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

LÊ THỊ HÀ

SƠ ĐỒ ĐỊNH DANH MẬT VÀ CHỮ KÝ SỐ ỨNG DỤNG TRONG THƯƠNG MẠI ĐIỆN TỬ

LUẬN VĂN THẠC SĨ: KHOA HỌC MÁY TÍNH

Thái Nguyên - 2012

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

LÊ THỊ HÀ

SƠ ĐỒ ĐỊNH DANH MẬT VÀ CHỮ KÝ SỐ ỨNG DỤNG TRONG THƯƠNG MẠI ĐIỆN TỬ

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. Bùi Thế Hồng

Thái Nguyên - 2012

LỜI CAM ĐOAN

Tôi xin cam đoan Luận văn " Sơ đồ định danh mật và chữ ký số ứng dụng trong thương mại điện tử " là công trình nghiên cứu của riêng tôi dưới sự hướng dẫn của **PGS.TS. Bùi Thế Hồng** Toàn bộ phần mềm do chính tôi xây dựng và kiểm thử . Tôi xin chịu trách nhiệm về lời cam đoan của mình.

Các số liệu và thông tin sử dụng trong luận văn này là trung thực.

Tác giả

Lê Thị Hà

MỤC LỤC

DANH MỤC CÁC KÝ HIỆU, CÁC TỪ VIẾT TẮT

Các từ viết tắt	**Nghĩa tiếng anh**	**Nghĩa tiếng việt**
	hash function	Hàm băm.
DSS	Digital Signature Standard	Chuẩn chữ ký số
RSA	Rivest, Shamir và Adleman	Tên ba tác giả của hệ mật mã RSA
TA	Trusted Authority	Cơ quan ủy thác
E	Elgamal	Sơ đồ chữ ký Elgamal

DANH MỤC HÌNH VẼ

LỜI MỞ ĐẦU

1. Lý do chọn đề tài

Ngày nay, cùng với sự phát triển không ngừng của ngành công nghệ thông tin là sự bùng nổ số lượng ứng dụng quản lý thông tin, công việc của tổ chức, doanh nghiệp, cá nhân, an toàn cho vấn đề xác nhận các thông báo. Mặt khác, trong môi trường cạnh tranh, người ta ngày càng cần có nhiều thông tin với tốc độ nhanh để trợ giúp việc ra quyết định và ngày càng có nhiều câu hỏi mang tính chất cần phải có giải pháp an toàn cho vấn đề xác nhận các thông báo cùng với người gửi trên các mạng truyền tin công cộng.

Trong thực tế cuộc sống, việc xưng danh theo thói quen thường không có tính an toàn chẳng hạn các số PIN, mật khẩu thường không có gì để đảm bảo là được giữ kín, người ngoài không biết.

Trong giao thức thực hiện trên điện thoại, bất kỳ kẻ nghe trộm nào cũng có thể dùng thông tin định danh cho mục đích riêng của mình. Những người này cũng có thể là người nhận thông tin. Các mưu đồ xấu trên thẻ tín dụng đều hoạt động theo cách này.

Như vậy với sự phát triển tin học trên mọi lĩnh vực như hiện nay, phần lớn các giao dịch được thực hiện trên các mạng tin học đòi hỏi phải có giải pháp về an toàn trong các khâu xưng danh và xác nhận danh tính cho các hoạt động đó.

Nhận thấy tính thiết thực của vấn đề này và được sự gợi ý của giảng viên hướng dẫn, em đã chọn đề tài "***Sơ đồ định danh mật và sơ đồ chữ ký số ứng dụng trong thương mại điện tử***" làm đề tài cho luận văn thạc sĩ của mình.

2. Mục tiêu nghiên cứu

- Tìm hiểu về lý thuyết mật mã học và hệ thống mật mã.
- Nghiên cứu chữ chữ ký số và quá trình xác thực chữ ký số.
-Chuẩn chữ ký số và hàm băm.

- Nghiên cứu các sơ đồ chữ ký số và các sơ đồ định danh mật.

- Nghiên cứu phương pháp chuyển sơ đồ định danh mật sang sơ đồ chữ ký số.

3. Phương pháp nghiên cứu

- Nghiên cứu qua các tài liệu như: sách, các bài báo, thông tin trên các website và các tài liệu liên quan.

- Phân tích, tổng hợp lý thuyết và giới thiệu các thuật toán của các sơ đồ định danh mật và cách chuyển sơ đồ định danh schnorr sang sơ đồ chữ ký schnorr.

- Sử dụng ngôn ngữ lập trình C# để triển khai xây dựng một chương trình ứng dụng về sơ đồ định danh schnorr và sơ đồ chữ ký schnorr ứng dụng trong thương mại điện tử.

4. Tổng quan luận văn

Luận văn được trình bày theo hình thức từ trên xuống. Bắt đầu của mỗi phần đều đưa ra những khái niệm cơ bản và quy định cho phần trình bày tiếp sau nhằm mục đích giúp dễ dàng trong khi đọc, dần dần đi sâu vào để thảo luận rõ hơn những vấn đề liên quan.

Luận văn cấu trúc thành 3 chương:

Chương 1: Tổng quan về mật mã và chữ ký số

Tìm hiểu lý thuyết mật mã, hệ thống mã khóa, chữ ký số, các sơ đồ chữ ký số.

Chương 2: Bài toán sơ đồ định danh mật và xác nhận thông tin

Trình bày bài toán định danh và sơ đồ xưng danh xác nhận danh tính. Các sơ đồ xưng danh Schnorr, Okamoto đòi hỏi người được ủy quyền tín nhiệm (TA) dựa trên bài toán tính logarit rời rạc, sơ đồ xưng danh Guillou – Quisquater, sơ đồ định danh dựa trên tính đồng nhất. Chuẩn chữ ký số và hàm băm.