

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

CAO HÙNG PHƯƠNG

NGHIÊN CỨU XÂY DỰNG LƯỢC ĐỒ CHỮ KÝ SỐ TRÊN CƠ SỞ
BÀI TOÁN PHÂN TÍCH SỐ

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

THÁI NGUYÊN, 2018

**ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**

CAO HÙNG PHƯƠNG

**NGHIÊN CỨU XÂY DỰNG LƯỢC ĐỒ CHỮ KÝ SỐ TRÊN CƠ SỞ
BÀI TOÁN PHÂN TÍCH SỐ**

Chuyên ngành: Khoa học máy tính

Mã số: 84 80 101

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Người hướng dẫn khoa học: TS. NGUYỄN NGỌC CƯỜNG

THÁI NGUYÊN, 2018

LỜI CAM ĐOAN

Em xin cam đoan tất cả các kết quả được trình bày trong luận văn: *“Nghiên cứu xây dựng lược đồ chữ ký số trên cơ sở bài toán phân tích số”* là công trình nghiên cứu của riêng em, không sao chép từ bất kỳ một công trình nào khác. Các số liệu, kết quả nghiên cứu trong luận văn được sử dụng là trung thực, đã được kiểm chứng và chưa được công bố trong bất kỳ công trình của tác giả nào khác.

Nếu sai em xin hoàn toàn chịu trách nhiệm.

Thái Nguyên, ngày 10 tháng 6 năm 2018

Học viên

Cao Hùng Phương

LỜI CẢM ƠN

Trước hết em xin bày tỏ lòng biết ơn sâu sắc đến thầy giáo TS Nguyễn Ngọc Cương Phó cục trưởng Cục công nghệ thông tin là người đã trực tiếp hướng dẫn, chỉ bảo tận tình và hết lòng giúp đỡ em trong suốt thời gian làm luận văn này..

Xin trân trọng cảm ơn tới Ban lãnh đạo, các thầy cô giáo trường Đại học Công nghệ thông tin và truyền thông Thái Nguyên đã chia sẻ và động viên giúp em vượt qua mọi khó khăn để hoàn thành tốt công việc nghiên cứu của mình.

Xin chân thành cảm ơn gia đình, bạn bè và những người đã luôn ủng hộ, quan tâm, giúp đỡ, động viên, tạo điều kiện tốt nhất và là chỗ dựa vững chắc giúp em có thể hoàn thành luận văn.

Cuối cùng em xin gửi lời chúc sức khỏe và thành công tới tất cả quý thầy cô và gia đình cùng toàn thể các bạn.

Thái Nguyên, ngày 10 tháng 6 năm 2018

Học viên

Cao Hùng Phương

MỤC LỤC

LỜI CAM ĐOAN	i
LỜI CẢM ƠN	ii
MỤC LỤC	iii
DANH MỤC CÁC KÝ HIỆU.....	v
LỜI MỞ ĐẦU	1
CHƯƠNG 1. TỔNG QUAN CÁC CHUẨN CHỮ KÝ SỐ.....	3
1.1. Giới thiệu về hệ mật mã khóa công khai các nguyên lý	3
1.2. Các khái niệm cơ bản	4
1.2.1 Hệ khoá công khai RSA.....	4
1.2.2 Khái niệm chữ ký số	5
1.2.3 Các bước tạo và kiểm tra chữ ký điện tử	7
1.2.4 Định nghĩa lược đồ chữ ký số	8
1.2.5 Chức năng của chữ ký số	8
1.2.6 Các yêu cầu thành phần để tạo ra được chữ ký số.....	9
1.2.7 Ưu, nhược điểm của chữ ký số	9
1.3 Các hệ chữ ký số điển hình	10
1.3.1 Cở sở toán học	10
1.3.2 Hệ mật khóa công khai RSA.....	12
1.3.3 Hệ chữ ký số Elgamal	18
1.3.4 Chuẩn chữ ký DSS.....	19
1.3.5 Hệ chữ ký GOST 3410.94.....	20
1.4 Khả năng ứng dụng của chữ ký số vào thực tiễn	22
1.4.1. Đối với người dùng cá nhân	22
1.4.2. Đối với các Cơ quan - Tổ Chức	22
1.4.3. Đối với các Doanh nghiệp	22
1.5. Kết luận chương 1	23
CHƯƠNG 2. XÂY DỰNG LƯỢC ĐỒ CHỮ KÝ SỐ TRÊN BÀI TOÁN PHÂN TÍCH SỐ	24

2.1. Cơ sở nghiên cứu	24
2.2. Xây dựng thuật toán trên bài toán phân tích số cơ bản.....	25
2.2.1. Thuật toán trên bài toán phân tích số.....	25
2.2.2. Thuật toán hình thành tham số và khóa.....	26
2.2.3. Thuật toán ký và kiểm tra chữ ký.....	26
2.3. Xây dựng lược đồ chữ ký số trên cơ sở bài toán phân tích số	27
2.3.1. Thuật toán hình thành tham số và khóa.....	27
<i>Chú thích:</i>	28
2.3.2. Thuật toán ký.....	28
2.3.3. Thuật toán kiểm tra chữ ký	28
2.3.4. Tính đúng đắn của lược đồ chữ ký số	29
2.3.5. Mức độ an toàn của lược đồ chữ ký số	29
2.4. Kết luận chương 2	30
CHƯƠNG 3. CÀI ĐẶT THỬ NGHIỆM.....	32
3.1. Kịch bản chương trình.....	32
3.2 Cài đặt, thử nghiệm chương trình	33
3.2.1. Cài đặt chương trình.....	33
3.2.2. Thử nghiệm chương trình.....	39
3.3. Kết luận chương 3	43
KẾT LUẬN VÀ KHUYẾN NGHỊ.....	44
1. Kết luận	44
2. Khuyến nghị	44
TÀI LIỆU THAM KHẢO	45

DANH MỤC CÁC KÝ HIỆU

Từ tắt	Tiếng Anh	Tiếng việt
CA	Certificate Authority	Tổ chức chứng thực
PKC	Public key certificate	Chứng chỉ số (chứng nhận khóa công)
PKI	Public Key Infrastructure	Hạ tầng cơ sở khóa công khai
RA	Registration Authority	Trung tâm đăng ký chứng chỉ số
CR	Certificate Repository	Kho lưu trữ chứng chỉ số
RSA	Ron Rivest, Adi Shamir và Leonard Adleman	Là từ viết tắt tên của 3 tác giả đã phát triển ra hệ mật mã khóa công khai

DANH MỤC CÁC HÌNH VẼ

CHƯƠNG 1

Hình 1.1 Hệ thống sử dụng mã hóa khóa công khai.....	3
Hình 1.2 Chữ ký số	6
Hình 1.3 Sơ đồ mã hóa công khai.....	13
Hình 1.4 Sơ đồ quy trình tạo chữ ký trong RSA	17
Hình 1.5 Sơ đồ quy trình xác minh chữ ký số RSA	17

CHƯƠNG 2

Hình 2.1 Sơ đồ thuật toán sinh khóa và ký.....	25
Hình 2.2 Sơ đồ thuật toán xác minh chữ ký	27

CHƯƠNG 3

Hình 3.1 Khai báo các giá trị tham số và khóa.....	33
Hình 3.2 Thuật toán tạo tham số cho chương trình	34
Hình 3.3 Câu lệnh cho nút tạo tham số chương trình.....	34
Hình 3.4 Câu lệnh nút lưu tham số	34
Hình 3.5 Thuật toán tạo khóa cho chương trình.....	34
Hình 3. 6 Câu lệnh cho nút tạo khóa chương trình.....	35
Hình 3.7 Câu lệnh nút lưu khóa.....	35
Hình 3.8 Thuật toán tạo chữ ký số.....	36
Hình 3.9 Câu lệnh cho nút tạo chữ ký số.....	37
Hình 3.10 Câu lệnh nút lưu chữ ký số	37
Hình 3.11 Câu lệnh nút nạp chữ ký số cần xác thực	37

Hình 3.12 Thuật toán kiểm tra hay xác thực chữ ký số.....	38
Hình 3.13 Giao diện chính của phần mềm	39
Hình 3.14 Giao diện của Modul tạo tham số và khóa	40
Hình 3.15 Giao diện của Modul tạo chữ ký số.....	41
Hình 3.16 Giao diện modul xác thực chữ ký.....	42

LỜI MỞ ĐẦU

1. Lý do chọn đề tài:

Hiện nay, khi mà Chính phủ điện tử và Thương mại điện tử là xu hướng tất yếu của hầu hết các quốc gia trên thế giới, trong đó có Việt Nam, thì chứng thực điện tử đã trở thành một yếu tố không thể thiếu được và ngày càng trở nên quan trọng. Hạ tầng công nghệ của chứng thực điện tử là cơ sở hạ tầng khoá công khai với nền tảng là mật mã khoá công khai và chữ ký số. Có nhiều nghiên cứu về lược đồ chữ ký số nói chung, phần lớn đều dựa trên bài toán logarit rời rạc, bài toán khai căn, phân tích số nguyên ra thừa số nguyên tố. Gần đây có một nghiên cứu mới xây dựng một lược đồ chữ ký số trên cơ sở bài toán phân tích một số nguyên lớn ra các thừa số nguyên tố (bài toán phân tích số) kết hợp với bài toán khai căn trong modulo hợp số (bài toán khai căn). Tuy nhiên, do bài toán khai căn không có vai trò quyết định đến mức độ an toàn của lược đồ nên đã không được đề cập đến. Trong nghiên cứu này chọn một phương pháp xây dựng lược đồ chữ ký số theo cùng nguyên tắc đã được chỉ ra, nhưng phương pháp ở đây được mô tả dưới dạng một lược đồ tổng quát từ đó cho phép triển khai ra các lược đồ chữ ký số khác nhau cho các ứng dụng thực tế. Trước tình hình nghiên cứu trong và ngoài nước về chữ ký số như hiện nay thì việc nghiên cứu, phát triển và từng bước đưa chữ ký số ứng dụng vào thực tiễn là rất cần thiết. Chính vì lý do trên tôi đã chọn đề tài ***“Nghiên cứu xây dựng lược đồ chữ ký số trên cơ sở bài toán phân tích số”*** để nghiên cứu làm luận văn tốt nghiệp của mình .

2. Mục đích nghiên cứu

- Tìm hiểu chung về bài toán phân tích số
- Tìm hiểu chuẩn chữ ký số dựa trên bài toán phân tích số và hàm băm.