MỤC LỤC

LỜI CẢM ƠN

Tôi xin chân thành cảm ơn Th.s Trần Ngọc Thái – người thầy luôn ân cần chỉ bảo, nhiệt tình hướng dẫn, cung cấp những tài liệu, giúp đỡ tôi trong quá trình học tập và hoàn thành bản luận văn này .

Tôi xin cảm ơn các thầy cô giáo khoa Công Nghệ Thông Tin cùng Ban giám hiệu nhà trường Đại Học Dân Lập Hải Phòng đã tạo điều kiện cho tôi được làm đồ án và hoàn thành bản luận văn của mình .

Tôi cũng xin cảm ơn tập thể các bạn trong lớp CT1002 đã cùng tôi trao đổi và giúp đỡ tôi trong quá trình học và trong việc tìm tài liệu hoàn thành luận văn này .

Hải Phòng ngày tháng năm

Sinh viên

Vương Thị Huyền Trang

DANH MỤC CÁC HÌNH VẼ, SƠ ĐỒ

MỞ ĐẦU

Trong những năm gần đây, cả thế giới đang chứng kiến một cuộc cách mạng mạnh mẽ, toàn diện và sâu sắc đã làm thay đổi các hoạt động trong mọi lĩnh vực kinh tế, văn hoá, chính trị, xã hội; thay đổi cả phương thức làm việc, học tập, giải trí, giao tiếp và quan hệ xã hội. Một trong những nội dung cơ bản của cuộc cách mạng này là ứng dụng công nghệ cao, hiện đại với công nghệ thông tin là công cụ có ý nghĩa quyết định, mang tính đột phá, góp phần rút ngắn quá trình công nghiệp hoá, hiện đại hóa. Trong đó mạng máy tính đã giúp cho con người tiếp cận, trao đổi những thông tin mới nhất một cách nhanh chóng, thuận tiện và nó đã mang lại cho con người những lợi ích không thể phủ nhận được.

Một xã hội dân chủ có nhiều việc phải cần đến "bỏ phiếu"; người ta "bỏ phiếu" để thăm dò các kế hoạch, chính sách nào đó hoặc để bầu cử các chức vụ, chức danh... Hiện nay có 2 loại bỏ phiếu chính là ***bỏ phiếu trực tiếp*** tại hòm phiếu bằng các lá phiếu in trên giấy (**"bỏ phiếu truyền thống"**) và ***bỏ phiếu từ xa*** bằng các lá phiếu "số hoá" tạm gọi là lá phiếu điện tử từ các máy tính cá nhân trên mạng, điện thoại di động... (**"bỏ phiếu điện tử"** hoặc **"bầu cử điện tử"**). Ngày nay, quĩ thời gian của mỗi cá nhân không nhiều, mặt khác một người có thể làm việc ở 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 này chỉ còn là thời gian và kỹ thuật cho phép.

Trên thế giới, trong cuộc bầu cử tổng thống Pháp và bầu luật năm 2002, đã có 1500 cử tri Pháp mở đầu việc bầu cử điện tử. Sự kiện này là bước khởi đầu trong quá trình hoàn thiện công cụ bầu cử, nó sẽ cách mạng hoá cách bầu cử ở châu Âu.

Các nước châu Âu như Bỉ, Hà Lan, Đức, Ba Lan đã hoàn thành một số cuộc thử nghiệm. Ở Italia, một nước của thành viên dự án "France telecom R&D,một thử nghiệm đã được hoàn thành trong một cuộc trưng cầu ý kiến của

nhân dân về vấn đề tự trị ở các vùng của quốc gia này và có 94% số cử tri đã bày tỏ sự tán thành việc áp dụng bầu cử điện tử. Tính đến năm 2005,sẽ có khoảng hơn 300 triệu cử tri Châu Âu tham gia bỏ phiếu điện tử. Nhờ ưu điểm thuận tiện, bỏ phiếu điện tử không chỉ làm gia tăng số cử tri tham gia mà còn thể hiện tính dân chủ.

Ở Việt Nam, có ít người nghiên cứu vấn đề này.

Cũng như cuộc bỏ phiếu truyền thống, cuộc bỏ phiếu thăm dò từ xa phải đảm bảo yêu cầu "bí mật", "toàn vẹn" và "xác thực" của lá phiếu.

Kỹ thuật bỏ phiếu thăm dò từ xa dựa trên những lý luận rất sâu sắc về an toàn và bảo mật dữ liệu trên đường truyền tin. Mặt khác lá phiếu phải bảo đảm hợp pháp: lá phiếu đúng là của người được phép bầu cử, mỗi cử tri chỉ được gửi một lá phiếu. Yêu cầu "bí mật" của lá phiếu là: ngoài cử tri, chỉ có ban kiểm phiếu mới được biết nội dung của lá phiếu nhưng họ không biết 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 đến hòm phiếu an toàn, đúng thời hạn và được kiểm phiếu đầy đủ. Yêu cầu "xác thực" của 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. Trải qua nhiều thế kỷ, đã có nhiều công nghệ bỏ phiếu khác nhau với những phương pháp và các hình thức khác nhau. Từ những hòn đá và mảnh vỡ bỏ vào trong lọ thời Hy lạp được thay thế bằng lá phiếu bỏ vào trong hộp gắn niêm phong.

Ngày nay, công nghệ mới phát triển việc bỏ phiếu, có thể tự động hoá. Việc bỏ phiếu tự động cần phải được bảo mật và an toàn như những cuộc bầu cử truyền thống (đặc biệt là bí mật riêng của lá phiếu). Phòng bỏ phiếu "cơ học" và những phiếu đục lỗ sẽ được thay thế bằng những lá phiếu "điện tử" để có thể kiểm phiếu nhanh hơn.

Bỏ phiếu điện tử trực tuyến qua Internet có lợi hơn rất nhiều. Các cử tri có thể bỏ phiếu từ bất cứ nơi đâu. Việc bỏ phiếu thuận tiện làm gia tăng số lượng cử tri. Nhanh chóng, rẻ và tiện lợi quá trình bỏ phiếu có thể tác động lớn trên

những xã hội dân chủ. Ví dụ những cuộc bầu cử cho phép công dân có thể bỏ phiếu vào bất cứ thời gian nào.

Những phương pháp bỏ phiếu hiệu quả có thể phân loại bằng 2 cách tiếp cận chính: sơ đồ sử dụng chữ ký mù và sơ đồ sử dụng mã hoá đồng cấu.

Luận văn gồm 3 chương

Chương 1: CÁC KHÁI NIỆM CƠ SỞ.

Chương 2: BỎ PHIẾU ĐIỆN TỬ .

Chương 3: XÂY DỰNG ỨNG DỤNG MÔ PHỎNG BỎ PHIẾU ĐIỆN TỬ.

Chương 1: CÁC KHÁI NIỆM CƠ SỞ

1.1. MỘT SỐ KHÁI NIỆM TOÁN HỌC

1.1.1. Ký hiệu chia hết

Cho a và b là hai số nguyên dương, số a chia hết cho số b ký hiệu là a : b $\Leftrightarrow$ Tồn tại n $\in$ N sao cho a=b*n. Khii đó người ta nói b là ước của a và ky kiệu là b|a.

1.1.2. Ước số chung lớn nhất

Cho a và b là hai số nguyên dương . USCLN của a và b là số tự nhiên m lớn nhất sao cho m | a và m | b . Khii đó ký hiệu là UCLN(a,b) = m.

1.1.3. Hai số nguyên tố cùng nhau

Cho a và b là hai số nguyên dương. Số a và b được gọi là hai nguyên tố cùng nhau $\Leftrightarrow$ UCLN(a,b) = 1

1.1.4. Đồng dư modulo

Cho n $\in$ i, n $\neq$ 0 và a,b $\in$ Zn

Ký hiệu i $\equiv$ b (mod n) nghĩa là a đồng dư b theo mod n

$\Leftarrow$ tồn tại số nguyên b $\in$ Zn^* sao cho a= b + k * n

Tức là (i-b)=k*n, nhu vậy n | (a-b)

1.1.5. Một số ký hiệu toán học

N: Số người kiểm phiếu .

A_1, A_2,…, A_n: N người kiểm phiếu.

t: Số lớn nhất những người hiểm độc và không trung thực.

A: tập bất kì (t + 1) người.

M: Số cử tri đủ tư cách.

m: Số cử tri tham gia cuộc bầu cử, m $\leq$ M.

V_1, V_2,…, V_M: M người đủ tư cách.

v_1, v_2,…, v_M: độ quan tâm của cử tri.

Z_p: trường các số nguyên dương modulo p, p nguyên tố.

Z_n: tập các số nguyên modulo n, { 0, 1,…., n-1 }

Z^*_n: tập các số nguyên của Z_n nguyên tố với n.

a / b: số nguyên a là ước của số nguyên b.

gcd (a, b): ước số chung lớn nhất của a và b.

a \\ b: phép ghép xâu a và b.

$x \in_R X$: x là phần tử ngẫu nhiên (tùy ý) của X (phân bố đều).

$X \subset_R Y$: X là tập con tùy ý của Y (phân bố đều).

x = y: kiểm tra xem x = y hay không.

1.1.6. Hàm một phía và hàm cửa sập một phía

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

Ví dụ : Hàm $f(x) = \alpha^x (\text{mod } p)$, với p là số nguyên tố lớn, (α là phần tử nguyên thủy) là hàm một phía.

Hàm f(x) được gọi là hàm cửa sập một phía nếu tính 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'

1.1.7. Vấn đề thặng dư bậc hai

Cho n là một số nguyên, $y \in Z_n^*$ được gọi là thặng dư bậc hai modulo n nếu tồn tại $x \in Z_n$ sao cho $y = x^2$ (modulo n). Tập hợp các thặng dư bậc hai modulo n được ký hiệu là Q_n. Nếu n = p là số nguyên tố thì ký hiệu lagrange được xác định như sau:

$$\left(\frac{a}{n}\right) = \begin{cases} 0, & \text{if } p \mid a \\ 1, & \text{if } a \in Q_{pi} \\ -1 & \text{if } a \notin Q_p \end{cases}$$

Nếu n là hợp số và $n = p_1^{e1} p_2^{e2} .. p_k^{ek}$ là sự phân tích thành thừa số nguyên tố, ký hiệu Jacobi được xác định như sau:

$$\left(\frac{a}{n}\right)=\left(\frac{a}{p_1}\right)^{e_1}...\left(\frac{a}{p_k}\right)^{e_k}$$

Có tồn tại loga hiệu nghiệm cho tính toán (a/n) với a, n tuỳ ý.

Rõ ràng, nếu a là một thặng dư bậc hai thì (a/n) = 1. Nhưng từ (a/n)=1 thì không suy ra được a là thặng dư bậc hai. Nếu a không là thặng dư bậc hai nhưng thoả mãn (a/n) = 1 thì a gọi là giả bình phương. Tập các giả bình phương được ký hiệu Q_n.

Nếu n = pq,ở đó p,q nguyên tố phân biệt thì $/Q_n/ = /Q_n/ = (p-1)(q-1)/4$. Bài toán thặng dư bậc hai được đặt ra như sau: Cho n là một hợp số lẻ và $a \in Z_n^*$ sao cho (a/n) = 1, xác định xem a có là thặng dư bậc hai modulo n hay không.

Nếu n = p là số nguyên tố thì dễ dàng xác định được $a \in Z_n$ là thặng dư bậc hai modulo p hay không. Khi đó theo sự xác định của kí hiệu Legendre (a/p) có thể tính toán một cách hiệu nghiệm.

Nếu $n = p_1^{e1}\ldots p_k^{ek}$ là hợp số thì a là thặng dư bậc hai modulo n khi và chỉ khi a là thặng dư bậc hai modulo p_i với mọi i= 1,…, k. Do đó nếu ta biết sự phân tích thành nhân tử của n thì bài toán thặng dư bậc hai có thể giải quyết được bằng cách kiểm tra xem $(a/p_i) = 1$ hay không mọi i=1,…,k. Trong trường hợp không biết được sự phân tích thành nhân tử của n thì không có phương pháp hữu nghiệm nào để giải quyết bài toán này.

1.2. CÁC KHÁI NIỆM VỀ MÃ HOÁ

1.2.1. Khái niệm mã hóa

Ta biết rằng tin truyền trên mạng rất dễ bị lấy cắp. Để đảm bảo việc truyền tin an toàn người ta thường mã hoá thông tin trước khi truyền đi. Việc mã hóa thường theo quy tắc nhất định gọi là hệ mật mã. Hiện nay có hai loại hệ mật mã là mật mã cổ điển và mật mã khoá công khai. Mật mã cổ điển dễ hiểu, dễ thực thi nhưng độ an toàn không cao. Vì giới hạn tính toán chỉ thực hiện trong phạm vi bảng chữ cái sử dụng văn bản cần mã hoã. Với các hệ mã cổ điển, nếu biết khóa lập mã hay thuật toán lập mã, người ta có thể ‘ dễ ‘ tìm ra được bản rõ. Ngược lại các hệ mật mã khóa công khai cho biết khóa lập mã K và hàm lập mã C_k thì cũng rất ‘khó’ tìm được cách giải mã.

1.2.1.1. Hệ mật mã

Hệ mật mã là hệ bao gồm 5 thành phần (P, C, K, E, D) thỏa mãn các tính chất sau:

P (Plaitext): là tập hợp hữu hạn các bản rõ có thể.

C (Ciphertext): Là tập hữu hạn các bản mã có thể

K (Key): Là tập hợp các bản khoá có thể

E (Encrytion):Là tập hợp các quy tắc mã hoá có thể

D (Decrytion): Là tập hợp các quy tắc giải mã có thể.

Chúng ta đã biết một thông báo thường được xem là bản rõ. Người gửi sẽ làm nhiệm vụ mã hoá bản rõ, kết quả thu được gọi là bản mã. Bản mã được gửi đi trên đường truyền tới người nhận. Người nhận giải mã để tìm hiểu nội dung bản rõ. Dễ dàng thấy được công việc trên khi định nghĩa hàm lập mã và hàm giải mã:

$$E_k(P) = C \quad \text{và } D_k(C) = P$$

1.2.1.2 Những yêu cầu đối với hệ mật mã.

Cung cấp một mức cao về tính bảo mật, tính toàn vẹn, chống chối bỏ và tính xác thực.

- Tính bảo mật: Bảo đảm bí mật cho các thông báo và dữ liệu bằng việc che dấu thông tin nhờ các kỹ thuật mã hoá.
- Tính toàn vẹn: Bảo đảm với các bên rằng bản tin không bị thay đổi trên đường truyền tin.
- Chống chối bỏ: Có thể xác nhận rằng tài liệu đã đến từ ai đó, ngay cả khi họ cố gắng từ chối nó.
- Tính xác thực: Cung cấp hai dịch vụ:

o Nhận dạng nguồn gốc của một thông báo và cung cấp một vài bảo đảm rằng nó là đúng sự thực.

o Kiểm tra định danh của người đang đăng nhập một hệ thống, tiếp tục kiểm tra đặc điểm của họ trong trường hợp ai đó cố gắng kết nối và giả danh là người sử dụng hợp pháp.

1.2.2. Các phương pháp mã hóa

1.2.2.1. Mã hóa đối xứng

Hệ mã hoá đối xứng: là hệ mã hoá tại đó khoá mã hoá có thể "dễ" tính toán ra được từ khoá giải mã và ngược lại. Trong rất nhiều trường hợp, khoá mã hoá và khoá giải mã là giống nhau. Thuật toán này có nhiều tên gọi khác nhau như thuật toán khoá bí mật, thuật toán khoá đơn giản, thuật toán một khoá. Thuật toán này yêu cầu người gửi và người nhận phải thoả thuận một khoá trước khi thông báo được gửi đi và khoá này phải được cất giữ bí mật. Độ an toàn của thuật toán này phụ thuộc vào khoá, nếu để lộ ra khoá này nghĩa là bất kỳ người nào cũng có thể mã hoá và giải mã thông báo trong hệ thống mã hoá. Sự mã hoá và giải mã của hệ mã hoá đối xứng biểu thị bởi:

$$E_k : P \rightarrow C \quad \text{Và } D_k: C \rightarrow P$$

Nơi ứng dụng: Sử dụng trong môi trường mà khoá đơn dễ dàng được chuyển như là trong cùng một văn phòng. Cũng dùng để mã hoá thông tin để lưu trữ trên đĩa.

Các vấn đề đối với Hệ mã hoá đối xứng:

- Phương pháp mã hoá đối xứng đòi hỏi người mã hoá và người giải mã phải cùng chung một khoá. Khoá phải được giữ bí mật tuyệt đối. "Dễ dàng" xác định một khoá nếu biết khoá kia và ngược lại.
- Hệ mã hoá đối xứng không an toàn nếu khoá bị lộ với xác xuất cao. Hệ này khoá phải được gửi đi trên kênh an toàn.
- Vấn đề quản lý và phân phối khoá là khó khăn, phức tạp khi sử dụng hệ mã hoá đối xứng. Người gửi và người nhận phải luôn thống nhất với nhau về khoá. Việc thay đổi khoá là rất khó và dễ bị lộ.
- Khuynh hướng cung cấp khoá dài mà nó phải được thay đổi thường xuyên cho mọi người, trong khi vẫn duy trì cả tính an toàn lẫn hiệu quả chi phí, sẽ cản trở rất nhiều tới việc phát triển hệ mật mã.

1.2.2.2 Mã hóa không đối xứng (Mã hóa công khai) .

Hệ mã hoá khoá công khai: là Hệ mã hoá trong đó khoá mã hoá là khác với khoá giải mã. Khoá giải mã "khó" tính toán được từ khoá mã hoá và ngược lại. Khoá mã hoá gọi là khoá công khai (Public key). Khoá giải mã được gọi là khoá riêng (Private key).

Nơi ứng dụng: Sử dụng chủ yếu trên các mạng công khai.

Các điều kiện của một hệ mã hoá công khai:

- Việc tính toán ra cặp khoá công khai K_B và bí mật k_B dựa trên cơ sở các điều kiện ban đầu, phải được thực hiện một cách dễ dàng, nghĩa là thực hiện trong thời gian đa thức.
- Người gửi A có được khoá công khai của người nhận B và có bản tin P cần gửi B, thì có thể dễ dàng tạo ra được bản mã C.

$$C = E_{KB} (P) = E_B (P)$$

Người nhận B khi nhận được bản mã C với khoá bí mật k_B, thì có thể giải mã bản tin trong thời gian đa thức.

$$P = D_{kB} (C) = D_B [E_B(P)]$$

- Nếu kẻ địch biết khoá công khai K_B cố gắng tính toán khoá bí mật thì chúng phải đương đầu với trường hợp nan giải, đó là gặp bài toán "khó".

1.2.3. Một số loại mã hoá

1.2.3.1 Hệ mã hoá RSA

Cho n=p*q với p,q là số nguyên tố lớn. Đặt P = C = Z_n

Chọn b nguyên tố với $\phi(n)$, $\phi(n)= (p-1)(q-1)$

Ta định nghĩa: $K=\{(n,a,b): a*b\equiv 1(\text{mod } \phi(n))\}$

Giá trị n và b là công khai và a là bí mật

Với mỗi K=(n,a,b), mỗi $x\in P$, $y\in C$ định nghĩa

Hàm mã hóa: $y = e_k(x) = x^b \text{ mod } n$

Hàm giải mã: $d_k(x) = y^a \text{ mod } n$

1.2.3.2 Hệ mã hoá ElGamal

Hệ thống mật mã với khoá công khai ElGamal có thể được dựa trên tuỳ ý các nhóm mà với họ đó lôga rời rạc được xem là không giải quyết được. Thông thường người ta dùng một nhóm con G_q(cấp q) của Z_p; ở đó p, q là các số nguyên tố lớn thoả mãn q|(p-1). Các nhóm khác có thể đạt được với các đường cong elliptic trên các trường hữu hạn. Vấn đề lôga rời rạc đối với các đường cong elliptic thì được xem là khó khăn hơn. Ở đây giới thiệu cách xây dựng nhóm Zp, với p là một số nguyên tố lớn.

Sơ đồ:

- Tạo ra số nguyên tố lớn p sao cho bài toán logarit rời rạc trong Z_p là khó (ít nhất $p = 10^{150}$); Chọn g là phần tử sinh trong Z^*_p .

- Lấy ngẫu nhiên một số nguyên α thoả mãn $1\leq \alpha \leq p-2$ và tính toán $h=g^{\alpha} \text{ mod } p$.

- Khoá công khai chính là (p, g, h), và khoá riêng là α.

Sự mã hoá : khoá công khai (p, g, h) muốn mã hoá thư tín m ($0\leq m <p$)

- Lấy ngẫu nhiên một số nguyên k, $0\leq k \leq p-2$.

- Tính toán $x = g^k \text{ mod } p$, $y = m*h^k \text{ mod } p$.

Sự giải mã. Để phục hồi được bản gốc m từ c = (x, y), ta làm như sau:

- Sử dụng khoá riêng α, tính toán $r = x^{p-1-\alpha}$. (Chú ý rằng $r = x^{p-1-\alpha} = x^{-\alpha} = (gk)^{-\alpha} = g^{-k\alpha}$).

- Phục hồi m bằng cách tính toán $m = y*r \text{ mod } p$.

1.2.3.3 Hệ mã hoá "ngưỡng"

Mục đích của hệ thống bí mật chìa khoá công khai bước đầu chỉ là chia sẻ 1 chìa khóa riêng giữa Ban kiểm phiếu để các thư tín được giải mã khi một nhóm lớn người kiểm phiếu cùng hợp tác. Chúng ta cần thay đổi sự tạo thành khoá và cách giải mã trong hệ thống bí mật ElGamal. Thư tín sẽ được mã hoá bình thường.

Sự tạo khoá: Kết quả của cách tạo khoá là mỗi người kiểm phiếu A_j sẽ sở hữu một phần s_j của bí mật s (một khoá riêng trong hệ thống bí mật ElGamal) và khoá công khai sẽ được tạo một cách công khai.

Ban kiểm phiếu đưa và công khai giá trị $h_j = g^{sj}$. Hơn nữa, các phần s_j được dùng để xây dựng lại bí mật s từ tập bất kì (t+1) phần, còn tập bất kì ≤ t phần thì không nói nên điều gì về bí mật s. Sơ đồ chia sẻ bí mật (t+1,N) của Shamir đã đạt được yêu cầu này. Để tính toán và phân phối các phần bí mật này đến Ban kiểm phiếu phải cần đến một nhóm thứ ba đáng tin cậy và dùng kênh untappable.

Do đó: $s = \sum_{j \in A} s_j \lambda_{j,A} = \prod l \in A - j \frac{\cdot l}{l - j}$

Khoá công khai là (p,q,h) với $h = g^s$

Sự giải mã: Để giải mã một văn bản mật mã (x,y) = (g^k, h^km) mà không có sự xây dựng lại bí mật s, Ban kiểm phiếu thực hiện theo cách sau:

1. Mỗi người kiểm phiếu A_j tung ra $w_j = x^{sj}$ và chứng minh bằng kiến thức cơ sở:

$$\text{Log}_g h_j = \log_x w_j$$

Giả sử A là tập bất kỳ (t+1) người kiểm phiếu vượt qua được chứng minh cơ sở ở trên.

Văn bản gốc có thể phục hồi bằng: m = y / x^s

$$x^s = x^{\sum_{j \in A} s_j \lambda_{j,A}} = \prod_{j \in A} w_j^{\lambda_{j,A}}$$

Nhiều nhất t phần s_j được công bố, vì từ (t+1) giá trị s_j sẽ tính toán được bí mật s (bằng phép nội suy Lagrange), và thư tín m sẽ được phục hồi trực tiếp như trong sự giải mã ElGamal.

1.2.3.4. Mã hoá đồng cấu

Xét một sơ đồ mã hoá xác suất. Giả sử P là không gian các văn bản chưa mã hoá và C là không gian các văn bản mật mã. Có nghĩa là P là một nhóm với phép toán 2 ngôi $\oplus$ và C là một nhóm với phép toán $\otimes$. Ví dụ E của sơ đồ mã hoá xác suất được hình thành bởi sự tạo ra khoá riêng và khoá công khai của nó. Giả sử $E_r(m)$ là sự mã hoá thư tín m sử dụng tham số (s) r ta nói rằng sơ đồ mã hoá xác suất là $(\oplus,\otimes)$-đồng cấu. Nếu với bất kỳ ví dụ E của sơ đồ này, ta cho $c_1 = E_{r1}(m_1)$ và $c_2 = E_{r2}(m_2)$ thì tồn tại r sao cho:

$$c_1 \otimes c_2 = E_r(m_1 \oplus m_2)$$

Chẳng hạn, sơ đồ mã hoá Elgamal là đồng cấu. Ở đây, P là tập tất cả các số nguyên modulo p ($P = Z_p$), còn $C = \{(a,b) \mid a,b \in Z_p\}$. Phép toán $\oplus$ là phép nhân modulo p . Đối với phép toán 2 ngôi $\otimes$ được định nghĩa trên các văn bản mật mã, ta dùng phép nhân modulo p trên mỗi thành phần.

Hai văn bản gốc m_0, m_1 được mã hoá:

$$E_{ko}(m_o) = (g^{ko}, h^{ko}m_o)$$
$$E_{k1}(m_1) = (g^{k1}, h^{k1}m_1)$$

Ở đó k_o,k_1 là ngẫu nhiên.

Từ đó: $E_{ko}(m_o)\, E_{k1}(m_1) = (g^{ko}, h^{ko}m_o)\, (g^{k1}, h^{k1}m_1) = E_k(m_om_1)$

với $k= k_o + k_1$

Bởi vậy, trong hệ thống bí mật ElGamal từ phép nhân các văn bản mật mã chúng ta sẽ có được phép nhân đã được mã hoá của các văn bản gốc tương ứng.

1.2.3.5 Mã nhị phân:

Giả sử rằng Alice muốn gửi cho Bob 1 chữ số nhị phân b. Cô ta không muốn tiết lộ b cho Bob ngay. Bob yêu cầu Alice không được đổi ý, tức là chữ số mà sau đó Alice tiết lộ phải giống với chữ số mà cô ta nghĩ bây giờ.

Alice mã hoá chữ số b bằng một cách nào đó rồi gửi sự mã hoá cho Bob. Bob không thể phục hồi được b tới tận khi Alice gửi chìa khoá cho anh ta. Sự mã hoá của b được gọi là một blob.

Một cách tổng quát, sơ đồ mã nhị phân là một hàm

ξ: {0,1} x X$\rightarrow$ Y, ở đó X, Y là những tập hữu hạn. Mỗi sự mã hoá của b là giá trị ξ (b,k), k$\in$ X. Sơ đồ mã nhị phân phải thoả mãn những tính chất sau:

- Tính che đậy (Bob không thể tìm ra giá trị b từ ξ (b,k))
- Tính mù (Alice sau đó có thể mở ξ (b,k) bằng cách tiết lộ b, k thì được dùng trong cách xây dựng nó. Cô ta không thể mở blob bởi 0 hay 1).

Nếu Alice muốn mã hoá một xâu những chữ số nhị phân, cô ta mã hoá từng chữ số một cách độc lập.

Sơ đồ mã hoá số nhị phân mà trong đó Alice có thể mở blob bằng 0 hay 1 được gọi là sự mã hoá nhị phân cửa lật.

Sự mã hoá số nhị phân có thể được thực hiện như sau:

Giả sử một số nguyên tố lớn p, một phần tử sinh g$\in$ Z_p và G$\in$ Z_p đã biết loga rời rạc cơ số g của G thì cả Alice và Bob đều không biết (G có thể chọn ngẫu nhiên).

Sự mã hoá nhị phân ξ: {0,1} x $Z_p \rightarrow Z_p$ là:

$$\xi (b,k) = g^k G^b$$

Đặt $\log_g G = a$. Blob có thể được mở bởi b bằng cách tiết lộ k và mở bởi –b bằng cách tiết lộ k-a nếu b=0 hoặc k+a nếu b=1. Nếu Alice không biết a, cô ta không thể mở blob bằng –b.

Tương tự, nếu Bob không biết k, anh ta không thể xác định b với chỉ một dữ kiện $\xi (b,k) = g^k G^b$.

Sơ đồ mã hoá chữ số nhị phân cưả lật đạt được trong trường hợp Alice biết a.

Nếu Bob biết a và Alice mở blob cho Bob thông qua kênh chống đột nhập đường truyền (untappable channel) Bob có thể sẽ nói dối với người thứ ba về sự mã hoá chữ số nhị phân b. Rất đơn giản, anh ta nói rằng anh ta nhận được k-a hoặc k+a (mà thực tế là k). Sơ đồ mã hoá số nhị phân mà cho phép người xác minh (Bob) nói dối về việc mở blob, được gọi là sự mã hoá nhị phân chameleon.

Thay vì mã hoá từng chữ số nhị phân trong sâu s một cách độc lập, Alice có thể mã hoá một cách đơn giản $0 \leq s \leq p$ bằng $\xi (b,k) = G^s g^k$. Hơn nữa, những thông tin về số a sẽ cho Alice khả năng mở ξ (s,k) bởi bất kì s', k' thoả mãn as+k= as'+k'.

1.3. KHÁI NIỆM VỀ KÝ ĐIỆN TỬ

1.3.1.Định nghĩa

Một sơ đồ chữ ký gồm bộ 5 (P, A, K, S, V) thỏa mãn các điều kiện dưới đây:

1. P là tập hữu hạn các bức điện (thông điệp) cụ thể
2. A là tập hữu hạn các chữ ký cụ thể
3. K không gian khóa là tập hữu hạn các khóa cụ thể

Sig_k là thuật toán ký $P \rightarrow A$

$$x \in P \rightarrow y = Sig_k(x)$$

Ver_k là thuật toán kiểm thử: (P, A) → (Đúng,sai)

$Ver_k(x, y)$ = | Đúng Nếu $y = Sig_k(x)$
| Sai Nếu $y \neq Sig_k(x)$

1.3.2. Phân loại các sơ đồ chữ ký điện tử

Chữ ký "điện tử" được chia làm 2 lớp, lớp chữ ký kèm thông điệp (message appendix) và lớp chữ ký khôi phục thông điệp (message recovery) như sau:

- Chữ ký kèm thông điệp: Đòi hỏi thông điệp ban đầu là đầu vào giải thuật kiểm tra . Ví dụ : chữ ký Elgamal.
- Chữ ky khôi phục thông điệp: Thông điệp ban đầu sinh ra từ bản thân chữ ký. Ví dụ: chữ ký RSA.

1.3.3. Một số sơ đồ ký số cơ bản

1.3.3.1. Sơ đồ chữ ký Elgamal

- Chọn p là số nguyên tố sao cho bài toán log rời rạc trong Z_p là khó.

Chọn g là phần tử sinh $\in Z_p^*$; $a \in Z_p^*$.

Tính $\beta \equiv g^a \bmod p$.

Chọn r ngẫu nhiên $\in Z^*_{p-1}$

- Ký trên x: Sig (x,r) = (γ, δ),

Trong đó $\gamma = g^k \bmod p$

$\delta = (x - a \gamma) r^{-1} \bmod (p-1)$.

- Kiểm tra chữ ký:

Ver(x, γ, δ)=True $\Leftrightarrow \beta^{\gamma} \gamma^{\delta} \equiv g^{x} \bmod p$

Ví dụ:

- chọn p=463; g=2; a=211;

$\beta \equiv 2^{211} \bmod 463 = 249$;

- chọn r =235; $r^{-1}=289$

- Ký trên x=112

Sig(x,r) = Sig (112,235)=(γ,δ)=(16,108)

$\gamma = 2^{235} \bmod 463 = 16$

δ= (112-211*16)*289 mod (463-1)=108

- Kiểm tra chữ ký:

Ver(x, γ, δ)=True $\Leftrightarrow \beta^{\gamma} \gamma^{\delta} \equiv g^{x} \bmod p$

$\beta^{\gamma} \gamma^{\delta} = 249^{16} * 16^{108} \bmod 463 = 132$

$g^{x} \bmod p = 2^{112} \bmod 463 = 132$

1.3.3.2. Sơ đồ chữ ký RSA

- Chọn p, q nguyên tố lớn .

Tính n=p.q; $\phi(n)=(p-1)(q-1)$.

Chọn b nguyên tố cùng $\phi(n)$.

Chọn a nghịch đảo với b; $a=b^{-1} \bmod \phi(n)$.

- Ký trên x: Sig (x) = $x^{a} \bmod n$

- Kiểm tra chữ ký: Ver (x,y)= True $\Leftrightarrow x \equiv y^{b} \bmod n$

Ví dụ: - p=3; q=5; n=15; $\phi(n)$= 8; chọn b=3; a=3

- Ký x =2:

Chữ ký : $y = x^{a} \bmod n = 2^{3} \bmod 15 = 8$

Kiểm tra: $x = y^{b} \bmod n = 8^{3} \bmod 15 = 2$ (chữ ký đúng)

1.3.3.3. Chữ ký "mù"

Chúng ta đòi hỏi chữ ký phải là thật (chỉ những người được ký mới ký) và được xác minh công khai (bất kì ai đều có thể xác minh xem chữ ký đưa ra ở thư tín là đúng hay không).

Nếu người ký có khoá công khai RSA: (n, e) và có khoá riêng tương ứng d, thì anh ta có thể ký thư tín x, $x \in Z_n$: $y = m^d$ (modulo). Cho ký số y của thư tín x, bất kỳ ai đều có thể xác minh tính đúng đắn của nó bằng cách kiểm tra xem $x = y^e$ (modulo) hay không.

Chú ý rằng phương pháp mã hoá và giải mã của hệ thống bí mật RSA được sử dụng trong việc làm dấu thư tín và xác minh ký số đó.

Giả sử rằng một người có nhu cầu muốn tìm ra ký số của thư tín x. Người này không muốn tiết lộ thư tín x cho bất kỳ ai, kể cả người đã ký thư tín đó. Người ký thì bị yêu cầu ký dấu một cách bí mật mà ngay cả người này cũng không biết mình ký gì.

Ví dụ: Giả sử Ban kiểm phiếu dùng sơ đồ chữ ký RSA (n, p, q, b, a).

- Cử tri che dấu x bởi $y = x*r^b \pmod n$, (r được chọn sao cho tồn tại phần tử nghịch đảo $r^{-1} \pmod n$).

- Cử tri gửi bí danh y cho Ban kiểm phiếu

- Ban kiểm phiếu ký trên bí danh y được chữ ký z: $z = y^a \pmod n$

- Ban kiểm phiếu gửi chữ ký z cho Cử tri.

- Cử tri "xoá mù" trên z sẽ tìm lại được chữ ký trên thư tín x bằng cách tính toán:

$$Unblind(z) = z*r^{-1} = (x*r^b)^a*r^{-1} = (x^a*r) * r^{-1} = x^a \pmod n$$

Cử tri đã có được chữ ký của Ban kiểm phiếu trên x, đó là $x^a \pmod n$.

Về mặt hình thức, sơ đồ ký số "mù" với khoảng trống thư tín x là một bộ 5 $(\eta,\chi,\sigma,\delta,\Gamma)$,ở đó:

- η là thuật toán xác suất đa thời gian, nó xây dựng được khoá công khai (pk) và khoá bí mật tương ứng (sk) của người làm dấu.

- χ là thuật toán đa thời gian, nó đưa vào thư tín $m \in M$, khoá công khai pk và một xâu tuỳ ý r, xây dựng một thư tín "mù" tuỳ ý.
- σ là thuật toán ký dấu đa thời gian, nó đưa vào thư tín mù y và chìa khoá bí mật sk, xây dựng ký số mù z trên y.
- δ là thuật toán hồi phục đa thời gian, nó đưa vào ký số mù z và giá trị tuỳ ý r.
- Γ là thuật toán xác minh ký số đa thời gian, nó đưa vào cặp thư tín – ký số (x,y) và khoá công khai pk cho kết quả đúng hoặc sai.

Đối với những ký số mù ở bước đầu (bước mà chìa khoá bí mật của sơ đồ ký số mù được chia sẻ trong N người kiểm phiếu).

1.4. CHIA SẺ BÍ MẬT

Khi bỏ phiếu từ xa, để đảm bảo bí mật, cử tri mã hoá nội dung lá phiếu. Ban kiểm phiếu phải giải mã mới biết được lá phiếu ghi gì. Thực tế có thể có một người hay một nhóm người của Ban kiểm phiếu muốn biết trước nội dung lá phiếu để thực hiện gian lận bầu cử (ví dụ: sửa nội dung lá phiếu). Để bảo đảm một người hay một nhóm người của Ban kiểm phiếu không thể biết trước nội dung lá phiếu, người ta dùng kỹ thuật "chia sẻ bí mật". Ví dụ:

- Chìa khoá để giải mã nội dung lá phiếu chia thành m mảnh, mỗi người trong Ban kiểm phiếu giữ một mảnh và đảm bảo rằng một nhóm người ít hơn m không thể khôi phục được.

- Bản thân nội dung lá phiếu có thể được chia thành m mảnh. Cử tri gửi cho m thành viên của Ban kiểm phiếu, mỗi người giữ một mảnh và phải bảo đảm rằng một nhóm ít hơn m không thể xác định được nội dung lá phiếu.

Với kỹ thuật này, cuộc bỏ phiếu bảo đảm được bí mật và kiểm soát được kết quả bỏ phiếu cụ thể là tránh gian lận.

Hiện nay có nhiều loại sơ đồ "chia sẻ bí mật" để thực hiện công việc trên.ví dụ: sơ đồ chia sẻ bí mật Shamir, cấu trúc mạch đơn điệu...

Sơ đồ "chia sẻ bí mật" Shamir:

Giả sử tập tất cả các bí mật có thể tạo thành 1 trường F (F có thể là tập các số thực, hoặc F = Z_p). F có ít nhất N + 1 phần tử khác nhau, biểu thị chúng bởi 0, 1, 2,…, N.

Sự phân phối khoá: Một bí mật s $\in$ F được phân bố trong số N người kiểm phiếu nhận được một phần s_j của nó, $s_j \in$ F. Chọn ngẫu nhiên một đa thức bậc t trên trường F thoả mãn f (0) = s. Người kiểm phiếu A_j nhận được phần s_j= f(j).

Sự xây dựng lại bí mật: Tập A gồm (t + 1) người kiểm phiếu lấy bí mật bằng cách xây dựng lại đa thức f (sử dụng phép nội suy Lagrange) và tính toán s = f(0):

$$S = f(0) = \sum f(j)\,\lambda_{j,A} = \sum s_j\,\lambda_{j,A}$$

$$\lambda_{j,A} = \prod_{l \in A - j} \frac{l}{l - j}$$

Thông tin mà t (hoặc ít hơn) người kiểm phiếu có về đa thức f không để lộ về giá trị f(0) = s. Với bất kì giá trị f(0) = r họ chọn, bằng khoá của mình họ có thể tính toán ra đa thức g thoả mãn g(0) = r.

1.5. KHÁI NIỆM XÁC THỰC ĐIỆN TỬ

Xác thực điện tử là việc chứng minh từ xa bằng phương tiện điện tử, sự tồn tại chính xác và hợp lệ danh tính của một chủ thể khi tham gia trao đổi thông tin điện tử như: cá nhân, tổ chức, dịch vụ,... hoặc một lớp thông tin nào đó mà không cần biết các thông tin đó cụ thể như thế nào, thông qua thông tin đặc trưng đại diện cho chủ thể đó mà vẫn đảm bảo được bí mật của chủ thể, hoặc lớp thông tin cần chứng minh.

Xác thực điện tử là việc cần thực hiện trước khi thực sự diễn ra các cuộc trao đổi thông tin điện tử chính thức.

Việc xác thực điện tử trong hệ thống trao đổi thông tin điện tử được uỷ quyền cho một bên thứ ba tin cậy. Bên thứ ba ấy chính là CA (Certification Authority), một cơ quan có tư cách pháp nhân thường xuyên tiếp nhận đăng ký các thông tin đặc trưng đại diện cho chủ thể: khoá công khai và lưu trữ khoá công khai cùng lý lịch của chủ thể trong một cơ sở dữ liệu được bảo vệ chặt chẽ. CA chuyên nghiệp không nhất thiết là cơ quan nhà nước. Điều quan trọng nhất của một CA là uy tín để khẳng định sự thật, bảo đảm không thể có chuyện "đổi trắng thay đen".

Mục đích của việc xác thực điện tử: chống giả mạo, chống chối bỏ, đảm bảo tính toàn vẹn, tính bí mật, tính xác thực của thông tin và mục đích cuối cùng là hoàn thiện các giải pháp an toàn thông tin.

Cơ sở ứng dụng để xây dựng các giải pháp an toàn cho xác thực điện tử là các hệ mật mã.

Ứng dụng trong: thương mại điện tử, trong các hệ thống thanh toán trực tuyến, là nền tảng của chính phủ điện tử.

Hiện nay, chứng thực điện tử được sử dụng trong khá nhiều ứng dụng, theo số liệu điều tra công bố vào tháng 8/2003 của tổ chức OASIS (Organization

for the Advancement of Structured Information Standard): 24,1% sử dụng trong việc ký vào các dữ liệu điện tử ; 16,3% sử dụng để đảm bảo cho e-mail ; 13,2% dùng trong thương mại điện tử ; 9,1% sử dụng để bảo vệ WLAN ; 8% sử dụng đảm bảo an toàn cho các dịch vụ web ; 6% sử dụng bảo đảm an toàn cho Web Server ; 6% sử dụng trong các mạng riêng ảo...

1.5.1. Xác thực dựa trên mật khẩu

Khi xác thực người dùng theo phương pháp này yêu cầu: Người dùng đã quyết định tin tưởng vào máy dịch vụ mà không có bảo mật theo giao thức SSL. Máy dịch vụ cần phải chứng thực người sử dụng trước khi cho phép họ có thể truy nhập tài nguyên của hệ thống.

Bước 1: Để đáp lại yêu cầu chứng thực từ máy dịch vụ, tại phía máy khách sẽ hiện một hộp hội thoại yêu cầu nhập mật khẩu. Người sử dụng phải nhập mật khẩu cho mỗi máy dịch vụ khác nhau trong cùng một phiên làm việc.

Bước 2: Máy khách sẽ gửi mật khẩu qua mạng mà không có một hình thức mã hoá nào.

Bước 3: Máy dịch vụ sẽ tìm kiếm mật khẩu trong cơ sở dữ liệu.

Bước 4: Máy dịch vụ sẽ xác định xem mật khẩu đó có quyền truy cập vào những tài nguyên nào của hệ thống.

Khi sử dụng hình thức này, mỗi người sử dụng phải nhập mật khẩu cho mỗi máy dịch vụ khác nhau. mỗi máy dịch vụ sẽ lưu lại dấu vết của các mật khẩu này cho mỗi người.

1.5.2. Xác thực định danh

Việc giao tiếp trên mạng điển hình là giữa một máy khách (như trình duyệt chạy trên máy cá nhân) và một máy dịch vụ (server – như máy chủ Web site). Việc chứng thực có thể được thực hiện ở cả hai phía. Máy dịch vụ có thể tin tưởng vào một máy khách và ngược lại.

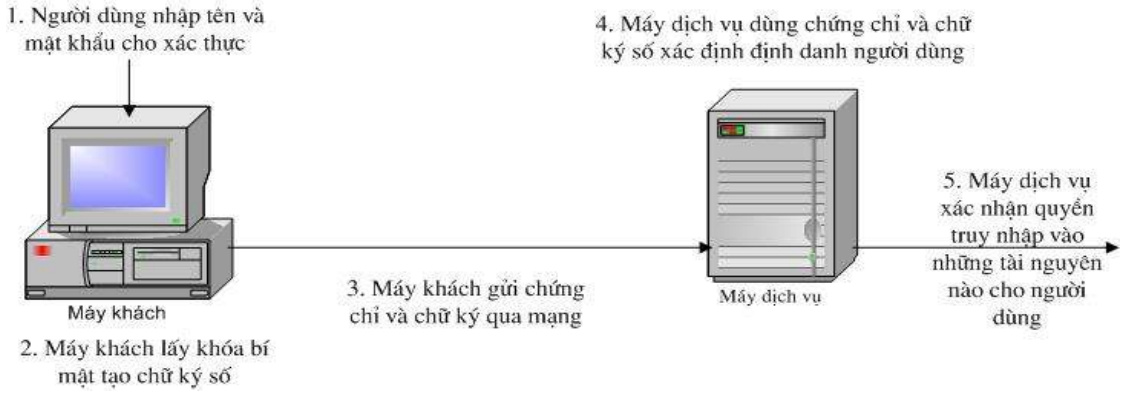
Việc xác thực ở đây không chỉ có ý nghĩa một chiều đối với người gửi, tức là người gửi muốn người nhận tin tưởng vào mình. Khi người gửi đã gửi thông điệp có kèm theo chữ ký số cùng với chứng chỉ số (ví dụ khi gửi thư điện

tử có sử dụng chữ ký số) thì không thể chối cãi là mình đã gửi. Có hai hình thức chứng thực máy khách sau:

- Dựa trên mẫu tên truy nhập và mật khẩu thông thường (username và password). Tất cả các máy dịch vụ cho phép người dùng nhập mật khẩu để có thể truy nhập vào hệ thống. Máy dịch vụ sẽ quản lý danh sách các username – password này.
- Chứng thực dựa trên chứng chỉ số. Chứng thực máy khách dựa trên chứng chỉ số (Là một phần của giao thức bảo mật SSL). Máy khách ký bằng số một phần được tạo ngẫu nhiên của dữ liệu, sau đó gửi cả chữ ký số và chứng chỉ số qua mạng. Máy dịch vụ(server) sẽ sử dụng ký thuật mã hoá khoá công khai để kiểm tra chữ ký số và xác định tính hợp lệ của chứng chỉ số.

1.5.3. Xác thực dựa trên chứng chỉ số

Chứng chỉ số có thể thay thế 3 bước đầu chứng thực bằng mật khẩu với một cơ chế cho phép người sử dụng chỉ phải nhập mật khẩu một lần mà không phải truyền qua mạng và người quản trị có thể điều khiển quyền truy nhập một cách tập trung.



Hình1.1 :Chứng chỉ số chứng thực cho máy khách kết nối tới máy dịch vụ

Các bước ở hình trên có sử dụng thêm giao thức bảo mật SSL. Máy khách phải có một chứng chỉ số để cho máy dịch vụ có thể nhận diện. Sử dụng chứng chỉ số để chứng thực được xem là có lợi thế hơn khi dùng mật khẩu. Bởi vì nó dựa trên những gì mà người sử dụng có : Khóa bí mật và mật khẩu để vảo vệ khóa bí mật. Nhưng có một điều cần chú ý là chỉ có chủ của máy khách mới

được phép truy nhập vào máy khách và phải nhập mật khẩu để vào cơ sở dữ liệu của chương trình có sử dụng khóa bí mật (mật khẩu này có thể phải nhập lại trong một khoảng thời gian định kỳ cho trước).

Cả hai cơ chế chứng thực dựa trên mật khẩu và chứng chỉ số đều cần phải truy nhập mức vật lý tới các máy cá nhân và mật khẩu. Mã hóa khóa công khai chỉ có thể kiểm tra việc sử dụng một khóa bí mật tương ứng với một khóa khóa công khai trong một chứng chỉ số. Nó không đảm nhận trách nhiệm bảo vệ mức vật lý và mật khẩu sử dụng khóa bí mật. Trách nhiệm này thuộc về người sử dụng.

Các bước trong hình trên:

- ***Bước 1:*** Phần mềm máy khách (ví dụ như Communicator) quản lý cơ sở dữ liệu về các cặp khóa bí mật và khóa khóa công khai. Máy khách sẽ yêu cầu nhập mật khẩu để truy nhập vào cơ sở dữ liệu này chỉ một lần hoặc theo định kỳ. Khi máy khách truy cập vào một máy dịch vụ có sử dụng SSL và cần chứng thực máy khách dựa trên chứng chỉ số, người sử dụng chỉ phải nhập mât khẩu một lần, họ không cần phải nhập lại khi cố gắng truy nhập lần thứ hai hoặc truy nhập vào một máy dịch vụ khác.

- ***Bước 2:*** Máy khách sẽ sử dụng khóa bí mật tương ứng với chứng chỉ cần thiết, và sử dụng khóa bí mật đó để ký cho một vài dữ liệu mà được tạo ra một cách ngẫu nhiên cho mục đích chứng thực từ cả phía máy khách và máy dịch vụ. Dữ liệu này và chữ ký số thiết lập một bằng chứng để xác định tính hợp lệ của khóa bí mật. Chữ ký số có thể được kiểm tra bằng khóa công khai tương ứng với khóa khóa bí mật đã dùng để ký, nó là duy nhất trong mỗi phiên làm việc của giao thức SSL.

- ***Bước 3:*** Máy khách sẽ gửi cả chứng chỉ và bằng chứng (một phần của dữ liệu được tạo một cách ngẫu nhiên và được ký) qua mạng.

- ***Bước 4:*** Máy dịch vụ sẽ sử dụng chứng chỉ số và bằng chứng đó để chứng thực người sử dụng.

- ***Bước 5:*** Tại bước này máy dịch vụ có thể thực hiện một cách tùy chọn các nhiệm vụ chứng thực khác, như việc xem chứng chỉ của máy khách có trong một cơ sở dữ liệu mà dùng để lưu trữ và quản lý các chứng chỉ số. Máy dịch vụ tiếp tục xác định xem người sử dụng có những quyền gì đối với tài nguyên của hệ thống.

Chương 2: BỎ PHIẾU ĐIỆN TỬ

2.1. QUI TRÌNH BỎ PHIẾU TỪ XA

Những cuộc bỏ phiếu từ xa hay những cuộc bỏ phiếu truyền thống đều cần có các thành phần trong Ban tổ chức bỏ phiếu và các thành phần kỹ thuật trong Hệ thống bỏ phiếu gồm có:

- Ban điều hành: quản lý các hoạt động bỏ phiếu, trong đó có thiết lập danh sách cử tri cùng các hồ sơ của mỗi cử tri, qui định có chế định danh cử tri.

- Ban đăng ký: nhận dạng cử tri và ký cấp quyền bỏ phiếu cho họ. Có hệ thống "ký" hỗ trợ.

- Ban kiểm tra: xác minh tính hợp lệ của lá phiếu; vì lá phiếu đã mã hoá nên Ban kiểm phiếu không thể biết được lá phiếu có hợp lệ không, nên cần phải xác minh tính hợp lệ của lá phiếu trước khi nó đến hòm phiếu. (Bỏ phiếu truyền thống không có ban này).

- Ban kiểm phiếu: tính toán và thông báo kết quả bỏ phiếu. Có hệ thống "kiểm phiếu" hỗ trợ.

- Hệ thống máy tính và các phần mềm phục vụ qui trình bỏ phiếu từ xa.

- Người trung thực kiểm soát Server đảm bảo yêu cầu bảo mật và toàn vẹn kết quả bỏ phiếu.

- Một số kỹ thuật bảo đảm an toàn thông tin: chữ ký mù, mã hoá đồng cấu, chia sẻ bí mật, "chứng minh không tiết lộ thông tin".

- Hệ thống phân phối khoá tin cậy sẵn sàng cung cấp khoá cho công việc mã hoá hay ký "số".

2.1.1. Qui trình tổng quát

Một qui trình bỏ phiếu từ xa bao gồm bốn giai đoạn chính: giai đoạn đăng ký, giai đoạn bỏ phiếu, giai đoạn kiểm tra và giai đoạn kiểm phiếu. Mỗi giai đoạn có thể gồm có nhiều pha hơn.

2.1.1.1.Giai đoạn đăng ký:

a. Công việc:

* Cử tri:

- Cử tri chọn bí mật số định danh x, giấy chứng minh thư điện tử (CMT), thông tin nhận dạng (ví dụ như vân tay). Cử tri "làm mù" x thành y=Blind(x).

- Cử tri gửi tới ban đăng ký thông tin nhận dạng của mình CMT, số y (định danh x được cử tri làm mù thành y).

* Ban đăng ký:

- Ban đăng ký nhận dạng cử tri , kiểm tra CMT của cử tri.

- Nếu hồ sơ của cử tri hợp lệ, khớp với danh sách cử tri của Ban điều hành, cử tri chưa xin cấp chữ ký lần nào, thì ra lệnh cho Hệ thống "ký" lên y. Đó là chữ ký z=sign(y).

- Ban đăng ký ghi số CMT của cử tri vào danh sách cử tri đã được cấp chữ ký (để tránh việc cử tri đăng ký bỏ phiếu nhiều lần).

- Ban đăng ký gửi chữ ký z về cho cử tri.

* Cử tri:

- Khi nhận được chữ ký này,cử tri "xoá mù" trên z, họ sẽ nhận được chữ ký sign(y)trên định danh thật x. Lá phiếu có gắn chữ ký sign(x) được xem như đã có chữ ký của Ban đăng ký; đó lá lá phiếu hợp lệ để cử tri ghi ý kiến của mình.

- Cử tri có thể kiểm tra chữ ký của Ban đăng ký trên lá phiếu của mình có hợp lệ hay không bằng cách dùng hàm kiểm tra chữ ký và khoá công khai của Ban đăng ký. (Chú ý: khoá ký trên định danh của cử tri được chia sẻ cho mọi thành viên của Ban đăng ký và Ban kiểm tra, nhờ đó sau này Ban kiểm tra có thể phát hiện ra những cử tri giả mạo chữ ký của Ban đăng ký.)

b. Kỹ thuật sử dụng:

- Kỹ thuật "chia sẻ khoá bí mật" :

- Hệ thống phân phối khoá tin cậy đã chia sẻ khoá ký cho các thành viên Ban đăng ký và ban kiểm tra trước đó. Sau khi xét duyệt hồ sơ xin chữ ký của cử

tri, nếu mọi thành viên của Ban đăng ký đều nhất trí cho ký thì họ sẽ khớp các mảnh khoá riêng để nhận được khoá ký.

- Mục đích của kỹ thuật: từng thành viên của Ban đăng ký không thể tuỳ tiện cấp chữ ký.

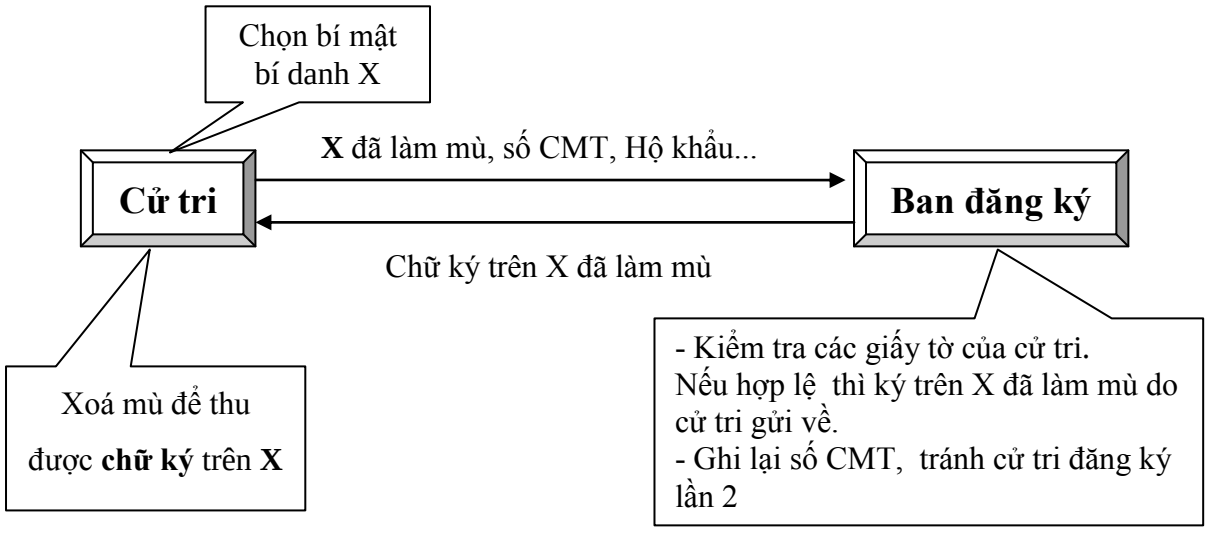
- Kỹ thuật "chữ ký mù":

- Ban đăng ký sử dụng kỹ thuật ký "mù" để ký tên lên định danh"mù" của cử tri.

- Mục đích của kỹ thuật: Ban đăng ký không thể biết được ai đã ghi ý kiến vào lá phiếu tức là bảo đảm không lộ danh tính cử tri.

c. Sơ đồ giai đoạn đăng ký:

Để được quyền bầu cử, cử tri phải có chữ ký của Ban đăng ký, qui trình diễn ra như sau:



Hình 2.1. Sơ đồ giai đoạn đăng ký

2.1.1.2.Giai đoạn bỏ phiếu:

a. Công việc:

- Sau khi lá phiếu có chữ ký của Ban đăng ký, cử tri ghi ý kiến (lựa chọn) của mình vào lá phiếu

- Cử tri mã hoá lá phiếu bằng khoá công khai của Ban kiểm phiếu.

- Cử tri gửi tới Ban kiểm phiếu: lá phiếu đã mã hoá, định danh thật (không bị làm mù) của họ, chữ ký của Ban đăng ký trên lá phiếu, "chứng minh không tiết lộ thông tin" về lá phiếu.

Chú ý rằng lá phiếu không được chuyển thẳng tới hòm phiếu, mà trước đó phải qua Ban kiểm tra. Tại đây họ kiểm tra chữ ký cấp quyền bỏ phiếu có bị giả mạo không, họ xác minh tính hợp lệ của lá phiếu.

b. Kỹ thuật sử dụng:

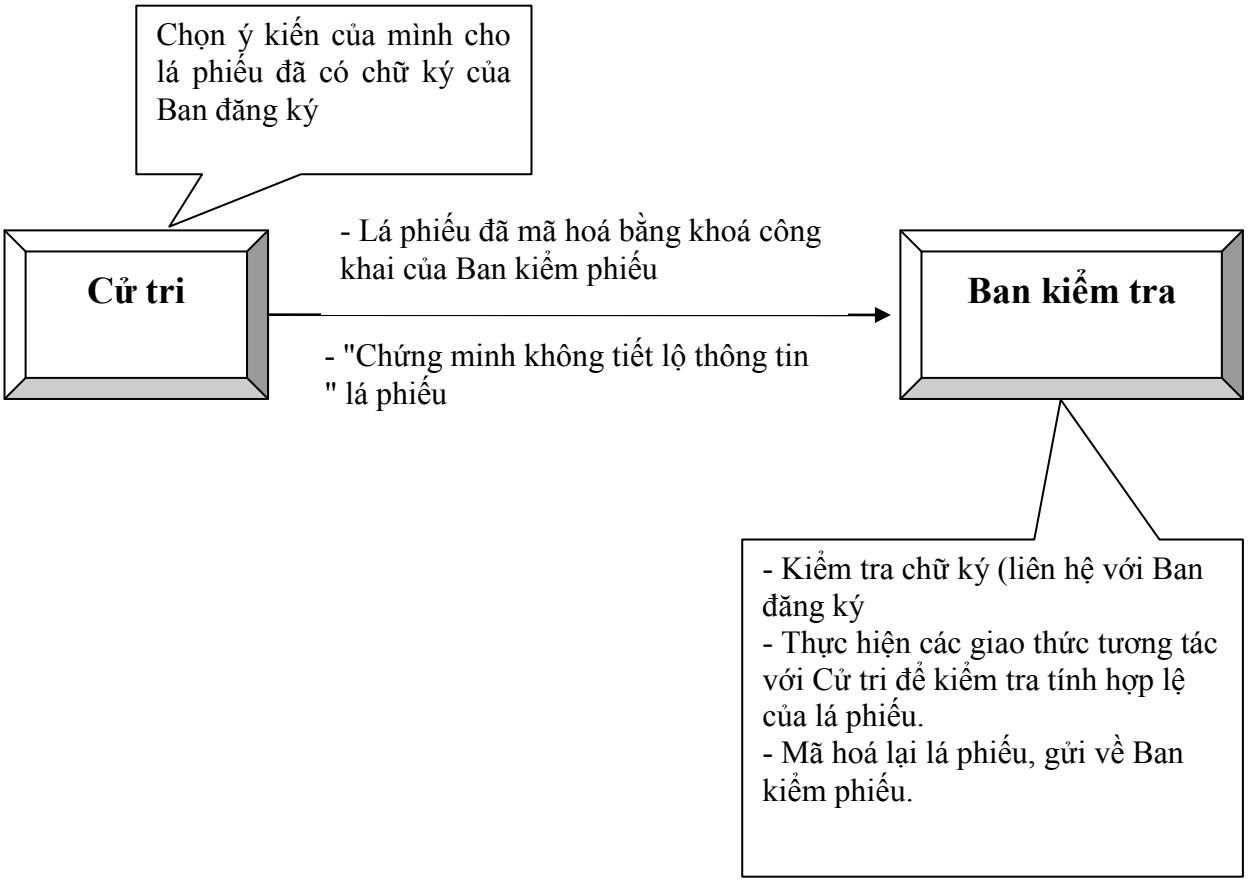
- Kỹ thuật "mã hoá đồng cấu": mã hoá đồng cấu có tính chất đặc biệt là tích của các lá phiếu được mã hoá bằng tổng các lá phiếu được mã hoá. Điều này rất thích hợp cho loại bỏ phiếu điện tử khi mã các lá phiếu được mã hoá thành 0 và 1.

- Mục đích của kỹ thuật: Ban kiểm phiếu không cần giải mã từng lá phiếu, vẫn có thể kiểm phiếu được.

- Kỹ thuật "chứng minh không tiết lộ thông tin"

- Mục đích của kỹ thuật: ở giai đoạn sau, ban kiểm tra có cơ sở để xác minh tính hợp lệ của lá phiếu (vì ở dưới dạng mã hoá, nên không thể biết lá phiếu có hợp lệ không)

c. Sơ đồ giai đoạn bỏ phiếu và kiểm tra:



Hình 2.2 Sơ đồ giai đoạn bỏ phiếu và kiểm tra

2.1.1.3. Giai đoạn kiểm tra:

a. Công việc:

- Kiểm tra chữ ký, cấp quyền bỏ phiếu trên lá phiếu (Liên hệ với Ban đăng ký).

- Kiểm tra tính hợp lệ của lá phiếu (tương tác với cử tri; nếu lá phiếu là giả mạo thì lá phiếu này sẽ không được gửi tới hòm phiếu).

- Mã hoá lại lá phiếu, gửi về hòm phiếu.

Ban kiểm tra đứng trung gian giữa Cử tri và Ban kiểm phiếu để ngăn chặn một số tình huống thiếu an toàn hay vi phạm luật bỏ phiếu, ví dụ trường hợp mua bán phiếu bầu (phương pháp bỏ phiếu truyền thống không cần giai đoạn này).

b. Kỹ thuật sử dụng:

- Kỹ thuật ký số:

- Mục đích của kỹ thuật: kiểm tra chữ ký cấp quyền bỏ phiếu trên lá phiếu.

- Kỹ thuật "chứng minh không tiết lộ thông tin":

- Mục đích của kỹ thuật: để kiểm tra tính hợp lệ của lá phiếu.

- Kỹ thuật mã hoá:

- Mục đích của kỹ thuật: mã hoá lại lá phiếu và gửi về hòm phiếu.

2.1.1.4.Giai đoạn kiểm phiếu

a. Công việc:

- 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 đã mã hoá gửi về. Theo phương pháp mã hoá đồng cấu, Ban kiểm phiếu không cần giải mã từng lá phiếu mà vẫn có thể kiểm phiếu được (tùy từng loại phiếu). Khi kiểm phiếu, các thành viên Ban kiểm phiếu dùng các mảnh khoá riêng của mình để khôi phục khoá bí mật (khoá này đã bị chia sẻ qua một sơ đồ chia sẻ bí mật). Ban kiểm phiếu dùng khoá bí mật này để tính kết quả cuộc bầu cử.

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

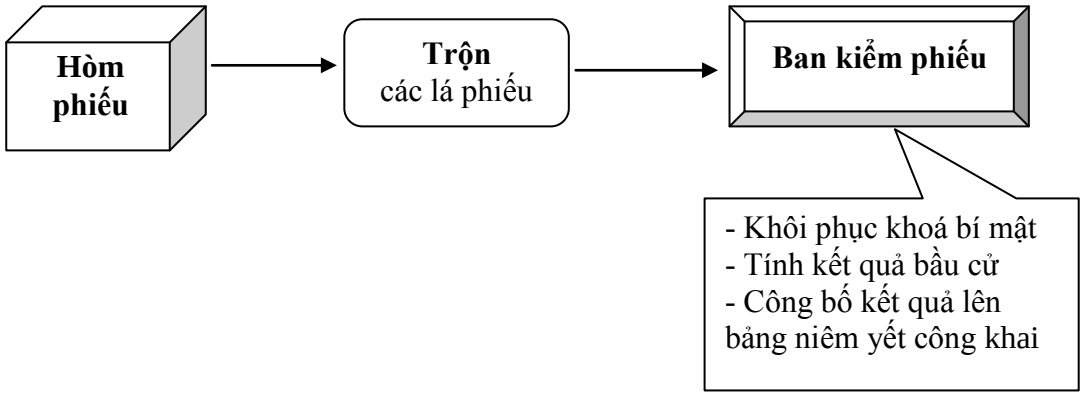
b. Kỹ thuật sử dụng:

- Kỹ thuật "Trộn":

Mục đích của kỹ thuật: ban kiểm phiếu gồm m thành viên, để họ không thể biết được lá phiếu nào là của ai, người ta xây dựng hệ thống mã hoá m tầng và giải mã m lần mới biết nội dung của các lá phiếu. Kỹ thuật "Chia sẻ bí mật"

- Kỹ thuật "Mã hoá đồng cấu"

c. Sơ đồ giai đoạn kiểm phiếu



Hình 2.3: Sơ đồ giai đoạn kiểm phiếu

2.1.1.4. Yêu cầu

Trong thực hành, qui trình bỏ phiếu từ xa phải thỏa mãn vài yêu cầu:

Tính hợp pháp: Chỉ có những cử tri hợp lệ được phép bỏ phiếu. Mỗi cử tri chỉ được bỏ phiếu 1 lần.

Tính bí mật: Không có sự liên hiệp nào của những người tham gia. Không cử tri nào có thể biết được bất kỳ thông tin lá phiếu của cử tri khác.

Tính cá nhân: Mỗi cử tri hợp pháp có thể kiểm tra rằng lá phiếu của anh ta thật sự được kiểm phiếu.

Tính xác minh phổ thông: Bất kỳ cử tri nào hoặc người quan sát có thể kiểm tra cuộc bầu cử rõ ràng, chung cuộc được công bố thật sự là tổng những lá phiếu.

Tính rõ ràng: Không có người tham gia nào có thể biết được bất kỳ thông tin nào quanh Bộ phận kiểm phiếu trước Giai đoạn kiểm phiếu.

Tính trung thực: Không có sự liên hiệp nào của những cử tri có thể phá vỡ cuộc bầu cử và bất kỳ hành vi gian lận nào cũng sẽ được phát hiện ra.

2.2. MỘT SỐ QUI TRÌNH BỎ PHIẾU

2.2.1. Qui trình bỏ phiếu Radwin

Đi cùng qui trình này là một Ban tổ chức bỏ phiếu đáng tin cậy, đóng vai trò vừa là một Hội đồng bầu cử, vừa là một Ban kiểm phiếu. Tất nhiên qui trình cũng có thể mở rộng để liên kết với Ban tổ chức để điều khiển cuộc bầu cử với sự an toàn cao hơn.

Cử tri nào mà cố gắng bỏ phiếu 2 lần đều bị phát hiện. Qui trình đòi hỏi sự tồn tại của 1 kênh ẩn danh để duy trì sự trao đổi qua lại (người nhận thư ẩn danh có thể gửi lại cho người gửi ẩn danh).

Giai đoạn mở đầu: Hội đồng bầu cử tạo ra và công bố khoá công khai RSA (n, e) và tham số chắc chắn l.

Giai đoạn đăng ký:

Cử tri V với CMND ID xây dựng tên riêng (dấu hiệu) P của mình. Để cho dễ hiểu, cách thức tiến hành được mô tả trong sơ đồ 2.4.

Cử tri lựa chọn các số a_k, c_k, d_k, r_k, (k=1,2,…,2l) một cách ngẫu nhiên từ Z_n và tính $B_k = r^e_k f(x_k, y_k)$.

Ở đó $x_k = g (a_k, c_k)$; $y_k = g (a_k \oplus ID, d_k)$

(B_k là thư mù $f(x_k, y_k)$). Anh ta gửi B_k tới Ban kiểm tra, k=1,2,…,2l.

Không có lý do nào khiến Ban tổ chức nghĩ rằng cử tri đã xây dựng B_k, k = 1,2,…,2l như trên. Do vậy, cử tri sẽ bị yêu cầu mở một nửa của B_k, nửa này do Ban kiểm tra chọn ngẫu nhiên. (Ta kí hiệu tập các B_k được chọn là R). Cử tri mở B_k bằng cách tiết lộ các số a_k, c_k, d_k, r_k được sử dụng trong phép xây dựng.

Ban kiểm tra xem các giá trị tiết lộ có thực sự phù hợp với B_k hay không, xác minh xem:

$$B_k = r^e_k f(g(a_k, c_k), g(a_k \oplus ID, d_k)) \text{ với mọi } k \in R.$$

Nếu điều này đúng thì nửa còn lại của B_k cũng được coi là xây dựng đúng. Trái lại Hội đồng bầu cử sẽ bác bỏ sự đăng ký.

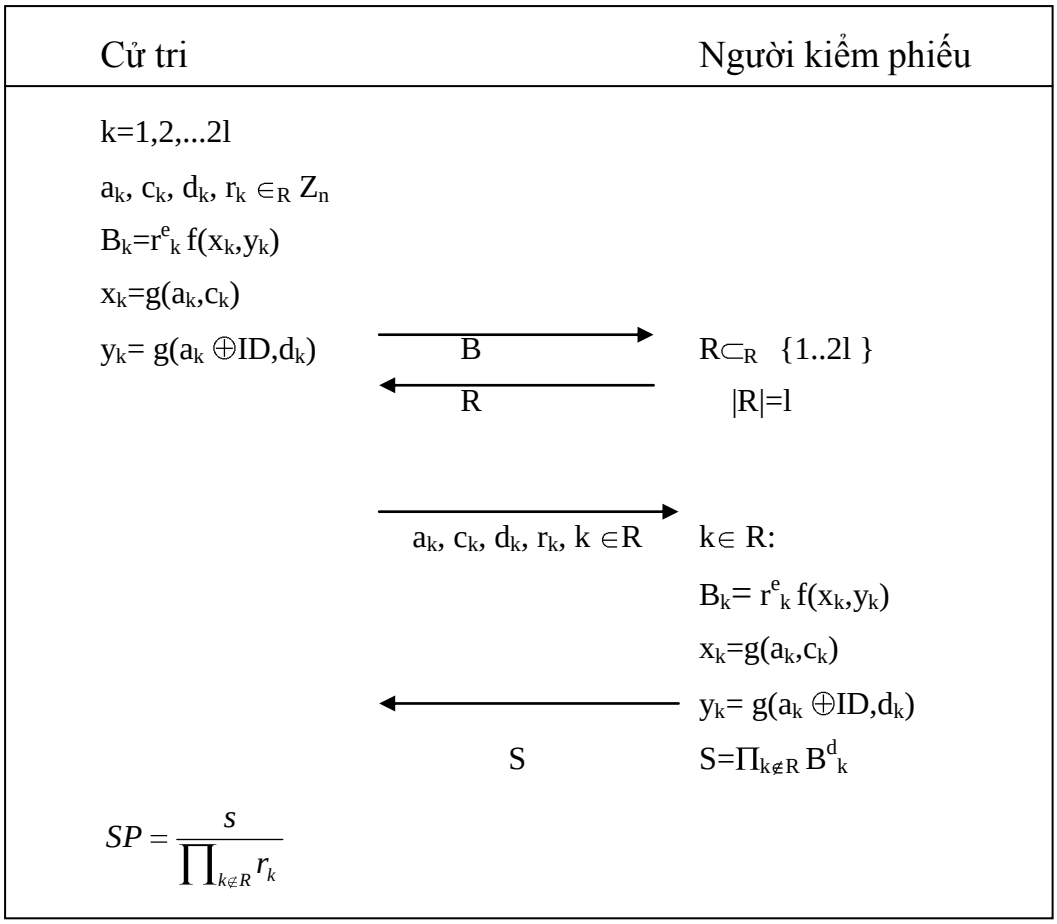
Hơn nữa, Hội đồng bầu cử phần B_k còn lại ($k \notin R$) bằng cách tính toán $S_k = B_k^d$, $k \notin R$, ở đó d là khoá bí mật RSA của nó và gửi tới cử tri $S = \prod_{k \notin R} S_k$

Chú ý rằng $S_k = B_k^d = (r^e_k f(x_k, y_k))^d = r^{ed}_k f(x_k, y_k)^d = r_k f(x_k, y_k)$ nên:

$$S = \prod_{i \notin \emptyset} r_k f(x_k, y_k)^d.$$

Cuối cùng cử tri tính toán tên riêng của anh ta là $P = \prod_{k \notin R} f(x_k, , y_k)$ và chữ kí của nó $SP = \frac{S}{\prod_{k \notin R} r_k} = \prod_{k \notin R} j(x_k, y_k)^d$

Tập hợp các a_k, c_k, d_k với $k \in R$ không còn ý nghĩa nữa. Để đơn giản ta kí hiệu các phần tử còn lại a_j, c_j, d_j với $j \in R$ là a_1, c_1, d_1,…,a_l, c_l, d_l.



Sơ đồ 2.4: Giai đoạn đăng kí - xây dựng tên riêng.

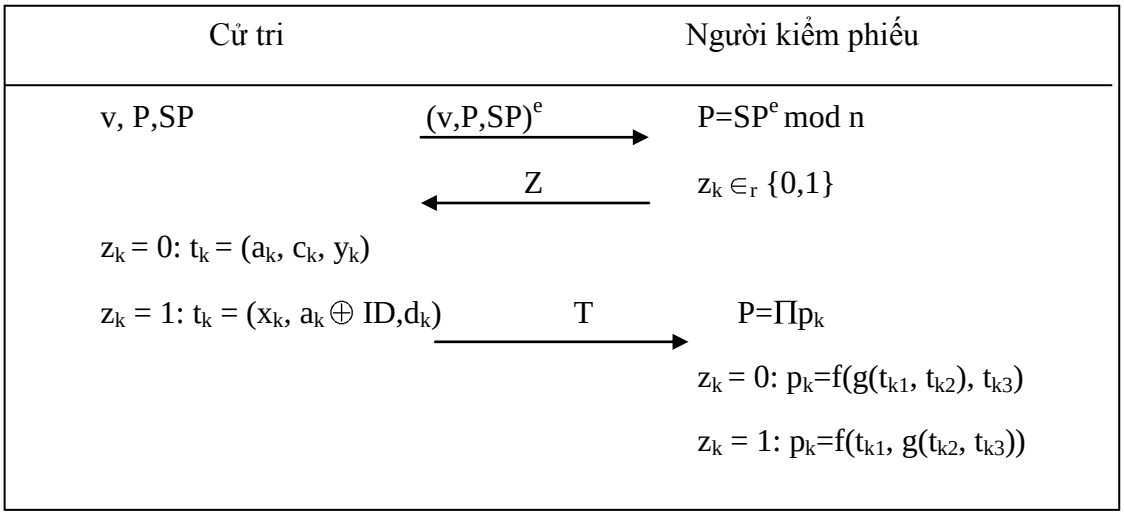
Giai đoạn bỏ phiếu: Cử tri chọn phiếu v của mình và tạo ra phiếu kín (v, P, SP), mã hoá nó với khoá công khai (e, n) của Hội đồng bầu cử và gửi $(v, P, SP)^e$ modulo qua kênh ẩn danh.

Ban kiểm phiếu giải mã thư tín này và xác minh chữ kí SP với tên riêng P, và gửi lại cử tri 1 vectơ nhị phân ngẫu nhiên $Z = (Z_1,\ldots,Z_l)$ với độ dài l.

Cử tri hồi âm với l bộ ba, mở một phần cấu trúc tên riêng của anh ta. Nếu $Z_k = 0$, bộ ba thứ k là a_k, c_k, y_k. Nếu $Z_k = 1$ bộ ba thứ k là x_k, $a_k \oplus ID$, d_k. Như vậy với mỗi k một đối số của f đã được tiết lộ trực tiếp, đối số còn lại có thể tính toán như là giá trị ra của hàm g, hàm này nhận hai số được tiết lộ còn lại làm đối số.

Ban kiểm phiếu xác minh rằng sự trả lời của cử tri là hoàn toàn phù hợp với tên riêng P mà anh ta gửi đến.

Nếu việc kiểm tra tên riêng P thành công, Ban kiểm phiếu có thể quyết định với xác suất cao sự đồng nhất của cử tri này.



Sơ đồ 2.5: Giai đoạn bầu cử

Giai đoạn kiểm phiếu: Ban kiểm phiếu đếm các phiếu hợp lý nhận được và công khai tổng số cuối cùng. Có 2 sự khác nhau có thể xảy ra trong quá trình đếm là:

1. Sự khác nhau không được liệt kê: Chỉ tổng của các phiếu mới được công khai.

2. Sự khác nhau được liệt kê: Ban kiểm phiếu công bố danh sách có chứa cả những phiếu kín đã nhận được $(v, P, SP)^e$ tên riêng P, SP thách đố Z với những câu trả lời T và những lá phiếu tương ứng v.

Những tính chất đạt được:

- Tính hợp pháp: chỉ có những cử tri hợp lệ mới được bỏ phiếu. Cử tri không thể xây dựng được tên riêng của mình. Cử tri cần có chữ kí của Hội đồng bầu cử. Hội đồng bầu cử chỉ cấp cho anh ta 1 tên riêng. Nếu anh ta cố gắng dùng tên riêng đó 2 lần thì sự giống nhau đó sẽ bị phát hiện với xác suất lớn. Tính hợp pháp đạt được nếu Hội đồng bầu cử trung thực.
- Tính bí mật: Đến tận cuối giai đoạn đăng kí, Hội đồng bầu cử có thể không biết gì về tên riêng của cử tri. Mối quan hệ giữa cử tri và tên riêng của anh ta được bảo vệ bởi sơ đồ chữ kí mù.

2.2.2.Qui trình bỏ phiếu JL

Qui trình này yêu cầu lá phiếu thực sự hợp lệ phải có dạng:

$$v_i = v_i||R_i||g(v_i||R_i||RD)$$

Ở đó v_i là sự chú tâm của cử tri V_i, g là hàm 1 chiều, R_i là các chữ số nhị phân nhẫu nhiên được tạo ra bởi cử tri và RD là một nhãn bầu cử. RD được xác định và công bố bởi Hội đồng bầu cử ở giai đoạn mở đầu và phải là duy nhất đối với mỗi cuộc bầu cử.

RD ngăn cản hiện tượng cử tri sử dụng lại lá phiếu của cuộc bầu cử trước. Vì lá phiếu là một phần của dấu hiệu, những dấu hiệu của cuộc bầu cử trước sẽ không còn tác dụng nữa. Hội đồng bầu cử không cần tạo lại sơ đồ chữ ký trước mỗi cuộc bầu cử.

Giai đoạn mở đầu: Hội đồng bầu cử tạo ra khoá công khai RSA (n, e) (cho chữ ký mù). Ban kiểm phiếu thành lập hệ thống mã hoá ElGamal với khoá công khai (p, g, h).

Giai đoạn đăng ký: Cử tri V_i với CMND ID_i chọn ngẫu nhiên xâu r_i, s_i và xây dựng dấu hiệu:

$$X_i = f(ID_i \,||\, s_i)||\, RD||\, EV_i.$$

Ở đó $EV_i = (g^{ki}, h^{ki} v_i)$, $k_i \in_R Z_p$, là phiếu thật v_i đã được mã hoá. Cử tri làm mù dấu hiệu của mình $e_i = r_i^e x_i$ và gửi thư tín đã làm mù đến Hội đồng bầu cử.

Hội đồng bầu cử kiểm tra xem cử tri V_i đã đăng kí chưa. Nếu chưa Hội đồng bầu cử sẽ gửi $d_i = e_i^d$ tới cử tri.

Giai đoạn bỏ phiếu: Cử tri đưa ra chữ kí $y_i = d_i/r_i = x_i^d$ và gửi (x_i, y_i) ẩn danh tới Hội đồng bầu cử. Hội đồng bầu cử kiểm tra $y_i^e = x_i$. Nếu đúng thì các chữ số nhị phân thừa RD từ x_i là hợp lý, anh ta ghi lại (x_i,y_i) và chỉ giữ một bản sao của x_i.

Giai đoạn kiểm phiếu: Ban kiểm phiếu công bố tất cả ngững phiếu kín được chấp nhận (x_i, y_i). Mỗi cử tri phải kiểm tra xem phiếu của anh ta đã được công bố chưa. Nếu phiếu kín của anh ta bị bỏ qua, anh ta có thể phản đối bằng cách đưa ra (x_i, y_i).

Ban kiểm phiếu yêu cầu (t+1) người kiểm phiếu trung thực gửi phần bí mật của họ đến. Anh ta tính toán khoá bí mật bước đầu và phục hồi được ý định của các cử tri. Hội đồng bầu cử công bố tất cả các phiếu kín (x_i, y_i, v_i), tất cả các sự đăng kí e_i và khoá bí mật bước đầu. Bất kì ai đều có thể kiểm tra tính hợp lý của các phiếu kín và xem tổng số phiếu kín có bằng tổng số đăng kí hay không để ngăn chặn Ban kiểm phiếu bỏ thêm phiếu kín vào.

Những tính chất đạt được:

- Tính hợp pháp: Mỗi cử tri chỉ có thể đạt được 1 dấu hiệu. Dấu hiệu không hợp lý hoặc trùng sẽ bị loại. Lá phiếu không hợp lệ cũng sẽ không được tính.

- Tính bí mật: sự liên hệ giữa phiếu kín (x_i, y_i) và cử tri được bảo vệ bởi sự đảm bảo trong sơ đồ chữ kí RSA. Việc lấy được ID_i từ phiếu kín cũng không thể thực hiện được vì f là hàm một chiều. Phiếu kín đã được gửi (x_i, y_i) không thể tìm lại được người bỏ phiếu đó vì nó được chuyển đi qua kênh ẩn danh.

- Tính cá nhân: Cử tri có thể kiểm tra xem dấu hiệu của mình có trên danh sách hay không.

- Tính chống chối bỏ: Cử tri không thể từ chối sau khi đã tham gia đăng ký.
- Tính trung thực: Hội đồng bầu cử không thể đóng giả cử tri từ chối bỏ phiếu vì không thể tạo ra chữ ký hợp lý được.

2.2.3. Qui trình bỏ phiếu Benaloh

Trong qui trình này, hai quá trình cơ bản được dùng là: chia sẻ bí mật và sự mã hoá khoá công khai xác suất với tính đồng cấu

$$E(m_1, k_1)\, E(m_2, k_2) = E(m_1 + m_2, k_1 k_2)$$

(k_1 , k_2 là các tham số ngẫu nhiên được dùng trong các mã hoá m_1, m_2)

➢ **Sơ đồ bầu cử Yes - No**

Giai đoạn mở đầu*:* mỗi người kiểm phiếu A_j tạo ra cặp khoá công khai của mình. Sự mã hoá m với khoá công khai của người kiểm phiếu A_j được ký hiệu là $E_j(m)$.

Giai đoạn bỏ phiếu: cử tri bỏ phiếu là 0 hoặc 1 theo cách sau:

1, Cử tri tạo cặp (v_1 , v_2) là một hoán vị của 0, 1

2, Với mỗi i =1,2 cử tri tạo ra các phần $s_1(v_i)$,..., $s_N(v_i)$ bằng cách dùng sơ đồ chia sẻ bí mật (t+1, N) cuả Shamir với các bí mật là v_i

3, Cử tri mã hoá phần thứ j với khoá công khai của người kiểm phiếu A_j. Cử tri nhận được:

$h=(h_1, h_2)$

với: $h_i= (h_{i1}, h_{i2},. . ., h_{iN})$, i=1,2

$h_2 =E_j(s_j(v_i), k_{ij})$, j = 1,...,N

4, Cử tri công bố h và chứng tỏ với người kiểm phiếu rằng nó được tạo đúng.

5, Cử tri chọn h_1 hoặc h_2 như lá phiếu anh ta muốn

* Cử tri chứng tỏ tính đúng đắn của lá phiếu mình đã bỏ như sau:

- Cử tri tạo thêm T cặp của các lá phiếu đã mã hoá h^1, ..., h^T

$h^T_{ij} = E_j(s^r_j(v^r_i), k^r_{ij})$, $1 \le r \le T$ và gửi chúng tới những người kiểm phiếu

- Người kiểm phiếu tạo T chữ số nhị phân c_1 ,..., $c_T$và gửi tới cử tri.

- Với mỗi c_r=0, cử tri tiết lộ cách xây dựng cặp h^r= (h^r_1, h^r_2) bằng cách gửi v^r_i, $s^r_i(v^r_i)$, k^r_{ij}i=1,2; j=1,...,N

Với mỗi c_r=1 cử tri tiết lộ hoán vị mà nó sẽ chỉ ra mối liên quan giữa (v_1,v_2) với (v^r_1, v^r_2). Giả sử $v_1 = v^r_1$; $v_2 = v^r_2$ thì $h_{ij} = E_j(s_j(v_i), k_{ij})$; h^r_{ij}= $E_j(s^r_j(v^r_i), k^r_{ij})$. Nhờ có tính chất đồng cấu, ta có h/h^r là sự mã hoá của lá phiếu (0,0): $h_{ij}/h^r_{ij} = E_j(s_j(v_i) - s^r_j(v^r_i), k_{ij} / k^r_{ij})$. Cử tri gửi $s_j(v_i) - s^r_j(v^r_i)$, k_{ij} / k^r_{ij} tới người kiểm phiếu.

- Những người kiểm phiếu kiểm tra xem hối âm của cử tri có phù hợp với h không:

Với mỗi c_r=0, họ kiểm tra xem h^r có được tạo đúng?

Với mỗi c_r=1, họ kiểm tra xem h/h^r có phải là sự mã hoá của lá phiếu (0,0).

Giai đoạn kiểm phiếu: giả sử lá phiếu của cử tri v_i là h_i=(h_{i1},..., h_{iN}). Người kiểm phiếu A_j tính toán nhờ tính chất đồng cấu như sau:

$$\prod_i h_{ij} = \prod_i E_j(s_j(v_i)) = E_j(\sum_i s_j(v_i))$$

A_j giải mã tổng các phần tương ứng của mình $S_j = \sum_i s_j(v_i)$

S_j và việc chứng minh sự giải mã là đúng được làm công khai. Gọi A là tập (t+1) người kiểm phiếu thành công trong việc giải mã các phần của mình và việc chứng minh giải mã là đúng. Tổng cuối cùng của lá phiếu có thể tính được bởi một người bất kỳ như sau:

$$S = \sum_{j\in A} S_j \lambda_j = \sum_{j\in A}(\sum_i S_j(v_i))\lambda_j = \sum_i \sum_{j\in A} s_j(v_i)\lambda_j = \sum_i v_i$$

Ở đây λ_j là hệ số Lagrăng

* Các tính chất:

- Tính hợp pháp: chỉ những cử tri hợp pháp mới được phép bầu cử và được bỏ phiếu nhiều nhất là 1 lần. Cử tri không thể bỏ phiếu không hợp lệ hay phiếu đôi vì anh ta phải chứng minh tính hợp lệ của lá phiếu mình đã bỏ.

- Tính bí mật: bí mật của cử tri được bảo đảm bởi sơ đồ mã hoá. Bất kỳ một nhóm ít hơn (t+1) người kiểm phiếu đều không có thể có được thông tin gì về lá phiếu của cử tri.

- Tính xác minh phổ thông: bất kỳ người nào cũng có thể xác minh tính hợp lệ của lá phiếu đã gửi, bất kỳ ai đều có thể nhận được mã hoá tương ứng với mỗi người kiểm phiếu và ai cũng có thể xác minh xem người kiểm phiếu đó có giải mã đúng tổng của các phần tương ứng hay không, từ đó có thể tính toán ra kết quả cuối cùng.

2.2.4. Qui trình bỏ phiếu Schoenmaker

Tương tự như qui trình của Benaloh, cử tri chia sẻ lá phiếu của mình với người kiểm phiếu nhờ sơ đồ chia sẻ bí mật. Việc tính toán cuối cùng dựa trên tính chất đồng cấu của quá trình chia sẻ bí mật (tổng các bí mật được xây dựng lại từ tích các phần chia).

Giai đoạn mở đầu: theo sơ đồ chia sẻ bí mật được kiểm tra lại một cách công khai (tạo phần tử sinh g, $g \in Z_p$, khoá công khai $h_j = g^{zj}$ của người kiểm phiếu đưa cho).

Giai đoạn bỏ phiếu: Cử tri V_i chọn lá phiếu v_i của mình, $v_i \in \{0,1\}$ và chọn ngẫu nhiên $s_i \in Z_p$. Cử tri dùng cách thức phân phối để chia sẻ bí mật g^{si} và công bố giá trị $U_i = g^{si + vi}$. Ngoài ra để chỉ ra rằng $v_i \in \{0,1\}$, cử tri đưa ra chứng minh:

$$\log_G C_0 = \log_g U_i \ \text{ v } \ \log_G(GC_0) = \log_g U_i$$

Bất kỳ người nào cũng đều có thể kiểm tra lá phiếu ở trên bảng thông báo vì tính xác minh công khai của sơ đồ chia sẻ bí mật và đưa ra việc chứng minh $v_i \in \{0,1\}$.

Giai đoạn kiểm phiếu: Giả sử các cử tri V_i (i=1,...,m) đều bỏ phiếu thành công và hợp lệ ; tất cả các phần chia đã được mã hoá của từng người được tích luỹ lại:

$$H_j^* = \prod_i H_{ij} = \prod_i h_j^{p_i(j)} = h_j^{\sum_i p_i(j)}$$

Sau đó, mỗi người kiểm phiếu A_j áp dụng chia sẻ có xác minh; để đạt được $g^{\sum_i p_i(0)} = g^{\sum_i s_i}$, nhờ tính đồng cấu. Kết hợp với $\prod_i U_i = g^{\sum_i s_i + v_i}$ ta có $g^{\sum_i v_i} = g^T$ .Và tổng cuối T có thể tính toán như trong sơ đồ CGS.

Những tính chất đạt được:

- Tính hợp pháp: chỉ những cử tri hợp lệ mới có thể viết lên bảng thông báo. Cử tri không thể bỏ phiếu không hợp lệ hoặc phiếu đôi, vì cử tri bị đòi hỏi phải chứng minh tính hợp lệ của lá phiếu.
- Tính bí mật: bất ký nhóm ít hơn (t+1) người kiểm phiếu đều không thể biết về lá phiếu của cử tri. Tính bí mật được đảm bảo bởi sơ đồ chia sẻ bí mật xác minh công khai.
- Tính xác minh phổ thông: ai cũng có thể xác minh tính hợp lệ của phiếu bầu. Sơ đồ chia sẻ bí mật có xác minh công khai ngăn cản được hiện tượng cử tri phân phối sai các phần bí mật tới người kiểm phiếu. Ai cũng có thể nhân các phần bí mật mã hoá của người kiểm phiếu thứ j và có thể xác minh xem người kiểm phiếu thứ j có giải mã đúng hay không. Ai cũng có thể tính toán tổng cuối cùng từ các tổng của các phần chia đã công bố.

2.2.5. Qui trình bỏ phiếu CGS

Qui trình rất hiệu quả và thoả mãn tất cả các yêu cầu đặt ra đối với một qui trình bầu cử. Qui trình này dựa trên sự giả định về loga rời rạc, và nó có thể được điều chỉnh với sự giả định thặng dư thứ q.

Giai đoạn mở đầu: hệ mật mã ngưỡng ElGamal được tạo lập; ban kiểm phiếu chia sẻ khoá giải mã s, khoá công khai (p,g,h), trong đó $h_j = g^{si}$ và một hàm sinh cố định G của G_q được công khai.

Giai đoạn bỏ phiếu: Cử tri V_i chọn lá phiếu của mình m_0= G đối với lá phiếu Yes, m_1= 1/G với lá phiếu No. Lá phiếu được mã hoá có dạng $(x,y)=g^k$, $h^k m_b$ (trong đó k là một số ngẫu nhiên, $b \in \{0, 1\}$. Cử tri phải chứng minh lá phiếu của mình đúng dạng như trên. Lá phiếu đã được mã hoá cùng với sự chứng minh tính hợp lệ của nó được đưa ra bảng thông báo.

Giai đoạn kiểm phiếu: Ban kiểm phiếu kiểm tra sự chứng minh tính hợp lệ của lá phiếu và tích của các lá phiếu đã được mã hoá hợp lệ: $(X,Y) = (\prod_i x_i, \prod_i y_i)$

Sau đó ban kiểm phiếu hợp tác thực hiện cách thức giải mã đối với (X,Y) để đạt được giá trị $W=Y/X^s$. Mỗi người kiểm phiếu cũng công khai chứng minh không tương tác (từ cách giải mã) và người kiểm phiếu đã sử dụng phần khoá được chia sẻ của mình.

Từ đó, ta có $W=G^T$, T là sai khác giữa số lá phiếu YES và NO; $-M \leq T \leq M$; M là số cử tri đủ tư cách ; suy ra $T=\log_G W$, nói chung giá trị này khó tính toán. T có thể được xác định bằng cách thực hiện phép nhân modulo 0(M) nhờ tính toán lặp: G^{-M}, G^{-M+1},... cho đến khi tìm ra W.

Những tính chất đạt được:

- Tính hợp lệ: lá phiếu không đúng của cử tri sẽ không được chấp nhận nhờ sự kiểm tra chứng minh tính hợp lệ.
- Tính trung thực: Qui trình cũng chống lại được t người kiểm phiếu không trung thực.
- Tính bí mật: của lá phiếu riêng lẻ được đảm bảo bởi sự an toàn của hệ thống bí mật Elgamal. Bất kỳ nhóm ≤ t người kiểm phiếu đều không biết rõ về lá phiếu.
- Tính xác minh phổ thông: bất kỳ một người nào cũng có thể kiểm tra phần chứng minh tính hợp lệ của lá phiếu, tính tích các lá phiếu hợp lệ và xác minh tính đúng đắn của việc giải mã bằng cách kiểm tra các phần chứng minh của các người kiểm phiếu về việc sử dụng đúng các phần bí mật của mình.

2.2.6. Qui trình bỏ phiếu HS

Trong qui trình HS, những lá phiếu thích hợp được mã hoá và hoán vị bởi ban kiểm phiếu. Một hoán vị của các lá phiếu đã mã hoá được gửi tới cử tri thông qua kênh chống đột nhập đường truyền. Cử tri chỉ ra lá phiếu mình

chọn. Qui trình này được thiết kế theo cách mà chỉ có cử tri mới biết hoán vị cuối cùng và cử tri có thể nói dối lá phiếu mình chọn với bất kỳ ai.

* Sơ đồ bầu cử 1 - L:

Các lá phiếu được mã hoá sử dụng hệ mã hoá Elgamal: sự lựa chọn thứ i được mã hoá thành (g^k mod p, $h^k G_i$ mod p). Trong đó (p,g, h) là khoá Elgamal công khai và k là một số ngẫu nhiên.

- Giai đoạn mở đầu: N người kiểm phiếu thiết lập hệ mật mã Elgamal ngưỡng mạnh. Các hàm sinh G_1, ... , G_L đại diện cho các sự lựa chọn có thể được công khai. Ban kiểm phiếu cũng tạo một danh sách công khai các lá phiếu hợp lệ được mã hoá chuẩn $e_1^{(0)}$, $e_2^{(0)}$, ..., $e_L^{(0)}$, trong đó $e_1^{(0)}$ là mã hoá của lựa chọn G_i, số ngẫu nhiên k=0; $e_1^{(0)}$= (1, G_i).

- Giai đoạn bỏ phiếu: đối với mỗi cử tri V, người kiểm phiếu tạo ra một danh sách các sự mã hoá của các lá phiếu có thể. Từ đó cử tri V lựa chọn một để đại diện cho quyết định của mình. Ngược lại, với mỗi người kiểm phiếu A_i (j=1,...,N): nhập danh sách $e_1^{(j-1)}$,..., $e_L^{(j-1)}$, mã hoá lại từng phần trong danh sách đó và hoán vị danh sách theo một trật tự ngẫu nhiên. Với cách này, A_j tạo ra một danh sách $e_1^{(j)}$,..., $e_L^{(j)}$. Hơn nữa, A_j còn bị yêu cầu chứng minh rằng danh sách vừa tạo ra được xây dựng là đúng. Nếu A_j thất bại trong cách nào đó hoặc cử tri phản đối A_j thì A_j coi như không có loại bỏ A_j và đặt $e^{(j)}$= $e^{(j-1)}$.

Người kiểm phiếu đầu tiên nhận danh sách mẫu $e_1^{(0)}$, ..., $e_L^{(0)}$. Sau đây là sự mô tả chi tiết phương thức này:

+ A_j tính toán danh sách đưa ra $e_1^{(j)}$,...,$e_L^{(j)}$ theo cách sau:

. A_j lựa chọn phép hoán vị ngẫu nhiên π_j: {1,...,L} $\rightarrow$ {1,...,L} và các số ngẫu nhiên k_1,..., $k_L \in_R Z_p$.

. Thứ tự (i) trong danh sách cuối cùng có được bằng cách mã hoá lại thứ tự i (là $e_i^{(j-1)}$) từ danh sách đầu vào với số ngẫu nhiên k_i.

+ Không tiết lộ phép hoán vị π_j cũng như các số ngẫu nhiên k_1,..., k_L; người kiểm phiếu A_j chỉ ra rằng danh sách đầu ra $e_1^{(j)}$,...,$e_L^{(j)}$ được xây dựng

đúng: với mỗi i = 1,...,L A_j chứng minh rằng tồn tại một sự mã hoá lại của thứ tự thứ i ($e_i^{(j-1)}$) của danh sách đầu vào trong danh sách đầu ra $e_1^{(j)}$,...,$e_L^{(j)}$.

+ A_j trao đổi với nhau một cách bí mật phép hoán vị π_j và chứng minh bí mật về tính đúng đắn của phép hoán vị đó, thông qua kênh chống đột nhập đường truyền tới cử tri V. Một cách cụ thể hơn: A_j chứng minh rằng với mỗi i, $e_{\pi_j(i)}^{(j)}$ là sự mã hoá lại của $e_i^{(j-1)}$.

+ Nếu cử tri không chấp nhận chứng minh, cử tri sẽ phản ánh một cách công khai về người kiểm phiếu đó. Sau đó, danh sách tương ứng quay lại giai đoạn trước $e_1^{(j-1)}$,..., $e_L^{(j-1)}$ và người kiểm phiếu thứ j bị lờ đi. Cử tri có thể khiếu nại nhiều nhất (N - t -1) người kiểm phiếu.

Cử tri thông báo công khai vị trí thứ i trong lá phiếu mong muốn của mình ở danh sách cuối cùng $e^{(N)}$.

- Giai đoạn kiểm phiếu: mỗi cử tri chọn lá phiếu của mình từ danh sách cuối cùng mà ban kiểm phiếu tạo ra cho cử tri. Các lá phiếu đã mã hoá được nhân lên để được mã hoá của tổng các lá phiếu. Ban kiểm phiếu liên kết giải mã tổng đó và công bố chứng minh giải mã đúng.

Những tính chất đạt được:

- Tính hợp pháp: cử tri chỉ có thể bỏ lá phiếu hợp lệ và chỉ được bỏ phiếu nhiều nhất 1 lần theo ý mình.

- Tính bí mật cao: lá phiếu đã mã hoá không thể giải mã bởi người ở ngoài hoặc bởi 1 nhóm ít hơn (t+1) người kiểm phiếu. Một nhóm ít hơn (t+1) người kiểm phiếu liên minh lại cũng không thể tìm ra được trật tự cũ của danh sách.

- Tính xác minh phổ thông: Bất kỳ người nào cũng có thể kiểm tra xem người kiểm phiếu A_j có hoán vị danh sách một cách chính xác hay không. Cũng với cách này, người xem nào cũng có thể xác minh xem danh sách cuối cùng $e^{(N)}$ có là danh sách của những sự mã hoá các lá phiếu có thể hay không. Người xem nào cũng có thể tính toán tích của những lá phiếu đã mã hoá mà cử tri đã chọn, xác minh xem Ban kiểm phiếu có giải mã đúng tổng cuối cùng hay không.

Chương 3: XÂY DỰNG ỨNG DỤNG MÔ PHỎNG BỎ PHIẾU ĐIỆN TỬ

3.1. MÔ TẢ BÀI TOÁN :

Bước 1: Chuẩn bị:

Ban tổ chức bầu cử cần chuẩn bị hệ mã RSA với :

2 số nguyên tố lớn (p,q)

n = p.q ; $\phi(n)=(p-1)(q-1)$

Chọn b nguyên tố cùng $\phi(n)$.

Chọn a nghịch đảo với b; $a=b^{-1} \bmod \phi(n)$.

Trong đó, a là khóa bí mật và b là khóa công khai.

- Ký trên x: Sig (x) = $x^a \bmod n$

- Kiểm tra chữ ký: Ver (x,y)= True $\Leftrightarrow x \equiv y^b \bmod n$

Ban tổ chức cấp cho các thành viên các mảnh khóa riêng. Sau khi xét duyệt hồ sơ xin chữ ký của cử tri nếu mọi thành viên của Ban tổ chức đều nhất trí cho ký thì họ sẽ khớp các mảnh khóa riêng để nhận được khóa ký.

Bước 2: Đăng ký :

Cử tri chọn bí mật số định danh x (tiêu biểu cho ứng cử viên), giấy chứng minh thư điện tử (CMT), thông tin nhận dạng và làm mù x thành y=Blind(x) và gửi tất cả các thông tin của mình về cho Ban tổ chức .

Ban tổ chức xác minh và ghi lại nhận dạng và chứng minh thư điện tử của Cử tri xem có khớp và hợp lệ với danh sách cử tri hay không và chưa bỏ phiếu lần nào. Sau đó Ban kiểm phiếu ký lên y. Đó là chữ ký z=sign(y) và chuyển lại cho Cử tri.

Cử tri sau khi khi nhận được chữ ký mù thì bắt đầu xóa mù trên z, họ sẽ nhận được chữ ký sign(y) xóa mù trên x và lá phiếu có chữ ký của Ban tổ chức được coi là hợp lệ để Cử tri có thể ghi ý kiến của mình.

Cử tri có thể kiểm tra chữ ký có phải là thật hay không bằng cách sử dụng hàm kiểm tra chữ ký và khóa công khai mà Ban tổ chức đã cấp cho.

Bước 3: Bỏ phiếu :

Sau khi lá phiếu có chữ ký của Ban tổ chức, cử tri ghi ý kiến (lựa chọn) của mình và lá phiếu bằng cách đánh dấu lên lá phiếu hoặc gạch tên ứng cử viên.

Cử tri mã hóa lá phiếu bằng khóa công khai của Ban tổ chức và gửi tới Ban tổ chức lá phiếu đã bị mã hóa, đinh danh thật (không bị làm mù) của họ, chữ ký của Ban tổ chức về cho Ban tổ chức.

Trước khi được kiểm phiếu, lá phiếu của cử tri phải được kiểm tra chữ ký cấp quyền bỏ phiếu có bị giả mạo không để xác minh tính hợp lệ của lá phiếu và được mã hóa lại gửi về hòm phiếu.

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

Ban tổ chức thông báo kết quả lên Bảng niêm yết công khai.

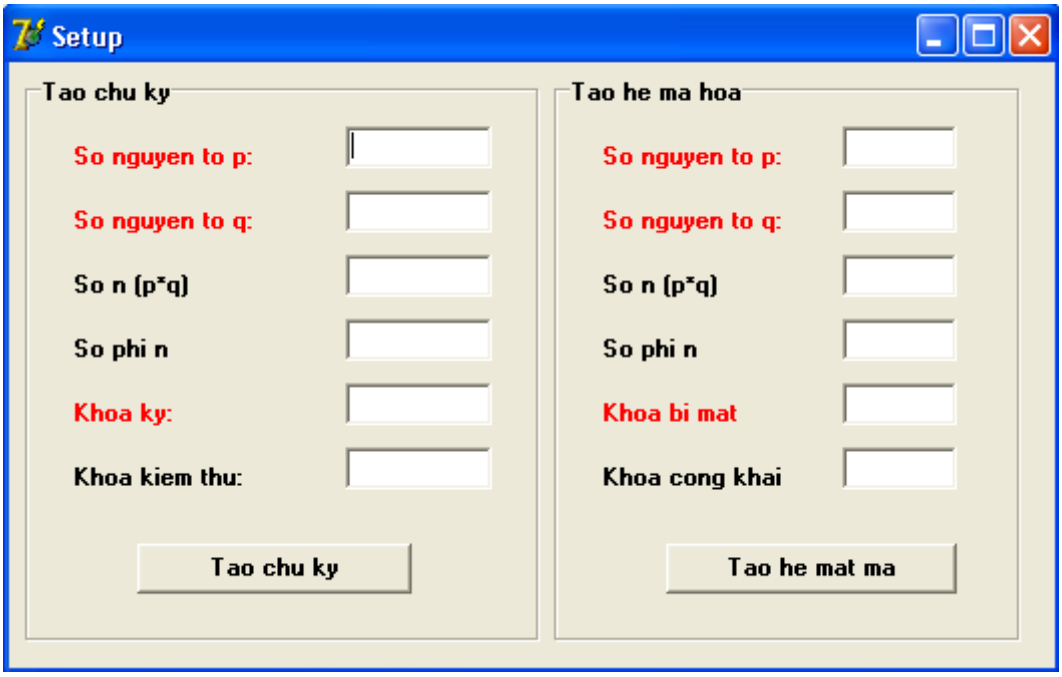
Sơ đồ mô phỏng bỏ phiếu điện tử :

Các bước thực hiện	Cử tri (CT)		Ban tổ chức (BTC)
Đăng ký	- Chọn bí mật bí danh x - Mã hóa lá phiếu -Xóa mù để thu chữ ký trên x	x đã làm mù,CMT,nhận dạng → ← Chữ ký trên x đã làm mù	- Kiểm tra và ghi lại thông tin cử tri - Nếu hợp lệ thì ký trên x đã làm mù do CT gửi về.
Bỏ phiếu	- Chọn ý kiến của mình cho lá phiếu đã có chữ ký của BTC.	Lá phiếu đã mã hóa bằng khóa công khai của BTC →	- Kiểm tra chữ ký và tính hợp lệ của lá phiếu. - Mã hóa lại lá phiếu và gửi về hòm phiếu. - Khôi phục khóa bí mật. - Tính kết quả bầu cử. - Thông báo và niêm yết công khai.

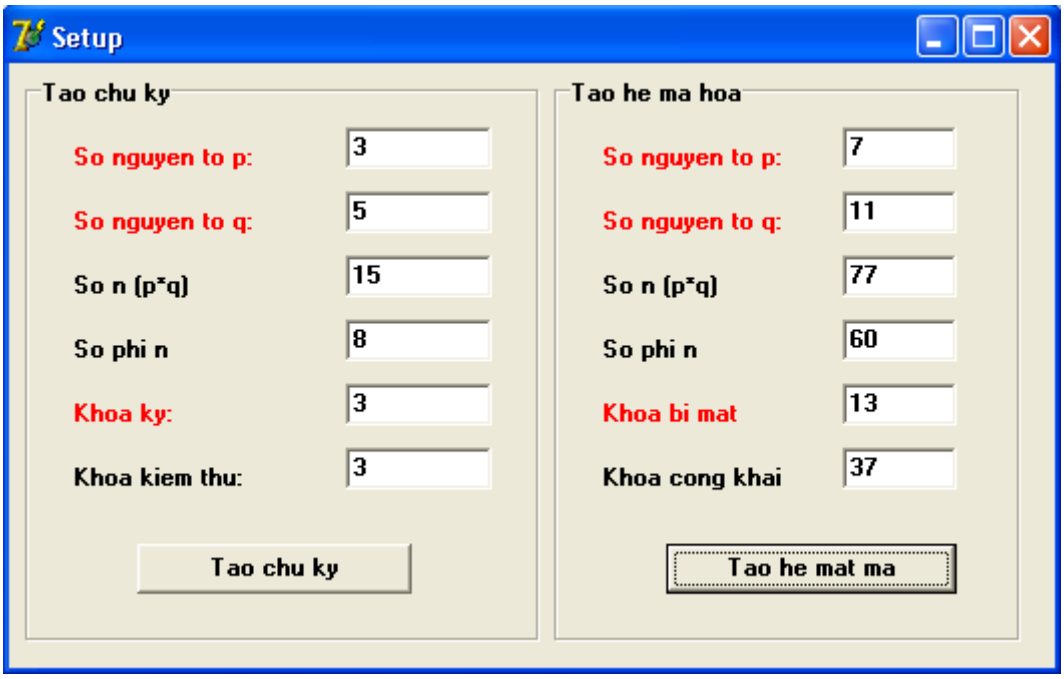
3.2. MÔ PHỎNG BỎ PHIẾU ĐIỆN TỬ :

Giao diện chương trình

Bước 1 : Chuẩn bị :

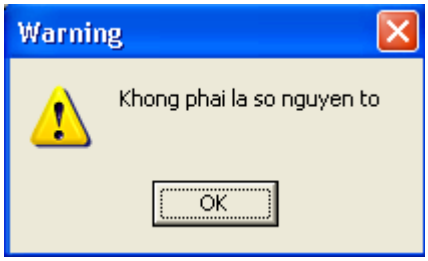


Nếu kết quả đúng:



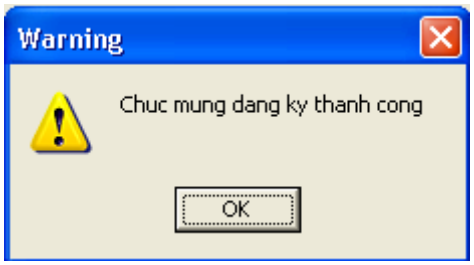
Nếu kết quả sai:

Hoặc :

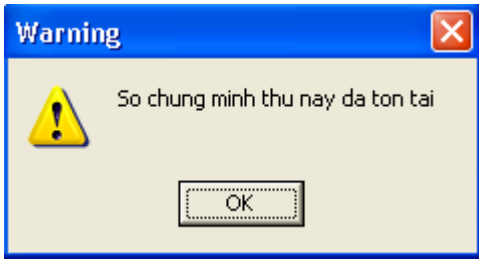


Bước 2 : Đăng ký :

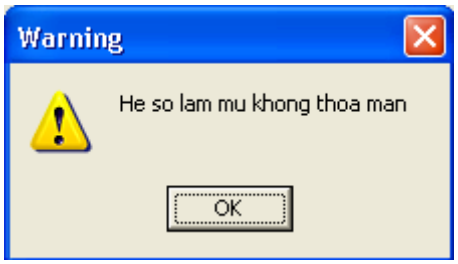
Nếu đăng ký thành công :



Trường hợp bị trùng số CMT hoặc cử tri gian lận bỏ phiếu nhiều lần :



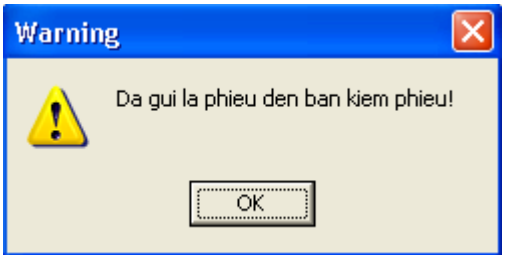
Hoặc :



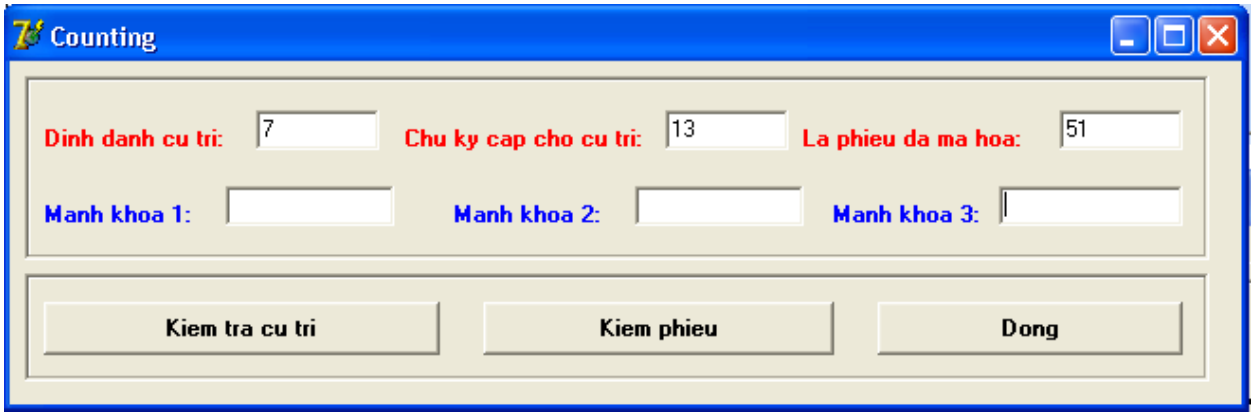
Bước 3 : Bỏ phiếu :

Mã hóa lá phiếu

Lá phiếu được gửi tới ban kiểm phiếu :



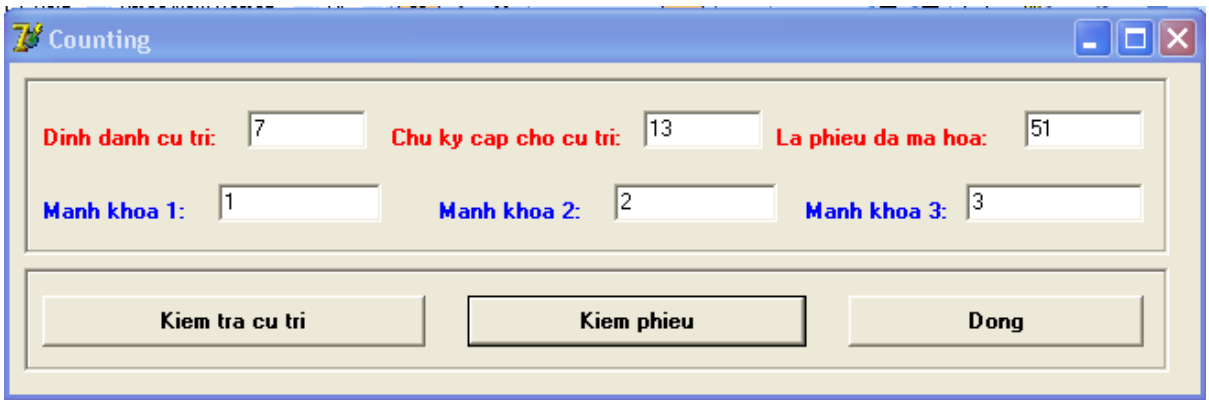
Kiểm tra cử tri :



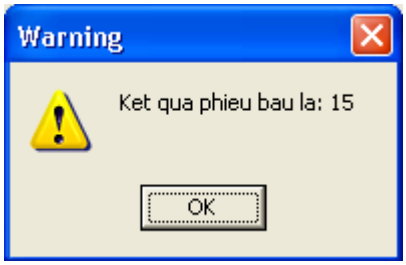
Nếu là giả mạo :

Nếu cử tri là hợp lệ :

Kiểm phiếu :



Và kết quả kiểm phiếu :



Nếu các mảnh khóa là không hợp lệ :

KẾT LUẬN

Trên đây là qui trình bỏ phiếu tổng quát và tóm tắt một số qui trình bỏ phiếu "điện tử" đang tồn tại cùng những đặc trưng của chúng. Những qui trình bỏ phiếu được giới thiệu có tính an toàn khác nhau và đạt được các yêu cầu: hợp pháp, riêng tư, rõ ràng, trung thực.

Bầu cử điện tử là một vấn đề có ý nghĩa đối với sự phát triển của xã hội và là một ứng dụng của mật mã học. Chúng ta hy vọng rằng, với một tương lai gần bầu cử điện tử có mặt tại Việt Nam, đóng góp cho sự tiến bộ của xã hội dân chủ.