ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

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

NGUYỄN KHẢI

NGHIÊN CỨU, SO SÁNH VÀ ĐÁNH GIÁ ĐỘ AN TOÀN CỦA HỆ MẬT MÃ RABIN VÀ RSA

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

THÁI NGUYÊN - 2016

LỜI CAM ĐOAN

Với mục đích nghiên cứu, tìm hiểu để nâng cao kiến thức và trình độ chuyên môn để áp dụng trong các bài toán cụ thể trong tương lai nên tôi đã làm luận văn này một cách nghiêm túc và hoàn toàn trung thực. Nội dung luận văn do tự tôi tìm hiểu và hoàn thành.

Trong luận văn, tôi có sử dụng tài liệu tham khảo của một số tác giả trong và ngoài nước để hoàn thành luận văn được nêu ở phần tài liệu tham khảo.

Tôi xin cam đoan và chịu trách nhiệm về nội dung, sự trung thực trong luận văn tốt nghiệp Thạc sỹ của mình.

Thái Nguyên, tháng 7 năm 2016

Học viên

Nguyễn Khải

LỜI CẢM ƠN

Em xin chân thành cảm ơn toàn thể các thầy cô giáo trong trường Đại học công nghệ thông tin và truyền thông, Đại học Thái Nguyên đã hết lòng dạy dỗ chỉ bảo, tạo điều kiện tốt cho em trong suốt quá trình học tập cũng như trong thời gian thực hiện luận văn này.

Đặc biệt em gửi lời cảm ơn chân thành và sâu sắc tới TS Hồ Văn Canh người đã trực tiếp quan tâm, tận tình hướng dẫn giúp đỡ và tạo điều kiện hết sức thuận lợi cho em trong quá trình thực hiện khóa luận.

Cảm ơn các bạn đồng khóa và gia đình đã động viên, giúp đỡ tôi rất nhiều trong quá trình học tập tại trường Đại học công nghệ thông tin và truyền thông Đại học Thái Nguyên cũng như trong quá trình thực hiện khóa luận.

Thái Nguyên, tháng 7 năm 2016

Học viên

Nguyễn Khải

MỤC LỤC

DANH MỤC BẢNG

DANH MỤC CHỮ VIẾT TẮT

Viết tắt	Tiếng Anh	Tiếng Việt
BSCNN		Bội số chung nhỏ nhất
ƯSC		Ước số chung
ƯSLCN		Ước số chung lớn nhất

LỜI MỞ ĐẦU

1. Sự cần thiết lựa chọn đề tài

Sự xuất hiện của mạng Internet cho phép mọi người có thể truy cập, chia sẻ và khai thác thông tin một cách dễ dàng và hiệu quả, tuy nhiên lại nảy sinh vấn đề về an toàn thông tin. Thực vậy, Internet có những kỹ thuật tuyệt vời cho phép mọi người truy nhập, khai thác, chia sẻ thông tin. Nhưng nó cũng là nguy cơ chính dẫn đến thông tin của bạn bị hư hỏng hoặc phá huỷ hoàn toàn.

Để vừa bảo đảm 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 một giải pháp tốt nhất là mã hoá thông tin. Có thể hiểu sơ lược mã hoá thông tin là che đi thông tin của mình làm cho kẻ tấn công nếu chặn được thông báo trên đường truyền thì cũng không thể đọc được và phải có một giao thức giữa người gửi và người nhận để có thể trao đổi thông tin, đó là các cơ chế mã và giải mã thông tin.

Năm 1949, C.Shannon đã đưa ra mô hình hệ mật mã đối xứng an toàn vô điều kiện dựa trên cơ sở lý thuyết thông tin. Các hệ mã này đều sử dụng chung một khóa bí mật trong cả hai quy trình mã hóa - giải mã và vì thế việc bảo mật thông tin đồng nghĩa với việc bảo mật khóa chung đó. Tuy nhiên, nếu trong hệ thống có nhiều nhóm người cần trao đổi thông tin mật với nhau thì số khóa chung cần giữ bí mật là rất lớn, khó có thể quản lý và trao đổi.

Trong thời đại ngày nay, nhiều bài toán mật mã trong thực tế được đặt ra là "chỉ cần giữ bí mật trong một thời gian nào đó cho một số thông tin nào đó mà thôi". Với mục đích giải quyết vấn đề trên, vào năm 1976, W.Diffie - M.E.Hellman đã để xuất mô hình hệ mật mã phi đối xứng hay còn gọi là hệ mật

mã khoá công khai, an toàn về mặt tính toán dựa trên cơ sở lý thuyết độ phức tạp tính toán. Các hệ mã bất đối xứng sử dụng hai loại khóa trong cùng một cặp khóa, khóa bí mật và khóa công khai. Khóa công khai được công bố rộng rãi và được sử dụng để mã hóa thông tin còn khóa bí mật chỉ do một người nắm giữ và được sử dụng để giải mã thông tin đã được mã hóa bằng khóa công khai. Đặc điểm quan trọng là không thể tìm được khóa giải mã khi chỉ biết khóa lập mã trong thời gian chấp nhận được.

Do thời gian, khả năng của bản thân, em không thể khảo sát hết được tất cả các hệ mật mã khoá công khai đã được biết, mà chỉ nghiên cứu 2 hệ mật mã được thế giới sử dụng nhiều, rộng rãi nhất hiện nay, đó là hệ mật mã RSA do Ron Rivert, Adi Shamir và Len Adleman sáng tạo, được công bố vào năm 1977 dựa vào bài toán phân tích số nguyên và hệ mật mã RABIN là hệ mật dựa trên độ phức tạp của việc tính căn bậc hai theo hợp số. Để hiểu rõ về 2 thuật toán này cũng như so sánh, đánh giá được độ an toàn của 2 thuật toán này, em lựa chọn đề tài: "*Nghiên cứu, so sánh và đánh giá độ an toàn của hệ mật mã Rabin và RSA*" làm luận văn tốt nghiệp Thạc sỹ của mình.

2. Mục tiêu nghiên cứu của đề tài

- Nghiên cứu về lý thuyết số và mật mã;

- Tìm hiểu, phân tích và nhận xét được ưu nhược điểm của hệ mật mã Rabin và RSA;

- So sánh và đánh giá độ an toàn của hệ mật mã Rabin và RSA.

3. Đối tượng và phạm vi nghiên cứu

3.1. Đối tượng