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

LÊ THỊ HUYỀN

NÂNG CAO TỐC ĐỘ TÍNH TOÁN CỦA PHƯƠNG PHÁP MÃ HÓA KHÓA CÔNG KHAI RABIN

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Thái Nguyên - Năm 2014

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

LÊ THỊ HUYỀN

NÂNG CAO TỐC ĐỘ TÍNH TOÁN CỦA PHƯƠNG PHÁP MÃ HÓA KHOÁ CÔNG KHAI RABIN

Chuyên ngành: Khoa học máy tính
Mã số: 60 48 01

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

NGƯỜI HƯỚNG DẪN KHOA HỌC

PGS.TS. Phạm Văn Ất

Thái Nguyên - Năm 2014

LỜI CAM ĐOAN

Tôi xin cam đoan bản luận văn **"Nâng cao tốc độ tính toán của phương pháp mã hóa khóa công khai Rabin"** là công trình nghiên cứu của tôi, dưới sự hướng dẫn khoa học của PGS.TS Phạm Văn Ất, tham khảo 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 từng được ai công bố trong bất cứ công trình nào.

Học viên thực hiện

Lê Thị Huyền

MỤC LỤC

DANH MỤC BẢNG

Trang

DANH MỤC HÌNH VẼ

Trang

MỞ ĐẦU

Hiện nay, ở tất cả các nước phát triển cũng như đang phát triển, mạng máy tính đang ngày càng đóng vai trò thiết yếu trong mọi lĩnh vực hoạt động của toàn xã hội, và một khi nó trở thành phương tiện điều hành các hệ thống thì nhu cầu bảo mật an toàn thông tin được đặt lên hàng đầu. Nhu cầu này không chỉ có ở các bộ *máy an ninh, quốc phòng, quản lý nhà nước*, mà đã trở thành bức thiết trong nhiều hoạt động kinh tế xã hội: *tài chính, ngân hàng, thương mại, ...* và thậm chí trong cả một số hoạt động thường ngày của người dân (thư điện tử, thanh toán, tín dụng, ...). Bởi vậy chúng ta phải làm sao đảm bảo được tính trong suốt của thông tin.

Nếu như bạn gửi thư cho một người bạn nhưng lại bị một kẻ lạ mặt nào đó xem trộm và sửa đổi nội dung bức thư trái với chủ ý của bạn, tệ hại hơn nữa là khi bạn ký một hợp đồng, gửi thông qua mạng và lại bị kẻ xấu sửa đổi những điều khoản trong đó, và sẽ còn nhiều điều tương tự như vậy nữa... Hậu quả sẽ như thế nào? Bạn bị người khác hiểu nhầm vì nội dung bức thư bị thay đổi, còn hợp đồng bị phá vỡ bởi những điều khoản đã không còn nguyên vẹn. Trước thực tế đó, yêu cầu quan trọng là làm sao để đảm bảo thông tin không bị sai lệch hoặc bị lộ do sự xâm nhập của kẻ thứ ba.

Mã hoá thông tin là một trong các phương pháp đảm bảo được tính trong suốt của thông tin. Nó có thể giải quyết các vấn đề rắc rối ở trên giúp bạn, một khi thông tin đã được mã hoá và gửi đi thì kẻ xấu rất khó hoặc không thể giải mã được.

Một số giải thuật mã hóa đã được xây dựng nhằm đảm bảo tính an toàn dữ liệu tại nơi lưu trữ cũng như khi dữ liệu được truyền trên mạng, như các giải thuật mã hóa đối xứng (DES), giải thuật mã hóa công khai.

Trong số các hệ mật mã hóa công khai thì hệ mật RSA thường được dùng nhiều nhất, kế đến là hệ mã Rabin. Hai hệ này có độ an toàn như nhau. Hệ Rabin có ưu điểm là tốc độ mã hóa nhanh hơn RSA, nhưng nhược điểm là việc giải mã không cho một lời giải duy nhất và một trong những lời giải đó là bản rõ cần tìm. Trong những năm gần đây đã có một số cải tiến để khắc phục nhược điểm này của hệ mật Rabin, nhưng hầu hết các sách và tài liệu tiếng Việt vẫn trình bày phương pháp

Rabin gốc. Chính vì vậy, em chọn đề tài: "*Nâng cao tốc độ tính toán của phương pháp mã hóa khóa công khai Rabin".*

Nội dung chính của luận văn:

Trình bày thuật toán kiểm tra và sinh số nguyên tố. Nhằm tìm ra các số nguyên tố làm khóa cho các hệ mật mã khóa công khai.

Nghiên cứu hướng cải tiến phương pháp mã hóa khóa công khai Rabin nhằm nâng cao tốc độ xử lý.

Luận văn bao gồm 3 chương:

Chương 1: Giới thiệu chung về mật mã và cơ sở toán học của lý thuyết mật mã

Nhằm giới thiệu lịch sử của mật mã, giới thiệu các hệ thống mật mã, đưa ra một số hệ mật mã khóa công khai.

Trình bày các kiến thức toán học làm nền tảng cho các nội dung chính trong luận văn như: Độ phức tạp của thuật toán, thuật toán Euclid, thuật toán Euclid mở rộng, số nguyên tố và các phương pháp kiểm tra số nguyên tố.

Chương 2: Một số sơ đồ cải tiến nâng cao tốc độ tính toán phương pháp mã hóa khóa công khai Rabin

Trình bày ký hiệu Legendre, Jacobi, định lí số dư Trung Quốc

Trình bày một số cải tiến phương pháp mã hóa khóa công khai Rabin nâng cao tốc độ xử lý: Cải tiến của Shimada, Chen-Tsu, THA.

Chương 3: Cài đặt và thực nghiệm

Cài đặt chương trình và kết quả thực nghiệm một số sơ đồ cải tiến phương pháp mã hóa khóa công khai Rabin.

Do thời gian và trình độ còn hạn chế nên luận văn khó tránh khỏi những thiếu sót, kính mong nhận được sự đóng góp, chỉ bảo của các thầy giáo, cô giáo và các bạn đồng nghiệp.

Cuối cùng, em xin chân thành bày tỏ lòng biết ơn sâu sắc đến thầy giáo PGS. TS. Phạm Văn Ất – Đại học Giao thông Vận tải đã tận tình hướng dẫn, chỉ bảo, giúp đỡ, khích lệ em trong suốt quá trình làm luận văn. Đồng thời, em xin chân thành cảm ơn các thầy cô trong Phòng Sau Đại học – Trường Đại học Công nghệ

thông tin và Truyền thông, các thầy cô trong Viện Công nghệ thông tin – Viện Khoa học và Công nghệ Việt Nam đã tạo điều kiện thuận lợi, giúp đỡ em hoàn thành luận văn này.

Thái Nguyên, tháng 09 năm 2014

Học viên thực hiện

Lê Thị Huyền