LỜI CẢM ƠN

Trong lời đầu tiên của báo cáo đồ án tốt nghiệp "Tìm hiểu về hành chính điện tử và an toàn bảo mật thông tin cho hệ thống" này, em muốn gửi những lời cám ơn và biết ơn chân thành nhất của mình tới tất cả những người đã hỗ trợ, giúp đỡ em về kiến thức và tinh thần trong quá trình thực hiện đồ án.

Trước hết, em xin chân thành cám ơn Thầy Giáo - Ts. Hồ Văn Canh, người đã trực tiếp hướng dẫn, nhận xét, giúp đỡ em trong suốt quá trình thực hiện đồ án. Xin chân thành cảm ơn các thầy cô trong Khoa Công Nghệ Thông Tin và các phòng ban nhà trường đã tạo điều kiện tốt nhất cho em cũng như các bạn khác trong suốt thời gian học tập và làm tốt nghiệp.

Cuối cùng em xin gửi lời cảm ơn đến gia đình, bạn bè, người thân đã giúp đỡ động viên em rất nhiều trong quá trình học tập và làm Đồ án Tốt Nghiệp. Do thời gian thực hiện có hạn, kiến thức còn nhiều hạn chế nên Đồ án thực hiện chắc chắn không tránh khỏi những thiếu sót nhất định. Em rất mong nhận được ý kiến đóng góp của thầy cô giáo và các bạn để em có thêm kinh nghiệm và tiếp tục hoàn thiện đồ án của mình.

Em xin chân thành cảm ơn!

Hải Phòng, ngày 30 tháng 06 năm 2014

Sinh viên

Đặng Văn An

MỤC LỤC

MỞ ĐẦU

Ngày nay, công nghệ thông tin ở nước ta đang phát triển với tốc độ cao. Số lượng người sử dụng tăng nhanh, lưu lượng truyền tải thông tin yêu cầu ngày càng lớn, mạng máy tính mở rộng khắp lãnh thổ và theo đó là sự xuất hiện của một số hoạt động giao dịch trên mạng inter-net, đặc biệt là hoạt động giao dịch điện tử nói chung hay trong giao dịch hành chính điện tử nói riêng.

Trước đây, các cơ quan hành chính của nhà nước cung cấp dịch vụ công cho nhân dân tại trụ sở của mình thì nay nhờ vào việc ứng dụng công nghệ thông tin như WAN, Internet và các phương tiện di động để làm việc với nhân dân, giới doanh nghiệp.

Ngày 10/4/2007, Nhà nước ban hành Nghị định 64/2007/NĐ-CP quy định về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước bao gồm các Bộ, cơ quan ngang Bộ, cơ quan thuộc chính phủ, Ủy ban nhân dân các cấp và các đơn vị sự nghiệp sử dụng ngân sách nhà nước. Theo đó nhiều dịch vụ hành chính sẽ được thực hiện qua mạng. Tuy nghị đinh này giúp rút ngắn thời gian cũng như công sức nhưng lại phát sinh vấn đề đảm bảo an toàn bảo mật dữ liệu lưu trữ trong kho và truyền trên đường truyền không bị trộm cắp, sửa đổi, giả mạo.

Các hoạt động giao dịch điện tử rất nhiều, đa dạng và phức tạp. Có nhiều bài toán đặt ra như quản lý và xử lý được các tài liệu, chữ ký và kiểm tra chữ kí nhanh, tin cậy, chi phí thấp để bảo vệ các tài liệu, chữ ký, chuyển giao các tài liệu hành chính an toàn. Do đó bảo vệ an toàn thông tin là yêu cầu tất yếu.

Hiện nay, công tác hành chính của nước ta cần phải có hệ thống thông tin mạnh để lưu trữ khối lượng lớn các tài liệu. Giúp cán bộ công chức và người dân có thể tìm kiếm thông tin một cách nhanh chóng, chính xác và xử lí được các nghiệp vụ hành chính phức tạp. Hệ thống cần phải có các công cụ để đảm bảo an toàn cho dữ liệu, chống thay đổi, giả mạo, trộm cắp góp phần giảm thiểu tiêu cực trong giao dịch hành chính điện tử.

Từ đó,ta thấy rằng giải pháp đảm bảo an toàn thông tin trong hành chính điện tử có hai công việc chính là: Bảo vệ dữ liệu trong kho lưu trữ và bảo vệ dữ liệu trên đường truyền. Để làm tốt được hai công việc trên, ta phải xây dựng được kiến trúc cơ sở hạ tầng trong hành chính điện tử hoàn thiện. Ứng dụng các công nghệ tiên tiến hiện nay hỗ trợ triển khai mô hình hành chính điện tử đã xây dựng, đưa ra các giải pháp, phần mềm, công cụ để bảo vệ an toàn và bảo mật thông tin.Bên cạnh các giải pháp công nghệ, không ngừng nghiên cứu, phát triển và hoàn thiện lý thuyết độ phức tạp tính toán, lý thuyết mật mã và an toàn thông tin. Chính vì vậy, nội dung chính của đồ án này là: Tìm hiểu về hành chính điện tử và An toàn bảo mật thông tin cho Hệ thống.

Đồ ángồm 4 chương:

Chương 1: Tổng quan về hành chính điện tử; Khái quát về hệ thống hành chính nhà nước Việt Nam, giới thiệu chung về hành chính điện tử, các mức giao dịch trực tuyến trong hành chính điện tử.

Chương 2: Tổng quan về an toàn thông tin: trình bày cơ sở hạ tầng và giao dịch trực tuyến, một số giao thức đảm bảo an toàn khi truyền tin.

Chương 3: Một số phương pháp bảo vệ thông tin trong hành chínhđiện tử: Trình bày về bài toán đảm bảo an toàn thông tin trong giao dịch hành chính điện tử và các bài toán nghiên cứu cơ sở hạ tầng công nghệ thông tin truyền thông trong giao dịch hành chính điện tử.

Chương 4: Thử nghiệm chương trình: Mã hóa dữ liệu.

CHƯƠNG 1: TỔNG QUAN VỀ HÀNH CHÍNH ĐIỆN TỬ

1.1. KHÁI QUÁT VỀ HỆ THỐNG HÀNH CHÍNH NHÀ NƯỚC VIỆT NAM

Tổ chức Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam bao gồm 4 cấp là trung ương(TW), tỉnh(thành phố), huyện(quận), xã(phường).

Ở cấp TW có Quốc hội, Chủ tịch nước, Chính phủ, Tòa án nhân dân tối cao, Viện kiểm sát nhân dân tối cao.

Quốc hội là cơ quan đại biểu cao nhất của nhân dân, cơ quan quyền lực nhà nước cao nhất của nước ta, do dân trực tiếp bầu ra với nhiệm kì 5 năm.

Các đại biểu Quốc hội bầu ra Chủ tịch nước, Thủ tướng chính phủ, Chánh án Tòa án nhân dân tối cao, Viện trưởng Viện kiểm sát nhân dân tối cao.

Chính quyền địa phương các cấp có Hội đồng nhân dân do nhân dân trực tiếp bầu ra với nhiệm kì 5 năm. Hội đồng nhân dân bầu ra Ủy ban nhân dân là cơ quan hành chính nhà nước ở địa phương.

Chính quyền và Ủy ban nhân dân các cấp hợp thành hệ thống cơ quan hành chính nhà nước ở Việt Nam, là cơ quan chấp hành của Quốc hội, cơ quan hành chính Nhà nước cao nhất của nước ta.

1.1.1. Chính phủ

Chính phủ thống nhất quản lý việc thực hiện các nhiệm vụ chính trị, kinh tế, văn hóa, xã hội, quốc phòng, an ninh và đối ngoại. Đảm bảo hiệu lực của bộ máy Nhà nước từ TW đến địa phương, việc tôn trọng và chấp hành Hiến pháp, phát huy quyền làm chủ của nhân dân trong sự nghiệp xây dựng và bảo vệ Tổ quốc. Thông qua đó ổn định và nâng cao chất lượng cuộc sống của nhân dân.

Chính phủ chịu trách nhiệm trước Quốc hội và báo cáo các công tác với Quốc hội, Ủy ban thường vụ Quốc hội, Chủ tịch nước.

1.1.2. Cơ quan thuộc chính phủ

Các cơ quan thuộc Chính phủ Chính phủ thành lập, bao gồm: Cơ quan thuộc Chính phủ thực hiện một số nhiệm vụ có đặc điểm, tính chất quan trọng mà Chính quyền phải trực tiếp chỉ đạo như các dịch vụ công thuộc ngành, lĩnh vực,quyền hạn về đại diện chủ sở hữu phần vốn của nhà nước tại doanh nghiệp có vốn đầu tư của nhà nước theo quy định của pháp luật. (Nghị định 30/2003/NĐ-CP ngày 1/4/2003 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của cơ quan thuộc Chính phủ).

Thủ trưởng các cơ quan thuộc Chính phủ là người đứng đầu và lãnh đạo một cơ quan thuộc Chính phủ, chịu trách nhiệm trước Thủ tướng Chính phủ, Chính phủ về việc thực hiện chức năng, nhiệm vụ, quyền hạn của mình. Mọi văn bản quy phạm pháp luật để thực hiện quản lý Nhà nước do Thủ tướng Chính phủ quyết định.

1.1.3. Các bộ, cơ quan ngang bộ

Lãnh đạo của các bộ, cơ quan ngang bộ và các cơ quan thuộc Chính phủ, Ủy ban nhân dân các cấp, xây dựng và kiện toàn hệ thống bộ máy hành chính nhà nước thống nhất từ TW đến địa phương; hướng dẫn, kiểm tra Hội đồng nhân dân thực hiện các văn bản của các cơ quan Nhà nước cấp trên. Tạo điều kiện để Hội đồng nhân dân thực hiện nhiệm vụ và quyền hạn theo luật định.

Thống nhất quản lý việc xây dựng, phát triển nền kinh tế quốc dân, văn hóa, giáo dục, y tế, khoa học và công nghệ; quản lý và đảm bảo sử dụng có hiệu quả tài sản thuộc sở hữu toàn dân.

Bảo đảm việc thi hành Hiến pháp và pháp luật trong các cơ quan nhà nước, tổ chức chính trị - xã hội, tổ chức kinh tế, đơn vị vũ trang nhân dân và công dân. Tổ chức và lãnh đạo các công tác tuyên truyền, giáo dục Hiến pháp và pháp luật trong nhân dân.

Thi hành những biện pháp bảo vệ quyền lợi và lợi ích hợp pháp của công dân, tạo điều kiện cho công dân sử dụng quyền và thực hiện nghĩa vụ của mình.

Củng cố và tăng cường nền quốc phòng toàn dân, an ninh nhân dân, bảo đảm an ninh quốc gia, trật tự - an toàn xã hội. Xây dựng các lực lương vũ trang nhân dân, thi hành lệnh động viên, lệnh ban bố tình trạng khẩn cấp và các biện pháp kiến thiết khác để bảo vệ đất nước.

Tổ chức và lãnh đạo công tác kiểm kê, thống kê cuả Nhà nước; các công tác thanh tra và kiểm tra nhà nước, chống tham nhũng, lãng phí và biểu hiện quan liêu, của quyền trong bộ máy nhà nước, giải quyết khiếu nại, tố cáo của công dân.

Thực hiện chính sách xã hội, chính sách dân tộc, chính sách tôn giáo. Thống nhất, quản lý công tác thi đua khen thưởng.

Quyết định việc điều chỉnh địa chính cấp dưới tỉnh, thành phố trược thuộc TW.

Phối hợp với Ủy ban TW Mặt trận Tổ quốc Việt Nam, Ban chấp hành Tổng liên đoàn lao động Việt Nam, Ban chấp hành TW của đoàn thể nhân dân trong khi thực hiện nhiệm vụ của mình; tạo điều kiện cho các tổ chức đó hoạt động có hiểu quả.

1.1.4. Ủy ban nhân dân các cấp

Là cơ quan hành chính nhà nước ở địa phương,do hội đồng nhân dân bầu ra. Ủy ban nhân dân là cơ quan chấp hành của hội đồng nhân dân, chịu trách nhiệm trước hội đồng nhân dân cùng cấp và các cơ quan nhà nước cấp trên.

Ủy ban nhân dân thực hiện chức năng quản lý nhà nước ở địa phương. Chịu trách nhiệm chấp hành Hiến pháp, luật, các văn bản của cơ quan nhà nước cấp trên và nghị quyết của hội đồng nhân dân cùng cấp. Góp phần bảo đảm sự chỉ đạo, quản lý, thống nhất trong bộ máy nhà nước từ TW đến địa phương. Bảo đảm thực hiện

chủ trương, biện pháp phát triển kinh tế - xã hội, củng cố quốc phòng, an ninh và thực hiện các chính sách khác trên địa bàn.

Các cơ quan chuyên môn thuộc Ủy ban nhân dân là cơ quan tham mưu, giúp Ủy ban nhân dân cùng cấp thực hiện chức năng quản lý nhà nước ở địa phương và thực hiện một số nhiệm vụ, quyền hạn theo sự ủy quyền của ủy ban nhân dân cùng cấp và theo quy định của pháp luật.

1.2. GIỚI THIỆU CHUNG VỀ HÀNH CHÍNH ĐIỆN TỬ

1.2.1. Công tác hành chính

1.2.1.1. Nhiệm vụ chính của cơ quan nhà nước

Mỗi tổ chức hay cơ quan có các nhiệm vụ, kế hoạch chính là:

- Nhiệm vụ trọng tâm của cơ quan: là nhiệm vụ số một của cơ quan.
- Nhiệm vụ đối nội, đối ngoại, hợp tác, phát triển: là những nhiệm vụ chính góp phần thực hiện nhiệm vụ trọng tâm.

1.2.1.2. Công tác hành chính

Bao gồm các công việc thường xuyên hàng ngày, để tiến hành thực hiện các nhiệm vụ theo đúng kế hoạch.

1.1.2.3. Nhiệm vụ giao dịch hành chính

Giao dịch hành chính bao gồm các công việc như sau: Soạn thảo công văn, xin chữ kí cấp trên, nhận công văn đến cơ quan, chuyển công văn đi tới cơ quan khác; Tổng hợp thông tin, phân loại tài liệu đi đến,…

Giao dịch hành chính thông thường như trước là bằng phương pháp thủ công. Ngày nay giao dịch hành hành chính bằng phương pháp điện tử, hay gọi là giao dịch trực tuyến.

1.2.2. Giao dịch hành chính trực tuyến

1.2.2.1 Giao dịch hành chính thông thường

Là những giao dịch giữa hai hay nhiều đối tác, họ trực tiếp gặp nhau tại một địa điểm và trao đổi thỏa thuận với nhau về một vấn đề nào đó.

Giao dịch hành chính bao gồm các công việc cụ thể: Soạn thảo công văn, xin chữ kí cấp trên, nhận công văn đến cơ quan, chuyển công văn đi tới cơ quan khác; Tổng hợp thông tin, phân loại tài liệu đi đến,…

Với giao dịch hành chính thông thường, các công văn hay tài liệu đều ghi trên giấy, chúng được chuyển qua các cơ quan(cá nhân) bằng đường bưu điện hay bộ phận văn thư.

1.2.2.2. Giao dịch hành chính trực tuyến

Giao dịch điện tử(Electronic Transaction): là hình thái hoạt động giao dịch bằng phương pháp điện tử. Tức là trao đổi thông tin thông qua các phương tiện công nghệ điện tử, thông tin giao dịch không cần in ra giấy.

Giao dịch hành chính trực tuyến: Các công văn hay tài liệu đều là dạng "số", chúng được chuyển qua các cơ quan(cá nhân) trên mạng máy tính.

1.2.3 Khái niệm về hành chính điện tử

Hành chính điện tử(HCĐT) là việc các cơ quan trong Chính quyền thực hiện giao dịch hành chính trực tuyến một cách có hệ thống công nghệ thông tin và viễn thông để thực hiện các giao dịch với công dân, doanh nghiệp và cámc tổ chức xã hội. Nhờ đó, giao dịch của các cơ quan Chính quyền với doanh nghiệp và các tổ chức sẽ được cải thiện, nâng cao chất lượng. Lợi ích thu được sẽ là giảm thiểu tham nhũng, tăng tính công khai, sự tiện lợi, giảm chi phí.

Giao dịch hành chính điện tử sử dụng hạ tầng công nghệ thông tin, mạng máy tính 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.

Giao dịch hành chính điện tử kết nối các cơ quan của Chính quyền trong các hoạt động cung cấp, chia sẻ thông tin, cung cấp các dịch vụ công chất lượng tốt nhất, phương thức mới nhất trên môi trường điện tử. Thay đổi mối quan hệ với công dân từ "xin - cho" thành "yêu cầu dịch vụ - cung ứng dịch vụ". Việc cung ứng các dịch vụ bằng công nghệ mới giúp mọi người có sự lựa chọn tối ưu cho các vấn đề của cá nhân trong cuộc sống. Các cơ quan hành chính trở 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.

Các giao dịch hành chính tập trung vào 4 nhóm đối tượng khách hàng chính là: Người dân, doanh nghiệp, công chức Chính phủ, cơ quan Chính phủ.

Mục đích của hành chính điện tử là làm cho các mối quan hệ qua lại giữa Chính quyền với người dân, doanh nghiệp, nhân viên Chính quyền và các cơ quan Chính quyền trở nên thuận tiện. thân thiện, minh bạch, đỡ tốn kém và hiệu quả hơn.

1.2.4. Các giao dịch hành chính điện tử trong cơ quan nhà nước

1.2.4.1. Các dịch vụ công

Là hình thức giao dịch khác ngoài các hình thức giao dịch hiện nay(face to face), thông qua mạng inter-net, các ki-ốt hoặc điện thoại di động.Tạo thuận lợi cho khách hàng có thể sử dụng các dịch vụ của Chính quyền mọi lúc, mọi nơi,

- **Các đặc điểm của dịch vụ công**

Theo Điều 9 nghị định 86/2002/NĐ-CP quy định chức năng, nhiệm vụ, tổ chức bộ máy của bộ, cơ quan ngang bộ về quản lý nhà nước các tổ chức thực hiện dịch vụ công thuộc lĩnh vực ngành cơ bản có những đặc điểm sau:

- Là một loại dịch vụ do Nhà nước trực tiếp thực hiện hoặc ủy quyền cho các tổ chức ngoài Nhà nước thực hiện dưới sự giám sát của Nhà nước.
- Nhằm đáp ứng các nhu cầu của xã hội.
- Nhà nước là người chịu trách nhiệm đến cùng trước nhân dân, xã hội về chất lượng dịch vụ cũng như số lượng dịch vụ.

- Không nhằm mục tiêu lợi nhuận.
- Đối tượng thụ hưởng Dịch vụ công không trực tiếp trả tiền.

⇨ Dịch vụ công là dịch vụ do Nhà nước chịu trách nhiệm. phục vụ các nhu cầu cơ bản, thiết yếu chung của người dân và cộng đồng, bảo đảm ổn định và công bằng xã hội, không vì mục tiêu lợi nhuận.

- **Các loại dịch vụ công hiện nay**

Loại 1: Dịch vụ sự nghiệp công.

Là các hoạt động phục vụ những nhu cầu thiết yếu cho xã hội, quyền và lợi ích công dân. Nhà nước thực hiện thông qua các tổ chức, đơn vị sự nghiệp của Nhà nước hoặc ủy quyền cho các tổ chức ngoài nhà nước thực hiện.

Loại 2: Dịch vụ công ích.

Là các hoạt động có một phần mang tính chất kinh tế hàng hó

Loại 3: Dịch vụ dành chính công.

Là các hoạt động thực thi pháp luật của các cơ quan nhà nước.

- **Dịch vụ công trực tuyến**

Là dịch vụ công được thực hiện trực tuyến. Trên thực tế chỉ có ”Phần giao dịch” của phần dịch vụ công này được thực hiện trực tuyến. Cụ thể hơn chị có “phần trao đổi thông tin” của dịch vụ công được thực hiện bằng phương tiện công nghệ điện tử.

1.2.4.2. Các loại hình giao dịch hành chính điện tử của cơ quan nhà nước

Theo điều 39, chương V luật giao dịch điện tử, quy định 3 loại hình giao dịch điện tử trong cơ quan nhà nước đó là:

- Giao dịch điện tử trong nội bộ cơ quan nhà nước .
- Giao dịch điện tử giữa các cơ quan nhà nước với nhau.
- Giao dịch điện tử giữa các cơ quan nhà nước với cơ quan, tổ chức, cá nhân.

Giao dịch G4C: Chính quyền với công dân

Giao dịch G4C cung cấp cấc dịch vụ của Chính quyền trực tiếp cho cộng đồng ví dụ như quản lý quy hoạch xây dựng đô thị, thăm dò dư luận, giám sát vầ thanh toán thuế,tư vấn, khiếu nại... Giao dịch G4C giúp phổ biến thông tin tới công chúng và hỗ trợ người dân các dịch vụ căn bản.

Giao dịch G2B: Chính quyền với Doanh nghiệp

Giao dịch G2B là những dịch vụ trao đổi giữa Chính quyền 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 thông qua giao dịch G2B như thông tin kinh doanh, tải mẫu đơn, gia hạn giấy phép, cấp phát giấy phép, nộp thuế,…,nó hỗ trợ phát triển kinh doanh, đặc biệt là với các doanh nghiệp vừa và nhỏ.

Giao dịch G2G: Chính quyền với Chính quyền

Giao dịch G2G được triển khai ở hai cấp độ ở địa phương hoặc trong nhà nước và ở quốc tế. G2G là những giao dịch giữa các Chính quyền TW/ quốc gia và chính quyền địa phương, giữa các công ty, cơ quan có liên quan. Đồng thời là giao dịch giữa các Chính quyền và có thể được sử dụng như là một công cụ của các mối quan hệ quốc tế.

Giao dịch này được hiểu như là khả năng phối hợp, chuyển giao và cung cấp các dịch vụ một cách có hiệu quả giữa các ngành, các cấp, các tổ chức, bộ máy của nhà nước trong việc điều hành và quản lý nhà nước.

Giao dịch G2E: Chính quyền với cán bộ công chức

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

G2E bao gồm G4C và các dịch vụ chuyên ngành khác dành riêng cho các công chức Chính quyền như việc cung cấp, đào tạo và phát triển nguồn nhân lực .

1.3. THỰC TRẠNG VẤN ĐỀ ỨNG DỤNG HÀNH CHÍNH ĐIỆN TỬ Ở VIỆT NAM

1.3.1. Tình hình ứng dụng giao dịch điện tử tại Việt Nam

Hầu hết các quốc gia phát triển trên thế giới và trong khu vực đã ứng dụng giao dịch điện tử trong tất cả các hoạt động hành chính và thương mại.

Theo kế hoạch tới năm 2015, 90% các văn bản hành chính ở nước ta là các tài liệu số hóa, như vậy nếu không sử dụng giao dịch điện tử thì sẽ không thể xử lý được các tài liệu trên.

Trong những năm gần đây, các dịch vụ giao dịch điện tử ở nước ta phát triển khát nhanh. Nhiều cơ quan, doanh nghiệp, tổ chức đã đầu tư ứng dụng giao dịch điện tử vào các hoạt hoạt động cua họ.

Hiện nay, có khoảng 90% các bộ ngành, 100% các tỉnh, thành phố và 30% các quận, huyện trên cả nước đã có Website cung cấp thông tin về các chính sách, thủ tục hành chính,… phục vụ người dân. Ngân hàng là ngành sử dụng giao dịch điện tử mạnh nhất ở nước ta. Họ dùng dịch vụ này trong việc gửi, nhận, cung cấp thông tin qua mạng, xử lý chứng từ kế toán;giao dịch giữa ngân hành với khách hàng. Tuy vậy, ứng dụng giao dịch điện tử ở nước ta mới chỉ dừng lại ở mức độ từng phần mà chưa có dịch vụ nào thực hiện được ở mức toàn phần.

Năm 2005, Việt Nam chính thức trở thành thành viên thứ 150 của WTO, qua đó mở cánh cửa hội nhập với các nước trên thế giới. Với tư cách là một thành viên của APEC, nước ta cũng tích cực tham gia ủng hộ chương trình thực hiện Thương mại phi giấy tờ từ năm 2005 với nhóm các nước phát triển và từ năm 2010 với nhóm các nước đang phát triển.

Năm 2003, Thủ tướng nước ta đã ký kết Hiệp định khung ASEAN điện tử với hai nội dung quan trọng là "Thương mại điện tử" và "Chính quyền điện tử". Về mặt pháp lý, đã có văn bản chính thức của Chính quyền và Quốc hội về "Giao dịch điện tử".

Sau hai năm soạn thảo, luật giao dịch điện tử số 51/2005/QH11 được thông qua ngày 29/11/2005 tại kì họp thứ 8 Quốc hội khóa XI, có hiệu lực chính thức từ ngày 1/3/2006. Sau đó là các nghị định 26/2007/NĐ-CP ngày 15/2/200 về Luật giao dịch điện tử, chữ ký số và chứng thực chữ ký số,nghị định 27/2007/NĐ-CP ngày 23/2/2007 về giao dịch điện tử trong hoạt động hành chính, nghị định 64/2007/NĐ-CP ngày 10/4/2007 về quy định ứng dụng công nghệ thông tin trong hoạt động của các cơ quan nhà nước. Quyết định 1605/QĐ-TTg, nghị định 102/2009/NĐ-CP, Nghị định 43/2011/NĐ-CP theo đó dần dần hoàn thiện bộ luật về Giao dịch điện tử, Hành chính điện tử.

Như vậy tình hình ứng dụng "giao dịch điện tử"trong các hoạt động hành chính ngày một phát triển mạnh mẽ và dần dần thay thế các "giao dịch hành chính thông thường".

Bảng 1.1: Xếp hạng theo tiêu chí thành phần về Website/Portal (cung cấp thông tin, chức năng hỗ trợ người sử dụng và công tác quản lý) của các Bộ, cơ quan ngang Bộ.

TT	Bộ, cơ quan ngang Bộ	Địa chỉ Website/Portal	Xếp hạng 2012 (điểm tối đa: 140)	Xếp hạng 2011 (điểm tối đa: 115)	Xếp hạng 2010 (điểm tối đa: 100)	Xếp hạng 2009 (điểm tối đa: 81)
Mức Tốt						
1	Bộ Thông tin và Truyền thông	www.mic.gov.vn	**01 (123,0)**	01 (103,3)	01 (92,0)	05 (69,0)
2	Bộ Xây dựng	www.moc.gov.vn	**02 (116,5)**	03 (93,0)	09 (78,0)	02 (73,0)
Mức Khá						
3	Bộ Tư pháp	www.moj.gov.vn	**03 (111,0)**	07 (87,5)	04 (85,5)	04 (72,0)
4	Bộ Nông nghiệp và Phát triển nông thôn	www.agroviet.gov.vn	**03 (111,0)**	04 (90,5)	05 (82,5)	08 (65,0)
5	Bộ Công thương	www.moit.gov.vn	**05 (110,0)**	02 (94,0)	10 (77,5)	02 (73,0)
6	Bộ Kế hoạch và Đầu tư	www.mpi.gov.vn	**06 (105,5)**	12 (74,0)	07 (80,0)	07 (66,0)
7	Bộ Tài chính	www.mof.gov.vn	**07 (105,0)**	08 (87,0)	03 (86,5)	06 (68,0)
8	Thanh tra Chính phủ	www.thanhtra.gov.vn	**08 (103,5)**	05 (89,0)	20 (30,5)	19 (36,0)
9	Bộ Khoa học và Công nghệ	www.most.gov.vn	**09 (97,0)**	06 (88,0)	02 (88,0)	11 (58,0)

TT	Bộ, cơ quan ngang Bộ	Địa chỉ Website/Portal	Xếp hạng 2012 (điểm tối đa: 140)	Xếp hạng 2011 (điểm tối đa: 115)	Xếp hạng 2010 (điểm tối đa: 100)	Xếp hạng 2009 (điểm tối đa: 81)
Mức Trung bình						
10	Bộ Giáo dục và Đào tạo	www.moet.gov.vn	**10 (93,5)**	09 (83,5)	08 (79,5)	01 (79,0)
11	Bộ Lao động – Thương binh và Xã hội	www.molisa.gov.vn	**11 (93,0)**	11 (77,0)	06 (82,0)	10 (60,0)
12	Ngân hàng nhà nước Việt Nam	www.sbv.gov.vn	12 **(87,5)**	13 (74,0)	12 (73,0)	13 (57,0)
13	Bộ Giao thông vận tải	www.mt.gov.vn	13 **(85,0)**	14 (72,5)	15 (65,0)	09 (61,0)
14	Bộ Nội vụ	www.moha.gov.vn	14 **(84,5)**	21 (53,8)	15 (65,0)	11 (58,0)
15	Bộ Tài nguyên và Môi trường	www.monre.gov.vn	15 **(80,0)**	15 (63,8)	17 (62,5)	16 (52,0)
16	Ủy ban Dân tộc	www.cema.gov.vn	16 **(79,5)**	17 (59,5)	18 (61,0)	13 (57,0)
17	Bộ Ngoại giao	www.mofa.gov.vn	17 **(77,0)**	16 (60,5)	14 (65,5)	15 (55,0)
18	Bộ Y tế	www.moh.gov.vn	18 **(76,0)**	18 (59,0)	13 (68,0)	17 (43,0)
19	Văn phòng Chính phủ	vpcp.chinhphu.vn	18 **(76,0)**	10 (80,8)	-	-
20	Bộ văn hóa – Thể thao và Du lịch	www.cinet.gov.vn	20 **(69,0)**	19 (56,5)	19 (84,0)	17 (43,0)
21	Bộ Công an	mps.gov.vn	21 (56,5)	20 (54,5)	11 (107,8)	-
22	Bộ Quốc phòng	www.mod.gov.vn	22 (59,0)	-	-	-

** Ghi chú: Dấu '-' trong các ô xếp hạng là đơn vị không có số liệu.*

Bảng 1.2: Xếp hạng theo tiêu chí thành phần về Cung cấp dịch vụ công trực tuyến của các Bộ, cơ quan ngang Bộ

TT	Bộ, cơ quan ngang Bộ	Xếp hạng 2012 (điểm tối đa: 100)	Xếp hạng 2011 (điểm tối đa: 100)	Xếp hạng 2010 (điểm tối đa: 80)
1	Bộ Ngoại giao	**01 (61,64)**	01 (45,45)	02 (67,48)
2	Bộ Thông tin và Truyền thông	**02 (42,43)**	06 (25,95)	04 (62,81)
3	Bộ Tài chính	**03 (29,25)**	05 (27,33)	05 (58,49)
4	Bộ Công Thương	**04 (28,27)**	02 (33,33)	03 (67,30)
5	Ngân hàng Nhà nước Việt Nam	**05 (25,56)**	04 (28,57)	10 (54,47)
6	Bộ Tư pháp	**06 (23,47)**	08 (20,00)	16 (18,41)
7	Bộ Giáo dục và Đào tạo	**07 (22,67)**	07 (22,67)	01 (80,00)
8	Thanh tra Chính phủ	**08 (20,00)**	08 (20,00)	-
9	Bộ Y tế	**08 (20,00)**	08 (20,00)	12 (51,78)
10	Bộ Văn hóa - Thể thao và Du lịch	**08 (20,00)**	08 (20,00)	13 (37,90)
11	Bộ Nội vụ	**08 (20,00)**	08 (20,00)	15 (26,75)
12	Bộ Quốc phòng	**08 (20,00)**	-	-
13	Bộ Nông nghiệp và Phát triển nông thôn	**13 (19,96)**	03 (29,00)	14 (27,83)
14	Bộ Giao thông vận tải	**14 (19,03)**	18 (15,50)	11 (53,81)
15	Bộ Khoa học và Công nghệ	**15 (15,99)**	08 (20,00)	06 (56,31)
16	Bộ Lao động - Thương binh và Xã hội	**16 (15,97)**	17 (16,03)	07 (55,48)
17	Uỷ ban Dân tộc	**17 (10,00)**	08 (20,00)	08 (54,72)
18	Bộ Tài nguyên và Môi trường	**18 (7,74)**	19 (6,13)	17 (14,69)
19	Bộ Xây dựng	**19 (2,67)**	08 (20,00)	18 (5,36)
20	Bộ Công an	-	08 (20,00)	-

** Ghi chú:*

- Bộ Kế hoạch và Đầu tư đã phân cấp hoàn toàn việc cung cấp các dịch vụ công trực tuyến cho các địa phương, Văn phòng Chính phủ không có dịch vụ công trực tuyến nên không xếp hạng;

- Dấu '-' trong các ô xếp hạng là đơn vị không có số liệu.

Bảng 1.3:Số lượng dịch vụ công trực tuyến các mức được cung cấp tại các Bộ, cơ quan ngang Bộ

TT	Bộ, cơ quan ngang Bộ	Năm 2012					Năm 2011					Năm 2010					Năm 2009			
		TS	Mức 1, 2	Mức 3	Mức 4	DVC khác	TS	Mức 1, 2	Mức 3	Mức 4	DVC khác	TS	Mức 1, 2	Mức 3	Mức 4	DVC khác	TS	Mức 1, 2	Mức 3	DVC khác
1	Bộ Công an	-	-	-	-	-	148	148												
2	Bộ Công Thương	58	49	6	3		211	205	4	2		209	198	10	1		200	198	2	
3	Bộ Giáo dục và Đào tạo	152	150	2			73	60	2			206	181	2		23	205	181	1	23
4	Bộ Giao thông vận tải	453	453				286	286				415	415							
5	Bộ Khoa học và Công nghệ	163	162	1			125	125				137	137	1			161	160	1	
6	Bộ Lao động - Thương binh và Xã hội	226	226				226	226				291	291				286	286		
7	Bộ Ngoại giao	71	51	20			60	44	16			65	62	3			70	69	1	
8	Bộ Nông nghiệp và Phát triển nông thôn	520	519	1			469	465	3		1	226	222	4			264	226		38
9	Bộ Nội vụ	175	175				175	175				88	88				2	2		
10	Bộ Quốc phòng	4	4				0													
11	Bộ Tài chính	963	957	5	1		917	899	3	1	43	887	840	4		43	17	17		
12	Bộ Tài nguyên và Môi trường	82	82				68	65			3	69	65			4	212	212		
13	Bộ Thông tin và Truyền thông	185	179	6			25	23	2			154	151	3			149	142	3	4
14	Bộ Tư pháp	111	100	11			106	106				106	106				112	112		
15	Bộ Văn hóa - Thể thao và Du lịch	124	124				124	124				124	124							
16	Bộ Xây dựng	12	12				11	11				10	10				10	10		
17	Bộ Y tế	247	247				247	247				247	247				133	133		
18	Ngân hàng Nhà nước Việt Nam	221	220	1			221	220	1			220	220				224	223	1	
19	Thanh tra Chính phủ	15	15				3	3												
20	Ủy ban Dân tộc	1	1				5	5				11	11							
	Tổng số		3726	53	4			3437	31	3	29		3368	27	1			1971	9	

** Ghi chú: - Bộ Kế hoạch và Đầu tư đã phân cấp hoàn toàn việc cung cấp các dịch vụ công trực tuyến cho các địa phương; Văn phòng Chính phủ không có dịch vụ công trực tuyến.*

Bảng 1.4: Danh sách dịch vụ công trực tuyến mức độ 4 của các Bộ, cơ quan ngang Bộ

TT	Bộ, cơ quan ngang Bộ	Tên dịch vụ công trực tuyến mức độ 4
1	Bộ Công Thương	1. Cấp giấy xác nhận khai báo hóa chất (2010) - www.cuchoachat.gov.vn 2. Đăng ký website thương mại điện tử (2011) - www.dangkywebsite.gov.vn 3. Chứng thực số (2010) - moit.vsign.vn
2	Bộ Tài chính	1. Dịch vụ kê khai thuế và nộp tờ khai trực tuyến (2009) - kekhaithue.gdt.gov.vn

** Ghi chú: Năm ghi trong cặp ngoặc đơn trong cột Tên dịch vụ là năm dịch vụ bắt đầu được cung cấp.*

1.3.2. Hiện trạng các công cụ thực hiện giao dịch hành chính

1.3.2.1. Hệ thống hỗ trợ giao dịch hành chính

Hệ thống này có thể hiểu là tập hợp các công cụ và phương tiện để phục vụ hiệu quả và hợp pháp các giao dịch hành chính. Là các công cụ và phương tiện dùngđể soạn thảo, quản lý tài liệu chính cà vận chuyển chúng giữa các đơn vị hành chính và giữa đơn vị hành chính với công dân.

Sự hiệu quả của Hệ thống hỗ trợ giao dịch hành chính đã được nâng lên ở mức cao. Thuận tiện, nhanh chóng, chính xác nhưng vẫn rất hợp pháp.

Các công cụ thực hiện giao dịch hành chính:

- Inter-net tại các cơ quan phục vụ các nhân viên hành chính tra cứu thông tin.
- Hệ thống thư điện tử(E-mail) phục vụ cho các trao đổi thư từ, tài liệu.
- Các công giao tiếp điện tử(Portal)có vai trò là cổng hành chính trực tuyến, cung cấp các thông tin, chính sách,… để mọi người dễ dàng truy cập và tra cứu thông tin.

1.3.2.2. Hiện trạng Hệ thống hỗ trợ giao dịch hành chính

Hiện nay, một số cổng giao tiếp điện tử đã đi vào hoạt động nhưng vẫn đang trong quá trình hoàn thiện, vẫn còn tồn tại một số lỗi và còn thiếu một số chức năng quan trọng, nhất là khả năng tương tác và giao dịch trực tuyến.

Hệ thống hỗ trợ giao dịch hành chính chưa có đầy đủ các công cụ đảm bảo an toàn thông tin. Cụ thể là các hệ thống mới chỉ dừng lại ở mức đảm bảo an toàn thông tin đơn giản như kiểm soát truy nhập trực tiếp, chức năng sao lưu, diệt virus mà chưa đảm bảo an ninh cơ sở dữ liệu, tự động kiểm soát truy nhập tự động (Firewall, VPN).

Hệ thống hỗ trợ giao dịch hành chính của chúng ta chưa có hạ tầng cơ sở mật mã khóa công khai (PKI) để thực hiện ký điện tử, xác thực số, bảo mật hay bảo toàn dữ liệu trên đường truyền.

1.3.2.3. Các vấn đề với Hệ thống hỗ trợ giao dịch hành chính

Hạ tầng cơ sở mạng máy tính sẽ phải xây dựng như thế nào để có thể quản lý, xử lý và vận chuyển được khối lượng lớn các tài liệu giao dịch như nêu trên. Từ đó thấy yêu cầu đầu tiên là hệ thống mạng phải có các giải pháp để lưu trữ nhiều, tìm kiếm nhanh, giảm thiểu tắc nghẽn mạng.

Hạ tầng cơ sở bảo đảm an toàn thông tin phải xây dựng như thế nào để có thể xác thực các tài liệu bằng chữ ký số hay bảo vệ bằng mật mã một cách an toàn với khối lượng lớn các tài liệu.

Hạ tầng cơ sở được xây dựng phải bảo đảm không chỉ quản lý, xử lý được lượng lớn tài liệu mà còn phải xử lý được độ phức tạp của tài liệu, phòng chống được các cuộc tấn công của các đối tượng phá hoại vào hệ thống thông tin.

1.3.2.4. Một số đề xuất cho Hệ thống hỗ trợ giao dịch hành chính

Từ những nhu cầu chuyển giao, ký số, xác thực số, bảo vệ tài liệu thì hệ thống hỗ trợ giao dịch hành chính điện tử cần được nâng cấp để phục vụ các giao dịch một cách hiệu quả và hợp pháp hơn nữa.

Có thể thông qua mạng máy tính để thao tác từ xa, giảm thiểu hạn chế về mặt không gian và thời gian. Mặt khác đảm bảo được các tài liệu này khó có thể đánh cắp, giả mạo, chỉnh sửa nếu không được phép.

1.4. CÁC MỨC GIAO DỊCH TRỰC TUYẾN TRONG HÀNH CHÍNH ĐIỆN TỬ.

Theo nghị định 43/2011/NĐ-CP, Dịch vụ công trực tuyến được quy định theo các mức độ sau:

1.4.1. Mức độ 1

Dịch vụ công trực tuyến ở mức độ 1 là dịch vụ đảm bảo cung cấp đầy đủ các thông tin về thủ tục hành chính và các văn bản có liên quan quy định về thủ tục hành chính đó. Các thông tin bao gồm:

- Quy trình thực hiện hành chính công.
- Thủ tục thực hiện dịch vụ, các giấy tờ cần thiết.
- Các bước tiến hành, thời gian thực hiện, chi phí thực hiện.

1.4.2. Mức độ 2

Một dịch vụ hành chính công trực tuyến được coi là đạt mức 2, nếu như dịch vụ hành chính công đó đáp ứng được các tiêu chí sau:

- Đạt tiêu chí mức 1.
- Cho phép người dùng tải về các mẫu đơn, hồ sơ để họ có thể in ra giấy hoặc điền vào các mẫu đơn.

Hồ sơ hoàn thiện có thể thực hiện qua bưu điện hoặc người dùng nộp trực tiếp tại các cơ quan thụ lý hồ sơ.

Ghi chú: Nếu một dịch vụ hành chính công trực tuyến được đăng kí mức 2, tuy có cung cấp các mẫu đơn hồ sơ để người dùng dịch vụ tải về nhưng không cung cấp đầy đủ các thông tin cần thiết đối với dịch vụ hành chính công trực tuyến mức 1 thì cũng không được xem là dịch vụ hành chính công ở mức 2 cũng như mức 1.

1.4.3. Mức độ 3

Một dịch vụ hành chính công trực tuyến được coi là đạt mức 3, nếu như dịch vụ hành chính công đó đáp ứng được các tiêu chí sau:

- Đạt tiêu chí mức 1.
- Đạt tiêu chí mức 2.
- Cho phép người dùng điền trực tuyến vào các mẫu đơn, hồ sơ và gửi lại trực tuyến các mẫu đơn, hồ sơ tới các cơ quan và người thụ lý hồ sơ.

Các giao dịch trong quá trình thụ lý hồ sơ và cung cấp dịch vụ được thực hiện qua mạng máy tính. Tuy vậy, việc thanh toán chi phí và trả kết quả sẽ thực hiện khi người dùng dịch vụ đến trực tiếp cơ quan cung cấp dịch vụ.

Ghi chú: Nếu một dịch vụ hành chính công trực tuyến được đăng kí mức 3, có cung cấp cơ chế điền biểu mẫu và xử lý trực tuyến nhưng không cung cấp đầy đủ các thông tin cần thiết đối với dịch vụ hành chính công trực tuyến mức 1 thì cũng không được xếp mức cho dịch vụ hành chính công.

1.4.4. Mức độ 4

Một dịch vụ hành chính công trực tuyến được coi là đạt mức 4, nếu như dịch vụ hành chính công đó đáp ứng được các tiêu chí sau:

- Đạt tiêu chí mức 1.
- Đạt tiêu chí mức 2.
- Đạt tiêu chí mức 3
- Việc thanh toán chi phí được thực hiện trực tuyến, việc kiểm tra kết quả có thể thực hiện trực tuyến hoặc qua đường bưu điện.

Ghi chú: Nếu một dịch vụ hành chính công trực tuyến được đăng kí mức 4, có cung cấp cơ chế điền biểu mẫu và xử lý trực tuyến nhưng không cung cấp đầy đủ các thông tin cần thiết đối với dịch vụ hành chính công trực tuyến mức 1 thì cũng không được xếp mức cho dịch vụ hành chính công.

CHƯƠNG 2: TỔNG QUAN VỀ AN TOÀN THÔNG TIN

2.1. VẤN ĐỀ AN TOÀN THÔNG TIN

2.1.1.Vì sao phải bảo đảm An toàn thông tin

Sự xuất hiện của Inter-net và mạng máy tính đã giúp cho công việc trao đổi thông tin trở nên nhanh gọn, dễ dàng. Theo đó nảy sinh ra vấn đề thông tin quan trọng nằm trong kho dữ liệu hay trên đường truyền có thể bị trộm cắp, làm sai lệch, giả mạo, …Điều đó có thể ảnh hưởng đến các tổ chức, công ty hay cả một quốc gia. Ví dụ như những kế hoạch, chiến lược kinh doanh tài chính là mục tiêu của các đối thủ cạnh tranh hay các thông tin mật về công tác an ninh, quốc phòng là mục tiêu của các tổ chức tình báo trong và ngoài nước.

Khi nhận được một bản tin trên mạng thì không có đặc điểm hay là bảo đảm gì đó là tài liệu mà bên đối tác gửi đi. Thông thường văn bản trước khi được chuyển đi phải ký phía dưới nhưng chữ ký này rất dễ bị gả mạo. Kẻ cắp có thể dán đè một chữ ký khác lên trên đó.

Từ yêu cầu cấp bách của tình hình trên, vấn đề bảo đảm an toàn thông tin được đặt ra và cần được coi trọng và quan tâm đặc biệt.

2.1.2. Một số rủi ro khi mất an toàn thông tin trong giao dịch điện tử

Giao thức TCP/IP và FTP là hai giao thức cho phép người dùng có thể chuyển thông tin từ các máy tính trong LAN hoặc ngoài Inter-net. Khi tài liệu được gửi đi dẫn đến tài liệu có nguy cơ mất an toàn như nghe trộm, mạo danh, giả mạo, chối bỏ nguồn gốc.

Nghe trộm(Eavesdropping): Việc này thường được tiến hành khi các hacker đã chiếm được quyền truy nhập hệ thống hay nắm quyền kiểm soát đường truyền dữ liệu. Từ đó, các tài liệu có thể bị thay thế bởi các thông tin nhằm vào một số mục đích như lừa đảo, quảng cáo,…

Mạo danh(Impersonation): Là hình thức gian lận trên mạng mà thủ phạm xưng danh một tổ chức, doanh nghiệp có uy tín nhằm lợi dụng lòng tin để đánh lừa người nhận gửi thông tin cho chúng hoặc là thông qua đó để phát tán virus.

Giả mạo(Tampering): Là một hình thức lừa đảo trên mạng bằng cách giả mạo email, website nhằm lấy cắp thông tin như thông tin tài khoản.

2.1.3. Hệ thống bảo vệ thông tin

Với sự phát triển bùng nổ của công nghệ thông tin trong những năm qua,các hệ thống máy tính đã được sử dụng rộng rãi trong mọi tổ chức cá nhân và công cộng. Sự phát triển về công nghệ giúp đáp ứng được yêu cầu về phần cứng. Bên cạnh đó độ tin cậy của phần mềm cũng ngày càng được nâng cao nhờ các kỹ năng chuyên môn của các chuyên viên. Vì vậy, các hệ quản trị cơ sở dữ liệu đã đáp ứng được yêu cầu về lưu trữ và quản lý dữ liệu.

Các hệ quản trị dữ liệu(Database Management System) được đầu tư xây dựng để chúng có khả năng quản trị và khai thác dữ liệu tốt.

Một đặc điểm của Database Management System là khả năng quản lý đồng thời nhiều giao diện ứng dụng. Mỗi ứng dụng có cảm giác chỉ có mình nó đang khai thác cơ sở dữ liệu.

Xử lý dữ liệu phân tán đã góp phần phát triển và tự động hóa các hệ thống thông tin. Nhờ đó các đơn vị xử lý thông tin của các tổ chức và các chi nhánh ở xa có thể giao tiếp mới nhau nhanh chóng, dễ dàng. Việc sử dụng rộng rãi các cơ sở dữ liệu phân tán cũng như tập trung đặt ra các yêu cầu nhằm bảo đảm an toàn thông tin như: tính bí mật, tính toàn vẹn, tính xác thực.

Bảo vệ chống truy cập trái phép: Là một vấn đề căn bản, bao gồm cấp quyền truy nhập cơ sở dữ liệu cho người dùng hợp pháp.

Bảo vệ toàn vẹn cơ sở dữ liệu: Là bảo vệ cơ sở dữ liệu khỏi các truy nhập trái phép mà có thể dẫn đến việc thay đổi nội dung dữ liệu.

Bảo vệ ngữ nghĩa của dữ liệu: Là bảo đảm tính tương thích logic của các dữ liệu bị thay đổi, bằng cách kiểm tra các giá trị dữ liệu có nằm trong khoảng cho phép hay không.

Khả năng lưu vết và kiểm tra: Là yêu cầu ghi lại lịch sử truy nhập tới dữ liệu qua đó bảo đảm tính toàn vẹn dữ liệu vật lý và trợ giúp cho việc phân tích dãy truy nhập vào cơ sở dữ liệu.

Xác thực người dùng: Yêu cầu này cần thiết trong việc xác thực định danh người dùng để cấp quyền truy nhập vào hệ thống.

2.1.4. Một số công nghệ bảo đảm an toàn thông tin

2.1.4.1. Tường lửa (Firewall)

Firewall là một hệ thống được tích hợp vào hệ thống mạng nhằm chống lại sự truy nhập không hợp lệ từ bên ngoài vào mạng trong, qua đó bảo vệ các nguồn thông tin nội bộ.

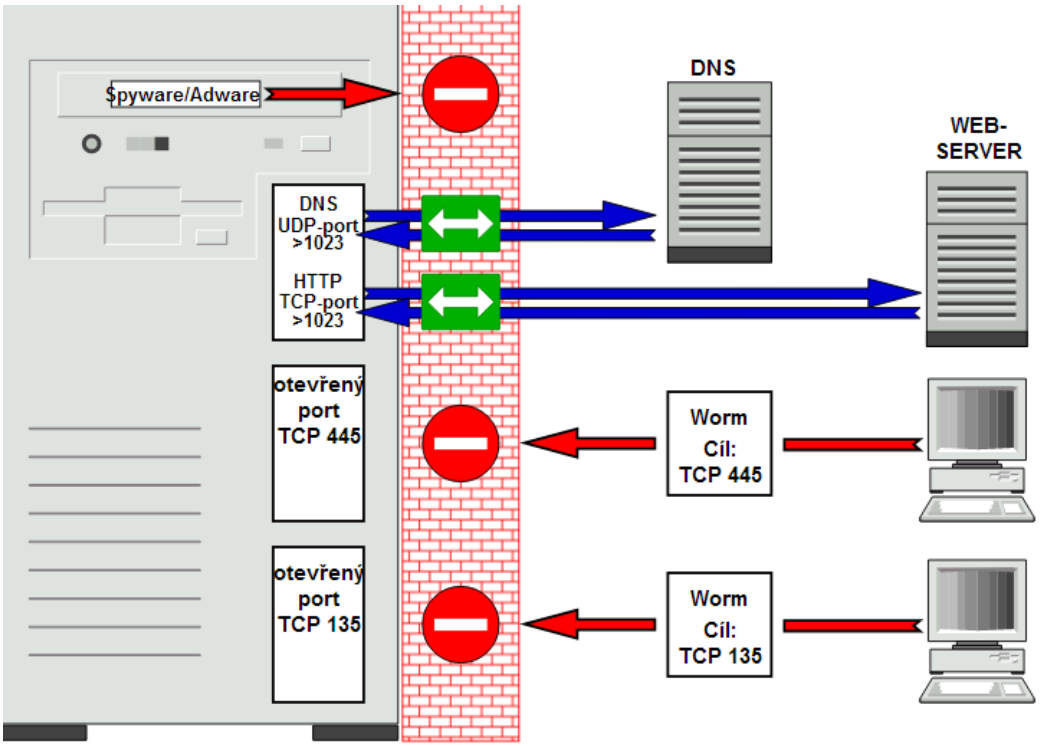
+ Chức năng của Firewall:

- Hạn chế truy nhập tại một điểm kiểm tra.

- Ngăn chặn các truy nhập từ ngoài vào trong hệ thống cần bảo vệ.

- Hạn chế các truy nhập ra ngoài.

Xây dựng firewall là một biện pháp hữu hiệu, vì nó cho phép bảo vệ và kiểm soát hầu hết các dịch vụ do đó được áp dụng phổ biến nhất trong các biện pháp bảo vệ mạng. Firewall là một gateway mà qua đó quản trị viên có thể hạn chế quyền truy nhập vào hệ thống và ngược lại.



Hình 2.1: Mô hình hệ thống tường lửa

2.1.4.2. Mạng riêng ảo (VPN)

Mạng riêng ảo là một kênh truyền bảo mật thông qua môi trường công cộng Internet. VPN không phải là một chuẩn kỹ thuật, nó là một công nghệ đươc kết hợp bởi định đường hầm, mã hóa và QoS(Chất lượng dịch vụ), trong đó:

Định đường hầm là cơ chế đóng gói một giao thức vào trong giao thức khác. Bên nhận phải gỡ bỏ vỏ bọc và giải mã(nếu có).

Mã hóa là việc chuyển các dữ kiệu đọc được thành các dữ liệu khó hiểu bằng một thuật toán nào đó và một khóa mã hóa.

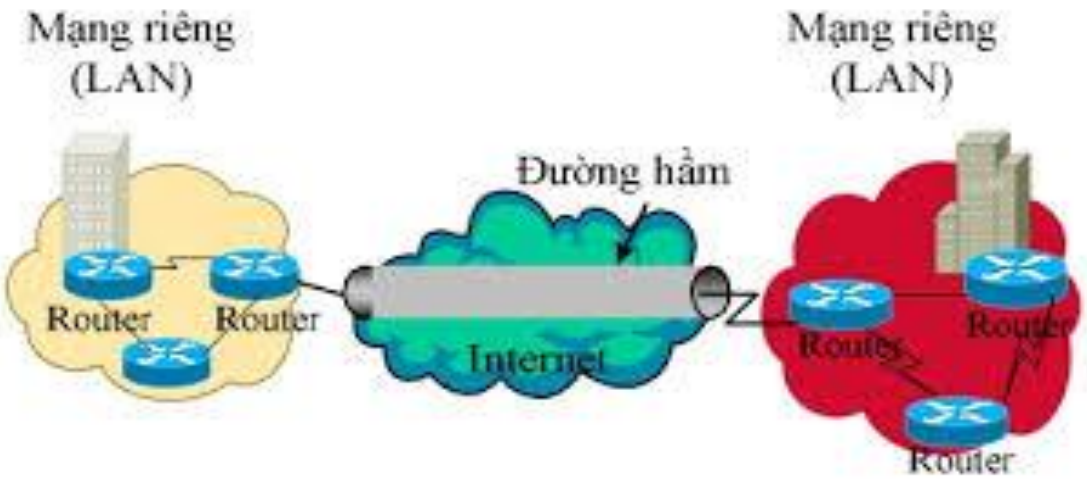
QoS là một chuẩn trong truyền thông, quy định về tỉ lệ độ trễ cũng như số lượng gói tin lỗi.

Giải pháp VPN được thiết kế cho những tổ chức có xu hướng tăng cường thông tin từ xa vì địa bàn hoạt động. Tài nguyên trung tâm có thể được kết nối đến từ nhiều nguồn qua đó tiết kiệm được chi phí và thời gian.

VPN được chia thành 2 loại chính là VPN S2S và VPN S2R.

+ VPN Site To Site: Kết nối từ văn phòng chi nhánh đến văn phòng của công ty qua đường Lease Line và DSL.

+ VPN Site To Remote: Hỗ trợ người dùng từ xa hay đối tác có thể truy cập vào mạng công ty qua đường kết nối với ISP địa phương để vào Internet.



Hình 2.2: Mô hình mạng riêng ảo VPN

2.1.5. Các giao thức bảo đảm an toàn truyền tin

2.1.5.1. Giao thức SSL(Secure sockets layer).

SSL nằm ở đỉnh tầng TCP/IP, cung cấp một bắt tay an toàn mà ở đó máy khách và máy chủ trao đổi một khối dữ liệu ngắn gọn các thông báo.

SSL quản lý các hoạt động mã hóa và giải mã trong một phiên Web. Thông thường SSL có hai độ dài là 40bit và 128bit, là các khóa phiên được sinh ra cho các giao dịch có mã hóa

2.1.5.2. Giao thức S-HTTP

S-HTTP là giao thức mở rộng của giao thức HTTP, cung cấp một số đặc tính an toàn, trong đó có xác thực máy khách và máy chủ., mã hóa và chống chối bỏ yêu cầu/đáp ứng. Giao thức này hoạt ở tầng 7 của mô hình OSI, nó cung cấp mã hóa đối xứng để thiết lập máy khách/máy chủ và các tóm lược thông báo nhằm bảo đảm tính toàn vẹn dữ liệu thông qua header.

Một khi thỏa thuận giữa khách-chủ được thiết lập, tất cả thông báo trong phiên giao dịch được đóng gói vào phong thư an toàn. Nhờ đó đảm bảo tính tính bí mật,toàn vẹn và xác thực. Các thông báo đều được mã hóa khi truyền trên đường truyền nên không ai có thể đọc trộm, mọi sửa đổi đều được phát hiện bởi kỹ thuật toàn vẹn.

2.1.5.3. Giao thức IPsec(IP security)

IPsec là hệ thống các giao thức bảo mật quá trình truyền thông tin trên nền tảng Internet Protocol. Bao gồm xác thực và/hoặc mã hóa cho mỗi gói IP trong quá trình truyền thông tin.

IPsec có một tính năng cao hơn SSL và các giao thức hoạt động ở tầng trên trong mô hình OSI là khi ứng dụng dùng IPsec mã(code) không bị thay đổi trong khi ở SSL bị thay đổi lớn.

IPsec cũng bao gồm các giao thức cung cấp cho mã hóa và xác thực, qua đó đảm bảo tính toàn vẹn của dữ liệu.

2.1.5.4. Giao thức TCP/IP

TCP/IP là một hệ thống giao thức hỗ trợ việc lưu truyền trên mạng, ra đời từ trước khi có mô hình OSI. Giao thức TCP/IP gồm 5 tầng: vật lý, liên kết dữ liệu, mạng, giao vận và ứng dụng. Bốn tầng đầu tương ứng với các tầng tương tự của mô hình OSI

TCP/IP kiểm soát các gói tin tại nút cuối của đường truyền, phát hiện các thay đổi trên đường truyền. Ráp các gói tin lại theo đúng trật tự và phát hiện các gói bị mất, các gói sai trật tự để yêu cầu bên gửi gửi lại dữ liệu. Giao thức này được dùng như một biện pháp đối phó, chống tấn công từ chối.

CHƯƠNG 3: MỘT SỐ BẢO VỆ THÔNG TIN TRONG HÀNH CHÍNH ĐIỆN TỬ

3.1. MỘT SỐ VẤN ĐỀ VỀ AN TOÀN THÔNG TIN TRONG GIAO DỊCH TRỰC TUYẾN

3.1.1. Mục tiêu, nhiệm vụ bảo vệ thông tin

Bảo vệ thông tin hay bảo đảm an toàn thông tin là bảo đảm tính bảo mật, tính toàn vẹn,tính xác thực và tính sẵn sàng.

- Tính bảo mật: Bảo đảm người dùng không hợp pháp không biết hay không hiểu được thông tin.
- Tính toàn vẹn: Bảo đảm người dùng không hợp pháp không biết hay không sửa đổi được thông tin.
- Tính xác thực: Bảo đảm người dùng hợp pháp có thể xác thực được nguồn gốc hay chủ sở hữu thông tin.
- Tính sẵn sàng: Bảo đảm thông tin sẵn sàng cho người dùng hợp pháp.

3.1.2. Các yêu cầu bảo vệ thông tin trong giao dịch trực tuyến

Hệ thống giao dịch điện tử phải đảm bảo được các mục tiêu chính là: tính bí mật, tính toàn vẹn, tính xác thực, tính không thể phủ nhận và sẵn sàng.

3.1.2.1. Tính bí mật

Thông tin không thể bị tiếp cận bởi những người không có thẩm quyền. Những thông tin bí mật phải được mã hóa và được cấp quyền khai thác, chỉ có chủ thể đích thực của nó mới có quyền khai thác sử dụng.

3.1.2.2. Tính toàn vẹn

Thông tin không thể sửa đổi, xóa hoặc bổ sung bởi những người không có thẩm quyền. Nội dung của một thông điệp dữ liệu được xem là toàn vẹn khi nội dung đó chưa bị thay đổi, trừ những thay đổi về hình thức phát sinh trong quá trình gửi, lưu trữ hoặc hiển thị thông điệp dữ liệu.

3.1.2.3. Tính xác thực

Bao gồm xác thực thông tin và xác thực một thực thể. Trong đó, xác thực thông tin là xác định nguồn gốc của thông tin còn xác thực một thực thể là xác định danh tính của thực thể tham gia trong hệ thống giao dịch.

3.1.2.4. Tính không thể phủ nhận

Người khởi tạo thông tin không thể phủ nhận trách nhiệm đối với thông tin do mình tạo ra. Yêu cầu này nhằm ngăn ngừa việc chối bỏ trách nhiệm đối với một cam kết đã có.

3.1.2.5. Tính sẵn sàng

Thông tin luôn sẵn sàng đáp ứng nhu cầu sử dụng của người dùng hợp pháp. Tính sẵn sàng phải đạt được các yêu cầu: sự hiện diện của đối tượng hoặc dịch vụ

dưới dạng có thể sử dụng được,khả năng đáp ứng các yêu cầu về dịch vụ, tiến trình – giới hạn thời gian đợi, thời gian đày đủ/tuyến thời gian của dịch vụ.

3.1.3. Giải pháp bảo đảm an toàn thông tin trong hành chính điện tử

+ Kiểm soát truy cập vào – ra trong máy tính:

Dịch vụ này chống lại việc sử dụng trái phép các tài nguyên do truy nhập thông qua các giao thức mạng.

Kỹ thuật kiểm soát truy cập có thể chia làm 3 nhóm:

- Nhóm kiểm soát tính hợp lệ của dữ liệu đầu vào.
- Nhóm kiểm soát truy cập nguồn tài nguyên máy tính.
- Nhóm kiểm soát phiên truy cập.

+ Che giấu thông tin:

Là kỹ thuật bảo vệ thông tin khỏi sự can thiệp không hợp lệ của đối tượng không có thẩm quyền. Một số kỹ thuật che giấu thông tin như mã hóa và giấu tin.

+ Kiểm soát các lỗ hổng thiếu an ninh:

Đây là một công việc khó và tốn kém. Việc Kiểm soát các lỗ hổng thiếu an ninh đòi hỏi chúng ta phải có hiểu biết tường tận về kỹ thuật và cơ chế đảm bảo an toàn thông tin đang áp dụng, biết phân tích, đánh giá để tìm ra hoặc đưa ra dự báo về các lỗ hổng thiếu an ninh. Từ đó, tìm ra các giải pháp để khắc phục các lỗ hổng này.

+ Quy định hành chính

Là các quy định của tổ chức về đảm bảo an toàn thông tin dựa trên các quy định hiện hành của nhà nước. Quy định có tính pháp lý cao nhất, chi phối tất cả các quy định hành chính trong giao dịch điện tử khác đó là Luật Giao dịch điện tử có hiệu lực từ ngày 01/03/2006. Bên cạnh đó còn các quy định dưới luật và các quy định hành chính khác có liên quan tới lĩnh vực tin học hóa của hệ thống ứng dụng.

Tóm lại, việc bảo đảm an toàn thông tin trong hành chính điện tử có hai công việc chính đó là bảo vệ thông tin trong bộ nhớ và bảo vệ thông tin trên đượcc truyền. Để làm tốt hai công việc này ta phải xây dựng kiến trúc cơ sở hạ tầng trong hành chính điện tử tốt đồng thời thực hiện các giải pháp công nghệ tiên tiến hỗ trợ triển khai mô hình kiến trúc hành chính điện tử đã xây dựng, đưa ra các giải pháp, phần mềm công cụ và dịch vụ được phát triển dựa trên các công nghệ mới hiện nay.

3.2. BẢO MẬT THÔNG TIN BẰNG PHƯƠNG PHÁP MẬT MÃ

3.2.1. Mục đích bảo mật thông tin

Bảo đảm người dùng không hợp pháp không biết hay không hiểu được thông tin.

Bảo mật thông tin có các trường hợp sau:

- Không cho phép xem thông tin: Kiểm soát lối truy nhập vào – ra của thông tin.
- Không cho phép xem thông tin: Giấu đi thông tin bằng biện pháp giấu tin.
- Cho phép xem thông tin nhưng không hiểu được ý nghĩa của thông tin: Dùng biện pháp mã hóa tin, nén tin.

3.2.2. Phương pháp mã hóa dữ liệu

Để bảo đảm an toàn cho thông tin người ta phải "che giấu" thông tin đi.

- Che thông tin là mã hóa thông tin gốc thành một hình dạng khác mà người khác khó có thể hiểu ra nội dung.
- Giấu thông tin là cất giấu thông tin vào một bản tin khác mà người khác khó có thể nhận ra.

3.2.2.1. Hệ mã hóa

Hệ mã hóa được định nghĩa là một bộ năm (**P**,**C**,**K**,**E**,**D**), trong đó:

P là tập hợp hữu hạn các bản rõ.

C là tập hợp hữu hạn các bản mã.

K là tập hợp hữu hạn các khóa.

E tập các hàm lập mã.

D tập các hàm giải mã.

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

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

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

3.2.2.2. Mã hóa và giải mã

Người gửi	→→	$e_{ke}(T)$	→→	Người nhận
(có khóa lập mã $\mathbf{k_e}$)				(có khóa giải mã $\mathbf{k_d}$)

Người gửi muốn gửi bản tin cho người nhận. Để bảo đảm tính bí mật, người gửi mã hóa bản tin bằng khóa lập mã $\mathbf{k_e}$để nhận được bản mã **T**, sau đó gửi cho người nhận.

Người nhận sau khi nhận được bản mã, họ dùng khóa giải mã $\mathbf{k_d}$để giải mã bản tin mã hóa **T** và nhận được bản tin gốc.

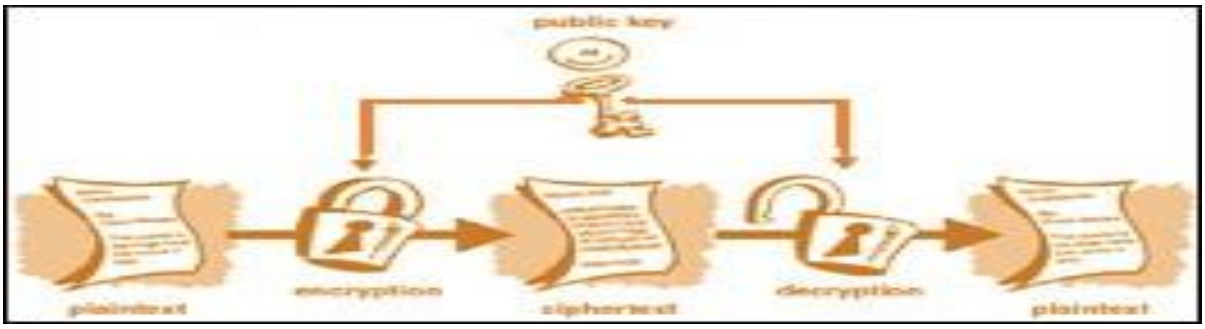
Tin tặc có thể đánh cắp bản mã **T** nhưng cũng khó có thể hiểu được bản tin gốc nếu không có khóa giải mã $\mathbf{k_d}$.

3.2.3. Phân loại hệ mã hóa

3.2.3.1. Hệ mã hóa khóa đối xứng

Mã hóa khóa đối xứng là Hệ mã hóa mà biết được khóa lập mã thì có thể dễ tính được khóa giải mã và ngược lại. Đặc biệt một số hệ mã hóa có khóa lập mã và khóa giải mã trùng nhau như hệ mã hóa dịch chuyển,DES,AES,…

Hệ mã hóa khóa đối xứng còn gọi là Hệ mã hóa khóa bí mật vì phải giữ bí mật cả hai khóa. Trước khi dùng hệ mã hóa khóa đối xứng, người gửi và người nhận phải thỏa thuận thuật toán mã hóa và khóa chung, khóa phải được giữ bí mật. Người gửi A sẽ sử dụng khóa để mã hóa bản rõ thành bản mã rồi gửi cho người nhận B. Sau khi người nhận B nhận được bản mã mà người gửi A đã gửi thì dùng chính khóa ấy để giải mã và nhận được bản rõ. Độ an toàn của Hệ mã hoá này phụ thuộc hoàn toàn vào khóa.



Hình 3.1: Mô hình hệ mã hóa khóa đối xứng

1, Đặc điểm của hệ mã hóa khóa đối xứng

Ưu điểm:

- Sử dụng đơn giản: chỉ cần dùng một khóa cho cả hai bước lập mã và giải mã.
- Hệ mã hóa khóa đối xứng mã hóa và giải mã nhanh hơn hệ mã hóa khóa công khai.

Hạn chế:

- Không an toàn vì khi có càng nhiều người biết khóa thì độ rủi ro càng cao. Người mã hóa và người giải mã phải có chung một khóa. Khóa phải được giữ bí mật tuyệt đối.
- Vấn đề thỏa thuận khóa và quản lý khóa chung là khá khó khăn và phức tạp. Khóa chung phải được chuyển cho nhau trên kênh an toàn.
- Không cho phép tạo ra chữ kí điện tử.

2, Nơi sử dụng hệ mã hóa khóa đối xứng.

Hệ mã hóa khóa đối xứng thường được sử dụng trong môi trường mà khóa chung có thể dễ dàng trao chuyển bí mật như trong cùng một mạng nội bộ.

Hệ này thường được dùng để mã hóa các bản tin lớn vì tốc độ mã hóa và giải mã nhanh hơn hệ mã hóa khóa công khai.

(*) Hệ mã hóa khóa đối xứng có thể chia thành hai loại: mã hóa khối và mã hóa dòng. Mã hóa khối là mã hóa thao tác trên từng khối của bản rõ và bản mã còn mã hóa dòng là mã hóa xử lý từng bit hoặc byte của bản rõ và bản mã tại một thời điểm

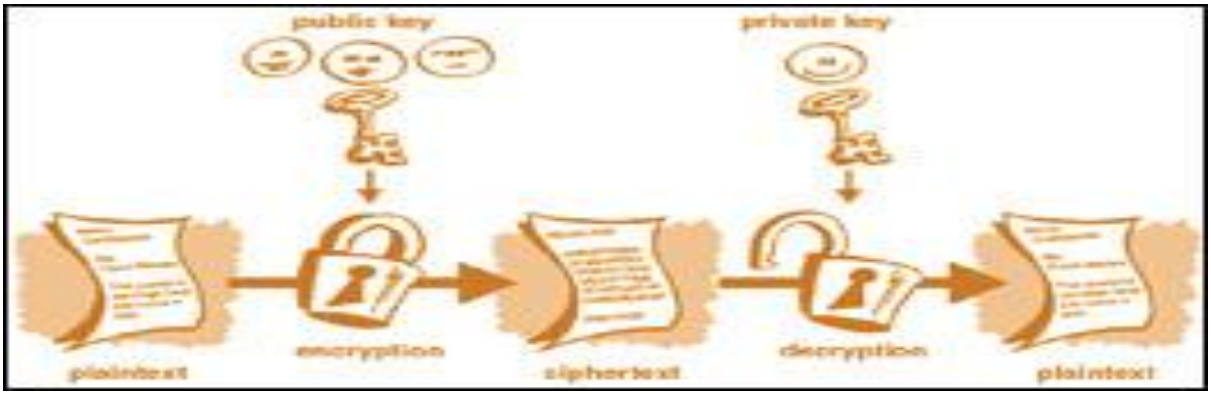
3.2.3.2. Hệ mã hóa khóa công khai

Hệ mã hóa này do Diffie và Hellman phát minh lần đầu tiên vào những năm 1970.

Hệ mã hóa khóa công khai là hệ mã hóa có khóa lập mã và khóa giải mã khác nhau, biết được khóa này cũng rất khó có thể tính được khóa kia.Một người bất kì có thể sử dụng khóa công khai để mã hóa bản tin nhưng chỉ người có khóa giải mã tương ứng mới có khả năng đọc được bản rõ.

Một số thuật toán mã hóa khóa công khai như RSA,ElGamal.

Mỗi hệ thống tạo ra một cặp khóa để dùng trong lập mã và giải mã. Người ta công bố rộng rãi khóa mã hóa, đây là khóa công khai và khóa còn lại được bí mật.



Hình 3.1: Mô hình hệ mã hóa khóa công khai.

1, Đặc điểm của hệ mã hóa công khai

Ưu điểm:

- Thuật toán được viết một lần, công khai cho nhiều lần dùng, chỉ cần giữ khóa bí mật của riêng mình.
- Việc tạo ra cặp khóa công khai và bí mật dễ.
- Việc mã hóa và giải mã cũng khá dễ dàng.
- Nếu biết được được khóa công khai thì cũng khó tìm được khóa bí mật tương ứng. Hay nếu có được khóa công khai và bản mã cũng khó có thể suy ra bản rõ vì số phép thử là vô cùng lớn.

Hạn chế:

Hệ mã hóa này mã hóa và giải mã chậm hơn hệ mã hóa khóa đối xứng nên khi bản tin cần mã hóa lớn thì sẽ mất nhiều thời gian hơn.

2, Nơi sử dụng hệ mã hóa khóa công khai

Thường được sử dụng trên các mạng công khai không an toàn như Internet.

Do tốc độ mã hóa và giải mã chậm nên hệ mã hóa khóa công khai được dùng để mã hóa những bản tin ngắn như để mã hóa khóa bí mật của hệ mã hóa khóa đối xứng. Đặc biệt, mật mã khóa bất đối xứng hay là mật mã khóa công khai được dùng cho ký số rất ưu việt.

3.2.3.3. Hệ mã hóa công khai RSA(Do Rivest,Shamir,Adleman cùng đề xuất)

- Chọn bí mật 2 số nguyên tố lớn khác nhau bất kì**p** và **q**.
- Đặt **n** = **p*****q**.
- Tính bí mật ϕ (**n**) = (**p**-1)(**q**-1).
- Lấy ngẫu nhiên một số b nguyên dương sao cho **b** và ϕ (**n**) là nguyên tố cùng nhau, tức là ước số chung lớn nhất của **b** và ϕ (**n**) là 1.
  (1 $\leq$**b** $\leq$ ϕ (**n**)). Công khai cặp khóa công khai k_e=(**n**,**b**).
- Tính a là phần tử nghịch đảo của b theo mod ϕ (**n**), **a*b** = 1 mod ϕ (**n**). Cặp khóa bí mật $\mathbf{k_d}$=(**n**,**a**) dành riêng cho người nhận.

Với bản rõ **x** ϵ **P** và bản mã **y** ϵ **C**, định nghĩa:

- Hàm mã hóa: **y** = $\mathbf{e_k}$(**x**) = $\mathbf{x^b}$mod **n**.
- Hàm giải mã: **x** = $\mathbf{e_k}$(**x**) = $\mathbf{y^a}$mod **n**.

2, Độ an toàn

Với hệ RSA thì cách tấn công dễ thấy là cố gắng phân tích n ra thừa số nguyên tố và sau khi thực hiện được phân tích này thì có thể dễ dàng tính được ϕ n = (p-1)(q-1) rồi tính số mũ từ b. Nhưng vì để đảm bảo tính an toàn thì p và q thường là những số có chừng 100 chữ số thập phân và khi đó thì n có tới 200 chữ số thập phân.Với những thuật toán phân tích hiện nay có khả năng phân tích tới số có 130 chữ số thập phân nên khả năng phân tích n thành thừa số là một việc rất khó khăn.

Ngoài cách phân tích n thành thừa số nguyên tố ta còn cách là tính ϕ n và n là tích của p và q thì có thể phân tích được n bằng cách giải hệ hai phương trình:

$$\begin{cases} n = p*q \ (1) \\ \phi(n)=(p-1)(q-1) \ (2) \end{cases}$$

Nếu thế q = n/p vào phương trình 2 ta được phương trình bậc hai chưa biết p: $p^2 - (n - \phi(n)+1) + n = 0$.

Khi tính được phương trình này ta sẽ có được p và q là hai nhân tử của n. Nhưng việc tính được ϕ n này cũng không dễ dàng hơn việc phân tích n.

Đặc biệt khi mã hóa và giải mã kiểu mã hóa khối thì độ phức tạp của thuật toán tăng theo số mũ vì việc tính x^c mod n có thể thực hiện bằng c-1 phép nhân module.Tuy nhiên c lớn thì phép tính này rất lớn nên đây cũng là một điểm giúp cho RSA được bảo mật.

+, Hệ mã hóa RSA đối với mỗi bản rõ **x** và một khóa bí mật **a** thì chỉ có một bản mã **y**.

+, Hệ mã RSA an toàn khi giữ bí mật được **a**,**p**,**q**, ϕ (**n**).

Nếu biết p,q thì ta có thể dễ dàng tính được ϕ (n).

Nếu biết ϕ (n) ta có thể thám mã tính được a theo thuật toán Euclide mở rộng.

Vì vậy, độ an toàn của Hệ mã hóa RSA phụ thuộc vào việc giữ bí mật khóa a và khả năng giải bài toán phân tích số nguyên tố lớn n thành tích của hai số p và q.

3.3. PHƯƠNG PHÁP BẢO TOÀN THÔNG TIN

3.3.1.. Mục đích bảo toàn thông tin

Người nhận thông tin nếu không được cấp quyền: Có thể nhìn được thông tin, có thể hiểu được ý nghĩa của thông tin nhưng nếu sửa đổi thông tin thì chủ nhân của thông tin này có thể nhận biết được sự sửa đổi này,

3.3.2. Khái niệm ký số

Ký số là một định danh điện tử được tạo ra bởi máy tính, được các tổ chức sử dụng nhằm đạt được tính hiệu quả và có hiệu lực như chứ ký tay.

Là một cơ chế xác thực hóa cho phép người tạo ra thông điệp đính kèm một mã số vào thông điệp giống như việc ký một chữ ký lên một văn bản bình thường.

Sơ đồ chữ ký số là một bộ lăm: (**P,A,K,S,V**), trong đó:

P là tập hữu hạn các thông điệp.

Alà tập hữu hạn các chữ ký.

Klà tập hữu hạn các khóa.

Slà tập các thuật toán ký.

Vlà tập các thuật toán kiểm tra chữ ký.

Với mỗi k ∈ **K** có thuật toán ký Sig_k ∈ **S** và thuật toán xác minh Ver_k ∈ **V**.

Mỗi thông điệp x ϵ **P** chữ ký y ϵ **A** thỏa mãn phương trình :

$$Ver_k = \begin{cases} True & \text{nếu } y = sig(x) \\ False & \text{nếu } y \neq sig(x) \end{cases}$$

Sig_k và Ver_k là các hàm có thời gian đa thức nên không thể dễ dàng giả mạo chữ ký trên thông điệp.

*** Quá trình tạo chữ ký số**

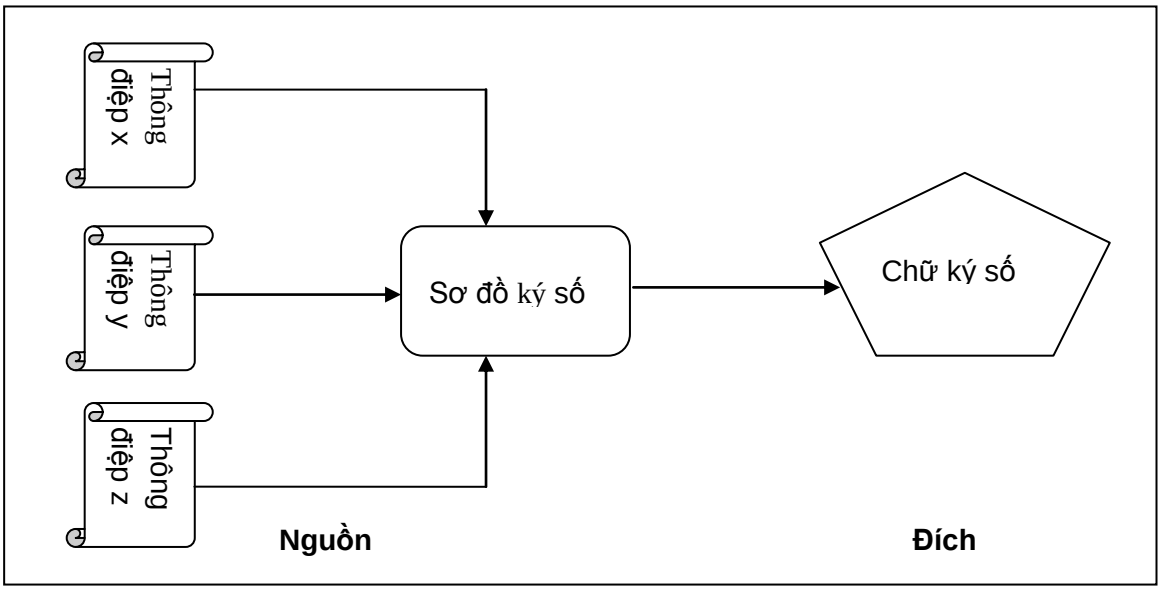
- Sinh khóa: Khóa bí mật, khóa công khai.
-Ký số.
- Kiểm tra ký số.

*** Một số dạng chữ ký số**

- Chữ ký RSA
- Chữ ký Elgamal
- Chữ ký DSS

3.3.3. Đại diện thông điệp và hàm băm

Sơ đồ chữ ký thường là mã hóa từng bit của thông tin, thời gian để ký tỷ lệ thuận với dung lượng của thông tin. Trường hợp với nhiều đầu vào khác nhau nhưng sử dụng sơ đồ ký số giống nhau cho thì cho ra chữ ký số giống nhau dẫn đến rắc rối cho việc xác thực về sau.



Hình 3.3: Minh họa nhiều thông điệp nguồn cho cùng một kết quả sau ký số

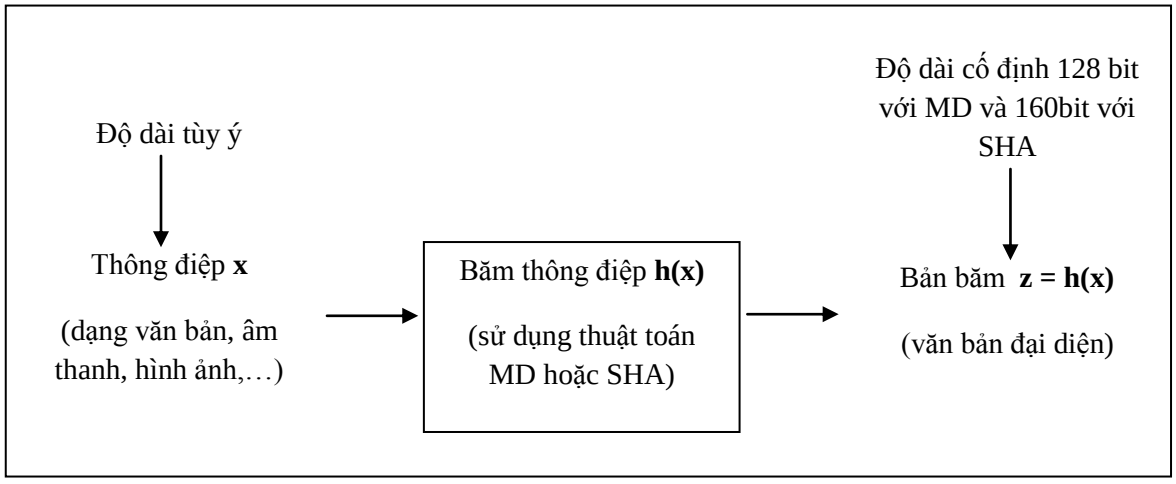
Với các sơ đồ ký số, chỉ cho phép ký các thông điệp có kích thước nhỏ và sau khi ký, bản ký số có kích thước gấp đôi bản thông điệp gốc. Trong thực tế, ta cần phải ký các thông điệp có kích thước lớn hơn nhiều. Hơn nữa, việc truyền dữ

liệu qua mạng không chỉ là thông điệp gốc mà còn cả bản ký số để đáp ứng việc xác thực sau khi thông tin đến được với người nhận.

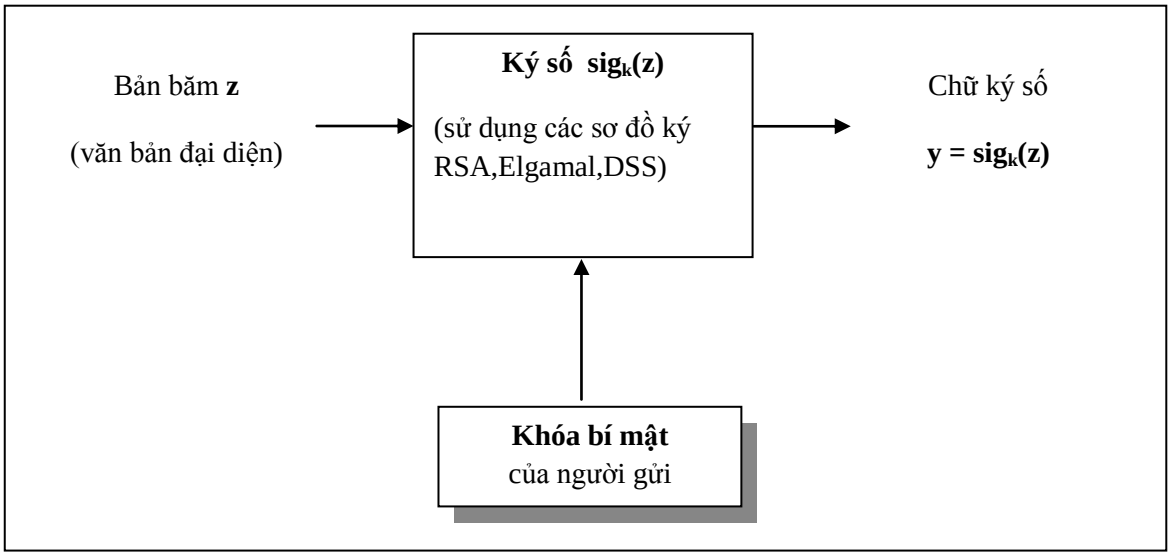
Vì các bản ký số có dung lượng lớn nên giải pháp cho vấn đề này là dùng hàm băm để trợ giúp cho việc ký số. Các thuật toán băm đầu vào là các thông điệp có dung lượng , kích thước tùy ý và thuật toán băm cho các văn bản đầu ra có kích thước cố định là 128bit với thuật toán dòng MD, 160 bit với dòng SHA.

Như vậy, thông điệp đầu vào với kích thước tùy ý sẽ được thu gọn thành văn bản đại diện có kích thước cố định 128bit hoặc 160bit. Với mỗi thông điệp đầu vào chỉ có thể tính ra được một văn bản đại diện duy nhất. Giống như vân tay người,hai thông điệp khác nhau sẽ có hai văn bản đại diện khác nhau. Khi đã có văn bản đại diện duy nhất ta áp dụng sơ đồ ký số ký trên văn bản đó.

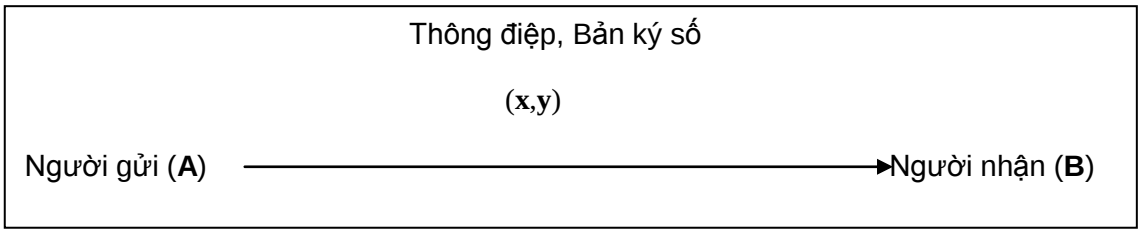
Cơ chế gửi thông tin sử dụng hàm băm trợ giúp cho chữ ký số được mô tả theo các hình sau :



Hình 3.4a : Băm thông điệp



Hình 3.4b: Ký đại diện trên thông điệp.



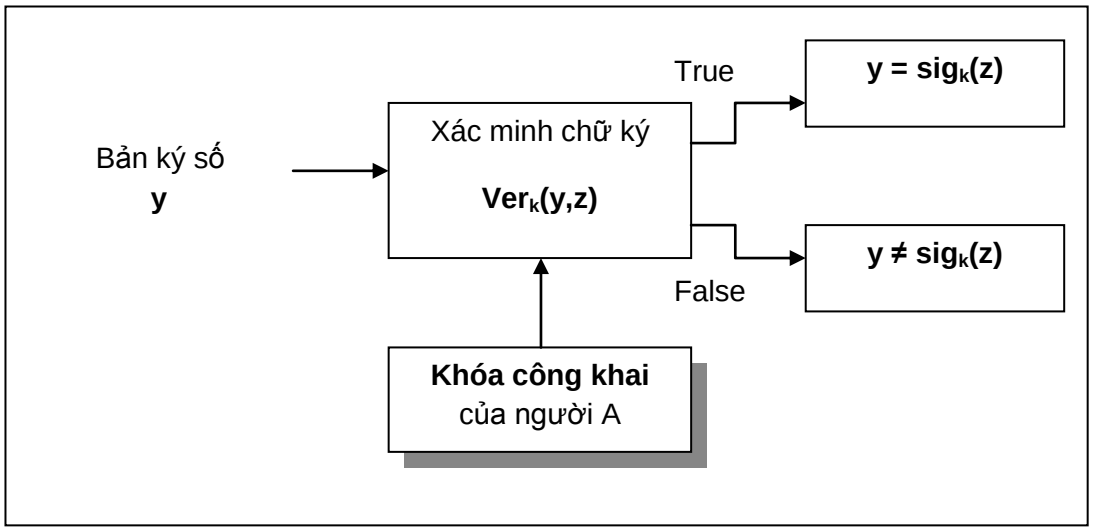
Hình 3.4c: Truyền dữ liệu thông tin cần gửi

Người gửi A muốn gửi thông điệp x. Thực hiện các bước:

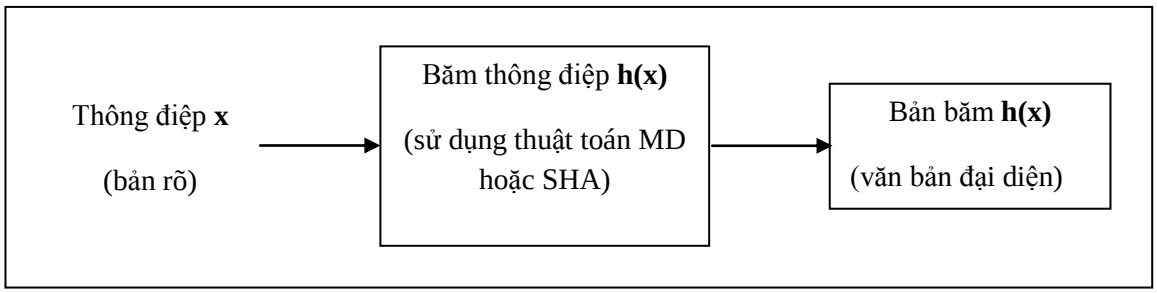
1. Băm thông điệp x, nhận được văn bản đại diện z =h(x).
2. Kí số lên văn bản đại diện z bằng khóa bí mật thu được bản ký số $y = sig^{k}_{1}(z)$.
3. Gửi x,y cho người nhận.

Người nhận B khi nhận được x,y. Thực hiện các bước:

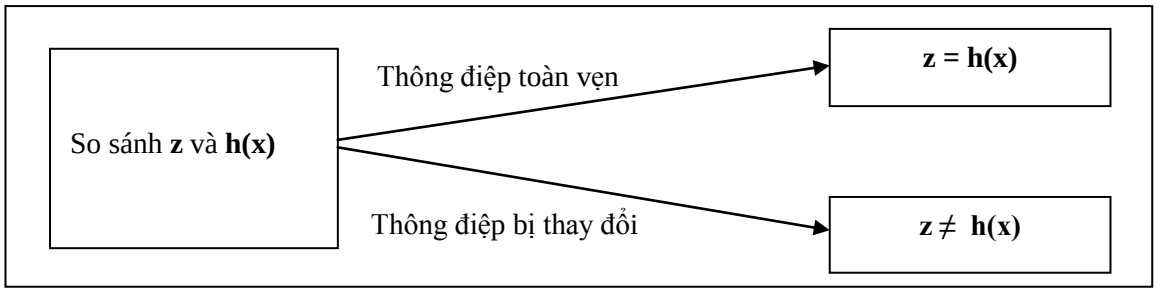
1. Kiểm tra chữ ký xem có phải của A đã gửi cho hay không bằng khóa công khai của A thu được z.
2. Dùng thuật toán băm như A đã dùng để băm thông điệp x thu được h(x).
3. So sánh z với h(x), nếu giống nhau thì thông điệp của A gửi và thông điệp x còn nguyên vẹn, nếu khác nhau thì ngược lại.



Hình 3.5a: Xác minh chữ ký.



Hình 3.5b: Băm thông điệp x di kèm.



Hình 3.5c: Kiểm tra tính toàn vẹn.

Hàm băm đã trợ giúp cho các sơ đồ ký số nhằm giảm dung lượng của dữ liệu cần thiết để truyền qua mạng tương đương với việc giảm thời gian truyền tin qua mạng.

Hàm băm được ứng dụng rất nhiều trong vấn đề an toàn thông tin trên đường truyền vì khi kết hợp hàm băm với chữ ký số để tạo ra một loại chữ ký điện tử vừa an toàn mà còn có thể dùng để kiểm tra tính toàn vẹn của thông tin.

*** Một số hàm băm thường gặp:**

MD5(Message Digest): Độ dài 128 bit, được sử dụng rộng rãi.

SHA(Secure Hash Algorithm): Độ dài 160bit, ít dùng hơn MD5.

3.3.4. Các loại chữ ký số

Chữ ký số được chia thành hai loại là chữ ký khôi phục thông điệp và chữ ký không thể khôi phục thông điệp.

3.3.4.1. Chữ ký khôi phục thông điệp

Thông điệp gốc có thể khôi phục được từ chính bản thân chữ ký. Loại này thường được dùng để ký vào các thông điệp ngắn.

*** Thuật toán sinh chữ ký và xác nhận chữ ký**

Sinh chữ ký trên thông điệp **m**:

- Chọn hàm băm h, tạo đại diện thông điệp của m là **m**’ = h(**m**).
- Chọn khóa ký k ϵ **K**(khóa bí mật), tính chữ ký trên **m**’ là s = Sig_k(**m**’).

Xác nhận chữ ký s:

- Chọn hàm băm h, tạo đại diện thông điệp của m là **m**’ = h(**m**).
- Với khóa kiểm tra chữ ký kk (khóa công khai), khôi phục đại diện thông điệp gốc được **m**’’.
- Chữ ký đúng nếu **m**’ = **m**’’.

3.3.4.2. Chữ ký không thể khôi phục thông điệp

Thông điệp ban đầu không thể khôi phục từ chữ ký.

*** Thuật toán sinh chữ ký và xác nhận chữ ký**

Sinh chữ ký trên thông điệp **m**:

- Chọn hàm băm h, tạo đại diện thông điệp của **m** là **m**’ = h(**m**).
- Chọn khóa ký k ϵ **K**(khóa bí mật), tính chữ ký trên m’ là s = Sig_k(**m**’).

Xác nhận chữ ký s:

- Chọn hàm băm h, tạo đại diện thông điệp của **m** là **m**’ = h(**m**).
- Với khóa kiểm tra chữ ký kk (khóa công khai), Tính u = Ver_{kk}(m’,s).
- Chữký đúng nếu u = True.

3.3.4.3. Chức năng của chữ ký số

Chữ ký số có thể thực hiện được hai chức năng bảo toàn tài liệu là bảo toàn và xác thực.

Bảo toàn: Nếu có chữ ký số trên tài liệu, khi kẻ gian sửa đổi tài liệu thì chữ ký cũng sẽ bị thay đổi và khác với chữ ký của tài liệu gốc. Từ đó người dùng sẽ phát hiện ra có sự thay đổi trong tài liệu.

Xác thực: Khi có chữ ký trên tài liệu, chữ ký dùng để chứng minh nguồn gốc của tài liệu,kẻ gian khó có thể tạo ra chữ ký số giống chữ ký số ban đầu.

3.3.5. Phương pháp Bảo toàn thông tin bằng chữ ký số và hàm băm

3.3.5.1. Dùng chữ ký số để bảo toàn thông tin tài liệu

Người gửi A cần chuyển tài liệu x tới người nhận B trên mạng công khai. Nếu dùng chữ ký số để bảo toàn x thì A phải chuyển cả x và chữ ký trên x là s cho B. Như vậy B sẽ nhận cặp tin(tài liệu, chữ ký).

Nếu kẻ gian thay đổi nội dung của x hay dùng tài liệu y thay x thì khi B kiểm tra chữ ký của A, chắc chắn chữ ký s là sai vì nội dung x đã bị thay đổi.

3.3.5.2. Dùng hàm băm để bảo toàn thông tin tài liệu

Hàm băm h là hàm một chiều với các đặc tính sau:

- Với mỗi tài liệu x chỉ thu được duy nhất một giá trị băm z= h(x).
- Nếu dữ liệu x bị thay đổi dù chỉ là 1bit dữ liệu thành x’ thì giá trị băm h(x’) ≠ h(x). Điều này có nghĩa hai thông điệp khác nhau thì giá trị băm của chúng cũng khác nhau.

  Dựa vào đặc điểm trên của hàm băm người ta bảo toàn tài liệu như sau:

  Người gửi A cần chuyển tài liệu x tới người nhận B trên mạng công khai. Nếu dùng hàm băm để bảo toàn x thì A phải chuyển x và cả giá trị băm trên x là z cho B. Như vậy B sẽ nhận được cặp tin (tài liệu,tài liệu đại diện). Sau đó B dùng thuật toán băm như A đã dùng băm lại x và nhận được giá trị băm z’. So sánh nếu z’ ≠ z thì chắc chắn x đã bị thay đổi trên đường truyền và ngược là thì x được bảo toàn.

CHƯƠNG 4. THỬ NGHIỆM CHƯƠNG TRÌNH

4.1. CHƯƠNG TRÌNH MÃ HÓA RSA

4.1.1. Các thành phần của chương trình

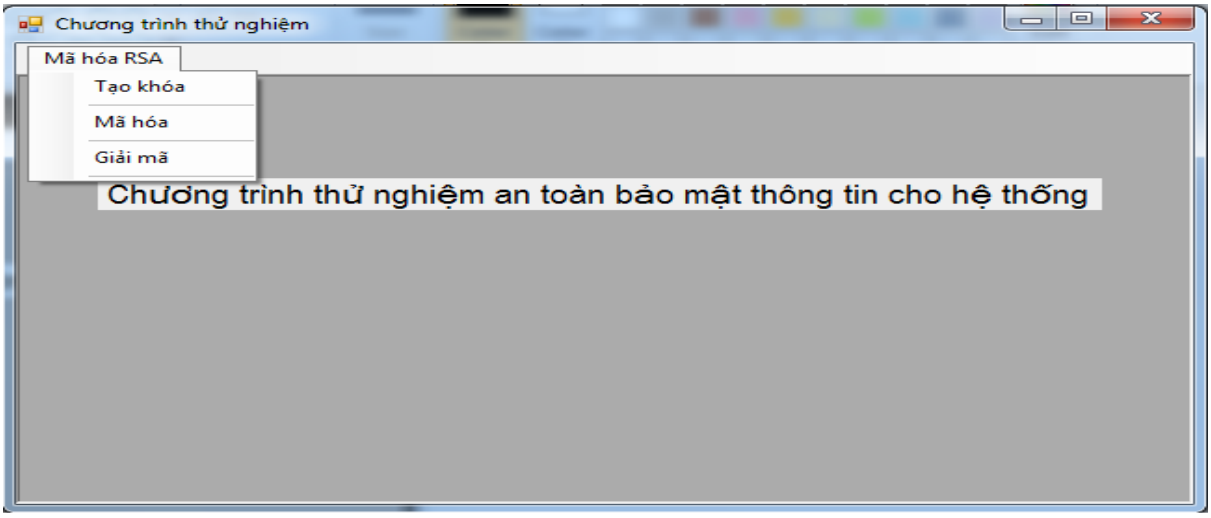
- Mã hóa tài liệu

- Giải mã tài liệu

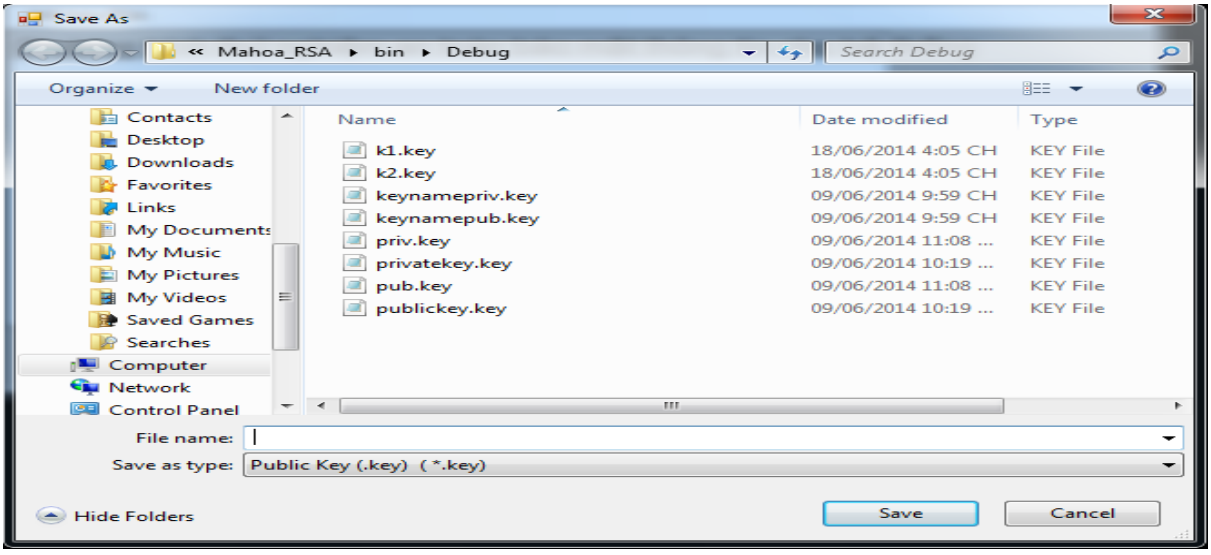
Hướng dẫn sử dụng chương trình

Tạo khóa

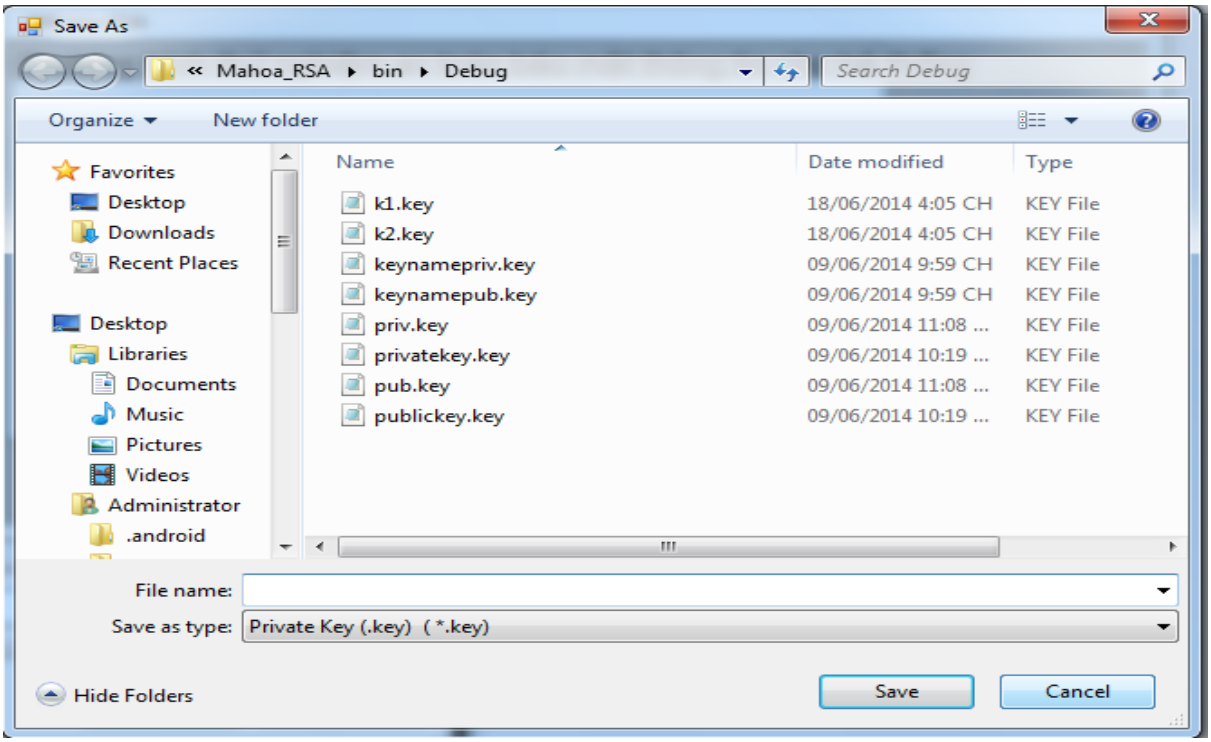
Bước 1: Từ giao diện chương trình chính, chọn chương trình Mã hóa RSA.



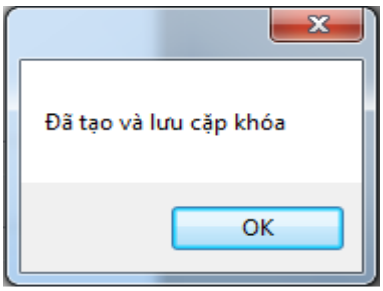
Bước 2: Tạo cặp khóa cho việc mã hóa và giải mã. Chọn vị trí lưu cặp khóa vừa tạo.



Lưu khóa công khai với tên publickey

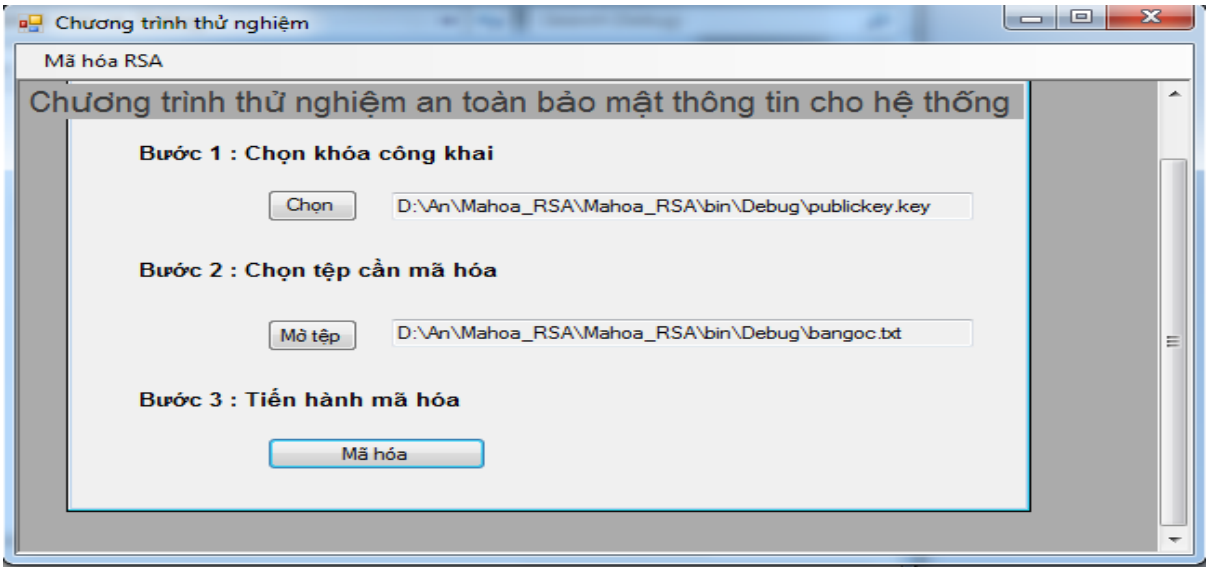


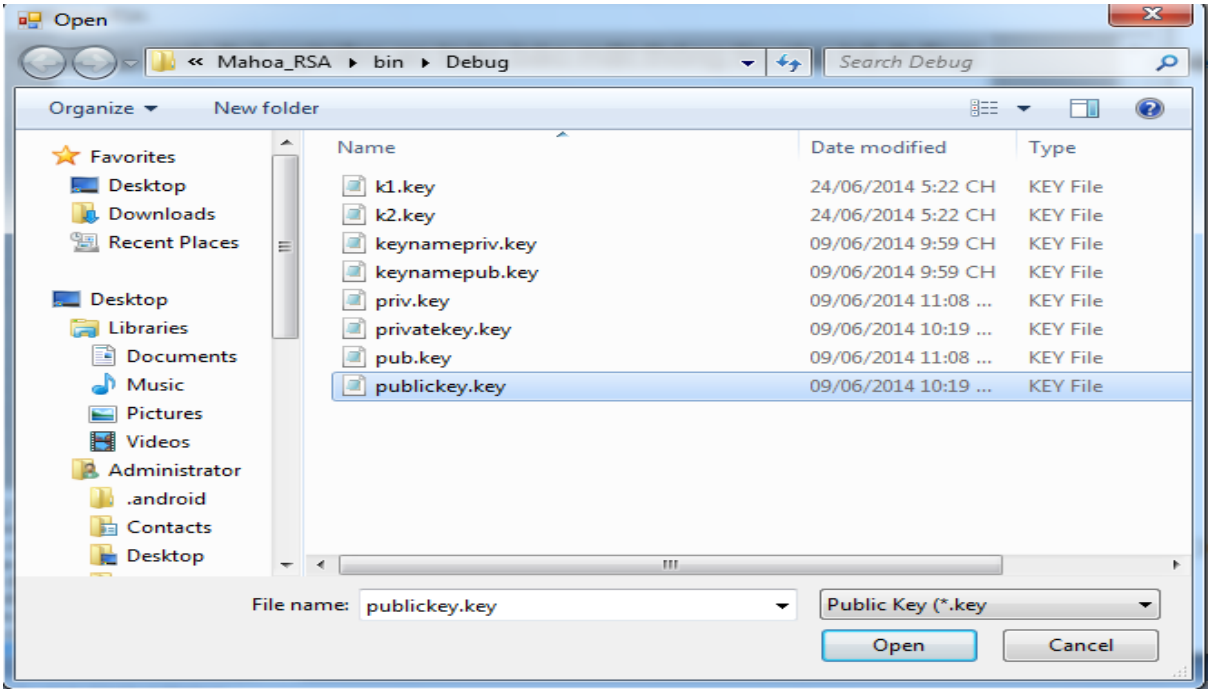
Lưu khóa bí mật với tên privatekey



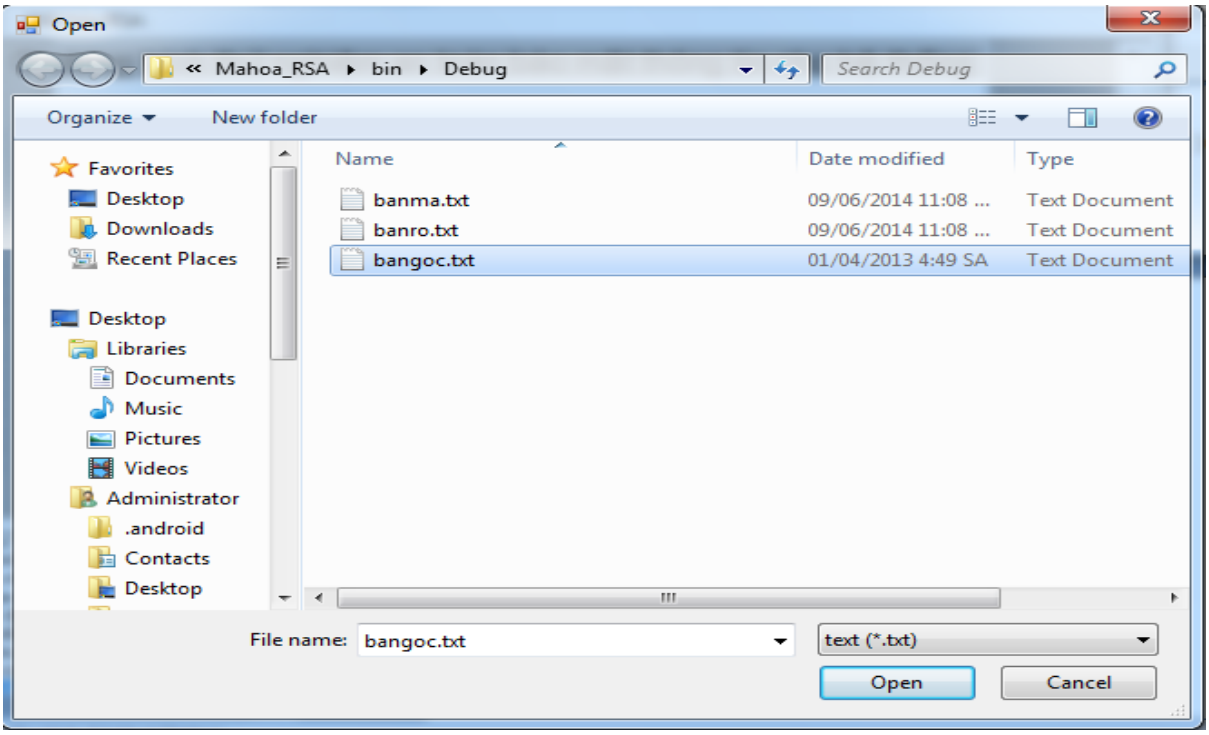
Mã hóa

Bước 1: Chọn khóa công khai và tài liệu để tiến hành mã hóa.

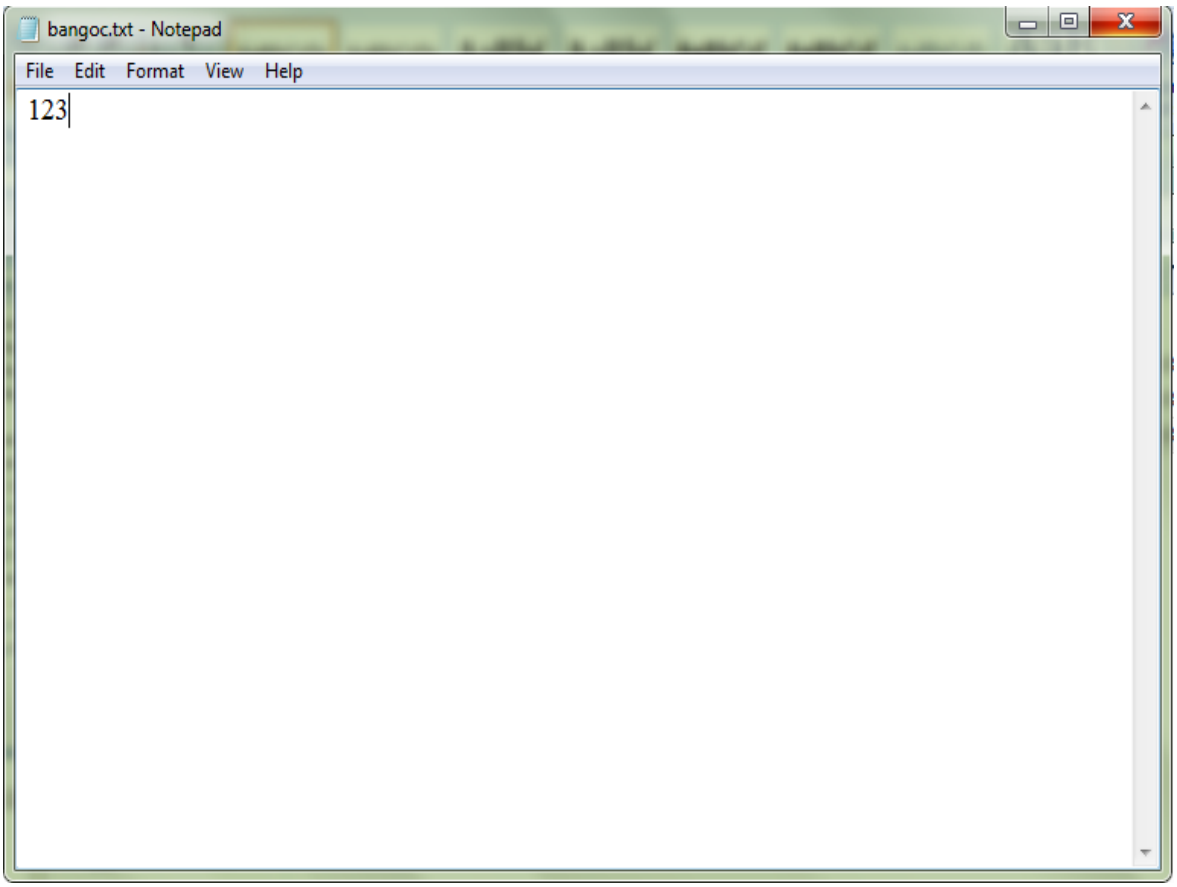




Chọn khóa công khai để mã hóa

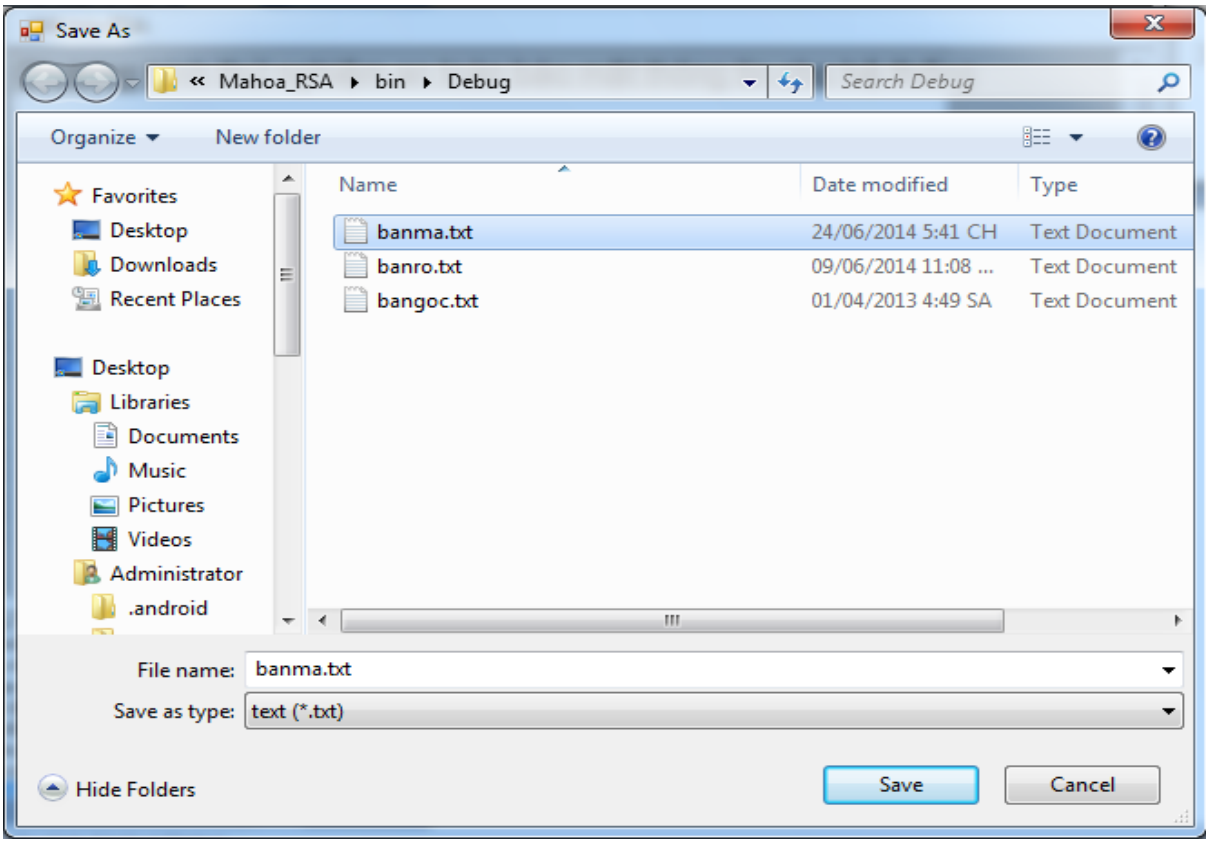


Chọn tài liệu cần mã hóa

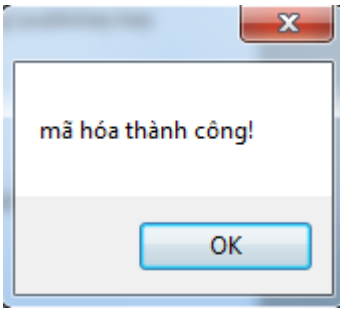


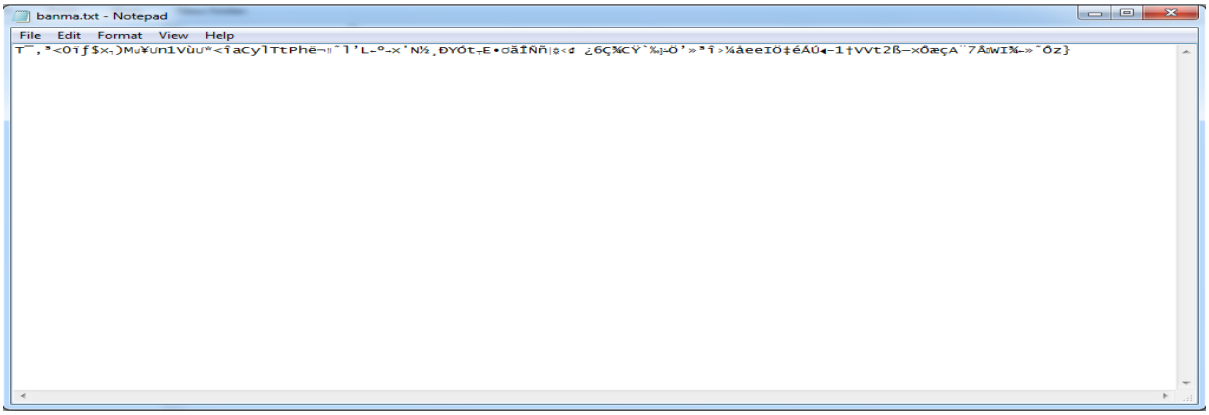
Nội dung tài liệu gốc

Bước 2: Tiến hành mã hóa và lưu tài liệu đã mã hóa



Lưu tài liệu đã được mã hóa.

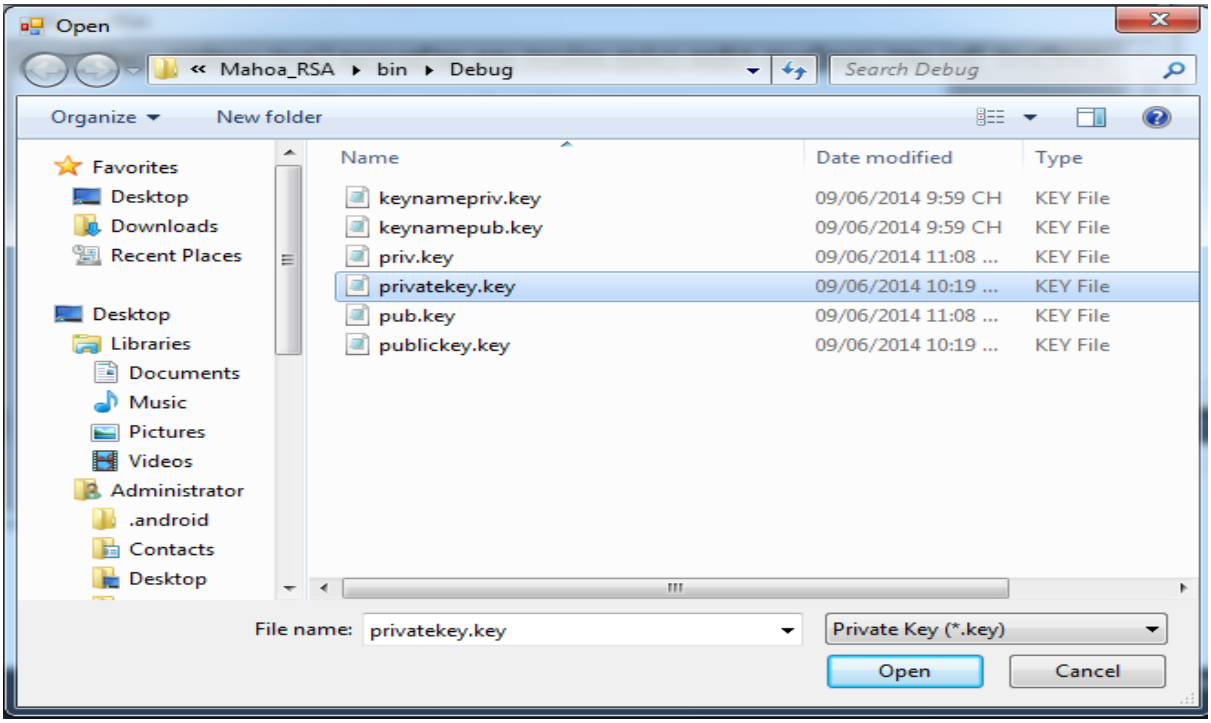




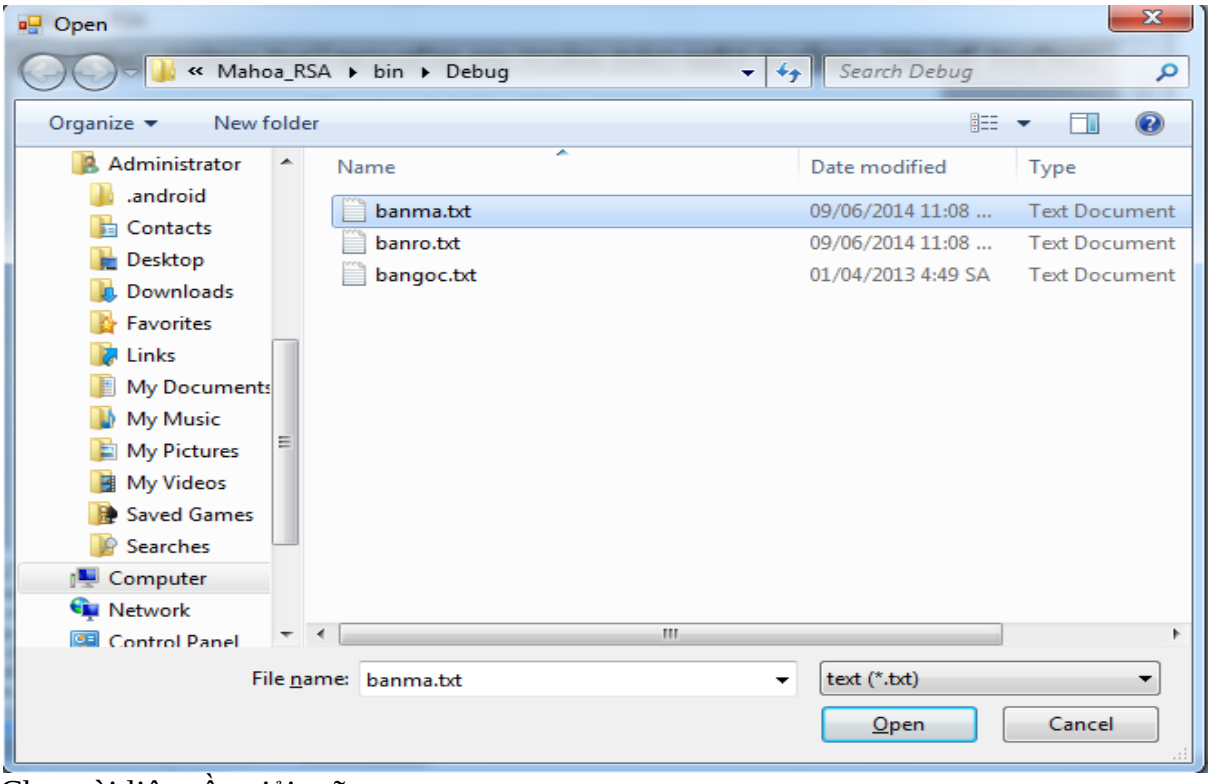
Kết quả tài liệu sau khi mã hóa.

Giải mã

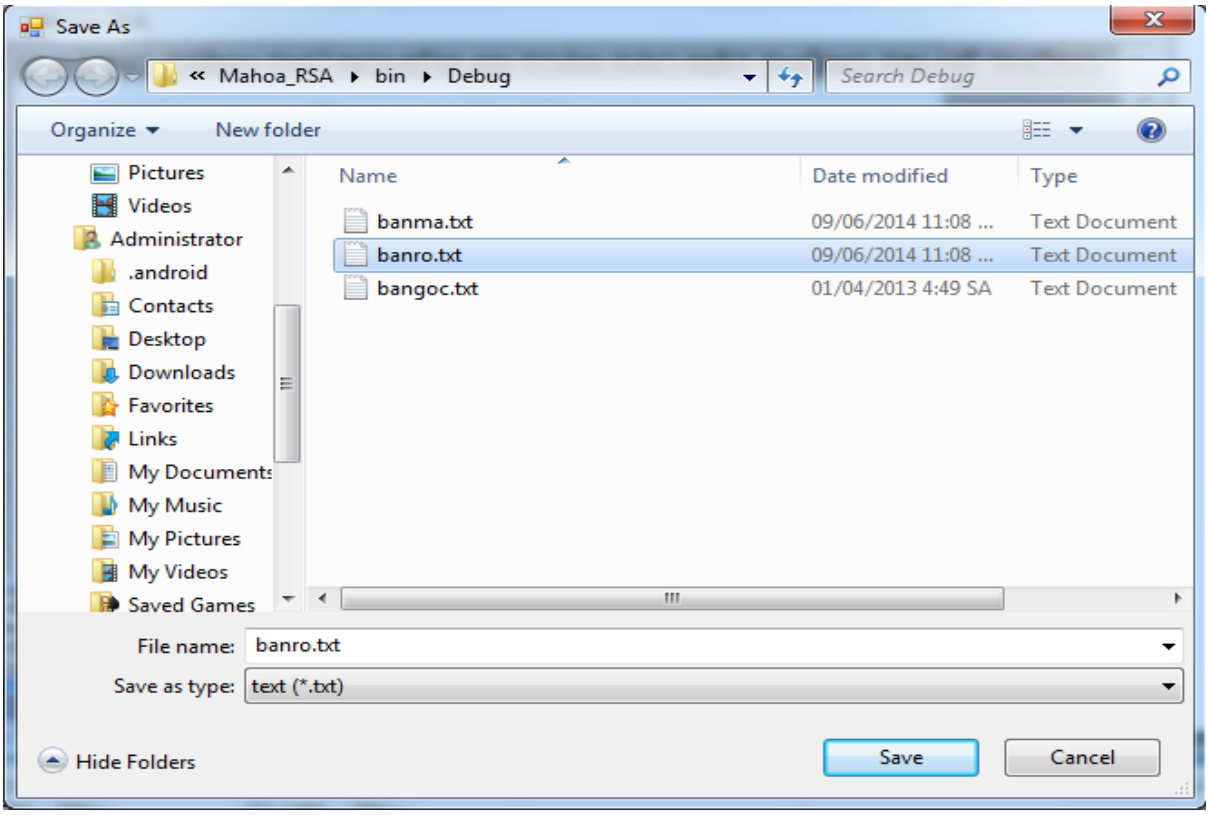
Bước 1: Chọn khóa bí mật và tài liệu cần giải mã.



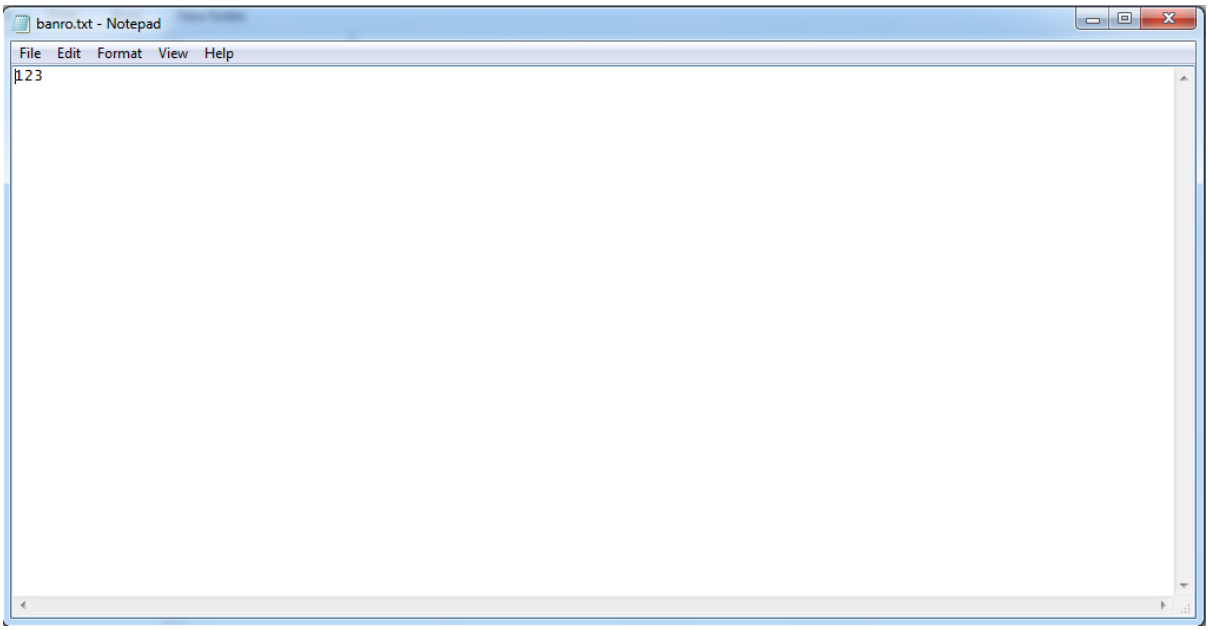
Chọn khóa bí mật để giải mã.



Chọn tài liệu cần giải mã.



Lưu tài liệu vừa giải mã.



Tài liệu sau khi được giải mã.

KẾT LUẬN

Việc ứng dụng công nghệ thông tin vào hành chính điện tử đã góp phần đẩy nhanh quá trình cải cách thủ tục hành chính.Ứng dụng công nghệ thông tin trong hoạt động cung ứng dịch vụ hành chính trực tuyến đã cải thiện đáng kể năng suất , chất lượng và hiệu quả. Từ đó tạo ra bước tiến mới của Nhà nước ta trong các mối quan hệ với công dân và tổ chức, giúp tiết kiệm thời gian thực hiện thủ tục hành chính và xử lý hồ sơ đúng hạn, đáp ứng được sự mong đợi của người dân cũng như các doanh nghiệp.

Hiện nay, Nhà nước đang quan tâm và khuyến khích các đơn vị hành chính cũng như tổ chức, cá nhân ứng dụng giao dịch điện tử trong các giao dịch hành chính để góp phần xây dựng hệ thống hành chính trong sạch hiệu quả. Để có thể đạt được điều này thì Nhà nước cần có những chủ trương, chính sách xây dựng hệ thống hạ tầng cũng như việc đảm bảo an toàn thông tin trong giao dịch hành chính điện tử.

Nội dung của đồ án này là:

1, Tìm hiểu về hành chính điện tử, cơ sở hạ tầng công nghệ thông tin đảm bảo an toàn thông tin trong giao dịch điện tử,một số bài toán đảm bảo an toàn thông tin trong giao dịch hành chính điện tử.

2, Thử nghiệm chương trình mã hóa thông tin.

Dự kiến hướng đi tiếp theo:

Tìm hiểu và xây dựng các chương trình ứng dụng phục vụ cho công tác đảm bảo an toàn và bảo mật thông tin cho hệ thống. Mở rộng phạm vi ứng dụng đối tượng nghiên cứu ra ngoài các khối cơ quan hành chính.

Do thời gian có hạn cũng như phạm vi kiến thức quanh đề tài khá rộng nên trong đồ án này còn nhiều thiếu sót cũng như chưa bao quát hết được các vấn đề liên quan về đề tài. Em mong nhận được sự chỉ bảo, đóng góp của các thầy cô và bạn bè cho em có thể hoàn thiện hơn về mặt kiến thức cũng có những hướng đi để đề tài sớm có thể ứng dụng vào thực tiễn.

CÁC TÀI LIỆU THAM KHẢO

1, Luật giao dịch điện tử ngày 1/3/2006 Ủy ban Khoa học công nghệ - môi trường Quốc hội.

2, Lê Hồng Hà; An toàn bảo mật thông tin trong giao dịch điện tử.

3, Báo cáo hiện trạng triển khai và định hướng ứng dụng công nghệ thông tin trong các hoạt động cả cơ quan Nhá nước của Cục úng dụng CNTT- Bộ TTTT 7/2012.

4, Lý thuyết mật mã và an toàn thông tin của thầy Phan Đình Diệu - NXB ĐHQG Hà nội 2002.

5, Luận văn nghiên cứu về an toàn thông tin trong hành chính điện tử của kỹ sư tin học Nguyễn Đăng Khoa.

6. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, Handbook of APPLIED CRYPTOGRAPHY, CRC Press, Boca Raton, New York, London , Tokyo- 1999.

7. Stinson, D.R. Cryptography: Theory and Practice. CRC Press, Inc. 1995.