

**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

LỜI CẢM ƠN	i
LỜI CAM ĐOAN	ii
MỤC LỤC.....	iii
DANH MỤC CÁC KÍ HIỆU, CÁC CHỮ VIẾT TẮT	v
DANH MỤC CÁC BẢNG	vi
DANH MỤC CÁC HÌNH VẼ	vii
MỞ ĐẦU.....	1
Chương 1: ĐẶT VẤN ĐỀ	5
1.1. Tổng quan về mật mã	5
1.1.1. Mật mã học.....	5
1.1.2. Hệ mật mã (cryptosystem)	6
1.1.3. Mô hình truyền tin cơ bản của mật mã học và nguyên lý Kerckhoffs	7
1.1.4. Một số ứng dụng của mật mã học	9
1.2. Một số nguy cơ mất an toàn bảo mật thông tin.....	10
1.2.1. Mất mã khóa.....	10
1.2.2. Thất lạc các vật mang tin	11
1.2.3. Truy cập trái phép các phần mềm quan trọng.....	12
1.2.4. Mất an toàn khi gửi/nhận thư điện tử.....	13
1.3. Đề xuất giải pháp bảo đảm an toàn bảo mật dữ liệu.....	13
1.3.1. Dùng khóa cứng để lưu giữ mã khóa	13
1.3.2. Dùng khóa cứng để khóa máy tính, dùng USB có bảo vệ khi truy cập	15
1.3.3. Dùng khóa cứng để bảo vệ phần mềm có bản quyền và phần mềm quan trọng	15
Chương 2:	
NGHIÊN CỨU LỰA CHỌN CÁC THUẬT TOÁN MÃ HÓA.....	17
2.1. Hệ mật mã khóa bí mật. Chuẩn mã AES	17
2.1.1. Hệ mật mã khóa bí mật (quy trình mã hóa đối xứng).....	17

2.1.2. Chuẩn mã AES (Advanced Encryption Standard).....	18
2.2. Hệ mật mã khóa công khai. Hệ mã RSA	45
2.2.1. Hệ mật mã khóa công khai (quy trình mã hóa bất đối xứng)	45
2.2.2. Hệ mã RSA	49

Chương 3

NGHIÊN CỨU XÂY DỰNG VÀ THỰC HIỆN THỬ NGHIỆM KHÓA CỨNG KẾT HỢP VỚI PHẦN MỀM MÃ/GIẢI MÃ	56
3.1. Nghiên cứu thiết kế khóa cứng	56
3.1.1. Thiết kế của khóa cứng	56
3.1.2. Lựa chọn chip giao tiếp với máy tính thông qua cổng giao tiếp USB	59
3.1.3. Lựa chọn chip vi xử lý tốc độ cao thực hiện thuật toán mã/giải mã, lưu trữ mã khóa	60
3.1.4. Phần mềm soạn thảo chương trình điều khiển vi xử lý	62
3.1.5. Modul mã hoá/giải mã sử dụng thuật toán AES viết trên vi xử lý	63
3.2. Nghiên cứu xây dựng và thử nghiệm Modul phần mềm kết hợp với khóa cứng thực hiện mã hóa/giải mã dữ liệu trên máy tính dùng thuật toán AES	76
3.2.1. Nghiên cứu xây dựng modul.....	76
3.2.2. Kết quả thử nghiệm.....	81
3.3. Nghiên cứu xây dựng và thử nghiệm Modul phần mềm kết hợp với khóa cứng để mã hóa/giải mã dữ liệu khi trao đổi qua email dùng thuật toán RSA	82
3.3.1. Nghiên cứu xây dựng modul.....	82
3.3.2. Kết quả thử nghiệm.....	84
KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN.....	87
TÀI LIỆU THAM KHẢO.....	88

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

Bảng 2.1. Bảng các khái niệm và ký hiệu dùng trong thuật toán AES.....	22
Bảng 2.2. Bảng biểu diễn các xâu 4 bit trong hệ Hexa.....	23
Bảng 2.3. Giá trị di số shift(r, N_b)	30
Bảng 2.4. Bảng mã khóa mở rộng và cách xác định mã khóa của các chu kỳ 36	
Bảng 2.5. Tốc độ của thuật toán Brent –Pollard	54
Bảng 2.6. Thời gian dự đoán của việc phân tích ra thừa số nguyên tố của các số nguyên.....	55
Bảng 3.1. So sánh hai thuật toán mã hóa T-DES và AES	63
Bảng 3.2. Số chu kỳ của AES	65
Bảng 3.3. Ma trận khóa	65
Bảng 3.4. Ma trận dữ liệu.....	65
Bảng 3.5. Dịch vòng mã hóa	66
Bảng 3.6. Giá trị trước và sau khi thực hiện Row Shift.....	71
Bảng 3.7. Thời gian thực hiện và lưu lượng của thuật toán mã hóa AES trên thiết bị dsPIC	75
Bảng 3.8. Bộ nhớ sử dụng cho các thuật toán mã hóa	75
Bảng 3.8. Kết quả thử nghiệm Modul phần mềm kết hợp với khóa cứng mã hóa/giải mã dữ liệu trên máy tính dùng thuật toán AES	82
Bảng 3.9. Bảng kết quả thử nghiệm Modul phần mềm kết hợp với khóa cứng để mã hóa/giải mã dữ liệu khi trao đổi qua email dùng thuật toán RSA	85

DANH MỤC CÁC HÌNH VẼ

Hình 1.1. Mô hình truyền tin cơ bản của mật mã học.....	8
Hình 2.1. Mô hình hệ mật mã khóa bí mật	17
Hình 2.2. Các trạng thái của AES	24
Hình 2.3. Sơ đồ thuật toán.....	27
Hình 2.4. Thao tác SubBytes tác động trên từng byte của trạng thái	28
Hình 2.5. Bảng thế S-Table của thuật toán AES.....	29
Hình 2.6. Thao tác ShiftRows tác động trên từng dòng của trạng thái.....	30
Hình 2.7. Thao tác MixColumns tác động lên mỗi cột của trạng thái	32
Hình 2.8. Thao tác AddRoundKey tác động lên mỗi cột của trạng thái.....	33
Hình 2.9. Thao tác InvShiftRows tác động lên từng dòng của trạng thái hiện hành	38
Hình 2.10. Bảng thế cho phép biến đổi InvSubBytes	40
Hình 2.11. Mô hình hệ thống mã hóa với khóa công khai.....	47
Hình 3.1. Hình ảnh khóa cứng và các modul trên khóa cứng.....	57
Hình 3.2: Sơ đồ nguyên lý mạch điện trên khoá cứng.....	58
Hình 3.3. Dữ liệu trên bộ nhớ lưu trữ trên khóa cứng A và B.....	58
Hình 3.4. Hiện thị giao tiếp USB nhận được khi cắm khóa cứng vào máy tính	59
Hình 3.5. Sơ đồ cấu trúc dòng vi xử lý 16 bit.....	61
Hình 3.6. Giao diện soạn thảo chương trình cho vi xử lý.....	63
Hình 3.7. Sơ đồ khối của thuật toán mã hóa AES	64
Hình 3.8. Sơ đồ khối của quá trình giải mã	69
Hình 3.9. Quy trình thực hiện mã file sử dụng mã khoá lấy từ khoá cứng	76
Hình 3.10. Quy trình thực hiện giải mã file sử dụng mã khoá lấy từ khoá cứng	77
Hình 3.11. Giao diện phần mềm mã/giải mã file dữ liệu và quản lý mã khóa	77
Hình 3.12. Thông báo của phần mềm khi không cắm khóa cứng	78
Hình 3.13. Giao diện phần mềm khi nhập mật khẩu đúng	78
Hình 3.14. Giao diện phần mềm khi thực hiện mã hóa dữ liệu.	79
Hình 3.15. Giao diện phần mềm khi thực hiện giải mã dữ liệu.	80
Hình 3.16. Danh sách các file đã mã hóa.	80
Hình 3.17. Giao diện phần mềm thực hiện lựa chọn file để mã hóa và gửi thư điện tử.....	83
Hình 3.18. Giao diện phần mềm khi thực hiện mã hóa file tại máy đầu A. ...	83
Hình 3.19. Giao diện phần mềm thực hiện giải mã tại máy đầu B.....	84

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 (Universal 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-тoкeн, 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 chip 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