao tác xủ lý dữ liệu, quá trình chuyển tiền …tất cả đều được thực hiện thông qua hệ thống máy tính, được nối bằng các giao thức riêng chuyên dụng.

Với TMĐT các bên mua-bán có thể giao dịch với nhau, không phải gặp nhau không phải dùng tiền mặt. Các bên trong hệ thống TMĐT sẽ chao đổi với nhau các chứng từ số hóa. Bên được thanh toán có thể thông qua ngân hàng của mình để chuyển tiền vào tài khoản của mình. Các quá trình này được phản ánh qua các giao thức thanh toán của hệ thống, đó là thứ tự các bước gửi thông tin và xử lý số liệu giữ các bên, mục đich là chuyển đầy đủ các chứng từ thanh toán đảm bảo an toàn và công bằng cho mọi bên theo yêu cầu tường minh ban đầu.

2.2.2 Các mô hình thanh toán

Hệ thống thanh toán điện tử thực hiện thanh toán cho khách hàng theo một số cách, mà tiền mặt và sec thông thường không thể làm được. Hệ thống thanh toán cũng cung cấp khả năng điều khiển thanh toán hàng hóa dịch vụ qua

thời gian bằng cách cho phép Người mua trả tiền ngay, trả tiền sau hay trả tiền trước. Thẻ tín dụng cung cấp khả năng thanh toán bằng tiền mặt qua tính sẵn sàng cho phép hoãn việc trả tiền hàng hóa và dịch vụ đã được phê chuẩn trước.

Có nhiều tiêu chí để phân biệt phương thức thanh toán điện tủ, một trong những phương thức đó là sự chênh lệch khác biệt giữ thời điểm bên trả tiền trao chứng từ ủy nhiệm cho bên được trả và thời điểm trả tiền thực sự xuất tiền khỏi tài khoản của Người mua. Với tiêu chí này, phương thức thanh toán điện tử có thể phân thành hai mô hình chính: mô hình trả sau và mô hình trả trước. Trong mô hình trả sau thời điểm bên trả tiền trao chứng từ ủy thác cho bên được trả, xảy ra trước thời điểm trả tiền thực sự (xuất tiền khỏi tài khoàn của người mua để trả cho người bán). Trong mô hình trả trước hai thời điểm này diễn ra theo thứ tự ngược lại, người mua phải trả tiền thực sự trước khi chứng từ ủy nhiệm được sử dụng trong các giao dịch mua bán.

Mô hình trả trước

Trong mô hình trả trước khách hàng liên hệ với ngân hàng (hay công ty môi giới-broker) để có được chứng từ do ngân hàng phát hành (chứng từ hay đồng tiền số này mang dấu ấn của ngân hàng), được đảm bảo bởi ngân hàng và do đó có thể dùng ở bất cứ nơi nào đã được xác lập hệ thống thanh toán với ngân hàng này.

Để đổi lấy chứng từ của ngân hàng, tài khoản của khách hàng sẽ bị chiết khấu đi tương ứng với giá trị của chứng từ đó. Như vậy, khách hàng đã thực sự trả tiền trước khi có thể sử dụng chứng từ này để mua hàng và thanh toán.

Chứng từ ở đây không phải do khách hàng tạo ra, không phải dùng cho một cuộc mua bán cụ thể mà do ngân hàng phát hành và có thể sử dụng vào mọi mục đích thanh toán. Vì nó có thể sử dụng giống như tiền mặt và do đó mô hình còn được gọi là **mô hình mô phỏng tiền mặt (**cash-like moden**)**

Khi có người mua hàng tại một của hàng nào đó và thanh toán bằng chứng từ này, cửa hàng sẽ tiến hành kiểm tra tính hợp lệ của chúng dựa trên những thông tin đặc biệt do ngân hàng tạo ra trên đó. Sau đó cửa hàng có thể

chọn một trong hai cách: thứ nhất là liên hệ với ngân hàng để chuyển vào tài khoản của mình ngay trước khi chấp nhận giao hàng (deposit-now), thứ hai là chấp nhận và liên hệ chuyển tiền sau vào thời gian thích hợp (deposit-later)

Trường hợp riêng phổ biến của mô hình mô phỏng tiền mặt là mô hình tiền điện tử (electronic cash).

Mô hình trả sau

Với mô hình trả sau, thời điểm tiền mặt được rút ra khỏi tài khoản bên mua để chuyển sang bên bán xảy ra ngay (pay-now) hoặc sau (pay-later) giao dịch mua bán. Hoạt động của hệ thống trên dựa trên nguyên tắc tín dụng (Credit Crendental) nào đó có tác dụng giống như sec (cheque). Bên bán có hai cách lựa chọn: hoặc là chấp nhận giá trị thay thế của tín dụng đó vì chỉ liên lạc chuyển khoản với ngân hàng của mình sau này,hoặc liên lạc với ngân hàng của mình khi quá trình mua bán đang diễn ra việc chuyển khoản xảy ra ngay trong quá trình giao dịch.

Với pha chuyển khoản (chearing process) người được thanh toán sẽ yêu cầu chuyển khoản với ngân hàng đại diện của mình để thực hiện liên lạc vơi ngân hàng đại diện của người thanh toán, thực hiện kiểm tra chấp nhận chứng từ tín dụng, khi đo việc chuyển tiền thực sự sẽ được diễn ra giữa tài khoản của người thanh toán và người được thanh toán.

Kết thúc quá trình này, ngân hàng đại diện của bên thanh toán sẽ gửi một thông báo lưu ý sụ chuyển khoản đó cho khách hàng của mình (notification). Mô hình thanh toán này tương tự như phương thức thanh toán bằng sec lên thường được gọi là **mô hình mô phỏng sec**(cheque-like model).

Pha chuyển tiền thực sự này nếu được làm ngay trong giao dịch thì an toàn nhất. nhưng như vậy thì tốc độ xử lý giao dịch sẽ chậm, chi phí truyền tin và xử lý dữ liệu trực tuyến trên các máy chủ ở các nhà băng sẽ cao. Vì vậy, mô hình pay-later cần được ưu tiên sử dụng khi số tiền thanh toán là không lớn.

CHƯƠNG 3 : THANH TOÁN BẰNG TIỀN ĐIỆN TỬ

3.1 GIỚI THIỆU TIỀN ĐIỆN TỬ

3.1.1 Khái niệm tiền điện tử

Tiền điện tử (digital money, electronic money, internet money, e-money,…vv)là những thuật từ vẫn còn mơ hồ và chưa định nghĩa đầy đủ. Tuy nhiên có thể hiểu tiền điện tử là loại tiền chao đổi theo phương pháp "điện tử" liên quan đến mạng máy tính và những hệ thống chứa giá trị ở dạng số (digital stored value systems).

Hệ thống tiền điện tử cho phép người dùng có thể thanh toán khi mua hàng, hoặc sử dụng các dịch vụ nhờ truyền đi các "dãy số" từ máy tính(hay thiết bị lưu trữ như smast card). Gống như dãy số(serial) trên tiền giấy, dãy số của tiền điện tử là duy nhất. Mỗi "đồng" tiền điện tử được phát hành bởi một tổ chức "ngân hàng" và biểu diễn một lượng tiền thật nào đó.

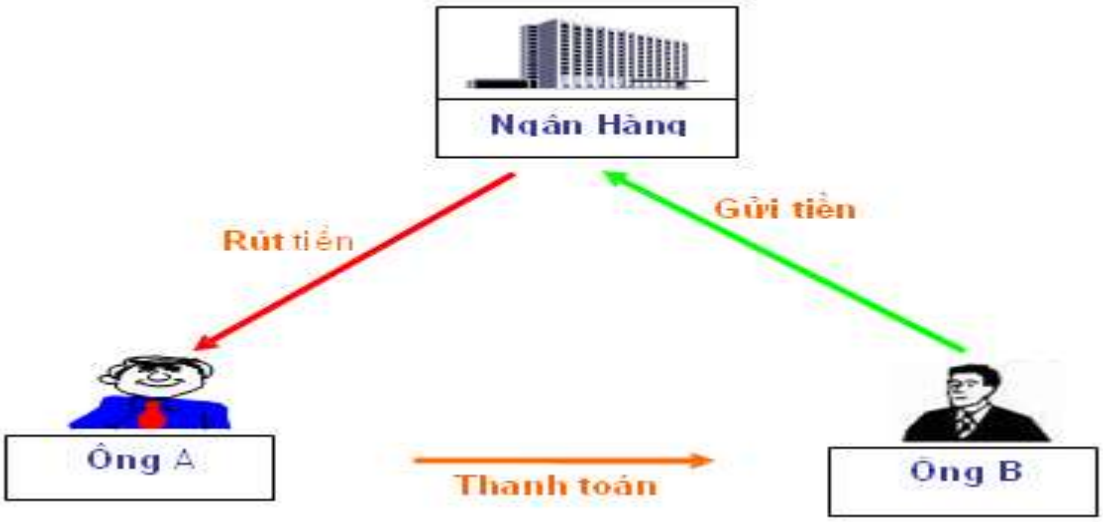
Tiền điện tử có loại **ẩn danh** và **định danh**. Hệ thống tiền ẩn danh không tiết lộ thông tin định danh của người sử dụng, và hệ thống này dựa vào sơ đồ chữ ký "mù". Hệ thống tiền định danh tiết lộ thông tin định danh của người sử dụng, hệ thống dựa vào sơ đồ chữ ký thông thường.

Tính ẩn danh của tiền điện tử tương tự như tiền mặt thông thường, hệ thống tiền định danh tương tự như hệ thống thẻ tín dụng.

Có nhiều cách tiếp cận tính ẩn danh khác nhau, có hệ thống tiền điện tử là ẩn danh đối với người bán, nhưng không ẩn danh với ngân hàng. Có hệ thống ẩn danh hoàn toàn, nghĩa là ẩn danh với tất cả mọi người.

3.1.2 Lược đồ giao dịch

Lược đồ giao dịch của hệ thống tiền điện tử cơ bản có 3 giao dịch chính sau:



Hình 3: Mô hình giao dịch cơ bản của hệ thống tiền điện tử

- Rút tiền: A chuyển tiền của ông ta từ tài khoản ở ngân hàng vào túi của mình (nó có thể là Smart card hay là máy pc).
- Thanh toán: A chuyển tiền từ túi của ông ta tới ông B.
- Gửi tiền: B chuyển tiền nhận được vào tài khoản của ông ta ở ngân hàng.

Lược đồ trên có ba đối tượng tham gia vào quá trình giao dịch đó là:

- Tổ chức tài chính.
- A: Người trả tiền (Người mua hàng).
- B: Người được trả tiền (Người bán hàng).

Trong lược đồ giao dịch này có thể thực hiện hai kiểu giao dịch: Trực tuyến (online) và ngoại tuyến (offline).

Trực tuyến: Ông B liên lạc với ngân hàng và kiểm tra tính hợp lệ của đồng tiền trươc khi tiến hành thủ tục thanh toán và phân phối. Quá trình thanh toán và trả tiền (ghi tiền vào tài khoản người bán) được tiến hành đồng thời.

Ngoại tuyến: Quá trình giao dịch với ngân hàng và việc kiểm tra tính hợp lệ của đồng tiền được tiến hành sau quá trình thanh toán.

3.1.3 Phân loại

Hiện nay tiền điệ tử có thể chia thành hai loại: **Tiền điện tử định danh (**identified e-money**)** và **Tiền điện tử ẩn danh(**anonymous identified e-money**).**

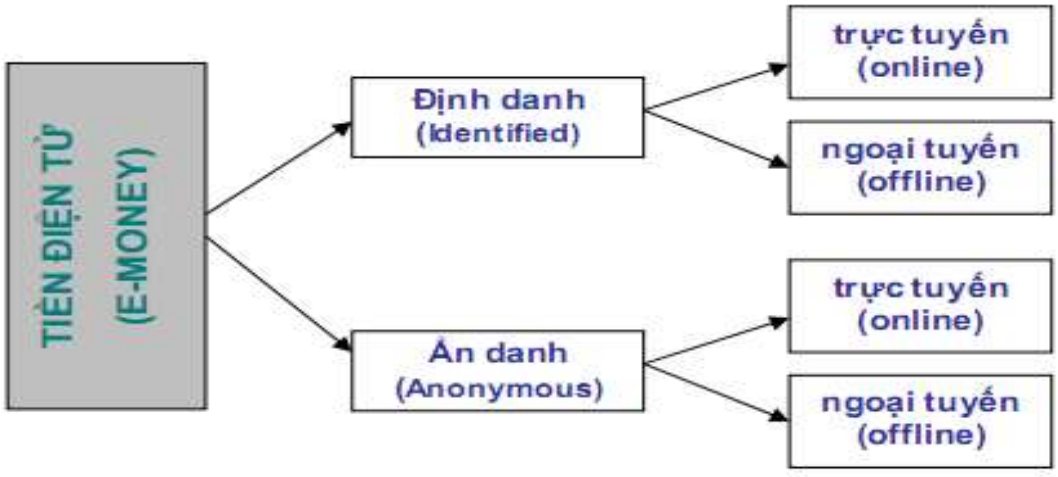
Tiền điện tử định danh chứa thông tin định danh của người sử dụng từ khi bắt đầu rút tiền từ ngận hàng. Kiểu lưu thông tin người dùng giống như trường hợp sử dụng thẻ tín dụng trong thanh toán, tiền điện tử định danh cũng cho phép ngân hàng lưu dấu vết của tiền khi luân chuyển.

Tiền điện tử ẩn danh giống như tiền giấy thực sự. Đồng tiền điện tử ẩn danh được rút từ một tài khoản, có thể được tiêu xài và chuyển cho người khác mà không để lại dấu vết.

Trong hai loại tiền điện tử trên, dựa vào phương pháp thực hiện, có thể chia mỗi loại trên thành hai dạng **trực tuyến** và **ngoại tuyến.**

Trực tuyến: Nghĩa là phải tương tác với phía thứ ba để kiểm tra giao dịch.

Ngoại tuyến: Nghĩa là có thể kiểm soát được giao dịch, mà không phải liên quan trực tiếp đến phía thứ ban (ngân hàng)



Hình 4: Phân loại tiền điện tử

Hiện nay có nhiều hệ thống tiền điện tử khác nhau sử dụng giải pháp là smart card. Trong khóa luận sẽ trình bày những hệ thống tiền điện tử sử dụng

nhiều thành tựu của lý thuyết mật mã để giải quyết khó khăn, mà những giải pháp khác không đáp ứng được.

3.1.4 Những đặc điểm của tiền điện tử

Có nhiều cách để đưa ra các đặc điểm cần thiết của một hệ thống tiền điện tử, tuy nhiên không thể đưa ra tập các đặc điểm, thuộc tính chung tốt nhất cho tất cả các hệ thống tiền điện tử. Bởi vì mỗi hệ thống tồn tại trên môi trường khác nhau, phục vụ cho những đối tượng khác nhau, thậm chí ngay cả sản phẩm của hệ thống là khác nhau (phần mềm hay smartcard).

Hiện nay tồn tại nhiều hệ thống tiền điện tử khác nhau. Tuy nhiên chúng có chung các đặc điểm sau:

1 : Tính an toàn

Tiền điện tử phải không bị được sao chép (sử dụng lại) hay giả mạo. Chính vì vậy khi phát triển hệ thống tiền điện tử, phải quan tâm đến vấn đề giảm thiểu rủi ro về sự giả mạo và xây dựng một hệ thống xác thực tốt. Tính an toàn không chỉ ở phần mềm của hệ thống, mà còn thể hiện ở quá trình giao dịch của người tham gia hệ thống.

2: Tính riêng tư

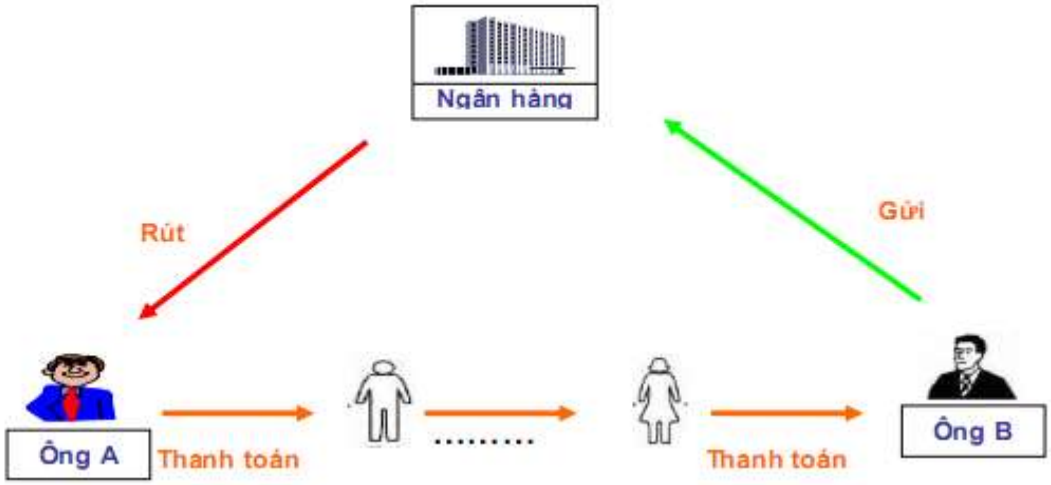
Quá trình thanh toán của người trả tiền phải được ẩn danh, không để lại dấu vết, nghĩa là ngân hàng không nói được tiền giao dịch là của ai.

3: Tính độc lập

Việc sử dụng tiền điện tử không phụ thuộc vào bất kỳ vị trí địa lý nào. Tiền có thể được chuyển qua mạng máy tính hay chứa trên những thiết bị nhớ khác nhau.

4: Tính chuyển nhượng

Cho phép hai bên có thể chuyển tiền cho nhau mà không phải liên hệ với bên thứ ba (ngân hàng). Tính chuyển nhượng là đặc trưng của tiền mặt, nó cho phép người sở hữu tiền chuyển cho Người khác, mà không cần liên hệ với ngân hàng.



Hình 5 : Mô hình giao dịch có tính chuyển nhượng

Chú ý: Với hệ thống hỗ trợ tính năng chuyển nhượng, một số vấn đề sẽ nảy sinh:

- kích cỡ dữ liệu sẽ tăng lên ở mỗi lần chuyển nhượng, vì thông tin mỗi lần chuyển nhượng phải được lưu trữ, thông tin này nhằm giúp cho ngân hàng có thể tìm ra được kẻ gian lận nào tiêu xài hai lần. Chính vì thế hệ thống phải giới hạn số lượng tối đa những chuyển nhượng được phép trong hệ thống.
- Vấn đề rửa tiền và trốn thuế là khó phát hiện.
- Việc phát hiện việc giả mạo và tiêu xài vài lần là quá trễ, bởi vì tiền đã được chuyển qua nhiều người.

5: Tính phân chia

Người dùng có thể phân chia đồng tiền số của mình thành những đồng tiền có giá trị nhỏ hơn, với điều kiện tổng giá trị của các đồng tiền này bằng giá trị của đồng tiền điện tử ban đầu.

Không phải hệ thống nào cũng đáp ứng được tính chất này, vì tiền điện tử thực chất là dãy số đã được mã hóa, việc chia dãy số này như thế nào để được những đồng tiền có giá trị nhỏ hơn không phải là vấn đề đơn giản.

6: Tính dễ sử dụng

Tính dễ sử dụng của đồng tiền với người dùng là đặc tính rất quan trọng. Bởi vì tiền điện tử là một giải pháp mang tính phổ biến, nhắm đến nhiều đối tượng sử dụng.

7: Hình thức thanh toán

Trực tuyến: Ông B sẽ yêu cầu ngân hàng kiểm tra tính hợp lệ (tiền này trước đây đã tiêu xài chưa) của đồng tiền mà ông A chuyển, trước khi chấp nhận việc thanh toán (cách này giống việc sử dụng thẻ tín dụng). Thanh toán trực tuyến cần thiết cho giao dịch có giá trị lớn. Hệ thống yêu cầu phải liên lạc với ngân hàng trong suốt mỗi lần giao dịch, chính vì thế sẽ tốn chi phí nhiều hơn(tiền và thời gian).

Hệ thống trực tuyến phải có khả năng kiểm tra sự đáng tin của người trả tiền. Nó hầu như là không thể bảo vệ tính ẩn danh của người sử dụng, bên canh đó hệ thống yêu cầu phải liên lạc với phía thứ ba trong mỗi lần giao dịch, chính vì điều này mà hệ thống trực tuyến không cho phép chuyển nhượng.

Ngoại tuyến: Ông B kiểm tra tiền của ông A, sau khi những giao dịch thanh toán đã hoàn thành. Điều này có nghĩa ông A có thể tự do chuyển tiền cho ông B bất cứ lúc nào mà không liên quan đến phía thứ ba (chẳng hạn như ngân hàng). Hệ thống ngoại tuyến có vẻ hoạt động thuận lợi hơn, tuy nhiên dễ gặp vấn đề "tiêu xài nhiều lần", do đó nó phù hợp cho những giao dịch có giá trị thấp.

3.2 MỘT SỐ VẤN ĐỀ VỀ TIỀN ĐIỆN TỬ

Hai vấn đề lớn nhất hiện nay đặt ra đối với tiền điện tử bao gồm: vấn đề **ẩn danh** người sử dụng và vấn đề ngăn chặn người sử dụng tiêu một đồng tiền điện tử **nhiều lần**.

Tùy theo từng loại tiền điện tử, sẽ có những phương pháp khác nhau để giải quyết vấn đề này.

3.2.1 Vấn đề ẩn danh

Tính ẩn danh là một đặc tính rất quan trọng của phương thức thanh toán bằng tiền điện tử, đây là ưu điểm của phương thức này so với những phương thức khác.

Trong hệ thống tiền điện tử, để giải quyết vấn đề này người ta đã dùng kỹ thuật "chữ ký số mù".Chữ ký số mù là một dạng đặc biệt của chữ ký điện tử, nó đòi hỏi người ký thực hiện ký vào một thông điệp mà không biết nội dung của nó. Thêm vào đó người ký sau này có thể nhìn thấy cặp chữ ký/thông điệp nhưng không thể biết được là mình đã ký khi nào và ở đâu. Nó giống như ký khi đang nhắm mắt.

Chữ ký mù đảm bảo ngân hàng không có được bất kỳ mối liên hệ nào giữa đồng tiền điện tử và chủ sở hữu của nó.

Tuy nhiên giải pháp sử dụng chữ ký mù làm nảy sinh một số vấn đề .Khi ông A cố tình gian lận, gửi tới ngân hàng đồng tiền điện tử có giá trị 50 $ để ký nhưng báo với ngân hàng là 1 $. Vì ngân hàng ký mù lên đồng tiền, nên rõ ràng là không biết được nội dung của nó. Để giải quyết vấn đề gian lận này có hai phương pháp được đặt gia:

1.Cách rõ ràng nhất là ngân hàng sử dụng một **khóa công khai** khác nhau cho mỗi loại tiền. Nghĩa là nếu có k đồng tiền khác nhau thì ngân hàng phải công khai k khóa công khai.

Giả sử tiền có giá trị **1 $** thì ngân hàng sử dụng khóa $\mathbf{k_1}$ và **50 $** thì sử dụng khóa $\mathbf{k_{50}}$. Như vậy trường hợp gian lận của ông A sẽ tạo ra đồng tiền có giá trị **50 $** với k_1, đây là đồng tiền không hợp lệ.

2. Phương pháp thứ hai là dùng giao thức "**cắt và chọn**" (Cut And Choose). Ý tưởng của giao thức này là: để có một đồng tiền có giá trị thì ông A phải tạo k đồng tiền ký hiệu là $\mathbf{C_1,C_2,….,C_k}$. Mỗi đồng tiền đều được gắn định danh, sự khác nhau duy nhất giữa chúng là số sê-ri.

Ông A làm mù những đồng tiền này và gửi chúng đến ngân hàng. Ngân hàng yêu cầu ông A cung cấp những thông tin tương ứng để có thể khử mù **k-1** đồng tiền bất kỳ. Ngân hàng khử mù và kiểm tra chúng. Nếu tất cả hợp lệ ngân hàng ký mù lên đồng tiền còn lại $\mathbf{C_i}$ (là đồng tiền ngân hàng không khử mù) và gửi lại cho ông A.

Ngân hàng có sự đảm bảo cao rằng đồng tiền còn lại cũng là hợp lệ, vì nếu ông A gửi kèm đồng tiền không hợp pháp trong số k đồng tiền, thì xác suất bị phát hiện ít nhất là k-1/k. Xác suất phát hiện càng lớn khi k càng lớn. Tuy nhiên k càng lớn thì hệ thống phải trao đổi nhiều dữ liệu.

3.2.2 Vấn đề tiêu xài hai lần

Với tính chất dạng số hóa, nên với tiền điện tử dễ dàng tạo bản sao từ bản gốc. Chúng ta không thể phân biệt được đây là bản sao của một bản gốc nào đấy, chính vì thế việc giả mạo là không thể phát hiện được. Một hệ thống tiền điện tử tầm thường sẽ cho phép tạo bản sao của tiền điện tử và kẻ gian có thể tiêu xài bản sao này bình thường mà không bị phát hiện. Hệ thống tiền điện tử khi được áp dụng vào thực tế thì thực sự phải có khả năng ngăn ngừa hay phát hiện được trường hợp tiêu xài hai lần. Để giải quyết vấn đề này, tùy theo từng loại hệ thống tiền điện tử mà có giải pháp khác nhau.

1. Đối vớ hệ thống **tiền điện tử trực tuyến**: Hệ thống yêu cầu người bán hàng liên lạc với ngân hàng mỗi lần bán hàng. Ngân hàng lưu giữ tất cả các thông tin của những đồng tiền đã tiêu xài trước đấy và dễ dàng cho người bán hàng biết được đồng tiền nào còn khả năng tiêu xài được. Nếu ngân hàng báo đồng tiền nào đó đã được tiêu xài rồi, thì người bán hàng lập tức từ chối bán hàng. Điều này giống như những nhà bán hàng hiện tại kiểm tra thẻ tín dụng tại những điểm bán hàng.

2. Đối với hệ thống **tiền điện tử ngoại tuyến**: Việc phát hiện đồng tiền tiêu xài hai lần theo hai cách khác nhau.

- Cách thứ nhất là tạo **thẻ thông minh đặc biệt** (special smart card) chứa con chíp chống trộm cắp. Trong những hệ thống khác, chíp này còn được gọi là người theo dõi. Chíp theo dõi sẽ lưu một lượng nhỏ dữ liệu của tất cả những tiền điện tử đã được tiêu xài qua smart card. Nếu người sở hữu smart card đó cố gắng sao chép tiền điện tử này và tiêu xài lần hai thì chíp thep dõi sẽ phát hiện được hành động này, và không cho phép giao dịch tiêu xài. Người sở hữu smart card này không thể xóa được dữ liệu trừ khi họ phá hủy smart card.

- cách thứ hai là dựa vào **cấu trức** của tiền điện tử và **những giao thức mật mã**

để có thể truy vết tìm ra kẻ gian lận (tiêu xài hai lần). Nếu như người tiêu xài biết họ sẽ bị bắt khi cố tình gian lận, về lý thuyết thì tỷ lệ hành động gian lận sẽ được giảm đi. Điều thuận lợi của phương pháp là chúng không đòi hỏi những con chíp đặc biệt. Hệ thống có thể được phát triển trên chương trình phần mềm và có thể chạy trên máy tính cá nhân thông thường hay smart card.

3. **Tiền điện tử định danh-ngoại tuyến**: Dựa vào thông tin định danh để truy vết tìm ra kẻ gian lận. Trong quá trình giao dịch ,định danh của người sử dụng được tích lũy đầy đủ trên đường đi của đồng tiền và thông tin định danh sẽ "trưởng thành" sau mỗi lần nó được tiêu xài. Những chi tiết thông tin mỗi lần giao dịch được gắn vào phần tiền điện tử, và đi với nó khi nó được chuyển từ người này sang người khác.

Khi tiền điện tử chuyển tới ngân hàng, họ kiểm tra dữ liệu của nó, để xem tiền điện tử có bị tiêu xài hai lần không? Ngân hàng sử dụng những thông tin này để lần theo vết của những lần giao dịch, để phát hiện ra người nào tiêu xài hai lần.

4.**Tiền điện tử ẩn danh-ngoại tuyến:** Đây là dạng phức tạp nhất, bởi vì hệ thống phải làm sao vừa đảm bảo tính ẩn danh của người dùng, vừa đảm bảo

có thể truy vết được định danh người dùng trong trường hợp xảy ra vi phạm (tiêu xài hai lần).

Giải pháp cho hệ thống này là gắn thông tin lên đồng tiền ở mỗi lần giao dịch. Thông tin này sẽ trưởng thành sau mỗi lần giao dịch, khi tiền điện tử đến ngân hàng, họ sẽ kiểm tra trong cơ sở dữ liệu xem tiền này đã được tiêu chưa. Nếu ngân hàng phát hiện tiền này đã được tiêu trước đây, thì họ sẽ sử dụng thông tin tích lũy để xác định định danh của kẻ gian lận.

Tuy nhiên thông tin tích lũy trong trường hợp này dùng để lần theo vết giao dịch nếu như tiền điện tử được tiêu hai lần, nghĩa là chỉ khi có gian lận thìn ngân hàng mới có thể truy lại thông tin của người sử dụng.

Nếu tiền điện tử ẩn danh không bị tiêu xài hai lần thì ngân hàng không thể biết được định danh của người tiêu tiền, cũng như không thể xây dựng lại đường đi của tiền điện tử.

3.3 MỘT SỐ HỆ THỐNG TIỀN ĐIỆN TỬ

3.3.1 Hệ thống tiền điện tử First Virtual

First Virtual (FV) là một trong những công ty đầu tiên cung cấp hệ thống chuyển tiền điện tử thông qua mạng internet.

Hệ thống FV nhắm tới những khách hàng sử dụng thẻ tín dụng mua bán thông qua mạng internet. Hệ thống giải quyết được những rủi ro về an ninh vốn có đối với phương thức thanh toán bằng thẻ tín dụng qua mạng truyền thống.

Phương thức hoạt động:

Để tham gia vào hệ thống, đầu tiên cả khách hàng cũng như người bán hàng phải đăng ký với VF.Cả hai cùng cấp cho VF số thẻ tín dụng, sau đó VF gửi trở lại một số PIN, nó là đại diện cho số thẻ tín dụng của khách hàng. Mọi thanh toán giao dịch sau này sẽ làm việc trên só PIN này, điều này đảm bảo thông tin về thẻ tín dụng sẽ không bị tiết lộ.

Quá trình đăng ký với VF mở một tài khoản gồm những bước sau:

- Người sử dụng vào trang Web của VF để điền thông tin vào mẫu đăng ký, thông tin gồm có: Tên, địa chỉ, địa chỉ e-mail và yêu cầu cung cấp code. Người dùng phải cung cấp địa chỉ e-mail chính xác, vì họ sẽ nhận được thông tin từ VF thông qua địa chỉ e-mail này.
- Nếu thông tin được kiểm tra hợp lệ, thì phần mềm của VF tự động gửi một e-mail đến người đăng ký, nội dung của e-mail sẽ cung cấp số tài khoản tạm thời và số điện thoại.
- Người sử dụng gọi đến VF qua số điện thoại tren e-mail, họ cung cấp cho VF số tài khoản tạm thời (do VF cấp), số thẻ tín dụng của họ.
- Việc đăng ký hoàn tất và VF sẽ thu từ người dùng khoản tiền nhỏ cho chi phí mở tài khoản.

Sau khi có được tài khoản của VF quá trình mua bán diễn ra như sau:

1. Khách hàng gửi yêu cầu mua hàng cùng số PIN đến ngân hàng.
2. Người bán hàng gửi những thông tin bao gồm: Thông tin mô tả mua hàng, tổng số tiền mua, số PIN của khách hàng và chính số PIN của người bán hàng đến VF.
3. VF gửi e-mail đến người mua ,xác nhận lại những yêu cầu mua hàng.
4. Người mua hàng xác nhận những gì họ yêu cầu .Nếu người mua hàng từ chối. VF sẽ lưu lại thông tin này và quá trình giao dịch bị hủy bỏ. Trường hợp người bán hàng thường xuyên hủy bỏ những giao dịch mua hàng, thì VF sẽ hủy tài khoản của người này.
5. Nếu người mua hàng xác nhận đồng ý mua hàng, VF sẽ thục hiện giao dịch tài chính, tiền được chuyển từ khách hàng đến VF, sau đó được chuyển đến tài khoản của người bán hàng.
6. Sau khi các bước thực hiện thàng công,VF gửi xác nhận đến người bán hàng. Người bán hàng có thể phân phối hàng và quá trình mua bán kết thúc.

3.3.2 Hệ thống tiền điện tử DigiCash

Công ty DigiCash có trụ sở tại Amsterdam được thàng lập năm 1990 bởi David Chaum, Ông là một chuyên gia về lĩnh vực mật mã.Một trong những sản phẩm của công ty Ecash, đây là một dạng tiền điện tử, sản phẩm này được thiết kế cho những giao dịch an toàn từ bất cứ Pc nào đến trạm làm việc khác. Sản phẩm được phát triển dựa trên những giải pháp của Chaum.

Có ba đối tượng sẽ liên quan đến hệ thống Ecash: Khách hàng, người bán và nhà phát hành. Thông thường người phát hành là ngân hàng, nơi sẽ phát hành ra Ecash.

Điểm nổi trội của hệ thống DigiCash đó chính là tính ẩn danh, khách hàng không cần tiết lộ thông tin của mình cho người bán hàng hay nhà phát hành. Ngoại trừ trường hợp có gian lận, nghĩa là người mua hàng cố gắng tiêu cài tiền

này hai lần, thì nhà phát hành có thể tìm được thông tin định danh của người mua hàng nhằm chống gian lận.

Phương thức hoạt động

Để có thể sử dụng được hệ thống này, đầu tiên cả hai khách hàng cũng như người bán hàng phải có tài khoản với ngân hàng mà có hỗ trợ Ecash(Ví dụ ngân hàng EU ở Phần Lan), tài khoản này dùng để rút và gửi Ecash. Đồng thời đăng ký với DigiCash để có phần mềm đặc biệt "cyberwallet"(túi số).

Quá trình giao dịch sẽ chia thành bốn giai đoạn:

A: Tạo tiền Ecash

1. Sau khi biết được số tiền cần thanh toán, phần mềm "cyberwallet" tại máy khách hàng sinh ra dãy số ngẫu nhiên, dãy số này được xem như là dãy số tiền tương ứng cho tiền cần phải rút từ ngân hàng. Tham số mù sẽ được đưa vào dãy số, nó khiến cho cả ngân hàng không có chính xác nội dung của dãy số tiền này, và sau này ngân hàng sẽ không biết được ai là người sở hữ tiền, đây chính là tính ẩn dang của giải pháp.

2. Dãy số đã được làm mù sẽ được gửi đến ngân hàng mà khách hàng đã có tài khoản trước đấy.

3. Ngân hàng kiểm tra thông tin được gửi đến, sau đó ngân hàng ký lên thông điệp, tại thời điểm đó, tài khoản của khách hàng sẽ bị trừ một khoản tiền tương ứng.

4. Ngân hàng gửi dãy số sau khi đã được ký đến khách hàng.

5. Khách hàng giải mù những dãy số này, như vậy dãy số cộng với chữ ký ngân hàng đến lúc này thực sự trở thành những đồng tiền số có gia trị và giá trị của chúng được bảo đảm bởi ngân hàng, những đồng tiền số này sẽ chứa trên máy tính của người sử dụng.

B: Tiêu tiền Ecash

6. Khách hàng gửi một yêu cầu mua sắm tới người bán hàng.

7. Người bán hàng gửi một yêu cầu ngược đến đến cyberwallet software (số tiền cần thanh toán, thông tin về sản phẩm yêu cầu).

8. Khách hàng xác nhận giao dịch và đồng ý giao dịch, thì phần mềm sẽ thu thập những đồng tiền cần thiết đủ số tiền yêu cầu.

9. Chuyển tiền đến người bán hàng.

C: Đổi lại tiền

10. Trước khi chấp nhận thanh toán này, người bán hàng phải kiểm tra tính hợp lệ của những đồng tiền số bằng cách gửi chúng đến ngân hàng.

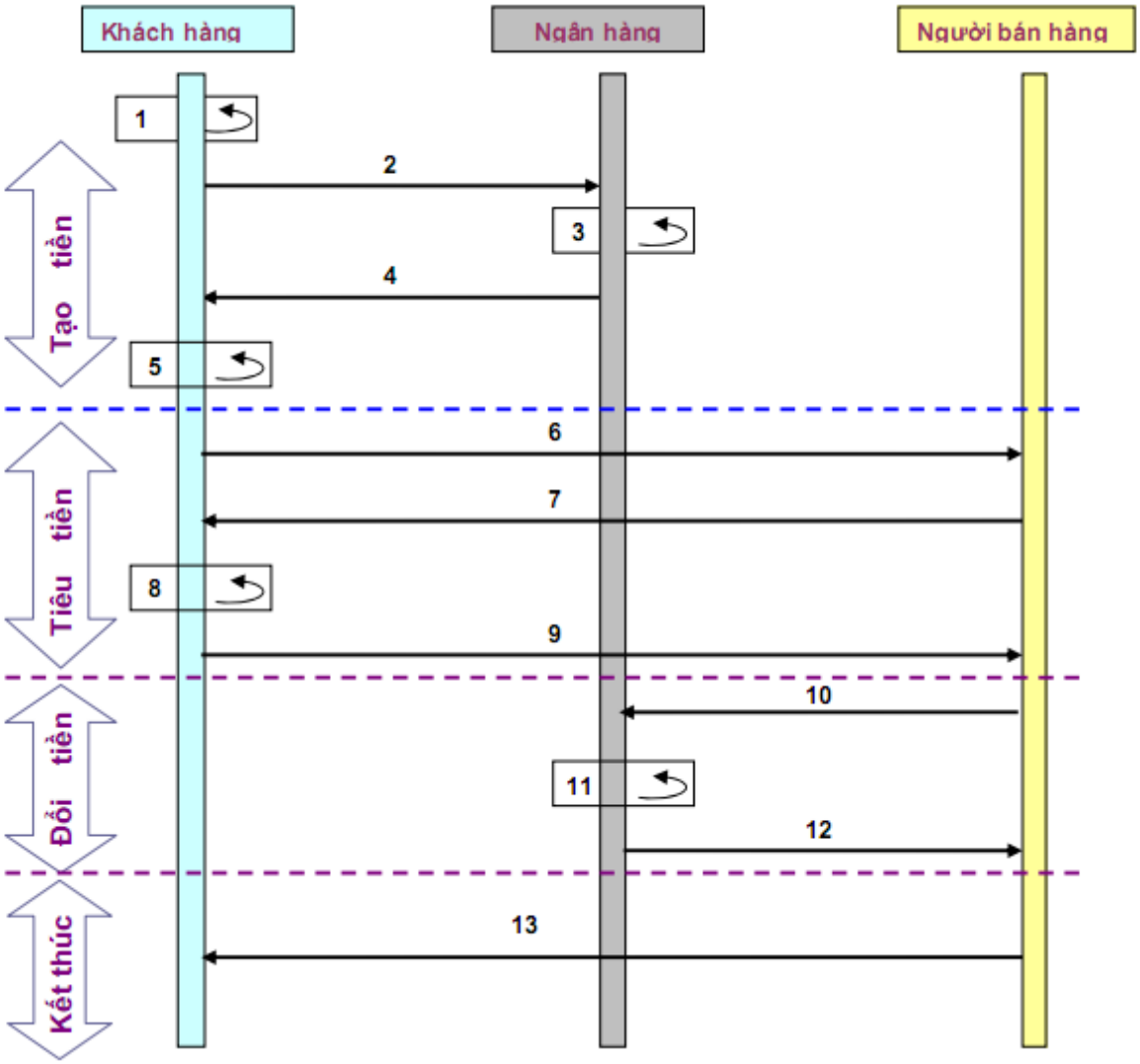
11. Ngân hàng kiểm tra tính hợp lệ của những đồng tiền số, đồng thời kiểm tra nó đã được tiêu trước đó chưa, bằng cách dựa vào dữ liệu lưu trữ của ngân hàng.

Nếu những đồng tiền là hợp lệ, ngân hàng sẽ phá hủy những đồng tiền số này, đồng thời lưu dãy số này vào dữ liệu của những đồng tiền đã sử dụng, và chuyển một khoản tiền đến tài khoản của người bán.

12. Ngân hàng phản hồi tính hợp lệ của những đồng tiền.

D: Kết thúc giao dịch

13. Sau khi những đồng tiền kiểm tra hợp lệ, người bán hàng gửi một biên nhận đến khách hàng và giao dịch tài chính được hoàn thành, như vậy hàng hóa có thể được phân phối.



Hình 6: Quá trình giao dịch của hệ thống DigiCash

3.3.3 Hệ thống tiền điện tử Millicent

Hệ thống được phát triển nhắm đến việc cung cấp một hệ thống thanh toán với giá trị giao dịch thấp thông qua cơ sở hạn tầng mạng internet. Millicent hỗ trợ những giao dịch có giá trị từ 1/10 cent đến 50 USD.

Phương thức hoạt động

Hoạt động của Millicent dựa vào ý tưởng những scrip(chứng khoán tạm thời). Trong hệ thống, một scrip giống như tiền mặt, nó cũng có giá trị. Tuy nhiên có điều khác biệt là những scrip chỉ có giá trị thực sự khi nó được đem ra tiêu với người bán cụ thể nào đấy.

Trung tâm của hệ thống là **nhà môi giới** (broker). Về lý thuyết thì bất kỳ tổ chức nào cũng có thể là nhà môi giới. Tuy nhiên trong thực tế chỉ tổ chức lớn mới đảm bảo tin cậy, ổn định mới thực hiện được chức năng này. Bởi vì nhà môi giới chính là đơn vị trung gian kết nối người bán hàng và khách hàng, mặc dù họ không biết nhau. Nhà môi giới phục vụ như một nhà trung gian, thay mặt khách hàng và làm việc với tất cả người bán hàng, và ngược lại là nhà trung gian thay mặt người bán hàng làm việc với tất cả khách hàng.

Có hai loại scrip, đó là Broker scrip và Merchant scrip. Broker scrip là scrip mà khách hàng mua từ nhà môi giới. Merchant scrip là scrip mà nhà môi giới mua từ người bán hàng.

Ví dụ người mua hàng mua nhà môi giới 50 Broker scrip ,mới scrip có giá trị 10 cent. Người mua muốn mua một vật có giá trị 2 cent. Ông ta sẽ gửi 1 scrip (có giá trị 10 cent) đến nhà môi giới, họ sẽ chuyển scrip này thành Merchant scrip có giá trị 10 cent của người bán hàng. Người bán hàng kiểm tra tính hợp lệ của những scrip này và gửi lại ngươi mua 1 Merchant scrip có giá trị 8 cent. Người mua có thể giữ scrip cho việc mua về sau với người bán đó, hay trả nó cho nhà môi giới, và nhận lại Broker scrip, để sau này có thể mua từ người bán hàng khác.

Về mặt kỹ thuật ,hệ thống bao gồm 3 phần mềm. Một cho khách hàng (client), một cho server của broker và một cho người bán hàng.

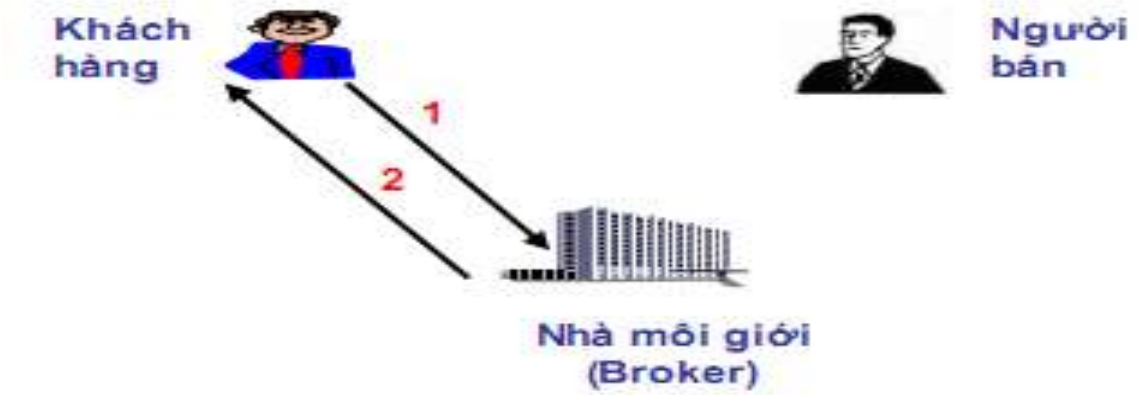
Phần mềm client của khách hàng dạng như “chiếc ví” để mua broker scrip và nhận “tiền thừa”.

Phần mềm phía người bán có khả năng tạo, phân phối hay xác nhận tính hợp lệ của scrip thuộc quyền sở hữu.

Broker server có những tính năng gần giống phần mềm phía người bán và nó có thể chuyển đổi Broker scrip thành Merchant scrip nào đấy.

Giao dich giữa khách hàng người bán và nhà môi giới diễn ra như sau:

Bước 1: Khách hàng kết nối đên nhà môi giới để mua Broker scrip



1: Khách hàng gửi yêu cầu mua Broker scrip

2: Nhà môi giới gửi Broker scrip

Hình 7: khách hàng mua Broker scrip

Bước 2: Để mua hàng của Người bán, người mua phải có Merchant scrip của cửa hàng đó. Hoặc là người mua hàng phải mua Merchant scrip từ nhà môi giới và trả bằng Broker scrip (đã mua trước đây).

3: khách hàng mua Merchant scrip và trả bằng Broker scrip.

Hình 8: Khách hàng mua Merchant scrip

Bước 3: Nếu nhà môi giới không có Merchant scrip mà khách hàng cần mua, thì nhà môi giới sẽ mua từ người bán hàng đó và gửi tới người mua hàng cùng với tiền thừa ở dạng Broker scrip mới (nếu có).

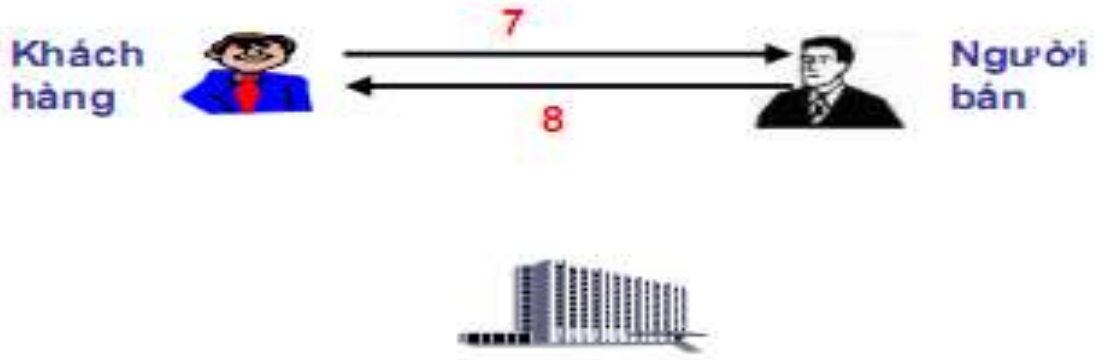
4: Nhà môi giới gửi yêu cầu mua Merchant scrip

5: Nhà môi giới nhận Merchant scrip

6: Nhà môi giới trả Merchant scrip cho khách hàng và Broker scrip thừa

Hình 9: Nhà môi giới mua Merchant scrip và gửi cho khách hàng

Bước 4: Người mua hàng gửi Merchant scrip cho Người bán để thanh toán và người bán gửi lại tiền thừa ở dạng Merchant scrip mới.



7: Khách hàng gửi Merchant scrip để thanh toán

8: Người bán hàng gửi lại Merchant scrip thừ nếu có

Hình 10: Khách hàng gửi Merchant scrip để thanh toán

3.3.4 Hệ thống tiền điện tử Modex

Hệ thống Modex được phát triển từ năm 1990. Tính đa năng là một trong những nét đặc biệt nhất của hệ thống Modex.

Phương thức hoạt đông

Nắm vai trò chính trong hệ thống là Smart Card, nó có tính năng chấp nhận, chứa và phân phối tiền. Smart Card không chỉ chứa tổng số tiền hiện tại mà còn chứa dữ liệu về lịch sử những lần giao dịch trước đấy. Khả năng chứa dữ liệu của Smart Card phụ thuộc và con chip trong đó.

Modex Card do ngân hàng phát hành, mỗi thẻ này liên quan đến một tài khoản ngân hàng. Mỗi thẻ có một chuỗi số đại diện, nhằng xác đinh định danh của người sở hữu, chuỗi số này là duy nhất. Mọi giao dịch đều ghi lại chuỗi số định danh này.

Hệ thống Modex hỗ trợ cho hai người trực tiếp thanh toán với nhau (tính chuyển nhượng). Nên việc chuyển tiền trong cả hai Card (gửi và nhận) phải được đưa và trong bộ đọc để giao tiếp để xác thực với nhau.

Mã hóa đóng vai trò trung tâm trong hệ thống Modex. Nó đảm bảo rằng những thẻ được xác thực là đúng và không bị giả mạo, được sử dụng trong hệ thống, và việc giao tiếp giữa hai thẻ không thể bị chặn. Do đó giấy biên nhận cuối mỗi phiên giao dịch chủ yếu để chứng minh việc chuyển tiền không bị đất quãng.

3.4 LƯỢC ĐỒ CHAUM-FIAT-NAOR

Hệ thống tiền điện tử được áp dụng thành công là nhờ một đặc tính quan trọng đó là tính ẩn danh. Một hệ thống tiền điện tử ẩn danh tin cậy sẽ ngăn ngừa việc bên thứ ba (ngân hàng, nhà cung cấp) biết được thông tin định danh của người tham gia vào hệ thống.

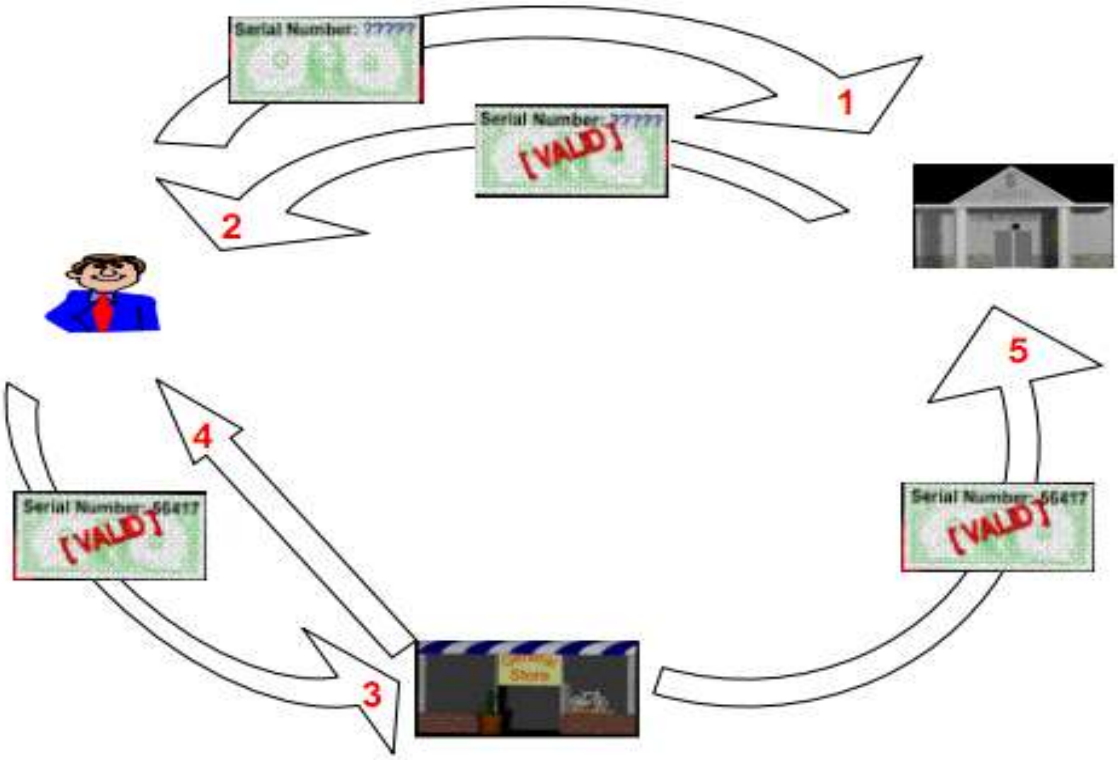
Lược đồ Chaum-Fiat-Naor là lược đồ ẩn danh đơn giản, áp dụng cho hệ thống tiền điện tử có tính ẩn danh. Lược đồ đã áp dụng **chữ ký mù RSA** và giao thức **cắt và chọn** để ngăn ngừa người tạo tiền có hành vi gian lận.

Việc kết hợp những kỹ thuật mật mã này cho phép ngân hàng ký tên trên những đồng tiền do người sử dụng gửi đến, nhưng ngân hàng không biết những gì đã được ký. Do đó họ không thể kiểm tra những thanh toán đã thực hiện. Nghĩa là ngân hàng không biết được hành động rút tiền này sẽ liên quan đến khoản tiền nào, điều này đảm bảo được tính ẩn danh của người sử dụng.

Để ngăn ngừa vấn đề "tiêu xài hai lần", lược đồ này dùng giao thức "**hỏi đáp**" để lấy một phần thông tin định danh gắn lên đồng tiền, và như vậy nếu đồng tiền được "tiêu xài hai lần", thì thông tin trên cả hai trường hợp được kết hợp lại để truy vết tìm kẻ gian lận.

Ngân hàng công khai khóa mật mã **RSA** là (**b,n**), và chọn tham số **k**. Ngân hàng cũng công khai hai hàm **f** và **g** (hàm không va chạm).

Mỗi người sử dụng có số tài khoản **u**, và ngân hàng sẽ giữ số đếm **v** liên quan đến số tài khoản này (nếu số đơn vị Ui được tạo), ngân hàng dựa vào **u** để xác định kẻ gian lận.



1: Khách hàng gửi tiền ở dạng "mù" yêu cầu ngân hàng ký.

2: Ngân hàng gửi trả tiền đã ký cho khách hàng(tiền vẫn còn mù).

3: Sau khi bỏ "mù" tiền, khách hàng chuyển tiền cho người bán.

4: Người bán tiến hành chuyển giao hàng.

5: Người bán chuyển tiền đến ngân hàng để kiểm tra tính hợp lệ của tiền.

Hình 11: Mô hình thanh toán trong lược đồ CHAUM-FIAT-NAOR

3.4.1 Giao thức rút tiền

1. Ông A muốn có một đồng tiền điện tủ ẩn danh, thì cần phải tạo k đơn vị U_i và chuyển nó đến ngân hàng, một đơn vị U_i được tạo ra từ những dãy số ngẫu nhiên a_i, c_i, d_i; $1 \le I \le k$, sao cho U_i độc lập và duy nhất.

$$U_i = f(x_i,y_i), \text{ với } 1 \le I \le k$$

$$x_i = g(a_i, c_i),\ y_i = g(a_i \oplus (u \wedge (v + i)), d_i).$$

$\oplus$: phép XOR, $\wedge$: phép nối

2. Ông A làm mù k đơn vị U_i với những tham số "mù" ngẫu hiên $\{r_1,\ldots,r_k\}$, và gửi chúng đến ngân hàng. Những tham số "mù" đó ngăn ngân hàng kiểm tra tức thì nội dung của những đồng tiền U_i.

(Làm "mù" theo giao thức RSA: $Blind(x)=r*r^b \bmod n$)

3. Ngân hàng chọn ngẫu nhiên k/2 đơn vị để kiểm tra, và yêu cầu ông A cung cấp các tham số: r_i, a_i,c_i, d_i tương ứng với những đơn vị U_i mà ngân hàng đã chọn.

4. Ông A cung cấp cho ngân hàng các tham số r_i, a_i, c_i, d_i theo yêu cầu.

5. Dựa vào các tham số do ông A cung cấp, ngân hàng sóa mù k/2 đơn vị đã chọn và kiểm tra để đảm bảo rằng ông A không gian lận. Nếu không có lỗi nào xảy ra, ngân hàng ký lên những đơn vị U_i còn lại(những đơn vị mà ngân hàng không xóa "mù") và gửi cho ông A.

$$B^a_j \bmod n$$

(j là ngẫu nhiên $\le$ k và chỉ dùng k/2 phần tủ B_j)

Sau đó ngân hàng trừ khoản tiền tương ứng vào tài khoản của ông A.

6. Ông A xóa "mù" đơn vị đã được ngân hàng ký bằng cách chia B_j cho r_j lúc này ông A có đồng tiền điện tử với giá trị thực sự.

$$T = f(x_j,y_j)^a \bmod n$$

3.4.2 Giao thức thanh toán

1. Ông A gửi tiền T đến ông B.

2. Ông B chọn chuỗi nhị phân ngẫu nhiên $z_1,z_2,\ldots,z_{k/2}$ và gửi nó đến ông A.

3. Ông A phản hồi lại tùy từng trường hợp sau:

+ Nếu z_i =1 thì ông A sẽ gửi đến ông B: a_i, c_i, và y_i.

+ Nếu z_i =0 thì ông A sẽ gửi đến ông B: x_i, $a_i \oplus (u \wedge (v+i))$ và d_i.

4. Ông B kiểm tra T là hợp lệ trước khi chấp nhận thanh toán của ông A.

3.4.3 Giao thức gửi

1. Ông B gửi lịch sử thanh toán đến ngân hàng.

2. Ngân hàng kiểm tra chữ ký số của ngân hàng.

3. Ngân hàng kiểm tra thực sự tiền này chưa bị tiêu xài trước đó.

4. Ngân hàng nhập vào cơ sở dữ liệu những tiền đã bị tiêu xài, đồng thời lưu giữ chuỗi nhị phân, và những phản hồi tương ứng từ ông A (điều này sẽ giúp cho sau này phát hiện kẻ tiêu xài hai lần)

5. Ngân hàng cộng khoản tiền tương ứng vào tài khoản của ông B.

3.4.4 Đánh giá

Tại giao thức rút tiền để ngăn ngừa khả năng gian lận của ông A. Lược đồ sử dụng giao thức " cut and choose". Ông A phải tiết lộ k/2 mẫu thông tin một cách ngẫu nhiên từ k mẫu. Như vậy khả năng ông A có thể thực hiện hành vi gian lận phụ thuộc vào độ lớn của k.

Nếu ông A tiêu đồng tiền T hai lần, khả năng ngân hàng có thể lấy được cả hai tham số a_i và $a_i \oplus (u \wedge (v+i))$ để tính được u. Đó là số tài khoản của ông A tại ngân hàng, chính vì vậy từ u, ngân hàng có thể truy ra được ông A là người có hành vi tiêu một đồng tiền hai lần. Vì khả năng có cặp bít khác nhau trong hai chuỗi $z_1,z_2,\ldots,z_{k/2}$ và $z_1',z_2',\ldots,z_{k/2}'$ là rất cao. Chỉ cần một cặp bít tương ứng z_i và z_i' khác nhau,là ngân hàng có thể có đủ thông tin định danh cảu ông A. Như

vậy xác suất để hai chuỗi hoàn toàn trùng nhau (trong trường hợp này ngân hàng không có đủ thông tin để tìm ra định danh của ông A) là $1/2^{k/2}$,và nếu chọn k đủ lớn thì khả năng hai chuỗi trùng nhau hoàn toàn có thể nói là không thể xảy ra.

3.4.5 Chi phí

Trong lược đồ CHAU-FIAT-NAOR, chi phí (thời gian, tính toán,..) phụ thuộc vào độ lớn của k. Tại giao thức rút tiền trong lược đồ, ông A phải gửi k packet đến ngân hàng, tuy nhiên ngân hàng chỉ phải gửi lại 1 packet. Việc tiến hành làm "mù" và xóa "mù" sẽ làm tăng sự tính toán và liên lạc.

Tại giao thức thanh toán ,sau khi ông A gửi tiền đến ông B. Ông này gửi chuỗi nhị phân đến ông A, sau đó ông A phải gửi k/2 phản hồi khác nhau, điều này sẽ khiến cho việc tăng khả năng và sụ tính toán, liên lạc và chi phí lưu trữ.

3.4.6 Tấn công

Đây là giải pháp dựa vào mật mã RSA, vì vậy tất cả những cách tấn công vào RSA, đều có thể được sử dụng để tấn công vào lược đồ này.

Tuy nhiên về mặt lý thuyết, có một khả năng xảy ra là ông A có thể tránh được sự phát hiện của ngân hàng khi tiêu xài một đồng tiền hai lần. Để thực hiện được điều này, phương pháp hợp tác tấn công giữa ông A và ông X sẽ tấn công vào giao thức "hỏi-đáp". Ông A sau khi thực hiện một giao dịch thanh toán với ông B, sẽ gửi những đồng tiền đã tiêu đến ông X và mô tả quá trình giao dịch với ông B cho ông X. Như vậy ngân hàng sẽ nhận được thông tin giao dịch từ ông B và ông X giống như nhau, lúc này ngân hàng sẽ không có khả năng xác định được định danh của ông A.

3.5 Chương trình mô phỏng tiền điện tử

3.5.1 Yêu cầu bài toán

Xây dựng chương trình mô phỏng *quá trình tạo lập* và *sử dụng* đồng tiền điện tử theo lược đồ CHAUM-FIAT-NAOR đảm bảo được hai yêu cầu chính của đồng tiền điện tử là *tính ẩn danh* và chống *tiêu xài hai lần*

3.5.2 Cấu hình hệ thống

Chương trình được xây dựng và thi hành trên hệ thống máy tính có cấu hình như sau:

Tốc độ sử lý 500 MHz.

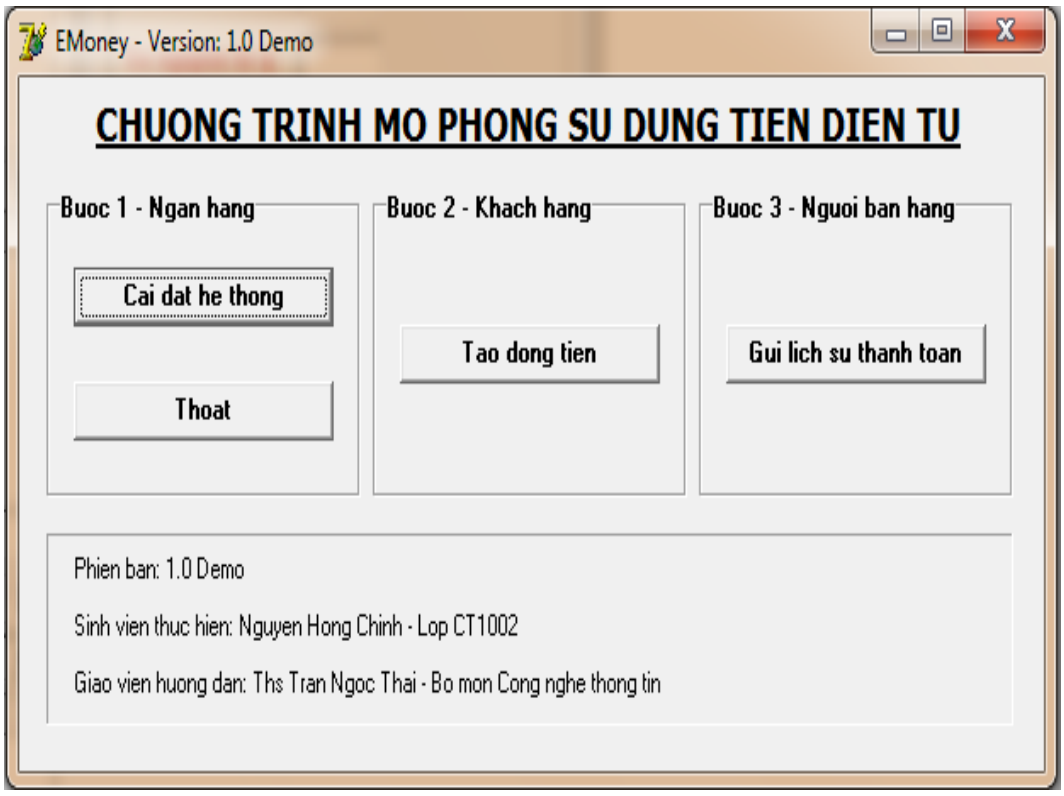
Bộ nhớ 128 MB.

Dung lượng ổ đĩa cứng: 200 MB Free.

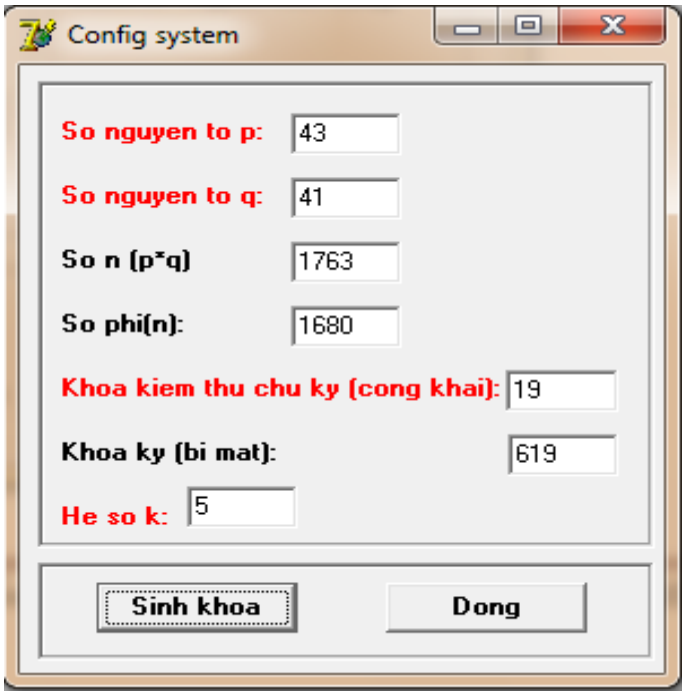
Hệ điều hành: Window XP, Vista, Window 7.

PHỤ LỤC

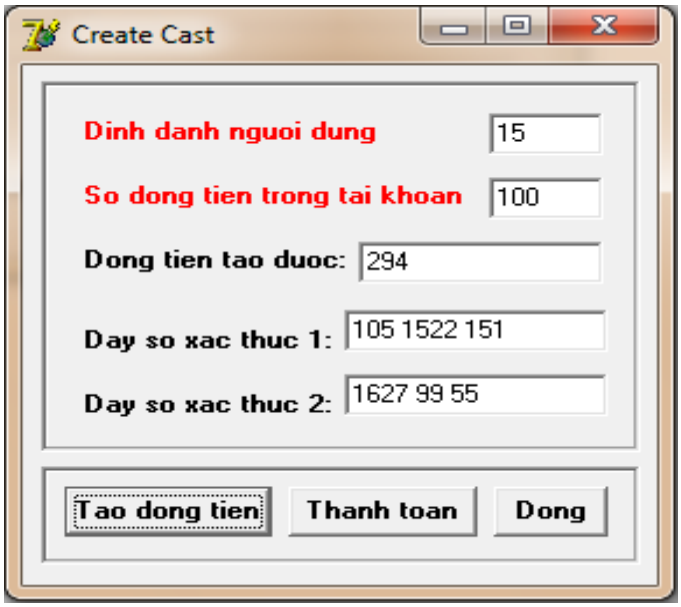
Các giao diện chính của chương trình



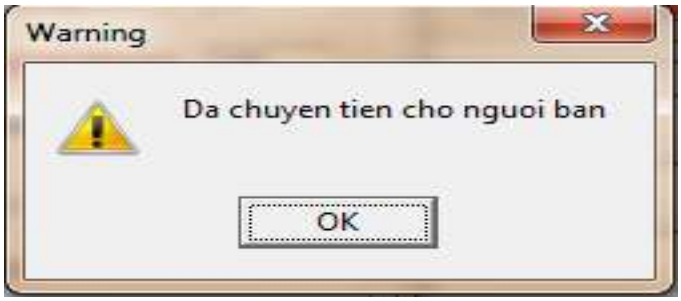
Hình 12: Giao diện chính của chương trình



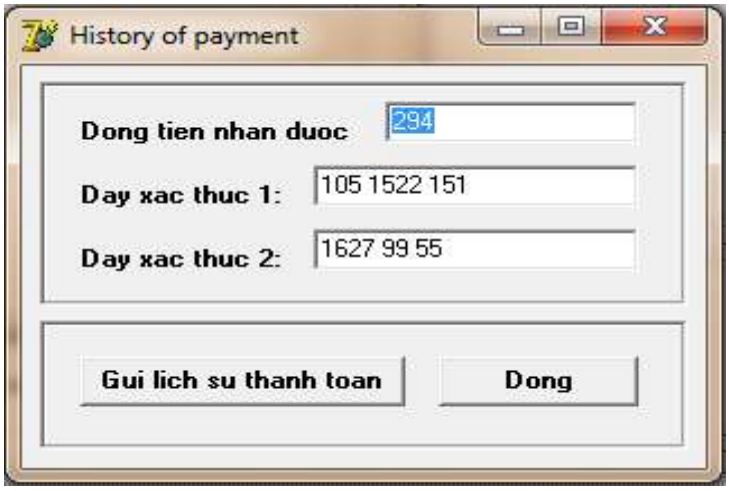
Hình 13: Giao diện cài đặt hệ thống



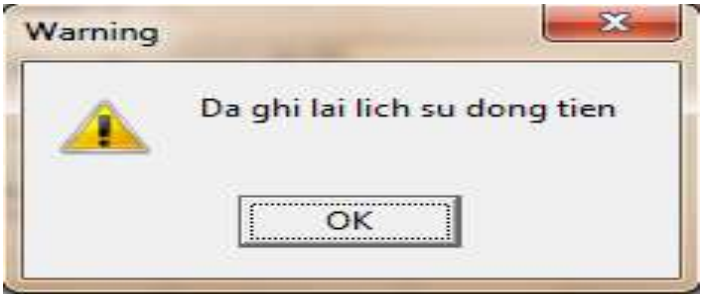
Hình 14: Giao diện tạo đồng tiền



Hình 15: Giao diện thông báo khi bấm nút thanh toán



Hình 16: Giao diện gửi lịch sử thanh toán tiền



Hình 17: Giao diện thông báo khi bấm nút Gửi lịch sủ thanh toán

Hình 18: Giao diện thông báo khi gửi lịch sủ thanh toán của đồng tiền đã được tiêu xài

KẾT LUẬN

Sau một thời gian làm việc nghiêm túc cùng với sự giúp đỡ, chỉ bảo nhiệt tình của thầy Trần Ngọc Thái cùng toàn thể các thầy giáo,cô giáo trong khoa công nghệ thông tin trường DHDL-HP. Em đã hoàn thành khóa luận trên cơ sở đã tìm hiểu và thực hiện được một số nội dung theo đề tài như:

- Tìm hiểu được các kiến thức cơ bản mật mã.
- Tìm hiểu được các kiến thức về chứng chỉ số.
- Tìm hiểu được một số lược đồ và mô hình thanh toán tiền điện tử.
- Xây dựng được chương trình mô phỏng sử dụng tiền điện tử bằng Delphi dựa trên mô hình CHAUM-FIAT-NAOR.

Tuy nhiên do lần đầu tiếp cận và thời gian cũng như kinh nghiệm và kiến thức còn hạn chế, khóa luận không tránh khỏi những thiếu sót. Khóa luận mới chỉ dừng lại ở mức tìm hiểu, nghiên cứu và tổng hợp các kiến thức đã có. Hướng phát triển tiếp của khóa luận là tiếp tục nghiên cứu tiềm hiểu sâu hơn các hệ thống và mô hình tiền điện trên thế giới, để từ đó có thể xây dựng thành công hệ thống sử dụng tiền điện tử một cách an toàn và phổ biến tại thị trường còn mới ở Việt Nam.

TÀI LIỆU THAM KHẢO

[1] PGS.TS Trịnh Nhật Tiến, Giáo trình An toàn dữ liệu.

[2] Brands Stefan, An efficient Off-line electronic cash system based on the representation problem, Technical report.

[3] Ruchan Ziya, Encryption Technipues, Cash Security Protocols, Cash systems, The degree of master of Sciences in Engineering Management.