ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN &TRUYỀN THÔNG

PHẠM AN HƯNG

SƠ ĐỒ CHIA SẺ CHỮ KÍ BÍ MẬT TRONG HỆ MẬT MÃ VÀ ỨNG DỤNG CHO BÀI TOÁN BỎ PHIẾU ĐIỆN TỬ

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

THÁI NGUYÊN - 2016

ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN & TRUYỀN THÔNG

PHẠM AN HƯNG

SƠ ĐỒ CHIA SẺ CHỮ KÍ BÍ MẬT TRONG HỆ MẬT MÃ VÀ ỨNG DỤNG CHO BÀI TOÁN BỎ PHIẾU ĐIỆN TỬ

Chuyên ngành: KHOA HỌC MÁY TÍNH

Mã số: 60 48 01 01

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

NGƯỜI HƯỚNG DẪN KHOA HỌC: TS. VŨ VINH QUANG

THÁI NGUYÊN - 2016

LỜI CAM ĐOAN

Tên tôi là: Phạm An Hưng

Sinh ngày: 14/10/1979

Học viên lớp cao học CK13A - Trường Đại học Công nghệ thông tin và Truyền thông - Đại học Thái Nguyên.

Hiện đang công tác tại: Trường THPT Hoàng Văn Thụ - Lục Yên - Yên Bái

Xin cam đoan: Đề tài "***Sơ đồ chia sẻ chữ kí bí mật trong hệ mật mã và ứng dụng cho bài toán bỏ phiếu điện tử***" do Thầy giáo, NGƯT - TS. Vũ Vinh Quang hướng dẫn là công trình nghiên cứu của riêng tôi. Tất cả tài liệu tham khảo đều có nguồn gốc, xuất xứ rõ ràng.

Tác giả xin cam đoan tất cả những nội dung trong luận văn đúng như nội dung trong đề cương và yêu cầu của thầy giáo hướng dẫn. Nếu sai tôi hoàn toàn chịu trách nhiệm trước hội đồng khoa học và trước pháp luật.

Thái Nguyên, ngày 15 tháng 5 năm 2016

TÁC GIẢ LUẬN VĂN

Phạm An Hưng

MỤC LỤC

DANH MỤC HÌNH VẼ

MỞ ĐẦU

Hiện nay Internet đã trở nên rất phổ biến trên toàn thế giới, thông qua mạng Internet mọi người có thể trao đổi thông tin với nhau một cách nhanh chóng và thuận tiện. Những tổ chức có các hoạt động trên môi trường Internet/Intranet phải đối diện với vấn đề là làm thế nào để bảo vệ những dữ liệu quan trọng, ngăn chặn những hình thức tấn công, truy xuất dữ liệu bất hợp pháp từ bên trong (Intranet) lẫn bên ngoài (Internet). Khi một người muốn trao đổi thông tin với một người hay một tổ chức nào đó thông qua mạng máy tính thì yêu cầu quan trọng là làm sao để đảm bảo thông tin không bị sai lệch hoặc bị lộ do sự can thiệp của người thứ ba. Trước các yêu cầu cần thiết đó, lý thuyết về mật mã thông tin đã ra đời nhằm đảm bảo tính an toàn dữ liệu tại nơi lưu trữ cũng như khi dữ liệu được truyền trên mạng. Vấn đề chia sẻ bí mật được đã được nghiên cứu từ những năm 70 của thế kỷ trước. Ý tưởng chính của chia sẻ bí mật dựa trên nguyên tắc đơn giản là không tin vào bất cứ ai. Để đảm bảo an toàn một thông tin nào đó thì ta không thể trao nó cho một người nắm giữ mà phải chia nhỏ thành các mảnh và chỉ trao cho mỗi người một hoặc một số mảnh, sao cho một người với một số mảnh mình có thì không thể tìm ra thông tin bí mật. Việc phân chia các mảnh phải theo một sơ đồ chia sẻ bí mật nhất định, sau đó có thể khôi phục lại thông tin bí mật ban đầu.

Được sự gợi ý của giáo viên hướng dẫn và nhận thấy tính thiết thực của vấn đề, tôi đã chọn đề tài: “Sơ đồ chia sẻ chữ kí bí mật trong hệ mật mã và ứng dụng cho bài toán bỏ phiếu điện tử” với mong muốn áp dụng các kiến thức đã được học, xây dựng thử nghiệm mô hình bỏ phiếu điện tử tại văn phòng ủy ban nhân dân tỉnh Yên Bái.

Nội dung luận văn bao gồm 3 chương:

Chương 1: "*Các kiến thức cơ bản về hệ mật mã*" Chương này giới thiệu tổng quan về an toàn và bảo mật thông tin, các cơ sở toán học về hệ mật mã. Khái niệm chữ kí số, một số hệ mật mã và sơ đồ chữ kí số, hàm băm và ứng dụng.

Chương 2: "*Hệ mật mã công khai và sơ đồ chia sẻ chữ kí bí mật*" Từ những bài toán, vấn đề đã đặt ra trong phần mở đầu và chương 1, chương 2 trình bày tổng quan về hệ mật mã khóa công khai, mã khóa bí mật và các phương pháp mã hóa để giải quyết các bài toán đặt ra.

Chương 3: "*Ứng dụng kĩ thuật chia sẻ khóa bí mật trong bài toán bỏ phiếu điện tử*", trong chương này đi sâu vào trình bày và phân tích hệ mã hóa công khai Elgamal cùng với tính chất đồng cấu của hệ mật này, tiếp đến là sơ đồ chia sẻ bí mật theo ngưỡng Shamir. Từ đó chỉ ra ứng dụng của hệ mật Elgamal trong bài toán "bỏ phiếu Có/ không"; Phối hợp hệ mật mã Elgamal và sơ đồ chia sẻ bí mật Shamir để giải quyết bài toán "bỏ phiếu chọn L trong K". Phần cuối chương khảo sát bài toán bầu cử tại UBND Tỉnh Yên Bái, từ đó làm căn cứ để xây dựng chương trình mô phỏng cho hai bài toán "bỏ phiếu Có/ không" và "bỏ phiếu chọn L trong K".

Chương 1
MỘT SỐ KIẾN THỨC CƠ BẢN VỀ AN TOÀN THÔNG TIN

Khi nhu cầu trao đổi thông tin dữ liệu ngày càng lớn và đa dạng, các tiến bộ về điện tử - viễn thông và công nghệ thông tin không ngừng được phát triển ứng dụng để nâng cao chất lượng và lưu lượng truyền tin thì các quan niệm ý tưởng và biện pháp bảo vệ thông tin dữ liệu cũng được đổi mới. Bảo vệ an toàn thông tin dữ liệu là một chủ đề rộng, có liên quan đến nhiều lĩnh vực và trong thực tế có thể có rất nhiều phương pháp được thực hiện để bảo vệ an toàn thông tin dữ liệu. Trong chương này sẽ trình bày một số kiến thức cơ bản về an toan thông tin, Các kiến thức dưới đây được tham khảo từ [2], [3], [9].

1.1. Tổng quan về an toàn và bảo mật thông tin

1.1.1. An toàn và bảo mật thông tin

Khi nhu cầu trao đổi thông tin dữ liệu ngày càng lớn và đa dạng, các tiến bộ về điện tử - viễn thông và công nghệ thông tin không ngừng được phát triển ứng dụng để nâng cao chất lượng và lưu lượng truyền tin thì các quan niệm ý tưởng và biện pháp bảo vệ thông tin dữ liệu cũng được đổi mới. Bảo vệ an toàn thông tin dữ liệu là một chủ đề rộng, có liên quan đến nhiều lĩnh vực và trong thực tế có thể có rất nhiều phương pháp được thực hiện để bảo vệ an toàn thông tin dữ liệu. Các phương pháp bảo vệ an toàn thông tin dữ liệu có thể được quy tụ vào ba nhóm sau:

- Bảo vệ an toàn thông tin bằng các biện pháp hành chính.
- Bảo vệ an toàn thông tin bằng các biện pháp kỹ thuật (phần cứng).
- Bảo vệ an toàn thông tin bằng các biện pháp thuật toán (phần mềm).