

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

HOÀNG VĂN QUYẾN

**ỨNG DỤNG HỆ MẬT MÃ KHÓA CÔNG KHAI
TRONG QUẢN LÝ ĐỀ THI**

LUẬN VĂN THẠC SĨ KHOA HỌC

Thái Nguyên - 2012

MỤC LỤC

MỞ ĐẦU	1
Chương 1 TỔNG QUAN HỆ MẬT MÃ KHÓA CÔNG KHAI	4
1.1. Khái niệm về hệ mật mã.....	4
1.1.1. Khái niệm chung về mật mã và hệ mật mã.....	4
1.1.2. Phân loại các hệ mật mã	6
1.2. Lý thuyết độ phức tạp	10
1.2.1. Khái niệm độ phức tạp của thuật toán	10
1.2.2. Các bài toán khó tính toán và ứng dụng trong mật mã học	12
1.3. Hệ mật mã khóa công khai.....	13
1.3.1. Các quan điểm cơ bản của hệ mật mã khoá công khai.....	13
1.3.3. Hoạt động của hệ mật mã khóa công khai.....	14
1.3.4. Các yêu cầu của hệ mật mã khóa công khai	14
1.4. Độ an toàn của hệ mật mã.....	15
1.2. Chữ ký số	16
1.2.1. Giới thiệu về chữ ký số.....	16
1.2.2. Quá trình ký và xác thực chữ ký.....	17
Chương 2 MỘT SỐ THUẬT TOÁN PHÂN PHỐI VÀ QUẢN LÝ KHÓA CÔNG KHAI	22
2.1. Hệ mật mã khóa công khai RSA	22
2.1.1. Cơ sở toán học của hệ mật mã RSA	22
2.1.2. Mô tả hệ mật mã RSA	24
2.1.3. Quá trình tạo khoá, mã hoá và giải mã.....	24
2.1.4. Tính đúng của quá trình giải mã	26
2.1.5. Chi phí thực hiện trong quá trình mã hóa và giải mã	28
2.1.6. Đánh giá độ mật của hệ mật mã khóa công khai RSA	28
2.1.7. Phân tích cơ chế hoạt động của hệ mã RSA.....	29
2.1.8. Khả năng bị bẻ khóa của hệ mã công khai RSA	30
2.2. Hệ mật mã khóa công khai ElGamal	33
2.2.1. Bài toán logarit rời rạc	34
2.2.2. Mô tả hệ mật mã ElGamal	34

2.2.3. Tính đúng của quá trình giải mã	36
2.2.4. Đánh giá độ an toàn và khả năng ứng dụng của hệ mật mã khóa công khai ElGamal.	36
2.3. Hệ mật mã khóa công khai Rabin	37
2.3.1. Sơ đồ hệ mã khóa Rabin	37
2.3.2. Tính an toàn của hệ mã hoá Rabin.....	40
2.3.3. Sử dụng dư thừa dữ liệu.....	41
2.3.4. Tính hiệu quả	42
2.4. Hệ mã hóa AES	43
2.4.1. Quá trình phát triển	43
2.4.2. Mô tả thuật toán	44
2.4.3. Mô tả mức cao của thuật toán.....	45
2.4.4. Tối ưu hóa.....	47
2.4.5. An toàn.....	47
2.4.5. Tấn công kênh bên (Side channel attacks)	48
Chương 3 XÂY DỰNG ỨNG DỤNG THỬ NGHIỆM	50
3.1. Bài toán quản lý đề thi trong hệ thống các trường phổ thông.....	50
3.2. Áp dụng hệ mật mã khóa công khai cho quản lý đề thi trong các trường phổ thông.....	52
3.2.1. Mô tả hệ thống.	52
3.2.2. Chức năng và giao diện chính của chương trình	54
3.2.3. Các bước thực hiện chương trình	56
3.2.5. Mã chương trình	64
Đánh giá kết quả thử nghiệm chương 3.....	64
KẾT LUẬN	65
TÀI LIỆU THAM KHẢO.....	66

LỜI CẢM ƠN

Tôi xin gửi lời cảm ơn tới trường Đại học CNTT & TT, Viện CNTT Việt Nam, nơi các thầy cô đã tận tình truyền đạt các kiến thức quý báu cho tôi trong suốt quá trình học tập. Xin cảm ơn Ban Giám Hiệu nhà trường và các cán bộ đã tạo điều kiện tốt nhất cho chúng tôi học tập và hoàn thành đề tài tốt nghiệp của mình. Đặc biệt, tôi xin gửi tới TS Bùi Văn Thanh, thầy đã tận tình chỉ bảo tôi trong suốt quá trình thực hiện đề tài lời cảm ơn và biết ơn sâu sắc nhất. Bên cạnh những kiến thức khoa học, thầy đã giúp tôi nhận ra những bài học về phong cách học tập, làm việc và những kinh nghiệm sống quý báu. Tôi xin bày tỏ lòng biết ơn tới gia đình, bạn bè, đồng nghiệp và những người thân đã động viên khích lệ tinh thần và giúp đỡ để tôi hoàn thành luận văn này.

Thái Nguyên, ngày 10 tháng 10 năm 2012

Hoàng Văn Quyển

DANH MỤC CÁC KÝ HIỆU, CÁC CHỮ VIẾT TẮT

STT	Ký hiệu/ Chữ viết tắt	Viết đầy đủ
1	RSA	Rivest - Shamir - Adleman
2	DES	Data Encryption Standard
3	AES	Advanced Encryption Standard
4	NIST	National Institute of Standards and Technology
5	FIPF	Farm Innovation and Promotion Fund
6	NSA	National Security Agency
7	THPT	Trung học phổ thông

LỜI CAM ĐOAN

Tôi xin cam đoan, toàn bộ nội dung liên quan tới đề tài được trình bày trong luận văn là bản thân tôi tự tìm hiểu và nghiên cứu, dưới sự hướng dẫn khoa học của TS Bùi Văn Thanh.

Các tài liệu, số liệu tham khảo được trích dẫn đầy đủ nguồn gốc. Tôi xin chịu trách nhiệm trước pháp luật lời cam đoan của mình.

Học viên thực hiện

Hoàng Văn Quyển

DANH MỤC CÁC BẢNG

	Trang
Bảng 1.1: Bảng chi phí thời gian phân tích số nguyên n ra thừa số nguyên tố.....	12
Bảng 2.1: Tóm tắt các bước tạo khoá, mã hoá, giải mã của Hệ RSA.....	20
Bảng 2.2: Bảng chi phí thời gian cần thiết để phân tích các số nguyên N	24

DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ

Trang

Hình 1.1: Sơ đồ hoạt động chung của hệ mật mã	5
Hình 1.2: Sơ đồ hoạt động của mã hóa khóa đối xứng	6
Hình 1.3: Sơ đồ hoạt động của mã hóa khóa không đối xứng	9
Hình 1.4: Lược đồ ký	18
Hình 1.5: Lược đồ xác thực	20
Hình 2.1: Đồ thị so sánh chi phí tấn công khóa bí mật và khóa công khai.	33
Hình 2.4: Bước SubBytes, một trong 4 bước của 1 chu trình.....	43
Hình 2.5: Mô tả thuật toán AES.....	44
Hình 2.6: Bước SubBytes	44
Hình 2.7: Bước ShiftRows.....	45
Hình.3.9: Sơ đồ bài toán quản lý đề thi của các trường THPT.....	51
Hình 3.10: Sơ đồ quy trình tổng quan hệ thống.....	52
Hình 3.11: Sơ đồ quy trình tạo khóa RSA	53
Hình 3.12: Sơ đồ quy trình mã hóa văn bản bằng thuật toán AES	53
Hình 3.13: Sơ đồ quy trình mã hóa khóa theo thuật toán RSA	53
Hình 3.14: Sơ đồ quy trình giải mã khóa theo thuật toán RSA	54
Hình 3.15: Giao diện chính của chương trình.....	54
Hình 3.16: Giao diện tạo khóa RSA	54
Hình 3.17: Mã hóa văn bản bằng AES	55
Hình 3.18: Mã hóa khóa bằng RSA	56
Hình 3.19: Giải mã khóa bằng RSA	56
Hình 3.20: Tạo khóa RSA tùy chọn.....	56
Hình 3.21: Tạo khóa RSA tự động	57
Hình 3.22: Lưu khóa RSA tự động thành tệp	57
Hình 3.23: Mã hóa nội dung văn bản.....	57
Hình 3.24: Mở tệp văn bản cần mã hóa	58
Hình 3.25: Thông báo mã hóa thành công.....	58
Hình 3.26: Xem nội dung tệp được mã hóa.....	58
Hình 3.27: Mã hóa tệp *.*	58
Hình 3.28: Chọn File cần mã hóa	59

Hình 3.29: Thông báo kết quả mã hóa.....	59
Hình 3.30: Xem kết quả file đã mã hóa.....	59
Hình 3.31: Giải mã nội dung văn bản.....	60
Hình 3.32: Chọn File cần giải mã.....	60
Hình 3.33: Thông báo kết quả giải mã.....	60
Hình 3.234: Xem nội dung tệp vừa giải mã.....	60
Hình 3.35: Giải mã File được mã hóa.....	61
Hình 3.36: Mở tệp cần giải mã.....	61
Hình 3.37: Thông báo kết quả giải mã.....	61
Hình 3.38: Xem nội dung tệp vừa giải mã.....	62
Hình 3.39: Mã hóa khóa RSA.....	62
Hình 3.40: Chọn File khóa cần mã hóa.....	62
Hình 3.41: Kết quả mã hóa khóa.....	63
Hình 3.42: Giải mã khóa RSA.....	63
Hình 3.43: Mở tệp giải mã khóa RSA.....	63
Hình 3.44: Kết quả giải mã khóa RSA.....	64

MỞ ĐẦU

Thế kỷ XXI là thế kỷ công nghệ thông tin. Công nghệ thông tin đã và đang tác động trực tiếp đến mọi mặt hoạt động kinh tế xã hội trên thế giới. Thông tin có vai trò hết sức quan trọng, vì vậy cần phải đảm bảo để thông tin không bị sai lệch, không bị thay đổi, hay bị lộ trong quá trình truyền từ nơi gửi đến nơi nhận. Với sự phát triển rất nhanh của công nghệ mạng máy tính, đặc biệt là mạng Internet, khối lượng thông tin ngày càng được truyền nhận nhiều hơn.

Vấn đề khó khăn đặt ra là làm sao giữ được tính bảo mật của thông tin, thông tin đến đúng được địa chỉ cần đến và không bị sửa đổi. Hậu quả sẽ khó lường nếu như thư được gửi cho một người nhưng lại bị một người khác xem trộm và sửa đổi nội dung bức thư trái với chủ ý của người gửi. Tệ hại hơn nữa là khi một hợp đồng được ký, gửi thông qua mạng và bị kẻ xấu sửa đổi những điều khoản trong đó. Người gửi thư bị hiểu nhầm vì nội dung bức thư bị thay đổi, còn hợp đồng bị phá vỡ bởi những điều khoản đã không còn như ban đầu. Điều này gây ra những mất mát cả về mặt tài chính và quan hệ, tình cảm, v.v... và còn có thể nêu ra rất nhiều tình huống tương tự. Mã hoá thông tin là một trong các phương pháp có thể đảm bảo được tính bảo mật của thông tin. Mã hoá, trong một mức độ nhất định, có thể giải quyết các vấn đề trên; một khi thông tin đã được mã hoá, kẻ xấu rất khó hoặc không thể giải mã để có được nội dung thông tin ban đầu.

Khi mã hóa, thông tin được biến đổi (được mã hóa) bằng thuật toán mã hóa thông qua việc sử dụng “khóa”. Chỉ có người dùng có cùng “khóa” mới phục hồi lại được thông tin ban đầu (giải mã). Do vậy “khóa” cần được bảo vệ nghiêm ngặt và được truyền từ người gửi đến người nhận trên một kênh an toàn riêng sao cho người thứ ba không thể biết được khóa. Phương pháp này được gọi là mã hóa bằng khóa riêng hoặc mật mã khóa đối xứng. Có một số chuẩn thuật toán khóa đối xứng, ví dụ như DES, AES, v.v... Người ta đã chứng minh được khả năng bảo mật cao của các thuật toán đối xứng chuẩn nói trên và chúng đã được kiểm định qua thời gian. Tuy nhiên, vấn đề nảy sinh với các thuật toán đối xứng là việc trao đổi khóa. Các bên tham gia giao tiếp đòi hỏi được chia sẻ một bí mật là “khóa”, “khóa” cần được trao đổi giữa họ qua một kênh thông tin an toàn. An toàn của thuật toán khóa đối xứng phụ thuộc vào độ mật của khóa. Khóa thường có độ dài hàng trăm bit, tùy thuộc vào thuật toán được sử dụng. Vì thông tin có thể trung chuyển qua các điểm trung gian