HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Nguyễn Trọng Hiếu

CHỮ KÝ SỐ VÀ ỨNG DỤNG TRONG GIAO DỊCH HÀNH CHÍNH ĐIỆN TỬ

Chuyên ngành: Truyền dữ liệu và mạng máy tính
Mã số: 60.48.15

TÓM TẮT LUẬN VĂN THẠC SĨ KỸ THUẬT

NGƯỜI HƯỚNG DẪN KHOA HỌC : GS. TS NGUYỄN BÌNH

HÀ NỘI – 2011

MỞ ĐẦU

1. Lý do chọn đề tài.

Bảo mật thông tin luôn là vấn đề quan trọng hàng đầu trong các lĩnh vực tình báo, quân sự, ngoại giao, và đây cũng là một vấn đề đã được nghiên cứu hàng nghìn năm nay. Bảo mật thông tin là duy trì tính bảo mật, tính toàn vẹn và tính sẵn sàng của thông tin. Bảo mật nghĩa là đảm bảo thông tin chỉ được tiếp cận bởi những người được cấp quyền tương ứng. Tính toàn vẹn là bảo vệ sự chính xác, hoàn chỉnh của thông tin và thông tin chỉ được thay đổi bởi những người được cấp quyền. Tính sẵn sàng của thông tin là những người được quyền sử dụng có thể truy xuất thông tin khi họ cần. Vấn đề bảo mật đang được nhiều người tập trung nghiên cứu và tìm mọi giải pháp để đảm bảo an toàn, an ninh cho hệ thống phần mềm, đặc biệt là các hệ thống thông tin trên mạng

Internet cho phép mọi người truy cập, khai thác và chia sẻ thông tin. Mặt khác nó cũng là nguy cơ chính dẫn đến thông tin bị rò rỉ hoặc bị phá hoại. Lúc này việc bảo mật an toàn dữ liệu là vấn đề thời sự, là một chủ đề rộng có liên quan đến nhiều lĩnh vực và trong thực tế có nhiều phương pháp được thực hiện để đảm bảo dữ liệu. Nhằm tìm hiểu một trong những phương pháp bảo vệ an toàn thông tin có tính an toàn cao hiện nay là dùng hệ mật mã khoá công khai RSA và đưa ra một vài ứng dụng của mật mã khoá công khai: Sử dụng chữ ký số trong việc xác thực, mã hóa và giải mã các tập tin. Đồng thời, được sự đồng ý và hướng dẫn tận tình của GS.TS Nguyễn Bình tôi đã chọn đề tài: "Chữ ký số và ứng dụng trong giao dịch hành chính điện tử " để làm đề tài nghiên cứu cho luận văn tốt nghiệp của mình.

2. Mục đích nghiên cứu.

Nghiên cứu về lý thuyết mật mã, mật mã hoá khoá công khai RSA, chữ ký số và ứng dụng thuật toán RSA trong mã hoá dữ liệu. Từ đó xây dựng hệ thống cho phép tạo và kiểm tra chữ ký số đối với các tài liệu: công văn, giấy tờ hành chính điện tử để bảo mật nội dung thông tin cũng như xác thực nguồn gốc của thông tin.

3. Phương pháp nghiên cứu.

Nghiên cứu, thu thập các tài liệu đã xuất bản, các bài báo trên các tạp chí khoa học và các tài liệu trên mạng Internet liên quan đến vấn đề đang nghiên cứu của các tác giả trong và ngoài nước. Từ đó chọn lọc và sắp xếp lại theo ý tưởng của mình.

• Tìm hiểu, vận dụng và kế thừa một số các hàm mật mã đã có trên Internet.

• Khai thác hệ thống mã nguồn mở và ngôn ngữ lập trình hướng đối tượng Java để xây dựng một ứng dụng về mã hóa dữ liệu và chữ ký số.

4. Đối tượng nghiên cứu

- Hệ mật mã khóa công khai RSA
- Mô hình chung về chữ ký số và các lược đồ chữ ký số cụ thể như lược đồ chữ ký RSA, lược đồ chữ ký ElGamal, lược đồ chữ ký DSA.

5. Ý nghĩa khoa học và thực tiễn của luận văn.

Về mặt lý thuyết:

- Trình bày trình bày khát quát về mật mã, khái niệm về hệ mật mã khoá bí mật và hệ mật mã khoá công khai.
- Trình bày lý thuyết chung về các phương pháp mã hoá: phương pháp mã hoá khóa bí mật và phương pháp mã hoá khóa công khai, nêu được các ưu điểm và nhược điểm của hai phương pháp này. Trình bày chi tiết hệ mật mã khóa công khai RSA.
- Trình bày lý thuyết chung về mô hình chữ ký số, các lược đồ chữ ký số cụ thể, được xây dựng trên mật mã hoá khoá công khai.

Về mặt thực tiễn

- Xây dựng được chương trình ứng dụng dựa vào hệ mật mã RSA có chức năng bảo mật nội dung cho các tập tin là các dữ liệu hoặc các tài liệu, tạo và kiểm tra chữ ký số cho các tập tin đó để xác định tính toàn vẹn nội dung và chủ nhân của tập tin khi thực hiện trao đổi qua mạng Internet.

6. Bố cục của luận văn.

Ngoài phần mở đầu và kết luận, luận văn gồm có ba chương:

Chương 1. Hệ mật mã khoá công khai

Chương 2. Chữ ký số

Chương 3. Cài đặt chương trình ứng dụng chữ ký số trong giao dịch hành chính điện tử.

Chương 1
HỆ MẬT MÃ KHÓA CÔNG KHAI

1.1. Giới thiệu về các hệ mật mã

Mật mã (Cryptogaraphy) là một môn khoa học nghiên cứu cách viết bí mật. Về phương diện lịch sử, mật mã gắn liền với quá trình mã hóa; điều này có nghĩa là nó gắn với cách thức để chuyển đổi thông tin từ dạng này sang dạng khác, từ dạng thông thường có thể nhận thức được thành dạng không thể nhận thức được, làm cho thông tin trở thành dạng không thể đọc được nếu như không có các thông tin bí mật. Quá trình mã hóa chủ yếu được sử dụng để đảm bảo tính bí mật của các thông tin quan trọng, chẳng hạn trong công tác tình báo, quân sự hay ngoại giao cũng như các bí mật về kinh tế, thương mại.

Một *hệ mật mã (Cryptosystem)* [5] là một bộ năm *(P, C, K, E, D)* thỏa mãn các điều kiện sau:

- *P* là một tập hợp *các bản rõ (chứa thông tin cần mã hóa).*
- *C* là tập hữu hạn các *bản mã (chứa thông tin đã được mã hóa từ bản rõ).*
- *K* là tập hữu hạn các khóa.
- Với mỗi khóa $k \in K$ tồn tại luật mã hóa $e_k \in E$ và luật giải mã $d_k \in D$ tương ứng. Luật mã hóa e_k: $P \rightarrow C$ và luật giải mã e_k: $C \rightarrow P$ là hai ánh xạ thỏa mãn $d_k(e_k(x)) = x, \forall\ x \in P$.

Có 2 phương pháp mã hóa khóa, đó là phương pháp mã hóa khóa đối xứng và phương pháp mã hóa khóa không đối xứng. Những hệ mật mã dựa trên phương pháp mã hóa khóa đối xứng gọi là hệ mật mã khóa đối xứng (Symmetric Key Cryptography) hay hệ mật mã khóa bí mật. Ngược lại, các hệ mật mã dựa trên phương pháp mã hóa khóa không đối xứng gọi là hệ mật mã khóa không đối xứng (Asymmetric Key Cryptography) hay hệ mật mã khóa công khai (Public Key Cryptography).

1.1.1. Hệ mật mã khóa bí mật (Secrete Key Gryposystem - SKG)

1.1.1.1. Giới thiệu

Hệ thống *mã hoá khóa bí mật* [2][5], là hệ thống mã hóa trong đó quá trình *mã hóa* và *giải mã* đều được sử dụng chung một khóa gọi là *khóa bí mật* (Secret key). Việc bảo mật thông tin phụ thuộc vào việc bảo mật khóa.

1.1.1.2. Đánh giá hệ mật mã khoá bí mật

- Ưu điểm:
- Nhược điểm
- Ứng dụng của hệ mật mã khoá bí mật

1.1.2. Hệ mật mã khóa công khai (Public Key Cryptosystem - PKC)

1.1.2.1. Giới thiệu

Nhằm khắc phục các nhược điểm quan trọng của phương pháp mật mã khoá bí mật đã nêu ở trên, năm 1976 Diffie và Hellman ở trường Đại học Stanford công bố một phát kiến mới *"các phương pháp mới trong mật mã"* (New Directions in Cryptography) [5][12]. . Hệ thống được dùng cặp khóa như vậy được gọi là *Hệ mật mã khóa công khai* hay *Hệ mật mã bất đối xứng* (Asymmetric Key Cryptography). Phương pháp mã hóa này đã giải quyết được những nhược điểm của phương pháp mã hóa khóa đối xứng. Đây chính là phương pháp mã hóa mà luận văn này sẽ đi sâu nghiên cứu chi tiết, để giải quyết vấn đề đã đặt ra.

- Khóa công khai (Public Key): là khóa được công bố công khai, mọi người có thể dùng để mã hóa thông tin (lập mã) gửi đến cho người nhận.
- Khóa bí mật (Private Key): hay còn gọi là khóa riêng, là khóa được giữ bí mật để giải mã thông tin mà người khác đã mã hóa bằng khoá công khai.

1.1.2.2. Lý thuyết về mật mã khóa công khai

Mật mã khóa khai đã cố gắng đề giải quyết hai vấn đề khó khăn nhất trong hệ mật mã khóa bí mật đó là: *Sự phân phối khóa* và *chữ ký số*.

Các bước trong mật mã khóa công khai:

- Hệ thống cuối trong mạng tạo ra một cặp khóa để dùng cho mã hóa và giải mã thông điệp mà nó sẽ nhận.

- Mỗi hệ thống công bố rộng rãi khóa mã hóa đây là khóa công khai, khóa còn lại được giữ bí mật.

1.1.2.3. Ứng dụng của hệ mật mã khóa công khai

Tùy thuộc vào những lĩnh vực ứng dụng cụ thể mà người gửi sử dụng khóa bí mật của mình, khóa công khai của người nhận hoặc cả hai để hình thành một số các mô hình ứng dụng phù hợp như sau:

- Mã hóa – giải mã
- Chữ ký số
- Chuyển đổi khóa

1.2. Hệ mật mã khóa công khai RSA

1.2.1. Giới thiệu

Hệ mật mã khóa công khai RSA [2][3][9] là hệ thống mật mã do các giáo sư Ronald Rivest, Adi Sharmir và Leonard Adleman phát mình năm 1978 tại học viện Công nghệ Massachusetts (MIT).

Hệ mã RSA được xây dựng trên cơ sở mã hóa khối trong đó khóa mã hóa là cặp (e,n) gồm số mũ e và module n. Với n là tích số của 2 số nguyên tố rất lớn nào đó, n = p*q còn (e, φ(n)) = 1, với φ(n) là giá trị hàm Euler của n, trong trường hợp này φ(n) = (p - 1)*(q - 1).

1.2.2. Các thuật toán hệ mật mã khóa công khai.

1.2.2.1. Thuật toán sinh khóa

Để sử dụng được hệ mật mã khóa công khai RSA [9][14], trước tiên mỗi người phải tạo riêng cho mình một cặp khóa gồm khóa công khai, và khóa bí mật. Việc tạo ra khóa công khai và khóa bí mật thực hiện theo các bước sau:

- Sinh ra 2 số nguyên tố lớn p và q ngẫu nhiên ($p \neq q$).
- Tính n = p*q.
- φ(n) = (p - 1)*(q - 1).
- Chọn một số tự nhiên e sao cho $1 < e < \varphi(n)$ và là số nguyên tố cùng nhau với φ(n).
- Tính d sao cho $d*e \equiv 1 \pmod{\varphi(n)}$ với $1 < d < \varphi(n)$.
- Khóa công khai (e,n), khóa bí mật (d,n).

1.2.2.2. Thuật toán mã hóa

Hệ RSA là một hệ mật mã điển hình về kiểu mã hóa khối. Nghĩa là, thông điệp được chia thành nhiều khối (hoặc chuỗi) có chiều dài cố định, và mỗi khối sẽ được mã hóa riêng. Giả sử để gửi thông

điệp bí mật M cho người nhận B trong nhóm gửi thông tin an toàn, người gửi A phải thực hiện các bước như sau:

- Thu nhận khóa công khai (e,n) của người nhận B.

Thực hiện một thuật toán để biến đổi thông điệp M thành những số nguyên m_i tương ứng sao cho $m_i < n$, (i = 1,…, k).

1.2.2.3. Thuật toán giải mã

Để thực hiện quá trình giải mã, khôi phục lại nội dung của thông điệp M từ bản mã C nhận được, người nhận B sẽ thực hiện các bước như sau:

- Tính $m_i = C_i^d \pmod n$ với $0 \le m_i \le n$.
- Thực hiện phép biến đổi ngược từ các số m_i thành chuỗi ký tự tương ứng chứa thông tin M ban đầu.

1.2.2.4. Chứng minh tính đúng đắn của quá trình giải mã

Từ: $ed \equiv 1 \pmod{\varphi(n)} \Rightarrow (ed - 1) \mid \varphi(n)$

$$\Leftrightarrow (ed - 1) \mid (p-1) * (q-1)$$

$$\Rightarrow (ed - 1) \mid (p-1) \qquad (1.1)$$

$$\text{và } (ed - 1) \mid (q-1) \qquad (1.2)$$

Từ (1.1) $\Rightarrow \exists k \in Z: ed - 1 = k(p-1)$ (p là số nguyên tố). (1.3)

Xét trường hợp tổng quát với mọi số $m \in Z_n$, khi nâng lũy thừa ed ta có:

$$m^{ed} \equiv m^{(ed-1)+1} \pmod p$$

$$\Leftrightarrow m^{ed} \equiv (m^{(ed-1)}) * m \pmod p \qquad (1.4)$$

Từ (1.3) & (1.4) $\Rightarrow m^{ed} \equiv (m^{k(p-1)}) * m \pmod p$ (1.5)

Vì p là số nguyên tố, vậy bất kỳ số $m \in Z_N$ có hai trường hợp: m nguyên tố cùng nhau với p (nghĩa là. gcd(m, p) = 1) hoặc m là bội số của p (nghĩa là gcd(m, p) = p).

- Trường hợp 1: gcd (m, p) = 1

Vậy $\Rightarrow m^{p-1} \equiv 1 \pmod p$ (theo định lý Fermat).

Từ: (1.5) $\Rightarrow m^{ed} \equiv (1)^k m \pmod p$

$$\Rightarrow m^{ed} \equiv m \pmod p \qquad (1.6)$$

- Trường hợp 2: nếu gcd(m, p) = p $\Rightarrow m \equiv 0 \pmod p$. Đồng thời, lũy thừa số m lên một số nguyên bất kỳ, thì cũng chia hết cho p. Nghĩa là, $m^{ed} \equiv 0 \pmod p$. Vậy trường hợp 2 cũng thỏa mãn phương trình (1.6)

Với cách tính tương với q, từ (1.2) $\Rightarrow m^{ed} \equiv m \pmod q$ (1.7)

Từ (1.6) & (1.7) $\Rightarrow m^{ed} \equiv m \pmod{pq} \equiv m \pmod{n}$ (đpcm).

1.2.2.5. Chuyển đổi văn bản rõ

- Trước khi thực hiện mã hóa, ta phải thực hiện việc chuyển đổi bản rõ (chuyển từ M sang m_i, $0 < i < n$) sao cho không có giá trị nào của M tạo ra bản mã không an toàn.

1.2.2.6. Các ví dụ

1.3. Đánh giá hệ mật mã khóa công khai RSA

1.3.1. Độ an toàn của RSA

Độ an toàn của RSA được thiết kế dựa trên độ khó giải bài toán phân tích ra thừa số nguyên tố n = p*q với 2 số nguyên tố bí mật lớn p, q. Nếu ta chọn các số p, q khoảng 100 chữ số thập phân thì nó sẽ có khoảng 200 chữ số thập phân. Để phân tích một số nguyên cỡ lớn như thế với các thuật toán nhanh nhất hiện nay cùng với những máy tính hiện đại nhất cũng mất hàng triệu năm. Như vậy việc phân tích số nguyên n thành các thừa số nguyên tố p, q nhằm mục đích bẻ gãy hệ mật mã RSA là điều khó có thể tính toán nổi nếu như trong quá trình thiết kế hệ RSA ta chọn số nguyên N lớn.

1.3.2. Hiệu suất thực hiện của thuật toán RSA

Tốc độ thực hiện của hệ RSA là một trong những điểm yếu so với các hệ mật mã khóa đối xứng.

Theo ước tính, thực hiện mã hóa và giải mã bằng hệ mật mã RSA chậm hơn 100 lần so với hệ mật mã khóa đối xứng DES (khi thực hiện bằng phần mềm). Và chậm hơn 1000 lần so với DES (khi thực hiện bằng phần cứng) [4].

1.4. Chi phí và tốc độ thực hiện của thuật toán RSA

1.4.1. Chi phí

Để thực hiện thuật toán RSA phần lớn phải tốn chi phí thực hiện các phép tính cơ bản như: tạo khoá, mã hoá, giải mã. Quá trình mã hoá và giải mã tương đương với chi phí thực hiện các phép tính luỹ thừa module n. Để đảm bảo cho khoá bí mật được an toàn thì thường chọn số mũ công khai e nhỏ hơn nhiều so với số mũ bí mật d, do đó chi phí thời gian để thực hiện mã hoá dữ liệu nhỏ hơn nhiều so với thời gian giải mã.

1.4.2. Tốc độ của hệ RSA

Tốc độ của RSA là một trong những điểm yếu của RSA so với các hệ mã đối xứng, so với hệ mã DES thì RSA chậm hơn từ 100 đến 1000 lần, vì vậy RSA không được dùng để mã hoá khối lượng dữ liệu lớn mà thường dùng để mã hoá những dữ liệu nhỏ.

1.5 Một số phương pháp tấn công hệ mã RSA

1.5.1. Tấn công lặp

Simons và Norris [9][13] đã chỉ ra rằng hệ thống RSA có thể bị tấn công khi sử dụng tấn công lặp liên tiếp. Đó là khi kẻ tấn công biết khóa công khai (*e, n*) và bản mã C thì anh ta có thể tính chuỗi các bản mã sau:

$C_1 = C^e \pmod n$

$C_2 = C_1^e \pmod n$

……

$C_i = C_{i-1}^e \pmod n$

Nếu có một phần tử C_j trong chuỗi $C_1, C_2, \ldots, C_i, \ldots$ sao cho $C_j = C$ thì khi đó anh ta sẽ tìm được $M = C_{j-1}$ bởi vì:

$C_j = C_{j-1}^e \pmod n$

$C = M^e \pmod n$

1.5.2. Kiểu tấn công module n dùng chung

Simons và Norris cũng chỉ ra rằng hệ thống RSA có thể bị tấn công khi sử dụng module n dùng chung, thực vậy nếu một thông điệp M được mã hoá bằng hai khoá công khai e_1 và e_2 từ hai thành viên trong hệ thống thì được:

$C_1 = M^{e_1} \pmod n$

$C_2 = M^{e_2} \pmod n$

Sau đó người tấn công dùng thuật toán Euclide mở rộng: $e_1*a + e_2*b = 1$ sao cho $\gcd(e_1,e_2) = 1$ thì M được khôi phục lại như sau: $M = C_1^a \cdot C_2^b \bmod n$.

1.5.3. Tấn công khi khoá công khai e nhỏ

Hastad đã đưa ra kiểu tấn công khi khoá công khai e nhỏ (e =3) của hệ mã công khai RSA như sau:

Giả sử để gửi thông điệp M đến các người dùng P_1, P_2 …,P_k với khoá công khai là (e_i , n_i). A mã hoá M bằng khoá công khai (e_i , n_i) và gửi các bản mã C_i đến người dùng P_i, biết M < n_i với i = 1, 2,…, n.

Ta có thể nghe trộm kết nối ra ngoài của A và thu thập được k bản mã C_i.

Giả sử các khoá công khai e_i = 3 thì có thể khôi phục M nếu k ≥ 3.

Thực vậy, nếu có được C_1, C_2, C_3 với $C_1 = M^3 \bmod n_1$; $C_2 = M^3 \bmod n_2$; $C_3 = M^3 \bmod n_3$ và gcd(n_i,n_j) = 1, i ≠ j. Áp dụng định lý số dư Trung Hoa với C_1; C_2, C_3 tìm được C' $\in Z_{n_1 n_2 n_3}$ thoả C' = $M^3 \bmod n_1 n_2 n_3$ → M^3 là số nguyên.

Vậy M = $\sqrt[3]{C'}$.

1.6. Ứng dụng của hệ mật mã RSA

Thực tiễn cho thấy tốc độ thực hiện của RSA là chậm. Tuy nhiên, người ta tìm thấy ở hệ mã RSA những khả năng ứng dụng độc đáo khác, thay vì trực tiếp mã hoá văn bản.

- Tạo vỏ bọc an toàn cho văn bản
- Tạo chữ ký số cho văn bản

1.7. Kết luận Chương 1

Chương này đã thể hiện những nội dung sau:

- Trình bày khát quát về mật mã, khái niệm về hệ mật mã khoá bí mật và hệ mật mã hoá khoá công khai.

- Trình bày một số thuật toán và định lý toán học dùng trong các hệ mã công khai.

- Trình bày chi tiết hệ mật mã hoá khoá công khai, thuật toán mã hoá, giải mã và một số phương pháp tấn công hệ mã RSA.

****

Chương 2
CHỮ KÝ SỐ

2.1. Các khái niệm cơ sở

2.1.1. Chữ ký điện tử

Chữ ký điện tử (electronic signature) không phải là hình thức số hoá chữ ký viết tay rồi gửi kèm theo một thông điệp mà là một phương thức để chứng thực nguồn gốc và nội dung của một thông điệp thông qua kỹ thuật mã hoá.

2.1.2. Chữ ký số

Chữ ký số (Digital signature) là một dạng *chữ ký điện tử* (là tập con của *chữ ký điện tử*) được tạo ra bằng sự biến đổi một *thông điệp dữ liệu* sử dụng hệ thống mật mã hoá khoá công khai, theo đó người có thông điệp dữ liệu ban đầu và khoá công khai của người ký có thể xác định được chính xác:

2.1.3. Phương tiện số

Là phương tiện hoạt động dựa trên công nghệ điện, số, kỹ thuật số, từ tính, truyền dẫn không dây, quang học, số hoặc công nghệ tương tự.

2.1.4. Giao dịch số

Giao dịch số được hiểu một cách đơn giản là hình thức giao dịch mà đối tượng không gặp gỡ trực tiếp với nhau. Các thông tin cần trao đổi giữa các bên được thực hiện qua các phương tiện số, chẳng hạn mạng Internet… Những thông điệp đó có giá trị pháp lý giống như những thông điệp trong giao dịch trực tiếp hàng ngày.

2.1.5. Thông điệp dữ liệu

Thông điệp dữ liệu là thông tin được tao ra, được gửi đi, được nhận và được lưu trữ bằng phương tiện số.

2.1.6. Chứng thực số

Chứng thực số là hoạt động chứng thực danh tính của những người tham gia vào việc gửi và nhận thông tin qua mạng, đồng thời cung cấp cho họ những công cụ, những dịch vụ cần thiết để thực hiện việc bảo mật thông tin, chứng thực nguồn gốc và nội dụng thông tin.

2.2. Hàm băm (Hash Funtion)

Hàm băm mật mã là hàm toán học chuyển đổi thông điệp (message) có độ dài bất kỳ (hữu hạn) thành một dãy bit có độ dài cố định (tuỳ thuộc vào thuật toán băm). Dãy bit này được gọi là *thông điệp rút gọn* (message digest) hay *giá trị băm* (hash value), đại diện cho thông điệp ban đầu.

2.2.1. Hàm băm MD5

Thuật toán băm MD5 (Message Digest 5) [5], [9] được thiết kế bởi Ronald Rivest vào năm 1991, thuật toán này là sự nâng cấp mở rộng từ thuật toán băm MD4, nhằm mục đích nâng cao độ an toàn và hiệu quả thực hiện.

2.2.2. Hàm băm SHA-1

Giống với thuật toán băm MD5, thuật toán băm SHA-1 nhận thông điệp ở đầu vào có chiều dài $k \leq 2^{64}$-bits, thực hiện xử lý và đưa ra thông điệp thu gọn (message digest) có chiều dài cố định 160-bits [5][9]. Quá trình tính toán cũng thực hiện theo từng khối 512-bits, nhưng bộ đệm xử lý dùng 5 thanh ghi 32-bits. Thuật toán này chạy tốt đối với các bộ vi xử lý có cấu trúc 32-bits.

2.3. Một số lược đồ chữ ký số

2.3.1. Định nghĩa

Một *lược đồ chữ ký số* là một bộ (***M, M*$_S$*, K, S, V***) trong đó [9][10]:

- ***M*** là tập hữu hạn các *văn bản* có thể.
- ***M*$_S$** là tập hữu hạn các *chữ ký* có thể.
- ***K*** là tập hữu hạn các *khóa*.
- ***S*** là tập các *thuật toán ký*.
- ***V*** là tập hợp các *thuật toán chứng thực chữ ký*.

Với mỗi $k \in \boldsymbol{K}$ là một cặp (k', k''), trong đó k' *là khóa bí mật* dùng để ký, k'' là *khóa công khai* dùng để *chứng thực chữ ký*.

Mỗi $k = (k', k'') \in \boldsymbol{K}$. Có một thuật toán ký $Sig_{k'}$: $\boldsymbol{M} \rightarrow \boldsymbol{M_s}$ ($Sig_{k'} \in$ S) và một thuật toán kiểm thử $Ver_{k''}$: $\boldsymbol{M}$ x $\boldsymbol{M_s} \rightarrow$ {True, False} ($Ver_{k''} \in \boldsymbol{V}$). Thoả mãn điều kiện sau đây với mọi $x \in \boldsymbol{M}$, $y \in \boldsymbol{M_s}$:

$$Ver_{k''}(x; y) = \begin{cases} \text{True, nếu } y = Sig_{k'}(x) \\ \text{False, nếu } y <> Sig_{k'}(x) \end{cases}$$

2.3.2. Yêu cầu của một hệ thống chữ ký số

Hệ thống chữ ký số cần thỏa mãn các yêu cầu sau :

- Tính an toàn (security).
- Tính hiệu quả (performance):
- Chống nhân bản chữ ký.
- Tính không thể phủ nhận (non-repudiation).

2.3.3. Phân loại các lược đồ chữ ký số

Dựa vào các lược đồ sinh chữ ký số, có thể chia lược đồ chữ ký số thành hai loại như sau [9][10]:

2.3.2.1. Lược đồ chữ ký số kèm theo bản rõ

Loại *lược đồ chữ ký số* này cũng được dùng phổ biến trong thực tế. Chúng dựa vào các hàm băm mật mã [9] và ít bị tấn công giả mạo hơn.

- Định nghĩa:

Lược đồ chữ ký số mà yêu cầu phải có *thông điệp* là đầu vào cho thuật toán chứng thực chữ ký được gọi là *lược đồ chữ ký số kèm theo bản rõ.*

2.3.2.2. Lược đồ chữ ký số tự khôi phục bản rõ

- Định nghĩa

Lược đồ chữ ký số tự khôi phục bản rõ là lược đồ chữ ký số không đòi hỏi phải có *thông điệp gốc* làm đầu vào để *chứng thực chữ ký* mà *thông điệp gốc* sẽ được phục hồi chính từ *chữ ký* đó [9].

- Thuật toán sinh khoá
- Thuật toán sinh chữ ký.
- Thuật toán xác thực chữ ký.

2.3.4. Một số lược đồ chữ ký số

2.3.4.1. Lược đồ chữ ký RSA

Trong phần này mô tả *lược đồ chữ ký RSA*. Độ an toàn của lược đồ chữ ký RSA dựa vào độ an toàn của hệ mã RSA. Lược đồ bao gồm cả chữ ký số kèm theo bản rõ và tự khôi phục thông điệp từ *chữ ký số.*

- ***Thuật toán sinh khóa cho lược đồ chữ ký RSA***
- ***Thuật toán sinh chữ ký RSA***
- ***Thuật toán chứng thực chữ ký RSA***

2.3.4.2. Lược đồ chữ ký ELGamal

Phương pháp chữ ký số ELGamal được giới thiệu vào năm 1985 [5][9]. Sau đó, Viện Tiêu Chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST) đã sửa đổi bổ sung phương pháp này thành chuẩn chữ ký số (Digital Signature Standard - DSS).

- ***Thuật toán sinh khoá cho lược đồ chữ ký ELGamal.***
- ***Thuật toán sinh chữ ký***
- ***Thuật toán chứng thực chữ ký***
- ***Thuật toán sinh khoá cho lược đồ chữ ký DSA***
- ***Thuật toán sinh chữ ký DSA***
- ***Thuật toán chứng thực chữ ký DSA***

2.4. Kết luận Chương 2

Chương 2 đã trình bày khái niệm về *chữ ký số* và một số khái niệm có liên quan đến *chữ ký số,* giới thiệu về hàm băm và trình bày hai giải thuật băm được dùng phổ biến là MD5 và SHA-1.

Nêu định nghĩa *lược đồ chữ ký số,* phân loại các lược đồ chữ ký số, trình bày chi tiết và nêu các ví dụ minh hoạ cho các lược đồ chữ ký số như: lược đồ chữ ký ELGamal, lược đồ chữ ký DSA, lược đồ chữ ký RSA. Trong đó lược đồ chữ ký RSA sẽ được cài đặt thành chương trình "**Ứng dụng trong giao dịch hành chính điện tử**" trong chương 3.

****

Chương 3
CÀI ĐẶT CHƯƠNG TRÌNH ỨNG DỤNG CHỮ KÝ SỐ TRONG GIAO DỊCH HÀNH CHÍNH ĐIỆN TỬ

3.1. Hành chính điện tử

Lợi ích giao dịch hành chính điện tử:

Lợi ích lớn nhất mà giao dịch hành chính điện tử đem lại chính là sự tiết kiệm chi phí và tạo thuận lợi cho các bên giao dịch. Giao dịch bằng phương tiện điện tử nhanh hơn so với giao dịch truyền thống, ví dụ gửi thư điện tử thì nội dung thông tin đến tay người nhận nhanh hơn gửi thư bằng phương pháp thông thường. Đặc biệt, các giao dịch qua Internet có chi phí rất rẻ.

3.1.1. Nguy cơ mất an toàn thông tin trong giao dịch hành chính điện tử

- Nghe trộm (Eavesdropping).
- Giả mạo (Tampering).
- Mạo danh (Impersonation).
- Chối bỏ nguồn gốc (Repudiation).

3.1.2. Tính pháp lý và ứng dụng chữ ký số trong và ngoài nước

3.1.2.1. Trong nước

3.1.2.2. Ở một số nước trên thế giới

3.1.2.3. Ứng dụng trong thực tế

Chữ ký số được sử dụng trong các công việc như: ký vào văn bản, tài liệu điện tử; bảo mật thư điện tử; bảo đảm an toàn cho Web Server (thiết lập kênh trao đổi bảo mật giữa Web client và Web server trên Internet)

3.2. Cài đặt chương trình ứng dụng

- Các yêu cầu của ứng dụng

- Tạo ra cặp khoá: *khoá công khai* và *khoá bí mật* bằng hệ mật mã khoá công khai RSA.
- Thực hiện *ký chữ ký số* lên thông điệp bằng cách dùng *khoá bí mật* của người ký.
- Thực hiện việc *chứng thực chữ ký số* bằng cách dùng *khoá công khai* của người đã ký lên thông điệp.
- Dùng *khoá công khai* của người nhận để thực hiện quá trình *mã hoá* thông điệp hoặc tập tin.
- Người nhận dùng *khoá bí mật* của mình để thực hiện quá trình *giải mã* thông điệp hoặc tập tin.

- Môi trường xây dựng ứng dụng

- Sử dụng thuật toán băm MD5 để băm thông điệp trước khi thực hiện ký chữ ký số.
- Sử dụng hệ mật mã khoá công khai RSA để thực hiện sinh khoá cho hệ thống.
- Dùng ngôn ngữ lập trình Java để viết mã cho chương trình.

3.2.1. Quá trình ký và xác thực chữ ký số

3.2.1.1. Ký văn bản số

3.2.1.2. Xác thực chữ ký số

3.2.1.2. Mã hoá tập tin

3.2.1.4. Giải mã tập tin

3.2.2. Thuyết minh chương trình

3.2.2.1. Quá trình tạo cặp khóa bí mật và khóa công khai

- ***Tính module n***
- ***Sinh khóa e***
- ***Tính khóa d***

3.2.2.2. Quá trình tạo chữ ký số

Để tạo và lưu chữ ký số ta lần lượt thực hiện các bước sau:

- ***Số hóa thông điệp:***
  - Nhập nội dung "Thông điệp ban đầu".
  - Chọn "Tập tin đính kèm" (nếu có).
  - Sau khi chọn xong các nội dung trên (ít nhất phải nhập vào Thông điệp ban đầu), chọn nút "**Số hóa thông điệp**".

Tạo và lưu chữ ký số: Chuyển sang thẻ "**Tạo chữ ký**", chọn nút "**Ký văn bản**".

Chọn nút "**Lưu chữ ký vào file**" để thực hiện việc lưu chữ ký. Nội dung file được lưu bao gồm: Nội dung chữ ký, module n và khóa e.

3.2.2.3. Quá trình xác thực chữ ký

Khi cá thể B nhận được chữ ký từ A, B sẽ thực hiện các bước sau để xác thực chữ ký:

- Vào menu **File → Xác thực chữ ký**, nhập vào "**Nội dung thông điệp**" và "**Chọn tập tin đính kèm**" (nếu có) sau đó chọn nút "**Xác thực chữ ký**".
- Nếu đúng là chữ ký của A thì sẽ nhận được thông báo "**Chữ ký đã được xác thực**".
- Nếu không đúng là chữ ký của A hoặc không đúng nội dung (Nội dung thông điệp hay Tập tin đính kèm) thì sẽ nhận được thông báo "**Thông điệp hoặc tập tin đính kèm đã bị thay đổi**".

3.2.2.4. Mã hóa tập tin bằng khóa công khai

Để mã hóa tập tin bằng khóa công khai của người nhận, ta thực hiện theo các bước sau:

- Vào menu **File → Mã hoá tập tin**.
- Chọn khóa công khai của người nhận để mã hóa tập tin (Khóa e, Module n).
- Chọn tập tin cần mã hóa.
- Chọn nút "**Mã hóa tập tin**".

Khi đó chương trình sẽ mã hóa tập tin vừa nhập.

3.2.2.5. Giải mã tập tin băng khóa bí mật

Để giải mã tập tin bằng khóa bí mật của người nhận ta thực hiện như sau:

- Vào menu **File → Giải mã tập tin**.
- Chọn khóa bí mật để giải mã tập tin (Khóa d, Module n).
- Chọn tập tin được mã hóa bằng khóa công khai của người nhận.
- Chọn nút "**Giải mã**".

Khi đó chương trình sẽ giải mã tập tin và hiện thông báo: "**Đã thực hiện giải mã tập tin**".

3.3. Kết luận Chương 3

Chương này giới thiệu về hành chính điện tử, tình hình ứng dụng cũng như tính pháp lý của chữ ký số. Trong chương này còn giới thiệu sơ lược về sự hình thành và phát triển của chữ ký số trên thế giới và ở Việt Nam. Sau đó phân tích cách thực hiện các quá trình: *ký và xác thực chữ ký số, mã hoá và giải mã tập tin*, từ đó xây dựng chương trình demo thực hiện các quá trình trên.

****

KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

Luận văn nghiên cứu về hệ mật mã khóa công khai, trong đó hệ mã RSA được tập trung tìm hiểu, từ đó có được những kiến thức cần thiết để xây dựng chương trình "**Chữ ký số, ứng dụng trong giao dịch hành chính điện tử**". Luận văn đã đạt được một số kết quả như sau:

- Giới thiệu một cách khái quát các kiến thức cơ bản như: lý thuyết mật mã, khái niệm về hệ mật mã khóa bí mật và hệ mật mã khóa công khai. Trình bày một số thuật toán và định lý toán học dùng trong các hệ mã công khai.

Trình bày chi tiết hệ mật mã hoá khoá công khai, thuật toán mã hoá, giải mã và một số phương pháp tấn công hệ mã RSA.

- Trình bày hai thuật toán băm được dùng phổ biến và có độ an toàn cao là MD5 và SHA-1 để tạo ra các thông điệp thu gọn (message digest), ứng dụng vào lược đồ chữ ký số. Phân loại các lược đồ chữ ký số, trình bày chi tiết và nêu các ví dụ minh họa lược đồ chữ ký RSA, DSA, ELGamal.
- Cài đặt chương trình ứng dụng "Chữ ký số và ứng dụng trong giao dịch hành chính điện tử" để thực hiện các quá trình: Ký và xác thực chữ ký, mã hóa và giải mã các tập tin… giao dịch qua mạng.

Hướng phát triển:

Do thời gian nghiên cứu có hạn, nên chương trình mới chỉ mô phỏng được các thao tác: ký, xác thực chữ ký, mã hóa và giải mã tập tin mà chưa thiết kế một cách hoàn chỉnh để có thể kết nối trực tiếp vào một số phần mềm : gửi nhận email, phần mềm quản lý văn bản … Hướng phát triển của đề tài là xây dựng chương trình để có thể kết nối trực tiếp vào một số phần mềm gửi nhận email và phần mềm quản lý văn bản. Đồng thời xây dựng một hệ thống chứng thực khóa công khai

cho các thành viên, nhằm tránh trường hợp bị người khác giả mạo khóa công khai của người nhận khi thực hiện trao đổi thông tin.

Cuối cùng, với những kết quả đạt được của luận văn, tuy còn có những hạn chế, nhưng đã giúp tôi có được khả năng nghiên cứu cơ bản về bảo mật và xác thực thông tin. Từ đó có thể xây dựng các ứng dụng về bảo mật và xác thực thông tin ở những cấp độ an toàn khác nhau.

****

TÀI LIỆU THAM KHẢO

Tiếng Việt

1. Đoàn Văn Ban (2005), *Lập trình hướng đối tượng với Java,* NXB Khoa học và kỹ thuật.
2. Nguyễn Hiếu Minh (2007), *Bài giảng lý thuyết mật mã***,** Học viện KTQS.
3. Nguyễn Đình Thúc, Bùi Doãn Khanh (2006), *Giáo trình mã hóa thông tin – Lý thuyết và ứng dụng***,** NXB Lao động xã hội.
4. Vũ Dương Thụy, Nguyễn Văn Nho, Trần Hữu Nam (2004), *Lý thuyết số các định lý cơ bản và bài tập chọn lọc***,** NXB Giáo dục.
5. Dương Anh Đức, Trần Minh Triết (2005), *Giáo trình Mã hoá và ứng dụng***,** Trường ĐH Khoa học tự nhiên, ĐH Quốc gia TP HCM.
6. Phạm Huy Điển, Hà Huy Khoái (2004), *Mã hoá thông tin cơ sở toán học và ứng dụng***,** Viện toán học.
7. Phan Đình Diệu (1999), *Giáo trình lý thuyết mật mã và an toàn thông tin***,** NXB Đại học Quốc gia HN.
8. Nguyễn Thành Nhân (2007), *Attacks and Defences on RSA cryptosystem***,** NXB Thanh niên.

Tiếng Anh

9. A. MENEZES, P. VAN OORSCHOT, AND S. VANSTONE (1997), *Handbook of Applied Cryptography*, CRC Press.

10. Rolf Oppliger (2005), *Contemporary Cryptography*, Artech House.

11. DAN BONEH (1999), *Twenty Year of Attacks on RSA***,** Stanford University.

12. WHITFIELD DIFFIE AND MARTIN E.HELLMAN (1976), *New Direction in Cryptography***,** Invited Paper.

13. AJREN LESNTRA, ERAN TROMER, ADI SHAMIR, WIL KORTSMIT, BRUCE DODSON, JAMES HUGHES, PAUL LEYLAND (2003), *Factoring Estimates for a 1024-bit RSA modulus***,** Paper.

14. DAN BONEH (1999), *Twenty Year of Attacks on RSA***,** Stanford University.

15. Adi Shamir and Eran Trome (2003), *Factoring Large Numbers with the TWIRL Device*, The Wiezman Institute Relation Locator.

Địa chỉ trên Internet

16. https://vasc-ca.vasc.com.vn

17. http://sms.fit.hcmuns.edu.vn/i-learning

18. http://www.rsasecurity.com/rsalabs/node.asp?id=2152

19. http://www.rsa.com/rsalabs/node.asp?id=2124

20. http://www.aci.net/kalliste/cryptnum.htm

21. http://www.newobjects.com/product.asp?Category=63&Story=293

22. http://williamstallings.com/Extras/Security-Notes/lectures/authent.html

23. http://www.cryptography.com

24. http://www.luatvietnam.vn

25. http://www.dongnai.gov.vn