ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

-------o0o-------

PHẠM THỊ TÂM

MỘT SỐ THUẬT TOÁN CHỮ KÝ SỐ VÀ ỨNG DỤNG TRONG BẢO MẬT TÀI LIỆU ĐIỆN TỬ

LUẬN VĂN THẠC SĨ KHOA HỌC
CÔNG NGHỆ THÔNG TIN

Chuyên ngành: Khoa học máy tính
Mã số: 60.48.01.01

Người hướng dẫn khoa học:
PGS.TS. Đoàn Văn Ban

Thái Nguyên, 2017

LỜI CẢM ƠN

Trước tiên tôi xin gửi lời cảm ơn chân thành nhất đến thầy giáo PGS. TS Đoàn Văn Ban, người đã định hướng và nhiệt tình hướng dẫn, cung cấp tài liệu, giúp đỡ tôi rất nhiều trong quá trình học tập và hoàn thiện luận văn.

Tôi xin gửi lời biết ơn sâu sắc đến các thầy, các cô đã tạo điều kiện thuận lợi và truyền đạt những kiến thức, kinh nghiệm quý báu cho chúng tôi trong suốt hai năm học cao học tại Trường Đại học Công nghệ thông tin và Truyền thông – Đại học Thái Nguyên.

Tôi xin cảm ơn bạn bè, đồng nghiệp và gia đình, những người luôn gần gũi, động viên và chia sẻ cùng tôi trong suốt thời gian làm luận văn tốt nghiệp.

Tôi xin chân thành cảm ơn!

Thái Nguyên, tháng 4 năm 2017

Tác giả

Phạm Thị Tâm

LỜI CAM ĐOAN

Tôi là Phạm Thị Tâm, học viên cao học lớp CK14B khóa 2015-2017.

Thầy giáo hướng dẫn là PGS.TS Đoàn Văn Ban.

Tôi xin cam đoan bản luận văn "Một số thuật toán chữ ký số và ứng dụng trong bảo mật tài liệu điện tử" là công trình nghiên cứu của tôi, dưới sự hướng dẫn khoa học của PGS.TS Đoàn Văn Ban, tham khảo các nguồn tài liệu đã được chỉ rõ trong trích dẫn và danh mục tài liệu tham khảo. Các nội dung công bố và kết quả trình bày trong luận văn này là trung thực và chưa được ai công bố trong bất kỳ công trình nào.

Thái Nguyên, ngày tháng năm 2017

Phạm Thị Tâm

MỤC LỤC

DANH MỤC CÁC KÝ HIỆU VÀ CÁC TỪ VIẾT TẮT

DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptographthy
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDSA	Elliptic Curve Digital Signature Algorithm
RSA	Rivesr, Shamir, Adleman
TCP/IP	Transfer Control Protocol/Internet Protocol
DES	Data Encryption Standard
IDEA	Internation Data Encryption Algorithm
AES	Advance Encryption Standard
P	Plaintext
C	Ciphertext
K	Key
E	Encrytion
D	Decrytion
DSS	Digital Signature Standart
SHA	Security Hash Algorithm
MD	Message Digest
FIPS	Federal Information Processing Standard
NIST	the National Institute of Standards and Technology
ISO	International Organization for Standardization
IEEE	Institute of Electrical and Elactronic Engineers
ANSI	American National Standard Institute
VNPT	Tập đoàn Bưu chính viễn thông Việt Nam

DANH MỤC CÁC HÌNH

MỞ ĐẦU

1. Đặt vấn đề

Hiện nay, các giao dịch điện tử ngày càng trở nên phổ biến, việc bảo mật, bảo đảm an toàn thông tin dữ liệu trở thành vấn đề thời sự, là một chủ đề rộng có liên quan đến nhiều lĩnh vực và trong thực tế có thể có nhiều phương pháp được thực hiện để đảm bảo an toàn thông tin dữ liệu. Ngày nay, với sự phát triển nhanh chóng của các hệ thống thông tin trên mạng thì các nguy cơ xâm nhập vào các hệ thống thông tin, các mạng dữ liệu ngày càng gia tăng. Vấn đề bảo mật đã và đang được nhiều người tập trung nghiên cứu, tìm mọi giải pháp để đảm bảo an toàn, an ninh cho hệ thống phần mềm, đặc biệt là các hệ thống thông tin trên mạng.

Sự phát triển mạnh mẽ của Internet về bản chất chính là việc đáp ứng lại sự gia tăng không ngừng của nhu cầu giao dịch trực tuyến trên hệ thống mạng toàn cầu. Các giao dịch trực tuyến trên Internet phát triển từ những hình thức sơ khai như trao đổi thông tin (email, message, …), quảng bá (publicshing) đến những giao dịch phức tạp thể hiện qua các hệ thống chính phủ điện tử, thương mại điện tử ngày càng phát triển mạnh mẽ trên toàn cầu. Tuy nhiên, vấn đề an toàn thông tin lại được nảy sinh từ đây. Internet có những kỹ thuật cho phép mọi người truy cập, khai thác và chia sẻ thông tin với nhau. Nhưng nó cũng là nguy cơ chính dẫn đến thông tin của chúng ta bị hư hỏng hay bị phá hủy hoàn toàn.

Để vừa đảm bảo tính bảo mật của thông tin lại không làm giảm sự phát triển của việc trao đổi thông tin quảng bá trên toàn cầu thì chúng ta phải có các giải pháp phù hợp. Hiện có rất nhiều giải pháp cho vấn đề an toàn thông tin trên mạng như mã hóa thông tin, chữ ký điện tử, chứng chỉ điện tử (chứng chỉ khóa công khai) , … Giải pháp chữ ký số hiện là một giải pháp an toàn và hiệu quả. Chữ ký số được sử dụng để bảo đảm tính bảo mật, tính toàn vẹn, tính chống chối bỏ của các thông tin giao dịch trên mạng Internet.

Chữ ký số tương đương với chữ ký tay nên có giá trị sử dụng trong các ứng dụng giao dịch điện tử với máy tính và mạng Internet cần tính pháp lý cao. Đồng thời, là một phương tiện điện tử được pháp luật thừa nhận về tính pháp lý. Bên cạnh đó, chữ ký số còn là một công nghệ mã hóa và xác thực rất mạnh, thể giúp bảo đảm an toàn, bảo mật cao cho các giao dịch trực tuyến, nhất là các giao dịch chứa các thông tin liên quan đến tài chính. Ứng dụng chữ ký số sẽ đem lại cho doanh nghiệp, tổ chức rất nhiều lợi ích như: Tiết kiệm chi phí giấy tờ, thời gian luân chuyển trong hoạt động quản lý công văn, giấy tờ, thư điện tử; Giúp đẩy nhanh các giao dịch qua mạng trong khi vẫn đảm bảo độ an toàn và bảo mật thông tin, …

Nhận thấy sự thiết thực của chữ ký số trong các tài liệu, văn bản điện tử, trong các giao dịch qua mạng, … và được sự gợi ý của giáo viên hướng dẫn, em đã chọn đề tài "Ứng dụng chữ ký số và ứng dụng trong bảo mật tài liệu điện tử" làm đề tài cho luận văn thạc sỹ của mình. Luận văn tập trung vào nghiên cứu hai thuật toán chính là thuật toán chữ ký số chuẩn DSA, thuật toán chữ ký số đường cong Eliptic. Đây là hai thuật toán mới mà các luận văn gần trước đây chưa đề cập đến khi nghiên cứu về thuật toán tạo chữ ký số.

2. Đối tượng và phạm vi nghiên cứu

**Đối tượng nghiên cứu:*

+ Tìm hiểu về các giải pháp mã hóa để bảo mật thông tin.

+ Nghiên cứu những phương pháp, kỹ thuật tạo chữ ký số trên các tài liệu, văn bản điện tử.

**Phạm vi nghiên cứu:*

Luận văn tập trung nghiên cứu các kiến thức có liên quan, các cơ sở lý thuyết: về một số giải pháp mã hóa và những phương pháp, kỹ thuật tạo chữ ký số để ứng dụng trong bảo mật tài liệu.

3. Hướng nghiên cứu của đề tài

Tập trung nghiên cứu hai vấn đề chính:

- Trình bày và làm rõ hơn ý tưởng về các hệ mật mã khóa thông dụng, việc ứng dụng của các hệ mật mã khóa trong kỹ thuật tạo chữ ký số đối với việc bảo mật, an toàn thông tin.

- Nghiên cứu những phương pháp, kỹ thuật tạo chữ ký số và ứng dụng của chữ ký số trong thương mại điện tử.

4. Những nội dung nghiên cứu chính

+ Nghiên cứu về các giải pháp mã hóa để bảo mật thông tin.

+ Nghiên cứu những phương pháp, kỹ thuật tạo chữ ký số trên các tài liệu, văn bản điện tử. Trong đó tập trung nghiên thuật toán chữ ký số chuẩn DSA, thuật toán chữ ký số đường cong Eliptic.

+ Nghiên cứu về một ngôn ngữ lập trình để viết một ứng dụng nhỏ về chữ ký số.

5. Tổng quan luận văn

Luận văn được trình bày theo hình thức từ trên xuống. Bắt đầu của mỗi phần đều đưa ra những khái niệm cơ bản và quy định cho phần trình bày tiếp sau nhằm mục đích giúp dễ dàng trong khi đọc, dần dần đi sâu vào để thảo luận rõ hơn những vấn đề liên quan, bao gồm việc bảo vệ an toàn thông tin dữ liệu dùng mật mã, mật mã khóa công khai và chữ ký số DSA, ECDSA.

Luận văn được trình bày trong 3 chương và phần kết luận

Chương 1: Bảo mật thông tin và chữ ký số

Vấn đề bảo mật thông tin, mã hóa tài liệu, khái niệm về chữ ký số; phân loại các lược đồ chữ ký số; nghiên cứu một số lược đồ chữ ký số cơ bản: RSA, DSA, ElGama; các phương pháp tấn công chữ ký điện tử; tính pháp lý của chữ ký số.