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

TRẦN MINH KHƯƠNG

NGHIÊN CỨU THIẾT KẾ, ỨNG DỤNG KHÓA ĐIỆN TỬ ĐẢM BẢO AN TOÀN THÔNG TIN TRONG CÁC GIAO DỊCH ĐIỆN TỬ.

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

LỜI CAM ĐOAN

Tôi xin cam đoan luận văn "*Nghiên cứu thiết kế, ứng dụng khóa điện tử đảm bảo an toàn thông tin trong các giao dịch điện tử*" này là công trình nghiên cứu của riêng tôi. Các số liệu sử dụng trong luận văn là trung thực. Các kết quả nghiên cứu được trình bày trong luận văn chưa từng được công bố tại bất kỳ công trình nghiên cứu nào khác.

Trần Minh Khương.

MỤC LỤC

DANH MỤC CÁC KÍ HIỆU, CÁC CHỮ VIẾT TẮT

AES	Advanced Encryption Standard
DES	Data Encryption Standart
DSA	Digital Signature Algorithm
EEPROM	Electrically Erasable Programmable Read-Only Memory
IDEA	International Data Encryption Algorithm
ID	Identification
IP	Internet Protocol
IDEA	International Data Encryption Algorithm
MD	Message Digest
MIPS	Mega Instruction Per Second
NIST	National Institute of Standards and Technology
PIC	Programmable Intelligent Computer
PIN	Personal Indentification Number
PKI	Public Key Infrastructure
RISC	Reduced Instructions Set Computer
RSA	Rivest – Shamir – Adleman
SHA	Secure Hash Algorithm
USB	Univeral Serial Bus

DANH MỤC CÁC BẢNG

DANH MỤC CÁC HÌNH VẼ

MỞ ĐẦU

Ngày nay, với sự phát triển nhanh chóng của công nghệ và các mạng giao dịch toàn cầu, việc lưu trữ dữ liệu và trao đổi thông tin ngày càng đơn giản và thuận tiện hơn nhưng bên cạnh đó cũng nảy sinh những yêu cầu cao hơn về bảo mật thông tin trong các hệ thống và ứng dụng điện tử. Mật mã là phương pháp an toàn và hiệu quả nhất để đảm bảo an toàn, bí mật thông tin. Các kết quả của khoa học mật mã ngày càng được triển khai trong nhiều lĩnh vực khác nhau của đời sống – xã hội, trong đó phải kể đến rất nhiều những ứng dụng đa dạng trong lĩnh vực dân sự, thương mại... Các ứng dụng mã hóa thông tin cá nhân, trao đổi thông tin kinh doanh, thực hiện các giao dịch điện tử qua mạng... đã ngày càng trở nên gần gũi và quen thuộc với mọi người.

Các thiết bị mang tin đa dạng về chủng loại và ngày càng được sử dụng phổ biến (USB, thẻ nhớ, ổ cứng di động, máy tính xách tay...) rất thuận tiện trong sử dụng, nhưng cũng dễ mất an toàn như bị thất lạc, bị sao chép trộm... Các phần mềm gián điệp, mã độc hại có thể lấy cắp dữ liệu đã trở nên ngày càng phổ biến, đặc biệt là trong an ninh quốc phòng như phần mềm đọc bàn phím (Keylogger) dễ dàng trợ giúp cho việc lấy cắp mật khẩu, mã khóa.... Một vấn đề khác là việc mất an toàn khi gửi/nhận thư điện tử (email), khi sao chép, in ấn hoặc khi kết nối mạng cũng thường xuyên xảy ra. Một trong những vấn đề chính hay gặp trong thực tế của các hệ thống mã hóa hiện nay là vấn đề an toàn trong việc sinh khóa, bảo quản và sử dụng mã khóa.

Khóa điện tử (khóa cứng) là một sản phẩm sử dụng chuẩn kết nối tuần tự đa dụng USB (Univeral Serial Bus), có nghĩa là giao tiếp với máy tính thông qua cổng USB. Không như các USB lưu trữ dữ liệu thông thường, các sản phẩm này được chế tạo bởi nhiều kiểu kiến trúc phần cứng khác nhau, có thể là chip EEPROM, hay Smartchip,… có chức năng chính là bảo vệ bản

quyền phần mềm, bảo vệ sourcecode, license của sản phẩm phần mềm và mã hóa dữ liệu. Khóa cứng đã được nghiên cứu, sản xuất và đưa vào sử dụng rộng khắp trong lĩnh vực công nghệ thông tin nói chung và an toàn thông tin nói riêng ở trong cũng như ngoài nước. Các ngành như công nghệ phần mềm, ngân hàng, an ninh bảo mật… cũng nghiên cứu và sử dụng các thiết bị khóa cứng và e-Token trong việc bảo mật, chống sao chép, chữ ký số...

Hiện nay, một số công ty thử nghiệm giải pháp dùng khoá cứng trong bảo vệ dữ liệu và bảo vệ bản quyền phần mềm, một số loại như Hasp, Rockey, Unikey, USB-токен, SecureDongle,... Tuy nhiên, đây đều là các sản phẩm nhập khẩu, vì vậy khả năng phát triển những ứng dụng có sử dụng khóa cứng phải phụ thuộc vào nhà cung cấp nước ngoài và các thiết bị này không đảm bảo có bị lỗi cổng hậu (backdoor) hay không. Gần đây khoá cứng bảo vệ phần mềm cũng đã bị bẻ khoá nhờ công nghệ giả lập khoá cứng.

Với mong muốn áp dụng các phương pháp mã hóa vào việc bảo mật dữ liệu và trao đổi thư điện tử, đồng thời từng bước tìm hiểu, làm chủ công nghệ khóa cứng, tác giả chọn đề tài: ***"Nghiên cứu thiết kế, ứng dụng khóa điện tử đảm bảo an toàn thông tin trong các giao dịch điện tử"*** nhằm nghiên cứu, đề xuất giải pháp ứng dụng khóa cứng với các chức năng: là thiết bị lưu trữ mã khóa, đảm bảo nhỏ gọn, kết nối với máy tính thông qua cổng USB, kết hợp được với phần mềm mã hóa, có ID riêng cho từng thiết bị, có bộ nhớ đủ lớn để lưu trữ mã khóa, lưu trữ dữ liệu, thuận tiện trong sử dụng; xây dựng phần mềm kết hợp với khóa cứng để thực hiện việc quản lý mã khóa và mã hóa dữ liệu.

Mục tiêu của luận văn

Nghiên cứu sản phẩm khoá cứng ứng dụng trong việc mã hóa dữ liệu trên máy tính và khi trao đổi thư điện tử (email).

Nghiên cứu xây dựng phần mềm kết hợp với khóa cứng thực hiện mã hóa/giải mã dữ liệu trên máy tính.

Nghiên cứu thiết kế modul mã hóa và giao tiếp với máy tính thực hiện mã hóa luồng dữ liệu khi thực hiện giao tiếp giữa khóa cứng và máy tính.

Từng bước làm chủ thiết bị an toàn bảo mật có tích hợp bên trong các thuật toán mã và giải mã.

Cơ sở khoa học và tính thực tiễn của luận văn

Xuất phát từ vai trò của mật mã trong các giải pháp an toàn thông tin - nghiên cứu và ứng dụng mật mã để bảo vệ thông tin. Cụ thể là nghiên cứu phương pháp mã hoá AES (Advanced Encryption Standard – chuẩn mã hóa nâng cao) được Viện Tiêu chuẩn và Công nghệ Hoa Kỳ (NIST) chính thức công bố ngày 02/10/2000 và phương pháp mã hóa khóa công khai RSA; các mô hình thực hiện mã khối trên nền công nghệ nhúng, trong luận văn ứng dụng thực hiện trên chíp vi xử lý 16 bit tốc độ cao.

Nghiên cứu sản phẩm khóa cứng ứng dụng các phương pháp mã hóa hiện đại nhằm: bảo vệ dữ liệu trên máy tính và khi trao đổi tin; làm chủ công nghệ các sản phẩm an toàn bảo mật thông tin mang nhãn hiệu Việt.

Kết quả nghiên cứu của đề tài góp phần làm rõ các phương pháp mã hóa mới có tính bảo mật cao, đưa ra một giải pháp cho việc bảo vệ dữ liệu trên máy tính và khi trao đổi thông tin.

Nội dung của luận văn được chia thành các chương sau:

Chương 1: Đặt vấn đề

Trong chương này, nghiên cứu tổng quan về mật mã học, vai trò của mật mã trong bảo đảm an toàn bảo mật dữ liệu, một số nguy cơ mất an toàn