

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

-----



**BÙI THU HÀ**

**NGHIÊN CỨU XÂY DỰNG CHỮ KÝ SỐ  
VÀ ỨNG DỤNG TRONG HÓA ĐƠN ĐIỆN TỬ TẠI CÔNG TY  
LDVC QUỐC TẾ HẢI VÂN**

**CHUYÊN NGÀNH : KHOA HỌC MÁY TÍNH**

**MÃ SỐ: 60.48.01.01**

**LUẬN VĂN THẠC SĨ KỸ THUẬT**

*(Theo định hướng ứng dụng)*

**NGƯỜI HƯỚNG DẪN KHOA HỌC: TS. NGUYỄN TRUNG KIÊN**

**HÀ NỘI - 2016**

Luận văn được hoàn thành tại:

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

Người hướng dẫn khoa học: TS. Nguyễn Trung Kiên

Phản biện 1: .....

Phản biện 2: .....

Luận văn sẽ được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông

Vào lúc: ... giờ .... ngày ..... tháng .... năm .....

Có thể tìm hiểu luận văn tại:

- Thư viện của Học viện Công nghệ Bưu chính Viễn thông

# MỞ ĐẦU

**Tính cấp thiết của đề tài**

**Tổng quan về vấn đề nghiên cứu**

**Mục đích, đối tượng, phạm vi và phương pháp nghiên cứu**

**Cấu trúc luận văn**

Nội dung của luận văn được trình bày trong ba phần chính như sau:

1. Phần mở đầu

2. Phần nội dung: bao gồm ba chương

Chương 1: Tổng quan về chữ ký số

Chương 2: Hệ mật mã và chữ ký số RSA

Chương 3: Xây dựng chữ ký số tại công ty LDVC quốc tế Hải Vân

3. Phần kết luận

# CHƯƠNG 1: TỔNG QUAN VỀ CHỮ KÝ SỐ

## 1.1 Tổng quan về chữ ký số

Con người đã sử dụng các hợp đồng với chữ ký dưới dạng điện tử từ hơn 100 năm nay với việc sử dụng mã Morse và điện tín. Tuy nhiên, chỉ với những phát triển của khoa học kỹ thuật gần đây thì chữ ký số mới đi vào cuộc sống.

Trong đời sống hàng ngày, chữ ký (viết tay) trên một văn bản là một minh chứng về “bản quyền” hoặc ít nhất cũng là sự “tán đồng, thừa nhận” các nội dung trong văn bản. Chẳng hạn như trên việc ký vào phiếu nhận tiền từ ngân hàng, hợp đồng mua bán, chuyển nhượng, thừa kế, tố tụng.... Chữ ký viết tay được chính tay người ký nên không thể sao chụp được. Thông thường chữ ký viết tay trên văn bản thì được dùng để xác nhận người ký nó. Những yếu tố nào làm nên “sức thuyết phục của nó”, về mặt lý thuyết

Chữ ký là bằng chứng thể hiện người ký có chủ định khi ký văn bản - Chữ ký thể hiện “chủ quyền”, nó làm cho người nhận văn bản biết rằng ai đích thị là người đã ký văn bản.

- Chữ ký không thể “tái sử dụng”, tức là nó là một phần của văn bản mà không thể sao chép sang các văn bản khác - Văn bản đã ký không thể thay đổi được

- Chữ ký không thể giả mạo và cũng là thứ không thể chối bỏ ( người đã ký văn bản không thể phủ định việc mình đã ký văn bản và người khác không thể tạo ra chữ ký đó ).

Trong cuộc sống đời thường, việc tạo một mô hình “lý tưởng” như trên là không dễ vì việc ký trên văn bản giấy có thể giả mạo chữ ký, nhưng với khả năng kiểm định sát sao thì việc làm thay đổi không phải dễ. Tuy nhiên trong thế giới máy tính thì vấn đề ký như trong thực tế sẽ gặp phải nhiều khó khăn : các dòng thông tin trên máy tính có thể thay đổi dễ dàng, hình ảnh của chữ ký tay của một người cũng dễ dàng cho “sang – truyền” từ một văn bản này sang một văn bản khác, và việc thay đổi nội dung một văn bản điện tử (sau khi ký) cũng chẳng để lại dấu vết gì về phương diện “tẩy, xóa”...

Vậy để có những đặc tính như trên “ký trong thế giới điện tử ” cần có công nghệ mã hóa. Sơ đồ chữ ký số là phương pháp ký một thông báo được lưu dưới dạng điện tử. Giao thức cơ bản của chữ ký số dựa trên ý tưởng của Diffie và Hellman :

- Người gửi (chủ nhân của văn bản) ký văn bản bằng cách mã hóa nó với khóa bí mật của mình.

- Người gửi chuyển văn bản đã ký cho người nhận.

- Người nhận văn bản kiểm tra chữ ký bằng việc sử dụng chìa khóa công khai của người gửi để giải mã văn bản.

**Khái niệm chung về chữ ký số:** Chữ ký số là một tập con của chữ ký điện tử, một thể chứng thực được mã hóa bởi khóa bí mật của người gửi. Chữ ký số là thông tin đi kèm theo dữ liệu (văn bản, hình ảnh, video,...) nhằm mục đích xác định chủ thể của dữ liệu đó. Là mô hình sử dụng các kỹ thuật mật mã để gắn với mỗi người sử dụng một cặp khóa công khai - bí mật và qua đó có thể ký các văn bản điện tử cũng như trao đổi các thông tin mật. Khóa công khai thường được phân phối thông qua chứng thực khóa công khai

## 1.2 Thực trạng về chữ ký số hiện nay:

Trên thế giới, hầu như tất cả nước cũng đều đã ứng dụng chữ ký số, đặc biệt là trong các công việc hành chính Nhà nước. Biểu hiện rõ ràng nhất cho sự chấp nhận chữ ký số phổ biến chính là sự ra đời của các bộ luật.

Tại Trung quốc: Luật chữ ký điện tử của Trung quốc - Mục tiêu hướng tới thống nhất việc thực hiện, khẳng định tính pháp lý và bảo vệ quyền lợi hợp pháp của các bên liên quan tới việc thực hiện chữ ký điện tử.

Tại Brazil: Medida provisória 2.200-2 - Luật Brazil thừa nhận tính pháp lý của văn bản số nếu được chứng nhận bởi ICP-Brasil (PKI chính thức của Brazil) hoặc một PKI khác nếu các bên đồng ý.

### ***Một số lược đồ chữ ký số:***

- ✓ Lược đồ chữ ký RSA
- ✓ Lược đồ chữ ký ElGamal
- ✓ Lược đồ chữ ký DSS
- ✓ Lược đồ chữ ký Elliptic

## 1.3 Vai trò của chữ ký số trong ứng dụng hiện nay

Ngày nay với xu hướng hội nhập, toàn cầu hóa đã và đang ảnh hưởng đến sự phát triển của thế giới. Việc trao đổi thông tin từ đó cũng yêu cầu nhanh gọn, chính xác và an toàn hơn. Tuy nhiên việc trao đổi thông tin, chứng thực thông tin theo phong cách truyền thống làm

giảm tốc độ và sự chính xác của thông tin. Những công việc ấy còn mang tính chất thủ công nên gây ra sự chậm trễ và thiếu chính xác trong trao đổi thông tin.

Chính khó khăn này đã làm nảy sinh sự phát triển mạnh mẽ của công nghệ thông tin và công nghệ mã hóa. Hiện nay, ở các nước trên thế giới công nghệ thông tin đang đóng vai trò thiết yếu trong mọi lĩnh vực hoạt động của toàn xã hội và nhu cầu bảo mật thông tin ngày càng được đặt lên hàng đầu. Có thể nhắc đến việc mã hóa bảo mật thông tin số của các doanh nghiệp, dùng chữ ký số để xác thực email trao đổi thông tin, ngân hàng điện tử, kiểm soát truy cập vào các sàn thương mại điện tử và xử lý các đơn hàng, mua sắm trực tuyến... mà vai trò chủ yếu là chữ ký số.

Giải pháp chữ ký số là tối ưu vì nó có hiệu lực pháp lý, do đó không cần in ấn tài liệu mà vẫn có thể xác nhận được tài liệu, đảm bảo tính toàn vẹn và không chối bỏ. Chữ ký số được phát hành bởi bên thứ ba là cơ quan chứng thực có thẩm quyền cấp phát, thu hồi, quản lý chứng chỉ số cho các thực thể thực hiện các giao dịch an toàn (Certificate Authority hoặc CA) nên đảm bảo tính khách quan. Quá trình tạo chữ ký số, xác nhận các yêu cầu pháp lý, bao gồm xác thực chữ ký, xác thực tin nhắn là thanh công và hiệu quả.

Chữ ký số dùng cho các văn bản số, cho biết toàn bộ văn bản đã được ký bởi người ký. Và người khác có thể xác minh điều này. Chữ ký số tương tự như chữ ký thông thường, đảm bảo nội dung tài liệu là đáng tin cậy, chính xác, không hề thay đổi trên đường truyền và cho biết người tạo ra tài liệu là ai. Tuy nhiên, chữ ký số khác chữ ký thường, vì nó tùy thuộc vào văn bản. Chữ ký số sẽ thay đổi theo văn bản còn chữ ký thường thì không hề thay đổi.

Chữ ký số được sử dụng để cung cấp chứng thực chủ sở hữu, tính toàn vẹn dữ liệu và chống chối bỏ nguồn gốc trong rất nhiều các lĩnh vực.

Chữ ký số không chỉ được thực hiện cho các giao dịch điện tử trên mạng Internet mà còn được sử dụng cho các hệ thống mạng viễn thông di động. Giúp cho việc giao dịch được nhanh chóng, đơn giản hóa mua sắm trực tuyến, giúp người dùng truy cập mọi nơi mọi lúc.

Chữ ký số ra đời có lợi ích to lớn về chiến lược và kinh tế: đối với các doanh nghiệp, chữ ký số làm doanh nghiệp tiết kiệm được rất nhiều thời gian và chi phí hành chính; việc ký kết có thể diễn ra ở bất kỳ đâu, trong bất cứ thời gian nào; việc vận chuyển tài liệu giữa các bên diễn ra thuận lợi và nhanh chóng.

## CHƯƠNG 2: HỆ MẬT MÃ VÀ CHỮ KÝ SỐ RSA

### 1.1 Cơ sở mật mã trong toán học

Toán học mà cụ thể là số học luôn có quan hệ mật thiết với công nghệ thông tin nói chung và ngành an ninh máy tính nói riêng. Số học giúp bảo vệ những dữ liệu nhạy cảm có khả năng bị đánh cắp. Những giao thức mã hóa mà đặc biệt là chữ ký số điện tử đều dựa trên lý thuyết số học để xây dựng khóa, mã hóa và giải mã. An toàn của những giao thức này đều liên quan đến giải thuật công khai và phân tích thừa số nguyên tố.

### 1.2 Các hàm băm

Một hàm băm là một hàm tính toán hiệu quả thực hiện ánh xạ các chuỗi nhị phân với độ dài tùy ý vào các chuỗi nhị phân có độ dài cố định, được gọi là các giá trị băm (hash – values).

Hàm băm là các thuật toán không sử dụng khóa để mã hóa, nó có nhiệm vụ băm thông điệp được đưa vào theo một thuật toán h một chiều nào đó, rồi đưa ra một bản băm – văn bản đại diện – có kích thước cố định. Do đó người nhận không biết được nội dung hay độ dài ban đầu của thông điệp đã được băm bằng hàm băm.

#### Một số giải thuật trong hàm băm:

- ✓ **Giải thuật MD5:** Giải thuật được phát triển bởi Ron Rivest tại đại học MIT. Nó đưa vào các khối đầu vào 512 bit và sinh ra các giá trị băm 128 bit. MD5 được sử dụng rất rộng rãi trong các chương trình an ninh mạng và cũng thường được dùng để kiểm tra tính nguyên vẹn của tập tin. MD5 được thiết kế để thay thế cho hàm băm trước đó MD4.
- ✓ **Giải thuật SHA-1:** SHA-1 là thuật toán “băm” một chiều dùng trong rất nhiều hệ thống như SSH, SSL, S/MIME, PGP,.... Nó được Cơ quan an ninh quốc gia Mỹ phát minh năm 1995 và trở thành chuẩn bảo mật cơ sở phổ biến nhất trên Internet và là thuật toán chữ ký điện tử duy nhất được Cơ quan Chuẩn Chữ ký Số của chính phủ Mỹ phê chuẩn.

### 1.3 Cơ sở hạ tầng khóa công khai PKI

Khái niệm hạ tầng khóa công khai (PKI) thường được dùng để chỉ toàn bộ hệ thống bao gồm nhà cung cấp chứng thực số (CA) cùng các cơ chế liên quan đồng thời với toàn bộ việc sử dụng các thuật toán mật mã hóa khóa công khai trong trao đổi thông tin.

## **Ứng dụng của PKI trong ký số và bảo mật dữ liệu:**

- ✓ Mã hóa: Lợi ích đầu tiên của chứng thư số là tính bảo mật thông tin. Khi người gửi đã mã hóa thông tin bằng khóa công khai của bạn, chắc chắn chỉ có bạn mới giải mã được thông tin để đọc. Trong quá trình truyền thông tin qua Internet, dù có đọc được các gói tin đã mã hóa này, kẻ xấu cũng không thể biết được trong gói tin có thông tin gì.
- ✓ Chống giả mạo: Khi bạn gửi đi một thông tin, có thể là một dữ liệu hoặc một email, có sử dụng chứng thư số, người nhận sẽ kiểm tra được thông tin của bạn có bị thay đổi hay không. Bất kỳ một sự sửa đổi hay thay thế nội dung của thông điệp gốc đều sẽ bị phát hiện. Địa chỉ mail của bạn, tên domain... đều có thể bị kẻ xấu làm giả để đánh lừa người nhận để lây lan virus, ăn cắp thông tin quan trọng. Tuy nhiên, chứng thư số thì không thể làm giả, nên việc trao đổi thông tin có kèm chứng thư số luôn đảm bảo an toàn.
- ✓ Chữ ký điện tử: Những thông điệp có thể gửi đi qua Internet, đến những khách hàng, đồng nghiệp, nhà cung cấp và các đối tác. Tuy nhiên, tài liệu rất dễ bị tổn thương bởi các hacker. Những thông điệp có thể bị đọc hay bị giả mạo trước khi đến người nhận. Bằng việc sử dụng chứng thư số cá nhân, bạn sẽ ngăn ngừa được các nguy cơ này. Với chứng thư số cá nhân, bạn có thể tạo thêm một chữ ký điện tử vào tài liệu như một bằng chứng xác nhận của mình. Chữ ký điện tử cũng có các tính năng xác thực thông tin, toàn vẹn dữ liệu và chống chối cãi nguồn gốc.

### **1.4 Tổng quan chữ ký số RSA**

Thuật toán được Ron Rivest, Adi Shamir và Len Adleman mô tả lần đầu tiên vào năm 1977 tại Học viện Công nghệ Massachusetts (MIT). Tên của thuật toán được lấy từ 3 chữ cái đầu của tên 3 tác giả.

Trước đó, vào năm 1973, Clifford Cocks – một nhà toán học người Anh làm việc tại GCHQ, đã mô tả một thuật toán tương tự. Với khả năng tính toán tại thời điểm đó thì thuật toán này không khả thi và chưa bao giờ được thực nghiệm. Tuy nhiên, phát minh này chỉ được công bố vào năm 1977 vì được xếp vào loại tuyệt mật.

Thuật toán RSA được MIT đăng ký bằng sáng chế tại Hoa Kỳ vào năm 1983 (Số đăng ký 4.405.829). Bằng sáng chế này hết hạn vào ngày 21 tháng 9 năm 2000. Tuy nhiên, do thuật toán đã được công bố trước khi đăng ký bảo hộ nên sự bảo hộ hầu như không có giá trị bên



ngoài Hoa Kỳ. Ngoài ra, nếu như công trình của Clifford Cocks đã được công bố trước đó thì bằng sáng chế RSA đã không thể được đăng ký.

### **Hoạt động của hệ mật mã RSA**

Thuật toán RSA được phát minh năm 1978, sử dụng chế độ mã hóa khối. Có hai khóa, mỗi khóa là những số cố định sử dụng trong quá trình mã hóa và giải mã:

- Khóa công khai (Public key): được công bố rộng rãi cho mọi người và được dùng để mã hóa.

- Khóa bí mật (Private key): Những thông tin được mã hóa bằng khóa công khai chỉ có thể được giải mã bằng mã bí mật tương ứng.

Nói cách khác, mọi người đều có thể mã hóa nhưng chỉ có người biết khóa cá nhân (bí mật) mới có thể giải mã được.

**Kiến trúc hệ mật mã RSA:** Trong thuật toán RSA, có hai quá trình chính đó là tạo khóa và xác nhận khóa.

Tính toán chuỗi đại diện (message digest/ hash value) của thông điệp sử dụng một giải thuật băm (Hashing algorithm) SHA-1.

- Chuỗi đại diện được ký sử dụng khóa riêng (Private key) của người gửi và giải thuật tạo chữ ký (Signature/ Encryption algorithm) RSA. Kết quả chữ ký số (Digital signature) của thông điệp hay còn gọi là chuỗi đại diện được mã hóa bởi giải thuật RSA (Encrypted message digest).

- Thông điệp ban đầu (message) được ghép với chữ ký số (Digital signature) tạo thành thông điệp đã được ký (Signed message).

- Thông điệp đã được ký (Signed message) được gửi cho người nhận.

### **Bảo mật RSA:**

Độ an toàn của hệ thống RSA dựa trên vấn đề của toán học: bài toán phân tích ra thừa số nguyên tố các số nguyên lớn. Nếu bài toán trên là khó (không tìm được thuật toán hiệu quả để giải chúng) thì không thể thực hiện được việc phá mã toàn bộ đối với RSA. Phá mã một phần phải được ngăn chặn bằng các phương pháp chuyển đổi bản rõ an toàn.

Bài toán RSA là bài toán tính căn bậc e môđun n (với n là hợp số): tìm số m sao cho  $c = m^e \bmod n$ , trong đó (e, n) chính là khóa công khai và c là bản mã. Hiện nay phương pháp triển vọng nhất giải bài toán này là phân tích n ra thừa số nguyên tố. Khi thực hiện được điều này, kẻ tấn công sẽ tìm ra số mũ bí mật d từ khóa công khai và có thể giải mã theo đúng quy trình

của thuật toán. Nếu kẻ tấn công tìm được 2 số nguyên tố  $p$  và  $q$  sao cho:  $n = pq$  thì có thể dễ dàng tìm được giá trị  $(p - 1)(q - 1)$  và qua đó xác định  $d$  từ  $e$ . Chưa có một phương pháp nào được tìm ra trên máy tính để giải bài toán này trong thời gian đa thức (polynomial - time). Tuy nhiên người ta cũng chưa chứng minh được sự không tồn tại của thuật toán. Chúng ta có thể tham chiếu bảng sau để thấy số thao tác và thời gian thực hiện phân tích số  $n$  thành số nguyên tố theo phương pháp General Number Field Sieve (GNFS):

$$O\left(\exp\left(\left(\frac{64}{9}\log n\right)^{\frac{1}{3}}(\log\log n)^{\frac{2}{3}}\right)\right)$$

Số bit của $n$	Số thao tác	Thời gian
100	$9,6 \times 10^8$	16 phút
200	$3,3 \times 10^{12}$	38 ngày
300	$1,3 \times 10^{15}$	41 năm
400	$1,7 \times 10^{17}$	5313 năm
500	$1,1 \times 10^{19}$	$3,5 \times 10^5$ năm
1024	$1,3 \times 10^{26}$	$4,2 \times 10^{12}$ năm
2048	$1,5 \times 10^{35}$	$4,9 \times 10^{21}$ năm

**Bảng 2.12: Thử nghiệm độ bảo mật của RSA**

## **CHƯƠNG 3: XÂY DỰNG CHỮ KÝ SỐ TẠI CÔNG TY LDVC QUỐC TẾ HẢI VÂN**

### **1.1 Giới thiệu bài toán**

Công ty LDVC QT HẢI VÂN là một doanh nghiệp hoạt động trong lĩnh vực vận chuyển nên có đặc thù là có rất nhiều chi nhánh hoạt động rộng khắp trên các địa bàn. Trụ sở chính của công ty đặt tại Lô C8, khu đô thị Nam Trung Yên, Cầu Giấy, Hà Nội. Tại các chi nhánh của công ty thường xuyên có các hoạt động giao dịch thu/chi tài chính.

### **1.2 Hiện trạng in biên lai/hóa đơn thu phí**

Hiện nay tại CÔNG TY LDVC QT HẢI VÂN, việc in biên lai thu tiền phí được in theo quy trình sau:

- Dữ liệu phí các đơn hàng được tổng hợp hàng ngày theo từng mã hàng trên cơ sở dữ liệu.
- Tạo file excel biên lai có cấu trúc theo từng đơn hàng.
- Lưu lại dữ liệu trong máy.
- Sau khi in, kế toán và trưởng bộ phận hàng mỗi người giữ một bản.
- Với mô hình quản lý của công ty là mô hình quản lý tập trung thì trao đổi dữ liệu tài chính cũng như các hóa đơn chứng từ giữa trụ sở chính và các chi nhánh là rất nhiều.

### **1.3 Một số nguy cơ có thể mắc phải**

- Ngoài ra những đơn hàng vận chuyển quốc tế, bên đối tác yêu cầu công ty chưa xuất được một cách nhanh chóng và chính xác.
- Vào những ngày đơn hàng xuất ra nhiều, kế toán tháng liên quan đến chi phí nhiên liệu rất nhiều gây ra những sai sót.
- Nhầm tên mặt hàng, loại tiền của đơn hàng.
- Những nhân viên tiếp nhận đơn hàng phải cầm rất nhiều hóa đơn trong một ngày.

Những sai sót này thường chỉ được phát hiện khi biên lai đã đến tay của trưởng bộ phận. Điều này sẽ làm tốn rất nhiều chi phí in ấn, giấy mực.

Lộ thông tin khi trao đổi file.

### **1.4 Yêu cầu bài toán**

Bài toán đặt ra ở đây là làm thế nào để trao đổi các file dữ liệu giữa trụ sở chính và các chi nhánh đảm bảo an toàn, chính xác. Cụ thể như sau:

Trong quá trình trao đổi file, người dùng phải đối mặt với 2 nguy cơ thường trực:

*Nguồn gốc không rõ ràng:* Khi nhận được một file, người dùng khó có thể chắc chắn rằng dữ liệu đó được cung cấp bởi chính xác một người đáng tin tưởng nào đó và trong quá trình trao đổi dữ liệu không bị thay đổi.

*Để lộ các thông tin nhạy cảm:* Khi trao đổi dữ liệu, đặc biệt là các thông tin nhạy cảm, người dùng luôn có một nhu cầu về tính bảo mật cho dữ liệu. Họ luôn muốn chắc chắn rằng chỉ có một số người mà họ mong muốn mới đọc được các thông tin nhạy cảm đó.

Sau khi đã đảm bảo giải quyết được 2 vấn đề trên, cũng nên có một phương pháp để các người dùng trao đổi file với nhau

Nội dung của hướng thiết kế giải pháp yêu cầu:

*Yêu cầu về nguồn gốc dữ liệu:* Mỗi người dùng sẽ được cấp một cặp public-private key. Phần mềm sẽ hỗ trợ chức năng ký bên phía người gửi và xác minh chữ ký trên file ở phía người nhận để đảm bảo nguồn gốc, tính toàn vẹn của dữ liệu.

*Yêu cầu thông tin nhạy cảm:* Phần mềm sẽ hỗ trợ chức năng mã hóa file sử dụng giải thuật RSA và xây dựng phương pháp thống nhất khóa giữa người gửi và nhận, phần mềm hỗ trợ việc tạo key ECDH để làm key đối xứng giữa 2 người.

*Yêu cầu về việc trao đổi file:* Phần mềm sẽ hỗ trợ việc tương tác gửi file qua email. Người dùng có thể đính kèm file trong các email để thực hiện quá trình trao đổi file.

## **1.5 Một số yêu cầu về phần cứng và phần mềm**

**Về phần cứng yêu cầu đề xuất:**

- CPU: Intel ®, Core™ i3- 3110 M
- RAM: 2GB
- HDD: 500 GB
- OS: windows 7
- Máy cài đặt Microsoft .NET Framework 4 Maintenance, dung lượng đĩa cứng còn trống ít nhất 20MB

**Về phần mềm cài đặt:**

Chương trình được xây dựng trên môi trường Visual C# trong bộ ứng dụng Microsoft Visual Studio 2010.

Đọc thông tin của USB TOKEN, lưu vào biến nhớ.

Đọc file Text có cấu trúc (mỗi dòng là một mã thanh toán), chuyển thành đối tượng thanh toán, đưa đối tượng vào hàng đợi.

Gọi các tiến trình (luồng) in đồng thời. Các tiến trình này vào hàng đợi lấy dữ liệu thanh toán.

Thực hiện ký hóa đơn.

Ghi dữ liệu hóa đơn ra đĩa cứng.

## 1.6 Mô tả quy trình sử dụng phần mềm

### **Đăng nhập**

Trước khi sử dụng phần mềm nhân viên phải đăng nhập với tài khoản:

- User: Admin
- Password: admin

### **+ Quy trình ký và in biên lai**

Sau khi đăng nhập vào phần mềm, ta sẽ có các chức năng sau:

### **+ Hệ thống**

Phần này bao gồm:

- Danh sách thu ngân: danh sách của tất cả các nhân viên trong phòng kế hoạch tài chính phụ trách việc thu tiền, in và ký biên lai cho nhân viên.
- Danh sách biên lai: danh sách nhân viên phải nộp tiền hàng ngày theo quy định.

### **+ Tạo biên lai**

Khi nhân viên đến nộp tiền, nhân viên phụ trách sẽ yêu cầu thẻ nhân viên và nhập mã nhân viên đó vào và xuất biên lai ra file docx rồi lưu lại.

### **+ Tạo khóa**

Nhân viên phụ trách sẽ phải tạo khóa khi được yêu cầu để tạo ra khóa công khai và khóa bí mật phục vụ cho việc phát sinh chữ ký và ký biên lai sau này.

Tạo khóa sẽ có hai chế độ

- Tùy chọn: Nhân viên tự mình nhập vào hai số nguyên tố P và Q rồi sau đó hệ thống sẽ tiến hành sinh khóa, sau đó nhân viên đó sẽ lưu lại khóa của mình.
- Tự động: Hệ thống sẽ tự động chọn hai số P và Q ngẫu nhiên rồi sinh khóa, nhân viên chỉ việc lưu lại khóa của mình vừa được tạo ra.

### **+ Chữ ký số**

Trong phần này sẽ có 2 chức năng:

### **Ký biên lai**

Nhân viên sẽ sử dụng khóa mà mình vừa tạo ra để ký lên file biên lai mà ta vừa tạo ra.

Để ký được biên lai cần có khóa và nhân viên sẽ phải nhập tên của mình vào biên lai rồi sau đó tiến hành ký chữ ký số.

### **Xác nhận chữ ký và in biên lai**

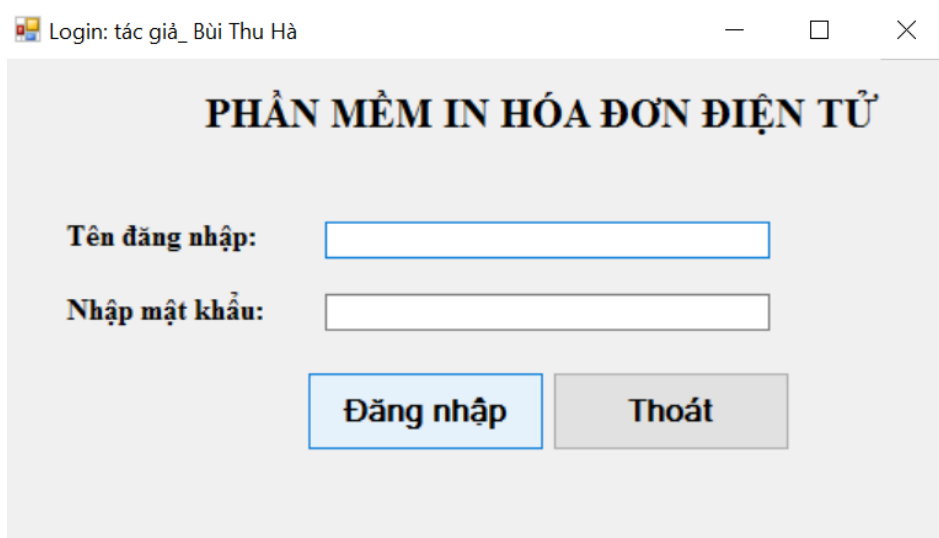
Sau khi ký, nhân viên phải xác nhận lại xem file vừa ký có đúng chữ ký của mình không.

- Nếu xác nhận chữ ký đúng, nhân viên phụ trách sẽ in biên lai đó. Biên lai được in ra sẽ có tên của người ký và mỗi biên lai sẽ đi kèm với mã số biên lai (là khóa công cộng hoặc khóa bí mật của nhân viên đó).
- Nếu xác nhận chữ ký không đúng thì sẽ tiến hành ký lại file biên lai đó.

## **1.7 Thực nghiệm chương trình chữ ký số**

Trước khi sử dụng phần mềm nhân viên phải đăng nhập vào với tài khoản:

- User: Admin
- Password: admin



**Hình 3.8: Giao diện đăng nhập**

Sau khi đăng nhập vào chúng ta có giao diện chính của phần mềm gồm 5 chức năng cơ bản:

- Hệ thống: cho phép người quản trị có thể có chức năng cấu hình phần mềm hoặc có thể thêm xóa một user người dùng.
- Tạo biên lai: tạo ra các biên lai hoặc hóa đơn điện tử
- Tạo khóa: dùng để tạo các khóa công khai và khóa bí mật
- Chữ ký số: dùng để tạo chữ ký, ký lên file và xác nhận lại chữ ký xem có đúng của người gửi hay không

- Trợ giúp: giúp cho người sử dụng dễ dàng thao tác và hiểu về nghiệp vụ quy trình của chương trình



**Hình 3.9: Giao chính của phần mềm chữ ký số**

*Phần tạo khóa:* nhân viên chưa có khóa sẽ sử dụng giao diện này để tạo khóa công khai và khóa bí mật cho chính mình.

Có hai chế độ: Tùy chọn và Tự động

**Hình 3.10. Giao diện tạo khóa**

Sau khi tạo khóa, ta đến với phần Chữ ký số gồm hai chức năng: Ký biên lai, xác nhận chữ ký và in biên lai.

Dưới đây là giao diện cho việc ký biên lai ta vừa xuất:

**KÝ BIÊN LAI**

File biên lai  Chọn

Khóa  Chọn

Người ký

☒ Ký không mã hóa ☐ Ký - Mã hóa ☐ Mã hóa - Ký

Ký biên lai

**Hình 3.11. Giao diện ký biên lai**

Sau khi ký biên lai ta sẽ xác nhận lại chữ ký rồi sau đó in biên lai cho nhân viên

**IN BIÊN LAI**

File biên lai  Chọn

Khóa  Chọn

Chữ ký

Kiểm tra chữ ký In biên lai

**Hình 3.12 . Giao diện Xác nhận chữ ký và in biên lai**



Biên lai sau khi in sẽ có tên của người ký và mã số biên lai

**Đơn vị : Công Ty LDVC Quốc Tế Hải Vân**

**Địa chỉ : Lô C2- Khu đô thị Nam Trung Yên- Cầu Giấy- Hà Nội**

**Mã đơn vị :**

**BIÊN LAI THU TIỀN**

**Mã số biên lai : 279**

*Ngày...tháng 4 năm 2016*

Tên người nộp : **Nguyễn Văn Nam** Mã số : **K12**

Phòng : **Kho**

Nội dung thu : **Tiền hàng xe 30LD-022.39**

Số tiền : **2.000.000**

Viết bằng chữ : **Hai triệu đồng chẵn**

*Hà Nội, ngày... tháng.... năm ...*

**Người nộp tiền**

(Ký, họ tên)

**Người thu tiền**

(Ký, họ tên)

**Hình 3.13: Biên lai sau khi ký và in**

## KẾT LUẬN

### 1. Kết quả đạt được

- ✓ Nắm được các kiến thức về chữ ký số(các giải thuật, cơ chế xác thực....) và việc ứng dụng chữ ký số trong các lĩnh vực khác nhau.
- ✓ Nghiên cứu tìm hiểu về chữ ký số bằng thuật toán RSA và giải pháp ứng dụng hóa đơn điện tử tại Công ty Liên doanh vận chuyển quốc tế hải vân.
- ✓ Xây dựng được chương trình ứng dụng “Chữ ký số trong việc in ấn hóa đơn điện tử tại Công ty LDVC quốc tế Hải Vân” để thực hiện các quá trình: Tạo khóa bí mật và khóa công khai, tạo chữ ký RSA, ký biên lai và xác thực được chữ ký, in biên lai.

### 2. Hướng phát triển

- ✓ 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 tương tự. 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 đề án tuy còn có những hạn chế, nhưng đã giúp em 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.

## DANH MỤC CÁC TÀI LIỆU THAM KHẢO

### Tiếng Việt

- [1]. Phan Đình Diệu (1999), Giáo trình lý thuyết mật mã và an toàn thông tin, Nhà xuất bản Đại học Quốc Gia Hà nội
- [2]. Phạm Huy Điền, Hà Huy Khoái (2004), Mã hóa thông tin cơ sở toán học và ứng dụng, Viện toán học.
- [3]. Thái Hồng Nhị, Phạm Minh Việt (2004), An toàn thông tin - mạng máy tính, truyền tin số và truyền số liệu, Nhà xuất bản khoa học và kỹ thuật.

### Tiếng Anh

- [4]. Blahut Richard, Cryptography and Secure Communication: Cambridge University Press, 2014.
- [5]. Burt Kaliski, RSA Laboratories, The Mathematics of the RSA Public-Key Cryptosystem.
- [6]. Douglas Stinson, Cryptography: Theory and Practice: CRC Press, 2007.
- [7]. Kenneth H. Rosen (1993), Elementary number theory and its applications – Third Edition.
- [8]. Khary Alexander, Ramesh Karri, Igor Minkin, Kaijie Wu, Piyush Mishra, Xuan Li., Towards 10-100 Gbps Cryptographic Architectures., IBM Corporation, Poughkeepsie, NY, 12601.
- [9]. Klaus Schmeih, Cryptography and Public Key Infrastructure on the Internet: Wiley and Sons Publishing, 2001.
- [10]. R. Rivest, A. Shamir, L. Adleman, Method for Obtaining Digital Signatures and Public-key Cryptosystems. Communications of the ACM, Vol.21 (2), pp.120-126. 1978. Previously released as an MIT “Technical Memo” in April 1977. Initial publication of the RSA scheme.
- [11]. S. Y. K. Bosworth, Michel E. Kabay, and Eric Whyne, Computer Security Handbook, , 6th Edition: Wiley and Sons, 2014.
- [12]. William Stallings, Cryptography and Network Security, 6th Edition: Pearson Ed. Inc., 2014.