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

PHẠM THỊ TUYẾT

NGHIÊN CỨU MỘT SỐ THUẬT TOÁN HỆ MẬT MÃ KHOÁ CÔNG KHAI ELGAMAL VÀ ỨNG DỤNG

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

THÁI NGUYÊN - 2015

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

PHẠM THỊ TUYẾT

NGHIÊN CỨU MỘT SỐ THUẬT TOÁN HỆ MẬT MÃ KHOÁ CÔNG KHAI ELGAMAL VÀ ỨNG DỤNG

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 NGUYỄN NGỌC CƯƠNG

THÁI NGUYÊN - 2015

LỜI CAM ĐOAN

Tôi xin cam đoan luận văn **" Nghiên cứu một số thuật toán hệ mật mã khoá công khai ElGamal và ứng dụng"** là công trình nghiên cứu của cá nhân tôi tìm hiểu, nghiên cứu dưới sự hướng dẫn của TS Nguyễn Ngọc Cương. Các kết quả là hoàn toàn trung thực, toàn bộ nội dung nghiên cứu của luận văn, các vấn đề được trình bày đều là những tìm hiểu và nghiên cứu của chính cá nhân tôi hoặc là được trích dẫn từ các nguồn tài liệu được trích dẫn và chú thích đầy đủ.

TÁC GIẢ LUẬN VĂN

Phạm Thị Tuyết

LỜI CẢM ƠN

Học viên xin bày tỏ lời cảm ơn chân thành tới tập thể các thầy cô giáo Viện công nghệ thông tin, các thầy cô giáo Trường Đại học Công nghệ thông tin và truyền thông - Đại học Thái Nguyên đã mang lại cho học viên kiến thức vô cùng quý giá và bổ ích trong suốt quá trình học tập chương trình cao học tại trường. Đặc biệt học viên xin bày tỏ lòng biết ơn sâu sắc tới thầy giáo TS Nguyễn Ngọc Cương - Học viện an ninh đã định hướng khoa học và đưa ra những góp ý, gợi ý, chỉnh sửa quý báu, quan tâm, tạo điều kiện thuận lợi trong quá trình nghiên cứu hoàn thành luận văn này.

Cuối cùng, học viên xin chân thành cảm ơn các bạn bè đồng nghiệp, gia đình và người thân đã quan tâm, giúp đỡ và chia sẻ với học viên trong suốt quá trình học tập.

Do thời gian và kiến thức có hạn nên luận văn chắc không tránh khỏi những thiếu sót nhất định. Học viên rất mong nhận được những sự góp ý quý báu của thầy cô và các bạn.

Thái Nguyên, ngày tháng năm 2015

HỌC VIÊN

Phạm Thị Tuyết

MỤC LỤC

MỤC CÁC HÌNH VẼ, ĐỒ THỊ

MỞ ĐẦU

1. Tính khoa học và cấp thiết của đề tài

Cùng với sự phát triển của công nghệ thông tin, hiện nay vấn đề an toàn thông tin trở nên hết sức cần thiết trên qui mô toàn cầu. Đảm bảo tính bảo mật, khả năng xác thực nguồn gốc gói tin trong quá trình truyền tải thông tin qua môi trường không an toàn như Internet là một vấn đề nóng trong nghiên cứu và thực tiễn. Để đảm bảo tính bảo mật và xác thực người ta cần phải mã hoá, có một số thuật toán mã hoá công khai rất nổi tiếng: RSA, ElGamal, ... Tuy nhiên, các hệ mật mã này có nhược điểm là không có cơ chế xác thực thông tin được bảo mật (nguồn gốc, tính toàn vẹn) do đó chúng không có khả năng chống lại một số dạng tấn công giả mạo trong thực tế. Chính vì vậy hiện nay, người ta [3] đã đề xuất một số cải tiến hệ mật mã ElGamal. Ưu điểm của các thuật toán mới đề xuất này là ở chỗ cho phép bảo mật và xác thực thông tin một cách đồng thời mà mức độ an toàn của các thuật toán mới đề xuất không nhỏ hơn mức độ an toàn của thuật toán ElGamal xét theo khả năng chống thám mã khi tấn công trực tiếp vào các thủ tục mã hóa và giải mã.

Để góp phần nâng cao hiệu năng của phương pháp mã hóa ElGamal. Trong luận văn này, học viên đặt mục tiêu nghiên cứu, thử nghiệm thuật toán mã hóa Elgamal và các cải tiến mới của các tác giả đã đưa ra, so sánh hiệu quả của chúng và kiểm định thuật toán này bằng một ứng dụng trong thực tiễn. Đây là bài toán lựa chọn các khả năng trong các giải pháp đã có bằng việc mã hóa và xác thực như bài toán bỏ phiếu điện tử do các cán bộ tiến hành hoặc bài toán thăm dò tín nhiệm lãnh đạo tại một đơn vị. Những bài toán này luôn đòi hỏi tính bí mật, ví dụ trong bỏ phiếu điện tử (e-voting), việc đảm bảo tính đúng đắn bảo mật ở đây có thể bao gồm cả việc không để lộ danh tính cử tri (ai bỏ phiếu cho ứng viên nào?), tính duy nhất (mỗi cử tri đảm bảo chỉ tối đa 1 lần bỏ phiếu)...

2. Đối tượng và phạm vi nghiên cứu

- Đối tượng nghiên cứu: Hệ mật khóa công khai ElGamal và các cải tiến của hệ mật mã.

- Phạm vi nghiên cứu: Nghiên cứu cải tiến dựa trên thuật toán đã có và xây dựng chương trình ứng dụng trong bài toán thăm dò dư luận về mức độ tín nhiệm đối với một đơn vị (ở đây là tổng công ty xăng dầu Việt Nam).

3. Hướng nghiên cứu của đề tài

- Nghiên cứu các đề xuất một số thuật toán mật mã khóa công khai được phát triển từ hệ mật ElGamal của các tác giả đã công bố để xây dựng chương trình ứng dụng trong bài toán bỏ phiếu thăm dò dư luận về mức độ tín nhiệm.

- Đánh giá ưu điểm của các thuật toán mới do các tác giả đã đề xuất về mức độ bảo mật và xác thực thông tin một cách đồng thời.

4. Những nội dung nghiên cứu chính

Luận văn được trình bày trong 3 chương, có phần mở đầu, phần kết luận, phần mục lục, phần tài liệu tham khảo. Các nội dung cơ bản của luận văn được trình bày theo cấu trúc sau:

***Chương 1*:** TỔNG QUAN VỀ CÁC HỆ MẬT MÃ

Trong chương này tổng trình bày một số khái niệm cơ bản trong toán học mà các hệ mã hoá thường sử dụng như: mod, số nguyên tố, vành Z_n, các phép toán cộng, nhân, bài toán logarrit rời rạc trên không gian Z_n.... Sau đó đưa ra các khái niệm mật mã, các thuật toán mã hoá, chữ ký số phục vụ cho việc mã hoá thông tin.

Chương 2: HỆ MẬT MÃ ELGAMAL CẢI TIẾN VÀ MÃ HÓA ĐỒNG CẤU

Tập trung nghiên cứu một số thuật toán mật mã ElGamal cải tiến, tính chất đồng cấu của hệ mật ElGamal và sơ đồ chia sẻ bí mật theo ngưỡng Shamir.

***Chương 3*:** ỨNG DỤNG HỆ MẬT MÃ ELGAMAL TRONG BÀI TOÁN BỎ PHIẾU THĂM DÒ TÍN NHIỆM

Cài đặt thử nghiệm thuật toán hệ mật ElGamal cải tiến và kỹ thuật chia sẻ khóa bí mật Shamir.