MỤC LỤC

LỜI CẢM ƠN

Trước hết em xin được bày tỏ sự trân trọng và lòng biết ơn đối với thầy giáo PGS.TS. Trịnh Nhật Tiến. Trong suốt quá trình làm khóa luận tốt nghiệp của em, thầy đã dành rất nhiều thời gian quí báu đê tận tình chỉ bảo, hướng dân, định hướng cho em trong việc nghiên cứu.

Em xin chân thành cảm ơn sự dạy bảo và giúp đỡ của các thầy giáo, cô giáo Khoa Công Nghệ Thông Tin – Trường Đại Học Dân Lập Hải Phòng đã trang bị cho em những kiến thức cơ bản nhất để em có thể hoàn thành tốt báo cáo tốt nghiệp này.

DANH MỤC HÌNH VẼ

BẢNG CHỮ VIẾT TẮT

BDK: Ban đăng ký.

BKP: Ban kiểm phiếu.

CA: Certificate Authority – tổ chức chứng thực số.

CMT: Chứng minh thư.

CPU: Central Processing Unit – đơn vị xử lý trung tâm.

CT: cử tri.

GHz: Gigahertz – đơn vị đo tần số.

HDD: Hard Disk Driver – thiết bị lưu trữ dữ liệu.

MB: Megabyte – đơn vị đo dung lượng.

MHz: Megahertz - đơn vị đo tần số.

RAM: Random Access Memmory – Bộ nhớ truy cập ngẫu nhiên.

RSA: là tên 1 hệ mã hóa khóa công khai được đặt tên bằng tên của 3 người sáng tạo ra hệ mã hóa là Ron Rivest, Adi Shamir và Len Adleman.

USB: Univeral Serial Bus – 1 chuẩn kết nối của máy tính với các thiết bị ngoại vi.

MỞ ĐẦU

Trong suốt nhiều thế kỉ qua trên thế giới, các cuộc bầu cử đã giữ một vai trò quan trọng trong việc xác lập thể chế chính trị của các quốc gia.

Và trong xu hướng phát triển của khoa học công nghệ ngày nay, công nghệ thông tin đã ngày càng phổ biến và được áp dụng trong mọi lĩnh vực đời sống. Các cuộc bầu cử cũng không phải là ngoại lệ. Người ta đã bỏ rất nhiều công sức để nghiên cứu cải tiến các phương thức bầu cử để nó ngày càng trở nên tốt và tiện lợi hơn. Các phương thức thay đổi theo từng thời kỳ, theo sự tiến bộ của xã hội. Và với sự tiến bộ của xã hội ngày nay thì các dự án chính phủ điện tử để giúp nhà nước điều hành đất nước là một điều tất yếu, kèm theo đó thì sự phát triển của bỏ phiếu điện tử để thay thế cho bỏ phiếu thông thường là điều sẽ diễn ra trong tương lai.

Nắm được tầm quan trọng và tính tất yếu của bỏ phiếu điện tử, các nước, các tổ chức đã và đang xây dựng giải pháp cho bỏ phiếu điện tử.

Khóa luận sẽ đi sâu về các bài toán về an toàn thông tin trong một cuộc bỏ phiếu điện tử, đặc biệt là trong giai đoạn đăng ký bỏ phiếu. Sau đó phân tích thiết kế thử nghiệm một ứng dụng nhỏ về bỏ phiếu điện tử.

Chương 1. MỘT SỐ KHÁI NIỆM CƠ BẢN

1.1. MỘT SỐ KHÁI NIỆM TOÁN HỌC

1.1.1. Số nguyên tố và nguyên tố cùng nhau

1/. Khái niệm.

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

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

Số nguyên tố thường được sử dụng trong các hệ mã hóa (thường là các số lớn hơn 10^{150}).

2/. Ví dụ:

+ Các số 2, 3, 5... là các số nguyên tố.

+ Hai số 9 và 14 là nguyên tố cùng nhau.

1.1.2. Đồng dư

1/. Khái niệm.

Cho các số nguyên a, b, n (n > 0), khi đó a được gọi là đồng dư với b theo modulo n, nếu chia a và b cho n có cùng một số dư. Số nguyên n được gọi là modulo của đồng dư.

Ký hiệu: $a \equiv b \pmod n$.

2/. Ví dụ: $5 \equiv 7 \bmod 2$ vì $5 \bmod 2 = 7 \bmod 2 = 1$.

3/. Tính chất của đồng dư:

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

+ $a \equiv b \bmod n$ nếu chỉ nếu a và b có cùng số dư khi chia cho n.

+ Tính phản xạ: $a \equiv a \bmod n$.

+ Tính đối xứng: 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 $a \equiv a_1 \bmod n$, $b \equiv b_1 \bmod n$ thì $a + b \equiv a_1 + b_1 \bmod n$ và $ab \equiv a_1b_1 \bmod n$.

1.1.3. Không gian Z_n và Z_n^*

1/. Khái niệm.

Không gian các số nguyên theo modulo n: Z là tập hợp các số nguyên không âm nhỏ hơn n. Tức là : $Z_n = \{0, 1, 2, ..., n-1\}$. Tất cả các phép toán trong Z_n đều được thực hiện trong modulo n.

Không gian Z_n^* là tập hợp các số nguyên p thuộc Z_n sao cho ước chung lớn nhất của p và n là 1. Tức là $Z_n^* = \{p \text{ thuộc } Z_n \mid UCLN(n, p) = 1\}$

2/. Ví dụ: $Z_6 = \{0, 1, 2, 3, 4, 5\}$, $Z_6^* = \{1, 5\}$

1.1.4. Khái niệm nhóm, nhóm con, nhóm Cyclic

1/. Khái niệm.

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

+ Tính chất kết hợp: (x * y) * z = x * (y * z)

+ Tính chất tồn tại phần tử trung gian e $\in$ G: e * x = x * e = x, $\forall$x $\in$ G

+ Tính chất tồn tại phần tử nghịch đảo x' $\in$ G: x' * x = x * x' = e

b) Nhóm con của G là tập S $\subset$ G, S $\neq \emptyset$, và thỏa mãn các tính chất sau:

+ Phần tử trung lập e của G nằm trong S.

+ S khép kín đối với phép tính (*) trong, tức là x * y $\in$ S với mọi x, y $\in$ S.

+ S khép kín đối với phép lấy nghịch đảo trong G, tức $x^{-1} \in$ S với mọi x $\in$ S.

c) Nhóm cyclic:

(G, *) là nhóm được sinh ra bởi một trong các phần tử của nó. Tức là có phần tử g $\in$ G mà với mỗi a $\in$ G, đều tồn tại số n $\in$ N để $g^n = a$. Khi đó g là phần tử sinh hay phần tử nguyên thủy của nhóm G.

2/. Ví dụ:

(Z^+, *) gồm các số nguyên dương là một nhóm cyclic có phần tử sinh là 1.

1.1.5. Hàm ϕ Euler

1/. Khái niệm:

Cho n ≥ 1. **ϕ**(n) được định nghĩa là các số nguyên trong khoảng [1, n] nguyên tố cùng nhau với n. Hàm **ϕ** được gọi là phi Euler.

2/. Tính chất:

+ Nếu p là số nguyên tố thì **ϕ**(n) = p - 1.

+ Hàm phi Euler là hàm có tính nhân:

+ Nếu UCLN(m, n) = 1 thì **ϕ**(mn) = **ϕ**(m) **ϕ**(n)

+ Nếu n = $p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ là thừa số nguyên tố của m thì

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right) \qquad [1.1]$$

1.1.6. Phần tử nghịch đảo

1/. Khái niệm.

Cho a ∈ Z_n. Nếu tồn tại b ∈ Z_n sao cho a b ≡ 1 (mod n), ta nói b là phần tử nghịch đảo của a trong Z_n và ký hiệu a^{-1}. Một phần tử có phần tử nghịch đảo, gọi là khả nghịch.

2/. Tính chất:

+ Cho a, b ∈ 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 khả nghịch theo modulo n.

+ Cho a ∈ Z_n, a khả nghịch khi và chỉ khi UCLN(a, n) = 1.

+ Giả sử d = UCLN (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 [0, n-1] thì các nghiệm đồng dư theo modulo $\frac{n}{d}$.

3/. Ví dụ: 4^{-1} = 7 mod 9 vì 4 . 7 ≡ 1 mod 9

1.1.7. Các phép tính cơ bản trong không gian modulo

Cho n là số nguyên dương. Các phần tử trong Z_n được thể hiện bởi các số nguyên {0, 1, 2, ..., n-1}. Nếu a, b $\in Z_n$ thì:

$$(a + b) \bmod n = \begin{cases} a + b \text{ nếu } a + b < n \\ a + b - n \text{ nếu } a + b \geq n \end{cases}$$

Vì vậy, phép cộng modulo (và phép trừ modulo) có thể được thực hiện mà không cần thực hiện các phép chia dài. Phép nhân modulo của a và b được thực hiện bằng phép nhân thông thường a với b như các số nguyên bình thường, sau đó lấy phần dư của kết quả sau khi chia cho n.

1.1.8. Độ phức tạp của thuật toán

1/. Chi phí của thuật toán.

Chi phí phải trả cho một quá trình tính toán gồm chi phí thời gian và bộ nhớ.

+ Chi phí thời gian của một quá trình tính toán là thời gian cần thiết để thực hiện một quá trình tính toán.

+ Chi phí bộ nhớ của một quá trình tính toán là số ô nhớ cần thiết để thực hiện một quá trình tính toán.

Gọi A là một thuật toán, e là dữ liệu vào của bài toán đã được mã hóa. Thuật toán A tính trên dữ liệu vào e phải trả một giá nhất định.

Ký hiệu: $t_A(e)$ là giá thời gian và $l_A(e)$ là giá bộ nhớ.

2/. Độ phức tạp về bộ nhớ:

$t_A(n) = \max \{ l_A(e)$, với $|e| \leq n\}$, n là "kích thước" đầu vào của thuật toán.

3/. Độ phức tạp về thời gian: $l_A(n) = \max \{ t_A(e)$, với $|e| \leq n\}$.

4/. Độ phức tạp tiệm cận:

Độ phức tạp PT(n) được gọi là tiệm cận tới hàm f(n), ký hiệu O(f(n)) nếu tồn tại các số n_0, c mà PT(n) $\leq$ c.f(n), $\forall n \geq n_0$.

5/. Độ phức tạp đa thức:

Độ phức tạp PT(n) được gọi là đa thức, nếu nó tiệm cận tới đa thức p(n).

6/. Thuật toán đa thức:

Thuật toán được gọi là đa thức, nếu độ phức tạp về thời gian là đa thức.

1.1.9. Hàm một phía và hàm cửa sập một phía

1/. Hàm một phía.

a/. Khái niệm.

Hàm f(x) được gọi là hàm một phía nếu tính xuôi y = f(x) thì dễ, nhưng tính ngược $x = f^{-1}(y)$ lại rất khó.

Trong trường hợp này "khó" có nghĩa là để tỉnh ra được kết quả thì phải mất rất nhiều thời gian để tính toán.

b/. Ví dụ.

Hàm một phía $y = f(x) = g^x \pmod p$ với p là số nguyên tố lớn (g là phần tử nguyên thủy mod p).

2/. Hàm cửa sập một phía

a/. Khái niệm.

Hàm f(x) được gọi là hàm cửa sập một phía nếu tính "xuôi" y = f(x) thì "dễ", tính $x = f^{-1}(y)$ lại rất "khó". Tuy nhiên có cửa sập Z để tính $x = f^{-1}(y)$ là dễ.

b/. Ví dụ.

Hàm $f(x) = x^a \bmod n$ là hàm một phía (n là tích 2 số nguyên tố lớn p và q). Nếu chỉ biết a và n thì tính $x = f^{-1}(y)$ là rất khó, nhưng nếu biết cửa sập p và q, thì tính được $f^{-1}(y)$ là "dễ".

1.2. KHÁI NIỆM MÃ HÓA

1.2.1. Giới thiệu

Để đảm bảo an toàn thông tin lưu trữ trong máy tính hay bảo đảm thông tin trên đường truyền tin, người ta phải "che giấu" các thông tin này.

+ "Che" thông tin hay "mã hóa" thông tin là thay đổi hình dạng thông tin gốc, và người khác "khó" nhận ra.

+ "Giấu" thông tin là cất giấu thông tin trong bản tin khác, và người khác cũng khó nhận ra.

Trong chương này chúng ta sẽ bàn về "mã hóa" thông tin.

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 các khóa có thể.

+ E là hàm lập mã.

+ D là tập các hàm giải mã.

Với khóa lập mã ke $\in$ K, có hàm lập mã $e_{ke} \in E$, e_{ke}: P $\rightarrow$ C.

Với khóa giải mã kd $\in$ K, có hàm giải mã $d_{kd} \in D$, d_{kd}: C $\rightarrow$ P.

Sao cho $d_{kd}(e_{ke}(x)) = x$, $\forall x \in P$.

Ở đây x được gọi là bản rõ, $e_{ke}(x)$ được gọi là bản mã.

Hiện có 2 loại hệ mã hóa chính: hệ mã hóa khóa đối xứng và mã hóa khóa bất đối xứng.

1.2.2. Hệ mã hóa khóa đối xứng

1/. Khái niệm.

Hệ mã hóa khóa đối xứng là hệ mã hóa có khóa lập mã và khóa giải mã là "giống nhau", theo nghĩa biết được khóa này thì "dễ" tính được khóa kia. Vì vậy phải giữ bí mật cả hai khóa.

Đặc biệt có một số hệ mã hóa có khóa lập mã và khóa giải mã trùng nhau (ke = kd), như hệ mã hóa "dịch chuyển" hay DES.

2/. Đặc điểm.

a). Ưu điểm:

+ Hệ mã hóa khóa đối xứng mã hóa và giải mã nhanh hơn hệ mã hóa khóa bất đối xứng.

b). Hạn chế:

+ Hệ mã hóa khóa đối xứng chưa thật an toàn với lý do sau:

Khóa phải được giữ bí mật tuyệt đối vì biết được khóa này dễ tính được khóa kia và ngược lại.

+ Vấn đề thỏa thuận khóa và quản lý khóa chung là khó khăn và phức tạp.

Người gửi và người nhận phải luôn thống nhất về khóa. Việc thay đổi khóa là rất khó và dễ bị lộ. Khóa chung phải được gửi cho nhau trên kênh an toàn.

3/. Ứng dụng.

Hệ mã hóa khóa đối xứng thường được sử dụng trong môi trường mà khóa chung có thể dễ dàng trao chuyển bí mật, chẳng hạn trong cùng một mạng nội bộ. Hệ mã hóa khóa đối xứng thường được sử dụng để mã hóa những bản tin lớn, vì tốc độ mã hóa và giải mã nhanh hơn hệ mã hóa bất đối xứng.

1.2.3. Hệ mã hóa khóa bất đối xứng

1/. Khái niệm.

Hệ mã hóa khóa bất đối xứng là hệ mã hóa có khóa lập mã và giải mã khác nhau (ke $\neq$ kd), biết được khóa này cũng khó tính được khóa kia. Hệ mã này còn được gọi là hệ mã hóa khóa công khai.

Khóa lập mã cho công khai, gọi là khóa công khai. Khóa giải mã giữ bí mật, gọi là khóa bí mật.

2/. Đặc điểm.

a). Ưu điểm:

+ Thuật toán viết một lần, công khai cho nhiều lần dùng, nhiều người dùng, họ chỉ cần giữ bí mật khóa riêng của mình.

+ Khi biết các tham số ban đầu của hệ mã hóa, việc tính ra cặp khóa công khai và bí mật phải là "dễ".

+ Khả năng lộ khóa bí mật khó hơn vì chỉ có một người giữ.

+ Nếu thám mã biết khóa công khai và bản mã C, thì việc tìm ra bản rõ P là một bài toán "khó", số phép thử là vô cùng lớn, không khả thi.

b). Hạn chế: Mã hóa và giải mã chậm hơn hệ mã hóa khóa đối xứng.

3/. Ứng dụng:

Hệ mã hóa khóa công khai được sử dụng chủ yếu trên mạng công khai như internet, khi mà việc trao chuyển khóa bí mật tương đối khó khăn. Đặc trưng nổi bật của hệ mã hóa khóa công khai là cả khóa công khai và bản mã C đều có thể gửi đi trên một kênh thông tin không an toàn.

4/. Ví dụ: Mã hóa RSA, Elgamal.

1.3. KHÁI NIỆM CHỮ KÝ SỐ

1.3.1. Giới thiệu

Trong môi trường mạng, giải thuật mật mã khóa công khai không chỉ dùng vào việc bảo đảm tính bí mật của thông điệp, mà còn là phương tiện để bảo đảm tính xác thực và tính toàn vẹn của thông điệp, ngăn chặn sự giả mạo, sự thay đổi.

1/. Khái niệm.

Sơ đồ ký là bộ năm (P, A, K, S, V), trong đó:

+ P là tập hữu hạn các văn bản có thể.

+ A là tập hữu hạn các chữ ký có thể.

+ K là tập hữu hạn các khóa có thể.

+ S là tập các thuật toán ký.

+ V là tập các thuật toán kiểm thử.

Với khóa k $\in$ K:

Có thuật toán ký $sig_k \in S$, sig_k: P $\rightarrow$ A.

Có thuật toán kiểm tra chữ ký $ver_k \in V$, ver_k: P $\times$ A $\rightarrow$ {đúng, sai}.

Thỏa mã điều kiện sau với mọi x $\in$ P, y $\in$ A:

$$Ver_k(x, y) = \begin{cases} Đúng, \ nếu \ y = Sig_k(x) \\ Sai, \ nếu \ y \neq Sig_k(x) \end{cases}$$

2/. Ví dụ.

+ Chữ ký RSA.

+ Chữ ký Elgamal.

1.3.2. Một số loại chữ ký số

1.3.2.1. Chữ ký RSA

1/. Sơ đồ chữ ký RSA:

+ Sinh khóa:

Chọn p, q là số nguyên tố lớn.

Tính n = p * q, $\phi(n)$= (p - 1)(q - 1). Đặt P = C = Z_n.

Chọn khóa công khai b < $\phi(n)$ và nguyên tố cùng nhau với $\phi(n)$. Khóa bí mật a là nghịch đảo của b theo modulo $\phi(n)$: $a = b^{-1} \pmod{\phi(n)}$.

{n, b} công khai, {a, p, q} bí mật.

+ Ký số :

Chữ ký trên x $\in$ P là y $\in$ A:

$$y = sign_a(x) = x^a \bmod n. \qquad [1.2]$$

+ Kiểm tra chữ ký.

$$Ver_b(x,y) = true \leftrightarrow x = y^b \bmod n.$$

2/. Ví dụ.

Chọn p = 3, q = 5; n = p*q = 15, $\phi(n) = (p - 1)*(q - 1) = 2 * 4 = 8$.

Chọn b = 3 (nguyên tố cùng nhau với $\phi(n)$); Khóa bí mật a = 3 là phần tử nghịch đảo của b theo mod $\phi(n)$.

Ký số: Chữ ký trên x = 2 $\in$ P là

$$Y = Sig_k(x) = x^a \pmod{n} = 2^3 \bmod 15 = 8$$

Kiểm tra chữ ký : $Ver_k(x, y)$ = đúng $\leftrightarrow x \equiv y^b \bmod n$

$\leftrightarrow 2 = 8^3 \bmod 15$

1.3.2.2. Chữ ký Elgamal

1/. Sơ đồ chữ ký Elgamal.

+ Sinh khóa:

Cho p là số nguyên tố sao cho bài toán logarit rời rạc trên Z_p là khó giải.

Đặt $P = Z_p^*$, $A = Z_p^* \times Z_{p-1}$.

Chọn phần tử nguyên thủy g, chọn khóa bí mật $a \in Z_p^*$.

Khóa công khai $h \equiv g^a \bmod p$.

Tập khóa $K = \{(p, g, a, h): h \equiv g^a \bmod p\}$

{p, g, h} công khai, a bí mật

+ Ký số:

Chọn $r \in Z_{p-1}^*$.

Chữ ký trên $x \in P$ là $y = Sig_k(x, r) = (y_1, y_2)$, $y \in A$.

Trong đó $y_1 \in Z_p^*$, $y_2 \in Z_{p-1}$:

$y_1 = g^r \bmod p$

$y_2 = (x - a * y_1) * r^{-1} \bmod (p-1)$

+ Xác minh chữ ký

$Ver_k(x, y_1, y_2)$ = đúng $\leftrightarrow h^{y_1} * y_1^{y_2} = g^x \bmod p$

2/. Ví dụ.

+ Sinh khóa**:** Cho p=467, a =127, g =2, $h = g^a \bmod p = 132$.

+ Ký số trên bản rõ x = 100 với r được chọn = 213.

$y_1 = 2^{213} \bmod 467 = 29$.

$y_2 = (100 - 127 * 29)\ 431 \bmod 466 = 51$.

+ Xác minh chữ ký:

$132^{29} * 29^{51} = 2^{100} \bmod 467$.

Chữ ký trên là đúng.

1.3.2.3. Chữ ký Mù

1/. Giới thiệu.

Phương pháp Bỏ phiếu điện tử dựa trên chữ ký mù là cách tiếp cận dễ hiểu nhất và tực nhiên nhất vì nó gần với tư tưởng của bỏ phiếu truyền thống.

Trong bỏ phiếu thông thường:

+ Khi đi bỏ phiếu theo phương pháp truyền thống mà ngày nay đa phần vẫn đang áp dụng, cử tri mang giấy tờ cá nhân và lá phiếu chưa có nội dung đến ban đăng ký. Ở đó, ban đăng ký sẽ kiểm tra giấy tờ để xác minh quyền bỏ phiếu, nếu hợp lệ thì đóng dấu xác thực trên lá phiếu trắng chưa có nội dung.

+ Sau đó, cử tri vào phòng bỏ phiếu, cất hết các giấy tờ cá nhân đi, như vậy lá phiếu hoàn toàn không có thông tin định danh. Công việc cuối cùng là điền nội dung vào lá phiếu và bỏ vào hòm. Quá trình bỏ phiếu truyền thống này được gọi là nặc danh nếu những người tham gia đều tuân thủ đúng quy định.

Trong bỏ phiếu điện tử:

+ Cử tri V_i tạo một số ngẫu nhiên x_i đủ lớn làm bí danh của mình. Vì x_i được tạo ngẫu nhiên nên nó sẽ không có liên quan gì đến V_i.

+ Khi V_i trình các giấy tờ hợp lệ thì cơ quan đăng ký sẽ ký lên bí danh x_i của anh ta. Nếu V_i đưa trực tiếp x_i cho Ban đăng ký, thì lập tức họ xác lập được mối liên hệ giữa V_i và x_i, điều này anh ta thực sự không muốn.

Vì vậy, cử tri tiến hành làm mù bí danh của mình bằng cách biến đổi x_i thành z_i = blind (x_i) trước khi đưa cho Ban đăng ký ký.

+ Ban đăng ký sẽ ký và trao chữ ký $y = sig(z_i) = sig(blind(x_i))$ cho V_i.

Lúc này V_i sẽ xóa mù chữ ký trên y được $sig(x_i)$ là chữ ký mà cử tri mong muốn có. Vì cơ quan cung cấp chữ ký cho x nhưng hoàn toàn không biết nội dung về x nên người ta gọi là chữ ký mù (blind signature).

2/. Sơ đồ chữ ký mù RSA.

+ *Sinh khóa.*

Chọn p, q là số nguyên tố lớn. Tính n = p * q, $\phi(n)$= (p - 1)(q - 1). Đặt P = C = Z_n.

Chọn khóa công khai b < $\phi(n)$ và nguyên tố cùng nhau với $\phi(n)$. Khóa bí mật a là nghịch đảo của b theo modulo $\phi(n)$: $a = b^{-1} \pmod{\phi(n)}$.

{n, b} công khai, {a, p, q} bí mật.

+ *Làm mù:* Chọn tham số r ngẫu nhiên, r $\in$ Z_n.

Làm mù x thành z:

$z = blind(x) = x.r^b \pmod n$ với tham số r ngẫu nhiên thuộc Z_n.

+ *Ký số:* Chữ ký trên z là y $\in$ P:

$y = sign_k(blind(x)) = sign(x.r^b) = x^a . (r^b)^a = x^a.r \pmod n$.

+ *Xóa mù:* Xóa mù trên y để có chữ ký trên x:

$sign(x) = unblind(y) = y * r^{-1} = x^a . r * r^{-1} = x^a \pmod n$

+ *Kiểm tra chữ ký*: $Ver_k(x, y) = true \Leftrightarrow x \equiv (unblind(y))^b \pmod n$

3/. Ví dụ :

+ *Sinh khóa:* Chọn p= 3, q= 5, n= p * q = 15, $\phi(n) = (p - 1) * (q - 1) = 8$.

Chọn b=3 (nguyên tố cùng nhau với Φ(n)); a = 3 (phần tử nghịch đảo của b theo Φ(n)).

+ *Làm mù:* làm mù x = 8 thành z sử dụng tham số r = 2.

$z = blind(x) = x * r^b \pmod n = 8 * 2^3 \pmod{15} = 4$.

+ *Ký số:* $y = sign(z) = z^a = 4^3 \pmod{15} = 4$.

+ *Xóa mù:* $unblind(y) = y * r^{-1} = 4 * 8 \pmod{15} = 2$.

+ *Kiểm tra chữ ký:* $8 = 2^3 \bmod 15$.

1.4. VẤN ĐỀ VỀ AN TOÀN THÔNG TIN

Ngày nay, sự xuất hiện Internet và mạng máy tính đã giúp cho việc trao đổi thông tin trở nên nhanh gọn, dễ dàng. Tuy nhiên lại phát sinh thêm những vấn đề mới.Thông tin quan trọng có thể bị trộm cắp, bị làm sai lệch, bị giả mạo.

1.4.1. Bảo đảm bí mật (Bảo mật)

Thông tin không bị lộ với người không được phép.

Vấn đề bào mật được giải quyết bằng nhiều cách, cách phổ biến nhất là mã hóa.

1.4.2. Bảo đảm toàn vẹn (Bảo toàn)

Ngăn chặn hay hạn chế việc bổ sung, loại bỏ và sửa dữ liệu mà không được phép.

1.4.3. Bảo đảm xác thực (Chứng thực)

Xác thực đúng danh tính của thực thể cần kết nối và giao dịch chẳng hạn một người, một máy tính cuối trong mạng, một thẻ tín dụng,...

Xác thực đúng thực thể có trách nhiệm về nội dung của thông tin (xác thực nguồn gốc thông tin).

1.4.4. Bảo đảm sẵn sàng

Thông tin sẵn sàng cho người dùng hợp pháp.

1.5. VẤN ĐỀ BỎ PHIẾU ĐIỆN TỬ

1.5.1. Khái niệm bỏ phiếu điện tử

Xã hội dân chủ có nhiều việc phải cần đến "bỏ phiếu" như: để thăm dò các kế hoạch, để bầu cử các chức vị, chức danh,… Nhưng quĩ thời gian của người ta không có nhiều, mặt khác một người có thể làm việc tại nhiều nơi, như vậy người ta khó có thể thực hiện được nhiều cuộc "bỏ phiếu" theo phương pháp truyền thống.

Rõ ràng "bỏ phiếu từ xa" đang và sẽ là nhu cầu cấp thiết, vấn đề trên chỉ còn là thời gian và kỹ thuật cho phép. Đó là cuộc "bỏ phiếu" được thực hiện từ xa trên mạng máy tính thông qua các phương tiện "điện tử" như máy tính cá nhân, điện thoại di động… Như vậy, mọi người trong cuộc "không thể nhìn thấy mặt nhau" và các "lá phiếu" được chuyển từ xa trên mạng máy tính tới "hòm phiếu".

Cũng như cuộc bỏ phiếu truyền thống, cuộc bỏ phiếu từ xa phải bảo đảm yêu cầu: " bí mật", "toàn vẹn" và "xác thực" của lá phiếu; mỗi cử tri chỉ được bỏ phiếu một lần, mọi người đều có thể kiểm tra tính đúng đắn của cuộc bỏ phiếu, cử tri không thể chỉ ra mình đã bỏ phiếu cho ai…

Yêu cầu bí mật của lá phiếu: ngoài cử tri, chỉ có ban kiểm phiếu mới được biết nội dung lá phiếu, nhưng họ lại không thể biết ai là chủ nhân của nó.

Yêu cầu toàn vẹn của lá phiếu: trên đường truyền tin, nội dung lá phiếu không thể bị thay đổi, tất cả các lá phiếu đều được chuyển tới hòm phiếu an toàn, đúng thời gian, chúng được kiểm phiếu đầy đủ.

Yêu cầu xác thực của lá phiếu: lá phiếu gửi tới hòm phiếu phải hợp lệ, đúng là của người có quyền bỏ phiếu, cử tri có thể nhận ra lá phiếu của họ.

1.5.2. So sánh bỏ phiếu điện tử và bỏ phiếu thông thường

1/. Bỏ phiếu thông thường.

a). Khái niệm.

Cử tri (người bỏ phiếu) phải trực tiếp đến địa điểm bỏ phiếu, trực tiếp đăng ký bỏ phiếu, viết phiếu và bỏ vào thùng phiếu, sau đó ban quản lý phải trực tiếp kiểm phiếu.

b). Ví dụ:

Bỏ phiếu bầu hội đồng nhân dân. Cử tri đi bỏ phiếu phải mang theo thẻ cử tri đến các địa điểm bỏ phiếu để đăng ký quyền bỏ phiếu rồi ghi lựa chọn ứng cử viên hội đồng vào lá phiếu và gửi vào hòm phiếu.

2/. Bỏ phiếu từ xa.

a). Khái niệm.

Các công việc từ đăng ký ,bỏ phiếu đến kiểm phiếu đều được thực hiện gián tiếp từ xa trên mạng máy tính qua các phương tiện điện tử như máy tính cá nhân, điện thoại di động,... Các lá phiếu số được chuyển tự động trên mạng tới hòm phiếu điện tử.

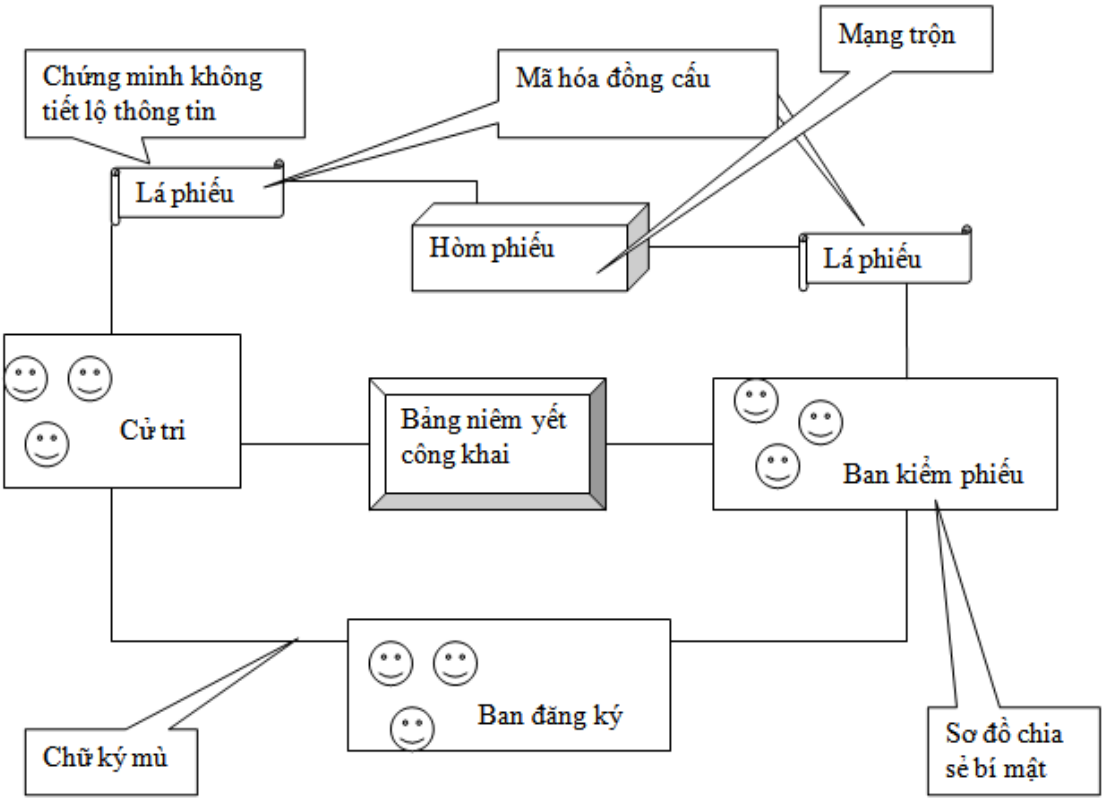
Trong bỏ phiếu từ xa phải áp dụng thêm các kỹ thuật mã hóa, ký số,... để bảo đảm an toàn thông tin.

b). Ví dụ.

Bỏ phiếu thăm dò quan điểm người dùng về giao diện trang vietnamnet.vn. Người dùng chỉ cần tích chọn (ưa nhìn, bình thường, quá sặc sỡ).

1.5.3. Các giai đoạn bỏ phiếu điện tử

Bỏ phiếu điện tử bao gồm 3 giai đoạn chính: Đăng ký, bỏ phiếu, kiểm phiếu.



Hình 1.1 Sơ đồ Quy trình bỏ phiếu điện tử.

1/. Giai đoạn đăng ký.

Cử tri:

- Chọn bí mật định danh x, rồi làm mù x thành bí danh y = blind (x).

- Cử tri gửi tới ban đăng ký chứng minh thư điện tử, bí danh y.

Ban đăng ký:

- Kiểm tra chứng minh thư (CMT), bí danh y của cử tri.

- Nếu hợp lệ (cử tri chưa đăng ký bỏ phiếu lần nào, chưa có ai đăng ký bí danh đó) thì ban đăng ký sẽ ra lệnh cho hệ thống ký lên y. Đó là chữ ký z = sign (y)

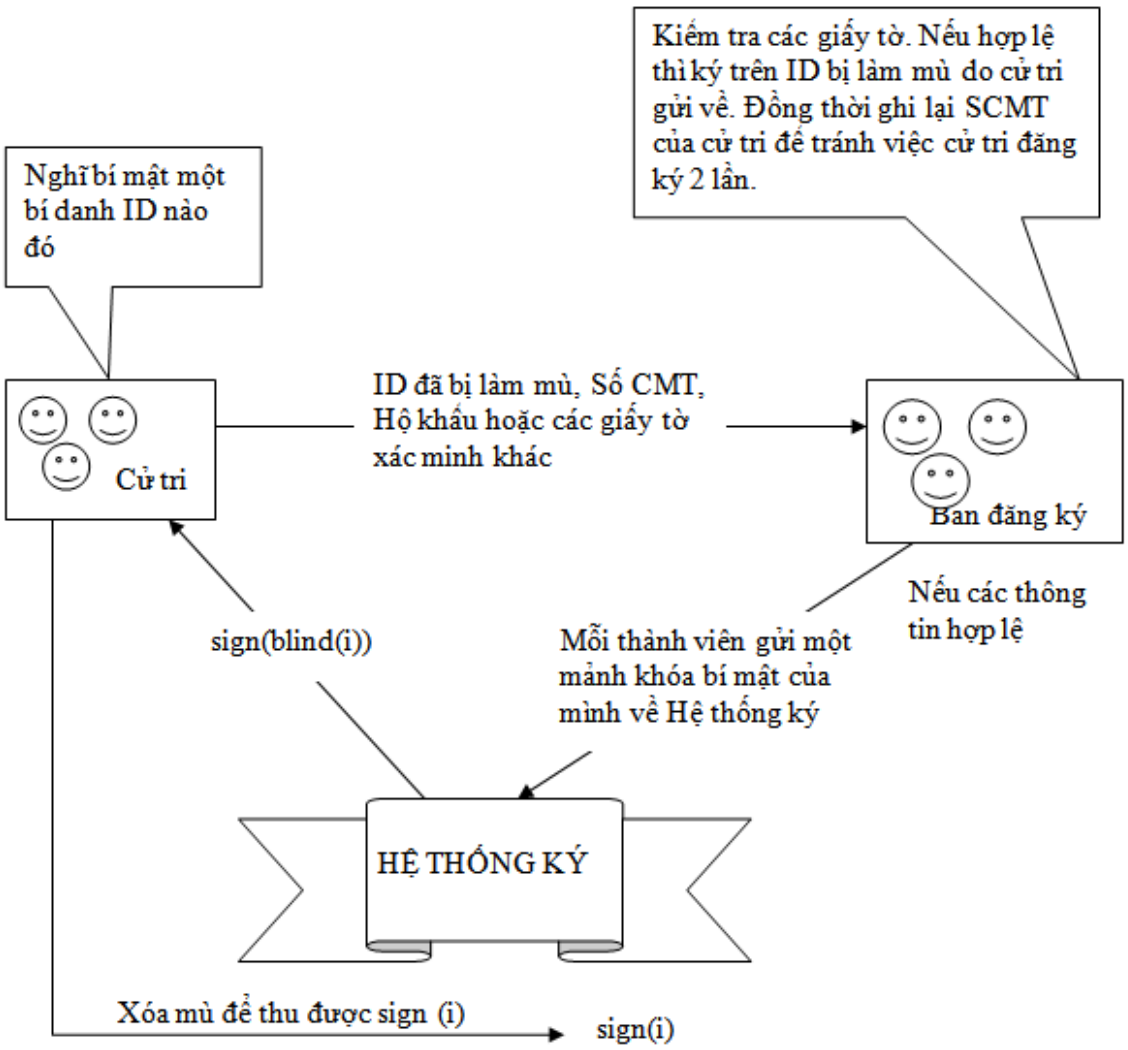
- Ban đăng ký ghi lại số chứng minh thư (SCMT), bí danh y và chữ ký z vào sổ đăng ký.

- Ban đăng ký gửi trả chữ ký z về cho cử chi.

Cử tri:

- Khi nhận được chữ ký z, cử tri xóa mù trên z sẽ nhận được chữ ký sign(x) trên định danh thật x.

- Cử tri có thể kiểm tra chữ ký của ban đăng ký trên định danh của mình có hợp lệ hay không bằng cách dùng khóa công khai của ban đăng ký.



Hình 1.2 Sơ đồ giai đoạn đăng ký bỏ phiếu.

2/. Giai đoạn bỏ phiếu.

Cử tri:

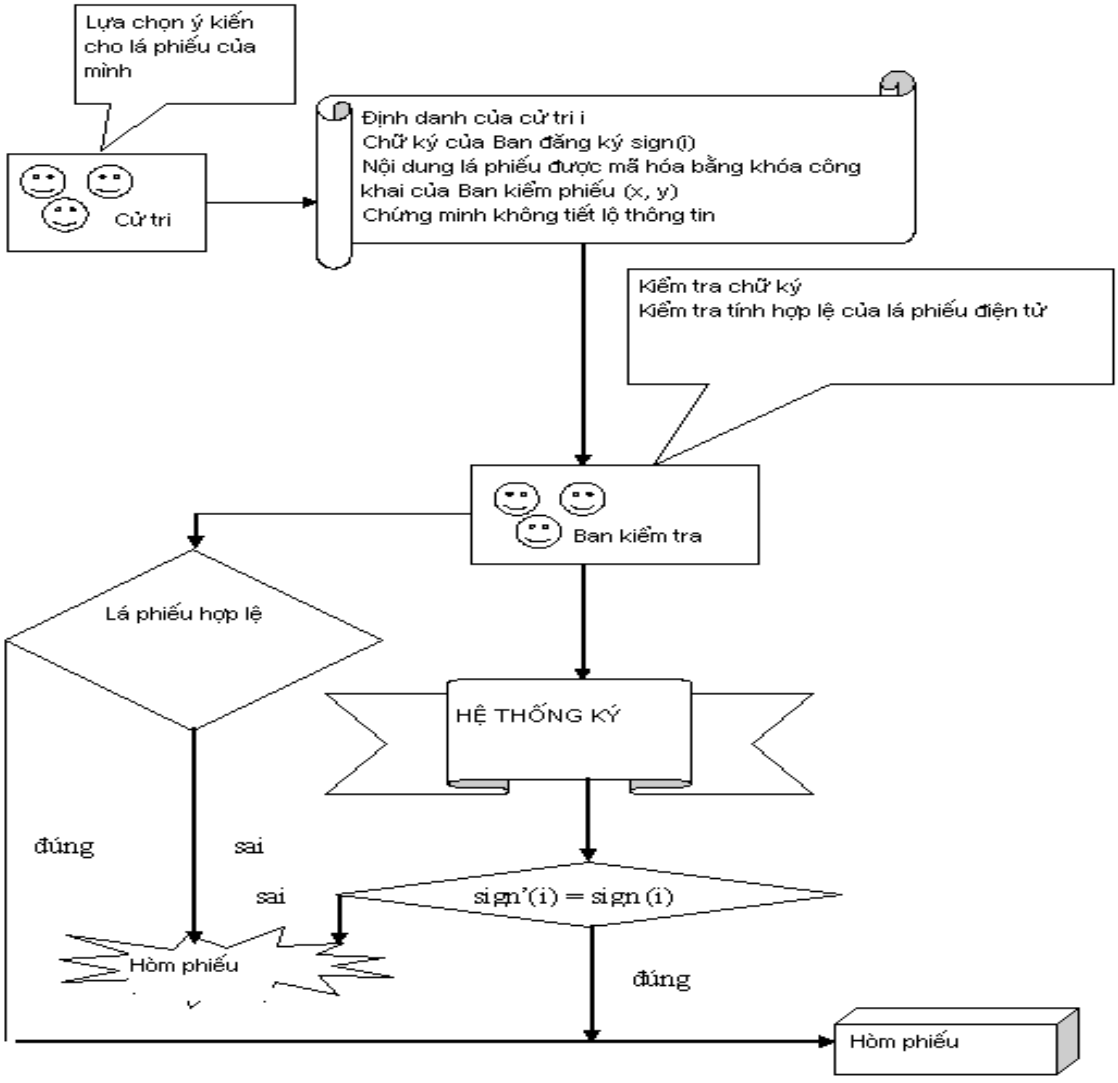
- Ghi thông tin sau đó mã hóa lá phiếu bằng khóa công khai của ban kiểm phiếu.

- Gửi lá phiếu đã mã hóa, định danh thật x, chữ ký z, " chứng minh không tiết lộ thông tin" của lá phiếu.

Ban kiểm tra:

- Kiểm tra tính hợp lệ của lá phiếu, kiểm tra chữ ký trên lá phiếu.

- Gửi lá phiếu đến hòm phiếu.



Hình 1.3 Sơ đồ giai đoạn bỏ phiếu.

3/. Giai đoạn kiểm phiếu.

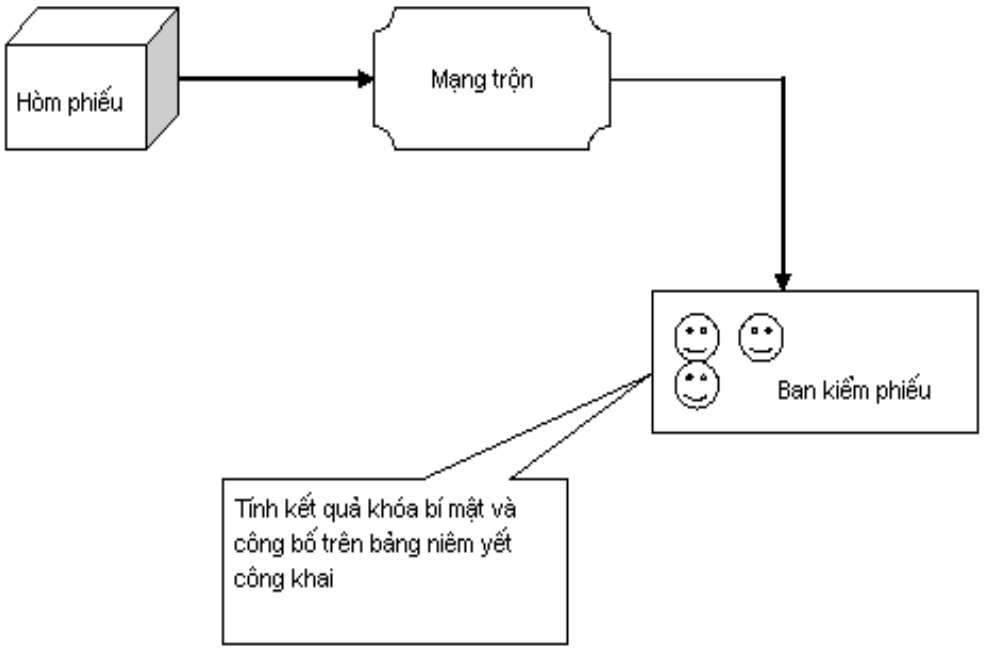
- Các lá phiếu sẽ được trộn nhờ kỹ thuật trộn trước khi chúng được chuyển về ban kiểm phiếu, nhằm giữ bí mật danh tính cho các cử tri.

- Ban kiểm phiếu tính kết quả dựa vào các lá phiếu gửi về.

- Theo phương pháp mã hóa đồng cấu, ban kiểm phiếu không cần giải mã từng lá phiếu, vẫn kiểm phiếu được (chỉ áp dụng với loại bỏ phiếu: chọn 1 trong 2).

- Khi kiểm phiếu, các thành viên ban kiểm phiếu dùng các mảnh khóa riêng của mình để khôi phục khóa bí mật, ban kiểm phiếu dùng khóa bí mật này để tính kết quả cuộc bầu cử.

- Ban kiểm phiếu thông báo kết quả lên bảng niêm yết công khai.



Hình 1.4 Sơ đồ giai đoạn kiểm phiếu.

Chương 2. GIẢI QUYẾT MỘT SỐ BÀI TOÁN TRONG GIAI ĐOẠN ĐĂNG KÝ BỎ PHIẾU ĐIỆN TỬ

2.1. MỘT SỐ BÀI TOÁN TRONG GIAI ĐOẠN ĐĂNG KÝ BỎ PHIẾU

2.1.1. Bài toán xác thực cử tri bỏ phiếu

Trong quá trình đăng ký bỏ phiếu điện tử để BDK có thể cấp quyền bầu cử cho CT (bằng cách ký lên định danh lá phiếu) thì BDK phải xác thực được thông tin của CT có đáp ứng được yêu cầu của cuộc bầu cử (ví dụ như CT phải là công dân việt nam, trên 18 tuổi, trong cuộc bỏ phiếu đang diễn ra thì đây là lần đầu…).

Vấn đề nảy sinh :

Nhưng vấn đề đặt ra là làm thế nào để xác thực được CT tham gia đăng ký đúng là người có thông tin như vậy trong môi trường mạng từ xa.

Phương pháp giải quyết :

Sử dụng các kỹ thuật chứng minh thư điện tử, mã hóa, hàm băm, chữ ký số.

2.1.2. Bài toán ẩn danh lá phiếu

Lá phiếu hợp lệ là lá phiếu có chữ ký của BDK trên định danh.

Vấn đề nảy sinh :

Nếu CT để lộ định danh lá phiếu của mình với BDK trong khi BDK đã biết CT (biết thông tin nhận dạng, chứng minh thư,…) thì lá phiếu sẽ bị lộ danh tính dẫn đến các việc mờ ám trong bỏ phiếu như: để lộ thông tin chủ nhân lá phiếu khiến các ứng cử viên có thể mua bán phiếu, bị kẻ gian sử dụng định danh để bỏ phiếu...

Phương pháp giải quyết : Sử dụng *chữ ký mù*.

2.1.3. Bài toán phòng tránh sự liên kết của nhân viên Ban bầu cử và Cử tri

Trong quá trình đăng ký chỉ có sự tham gia của hai bên là thành viên trong ban bầu cử và CT.

Vấn đề nảy sinh :

CT có thể cấu kết với thành viên trong ban bầu cử để cấp chữ ký cho mình trong khi mình không đủ điều kiện bỏ phiếu.

Phương pháp giải quyết :

Cho nên người ta đã áp dụng quy tắc BDK không thể cấp chữ ký cho CT nếu như không có sự chấp thuận của tất cả các thành viên trong BDK (CT có thể cấu kết với nhiều người trong BDK, nhưng khó có thể mua chuộc cả BDK).

- Bằng kỹ thuật *chia sẻ khóa bí mật* các thành viên trong BDK, mỗi người sẽ có một mảnh khóa. Chỉ khi nào tất cả cùng đồng ý thì mới ghép lại thành 1 khóa ký hoàn chỉnh dùng để ký.

- Kỹ thuật: *chữ ký nhóm mù.*

2.2. GIẢI QUYẾT CÁC BÀI TOÁN TRÊN

2.2.1. Bài toán xác thực cử tri bỏ phiếu

Kỹ thuật áp dụng: Chứng minh thư điện tử.

Mỗi người khi muốn tham gia bầu cử phải có giấy chứng nhận số quốc gia (national digital certificate) được cấp bởi một cơ quan chứng thực số (Certificate Authority - CA), được lưu trữ trên 1 thiết bị lưu trữ (e-token USB driver – loại thiết bị đặc biệt kết nối với máy tính bằng chuẩn USB, lưu trữ cặp khóa công khai và khóa bí mật của chứng nhận số)

+ Đầu tiên cử tri phải gửi khóa công khai có trong thiết bị lưu trữ (USB flash) của mình tới máy chủ đăng ký.

+ Máy chủ xác thực cử tri bằng cách sử dụng challenge/response thông tin để xác thực xem người gửi khóa có phải là chủ nhân của khóa không(nếu người gửi khóa không vượt qua được challenge/response, hoặc cặp khóa công khai của người gửi không đạt đủ điều kiện đăng ký bỏ phiếu thì phiên làm việc sẽ kết thúc)

+ Máy chủ sẽ gửi thông tin tới CA để xác thực.

+ Nếu thông tin là đúng CA sẽ gửi lại thông tin của cử tri cho máy chủ.

+ Máy chủ sẽ kiểm tra thông tin đó dựa trên các quy định mà cuộc bầu cử hiện hành đề ra để quyết định xem cử tri có đạt đủ điều kiện hay không (nếu không hợp lệ thì kết thúc phiên). Sau đó gửi lại chứng nhận hợp lệ và lưu thông tin của cử tri vào trong sổ đăng ký.

2.2.2. Bài toán ẩn danh lá phiếu

Kỹ thuật áp dụng: Chữ ký mù (trình bày chi tiết trong mục 1.3.2.3).

Trong bỏ phiếu thông thường:

+ Khi đi bỏ phiếu theo phương pháp truyền thống mà ngày nay đa phần vẫn đang áp dụng, cử tri mang giấy tờ cá nhân và lá phiếu chưa có nội dung đến ban đăng ký. Ở đó, ban đăng ký sẽ kiểm tra giấy tờ để xác minh quyền bỏ phiếu, nếu hợp lệ thì đóng dấu xác thực trên lá phiếu trắng chưa có nội dung.

+ Sau đó, cử tri vào phòng bỏ phiếu, cất hết các giấy tờ cá nhân đi, như vậy lá phiếu hoàn toàn không có thông tin định danh. Công việc cuối cùng là điền nội dung vào lá phiếu và bỏ vào hòm. Quá trình bỏ phiếu truyền thống này được gọi là nặc danh nếu những người tham gia đều tuân thủ đúng quy định.

Trong bỏ phiếu điện tử:

+ Cử tri V_i tạo một số ngẫu nhiên x_i đủ lớn làm bí danh của mình. Vì x_i được tạo ngẫu nhiên nên nó sẽ không có liên quan gì đến V_i.

+ Khi V_i trình các giấy tờ hợp lệ thì cơ quan đăng ký sẽ ký lên bí danh x_i của anh ta. Nếu V_i đưa trực tiếp x_i cho Ban đăng ký, thì lập tức họ xác lập được mối liên hệ giữa V_i và x_i, điều này anh ta thực sự không muốn.

Vì vậy, cử tri tiến hành làm mù bí danh của mình bằng cách biến đổi x_i thành z_i = blind (x_i) trước khi đưa cho Ban đăng ký ký.

+ Ban đăng ký sẽ ký và trao chữ ký $y = sig(z_i) = sig(blind(x_i))$ cho V_i.

Lúc này V_i sẽ xóa mù chữ ký trên y được $sig(x_i)$ là chữ ký mà cử tri mong muốn có. Vì cơ quan cung cấp chữ ký cho x nhưng hoàn toàn không biết nội dung về x nên người ta gọi là chữ ký mù (blind signature).

2.2.3. Bài toán phòng tránh sự liên kết của nhân viên Ban bầu cử và Cử tri

Kỹ thuật áp dụng: Sơ đồ ngưỡng Shamir để chia sẻ khóa bí mật.

1/. Chia sẻ khóa.

a). Khái niệm:

Sơ đồ chia sẻ bí mật dùng để chia sẻ một thông tin cho m thành viên, sao cho chỉ dùng những tập con hợp thức các thành viên mới có thể khôi phục lại thông tin bí mật, còn lại không ai có thể làm việc đó.

b). Sơ đồ:

Cho t, m nguyên dương, $t \leq m$. Sơ đồ ngưỡng A(t, m) là phương pháp phân chia bí mật k cho một tập gồm m thành viên, sao cho t thành viên bất kỳ có thể tính được k, nhưng không một nhóm gồm (t - 1) thành viên nào có thể làm được điều đó. Người phân chia các mảnh khóa không được nằm trong sô m thành viên trên.

+ Khởi tạo:

Chọn số nguyên tố p.

Chọn m phần tử x_i khác nhau ($1 \leq i \leq m$, $x_i \neq 0$, $x_i, m \in Z_p$).

Trao x_i cho thành viên P_i. Giá trị x_i là công khai.

+ Phân phối:

Phân phối $k \in Z_p$. Chọn t -1 phần tử $\in Z_p$: $a_1, a_2, \ldots, a_{t-1}$.

Với $1 \leq i \leq m$, tính:

$y_i = P(x_i)$, $P(x) = k + \sum_{j=1}^{t-1} a_j x_j^j \ mod \ p.$

Với $1 \leq i \leq m$, trao y_j cho thành viên P_i.

Kết thúc, mỗi thành viên P_i sẽ có 1 cặp khóa (x_i, y_i) sử dụng để khôi phục khóa.

2/.Khôi phục khóa:

Để tìm ra khóa bí mật từ các mảnh khóa trên ta phải giải được hệ t phương trình t ẩn để tìm ra các nghiệm của hệ phương trình. Bằng cách sử dụng giải thuật khử Gauss.

Giải thuật khử Gauss : Được biểu diễn thông qua các bước thực hiện đối với một hệ phương trình tuyến tính n ẩn n phương trình tổng quát như sau:

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & & a_{1j} & & a_{1n} \\ a_{21} & a_{22} & a_{23} & & a_{2j} & & a_{2n} \\ a_{31} & a_{32} & a_{33} & & a_{3j} & & a_{3n} \\ \vdots & \vdots & \vdots & \dots & \vdots & \dots & \vdots \\ a_{i1} & a_{i2} & a_{i3} & & a_{ij} & & a_{in} \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ a_{n1} & a_{n2} & a_{n3} & & a_{nj} & & a_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_i \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \\ b_i \\ \vdots \\ b_n \end{bmatrix}$$

Bước 1. Sử dụng phương trình thứ nhất (hàng 1) để loại x_1 ra khỏi các phương trình còn lại. Làm cho các phần tử từ hàng 2 đến hàng thứ *n* của cột 1 bằng không nhờ phép biến đổi (2.2):

$$\begin{cases} a_{ij} = a_{ij} - \frac{a_{i1}}{a_{11}} a_{1j} \\ b_i = b_i - \frac{a_{i1}}{a_{11}} b_1 \end{cases} \qquad (2.2)$$

Trong đó: i, j = 2, 3, …, n.

Ta được kết quả:

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & & a_{1j} & & a_{1n} \\ 0 & a_{22} & a_{23} & & a_{2j} & & a_{2n} \\ 0 & a_{32} & a_{33} & & a_{3j} & & a_{3n} \\ \vdots & \vdots & \vdots & \dots & \vdots & \dots & \vdots \\ 0 & a_{i2} & a_{i3} & & a_{ij} & & a_{in} \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & a_{n2} & a_{n3} & & a_{nj} & & a_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_i \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \\ b_i \\ \vdots \\ b_n \end{bmatrix}$$

Bước 2. Tương tự sử dụng phương trình thứ hai (hàng 2) để loại x_2 ra khỏi các phương trình từ hàng 3 trở đi.

Bước k. Một cách tổng quát, tại bước thứ k ta có hệ phương trình đầu vào:

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & & a_{1k} & & a_{1j} & & a_{1n} \\ 0 & a_{22} & a_{23} & & a_{2k} & & a_{2j} & & a_{2n} \\ 0 & 0 & a_{33} & & a_{3k} & & a_{3j} & & a_{3n} \\ \vdots & \vdots & \vdots & & \vdots & & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & a_{kk} & \dots & a_{kj} & \dots & a_{kn} \\ \vdots & \vdots & \vdots & & \vdots & & \vdots & & \vdots \\ 0 & 0 & 0 & & a_{ik} & & a_{ij} & & a_{in} \\ \vdots & \vdots & \vdots & & \vdots & & \vdots & & \vdots \\ 0 & 0 & 0 & & a_{nk} & & a_{nj} & & a_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_k \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \\ b_k \\ \vdots \\ b_n \end{bmatrix}$$

Ở bước này, để loại x_k ra khỏi các phương trình ta sử dụng

$$\begin{cases} a_{ij} = a_{ij} - \frac{a_{ik}}{a_{kk}} a_{kj} \\ b_i = b_i - \frac{a_{ik}}{a_{kk}} b_k \end{cases} \quad (2.3)$$

Trong đó: i, j = k, k+1, …, n

Bước n-1. Sau n-1 bước như trên, chúng ta nhận được kết quả:

$$\begin{bmatrix} a_{[1][1]} & a_{[1][2]} & a_{[1][3]} & & a_{[1][n-1]} & a_{[1][n]} \\ 0 & a_{[2][2]} & a_{[2][3]} & & a_{[2][n-1]} & a_{[2][n]} \\ 0 & 0 & a_{[3][3]} & \dots & a_{[3][n-1]} & a_{[3][n]} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & & a_{[n-1][n-1]} & a_{[n][n-1]} \\ 0 & 0 & 0 & & 0 & a_{[n][n]} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_{n-1} \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \\ b_{n-1} \\ b_n \end{bmatrix}$$

Bằng phương pháp thế ngược từ dưới lên ta nhận được các nghiệm của hệ phương trình như sau:

$$x_n = \frac{b_n}{a_{nn}}$$

$$x_i = \frac{b_i - \sum_{j=i+1}^{n} a_{ij} x_j}{a_{ii}} \quad (2.4)$$

Trong đó: i = n – 1, n – 2, …, 1

3/. Ví dụ.

Chọn số nguyên tố p =17. Cần chia sẻ khóa k = 13. Trong bỏ phiếu điện tử thì số người cần thiết để tìm lại khóa ký trong ban đăng ký là tất cả các thành viên.

↔ t = m = 3. Phần tử x_i = i trong Z_p, i = 1, 2, 3.

Chọn bí mật, ngẫu nhiên t – 1 phần tử trong Z_p: $a_1 = 10$, $a_2 = 2$.

Tính $y_i = P(x_i)$, $1 \leq i \leq m$, trong đó:

$$P(x) = k + \sum_{j=1}^{t-1} a_j x_j^j \ (mod\ p) = 13 + a_1x + a_2 x^2 \ (\text{mod } 17).$$

$y_1 = 13 + 10 * 1 + 2 * 1 \text{ mod } 17 = 8.$

$y_2 = 13 + 10 * 2 + 2 * 4 \text{ mod } 17 = 7.$

$y_3 = 13 + 10 * 3 + 2 * 9 \text{ mod } 17 = 10.$

Trao khóa cho 3 thành viên (1, 8), (2, 7), (3, 10).

Để tìm lại khóa ban đầu, giải hệ 3 phương trình 3 ẩn:

$$\begin{cases} a_2 + a_1 + k = 8 \\ 4 * a_2 + 2 * a_1 + k = 7 \\ 9 * a_2 + 3 * a_1 + k = 10 \end{cases}$$

Phép khử Gauss:

$$\begin{bmatrix} 1 & 1 & 1 \\ 4 & 2 & 1 \\ 9 & 3 & 1 \end{bmatrix} \begin{bmatrix} a_2 \\ a_1 \\ k \end{bmatrix} = \begin{bmatrix} 8 \\ 7 \\ 10 \end{bmatrix}$$

Bước 1: Áp dụng công thức (2.2) ta có:

$b_2 = b_2 - \frac{a_{21}}{a_{11}} b_1 = 7 - \frac{4}{1} 8 = -25$, $b_3 = b_3 - \frac{a_{31}}{a_{11}} b_1 = 10 - \frac{9}{1} 8 = -62$

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & -2 & -3 \\ 0 & -6 & -8 \end{bmatrix} \begin{bmatrix} a_2 \\ a_1 \\ k \end{bmatrix} = \begin{bmatrix} 8 \\ -25 \\ -62 \end{bmatrix}$$

Tước 2: $b_3 = b_3 - \frac{a_{32}}{a_{22}} b_1 = -62 - \frac{-6}{-2}(-25) = 13$

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & -2 & -3 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} a_2 \\ a_1 \\ k \end{bmatrix} = \begin{bmatrix} 8 \\ -25 \\ 13 \end{bmatrix}$$

→ k = 13. (Khóa bí mật cần tìm).

Chương 3. THỬ NGHIỆM XÂY DỰNG HỆ THỐNG ĐĂNG KÝ BỎ PHIẾU

3.1. BÀI TOÁN.

Hệ thống bỏ phiếu điện tử cho công dân Việt Nam bỏ phiếu về việc đồng ý hay không đồng ý về một dự luật sắp được ban hành, hay cuộc bỏ phiếu lựa chọn 1 trong k người vào 1 vị trí nào đó.

Trước tiên ban bầu cử phải giới thiệu, đưa ra các thông tin về cuộc bỏ phiếu để cho cử tri (CT) đọc và tìm hiểu. Sau khi tìm hiểu, cử tri mới tiến hành bỏ phiếu.

Bỏ phiếu gồm 3 giai đoạn: Giai đoạn cử tri đăng ký với ban đăng ký (BDK) để có quyền bỏ phiếu, giai đoạn 2 là bỏ phiếu và giai đoạn 3 là kiểm phiếu.

1/. Đăng ký bỏ phiếu.

Thông tin về CT được lưu trong danh sách cử tri (số CMT, họ tên, địa chỉ)

Để đăng ký quyền bỏ phiếu, CT cần gửi thông tin cá nhân để xác thực và chọn cho mình 1 định danh gán lên lá phiếu (mỗi lá phiếu đều cần có một định danh), nhưng định danh đó phải được bảo mật đối với ban đăng ký, cho nên CT sẽ phải làm mù định danh đó thành bí danh.

Sau khi gửi bí danh, thông tin cá nhân đến cho ban đăng ký (gọi chung là thông tin đăng ký). CT sẽ phải chờ quyết định xác thực thông tin cử tri của tất cả các thành viên trong ban đăng ký.

BDK kiểm tra bí danh, chứng minh thư:

- Phản hồi nếu chứng minh thư điện tử hay bí danh không hợp lệ.

- Còn nếu hợp lệ thì lưu thông tin vào sổ đăng ký đồng thời ký lên bí danh, và gửi lại cho CT.

Chú ý : Việc lưu lại bí danh, chứng minh thư điện tử vào sổ đăng ký để kiểm tra những lần đăng ký sau. Chứng minh thư điện tử và bí danh không hợp lệ khi một CT đăng ký 2 lần (theo yêu cầu của cuộc bầu cử thì mỗi người chỉ được đăng ký 1 lần), hay 2 CT có bí danh trùng nhau (nếu bí danh trùng nhau sẽ có thể có 2 lá phiếu có cùng định danh).

Khi CT nhận được chữ ký của BDK trên bí danh thì CT sẽ tiến hành xóa mù để nhận được chữ ký của BDK trên định danh thật. Chữ ký này sẽ được CT sử dụng cho quá trình bỏ phiếu.

2/. Bỏ phiếu.

CT lựa chọn và ghi thông tin vào lá phiếu của mình. Để không bị lộ thông tin về bỏ phiếu, CT mã hóa nội dung lá phiếu, sau đó gửi nó đi kèm với định danh thật, và chữ ký của BDK đến cho ban kiểm tra (BKT). BKT sử dụng khóa ký của BDK để ký lên định danh rồi so sánh kết quả nếu không đúng chữ ký thì loại.

Sau đó kiểm tra xem định danh đó đã bỏ phiếu lần nào chưa.

Thông tin về bỏ phiếu sẽ được lưu trong sổ bỏ phiếu bao gồm thông tin định danh, thời gian bỏ phiếu.

Lá phiếu sẽ được lưu lại trong hòm phiếu, để sau đó có thể tiến hành kiểm phiếu.

3/. Kiểm phiếu.

Ban kiểm phiếu tính toán kết quả (việc tính toán này có thể không cần đến việc giải mã từng lá phiếu, mã hóa lá phiếu sử dụng thuật toán mã hóa đồng cấu có thể tính ra kết quả mà không cần giải mã các lá phiếu – áp dụng cho trường hợp chọn một trong hai).

Sau đó kết quả kiểm phiếu sẽ được thông báo qua bảng thông báo cho mọi người biết.

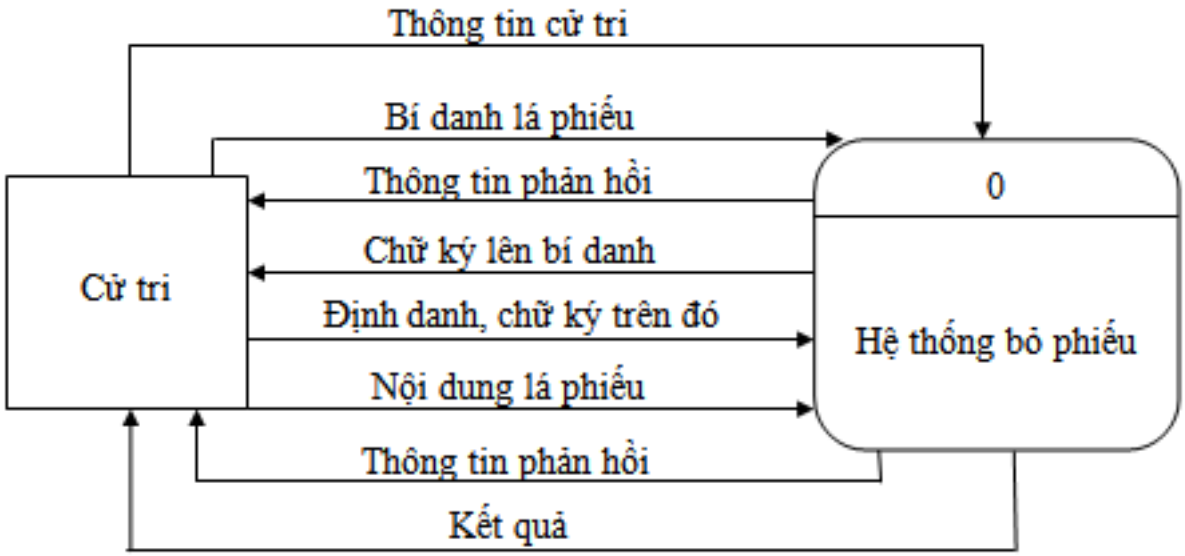
3.2. PHÂN TÍCH THIẾT KẾ HỆ THỐNG

3.2.1. Bảng phân tích

Bảng 3.1 bảng phân tích

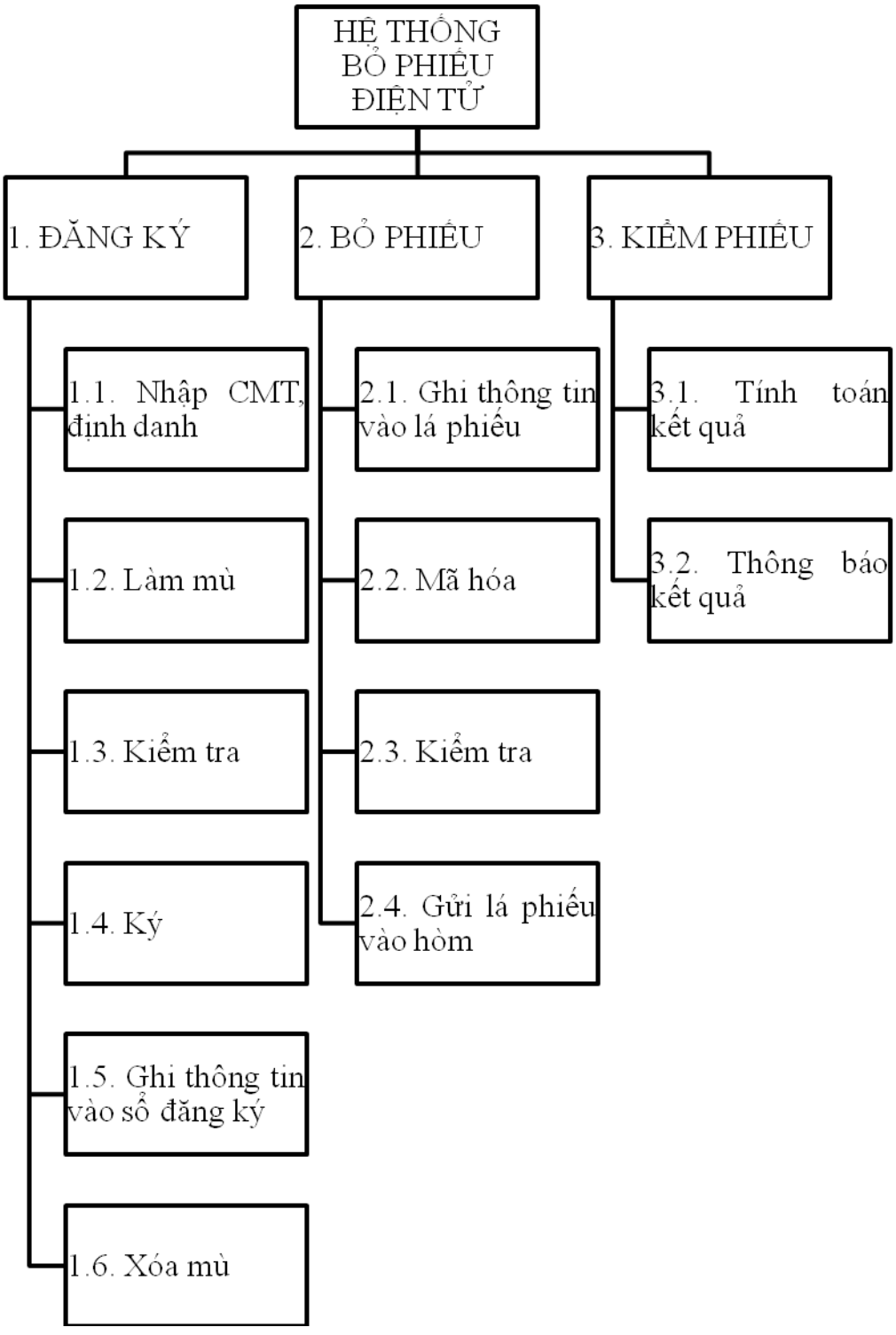
Động từ + Bổ ngữ		Danh từ	Nhận xét
Gửi	Chứng minh thư	CỬ TRI	Tác nhân ngoài
Kiểm tra	Chứng minh thư	BAN ĐĂNG KÝ	Tác nhân
Chọn	Định danh	Chứng minh thư	=
Làm mù	Định danh	Định danh	=
Kiểm tra	Bí danh	Bí danh	=
Ký	Bí danh	Chữ ký	=
Ghi	Thông tin vào sổ đăng ký	Sổ đăng ký	Hồ sơ dữ liệu
Xóa mù	Bí danh	Lá phiếu	Hồ sơ dữ liệu
Ghi	Nội dung lá phiếu	Sổ bỏ phiếu	Hồ sơ dữ liệu
Mã hóa	Nội dung	BAN ĐĂNG KÝ	Tác nhân
Lưu lại	Thông tin lá phiếu	Hòm phiếu	=
Kiểm tra	Chữ ký, định danh	Bảng thông báo	Hồ sơ dữ liệu
Tính toán	Lá phiếu		
Thông báo	Kết quả		

3.2.2. Biểu đồ ngữ cảnh



Hình 3.1 Biểu đồ ngữ cảnh.

3.2.3. Biểu đồ phân rã chức năng



Hình 3.2 Biểu đồ phân rã chức năng.

Mô tả chức năng lá **:**

(1.1) Nhập CMT, định danh

Để đăng ký quyền bỏ phiếu cử tri phải có chứng minh thư điện tử và phải chọn ngẫu nhiên một định danh.

(1.2) Làm mù định danh

Để không bị lộ định danh khi bỏ phiếu, định danh sẽ được cử tri làm mù thành bí danh.

(1.3) Kiểm tra CMT, bí danh

Khi cử tri gửi CMT, bí danh sang cho ban đăng ký, ban đăng ký sẽ kiểm tra xem CMT, bí danh của cử tri có hợp lệ không.

(1.4) Ký lên bí danh:

Khi CMT và bí danh là hợp lệ, ban đăng ký sẽ ký lên bí danh của cử tri và gửi chữ ký trở lại cho cử tri.

(1.5) Ghi thông tin vào sổ đăng ký

Đồng thời với việc gửi chữ ký trở lại cho cử tri, thì ban đăng ký sẽ lưu định danh và CMT vào sổ đăng ký.

(1.6) Xóa mù trên bí danh

Khi nhận được chữ ký từ ban Đăng ký trên bí danh, cử tri sẽ xóa mù trên bí danh này để nhận được chữ ký thật trên dịnh danh.

(2.1) Ghi thông tin vào lá phiếu

Cử tri ghi ý kiến của mình vào lá phiếu.

(2.2) Mã hóa nội dung lá phiếu

Để không bị lộ thông tin về sự lựa chọn của mình, cử tri sẽ mã hóa nội dung lá phiếu trước khi lá phiếu được chuyển tới hòm phiếu.

(2.3) Kiểm tra lá phiếu.

Trước khi lá phiếu số được chuyển đến hòm phiếu. Thì lá phiếu sẽ được kiểm tra chữ ký bằng cách gửi thông tin định danh lá phiếu và chữ ký trên lá phiếu đến cho ban kiểm tra. Ban kiểm tra sẽ xác định xem chữ ký đó có đúng là của ban đăng ký không.

Tiếp theo sẽ kiểm tra xem định danh đó đã bỏ phiếu lần nào chưa.

(2.4) Gửi lá phiếu vào hòm phiếu

Thông tin trong hòm phiếu lưu lại định danh, chữ ký, thời gian bỏ phiếu, nội dung.

(3.1) Tính toán kết quả

Khi các lá phiếu hợp lệ , thì ban kiểm phiếu sẽ kiểm tra kết quả.

(3.2) Thông báo kết quả

Kết quả cuộc kiểm phiếu sẽ được thông báo công khai.

3.2.3. Các hồ sơ sử dụng

Qua bài toán, ta có các hồ sơ dữ liệu sau :

a). Sổ đăng ký

Số CMT:...

Họ tên :....

Số ID :...

b). Sổ bỏ phiếu

Định danh :...

Thời gian bỏ phiếu :...

c). Thông báo

Tổng số phiếu :...

Số phiếu đồng ý :....

Đạt hay không đạt :...

d). Lá phiếu

Định danh :...

Chữ ký :...

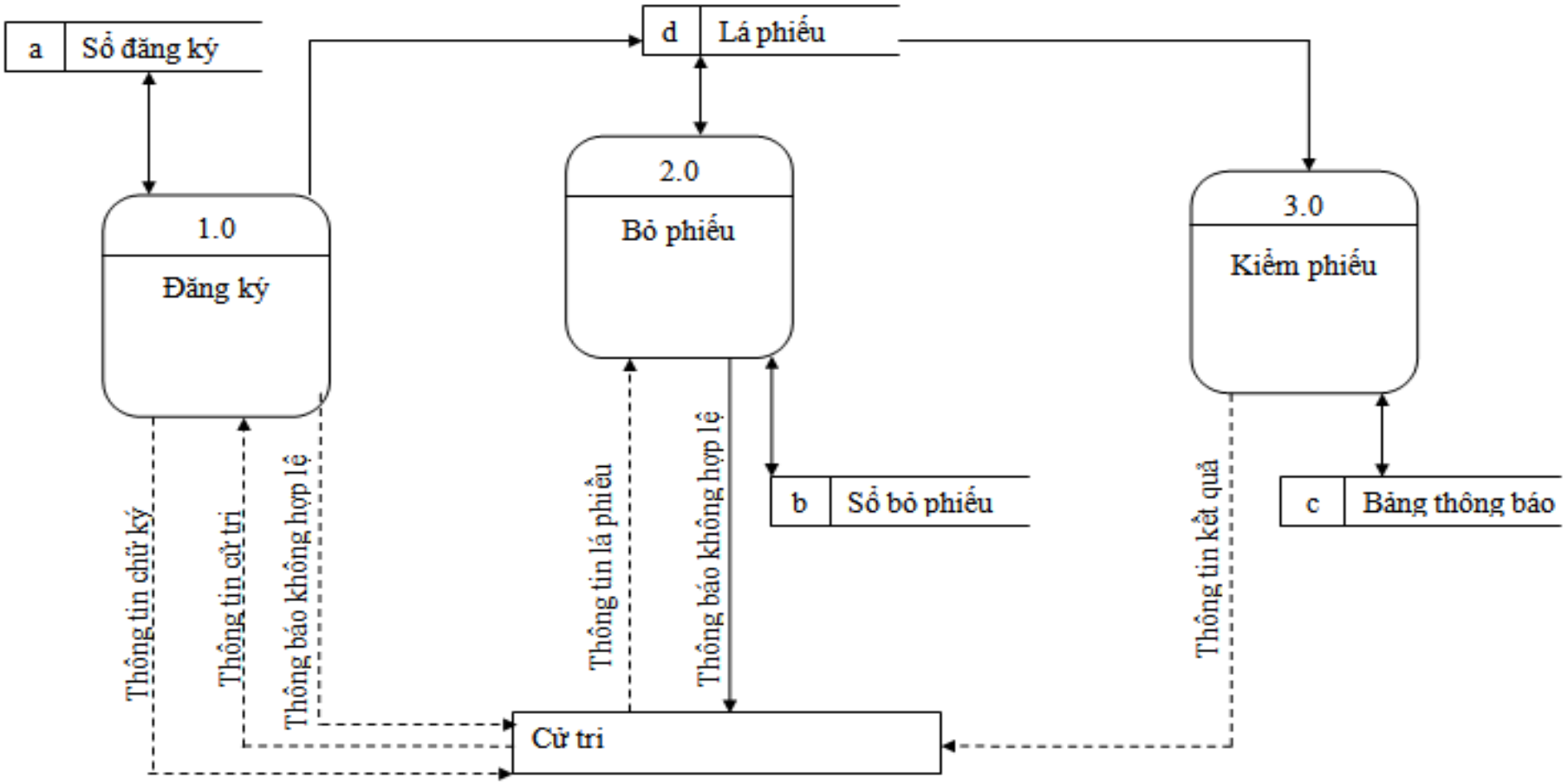
Nội dung :...

3.2.4. Ma trận thực thể chức năng

a.Sổ đăng ký				
c.Bảng thông báo				
b.Sổ bỏ phiếu				
d.lá phiếu				
	a	b	c	d
Đăng ký	U			C
Bỏ phiếu			U	R
Kiểm phiếu		U		R

Hình 3.3 Ma trận thực thể chức năng.

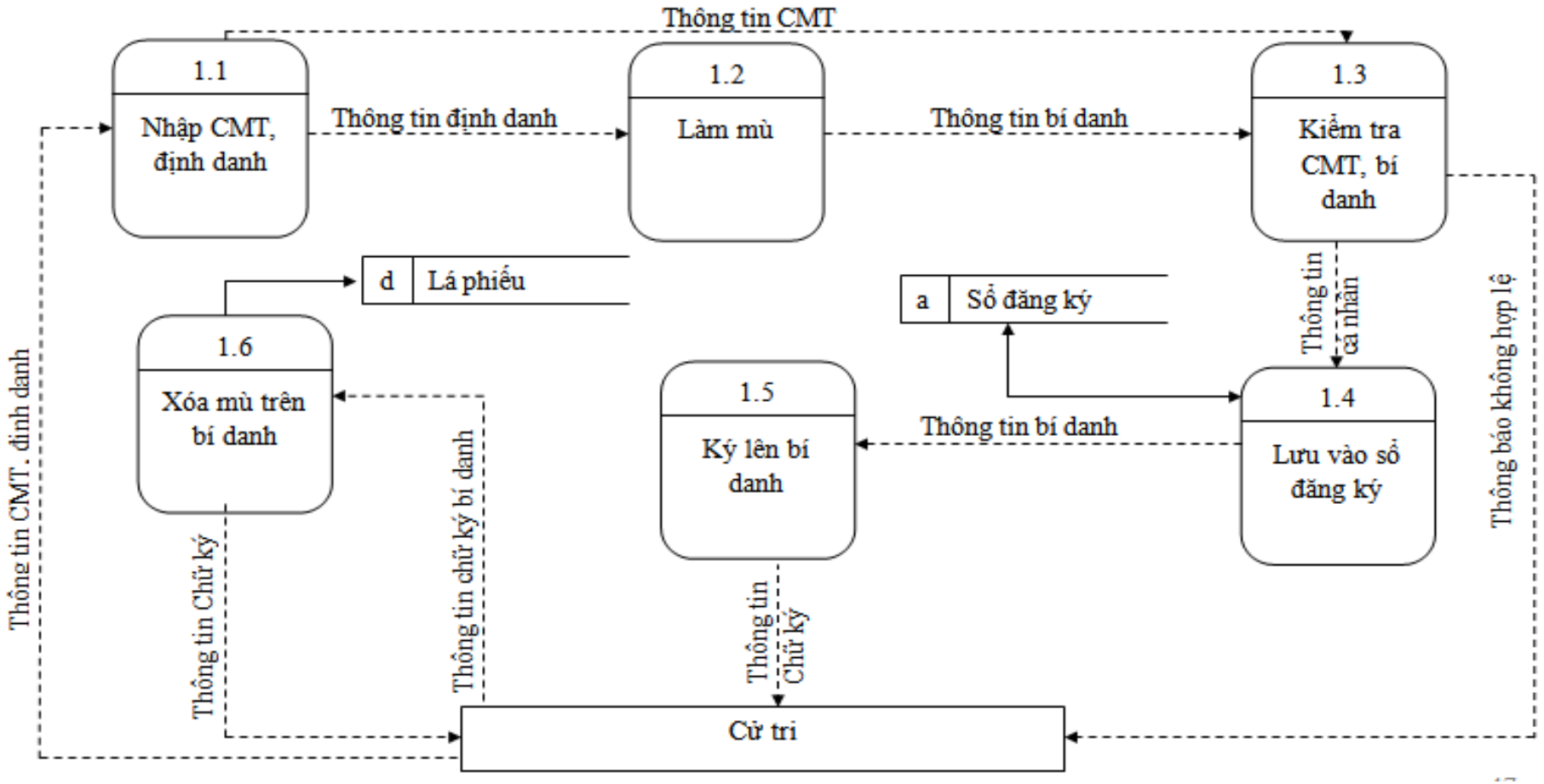
3.2.5. Biểu đồ luồng dữ liệu mức 0



Hình 3.4 Biểu đồ luồng dữ liệu mức 0 của hệ thống bỏ phiếu.

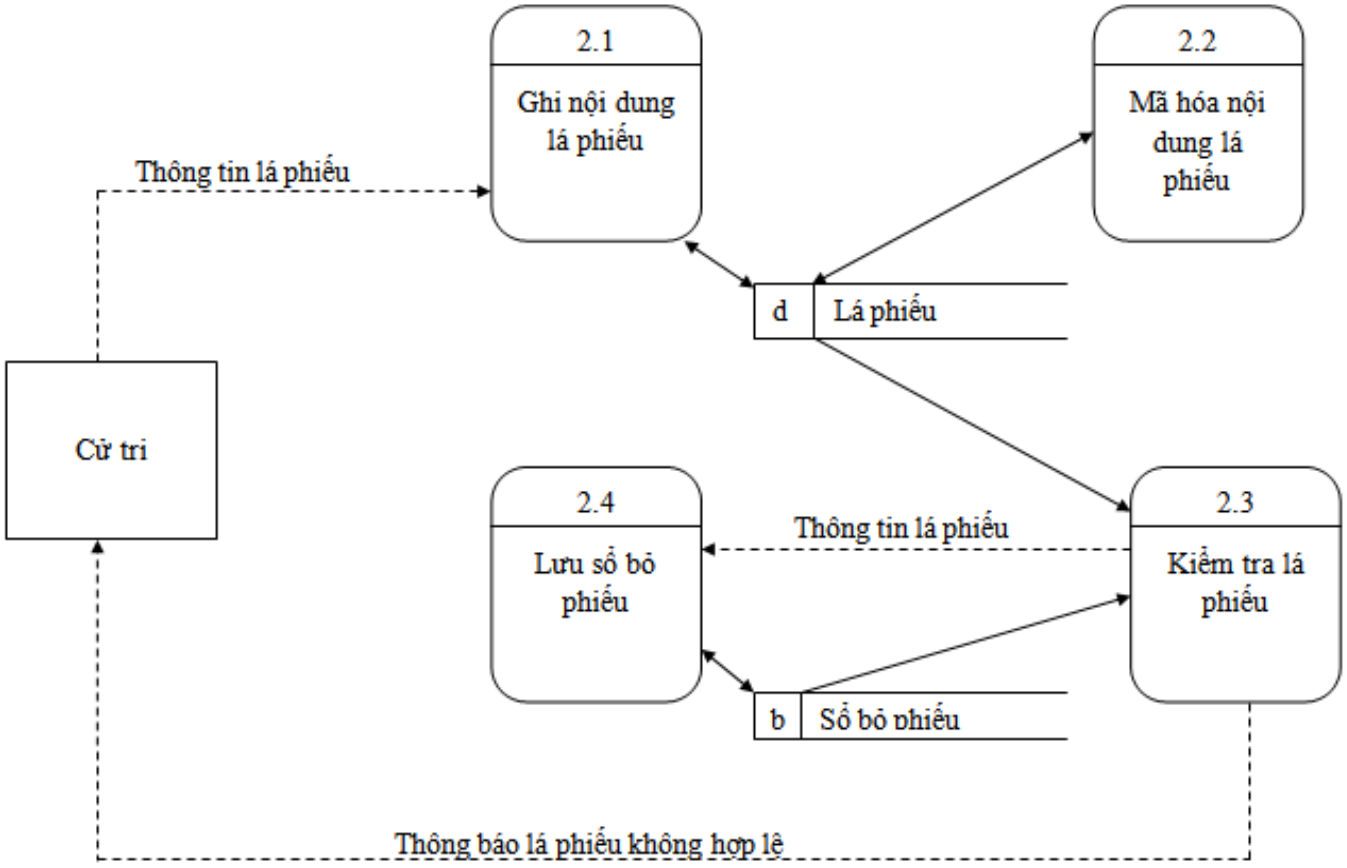
3.2.6. Biểu đồ dữ liệu logic mức 1

1). Biểu đồ của tiến trình "1.0 Đăng ký".



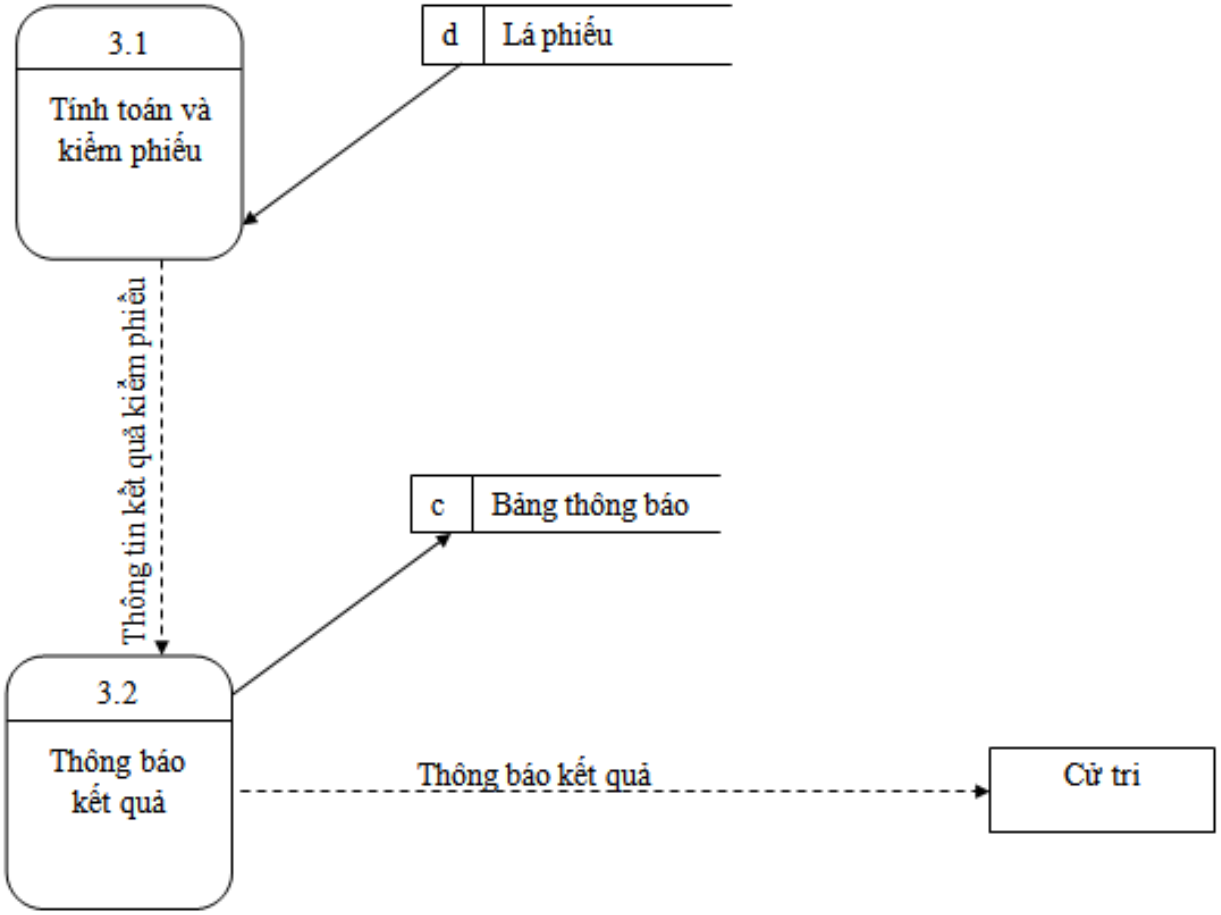
Hình 3.5 Biểu đồ luồng dữ liệu mức 1 của tiến trình đăng ký bỏ phiếu.

2). Biểu đồ của tiến trình "2.0 Bỏ phiếu"



Hình 3.6 Biểu đồ luồng dữ liệu mức 1 của tiến trình bỏ phiếu.

3). Biểu đồ của tiến trình "3.0 Kiểm phiếu"



Hình 3.7 Biểu đồ luồng dữ liệu mức 1 của tiến trình kiểm phiếu.

3.2.7. Mô hình quan hệ thực thể

1). Mô tả các thực thể và thuộc tính.

a). CỬ TRI

Thực thể CỬ TRI chứa các thông tin về cử tri như :

Chứng minh thư, họ tên, địa chỉ, ngày sinh, ...

b). BAN BẦU CỬ

Thực thể BAN BẦU CỬ chứa các thông tin về các ban trong quá trình bầu cử (ban kiểm tra, ban đăng ký, ban kiểm phiếu)

Mã ban, tên ban,...

c). THÀNH VIÊN

Thực thể THÀNH VIÊN chứa các thông tin về những người tham gia trong ban bầu cử

Mã thành viên, tên, khóa, ...

d). HÒM PHIẾU

Thực thể HÒM PHIẾU gồm các thông tin :

Mã hòm, nội dung...

2). Mô tả quan hệ

<Đăng ký>

Ai đăng ký? Cử tri

Khi nào? Ngày đăng ký

Đăng ký với ai? Thành viên ban bầu cử

<Bỏ phiếu>

Bỏ gì? Lá phiếu

Ai bỏ? Cử tri

Khi nào? Ngày bỏ phiếu

<Kiểm phiếu>

Kiểm cái gì? Hòm phiếu

Ai kiểm? Thành viên ban bầu cử

Khi nào? Ngày kiểm

<Bao gồm>

Bao gồm những ai? Thành viên ban bầu cử

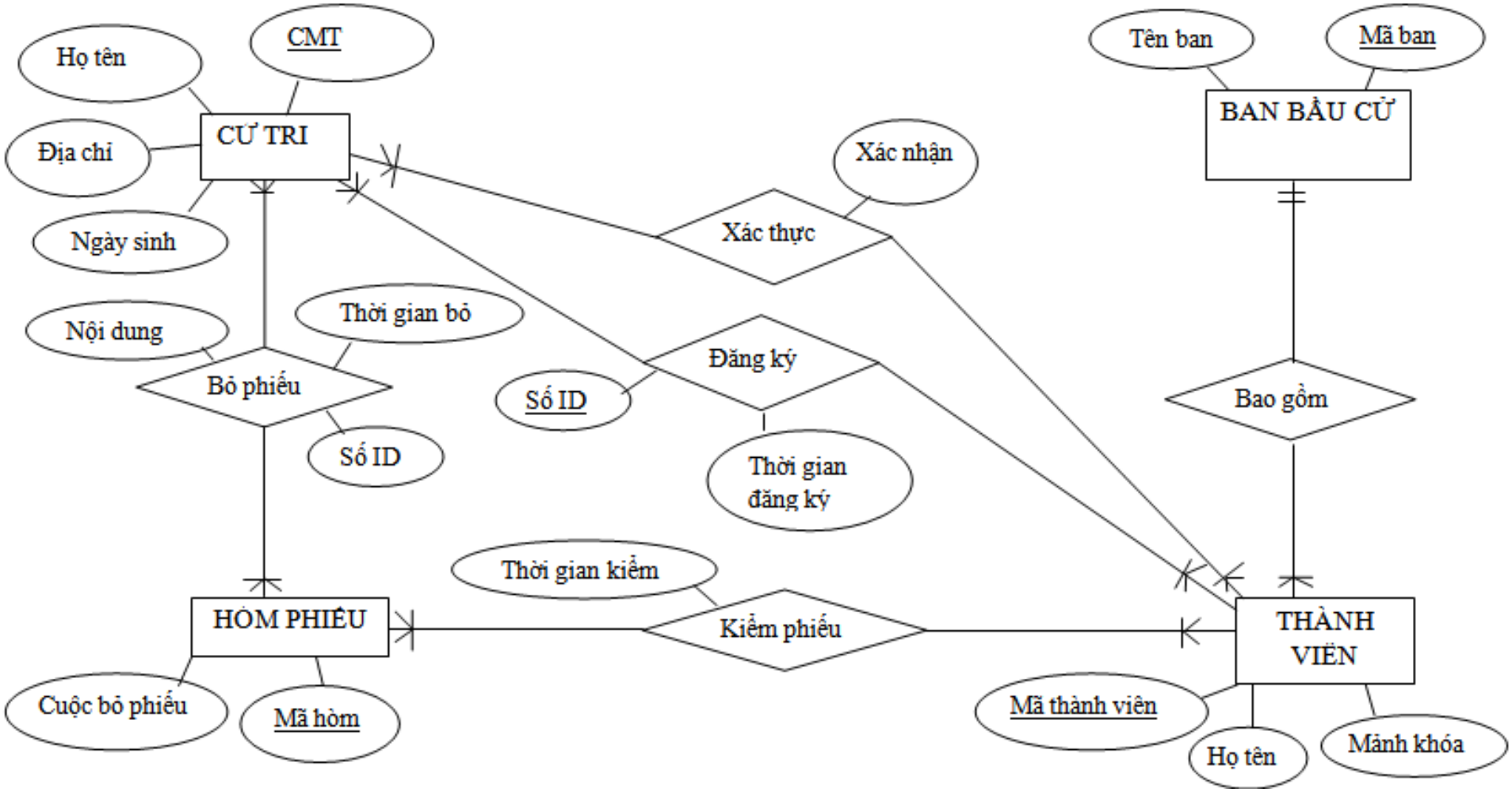
Ai bao gồm? Ban bầu cử

<Xác thực>

Ai xác thực? Thành viên

Xác thực ai? Cử tri

3). Sơ đồ ER.



Hình 3.8 Biểu đồ ER của hệ thống bỏ phiếu.

3.2.8. Mô hình quan hệ

1). Áp dụng các thuật toán chuyển mô hình ER sang mô hình quan hệ.

CỬ TRI

(CMT, họ tên, ngày sinh, địa chỉ)

BAN BẦU CỬ

(Mã ban, tên ban)

THÀNH VIÊN

(Mã thành viên, họ tên, mảnh khóa, mã ban)

HÒM PHIẾU

(Mã hòm, cuộc bỏ phiếu)

CỬ TRI ĐĂNG KÝ THÀNH VIÊN

(số ID, CMT, Mã thành viên, thời gian đăng ký)

THÀNH VIÊN KIỂM PHIẾU HÒM PHIẾU

(Mã hòm, mã thành viên, thời gian kiểm)

CỬ TRI BỎ PHIẾU HÒM PHIẾU

(CMT, Mã hòm, Số Id, nội dung, thời gian bỏ)

THÀNH VIÊN XÁC THỰC CỬ TRI

(Mã thành viên, CMT, xác nhận)

2). Chuyển mô hình quan hệ thành cơ sở dữ liệu vật lý

Bảng CU_TRI

1	CMT	nvarchar	10	not null
2	hoten	nvarchar	50	not null
3	ngaysinh	datetime		not null
4	diachi	nvarchar	50	not null

Bảng THANH_VIEN

1	mathanhvien	nvarchar	10	not null
2	hoten	nvarchar	50	not null
3	manhkhoax	nvarchar	10	allow null
4	manhkhoay	nvarchar	10	allow null
5	maban	nvarchar	10	not null

Bảng BAN_BAU_CU

1	maban	nvarchar	10	not null
2	tenban	nvarchar	50	not null

Bảng HOM_PHIEU

1	mahom	nvarchar	10	not null
2	noidung	nvarchar	50	not null

Bảng CT_DANGKY_TV

1	soID	int		not null
2	CMT	nvarchar	10	not null
3	thoigiandk	datetime		not null
4	mathanhvien	nvarchar	10	not null

Bảng TV_KIEMPHIEU_HP

1	mahom	nvarchar	10	not null
2	mathanhvien	nvarchar	10	not null
3	thoigiankp	datetime		not null

Bảng CT_BOPHIEU_HP

1	CMT	nvarchar	10	not null
2	mahom	nvarchar	10	not null
3	soID	int		not null
4	noidung	nvarchar	50	not null
5	thoigianbp	datetime		not null

Bảng TV_XACTHUC_CT

1	mathanhvien	nvarchar	10	not null
2	CMT	nvarchar	10	not null
3	xacthuc	bit		

Chương 4: THỬ NGHIỆM XÂY DỰNG CHƯƠNG TRÌNH ĐĂNG KÝ BỎ PHIẾU (RSA)

4.1. CẤU HÌNH HỆ THỐNG

4.1.1. Phần cứng

Yêu cầu phần cứng của chương trình:

CPU

Tối thiểu: 600MHz pentinum processor

Đề nghị: 1GHz pentinum processor hoặc cao hơn

RAM

Tối thiểu: 256 MB

Đề nghị: 512 MB hoặc cao hơn

HDD

Tối thiểu: 5 MB

4.1.2. Phần mềm

Yêu cầu phần mềm của chương trình:

+ Máy phải cài đặt và sử dụng một trong các hệ điều hành sau : window 2000, window XP (pack 1,2,3), window server, window 7.

+ Yêu cầu cài đặt hệ quản trị cơ sở dữ liệu SQL 2005 trở lên.

+ Yêu cầu cài đặt .net framework.

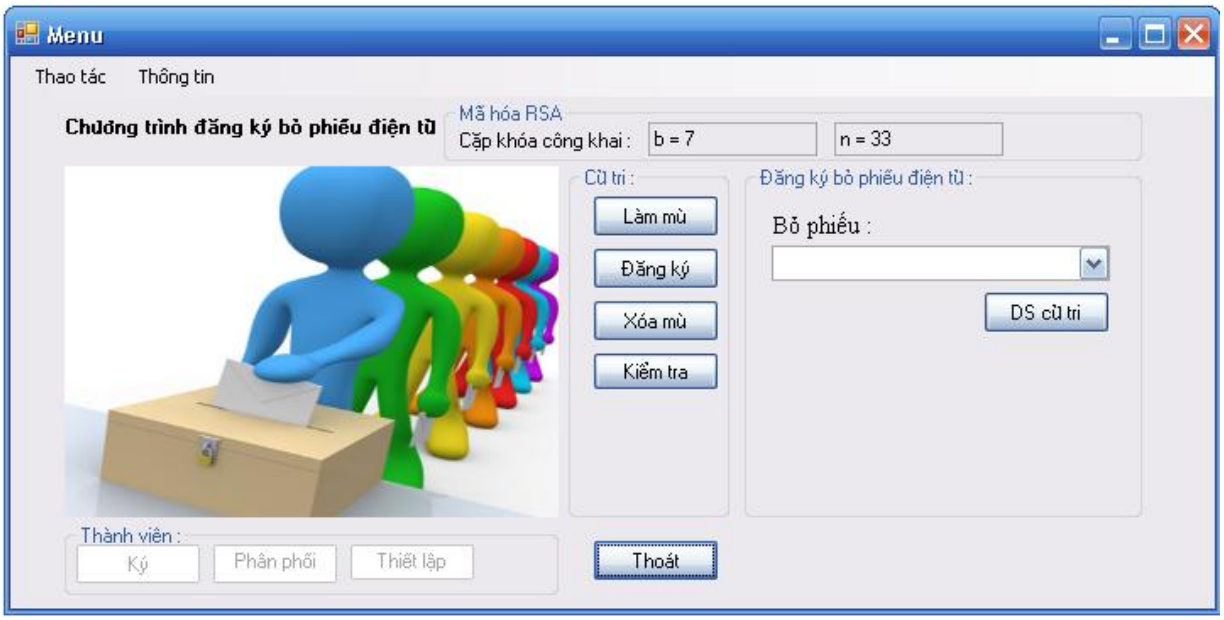
4.2. CÁC THÀNH PHẦN CỦA CHƯƠNG TRÌNH

4.2.1. Phần kết nối

Phần kết nối của chương trình sử dụng kết nối vào cơ sở dữ liệu SQL 2005. Được viết trên ngôn ngữ vb.net sử dụng lớp ADO.NET.

4.2.2. Phần giao diện

Giao diện được thiết kế bằng phần mềm visual studion 2005.



Hình 4.1 Giao diện chính của chương trình.

4.2.3. Phần thuật toán áp dụng

- Thuật toán ký với hệ mã hóa RSA.

- Phân phối khóa ký dựa trên nội suy Lagrange.

- Phần hợp nhất các mảnh khóa để tìm ra khóa ký : Sử dụng phép khử Gauss để giải hệ n phương trình với n ẩn.

4.3. CHƯƠNG TRÌNH

Chương trình cung cấp chức năng đăng ký bỏ phiếu cho cử tri và chức năng cấp chữ ký cho các thành viên trong ban bầu cử.

4.3.1. Chức năng khách

Chương trình cung cấp các chức năng hỗ trợ cử tri đăng ký bỏ phiếu như :

1/. Làm mù định danh.

Nhập định danh và tham số làm mù. Kết quả trả ra là bí danh.

2/. Đăng ký bỏ phiếu.

Nhập thông tin cá nhân và bí danh. Kết quả là bí danh có chữ ký.

3/. Xóa mù.

Nhập bí danh. Kết quả là định danh.

4/. Kiểm tra chữ ký.

Nhập định danh và định danh có chữ ký để kiểm tra chữ ký.

4.3.2. Chức năng người sử dụng.

Chương trình cung cấp các chức năng hỗ trợ thành viên ban bầu cử quản lý cuộc bầu cử :

1/. Chia sẻ và khôi phục khóa ký.

Dựa trên khóa ký bí mật của hệ mã RSA, sử dụng chia sẻ khóa ngưỡng Shamir. Sau đó hợp nhất các mảnh khóa.

2/. Ký số.

Sử dụng ký số RSA.

3/. Thiết lập hệ mã hóa (sinh khóa).

Là quá trình sinh khóa trong hệ mã RSA (lựa chọn p, q, b).

4.4. HƯỚNG DẪN SỬ DỤNG CHƯƠNG TRÌNH

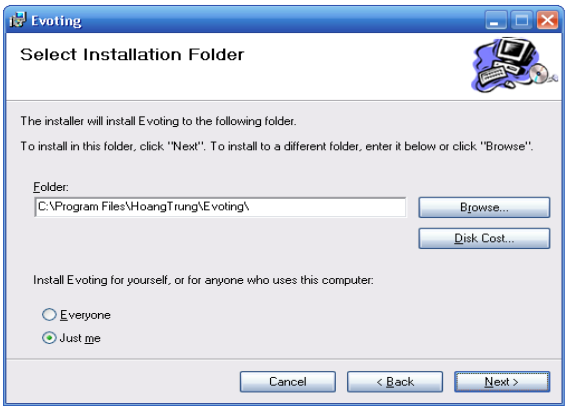
4.4.1. Hướng dẫn cài đặt chương trình

1/. Cài đặt chương trình.

Chạy tệp setup.exe để bắt đầu quá trình cài đặt. Bấm [next].

Hình 4.2 Giao diện bắt đầu quá trình cài đặt.

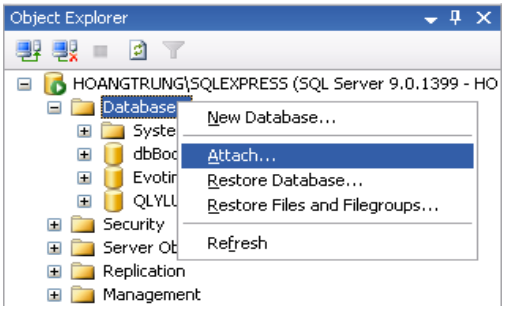
Sau đó lựa chọn đường dẫn để cài chương trình (hình 4.3). Bấm [next].



Hình 4.3 Thiết lập cài đặt.

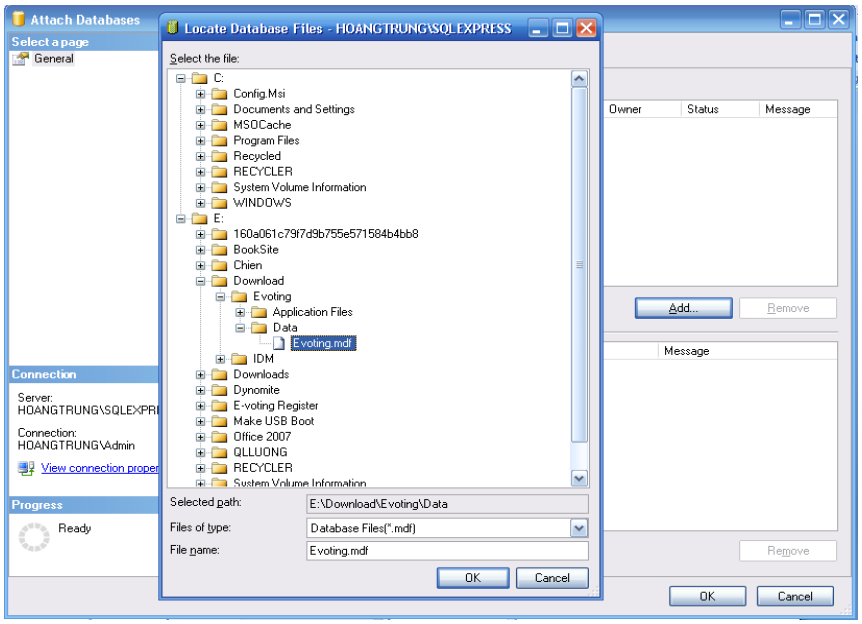
2/. Gán cơ sở dữ liệu (attach database).

+ Khởi động SQL Management Studio Express. Trong cửa sổ đối tượng (Object Explorer), nhấn chuột phải lên Database và chọn Attach…



Hình 4.4 Gán (attach) cơ sở dữ liệu.

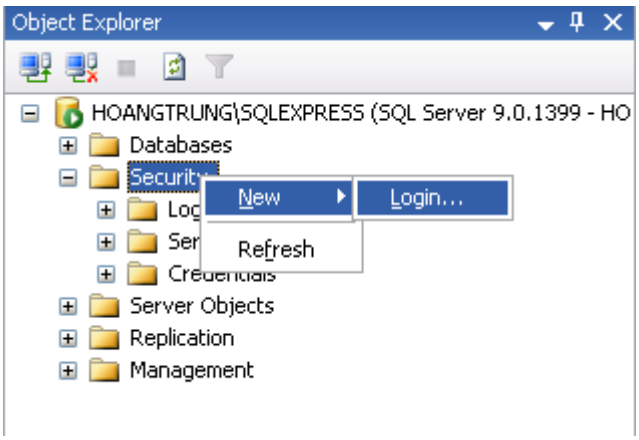
+ Trong cửa sổ Attach Database (hình 4.3), bấm [Add], chọn đường dẫn (Evoting.mdf nằm trong thư mục Data của chương trình vừa cài đặt). Sau đó bấm [OK] để hoàn tất quá trình.



Hình 4.5 Chọn đường dẫn đến cơ sở dữ liệu.

3/. Tạo tài khoản truy cập cơ sở dữ liệu.

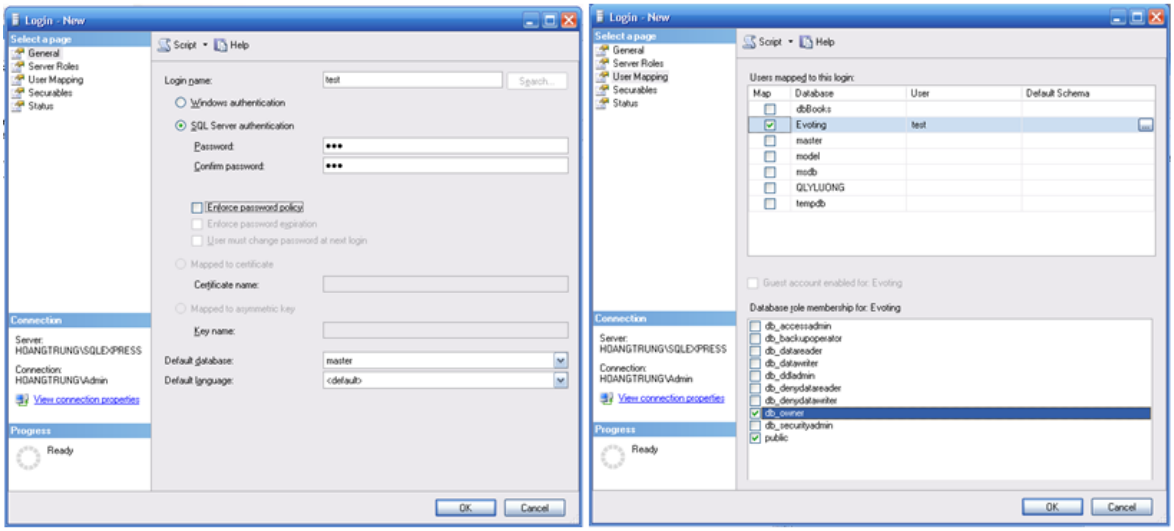
+ Trong cửa sổ đối tượng chuột phải lên Security, lựa chọn Login…



Hình 4.6 Tạo tài khoản trong SQL server 2005.

+ Trong cửa sổ tạo mới(Login - New) nhập các thông tin tên, mật khẩu tại thẻ General. Sau đó chuyển sang thẻ User Mapping, lựa chọn cơ sở dữ liệu vừa gán ở bước 1, chọn db_owner. Rồi bấm OK.

Ví dụ: Tạo một tài khoản tên là test, mật khẩu là 123.



Hình 4.7 Tạo tài khoản truy cập SQL server 2005.

4.4.2. Hướng dẫn chạy chương trình

+ Khởi động tệp Evoting Register.exe để vào chương trình.

+ Nhập thông tin kết nối cơ sở dữ liệu: tên máy chủ, tên cơ sở dữ liệu, tên người dùng và mật khẩu vừa tạo. Sau đó bấm [đăng nhập].

Ví dụ: Tên SQL server trên máy chủ là "HOANGTRUNG\SQLEXPRESS" (có thể xem bằng cách mở SQL server managerment studio express), cơ sở dữ liệu là "Evoting", tên tài khoản đã tạo (mục 4.4.1) "test", mật khẩu "123".

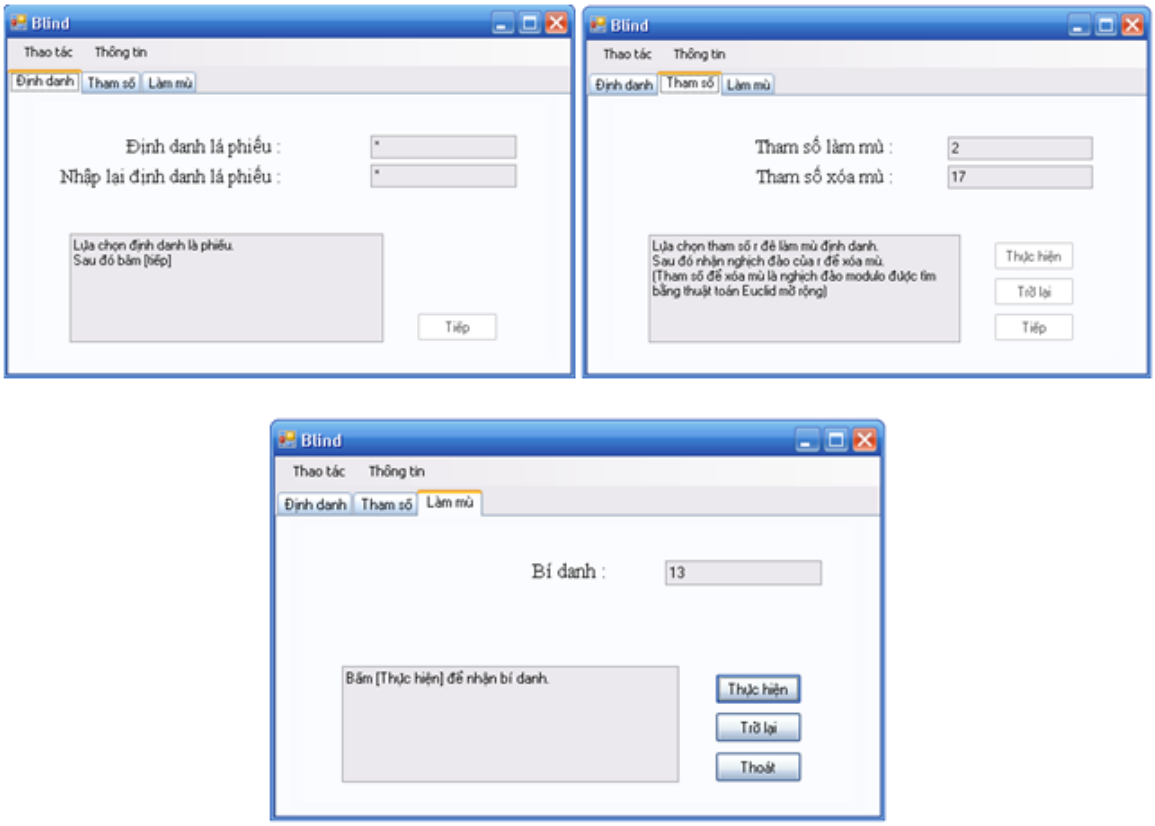
Hình 4.8 Đăng nhập.

+ Nếu đăng nhập thành công sẽ mở ra giao diện chính. (Hình 4.1)

Trong giao diện chính là thông tin về cuộc bỏ phiếu, cặp khóa công khai của chương trình, các nút chức năng.

4.4.3. Hướng dẫn chức năng khách

4.4.3.1. Hướng dẫn quá trình làm mù



Hình 4.9 Các bước làm mù định danh.

+ **Bước 1**: Nhập định danh.

+ **Bước 2**: Chọn tham số làm mù, bấm [thực hiện] sẽ nhận được tham số xóa mù (yêu cầu tham số làm mù phải có nghịch đảo modulo n). Sau đó bấm [Tiếp].

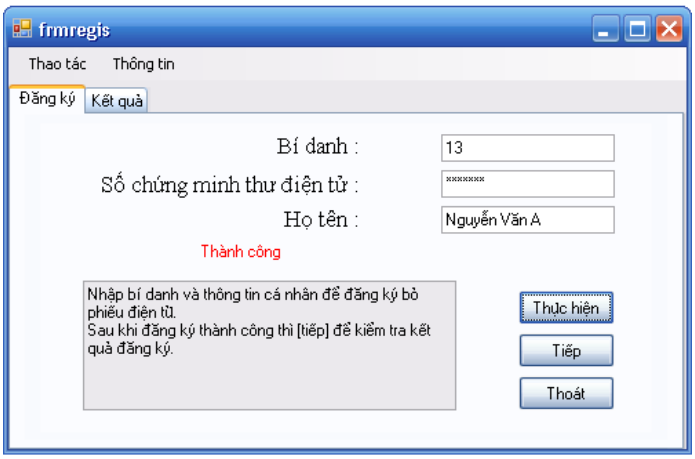
+ **Bước 3**: Bấm [thực hiện] để nhận bí danh.

Ví dụ : chọn định danh 5, tham số làm mù r là 2. Ta sẽ có

Tham số xóa mù: $r^{-1} = 17$ vì $2 * 17 = 1 \bmod 33$, bí danh: $5* 2^7 \bmod 33 = 13$

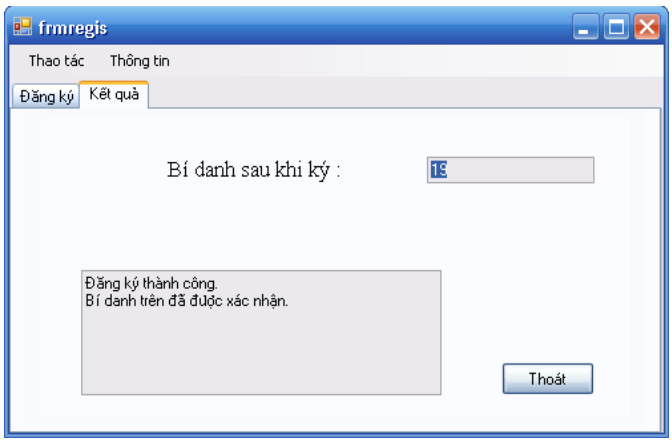
4.4.3.2. Hướng dẫn quá trình đăng ký

+ Nhập thông tin đầy đủ để đăng ký(bước này yêu cầu cử tri phải có tên trong danh sách cử tri thì mới có quyền đăng ký) rồi bấm [thực hiện] để đăng ký.



Hình 4.10 Thao tác đăng ký bỏ phiếu.

+ Nhập số chứng minh thư điện tử, họ tên rồi bấm [Tiếp]. Chương trình sẽ gửi trả bí danh sau khi ký của cử tri nếu như ban đăng ký đã ký.

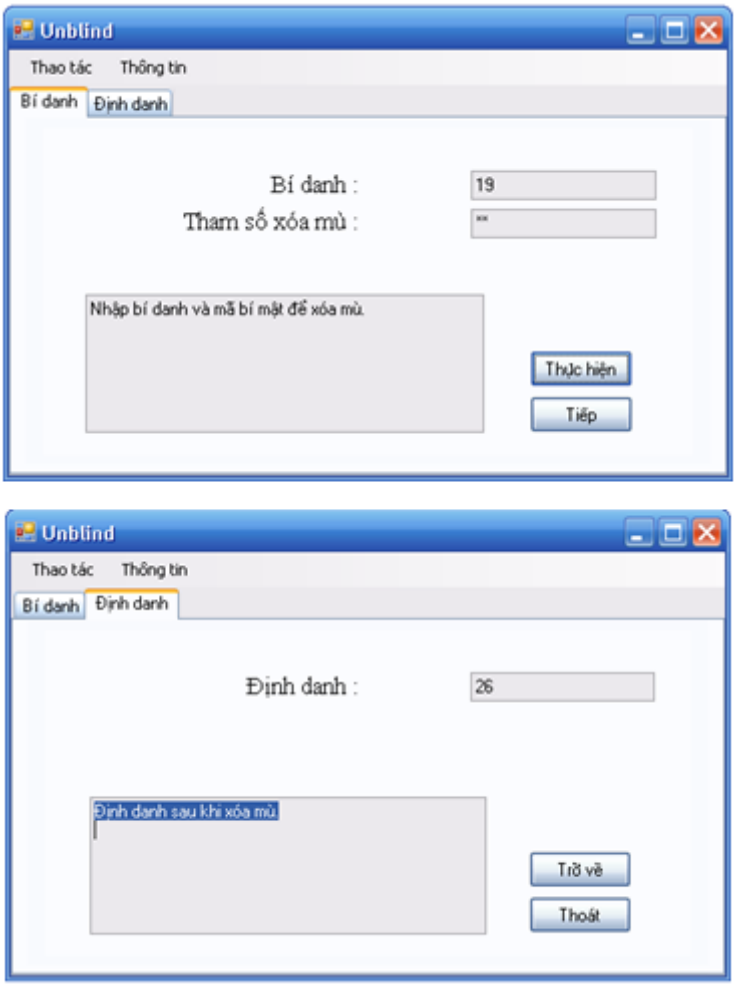


Hình 4.11 Thao tác nhận kết quả đăng ký..

Ví dụ: số chứng minh thư "1234567" của cử tri "Nguyễn Văn A" được chấp nhận cho phép đăng ký. Sau khi thực hiện quá trình ký (trình bày ở mục 4.4.4.1) thì ta sẽ được kết quả bí danh sau khi ký là $13^3 \bmod 33 = 19$.

4.4.3.3. Hướng dẫn quá trình xóa mù

Nhập lại bí danh và tham số bí mật nhận được khi làm mù để xóa mù rồi nhận định danh sau khi xóa mù.

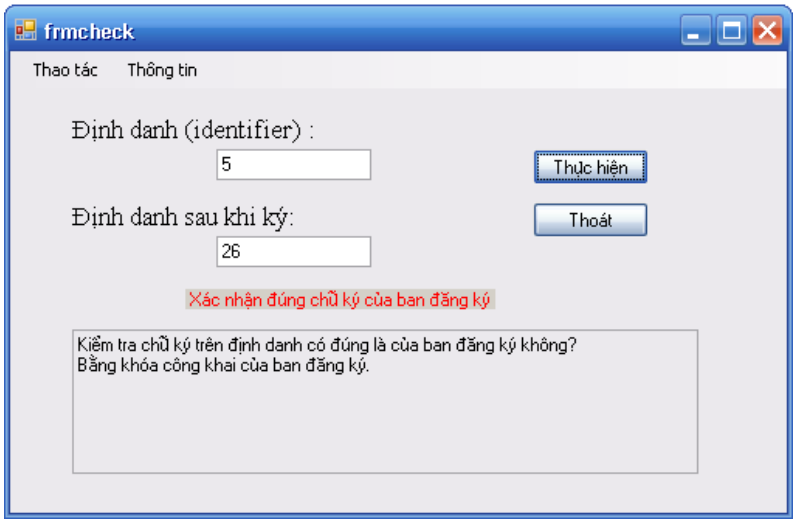


Hình 4.12 Thao tác xóa mù.

Ví dụ: Với bí danh nhận được = 19 (trong mục 4.4.3.2) và tham số xóa mù = 17 (trong mục 4.4.3.1). Ta có định danh = 19 * 17 mod 33 = 26.

4.4.3.4. Hướng dẫn quá trình kiểm tra chữ ký

Nhập định danh, định danh sau khi ký để chương trình có thể kiểm tra chữ ký. Nếu như chữ ký là đúng thì sẽ hiện thông báo xác nhận đúng là chữ ký của ban đăng ký (hình 4.11).



Hình 4.13 Kiểm tra chữ ký.

Ví dụ: nhập định danh ban đầu (mục 4.4.3.1) và định danh lấy được sau khi xóa mù (mục 4.4.3.3). Ta có hàm kiểm tra theo khóa công khai b.

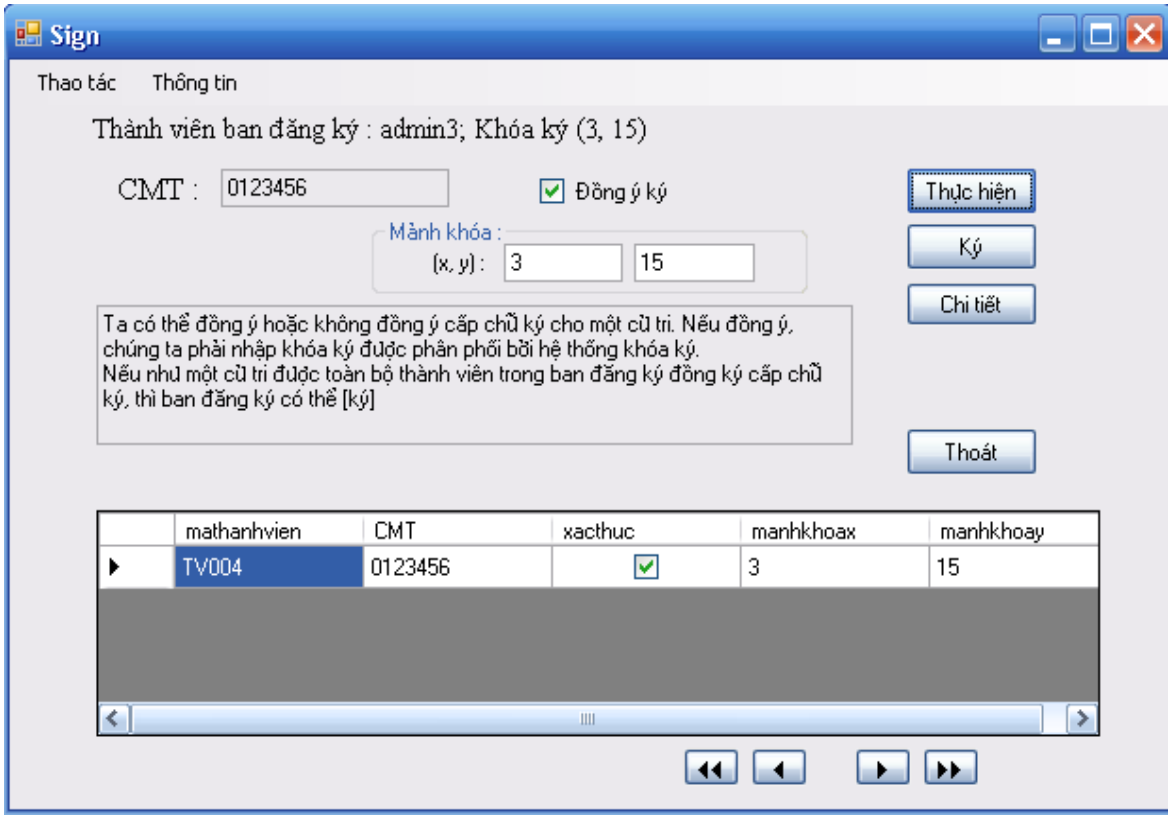
Ver(x, y) = true ↔ $5 = 26^7 \bmod 33$.

4.4.4. Hướng dẫn chức năng người sử dụng

4.4.4.1. Hướng dẫn quá trình xác nhận ký

Khi đăng nhập, nếu chương trình kiểm tra quyền hạn của người đăng nhập là thành viên ban đăng ký, thì người đó có thể xem được thông tin của các cử tri đang đăng ký, và có quyền đồng ý hoặc không đồng ý cử tri bất kỳ (là quá trình xác nhận lại thông tin cử tri của mỗi thành viên trong ban đăng ký).

Thành viên phải chọn vào ô đồng ý ký, nhập mảnh khóa của mình, rồi bấm [thực hiện]. Bấm [Ký] khi đã có sự đồng ý của tất cả thành viên.



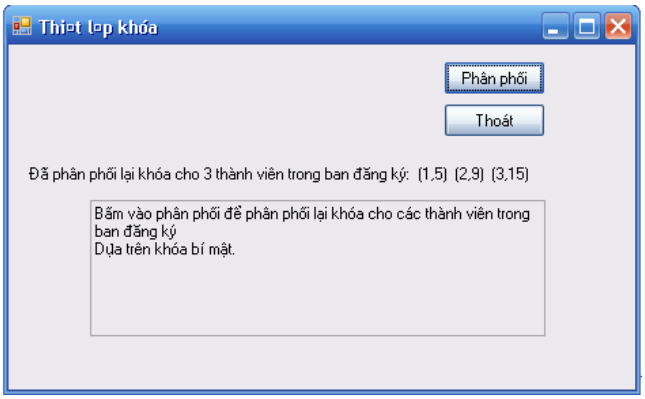
Hình 4.14 Quá trình xác nhận thông tin ký.

Ví dụ: Hiện tại hệ thống có 3 thành viên lần lượt có tên tài khoản “member1”, “member2”, “member3” (mật khẩu trùng với tên tài khoản)..

Trong ví dụ này ta sẽ đăng nhập vào từng tài khoản rồi xác nhận đồng ý. Sau đó bấm [Ký] khi đã xác nhận bằng cả 3 tài khoản.

4.4.4.2. Hướng dẫn quá trình chia sẻ khóa

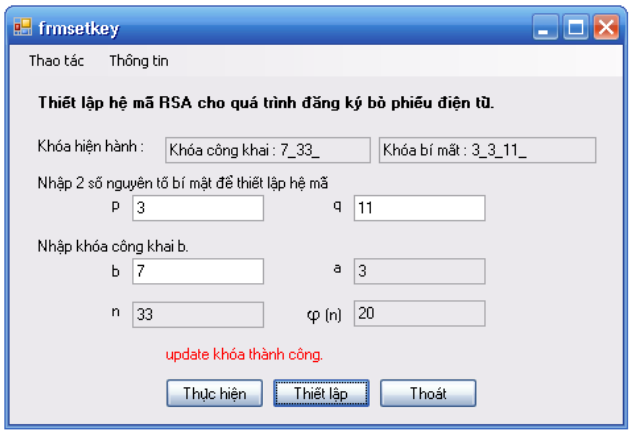
Đăng nhập tài khoản "admin", mật khẩu "admin". Vào phân phối khóa (hình 4.15), bấm [Phân phối], hệ thống tự động kiểm tra số lượng thành viên trong ban đăng ký và khóa bí mật của đợt bỏ phiếu được thiết lập bởi hệ thống để thực hiện chia sẻ khóa.



Hình 4.15 Chia sẻ khóa ký cho các thành viên.

4.4.4.3. Hướng dẫn quá trình thiết lập khóa

Đăng nhập: tài khoản "admin", mật khẩu "admin". Nhập số nguyên tố (p, q) và lựa chọn khóa công khai b. Sau đó bấm [thực hiện] chương trình sẽ tính n và khóa bí mật a. Sau đó bấm [thiết lập].



Hình 4.16 Thiết lập khóa cho hệ thống.

Ví dụ: p = 3, q = 11, b = 7.

→ n = p * q = 33, $\phi(n)$ = (11 – 1) * (3 – 1) = 20, a = 3 vì 3 * 7 = 1 mod 20.

KẾT LUẬN

Khóa luận gồm hai kết quả chính :

1/. Tìm hiểu và nghiên cứu qua tài liệu để hệ thống lại các vấn đề sau:

+ Tổng quan về bỏ phiếu điện tử, và an toàn thông tin

Như đã trình bày ở trên, việc nghiên cứu xây dựng các hệ thống bỏ phiếu điện tử để đáp ứng những yêu cầu mới trong các cuộc bỏ phiểu là một hướng nghiên cứu rất cần thiết hiện nay.

Ưu điểm của bỏ phiếu điện tử là các cử tri có thể tham gia bỏ phiếu ở mọi nơi góp phần làm tăng số cử tri tham gia bỏ phiếu. Nhờ đặc điểm này, các cuộc bầu cử có thể diễn ra thường xuyên hơn cho phép các công dân chuyển nhanh các ý kiến của họ bất cứ lúc nào. Nhưng bỏ phiếu điện tử cũng có nhiều hạn chế, là việc xây dựng các hạ tầng cơ sở cho việc bỏ phiếu là một vấn đề khó khăn đặc biệt là ở vùng sâu vùng xa. Bên cạnh đó, cho đến nay, chưa có một giải pháp nào hoàn thiện được tìm thấy để đảm bảo tính an toàn tuyệt đối của cuộc bỏ phiếu.

Ở những phạm vi nhỏ, bỏ phiếu điện tử chỉ đơn giản là các cuộc lấy ý kiến thì có thể bỏ qua một số giai đoạn nhằm giảm sự phức tạp trong công việc triển khai.

Tuy nhiên, ở các cuộc bầu cử có quy mô lớn, đặc biệt là cuộc bầu cử cấp quốc gia thì các hệ thống bỏ phiếu cần phải đặt việc bảo mật lên hàng đầu không thể bỏ qua được bất kỳ giai đoạn nào.

+ Một số bài toán về ATTT trong giai đoạn đăng ký Bỏ phiếu:

Qua bài toán đăng ký bỏ phiếu, ta có thể thấy được các vấn đề mà hệ thống mắc phải thường là về bảo mật, xác thực,...

+ Phương pháp giải quyết các bài toán:

Như đã trình bày trong khóa luận với các vấn đề về an toàn thông tin thì có rất nhiều cách khắc phục, tuy nhiên để tìm ra một cách toàn vẹn nhất thì vẫn còn trong giai đoạn nghiên cứu.

Ta có thể thấy được một số cách sau : mã hóa, ký số, chia sẻ khóa bí mật, chứng thực số, hàm băm,...

2/. Thử nghiệm xây dựng chương trình đăng ký bỏ phiếu dựa trên hệ mã hóa RSA trong phạm vi nhỏ.

Chương trình mô phỏng các bước trong giai đoạn đăng ký bỏ phiếu và giải quyết được một số các bài toán an toàn thông tin bằng ký mù, chia sẻ khóa, mã hóa RSA.

Bỏ phiếu điện tử còn là một hình thức rất mới mẻ chưa được áp dụng thực tế ở Việt Nam. Nên trong quá trình nghiên cứu và làm khóa luận này, không thể tránh khỏi những thiếu sót. Kính mong được sự bổ khuyết của quý thầy cô và mọi người quan tâm, để cho khóa luận trở nên hoàn chỉnh.

TÀI LIỆU THAM KHẢO

Tiếng Việt.

[1] Trịnh Nhật Tiến, Trương Thị Thu Hiền, "*Về một quy trình bỏ phiếu từ xa*", Đại học công nghệ, đại học quốc gia Hà Nội.

[2] PGS.TS Trịnh Nhật Tiến, "*Giáo trình an toàn dữ liệu*", Đại học công nghệ, đại học quốc gia Hà Nội.

Tiếng Anh.

[1] Ivan Damgard, Jens Groth and Gorm Salomonsen, "*The theory and implenmentation of an Electronic Voting Sytem"*

PHỤ LỤC

Các phụ lục sau được bổ sung vào khóa luận :

1). Hàm tìm nghịch đảo bằng thuật toán euclid mở rộng.

Đầu vào: số a, m.

Đầu ra: nghịch đảo của a trên modulo m.

```
Protected Function euclidextend(ByVal a As Integer, ByVal m As Integer)
    Dim y0 = 0, y1 = 1, y = 0, m2 = m, a2 = a
    Dim r, q
    While a > 0
      r = m Mod a
      If r = 0 Then
        Exit While
      End If
      q = m \ a
      y = y0 - y1 * q
      m = a : a = r
      y0 = y1 : y1 = y
    End While
    If a > 1 Then
      Return a2 & " không khả nghịch theo modulo " & m2
    Else
      If y < 0 Then
        y = m2 + y
      End If
      Return y
    End If
End Function
```

(Ngôn ngữ lập trình vb.net)

2). Hàm lấy ghép khóa ký bằng phép khử gauss.

Sử dụng phép khử Gauss áp dụng trên ma trận mở rộng. (Đã trình bày trong mục 2.2.3 tiểu mục "*hợp nhất khóa*")

Đầu vào: ma trận mt(n-1, n) chứa giá các tham số của hệ phương trình, với n bằng số hệ phương trình.

Đầu ra: khóa bí mật.

```
Protected Function gauss(ByVal mt(,) As Integer, ByVal n As Integer)
    Dim i, j, k, tg
     For k = 0 To n - 2
        For i = k + 1 To n - 1
           tg = mt(i, k) / mt(k, k)
           For j = k To n - 1
              mt(i, j) = mt(i, j) - tg * mt(k, j)
           Next
           mt(i, n) = mt(i, n) - tg * mt(k, n)
        Next
     Next
    Return mt(n - 1, n)
End Function
```

(Ngôn ngữ lập trình vb.net)