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 SỸ KHOA HỌC

Thái Nguyên - 2012

MỤC LỤC

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 Quyến

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 Quyến

DANH MỤC CÁC BẢNG

Trang

DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ

Trang

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 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 khoá. 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