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 CƯƠNG

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

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 cở khóa công khai
RA	Registration Authority	Trung tâm đăng ký chứng chỉ số
CR	Certificate Repository	Kho lưu trữ chứng chỉ số
RSA	**R**on Rivest, Adi **S**hamir và Leonard **A**dleman	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

CHƯƠNG 2

CHƯƠNG 3

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.