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

NGUYỄN THỊ NGHĨA

VẤN ĐỀ BẢO MẬT CỦA PHƯƠNG PHÁP MÃ HÓA SỐ HỌC

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Thái Nguyên - 2014

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

NGUYỄN THỊ NGHĨA

VẤN ĐỀ BẢO MẬT CỦA PHƯƠNG PHÁP MÃ HÓA SỐ HỌC

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 - 2014

LỜI CAM ĐOAN

Tôi xin cam đoan bản luận văn "***Vấn đề bảo mật của phương pháp mã hóa số học***" 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 luận văn

Nguyễn Thị Nghĩa

MỤC LỤC

Trang

Chương 3

CHƯƠNG TRÌNH THỬ NGHIỆM

DANH MỤC CÁC HÌNH VẼ

DANH MỤC CÁC BẢNG

MỞ ĐẦU

Mật mã học là ngành nghiên cứu các kỹ thuật Toán học nhằm cung cấp các dịch vụ an toàn thông tin. Mặc dù khoa học mật mã đã ra đời từ hàng nghìn năm nhưng trải qua nhiều thế kỷ, các kết quả của Mật mã học chủ yếu chỉ được sử dụng trong lĩnh vực quân sự, chính trị, ngoại giao... Ngày nay, Các ứng dụng mã hóa và bảo mật thông tin được sử dụng ngày càng phổ biến trong các lĩnh vực khác nhau trên thế giới, từ việc bảo mật nội dung các tài liệu điện tử, bảo vệ an toàn các giao dịch thương mại điện tử, đấu giá trên mạng, bầu cử trực tuyến,... đến ứng dụng trong các hệ thống thể thông minh, mạng cảm ứng không dây...

Cho đến thập niên 1970, hầu hết các nghiên cứu và ứng dụng của mật mã học tập trung vào việc bảo mật thông tin. Từ giữa thập niên 1970 cho đến nay, phạm vi nghiên cứu của Mật mã học đã được mở rộng, các ứng dụng của Mật mã học ngày càng đa dạng và phong phú. Tùy vào đặc thù của mỗi hệ thống bảo vệ thông tin mà ứng dụng sẽ có các tính năng với đặc trưng riêng sau:

Bảo mật thông tin: hệ thống đảm bảo thông tin được bí mật. Ví dụ như trong quá trình truyền nhận thông tin, thông tin có thể bị phát hiện bởi người tấn công, nhưng người tấn công đó không thể hiểu được nội dung thông tin đánh cắp được.

Toàn vẹn thông tin: hệ thống bảo đảm tính toàn vẹn thông tin trong liên lạc hoặc giúp phát hiện ra rằng thông tin đã bị sửa lỗi.

Xác thực các đối tác trong liên lạc và xác thực nội dung thông tin trong liên lạc.

Chống từ chối trách nhiệm: hệ thống đảm bảo một đối tác bất kỳ trong hệ thống không thể từ chối trách nhiệm về hành động mà mình đã thực hiện.

Các ứng dụng đầu tiên và phổ biến nhất của Mật mã học là bảo mật nội dung thông tin sử dụng hệ thống mã hóa đối xứng (hay còn gọi là hệ thống mã

hóa quy ước). Trong hệ thống này, quá trình mã hóa và giải mã một thông điệp sử dụng cùng một khóa gọi là khóa bí mật (secret key) hay khóa đối xứng (symmetric key). Do đó, vấn đề bảo mật thông tin đã mã hóa hoàn toàn phụ thuộc vào việc giữ bí mật nội dung của khóa đã được sử dụng.

Trong lĩnh vực bảo mật thông tin, phương pháp mã hóa số học được xem là một trong những phương pháp hay. Tuy nhiên, phương pháp này chưa được ứng dụng phổ biến vào thực tế do gặp phải một số khó khăn nhất định như: tốc độ thực hiện của thuật toán mã hóa và giải mã chậm, đồng thời độ bảo mật của thuật toán này còn chưa cao. Luận văn tập trung đi sâu vào nghiên cứu cơ sở toán học của phương pháp mã hóa số học và các vấn đề liên quan. Luận văn nghiên cứu một số cải tiến trong thuật toán mã hóa và giải mã nhằm tăng tốc độ thực hiện. Phát triển mô hình mã hóa số học nhị phân với miền phân bố động (không cố định) đối với mô hình 8 bit (256 ký tự) để nâng cao độ bảo mật của phương pháp mã hóa.

Dựa trên mục tiêu đã xác định, nội dung của luận văn sẽ được trình bày qua 3 chương như sau:

- Chương 1: Tổng quan về mã hóa thông tin.
- Chương 2: Phương pháp mã hóa số học và một số cải tiến.
- Chương 3: Chương trình thử nghiệm.

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, tác giả 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 tác giả trong suốt quá trình làm luận văn. Đồng thời, tác giả 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 tác giả hoàn thành luận văn này.

Thái Nguyên, ngày tháng năm 2014

Học viên thực hiện

Nguyễn Thị Nghĩa