ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CNTT&TT

LÊ ĐÌNH QUYẾN

NGHIÊN CỨU VẤN ĐỀ CHIA SẺ BÍ MẬT VÀ ỨNG DỤNG TRONG BỎ PHIẾU ĐIỆN TỬ

Chuyên ngành: **Khoa học máy tính**
Mã số chuyên ngành: **60.48.01**

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

NGƯỜI HƯỚNG DẪN KHOA HỌC

PGS.TS TRỊNH NHẬT TIẾN

THÁI NGUYÊN, NĂM 2012

LỜI CAM ĐOAN

Tôi xin cam đoan luận văn này của tự bản thân tôi tìm hiểu, nghiên cứu dưới sự hướng dẫn của PGS.TS Trịnh Nhật Tiến. Các chương trình thực nghiệm do chính bản thân tôi lập trình, các kết quả là hoàn toàn trung thực. Các tài liệu tham khảo được trích dẫn và chú thích đầy đủ.

TÁC GIẢ LUẬN VĂN

Lê Đình Quyến

Số hóa bởi Trung tâm Học liệu – Đại học Thái Nguyên *http://www.lrc-tnu.edu.vn*

LỜI CẢM ƠN

Trước hết em xin trân trọng gửi lời cảm ơn đến toàn thể các thầy cô giáo Trường Đại học Công nghệ – Đại học Quốc gia Hà Nội và Trường Đại học Công nghệ thông tin và Truyền thông – Đại học Thái nguyên đã dạy dỗ chúng em trong suốt quá trình học tập chương trình cao học tại trường.

Đặc biệt em xin bày tỏ lòng biết ơn sâu sắc tới thầy giáo PGS.TS Trịnh Nhật Tiến, Trường Đại học Công nghệ – Đại học Quốc gia Hà Nội đã quan tâm, định hướng và đưa ra những góp ý, gợi ý, chỉnh sửa quí báu cho em trong quá trình làm luận văn tốt nghiệp.

Cuối cùng, em xin chân thành cảm ơn các bạn bè đồng nghiệp, gia đình và người thân đã quan tâm, giúp đỡ và chia sẻ với em trong suốt quá trình làm luận văn tốt nghiệp.

Thái Nguyên, ngày 28 tháng 10 năm 2012

HỌC VIÊN

Lê Đình Quyến

MỤC LỤC

DANH MỤC CÁC THUẬT NGỮ

gcd	greatest common divisor (ước số chung lớn nhất)
CRT	Chinese Remainder Theorem (định lý phần dư Trung Hoa)
DES	Data Encryption Standard (Tiêu chuẩn mã hóa dữ liệu)
RSA	Rivest, Sharmir, Adleman
SHA	Secure Hash Algorithm (Thuật giải băm an toàn)
PKI	Public Key Infastructure (Hạ tầng khóa công khai)
CA	Certification Authority (Chứng thực chữ kí số)
DSS	Digital Signature Standard (Chuẩn chữ kí số)

DANH MỤC CÁC BẢNG

DANH MỤC CÁC HÌNH

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, em đã chọn đề tài: ***Nghiên cứu vấn đề chia sẻ bí mật và ứng dụng trong "Bỏ phiếu điện tử"*** để làm nội dung cho luận văn tốt nghiệp của mình.

Luận văn này tập trung vào nghiên cứu cơ sở lý thuyết toán học và một số kỹ thuật mật mã để thực hiện chia sẻ thông tin mật, sau đó áp dụng giải quyết một số bài toán về an toàn thông tin trong "Bỏ phiếu điện tử".

Nội dung chính của luận văn gồm ba chương

Chương 1: Các khái niệm cơ bản

Trong chương này luận văn trình bày các kiến thức cơ bản về lý thuyết toán học Modulo, vấn đề mã hóa, kí điện tử, chữ kí số và vấn đề quản lý khóa.

Chương 2: Sơ đồ chia sẻ bí mật

Nội dung chương 2 trình bày khái niệm về chia sẻ bí mật, các sơ đồ chia sẻ bí mật và tính chất mở rộng của các sơ đồ chia sẻ bí mật, ưu điểm của sơ đồ Shamir trong bài toán bỏ phiếu điện tử.

Chương 3: Ứng dụng trong bỏ phiếu điện tử.

Chương này đề cập tới một số bài toán về an toàn thông tin trong "Bỏ phiếu điện tử", Giải quyết bài toán chia sẻ khóa ký phiếu bầu cử, Giải quyết bài toán chia sẻ nội dung phiếu bầu cử. Chương trình thử nghiệm được viết bằng ngôn ngữ lập trình C# 2012.

Số hóa bởi Trung tâm Học liệu – Đại học Thái Nguyên *http://www.lrc-tnu.edu.vn*