**TRƯỜNG ĐẠI HỌC TÀI NGUYÊN VÀ MÔI TRƯỜNG HÀ NỘI**

**KHOA CÔNG NGHỆ THÔNG TIN**

🙧🙥🙥🙥

****

**NGHIÊN CỨU THUẬT TOÁN RSA VÀ XÂY DỰNG ỨNG DỤNG CHỮ KÝ ĐIỆN TỬ CHO PHIẾU THU CỦA CÔNG TY CỔ PHẦN HOSCO**

**Hà Nội – Năm 2016**

**TRƯỜNG ĐẠI HỌC TÀI NGUYÊN VÀ MÔI TRƯỜNG HÀ NỘI**

**KHOA CÔNG NGHỆ THÔNG TIN**

🙧🙥🙥🙥

****

**NGÔ THỊ B**

**NGHIÊN CỨU THUẬT TOÁN RSA VÀ XÂY DỰNG ỨNG DỤNG CHỮ KÝ ĐIỆN TỬ CHO PHIẾU THU CỦA CÔNG TY CỔ PHẦN HOSCO**

**Chuyên ngành: Công nghệ thông tin**

**Mã ngành: D480201**

**NGƯỜI HƯỚNG DẪN: ThS Nguyễn Văn A**

**Hà Nội – Năm 2016**

# LỜI CAM ĐOAN

Những nội dung trong đồ án tốt nghiệp này là thành quả từ sự nghiên cứu và được thực hiện dưới sự trực tiếp hướng dẫn của giảng viên hướng dẫn ThS. Nguyễn Văn Hách.

Đồ án được thực hiện hoàn toàn mới, là thành quả của riêng em, không sao chép theo bất cứ đồ án tương tự nào. Mọi sự tham khảo sử dụng trong đồ án đều được trích dẫn các nguồn tài liệu trong báo cáo và danh mục tài liệu tham khảo.

Mọi sao chép không hợp lệ, vi phạm quy chế của nhà trường, em xin hoàn toàn chịu trách nhiệm

Sinh viên thực hiện

 **Nguyễn Văn A**

# LỜI CẢM ƠN

 Để hoàn thành được đề tài đồ án tốt nghiệp này, trước hết em xin gửi lời cảm ơn chân thành nhất đến các Cán bộ Giảng viên Khoa Công nghệ Thông tin, các cán bộ giảng viên trong Trường Đại học Tài nguyên Môi trường Hà Nội đã tận tình giảng dạy và truyền đạt kiến thức cho em. Đồng thời em xin gửi lời cảm ơn đặc biệt về sự chỉ dạy, hướng dẫn tận tình của ThS. Nguyễn Văn Hách đã luôn tận tình hướng dẫn, giúp đỡ em trong suốt thời gian thực hiện đồ án.

Em cũng xin gửi lời cảm ơn tới Khoa Công nghệ Thông tin – Trường Đại Học Tài nguyên Môi trường Hà Nội đã luôn quan tâm và tạo điều kiện giúp em hoàn thành đề tài đồ án tốt nghiệp này. Ngoài ra, em xin cảm ơn những người bạn đã giúp đỡ và trao đổi thêm nhiều thông tin về đề tài trong quá trình thực hiện đề tài này.

Cuối cùng em vô cùng biết ơn gia đình và bạn bè, những người đã luôn luôn ở bên cạnh em, động viên, chia sẻ với em trong suốt thời gian thực đề tài đồ án tốt nghiệp “**Nghiên cứu thuật toán RSA và xây dựng ứng dụng chữ ký điện tử cho phiếu thu của Công ty Cổ phần HOSCO**”.

Do kiến thức còn hạn chế, bài báo cáo của em không tránh khỏi những sai sót. Rất mong nhận được những lời góp ý từ quý Thầy cô để đồ án tốt nghiệp của em được hoàn thiện và giúp em có thêm những kinh nghiệm quý báu.

Cuối cùng, em xin kính chúc các thầy cô giảng viên trường Đại học Tài nguyên và Môi trường Hà Nội nói chung, các thầy cô khoa công nghệ thông tin nói riêng dồi dào sức khỏe và thành công trong sự nghiệp cao quý.

 *Hà Nội, tháng 5 năm 2016*

 Sinh viên thực hiện

 **Ngô Thu Thủy**

MỤC LỤC

[LỜI CAM ĐOAN](#_Toc452998735)

[LỜI CẢM ƠN](#_Toc452998736)

[MỤC LỤC](#_Toc452998737)

[DANH MỤC CÁC CHỮ VIẾT TẮT](#_Toc452998738)

[DANH MỤC CÁC BẢNG](#_Toc452998739)

[DANH MỤC HÌNH ẢNH](#_Toc452998740)

[MỞ ĐẦU 1](#_Toc452998741)

[CHƯƠNG 1: GIỚI THIỆU VỀ HỆ MẬT MÃ HỌC 3](#_Toc452998742)

[1.1. Các khái niệm cơ sở 3](#_Toc452998743)

[*1.1.1.* *Khái niệm về mật mã học* 3](#_Toc452998744)

[*1.1.2.* *Các khái niệm cơ bản* 3](#_Toc452998745)

[*1.1.3.* *Các tính chất của hệ mật* 4](#_Toc452998746)

[1.2. Lịch sử phát triển 5](#_Toc452998748)

[1.3. Phân loại hệ mật mã học 6](#_Toc452998749)

[*1.3.1* *Mật mã cổ điển* 6](#_Toc452998750)

[*1.3.2* *Mật mã hiện đại* 9](#_Toc452998751)

[CHƯƠNG 2: GIỚI THIỆU VỀ CHỮ KÝ SỐ 13](#_Toc452998752)

[2.1. Khái niệm về chữ ký số 13](#_Toc452998753)

[2.2. Kiến trúc của chữ ký số 14](#_Toc452998754)

[*2.2.1.* *Tính chất của chữ ký số* 14](#_Toc452998755)

[*2.2.2.* *Kiến trúc của chữ ký số* 15](#_Toc452998756)

[*2.2.3.* *Sơ đồ hệ thống chữ ký số* 17](#_Toc452998757)

[2.3. Vị trí, vai trò của chữ ký số trong thực tế 18](#_Toc452998759)

[2.4. Giới thiệu về hàm băm và tính chất của hàm băm 20](#_Toc452998760)

[*2.4.1.* *Tổng quan về hàm băm* 20](#_Toc452998761)

[*2.4.2.* *Tính chất của hàm băm* 23](#_Toc452998762)

[2.5. Một số hàm băm mật mã học 24](#_Toc452998763)

[*2.5.1.* *Danh sách các hàm băm mật mã học* 24](#_Toc452998764)

[*2.5.2.* *Hàm băm MD4* 25](#_Toc452998765)

[*2.5.3.* *Hàm băm MD5* 26](#_Toc452998766)

[*2.5.4.* *Hàm băm SHA-1* 28](#_Toc452998767)

[CHƯƠNG 3: CƠ SỞ LÝ THUYẾT VÀ ỨNG DỤNG RSA TRONG XÂY DỰNG CHỮ KÝ SỐ 30](#_Toc452998768)

[3.1. Tổng quan về hệ mật mã RSA 30](#_Toc452998769)

[*3.1.1.* *Lịch sử của chữ ký số RSA* 30](#_Toc452998770)

[*3.1.2.* *Hoạt động của hệ mật mã RSA* 31](#_Toc452998771)

[3.2. Kiến trúc và giải thuật của hệ mật RSA 32](#_Toc452998772)

[*3.2.1.* *Mô hình kiến trúc của hệ mật RSA* 32](#_Toc452998773)

[*3.2.2.* Giải thuật của thuật toán RSA 35](#_Toc452998775)

[3.3. Độ an toàn và bảo mật của hệ mật RSA 37](#_Toc452998776)

[3.4. Giới thiệu về lược đồ chữ ký số RSA 38](#_Toc452998777)

[*3.4.1.* *Thuật toán khởi tạo tham số của hệ thống* 38](#_Toc452998778)

[*3.4.2.* *Thuật toán sinh khóa* 38](#_Toc452998780)

[*3.4.3.* *Thuật toán sinh chữ ký* 39](#_Toc452998782)

[*3.4.4.* *Thuật toán xác thực chữ ký số* 39](#_Toc452998783)

[3.5. Một số khái niệm toán học được sử dụng trong RSA 40](#_Toc452998784)

[CHƯƠNG 4: XÂY DỰNG CHỮ KÝ SỐ TRONG PHIẾU THU ĐIỆN TỬ TẠI CÔNG TY CỔ PHẦN HOSCO 42](#_Toc452998785)

[4.1. Hiện trạng thực tế đối với vấn đề in ấn phiếu thu tại đơn vị 42](#_Toc452998786)

[4.2. Phân tích thiết kế hệ thống 43](#_Toc452998787)

[*4.2.1.* *Sơ đồ usecase tổng quát* 43](#_Toc452998788)

[*4.2.2.* *Mô hình usecase phân rã chức năng* 44](#_Toc452998789)

[*4.2.3.* *Biểu đồ tuần tự của hệ thống* 46](#_Toc452998790)

[*4.2.4.* *Biểu đồ hoạt động của hệ thống* 52](#_Toc452998791)

[4.3. Xây dựng giao diện và chương trình 57](#_Toc452998792)

[*4.3.1.* *Tổng quan về ngôn ngữ lập trình C sharp* 57](#_Toc452998793)

[*4.3.2.* *Một số hàm sử dụng trong chương trình* 59](#_Toc452998795)

[*4.3.3.* *Quy trình hoạt động của phần mềm* 61](#_Toc452998796)

[*4.3.4.* *Giao diện của chương trình* 62](#_Toc452998797)

[KẾT LUẬN VÀ KIẾN NGHỊ 70](#_Toc452998798)

[TÀI LIỆU THAM KHẢO 72](#_Toc452998799)

# DANH MỤC CÁC CHỮ VIẾT TẮT

|  |  |  |
| --- | --- | --- |
| **Chữ viết tắt** | **Tên tiếng anh** | **Nghĩa tiếng việt** |
| RSA |  | Viết theo 3 chữ cái đầu của tên ba tác giả Rivest– Shamir - Adleman |
| C# |  | Ngôn ngữ lập trình C Sharp |
| DES | Data Encryption Standard | Tiêu chuẩn mã hóa dữ liệu |
| PKI | Public Key Infrastructure | Hạ tầng khóa công khai |
| IBM | International Bussiness Machines | Tập đoàn công nghệ máy tính đa quốc gia |
| MD4 | Message – Digest Algorithm 4 | Giải thuật tiêu hóa thông tin 4 |
| MD5 | Message – Digest Algorithm 5 | Giải thuật tiêu hóa thông tin 5 |
| MIT | Massachusetts Institute of Technology | Viện công nghệ Massachusetts |
| SHA | Secure Hash Algorithm | Thuật giải băm an toàn |
| VPN | Virtual Private Network | Công nghệ mạng riêng ảo |
| DSA | Digital Signature Algorithm | Giải thuật chữ ký số |
| UCLN |  | Ước chung lớn nhất |

**DANH MỤC CÁC BẢNG**

[Bảng 1.1 So sánh ưu, nhược điểm của mã hóa đối xứng và mã hóa bất đối xứng 12](#_Toc452627357)

[Bảng 2.1 Danh sách các hàm băm mật mã học 24](#_Toc451977675)

**DANH MỤC HÌNH ẢNH**

[Hình 1.1 Nguyên tắc của mật mã Caesar 7](#_Toc451463507)

[Hình 2.1 Quá trình ký và xác nhận chữ ký 16](#_Toc451463511)

[Hình 2.2 Ví dụ về hàm băm 21](#_Toc451463512)

[Hình 2.3 Mô hình quá trình thực hiện trong 1 vòng của MD5 27](#_Toc451463513)

[Hình 3.1 Quá trình gửi và nhận của Bob và Alice 31](#_Toc451463516)

[Hình 3.2 Mô tả các bước tạo khóa RSA 32](#_Toc451463517)

[Hình 3.3 Quá trình xác nhận khóa RSA 33](#_Toc451463518)

[Hình 3.4 Sơ đồ giải thuật hệ mật mã RSA 35](#_Toc451463519)

[Hình 4.1 Mô hình use-case tổng quát của hệ thống phần mềm 44](#_Toc453013991)

[Hình 4.2 Sơ đồ Usecase phân rã chức năng tạo khóa 45](#_Toc453013992)

[Hình 4.3 Sơ đồ Usecase phân rã chức năng tạo chữ ký và ký 45](#_Toc453013993)

[Hình 4.4 Sơ đồ Usecase phân rã chức năng xác nhận chữ ký và in phiếu thu 46](#_Toc453013994)

[Hình 4.5 Biểu đồ tuần tự thực hiện chức năng đăng nhập hệ thống 47](#_Toc453013995)

[Hình 4.6 Biểu đồ tuần tự chức năng Nhập số nguyên tố 48](#_Toc453013996)

[Hình 4.7 Biểu đồ tuần tự chức năng Tạo khóa 49](#_Toc453013997)

[Hình 4.8 Biểu đồ tuần tự chức năng Tạo chữ ký và ký phiếu thu 50](#_Toc453013998)

[Hình 4.9 Biểu đồ tuần tự chức năng chứng thực chữ ký 51](#_Toc453013999)

[Hình 4.10 Biểu đồ hoạt động thực hiện chức năng đăng nhập 52](#_Toc453014000)

[Hình 4.11 Biểu đồ hoạt động thực hiện chức năng nhập số nguyên tố 53](#_Toc453014001)

[Hình 4.12 Biểu đồ hoạt động thực hiện chức năng tạo khóa 54](#_Toc453014002)

[Hình 4.13 Biểu đồ hoạt động thực hiện chức năng tạo chữ ký và ký phiếu thu 55](#_Toc453014003)

[Hình 4.14 Biểu đồ hoạt động thực hiện chứng thực chữ ký và in phiếu thu 56](#_Toc453014004)

[Hình 4.15 Giao diện form đăng nhập 63](#_Toc453014005)

[Hình 4.16 Giao diện chính của chương trình 63](#_Toc453014006)

[Hình 4.17 Giao diện form đổi mật khẩu 64](#_Toc453014007)

[Hình 4.18 Giao diện form xuất phiếu thu 64](#_Toc453014008)

[Hình 4.19 Giao diện form tạo khóa 65](#_Toc453014009)

[Hình 4.20 Giao diện form ký phiếu thu 66](#_Toc453014010)

[Hình 4.21 Giao diện form xác nhận chữ ký 67](#_Toc453014011)

[Hình 4.22 Phiếu thu khi đã được ký và in 67](#_Toc453014012)

[Hình 4.23 Giao diện form quản lý danh sách nhân viên 68](#_Toc453014013)

[Hình 4.24 Giao diện form danh sách phiếu thu 68](#_Toc453014014)

[Hình 4.25 Giao diện form trang trợ giúp 69](#_Toc453014015)

# MỞ ĐẦU

1. Lý do chọn đề tài

**2. Mục tiêu của đề tài**

**3. Phương pháp nghiên cứu đề tài**

**4. Đối tượng và phạm vi nghiên cứu đề tài**

**-**

# CHƯƠNG 1: GIỚI THIỆU VỀ HỆ MẬT MÃ HỌC

* 1. **Các khái niệm cơ sở**
		1. ***Khái niệm về mật mã học***

Mật mã học (Cryptography) là khoa học nghiên cứu cơ sở lý thuyết và công nghệ để thực hiện việc xây dựng và sử dụng các hệ thống mật mã.

Mật mã học là ngành khoa học ứng dụng toán học vào việc biến đổi thông tin thành một dạng khác nhằm mục đích che dấu nội dung, ý nghĩa thông tin cần mã hóa. Đây là một ngành quan trọng và có nhiều ứng dụng trong đời sống xã hội. Ngày nay, các ứng dụng mã hóa và bảo mật thông tin đang được sử dụng ngày càng phổ biến hơn trong các lĩnh vực khác nhau trên thế giới, từ các lĩnh vực an ninh, quân sự, quốc phòng, cho đến các lĩnh vực dân sự như thương mại điện tử, ngân hàng… Mật mã học hiện nay đang là lĩnh vực được quan tâm và mở rộng với nhiều ứng dụng quan trọng như: chứng thực khóa công khai, chữ ký số, thanh toán điện tử.

* + 1. ***Các khái niệm cơ bản***

- *Tính không thể chối bỏ (Non-repudiation)*: người gửi, người nhận không thể chối bỏ sau khi đã gửi hoặc nhận thông điệp.

* 1. **Lịch sử phát triển**

# CHƯƠNG 2: GIỚI THIỆU VỀ CHỮ KÝ SỐ

* 1. **Khái niệm về chữ ký số**
	2. **Kiến trúc của chữ ký số**
		1. ***Tính chất của chữ ký số***
* **Quá trình kiểm tra chữ ký (Receiver)**

- Thôn**Vị trí, vai trò của chữ ký số trong thực tế**

Internet đang ngày càng phát triển và có vị trí vô cùng quan trọng trong cuộc sống hiện nay, cùng với đó là sự phát triển vượt bậc của công nghệ thông tin. Điều này đã cho phép chúng ta thực hiện những giao dịch điện tử thông qua internet, nhưng tính linh hoạt của internet cũng tạo cơ hội cho “bên thứ ba” có thể thực hiện các hành động bất thường ví dụ như nghe trộm, giả mạo. Để đảm bảo an toàn trong an ninh mạng và trong thương mại điện tử, khái niệm chữ ký số điện tử ra đời.

Với sự phát triển mạnh mẽ của xu thế quốc tế hóa, toàn cầu hóa, việc trao đổi thông tin cũng yêu cầu nhanh gọn, chính xác và đặc biệt là phải an toàn. Từ những khó khăn trong thực tế, công nghệ thông tin cũng như công nghệ mã hóa cũng từ đó mà được phát triển một cách mạnh mẽ. Hiện nay, trên thế giới ở tất cả các nước phát triển cũng như đang phát triển, mạng máy tính đang ngày càng đóng vai trò thiết yếu trong mọi lĩnh vực hoạt động của toàn xã hội. Chính vì vậy mà nhu cầu bảo mật thông tin cũng được đặt lên hàng đầu.

Điển hình là việc mã hóa bảo mật các thông tin, dùng chữ ký số xác thực email trao đổi thông tin, kiểm soát truy cập vào các sàn thương mại điện tử,… mà vai trò chủ yếu là chữ ký số điện tử.

* Chữ ký số được sử dụng trong các giao dịch thư điện tử, ký vào các email để xác thực danh tính người gửi.
* Sử dụng chữ ký số này để mua bán hàng trực tuyến, đầu tư chứng khoán trực tuyến, có thể chuyển tiền ngân hàng, thanh toán trực tuyến mà không sợ bị đánh cắp tiền như với các tài khoản VISA, Master.
* Sử dụng chữ ký số với các ứng dụng quản lý của tổ chức / doanh nghiệp với mức độ tin cậy, bảo mật và xác thực cao hơn rất nhiều.
* Dùng chữ ký số để ký hợp đồng với các đối tác hoàn toàn trực tuyến trên mạng mà không cần ngồi trực tiếp với nhau, chỉ cần ký vào file hợp đồng và gửi qua email.
* Sử dụng với các ứng dụng chính phủ điện tử, các cơ quan nhà nước trong tương lai sẽ làm việc với nhân dân hoàn toàn trực tuyến và một cửa. Khi cần làm thủ tục hành chính hay xin một xác nhận của cơ quan nhà nước chỉ cần ngồi ở nhà khai vào mẫu và ký số vào để gửi là xong…

Trên thực tế, chữ ký số không chỉ được thực hiện cho các giao dịch điện tử trên mạng internet mà còn được thực hiện thông qua hệ thống mạng viễn thông di động. Đặc biệt, hiện nay nhiều nước trên thế giới không chỉ triển khai ứng dụng chữ ký số trên mạng máy tính mà còn áp dụng trên mạng điện thoại di động để thực hiện các giao dịch điện tử. Chữ ký số có thể bao hàm các cam kết gửi bằng email, nhập các số định dạng cá nhân (PIN) vào các máy ATM, ký bằng bút điện tử với thiết bị màn hình cảm ứng tại các quầy tính tiền, chấp nhận các điều khoản người dùng khi cài đặt phần mềm máy tính, ký các hợp đồng điện tử online...

Sự ra đời của chữ ký số ngày càng khẳng định được lợi ích to lớn về chiến lược và kinh tế, đồng thời các vấn đề liên quan đến chữ ký số cũng là những chủ đề quan trọng nhất của mật mã học.

* 1. **Giới thiệu về hàm băm và tính chất của hàm băm**
		1. ***Tổng quan về hàm băm***
* **Hàm băm**

Hàm băm (Hash funtion - ***h***) là giải thuật nhằm sinh ra các giá trị băm tương ứng với mỗi khối dữ liệu (có thể là một chuỗi kí tự, một đối tượng trong lập trình hướng đối tượng, v.v…). Nói cách khác, hàm băm là một hàm toán học chuyển đổi một thông điệp đầu vào có độ dài bất kỳ thành một dãy bit có độ dài cố định (tuỳ thuộc vào thuật toán băm). Dãy bit này được gọi là thông điệp rút gọn (*message digest*) hay giá trị băm (*hash value*), đại diện cho thông điệp ban đầu.

* 1. **Một số hàm băm mật mã học**

# CHƯƠNG 3: CƠ SỞ LÝ THUYẾT VÀ ỨNG DỤNG RSA TRONG XÂY DỰNG CHỮ KÝ SỐ

Trước những nhu cầu về giao dịch an toàn trên mạng Internet ngày nay, những ứng dụng của việc mã hóa công khai ngày càng có vai trò hết sức quan trọng. Một trong những thuật toán mã hóa công khai phổ biến đó là RSA. Thuật toán được ứng dụng rộng rãi cho công nghệ VPN. Chương này sẽ giới thiệu tổng quan về thuật toán RSA và ứng dụng của RSA trong xây dựng chữ ký số. Cụ thể là:

* Giới thiệu chung về hệ mật RSA.
* Kiến trúc và giải thuật của RSA.
* Lược đồ chữ ký số RSA.
* Độ an toàn và bảo mật của hệ mật RSA.
	1. **Tổng quan về hệ mật mã RSA**
		1. ***Lịch sử của chữ ký số RSA***

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

* + 1. *Hoạt động của hệ mật mã RSA*
* **Mục đích của việc xác thực chữ ký**

– Xác thực được người gửi: Các hệ thống mật mã hóa khóa công khai cho phép mật mã hóa văn bản với khóa bí mật mà chỉ có người chủ của khóa biết. Để sử dụng chữ ký số thì văn bản không cần phải được mã hóa mà chỉ cần mã hóa hàm băm của văn bản đó (thường có độ dài cố định và ngắn hơn văn bản). Khi cần kiểm tra, bên nhận thực hiện giải mã (với khóa công khai) để lấy lại hàm băm và kiểm tra với hàm băm của văn bản nhận được. Nếu 2 giá trị này khớp nhau thì bên nhận có thể tin tưởng rằng văn bản xuất phát từ người sở hữu khóa bí mật. Tất nhiên là chúng ta không thể đảm bảo 100% là văn bản không bị giả mạo vì hệ thống vẫn có thể bị phá vỡ. Vấn đề xác thực đặc biệt quan trọng đối với các giao dịch tài chính. Chẳng hạn một chi nhánh ngân hàng gửi một gói tin về trung tâm dưới dạng (a, b), trong đó a là số tài khoản và b là số tiền chuyển vào tài khoản đó. Một kẻ lừa đảo có thể gửi một số tiền nào đó để lấy nội dung gói tin và truyền lại gói tin thu được nhiều lần để thu lợi (tấn công truyền lại gói tin).

– Chống chối bỏ: Trong giao dịch, một bên có thể từ chối nhận một văn bản nào đó là do mình gửi. Để ngăn ngừa khả năng này, bên nhận có thể yêu cầu bên gửi phải gửi kèm chữ ký số với văn bản. Khi có tranh chấp, bên nhận sẽ dùng chữ ký này như một chứng cứ để bên thứ ba giải quyết. Tuy nhiên, khóa bí mật vẫn có thể bị lộ và tính không thể phủ nhận cũng không thể đạt được hoàn toàn.

– Xác thực sự toàn vẹn của thông tin: Cả hai bên tham gia vào quá trình thông tin đều có thể tin tưởng là văn bản không bị sửa đổi trong khi truyền vì nếu văn bản bị thay đổi thì hàm băm cũng sẽ thay đổi và lập tức bị phát hiện. Quá trình mã hóa sẽ ẩn nội dung của gói tin đối với bên thứ 3 nhưng không ngăn cản được việc thay đổi nội dung của nó.

* + 1. **Giải thuật của thuật toán RSA**
	1. **Độ an toàn và bảo mật của hệ mật RSA**
	2. **Giới thiệu về lược đồ chữ ký số RSA**
		1. ***Thuật toán khởi tạo tham số của hệ thống***
	3. **Một số khái niệm toán học được sử dụng trong RSA**

# CHƯƠNG 4: XÂY DỰNG CHỮ KÝ SỐ TRONG PHIẾU THU ĐIỆN TỬ TẠI CÔNG TY CỔ PHẦN HOSCO

Được ứng dụng khá phổ biến hiện nay, phiếu thu điện tử đã giúp nhiều công ty tiết kiệm được khá nhiều chi phí, thời gian trong việc thu tiền, lên sổ sách và nâng cao mức độ chuyên nghiệp trong giao dịch hàng hóa. Công ty cổ phần HOSCO cũng là một công ty kinh doanh các phần mềm bán hàng khác nhau, có số lượng đơn đặt hàng cũng khá lớn, nên hệ thống phiếu thu điện tử là khá cần thiết cho công ty. Chương này sẽ xây dựng ứng dụng chữ ký số trong phiếu thu điện tử tại công ty bằng thuật toán RSA với các nội dung sau:

* Hiện trạng thực tế đối với vấn đề in ấn phiếu thu tại công ty
* Phân tích thiết kế.
* Xây dựng giao diện chương trình (giới thiệu ngôn ngữ, xây dựng giao diện)
	1. **Hiện trạng thực tế đối với vấn đề in ấn phiếu thu tại đơn vị**
	2. **Phân tích thiết kế hệ thống**
		1. ***Sơ đồ usecase tổng quát***
		2. ***Mô hình usecase phân rã chức năng***

Hình 4.3 Sơ đồ Usecase phân rã chức năng tạo chữ ký và ký

* **Sơ đồ Usecase phân rã chức năng chứng thực chữ ký và in phiếu thu**

Trong chức năng chứng thực chữ ký và in phiếu thu, gồm hai chức năng: xác nhận chữ ký và in phiếu thu.

Hình 4.4 Sơ đồ Usecase phân rã chức năng xác nhận chữ ký và in phiếu thu

* + 1. ***Biểu đồ tuần tự của hệ thống***
* **Biểu đồ tuần tự thực hiện chức năng đăng nhập hệ thống**

Hình 4.8 Biểu đồ tuần tự chức năng Tạo chữ ký và ký phiếu thu

* **Biểu đồ tuần tự thực hiện chức năng chứng thực chữ ký**

*Hình 4.9 Biểu đồ tuần tự chức năng chứng thực chữ ký*

* + 1. ***Biểu đồ hoạt động của hệ thống***
* **Biểu đồ hoạt động chức năng Đăng nhập**

Hình 4.10 Biểu đồ hoạt động thực hiện chức năng đăng nhập

* **Biểu đồ hoạt động thực hiện chức năng tạo khóa**

Hình 4.11 Biểu đồ hoạt động thực hiện chức năng nhập số nguyên tố

Biểu đồ hoạt động thực hiện chức năng tạo khóa

Hình 4.13 Biểu đồ hoạt động thực hiện chức năng tạo chữ ký và ký phiếu thu

* **Biểu đồ hoạt động chức năng Chứng thực chữ ký và in phiếu thu**

Admin yêu cầu xác nhận chữ ký sau khi gửi, hệ thống sẽ gửi yêu cầu điền đầy đủ các thông tin vào form cần xác nhận, chọn khóa và chọn người ký. Hệ thống tiến hành kiểm tra thông tin khi nhân viên nhập dữ liệu vào. Nếu đủ tiến hành xác nhận chữ ký phiếu thu; ngược lại hệ thống sẽ yêu cầu chọn đủ thông tin trước khi xác nhận chữ ký. Có thể thực hiện in phiếu thu nếu muốn.

Hình 4.14 Biểu đồ hoạt động thực hiện chứng thực chữ ký và in phiếu thu

* 1. **Xây dựng giao diện và chương trình**
		1. ***Tổng quan về ngôn ngữ lập trình C sharp***

.

* **Form giao diện chính của chương trình**

Hình 4.16 Giao diện chính của chương trình

Phần hệ thống gồm chức năng đăng xuất và đổi mật khẩu.

* **Form đổi mật khẩu**

Hình 4.17 Giao diện form đổi mật khẩu

Trong phần chức năng có các chức năng nhỏ:

* **Form xuất phiếu thu**

Nhân viên sẽ chọn mã phiếu thu trong ô combobox rồi chọn xuất phiếu thu và lưu lại với định dạng \*.doc.

Hình 4.18 Giao diện form xuất phiếu thu

* Form tạo khóa

- Phần tạo khóa: thủ trưởng đơn vị chưa có khóa sẽ được admin sử dụng giao diện này để tạo ra khóa công khai và khóa bí mật cho người thủ trưởng đó. Có hai chế độ: Tùy chọn và Tự động tạo khóa.

- Khóa chỉ được admin tạo và cấp cho thủ trưởng đơn vị để thực hiện việc ký phiếu thu với khóa bí mật.

KẾT LUẬN VÀ KIẾN NGHỊ

**Kết luận**

Phần mềm chưa được thiết kế một cách hoàn chỉnh để có thể kết nối trực tiếp vào một số phần mềm: gửi nhận email, phần mềm quản lý… để có thể thực hiện được đầy đủ các nghiệp vụ trong hoạt động tạo phiếu thu.

**Hướng phát triển của đề tài**

TÀI LIỆU THAM KHẢO

**Tiếng Việt**

[1] Nguyễn Xuân Dũng (2007), Bảo mật thông tin, mô hình và ứng dụng, Nhà xuất bản Thống Kê.

[2] Phan Đình Diệu (1999), Giáo trình lý thuyết mật mã và an toàn thông tin, Nhà xuất bản Đại học Quốc Gia Hà Nội.