MỤC LỤC

LỜI CẢM ƠN

Trước hết em xin được bày tỏ sự trân trọng và lòng biết ơn sâu sắc đối với thầy giáo hướng dẫn, PGS.TS. Trịnh Nhật Tiến, Đại học công nghệ, đại học quốc gia Hà Nội. Trong suốt quá trình làm khóa luận tốt nghiệp của em, thầy đã dành rất nhiều thời gian quí báu của mình để tận tình chỉ bảo, hướng dẫn, định hướng cho em trong việc nghiên cứu, hoàn thành đồ án.

Em xin cảm ơn thầy Lưu Hồng Dũng, Học viện Kỹ thuật Quân sự vì đã góp ý, chỉ dẫn thêm cho em trong quá trình xây dựng chương trình chữ ký bội.

Em xin cảm cô giáo phản biện Hồ Thị Hương Thơm, Trường Đại Học Dân Lập Hải Phòng vì đã cho em những ý kiến đóng góp vô cùng hữu ích và nhận ra các khuyết điểm cần sửa chữa của đồ án.

Em cũng xin chân thành cảm ơn các thầy giáo, cô giáo của Khoa Công Nghệ Thông Tin, Trường Đại Học Dân Lập Hải Phòng đã dạy bảo, hướng dẫn, trang bị cho em những kiến thức quý báu, hữu ích để em có thể hoàn thành tốt báo cáo tốt nghiệp này.

DANH MỤC HÌNH VẼ

BẢNG CHỮ VIẾT TẮT

UCLN: Ước chung lớn nhất.

BCNN: Bội chung nhỏ nhất.

CPĐT: Chính phủ điện tử.

CNTT: Công nghệ thông tin.

CNTT-TT: Công nghệ thông tin – Truyền thông.

G2C: Government to Citizen.

G2E: Government to Employee.

G2G: Government to Government.

G2B: Government to Bussiness.

MỞ ĐẦU

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. Việc phát triển ngày một mạnh mẽ và cấp thiết của hệ thống chính phủ điện tử đã nảy sinh các nhu cầu liên quan tới giao dịch hành chính điện tử.

Nắm được tầm quan trọng và tính tất yếu của giao dịch hành chính điện tử, vấn đề xác minh, chứng thực các văn bản trong các giao dịch điện tử, nhằm đáp ứng các yêu cầu về: tính xác thực, tính toàn vẹn và tính chống chối bỏ trách nhiệm cũng đòi hỏi ngày càng cao. Chữ ký điện tử là một trong những cách thức để giải quyết vấn đề đó.

Đồ án sẽ đi sâu về chữ ký bội và ứng dụng của nó trong giao dịch hành chính điện tử. Sau đó xây dựng, thử nghiệm một chương trình chữ ký bội để tiến hành ký số, kiểm tra chữ ký trên tài liệu điện tử.

Chương 1. CHỮ KÝ BỘI

1.1. MỘT SỐ KHÁI NIỆM TRONG SỐ HỌC VÀ ĐẠI SỐ

1.1.1. Một số khái niệm trong số học

1.1.1.1. Ước chung lớn nhất, bội chung nhỏ nhất

1/. Khái niệm ước số và bội số

Cho hai số nguyên a và b, $b \neq 0$. Nếu có một số nguyên q sao cho a=b*q, thì ta nó rằng a chia hết cho b, kí hiệu b\a. Ta nói b là ước của a, và a là bội của b.

Ví dụ:

+ Cho a = 12, b = 3, ta có 12 = 3*4, ký hiệu 2\12. Ở đây 12 là bội của 3 và 3 là ước của 12.

Cho các số nguyên a, $b \neq 0$, tồn tại cặp số nguyên (q, r) ($0 \leq r < |b|$) duy nhất sao cho a = b*q + r. Khi đó q gọi là thương nguyên, r gọi là số dư của phép chia a cho b. Nếu r = 0 thì ta có phép chia hết.

Ví dụ:

+ Cho a = 9, b = 2, ta có 12 = 2*4 + 1. Ở đây thương là q = 4, số dư là r = 1.

2/. Khái niệm ước chung lớn nhất

Số nguyên d được gọi là ước chung của các số nguyên $a_1, a_2, \ldots, a_n$, nếu nó là ước của các số đó. Một ước chung $d > 0$ của các số nguyên $a_1, a_2, \ldots, a_n$, trong đó mọi ước chung của $a_1, a_2, \ldots, a_n$ đều là ước của d, thì d được gọi là ước chung lớn nhất (UCLN) của $a_1, a_2, \ldots, a_n$.

Ký hiệu $d = \gcd(a_1, a_2, \ldots, a_n)$ hay $d = UCLN(a_1, a_2, \ldots, a_n)$.

Nếu $\gcd(a_1, a_2, \ldots, a_n) = 1$, thì các số $a_1, a_2, \ldots, a_n$ được gọi là nguyên tố cùng nhau.

Ví dụ:

+ Cho a = 10, b = 15, gcd(10,15) = 5.

+ Hai số 7 và 9 là nguyên tố cùng nhau, vì gcd(7,9) = 1.

3/. Khái niệm bội chung nhỏ nhất

Số nguyên m được gọi là bội chung của các số nguyên $a_1, a_2, \ldots, a_n$, nếu nó là bội của tất cả các số đó.

Một bội chung $m > 0$ của các số nguyên $a_1, a_2, \ldots, a_n$, trong đó mọi bội chung của $a_1, a_2, \ldots, a_n$ đều là bội của m, thì m được gọi là bội chung nhỏ nhất (BCNN) của $a_1, a_2, \ldots, a_n$.

Ký hiệu $m = \text{lcm}(a_1, a_2, \ldots, a_n)$ hay $m = \text{BCNN}(a_1, a_2, \ldots, a_n)$.

Ví dụ:

+ Cho a = 10, b = 15, lcm(10,15) = 30.

4/. Một số ký hiệu

+ $Z_n = \{0, 1, 2, \ldots, n-1\}$ là tập các số nguyên không âm < n.

+ $Z_n^* = \{e \in Zn$, e là nguyên tố cùng nhau với n$\}$, Tức $e \neq 0$.

Ví dụ:

+ $Z_4 = \{0, 1, 2, 3\}$. Khi đó số phần tử của Z_4 là $|Z_4| = 4$.

+ $Z_4^* = \{1, 3\}$. Khi đó số phần tử của Z_4^* là $| Z_4^*| = 2$.

5/. Tính chất

+ $d = \gcd(a_1, a_2, \ldots, a_n)$ khi và chỉ khi tồn tại các số $x_1, x_2, \ldots, x_n$ sao cho:

$d = a_1x_1 + a_2x_2 + \ldots + a_nx_n$.

Đặc biệt: a $a_1, a_2, \ldots, a_n$ nguyên tố cùng nhau $\Leftrightarrow$ tồn tại các số $x_1, x_2, \ldots, x_n$ sao cho: $1 = a_1x_1 + a_2x_2 + \ldots + a_nx_n$.

+ $d = \gcd(a_1, a_2, \ldots, a_n) \Leftrightarrow \gcd(a_1/d, a_2/d, \ldots, a_n/d) = 1$.

+ $m = \text{lcm}(a_1, a_2, \ldots, a_n) \Leftrightarrow \gcd(m/a_1, m/a_2, \ldots, m/a_n) = 1$.

+ $\gcd(m*a_1, m*a_2, \ldots, m*a_n) = m * \gcd(a_1, a_2, \ldots, a_n)$ (với $m \# 0$).

+ Nếu gcd(a,b) = 1 thì lcm(a,b) = a*b.

+ Nếu b > 0, a = bq + r thì gcd(a,b) = gcd(b,r).

1.1.1.2. Quan hệ "Đồng dư"

1/. Khái niệm

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

Ký hiệu: $a \equiv b \pmod{m}$.

Ví dụ: $9 \equiv 7 \pmod{2}$ vì $9 \bmod 2 = 7 \bmod 2 = 1$.

2/.Tính chất của đồng dư

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

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

+ Tính phản xạ: $a \equiv a \bmod m$.

+ Tính đối xứng: Nếu $a \equiv b \bmod m$ thì $b \equiv a \bmod m$.

+ Tính bắc cầu: Nếu $a \equiv b \bmod m$ và $b \equiv c \bmod m$ thì $a \equiv c \bmod m$.

+ $(a + b) \bmod m \equiv [(a \bmod m) + (b \bmod m)] \bmod m$.

+ $(a - b) \bmod m \equiv [(a \bmod m) - (b \bmod m)] \bmod m$.

+ Nếu $a \equiv a_1 \bmod m$, $b \equiv b_1 \bmod m$ thì $a + b \equiv a_1 + b_1 \bmod m$ và $ab \equiv a_1 b_1 \bmod m$.

1.1.1.3. Số nguyên tố

1/. Khái niệm

Số nguyên tố là số tự nhiên lớn hơn 1 và chỉ có hai ước là 1 và chính nó.

Ví dụ: 2,3,5,7,11,13,17 là số nguyên tố.

Số 2 là số nguyên tố chẵn duy nhất.

2/. Định lý

a) Định lý về số nguyên dương lớn hơn 1: Mọi số nguyên dương n > 1 đều có thể biểu diễn được duy nhất dưới dạng: $n = P_1^{n1} * P_2^{n2} * P_k^{nk}$, trong đó:

k, n_i (i = 1, 2, …, k) là các số tự nhiên, P_i là các số nguyên tố, từng đôi một khác nhau.

b) Định lý Mersenne:

Cho $p = 2^k - 1$, nếu p là số nguyên tố, thì k phải là số nguyên tố.

+ Chứng minh:

Bằng phản chứng, giả sử k không là số nguyên tố. Khi đó k = a*b với 1 < a, b < k.

Như vậy: $p = 2^k - 1 = 2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1).E$, trong đó E là một số nguyên (áp dụng định thức Niu-tơn).

Điều này mâu thuẫn giả thiết p là nguyên tố. Vậy là sai, hay k là số nguyên tố.

c) Định lý Euler:

Cho số nguyên dương n, số lượng các số nguyên dương bé hơn n và nguyên tố cùng nhau với n được ký hiệu $\phi(n)$ và gọi là hàm Euler.

Nếu p là số nguyên tố, thì $\phi(p) = p - 1$.

Định lý về hàm Euler:

+ Nếu n là tích hai số nguyên tố n = p*q, thì $\phi(n) = \phi(p) * \phi(q) = (p - 1) * (q - 1)$.

1.1.2. Một số khái niệm trong đại số

1.1.2.1. Cấu trúc nhóm

1/. Khái niệm nhóm

Nhóm là một bộ (G, *), trong đó G ≠ ∅, * là phép toán hai ngôi trên G thỏa mãn ba tính chất sau:

+ Phép toán có tính chất kết hợp: (x * y) * z = x * (y * z)

+ Tồn tại phần tử trung lập e ∈ G: e * x = x * e = x, ∀x ∈ G

+ ∀x ∈ G, tồn tại phần tử nghịch đảo x’ ∈ G: x’ * x = x * x’ = e

Cấp của nhóm G được hiểu là số phần tử của nhóm, ký hiệu là |G|.

Nhóm Abel là nhóm (G, *), trong đó phép toán hai ngôi * có tính giao hoán.

2/. Nhóm con của nhóm (G, *)

Nhóm con của G là tập S ⊂ G, S ≠ ∅, 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 ∈ S với mọi x, y ∈ S.

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

1.1.2.2. Nhóm Cyclic

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

Cho (G, *) là nhóm Cyclic với phần tử sinh g và phần tử trung lập e. Nếu tồn tại số tự nhiên nhỏ nhất n mà g^n = e, thì G sẽ chỉ gồm có n phần tử khác nhau: e, g, g^2, g^3,…, g^{n-1}. Khi đó G được gọi là nhóm Cyclic hữu hạn cấp n.

Nếu không tồn tại số tự nhiên n để g^n = e, thì G có cấp ∞.

Phần tử a ∈ Z_n^* có cấp d nếu d là số nguyên dương nhỏ nhất sao cho a^d = e, trong đó e là phần tử trung lập của G.

1.1.2.3. Nhóm (Z_n^*, phép nhân mod n)

1/. Khái niệm Tập thặng dư thu gọn theo modulo

a) Ký hiệu $Z_n = \{0, 1, 2, ..., n-1\}$ là tập các số nguyên không âm < n.

Z_n và phép cộng (+) lập thành nhóm Cyclic có phần tử sinh là 1, pt trung lập e = 0.

$(Z_n, +)$ được gọi là nhóm cộng, đó là nhóm hữu hạn có cấp n.

b) Ký hiệu $Z_n^* = \{e \in Zn$, e là nguyên tố cùng nhau với n$\}$. Tức là e phải $\neq 0$.

+ Z_n^* được gọi là Tập thặng dư thu gọn theo mod n, có số phần tử là $\phi(n)$.

+ Z_n^* với phép nhân mod n lập thành một nhóm (nhóm nhân), pt trung lập e = 1.

Tổng quát phép nhân (Z_n^* , phép mod n) không phải là nhóm Cyclic. Nhóm nhân Z_n^* = là Cyclic chỉ khi n có dạng: 2, 4, p^k hay $2p^k$ với p là số nguyên tố lẻ.

2/. Một số kết quả đã được chứng minh

a) Định lý Lagrange: Nếu G là nhóm cấp n và $a \in G$ thì cấp của a là ước của n.

b) Hệ quả: Giả sử $a \in Z_n^*$ có cấp m, thì m là ước của $\phi(n)$.

c) Định lý: Nếu p là số nguyên tố thì Z_p^* là nhóm Cyclic.

Nếu $b \in Z_n^*$ thì $b^{\Phi(n)} \equiv 1 \pmod n$. Nếu p là số nguyên tố thì $\phi(p) = p - 1$. Do đó với $b \in Z_p^*$ (tức b nguyên tố với p), thì $b^{\Phi(n)} \equiv 1 \pmod n$, hay $b^{p-1} \equiv 1 \pmod n$.

d) Chú ý:

Theo định nghĩa, phần tử $a \in Z_n^*$ có cấp d nếu d là số nguyên dương nhỏ nhất sao cho $a^d = e$ trong Z_n^*. Như vậy trong Z_n^* ta hiểu là $a^d \equiv e \pmod n$.

Định lý: Nhóm con của một nhóm Cyclic cũng là một nhóm Cyclic.

3/. Phần tử nghịch đảo đối với phép nhân

a) Định nghĩa:

Cho $a \in Z_n$. Nếu tồn tại $b \in Z_n$ sao cho $a\,b \equiv 1 \pmod n$, 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.

b) Định lý:

UCLN(a, n) = 1 $\Leftrightarrow$ Phần tử $a \in Z_n$ có phần tử nghịch đảo.

Chứng minh:

Nếu $a\,a^{-1} \equiv 1 \pmod n$ thì $a\,a^{-1} = 1 + kn \Leftrightarrow a\,a^{-1} - kn = 1 \rightarrow (a,n) = 1$. Nếu (a,n) = 1, ta có $a\,a^{-1} + kn = 1 \rightarrow a\,a^{-1} = 1 + kn$, do đó $a\,a^{-1} \equiv 1 \pmod n$.

c) Hệ quả: Mọi phần tử trong Z_n^* đều có phần tử nghịch đảo.

4/. Khái niệm Logarit rời rạc

Cho p là số nguyên tố, g là phần tử nguyên thủy của Z_p, $\beta \in Z_p^*$. "Logarit rời rạc" chính là việc giải phương trình $x = \log_g \beta \pmod p$ với ẩn x. Hay phải tìm số x duy nhất sao cho: $g^x \equiv \beta \pmod p$.

5/. Thăng dư bậc hai

Cho p là số nguyên tố lẻ, x là số nguyên dương $\leq p - 1$. x được gọi là "thăng dư bậc hai" mod p, nếu phương trình $y^2 \equiv x \bmod p$ có lời giải.

1.2. MỘT SỐ KHÁI NIỆM VỀ MẬT MÃ

1.2.1. Khái niệm mật mã

Mật mã có lẽ là kỹ thuật được dùng lâu đời nhất trong việc đảm bảo "An toàn thông tin". Kỹ thuật "mật mã" là công khai cho người dùng. Điều bí mật nằm ở "khóa" mật mã.

Hiện có nhiều kỹ thuật mật mã khác nhau với những ưu, nhược điểm riêng. Tùy theo yêu cầu của môi trường ứng dụng mà ta dùng kỹ thuật này hay kỹ thuật khác.

Mật mã cổ điển chủ yếu dùng để "che giấu" dữ liệu. Với mật mã hiện đại, ngoài khả năng "che giấu" dữ liệu, còn dùng để thực hiện: Ký số (ký điện tử), tạo đại diện thông điệp, giao thức bảo toàn dữ liệu, giao thức xác thực thực thể, giao thức xác thực tài liệu, …

Theo nghĩa hẹp, mật mã chủ yếu dùng để bảo mật dữ liệu, người ta quan niệm: Mật mã là Khoa học nghiên cứu mật mã: Tạo mã và Phân tích mã.

Phân tích mã là kỹ thuật, nghệ thuật phân tích mật mã, kiểm tra tính bảo mật của nó hoặc phá vỡ sự bí mật của nó. Phân tích mã còn được gọi là thám mã.

Theo nghĩa rộng, mật mã là một trong những công cụ hiệu quả bảo đảm An toàn thông tin nói chung: bảo mật, bảo toàn, xác thực, chống chối cãi, …

1.2.2. Khái niệm mã hóa (Encryption)

Mã hóa là quá trình chuyển thông tin có thể đọc được (gọi là Bản rõ) thành thông tin "khó" có thể đọc được theo cách thông thường (gọi là Bản mã).

Giải mã là quá trình chuyển thông tin ngược lại: từ Bản mã thành Bản rõ.

Thuật toán mã hóa hay giải mã là thủ tục tính toán để thực hiện mã hóa hay giải mã.

Khóa mã hóa là một giá trị làm cho thuật toán mã hóa thực hiện theo cách riêng biệt và sinh ra bản rõ riêng. Thông thường khóa càng lớn thì bản mã càng an toàn. Phạm vi các giá trị có thể của khóa được gọi là không gian khóa.

Hệ mã hóa là tập các thuật toán, các khóa nhằm che giấu thông tin, cũng như làm cho rõ nó.

1.2.2.1. 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.

1.2.2.2. 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.

1.2.3. Khái niệm ký số (Digital Signature)

"Chữ ký số" dùng để chứng thực "tài liệu số". Người ta tạo ra "chữ ký số" trên "tài liệu số" giống như tạo ra "bản mã" của tài liệu với "khóa lập mã". Như vậy, ký số trên tài liệu số là "ký" trên từng bit dữ liệu. Kẻ gian khó có thể giả mạo "chữ ký số" nếu không biết "khóa lập mã". Thực chất, ký số trên "tài liệu số" là "mã hóa" tài liệu số. Bản mã chính là "chữ ký số" hay "chữ ký điện tử" (Digital Signature). Xác nhận "chữ ký" là kiểm tra việc mã hóa trên có đúng không. Như vậy khi gửi một tài liệu số có chữ ký trên đó, người ta phải gửi cả hai file: một file tài liệu và một file chữ ký. Nhờ đó mới kiểm tra được có đúng chữ ký đó ký trên tài liệu đi kèm hay không. Để kiểm tra một chữ ký số thuộc về một tài liệu số, người ta giải mã chữ ký số bằng khóa giải mã và so sánh với tài liệu gốc.

Chữ ký số có thể ký vào tài liệu từ rất xa trên mạng công khai, có thể ký bằng thiết bị cầm tay tại khắp mọi nơi, miễn là kết nối được mạng. Ký số được thực hiện trên từng bít tài liệu, nên độ dài của chữ ký số ít nhất cũng bằng độ dài của tài liệu. Do đó, thay vì ký trên tài liệu dài, người ta thường dùng "hàm băm" để tạo "đại diện" cho tài liệu, sau đó mới "ký số" lên "đại diện này".

Sơ đồ chữ ký số 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:

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

1.2.4. Một số loại chữ ký số

1.2.4.1. Chữ ký RSA

+ *Sinh khóa:*

Chọn p, q là số nguyên tố lớn.

Tính n = p * q.

Tính $\phi(n)= (p - 1)(q - 1)$.

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 $y \in A$:

$$y = Sig_k(x) = x^a \bmod n.$$

+ *Kiểm tra chữ ký.*

$$Ver_k(x,y) = true \Leftrightarrow x = y^b \bmod n.$$

1.2.4.2. Chữ ký Elgamal

+ Sinh khóa:

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

Chọn phần tử nguyên thủy $g \in Z_p^*$.

Chọn khóa bí mật $a \in Z_p^*$.

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

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

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

Các giá trị {p, g, h} công khai, a phải giữ bí mật.

+ Ký số:

Dùng 2 khóa ký: khóa a và chọn khóa ngẫu nhiên bí mật $r \in Z_{p-1}^*$.

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 $\Leftrightarrow h^{y_1} * y_1^{y_2} = g^x \bmod p$

1.2.4.3. Chữ ký DSS

+ Sinh khóa:

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

Chọn q là ước nguyên tố của p - 1. Tức là p - 1 = t * q hay p = t * q + 1.

Chọn g $\in Z_p^*$ là căn bậc q của 1 mod p. (g là phần tử sinh của Z_p^*).

Tính b = g^t, chọn khóa bí mật a $\in Z_p^*$.

Tính khóa công khai h $\equiv b^a$ mod p.

Các tham số p, q, b, h là công khai, a là tham số bí mật.

+ Ký số:

Dùng 2 khóa ký: a và khóa ngẫu nhiên bí mật r $\in Z_p^*$.

Chữ ký trên x $\in Z_p^*$ là Sig_k (x, r) = (y_1, y_2) trong đó:

$y_1 = (b^r \bmod p) \bmod q$.

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

+ Xác minh chữ ký

$Ver_k(x, y_1, y_2)$ = đúng $\Leftrightarrow (b^{e1} * h^{e2} \bmod p) \bmod q = y_1$ với:

$e1 = x * y_2^{-1} \bmod q$.

$e2 = y_1 * y_2^{-1} \bmod q$.

1.3. KHÁI NIỆM VỀ CHỮ KÝ BỘI

1.3.1. Đặt vấn đề

Chữ ký số (Digital Signature) được sử dụng để chứng thực các văn bản trong các giao dịch điện tử, nhằm đáp ứng các yêu cầu về: tính xác thực, tính toàn vẹn và tính chống chối bỏ trách nhiệm.

Chữ ký số được phân thành hai lớp: chữ ký đơn (Single Digital Signature) và chữ ký bội hay chữ ký tập thể (Digital Multi-Signature). Chữ ký đơn được sử dụng trong trường hợp chỉ một người ký vào một văn bản, còn chữ ký bội được sử dụng trong trường hợp một nhóm người có quan hệ với nhau cùng hợp tác để ký vào một văn bản.

Nhược điểm của chữ ký số đơn là khi cần ký tập thể (bao gồm nhóm n người), thì chữ ký sẽ dài, xem như, gấp n lần chữ ký của một người. Trong thực tế, chúng ta thường gặp các hợp đồng, thỏa thuận… cần được ký bởi một vài đối tác. Vậy nên trong một chừng mực nào đấy, chữ ký bội cũng rất phổ biến và quan trọng như chữ ký số đơn.

Chữ ký bội là phương pháp tạo ra chữ ký số có độ dài không đổi, không phụ thuộc vào số lượng người tham gia ký vào một văn bản, không làm giảm độ tin cậy của chữ ký số. Chữ ký bội cũng tương tự như chữ ký đơn, nhưng để phát sinh chữ ký bội phải có sự hợp tác của các thành viên trong nhóm ký với khóa riêng của từng người.

Chữ ký bội được chia thành hai dạng cơ bản theo hai phương pháp ký khác nhau: ký đồng thời và ký tuần tự, do đó các lược đồ chữ ký bội cũng được chia thành hai dạng cơ bản là: lược đồ chữ ký bội song song và lược đồ chữ ký bội tuần tự. Với các lược đồ thuộc loại song song, việc ký vào văn bản của các thành viên được thực hiện một cách đồng thời, còn ngược lại trong các lược đồ tuần tự, việc ký vào văn bản của các thành viên trong nhóm ký được thực hiện nối tiếp nhau. Trong thực tiễn, thứ tự ký vào văn bản của các thành viên cần phải được bảo đảm theo quy định.

1.3.2. Bài toán Logarit rời rạc

Cho số nguyên tố p, gọi $\alpha \in Z_p^*$ là phần tử sinh (generator) và một phần tử $\beta \in Z_p^*$. Cần xác định số nguyên dương $a \in Z_p^*$ sao cho $\alpha^a \equiv \beta (\mathrm{mod}\, p)$, kí hiệu $a = \log_\alpha \beta$.

Trên thực tế, bài toán Logarit rời rạc thuộc loại bài toán khó, hiện nay chưa có thuật toán đơn định đa thức để giải nó.

Với p có tối thiểu 300 chữ số (hệ mười) và p – 1 có thừa số nguyên tố đủ lớn, phép toán lũy thừa modulo p có thể xem như là hàm một chiều hay việc giải bài toán logarit rời rạc trên Z^*_p xem như không thể thực hiện được trên thực tế.

Lợi thế của bài toán Logarit rời rạc trong xây dựng hệ mật là khó tìm được logarit rời rạc, song bài toán lấy luỹ thừa lại có thể tính toán hiệu quả theo thuật toán "bình phương và nhân". Nói cách khác, luỹ thừa theo modulo p là hàm một chiều với các số nguyên tố p thích hợp.

1.3.3. Lược đồ chữ ký bội dựa trên bài toán Logarit rời rạc

1.3.3.1. Giới thiệu

Lược đồ đa chữ ký bội ở đây được phát triển với các yêu cầu như sau:

+ Chữ ký bội được phát sinh bởi một nhóm người với các khóa riêng của từng thành viên. Không có khả năng phát sinh đa chữ ký nếu không có đủ số lượng các thành viên.

+ Độ dài của chữ ký bội là cố định không phụ thuộc vào số lượng người ký.

+ Chữ ký bội được thẩm tra nhờ khóa công khai chung của cả nhóm, hơn nữa khóa công khai chung được hình thành từ các khóa công khai của mỗi thành viên theo một luật xác định.

1.3.3.2. Thuật toán hình thành và kiểm tra chữ ký bội

Giả thiết rằng nhóm người có thẩm quyền ký gồm *n* thành viên, để ký vào văn bản *M*, quá trình ký và xác minh được tiến hành như sau:

1/. Các tham số dùng chung

+ p, q là 2 số nguyên tố lớn, sao cho: p = Z.q +1, Z là số nguyên.

+ p, q có thể chọn theo chuẩn chữ ký số DSS của Mỹ như sau:

$$2^{L-1} < p < 2^{L}, \quad 2^{N-1} < q < 2^{N}$$

với: L = 1024, N = 160; L = 2048, N = 224; L = 2048, N = 256; L = 3072, N = 256.

+ g là phần tử sinh có bậc q của nhóm Z_p^*, nghĩa là: $0 < g < p$, và: $g^q \equiv 1 \bmod p$.

Các giá trị (p, q, g) là các tham số công khai trong quá trình hình thành và kiểm tra chữ ký.

2/. Hình thành khóa công khai chung cho cả nhóm

+ Mỗi thành viên chọn ngẫu nhiên số nguyên: $x_i \in [1, q-1]$ làm khóa bí mật và tính khóa công khai tương ứng: $y_i = g^{x_i} \bmod p$

+ Khóa công khai chung của nhóm được tính theo công thức: $Y = \prod_{i=1}^{n} y_i \bmod p$

3/. Hình thành đa chữ ký số

a) Phương án thứ nhất:

+ Mỗi thành viên chọn ngẫu nhiên số nguyên bí mật: $k_i \in [1, q-1]$ và tính:

$$r_i = g^{k_i} \bmod p$$

+ Một người làm đại diện cho nhóm tính giá trị công khai:

$$R = \prod_{i=1}^{n} r_i \bmod p$$

+ Người đại diện cho nhóm tính phần thứ nhất của chữ ký tập thể:

$$E = R.H \bmod q$$

Ở đây : $H = h(M)$ – bản tóm lược của *M*, với *h* – hàm băm được chọn đủ an toàn, chẳng hạn: SHA-1, 2.

Sau đó *E* được gửi cho mọi thành viên trong nhóm;

+ Mỗi người ký tính phần thứ hai của chữ ký cá nhân theo công thức:

$$s_i = g^{(k_i + x_i.E) \bmod q} \bmod p \qquad (1)$$

Sau đó gửi s_i cho người đại diện nhóm. Cặp giá trị (r_i, s_i) là chữ ký cá nhân của thành viên thứ *i* vào văn bản *M*.

+ Sau khi nhận được tất cả các chữ ký cá nhân (r_i, s_i), người đại diện cho nhóm kiểm tra sự hợp lệ của các chữ ký này nhờ công thức:

$$r_i^{'} = y_i^{-E}.s_i \bmod p$$

và:

$$R' = \prod_{i=1}^{n} r_i^{'} \bmod p$$

rồi tính:

$$E' = R'.H \bmod q .$$

Nếu: *E' = E*, người đại diện nhóm sẽ tính thành phần thứ 2 của đa chữ ký:

$$S = \prod_{i=1}^{n} s_i \bmod p \qquad (2)$$

Cặp giá trị *(E, S)* là đa chữ ký số của nhóm người ký trên văn bản *M*.

+ Như vậy việc hình thành đa chữ ký trong lược đồ trên cần 4 bước để thực hiện.

Tuy nhiên, thay (1) vào (2) ta có:

$$S = g^{(k_1+x_1.E) \bmod q}.g^{(k_2+x_2.E) \bmod q}...g^{(k_n+x_n.E) \bmod q} \bmod p$$
$$\Leftrightarrow S = g^{k_1 \bmod q}.g^{k_2 \bmod q}...g^{k_n \bmod q}.g^{x_1.E \bmod q}.g^{x_2.E \bmod q}...g^{x_n.E \bmod q} \bmod p$$
$$\Leftrightarrow S = (g^{k_1}.g^{k_2}...g^{k_n}).(g^{x_1}.g^{x_2}...g^{x_n})^{E \bmod q} \bmod p$$
$$\Leftrightarrow S = (r_1.r_2...r_n).(y_1.y_2...y_n)^E \bmod p$$
$$\Leftrightarrow S = R.Y^E \bmod p.(3)$$

b) Như vậy ta sẽ có phương án thứ 2 cho việc hình thành đa chữ ký như sau:

+ Mỗi thành viên chọn ngẫu nhiên số nguyên: $k_i \in [1, q-1]$ và tính: $r_i = g^{k_i} \bmod p$

+ Một người làm đại diện cho nhóm tính giá trị công khai: $R = \prod_{i=1}^{n} r_i \bmod p$

rồi tính phần thứ nhất của đa chữ ký:

$E = R.H \bmod q$ với H = h(M) là bản tóm lược của M.

và tính phần thứ hai của đa chữ ký:

$S = R.Y^E \bmod q$

4/. Kiểm tra chữ ký số

Ta có: $E' = R.H' \bmod q$, $S' = R.Y^{E'} \bmod q$ trong đó: $H' = h(M)$.

Nếu văn bản *M* và chữ ký *(E, S)* nhận được là đúng thì: *E' = E* và *S' = S*

Như vậy, việc kiểm tra được thực hiện qua các bước sau:

+ Từ *M* tính: $H' = h(M)$;

+ Sử dụng khóa công khai Y và tham số công khai R để tính:

$E' = R.H' \bmod q$

$S' = R.Y^{E'} \bmod q$

+ So sánh *E'* với *E* và S' với S. Nếu: *E' = E* và *S' = S* thì chữ ký là hợp lệ và văn bản là toàn vẹn.

Chương 2. GIAO DỊCH HÀNH CHÍNH ĐIỆN TỬ

2.1. KHÁI NIỆM CHÍNH PHỦ ĐIỆN TỬ

2.1.1. Giới thiệu

Chính phủ điện tử (CPĐT) là Chính phủ ứng dụng Công nghệ thông tin – truyền thông (CNTT-TT) để các cơ quan Chính phủ đổi mới tổ chức, đổi mới các quy trình hoạt động, tăng cường năng lực của Chính phủ, khiến Chính phủ làm việc hiệu lực, hiệu quả và minh bạch hơn, cung cấp thông tin, dịch vụ tốt hơn cho người dân, doanh nghiệp và các tổ chức và tạo điều kiện thuận lợi hơn cho người dân thực hiện quyền dân chủ và tham gia quản lý Nhà nước. Nói một cách ngắn gọn, CPĐT là Chính phủ hoạt động hiệu lực, hiệu quả hơn, cung cấp dịch vụ tốt hơn trên cơ sở ứng dụng CNTT-TT.

CPĐT là một hệ thống CNTT-TT hỗ trợ công tác quản lý (điều hành) của chính phủ một cách hiệu quả. CPĐT là "nhúng" toàn bộ hoạt động quản lý Nhà nước vào môi trường thông tin điện tử, sử dụng Internet và công nghệ Internet để mở rộng khả năng truy cập và cung cấp các dịch vụ công của Chính quyền đến công dân, công chức và doanh nghiệp. Qua đó, Chính phủ có thể quản lý và phục vụ người dân. Người dân chấp hành quy định và thực hiện trách nhiệm công dân của mình thông qua môi trường đó.

Mục tiêu của CPĐT là:

+ Thiết lập môi trường kinh doanh thuận lợi.

+ Khách hàng "trực tuyến" (Online) chứ không phải "xếp hàng" (inline).

+ Tăng cường sự điều hành có hiệu quả của Chính phủ với sự tham gia của cộng đồng.

+ Nâng cao hiệu lực và hiệu quả của các cơ quan Nhà nước.

+ Nâng cao chất lượng cuộc sống cho các cộng đồng vùng sâu vùng xa.

2.1.2. Các định nghĩa về CPĐT

Có nhiều cách tiếp cận khác nhau nên có nhiều định nghĩa về CPĐT

2.1.2.1. Cách tiếp cận 1

Theo định nghĩa của Ngân hàng thế giới: CPĐT là việc các cơ quan của Chính phủ sử dụng một cách có hệ thống công nghệ thông tin và viễn thông để thực hiện các quan hệ với công dân, với doanh nghiệp và các tổ chức xã hội. Nhờ đó, giao dịch của các cơ quan Chính phủ với công dân và các tổ chức sẽ được cải thiện, nâng cao chất lượng. Lợi ích thu được sẽ là giảm thiểu tham nhũng, tăng cường tính công khai, sự tiện lợi, góp phần vào sự tăng trưởng và giảm chi phí.

2.1.2.2. Cách tiếp cận 2

CPĐT là sự tối ưu hóa liên tục việc chuyển giao các dịch vụ, sự tham gia của các thành phần và sự quản lý của nhà nước bởi việc chuyển đổi các quan hệ bên trong và bên ngoài thông qua công nghệ, Internet và các phương tiện mới.

Các thành phần bên ngoài: các dịch vụ trước tuyến (Online Services) đối với công dân hay doanh nghiệp.

Các thành phần bên trong: các hoạt động của Chính phủ từ các công chức cho tới bộ máy nhà nước.

CPĐT là một Chính phủ vận hành trực tuyến (Government Online – GOL), hay Chính phủ 24x7, thậm chí là 24x365. Một điểm cơ bản của CPĐT là khả năng sử dụng các công nghệ mới như hạ tầng cơ sở công nghệ thông tin, mạng máy tính và cao nhất là Internet làm nền tảng cho việc quản lý và vận hành của bộ máy nhà nước nhằm cung cấp các "dịch vụ" cho toàn xã hội một cách tốt nhất.

Trong xã hội thông tin hiện nay, quá trình hoạt động và quản lý từ cấp cao nhất đến cơ sở cần phải được dựa trên các hệ thống tập hợp, lưu trữ, xử lý, sử dụng và khai thác thông tin có hiệu quả để cai quản và điều hành vĩ mô mọi hoạt động của nền kinh tế toàn xã hội. Tốc độ phát triển mạnh mẽ như vũ bão của Internet hiện nay đã và đang là động lực làm thay đổi cách thức kinh doanh và vận hành doanh nghiệp và cũng là nhân tố tích cực cho việc hình thành và phát triển khái niệm CPĐT, để trở thành một hệ thống "hiệu quả hơn" và "phục vụ tốt hơn".

2.1.2.3. Cách tiếp cận 3

Chính phủ điện tử là hệ thống thông tin đặc biệt, nhằm:

+ Kết nối các cơ quan của chính phủ trong hoạt động, cung cấp, chia sẻ thông tin và phối kết hợp cung cấp giá trị tốt nhất trong việc cung ứng các dịch vụ công với chất lượng tốt nhất, phương thức mới nhất trên môi trường điện tử.

+ Xây dựng và hình thành cổng điện tử của các cơ quan hành chính địa phương, cung cấp thông tin cho mọi người dân về những công việc của cơ quan hành chính, các quy định và thủ tục, dịch vụ mà cơ quan hành chính cung cấp cho nhu cầu người dân.

+ Coi "công dân" là "khách hàng": thay đổi cách tiếp cận về quan hệ giữa công dân và Chính phủ, từ quan hệ "xin-cho" thành quan hệ "phục vụ, cung ứng dịch vụ". Khách hàng là công dân có nhiều khả năng lựa chọn dịch vụ tốt nhất cho cuộc sống.

+ Việc cung ứng các sản phẩm, dịch vụ và tư vấn bằng công nghệ mới đã được chuyển thành các "Trung tâm kết nối", giúp cho mọi người có thể tự lựa chọn phương án, cách thức để giải quyết những vấn đề của cá nhân trong cuộc sống. Cơ quan hành chính biến thành các Trung tâm kết nối thông tin, giúp đỡ, hướng dẫn, hỗ trợ người dân lựa chọn và thực hiện các dịch vụ hành chính.

2.1.2.4. Cách tiếp cận 4

CPĐT có thể coi là:

+ Việc sử dụng CNTT nhằm giải phóng các hoạt động thông tin, vượt qua các rào vản vật lý của hệ thống giấy tờ truyền thống và các hệ thống cơ sở khác.

+ Nhằm sử dụng công nghệ để tăng cường khả năng tiếp cận cho công dân, doanh nghiệp, các đối tác và người lao động đến các dịch vụ của Chính phủ.

2.2. KHÁI NIỆM GIAO DỊCH HÀNH CHÍNH ĐIỆN TỬ

Về tổng thể có thể phân loại giao dịch của CPĐT thành bốn loại:

+ Chính phủ với Công dân (G2C).

+ Chính phủ với Người lao động (G2E).

+ Chính phủ với Chính phủ (G2G).

+ Chính phủ với Doanh nghiệp (G2B).

Ngoài bốn mô hình chủ yếu trên, còn có nhiều hình thức giao tiếp khác trong CPĐT như: C2C, C2G, C2B, C2N, B2C…

2.2.1. G2C (Government to Citizen)

G2C được hiểu như khả năng giao dịch và cung cấp các dịch vụ của Chính phủ trực tiếp cho cộng đồng, thí dụ tổ chức bầu cử của công dân, thăm dò dư luận, quản lý quy hoạch xây dựng đô thị, tư vấn, khiếu nại, giám sát và thanh toán thuế, hóa đơn của các nghành với người thuê bao, dịch vụ thông tin trực tiếp 24x7, phục vụ công cộng, môi trường giáo dục.

G2C bao gồm phổ biến thông tin tới công chúng, các dịch vụ công dân cơ bản như gia hạn giấy phép, cấp giấy khai sinh/ khai tử/ đăng ký kết hôn và kê khai các biểu mẫu nộp thuế thu nhập cũng như hỗ trợ người dân đối với các dịch vụ cơ bản như giao dục, chăm sóc y tế, thông tin bệnh viện, thư viện và rất nhiều dịch vụ khác.

2.2.2. G2E (Government to Employee)

G2E chỉ các dịch vụ, giao dịch trong mối quan hệ giữa Chính phủ đối với người làm công lao động như bảo hiểm, dịch vụ việc làm, trợ cấp thất nghiệp, y tế, nhà ở…

2.2.3. G2G (Government to Government)

G2G được hiểu như khả năng phối hợp, chuyển giao và cung cấp các dịch vụ một cách có hiệu quả giữa các cấp, ngành, tổ chức, bộ máy của Nhà nước trong việc điều hành và quản lý Nhà nước, trong đó chính bản thân bộ máy của Chính phủ vừa đóng vai trò là chủ thể và khách thể trong mối quan hệ này.

2.2.4. G2B (Government to Bussiness)

G2B là dịch vụ và quan hệ của Chính phủ đối với các doanh nghiệp, các tổ chức phi Chính phủ, nhà sản xuất như dịch vụ mua sắm, thanh tra, giám sát doanh nghiệp (về đóng thuế, tuân thủ luật pháp…); thông tin về phát triển đất đai, đấu thầu, xây dựng; cung cấp thông tin dạng văn bản, hướng dẫn sử dụng, quy định, thi hành chính sách… cho các doanh nghiệp. Đây là thành phần quan hệ cơ bản trong mô hình Nhà nước là chủ thể quản lý vĩ mô nền kinh tế, xã hội thông qua chính sách, cơ chế và luật pháp, doanh nghiệp như là khách thể đại diện cho lực lượng sản xuất trực tiếp ra của cải vật chất của nền kinh tế.

Các giao dịch G2B bao gồm nhiều dịch vụ khác nhau được trao đổi giữa Chính phủ và cộng đồng doanh nghiệp bao gồm cả việc phổ biến các chính sách, biên bản ghi nhớ, các quy định và thể chế. Các dịch vụ được cung cấp bao gồm truy xuất các thông tin về kinh doanh, tải các mẫu đơn, gia hạn giấy phép, đăng ký kinh doanh, xin cấp phép và nộp thuế. Các dịch vụ được cung cấp thông qua các giao dịch G2B cũng hỗ trợ việc phát triển kinh doanh, đặc biệt là phát triển các doanh nghiệp vừa và nhỏ. Việc đơn giản hóa các thủ tục xin cấp phép, hỗ trợ quá trình phê duyệt đối với các yêu cầu của doanh nghiệp vừa và nhỏ sẽ thúc đẩy kinh doanh phát triển.

Ở mức cao hơn, các dịch vụ G2B bao gồm việc mua sắm điện tử và trao đổi trực tuyến giữa Chính phủ với các nhà cung cấp để mua sắm hàng hóa và dịch vụ cho Chính phủ. Tùy theo từng phương pháp, người mua hoặc người bán có thể xác định giá cả hoặc mở thầu. Việc mua sắm điện tử làm cho quá trình đấu thầu trở nên minh bạch và cho phép các doanh nghiệp nhỏ có thể tham gia đấu thầu với các dự án lớn của Chính phủ. Hệ thống này cũng giúp cho Chính phủ có thể tiết kiệm chi tiêu nhiều hơn thông qua việc cắt giảm chi phí cho người môi giới trung gian và giảm chi phí hành chính của các đại lý mua bán.

2.3. ỨNG DỤNG CHỮ KÝ BỘI TRONG GIAO DỊCH HÀNH CHÍNH ĐIỆN TỬ

2.3.1. Giá trị pháp lý của chữ ký điện tử

Để ghi nhận tính xác thực của thông tin được chứa đựng trong văn bản, từ trước đến nay chữ ký được coi là phương thức phổ biến nhất với một số đặc trưng cơ bản sau:

+ Chữ ký xác định tác giả của văn bản.

+ Chữ ký thể hiện sự khẳng định của tác giả với nội dung thông tin chứa đựng trong văn bản.

Thông qua các phương tiện điện tử, các yêu cầu về đặc trưng của chữ ký tay trong giao dịch thương mại có thể đáp ứng bằng hình thức chữ ký điện tử. Chữ ký điện tử trở thành một thành tố quan trọng trong văn bản điện tử. Chữ ký điện tử phải đáp ứng được sự an toàn và thể hiện ý chí rõ ràng của các bên về thông tin chứa đựng trong văn bản điện tử.

Đối với Việt Nam, chữ ký điện tử đã được Chính phủ chấp nhận trong thanh toán liên ngân hàng do Ngân hàng Nhà nước Việt Nam đề nghị vào tháng 3/2002. Tháng 7/2006, Bộ Thương Mại đã công nhận chữ ký điện tử trong giao dịch.

Chúng ta đã có Nghị định hướng dẫn chi tiết Luật Giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số. Nghị định này quy định giá trị của chữ ký số và bản tin điện tử được ký số; việc quản lý, cung cấp và sử dụng dịch vụ chứng thực chữ ký số trong hoạt động của các cơ quan Nhà nước, trong lĩnh vực dân sự, kinh doanh, thương mại và các lĩnh vực khác do pháp luật quy định.

2.3.2. Chữ ký bội trong giao dịch hành chính điện tử

Quản lý tài liệu điện tử và truyền thông tin điện tử đã tạo thành một phần rộng lớn của hoạt động giao dịch hành chính. Người ta dự kiến việc sử dụng dữ liệu kỹ thuật số sẽ được phổ biến trong những năm tới và nó sẽ dần dần thay thế phương pháp làm việc với giấy tờ như truyền thống. Tài liệu giấy sẽ không hoàn toàn biến mất nhưng hình thức trên giấy sẽ không còn là cốt lõi của hệ thống quản lý tài liệu. Vai trò của nó sẽ được giảm đến mức cơ bản trong đầu ra của một hệ thống giao dịch hành chính điện tử, thay vào đó là hình thức quản lý số. Xu hướng này đã được thể hiện rõ ràng trong các môi trường hành chính tiên tiến, ví dụ trong lĩnh vực ngân hàng hoặc trong lĩnh vực bảo hiểm, và nó sẽ sớm hay muộn cũng sẽ xuất hiện trong chính quyền của chính phủ, quốc hội và tòa án.

Mặc dù vậy, việc sử dụng tài liệu số, thông tin điện tử vẫn không thể tránh khỏi một số hoài nghi, đặc biệt khi tiến hành giao dịch với các thông tin, tài liệu quan trọng. Một trong những lý do là thiếu bảo đảm về khả năng xác thực thông tin, tính xác thực, tính toàn vẹn và tính chống chối bỏ trách nhiệm trong văn bản đó. Vậy nên chữ ký số là một giải pháp thiết yếu cho vấn đề này.

Trong thực tế, có rất nhiều giao dịch, thỏa thuận… cần được ký kết bởi nhiều người, nhiều đối tác. Vậy nên, trong một chừng mực nào đấy, chữ ký bội cũng rất phổ biến và quan trọng như chữ ký số đơn. Đối với giao dịch hành chính điện tử, việc xác xác thực của thông tin được chứa đựng trong văn bản do nhiều người chịu trách nhiệm lại càng cấp thiết.

Chữ ký bội được bổ sung vào tài liệu cho phép những người có liên quan, cơ quan có thẩm quyền kiểm tra tính xác thực của tài liệu, cũng như kiểm tra tính toàn vẹn và tính chống chối bỏ trách nhiệm trong văn bản đó.

Việc tạo ra tạo ra chữ ký số có độ dài không đổi, không phụ thuộc vào số lượng người tham gia ký vào một văn bản, không làm giảm độ tin cậy của chữ ký số khiến chữ ký bội sẽ là một giải pháp được sử dụng rất nhiều trong giao dịch hành chính điện tử hiện tại và tương lai.

Chương 3. THỬ NGHIỆM CHƯƠNG TRÌNH CHỮ KÝ BỘI

3.1. CẤU HÌNH HỆ THỐNG

3.1.1. 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

3.1.2. 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 .net framework.

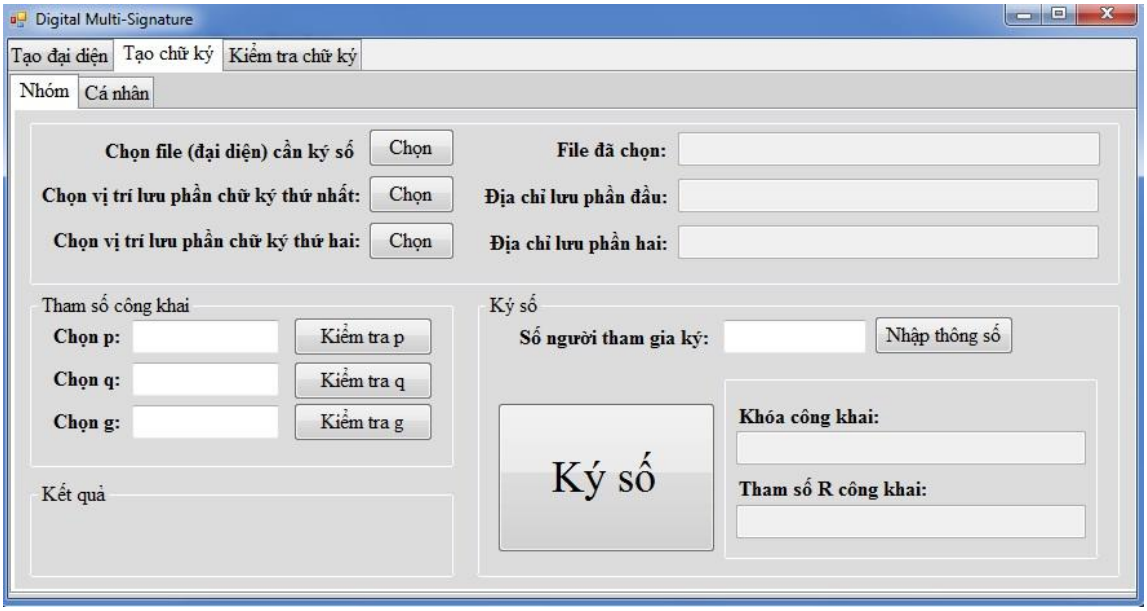
3.2. CÁC THÀNH PHẦN CỦA CHƯƠNG TRÌNH

Chương trình "Chữ ký bội" (Digital Multi-Signature) sử dụng ngôn ngữ vb.net với giao diện được thiết kế trên Visual Studio 2008, gồm ba phần chính:

+ Tạo đại diện.

+ Tạo chữ ký.

+ Kiểm tra chữ ký.



Hình 3.1 Giao diện chương trình.

3.2.1. Tạo đại diện

Phần "Tạo đại diện" sử dụng thuật toán hàm băm MD5 để tạo ra file đại diện từ file cần tạo đại diện ban đầu.

3.2.2. Tạo chữ ký

Phần "Tạo chữ ký" sử dụng thuật toán "hình thành chữ ký số bội" trong "phát triển lược đồ chữ ký bội dựa trên cơ sở bài toán logarit rời rạc" để tiến hành ký số lên file đại diện đầu vào.

3.2.3. Kiểm tra chữ ký

Phần "Kiểm tra chữ ký" sử dụng thuật toán "kiểm tra chữ ký" trong "phát triển lược đồ chữ ký bội dựa trên cơ sở bài toán logarit rời rạc" để tiến hành kiểm tra chữ ký có chính xác với file đầu vào hay không.

3.3. CHƯƠNG TRÌNH

Chương trình cung cấp chức năng tạo đại diện cho tài liệu và lập, kiểm tra chữ ký của file đại diện ấy.

3.3.1. Chức năng tạo đại diện

Đầu vào: File cần tạo đại diện.

Đầu ra: File đại diện.

3.3.2. Chức năng tạo chữ ký

Đầu vào:

+ File đại diện.

+ Các tham số công khai p, q, g.

+ Khóa công khai cá nhân, tham số r cá nhân.

Đầu ra:

+ File phần thứ nhất của chữ ký.

+ File phần thứ hai của chữ ký.

3.3.3. Chức năng kiểm tra chữ ký

Đầu vào:

+ File đại diện.

+ File phần thứ nhất của chữ ký.

+ File phần thứ hai của chữ ký.

+ Các tham số p, q, khóa công khai.

Đầu ra:

+ Kết quả kiểm tra chữ ký.

3.4. HƯỚNG DẪN SỬ DỤNG CHƯƠNG TRÌNH

3.4.1. Hướng dẫn cài đặt chương trình

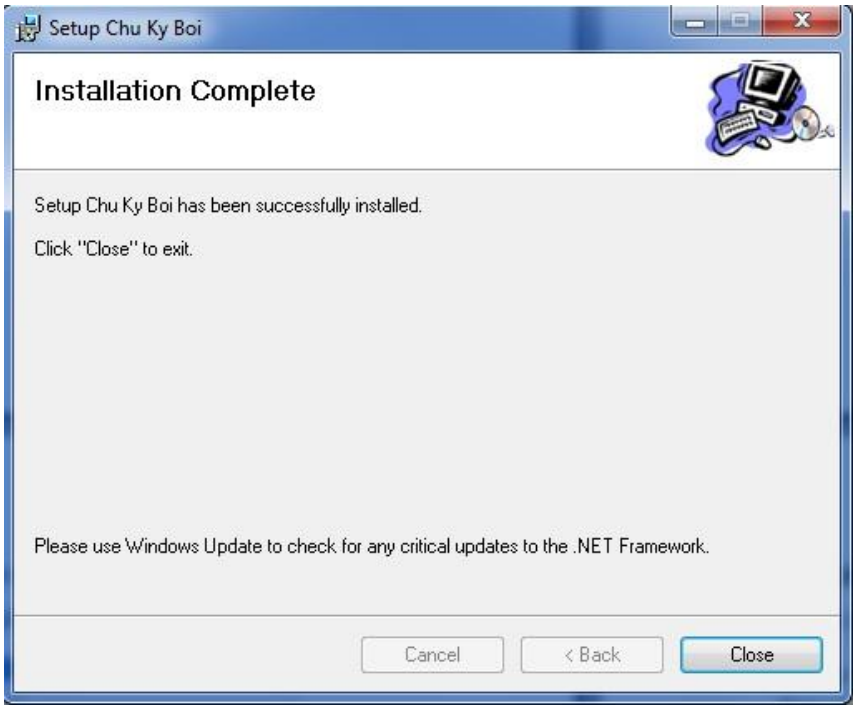
Chạy tệp setup.exe để bắt đầu quá trình cài đặt. Bấm [next].

Hình 3.3 Giao diện bắt đầu quá trình cài đặt.

Sau đó lựa chọn đường dẫn để cài chương trình (hình 3.3). Bấm [next].

Hình 3.4 Thiết lập cài đặt.

Sau khi cài đặt thành công sẽ nhận được thông báo (hình 3.4). Bấm [Close].

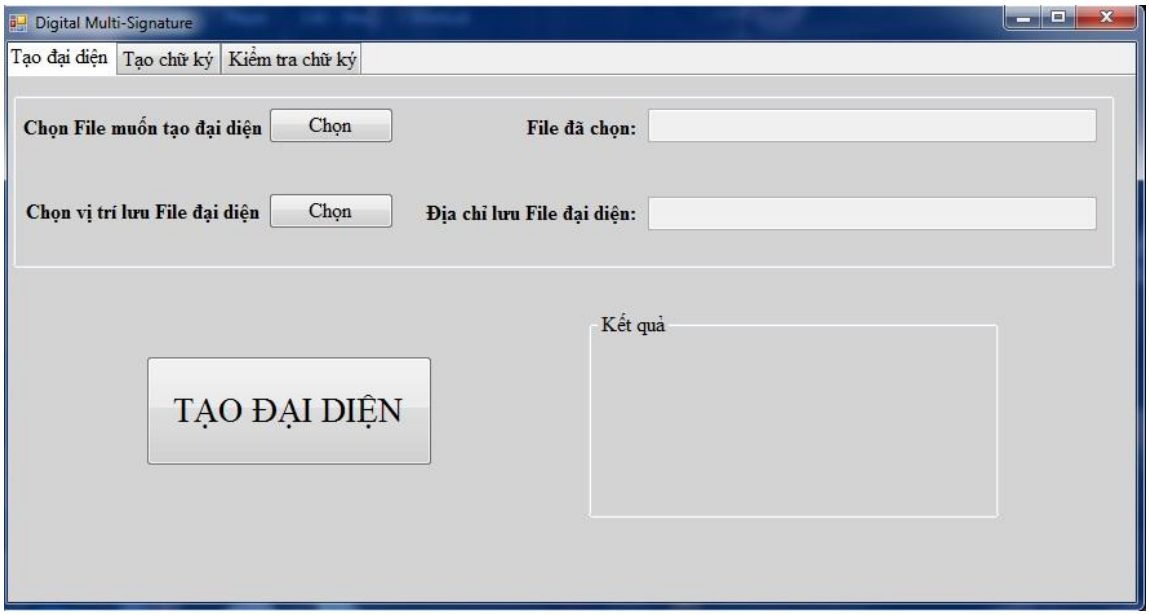


Hình 3.4 Cài đặt thành công.

3.4.2. Hướng dẫn chạy chương trình

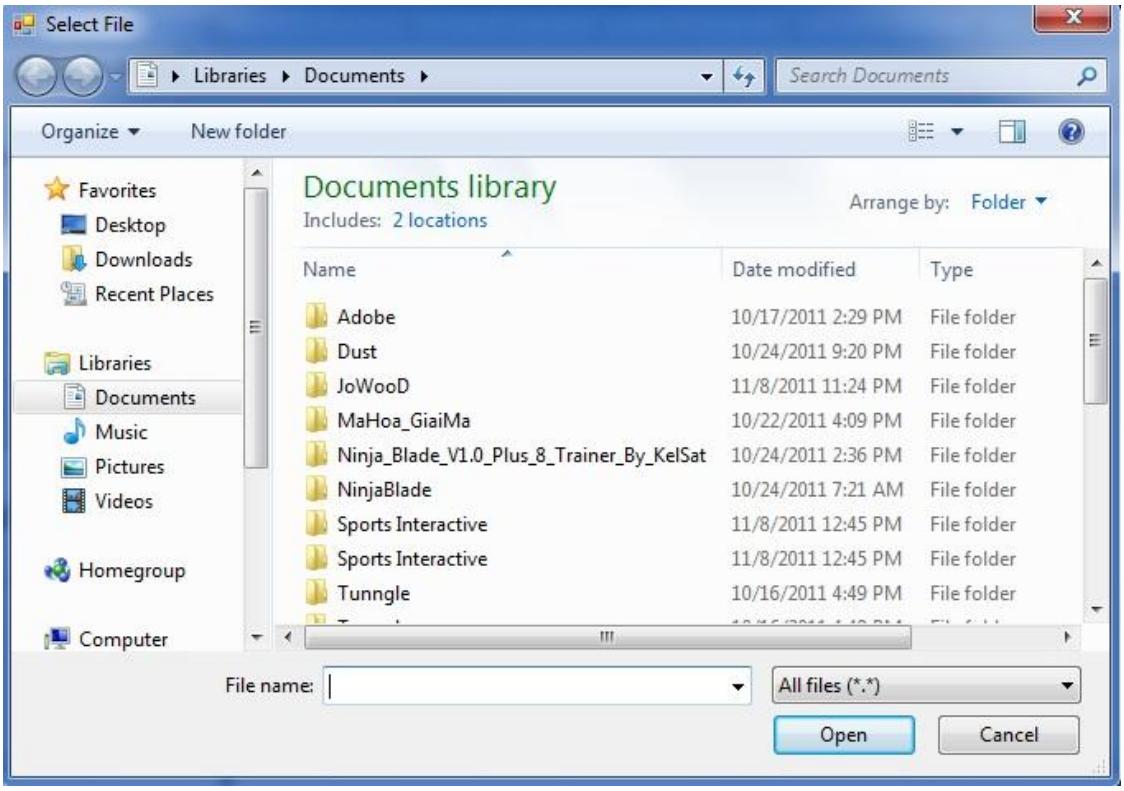
Chạy file ChuKyBoi.exe để vào chương trình.

3.4.2.1. Hướng dẫn chức năng "Tạo đại diện"



Hình 3.5 Giao diện chức năng "Tạo đại diện".

Chọn vị trí File muốn tạo đại diện và vị trí file đại diện sẽ lưu bằng cách bấm [Chọn] ở lần lượt hai vị trí tương ứng.



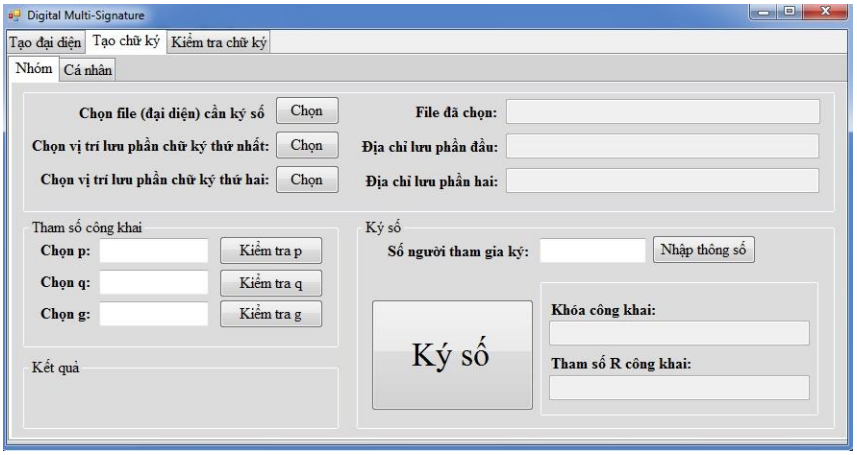
Hình 3.6 Chọn vị trí File cần tạo đại diện.

Sau khi chọn xong vị trí file muốn tạo đại diện và vị trí lưu file đại diện, bấm nút [Tạo đại diện]. Nếu thành công, sẽ nhận được thông báo như trong hình 3.7:

Hình 3.7 Tạo đại diện thành công.

3.4.2.2. Hướng dẫn chức năng "Tạo chữ ký"

Trong chức năng "tạo chữ ký", chọn thẻ "Nhóm" nếu bạn là Trưởng nhóm hoặc người có trách nhiệm thực hiện ký số cho nhóm.



Hình 3.8 Giao diện thẻ "Nhóm".

Trong thẻ "Nhóm", điền các tham số p, q, g thỏa mãn:

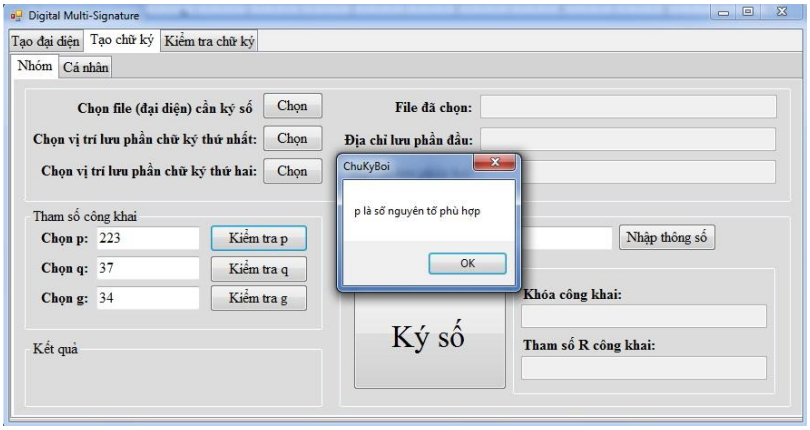
+ p, q là 2 số nguyên tố lớn, sao cho: p = Z.q +1, Z là số nguyên.

+ g là phần tử sinh có bậc q của nhóm Z_p^*, nghĩa là: $0 < g < p$, và: $g^q \equiv 1 \bmod p$.

Bấm nút [Kiểm tra p], [Kiểm tra q], [Kiểm tra g] tương ứng bên cạnh để kiểm tra xem các tham số điền vào có hợp lệ không.

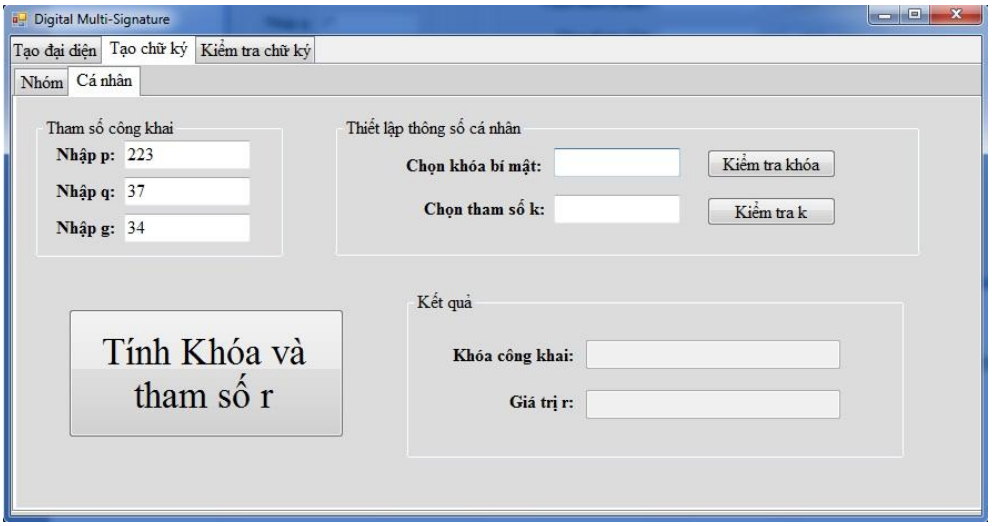
Nếu thông báo trả về là không hợp lệ, điền lại tham số đó và tiếp tục bấm các nút kiểm tra để xác định xem tham số mới có hợp lệ hay không.

Nếu tham số hợp lệ, sẽ hiện thông báo như hình 3.9:



Hình 3.9 Tham số hợp lệ.

Bấm sang thẻ "Cá nhân". Điền các tham số p, q, g hợp lệ do Trưởng nhóm hoặc người có trách nhiệm thực hiện ký số cho nhóm gửi tới.



Hình 3.10 Giao diện thẻ "Cá nhân".

Điền khóa bí mật x của cá nhân và tham số k của cá nhân thỏa mãn:

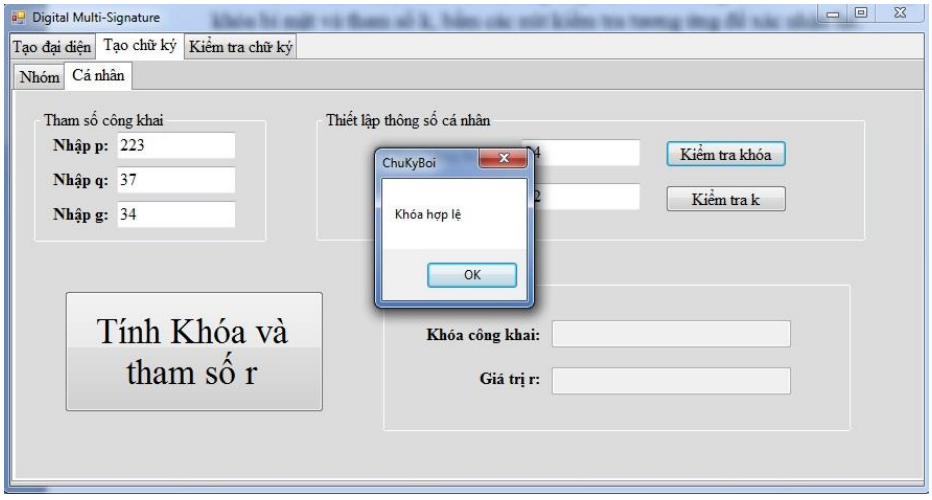
+ $x_i \in [1, q-1]$

+ $k_i \in [1, q-1]$

Bấm [Kiểm tra khóa], [Kiểm tra k] với khóa cá nhân và tham số k tương ứng.

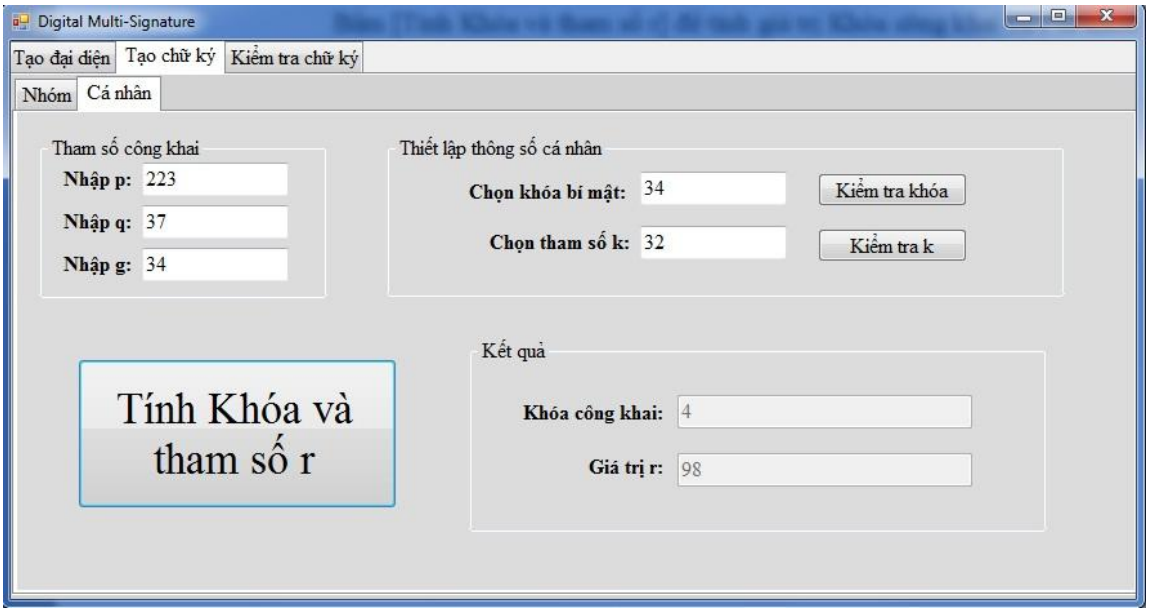
Nếu khóa hoặc tham số không hợp lệ sẽ có thông báo lỗi trả về. Nhập lại khóa bí mật và tham số k, bấm các nút kiểm tra tương ứng để xác nhận lại.

Nếu khóa bí mật và tham số k hợp lệ, sẽ có thông báo như trong hình 3.11:



Hình 3.11 "Khóa cá nhân" hợp lệ.

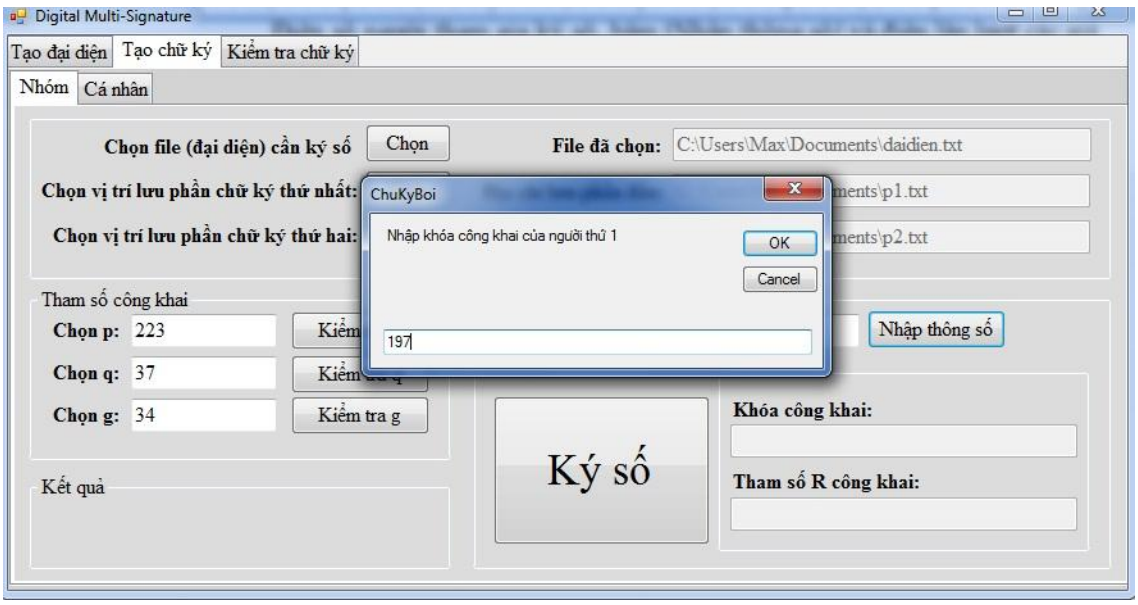
Bấm [Tính Khóa và tham số r] để tính giá trị Khóa công khai và r từ khóa bí mật và tham số k.



Hình 3.12 Tính khóa công khai và tham số r.

Trưởng nhóm hoặc người có trách nhiệm thực hiện ký số cho nhóm bấm trở lại thẻ "Nhóm".

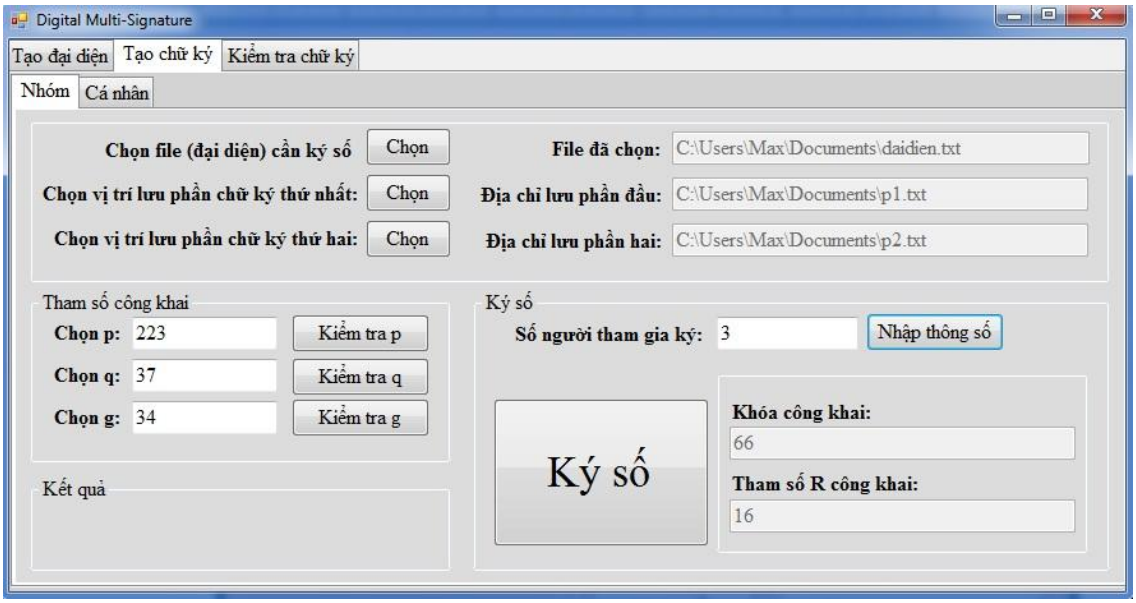
Điền số người tham gia ký số, bấm [Nhập thông số] và điền lần lượt các giá trị "Khóa công khai", "tham số r" tương ứng của họ theo yêu cầu.



Hình 3.13 Nhập khóa công khai và tham số r.

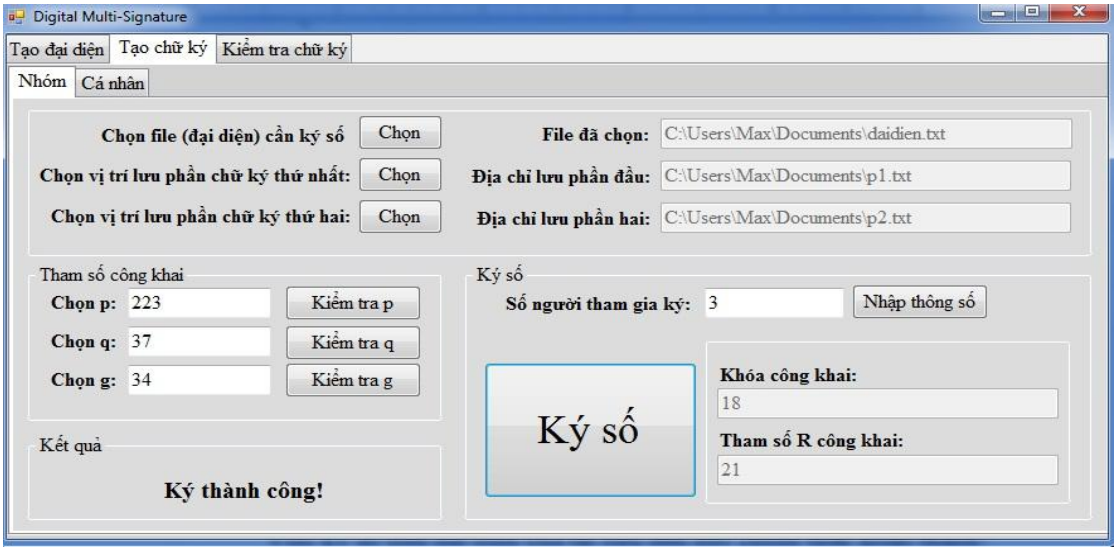
Bấm [OK] để xác nhận, chương trình sẽ hiển thị giá trị khóa công khai, tham số R của nhóm trong mục "Khóa công khai" và "tham số R công khai"

Bấm [Chọn] ở "Chọn file (đại diện) cần ký số", "Chọn vị trí lưu phần chữ ký thứ nhất", "Chọn vị trí lưu phần chữ ký thứ hai" để chọn lựa các file tương ứng.



Hình 3.14 Chọn file cần ký số.

Bấm [Ký số] để tạo hai phần của chữ ký bội. Hai phần này sẽ được lưu vào hai file trong thư mục do người dùng chọn bên trên, đồng thời thông báo việc ký số thành công như hình 3.15:



Hình 3.15 Ký thành công.

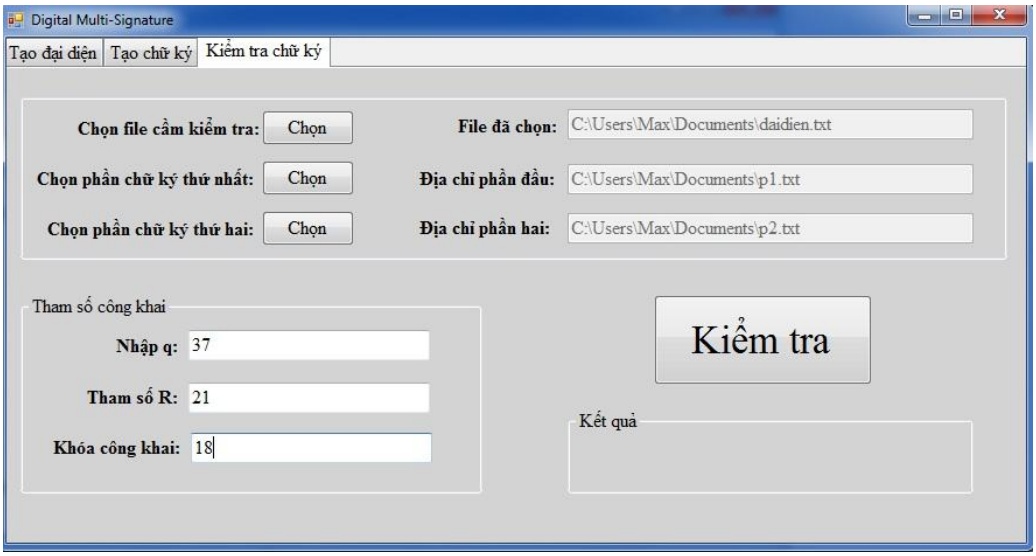
Việc ký số trên đại diện của tài liệu đến đây chính thức hoàn thành!

3.4.2.3. Hướng dẫn chức năng "Kiểm tra chữ ký"

Sau khi nhận được tài liệu và hai file ghi hai phần của chữ ký bội, người sử dụng sẽ dùng chức năng "Tạo đại diện" để tạo một đại diện của tài liệu ấy.

Trong thẻ "Kiểm tra chữ ký", bấm [Chọn] ở "Chọn file cần kiểm tra", "Chọn phần chữ ký thứ nhất", "Chọn phần chữ ký thứ hai" để chọn lựa các file tương ứng.

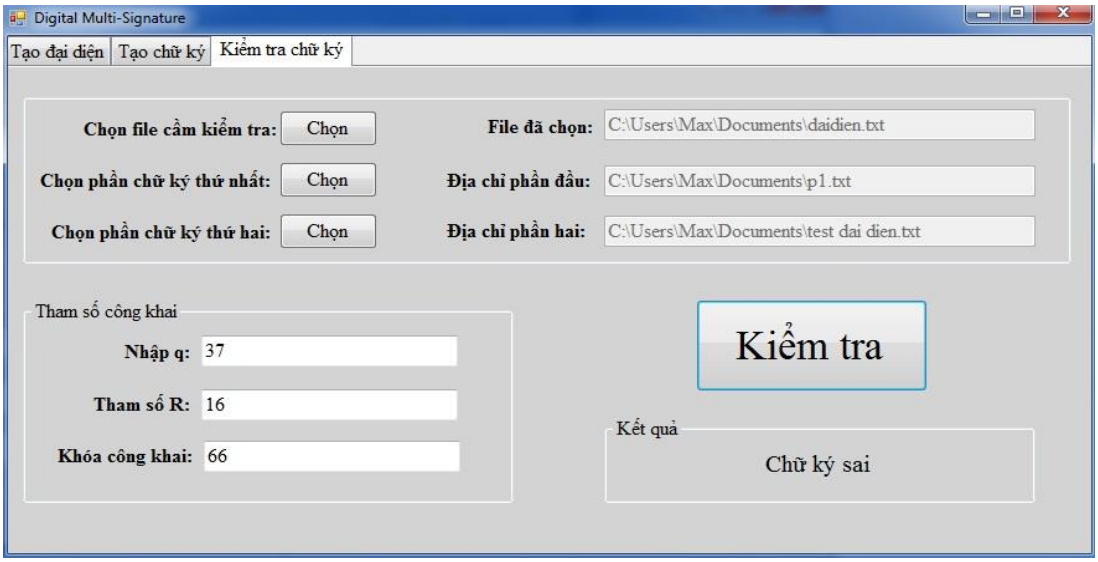
Nhập các tham số q, R công khai, khóa công khai.



Hình 3.16 Giao diện chức năng "kiểm tra chữ ký".

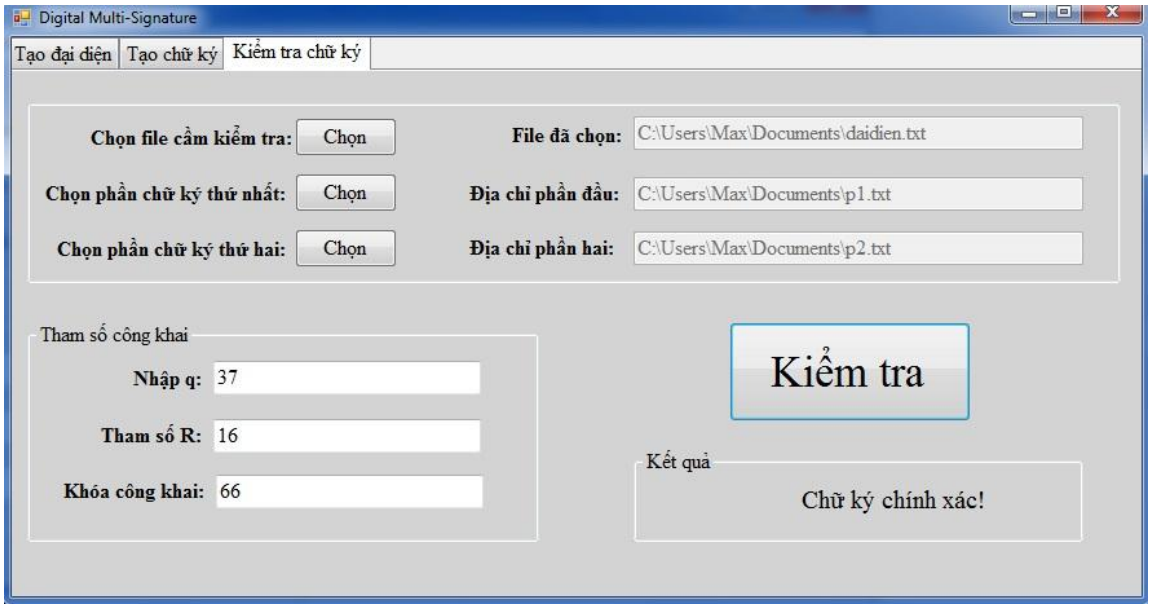
Bấm [Kiểm tra] để tiến hành kiểm tra chữ ký.

Nếu chữ ký không khớp với file cần kiểm tra, kết quả sẽ trả ra như hình 3.17:



Hình 3.17 Chữ ký sai.

Nếu chữ ký chuẩn xác, chương trình sẽ báo về như hình 3.18:



Hình 3.18 Chữ ký chính xác.

KẾT LUẬN

Đồ án 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 chữ ký bội:

Chữ ký bội được sử dụng trong trường hợp một nhóm người có quan hệ với nhau cùng hợp tác để ký vào một văn bản.

Chữ ký bội là phương pháp tạo ra chữ ký số có độ dài không đổi, không phụ thuộc vào số lượng người tham gia ký vào một văn bản, không làm giảm độ tin cậy của chữ ký số. Chữ ký bội cũng tương tự như chữ ký đơn, nhưng để phát sinh chữ ký bội phải có sự hợp tác của các thành viên trong nhóm ký với khóa riêng của từng người.

+ Tổng quan về chính phủ điện tử, giao dịch hành chính điện tử:

Chính phủ điện tử (CPĐT) là Chính phủ ứng dụng Công nghệ thông tin – truyền thông (CNTT-TT) để các cơ quan Chính phủ đổi mới tổ chức, đổi mới các quy trình hoạt động, tăng cường năng lực của Chính phủ, khiến Chính phủ làm việc hiệu lực, hiệu quả và minh bạch hơn, cung cấp thông tin, dịch vụ tốt hơn cho người dân, doanh nghiệp và các tổ chức và tạo điều kiện thuận lợi hơn cho người dân thực hiện quyền dân chủ và tham gia quản lý Nhà nước.

CPĐT là "nhúng" toàn bộ hoạt động quản lý Nhà nước vào môi trường thông tin điện tử, sử dụng Internet và công nghệ Internet để mở rộng khả năng truy cập và cung cấp các dịch vụ công của Chính quyền đến công dân, công chức và doanh nghiệp. Qua đó, Chính phủ có thể quản lý và phục vụ người dân. Người dân chấp hành quy định và thực hiện trách nhiệm của mình thông qua môi trường đó.

Về tổng thể có thể phân loại giao dịch của CPĐT thành bốn loại:

+ Chính phủ với Công dân (G2C).

+ Chính phủ với Người lao động (G2E).

+ Chính phủ với Chính phủ (G2G).

+ Chính phủ với Doanh nghiệp (G2B).

Ngoài bốn mô hình chủ yếu trên, còn có nhiều hình thức giao tiếp khác trong CPĐT như: C2C, C2G, C2B, C2N, B2C…

+ Ứng dụng chữ ký bội trong giao dịch hành chính điện tử:

Giao dịch hành chính điện tử phát sinh rất nhiều các văn bản điện tử cần bảo đảm về khả năng xác thực thông tin, tính xác thực, tính toàn vẹn và tính chống chối bỏ trách nhiệm trong văn bản đó. Vậy nên chữ ký số là một giải pháp thiết yếu cho vấn đề này.

Trong thực tế, có rất nhiều giao dịch, thỏa thuận… cần được ký kết bởi nhiều người, nhiều đối tác. Đối với giao dịch hành chính điện tử, việc xác xác thực của thông tin được chứa đựng trong văn bản do nhiều người chịu trách nhiệm lại càng cấp thiết.

Chữ ký bội được bổ sung vào tài liệu cho phép những người có liên quan, cơ quan có thẩm quyền kiểm tra tính xác thực của tài liệu, cũng như kiểm tra tính toàn vẹn và tính chống chối bỏ trách nhiệm trong văn bản đó.

Việc tạo ra tạo ra chữ ký số có độ dài không đổi, không phụ thuộc vào số lượng người tham gia ký vào một văn bản, không làm giảm độ tin cậy của chữ ký số khiến chữ ký bội sẽ là một giải pháp được sử dụng rất nhiều trong giao dịch hành chính điện tử hiện tại và tương lai.

2/. Thử nghiệm xây dựng chương trình chữ ký bội.

Chương trình mô phỏng các bước trong quá trình lập chữ ký bội, cũng như kiểm tra chữ ký với tài liệu số.

Chữ ký số nói chung và chữ ký bội nói riêng là một hình thức mới, có tính ứng dụng cao trong tương lai. Tuy nhiên, hiện tại ở Việt Nam, chữ ký bội cũng chưa được phổ biến rộng rãi và ứng dụng nhiều trong thực tế, nên trong quá trình nghiên cứu, thực hiện đồ án sẽ không khỏi có những thiếu sót. Kính mong các thầy cô và mọi người quan tâm, bổ xung để đồ án trở nên hoàn chỉnh hơn.

TÀI LIỆU THAM KHẢO

Tiếng Việt.

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

[2] TS Nguyễn Đăng Khoa, "*Tài liệu tập huấn Chính phủ điện tử*".

[3] Lưu Hồng Dũng, "*Phát triển lược đồ đa chữ ký số trên cơ sở bài toán Logarit rời rạc*", Học viện Kỹ thuật Quân sự.

Tiếng Anh.

[1] Harald Baier and Markus Ruppert, "*Interoperable and Flexible Digital Signatures for E-Government"*, Darmstadt Centre of IT Security and FlexSecure Ltd.

[2] Jos Dumortier, *"E-Government and Digital Preservation",* K.U.Leuven – ICRI.