ĐẠI HỌC THÁI NGUYÊN

ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

NGUYỄN QUANG TRUNG

HỆ MÃ HÓA ĐỐI XỨNG VÀ ỨNG DỤNG TRONG VẤN ĐỀ BẢO MẬT TÀI LIỆU TẠI TRUNG TÂM KỸ THUẬT TÀI LIỆU NGHIỆP VỤ

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

THÁI NGUYÊN, 2017

ĐẠI HỌC THÁI NGUYÊN

ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

NGUYỄN QUANG TRUNG

HỆ MÃ HÓA ĐỐI XỨNG VÀ ỨNG DỤNG TRONG VẤN ĐỀ BẢO MẬT TÀI LIỆU TẠI TRUNG TÂM KỸ THUẬT TÀI LIỆU NGHIỆP VỤ

Chuyên ngành: Khoa học máy tính

Mã số: 60 48 01 01

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Người hướng dẫn khoa học: TS. VŨ VINH QUANG

THÁI NGUYÊN, 2017

LỜI CAM ĐOAN

Sau quá trình học tập tại **Trường Đại học công nghệ thông tin & truyền thông**, với những kiến thức lý thuyết và thực hành đã tích lũy được, với việc vận dụng các kiến thức vào thực tế, em đã tự nghiên cứu các tài liệu, các công trình nghiên cứu, đồng thời có sự phân tích, tổng hợp, đúc kết và phát triển để hoàn thành luận văn thạc sĩ của mình.

Em xin cam đoan luận văn này là công trình do bản thân em tự tìm hiểu, nghiên cứu và hoàn thành dưới sự hướng dẫn của thầy giáo **TS. Vũ Vinh Quang**.

Thái Nguyên, tháng 5 năm 2017

Học viên

Nguyễn Quang Trung

MỤC LỤC

DANH MỤC CÁC KÍ HIỆU, CHỮ VIẾT TẮT

STT	Viết tắt	Đầy đủ	Ý nghĩa
1	AES	Advanced Encryption Standard	Chuẩn mã hóa cao cấp
2	BCNN	Bội Chung Nhỏ Nhất	
	CBC	Cipher Block Chaining	Chế độ mã hóa của AES khi mã hóa sử dụng cả key và kết quả của block trước làm tham số
3	DES	Data Encryption Standard	Chuẩn mã hóa dữ liệu
	ECB	Electronic Code Book	Chế độ mã hóa của AES trong đó các block được mã hóa riêng rẽ
4	GCD	Greatest Common Divisor	Ước chung lớn nhất
5	MDV	Mã Dịch Vòng	
6	TDES hoặc 3DES	Triple DES	DES bội ba
7	TTP	Trusted Third Party	Đơn vị thứ ba tin cậy
8	UCLN	Ước Chung Lớn Nhất	

DANH MỤC CÁC BẢNG BIỂU

DANH MỤC CÁC HÌNH VẼ

LỜI NÓI ĐẦU

Mã hóa là công cụ cơ bản của việc đảm bảo an toàn dữ liệu. Thời kỳ sơ khai, con người đã sử dụng nhiều phương pháp để bảo vệ các thông tin bí mật. Ban đầu, mật mã học được sử dụng phổ biến trong quân đội, qua nhiều cuộc chiến tranh, vai trò của mật mã ngày càng quan trọng và mang lại nhiều thành quả không nhỏ, chúng là nền tảng cho mật mã học ngày nay.

Ngày nay, các ứng dụng mã hóa và bảo mật thông tin đang được sử dụng ngày càng phổ biến trong các lĩnh vực khác nhau trên thế giới, từ các lĩnh vực an ninh, quân sự, quốc phòng cho đến các lĩnh vực dân sự như thương mại điện tử, ngân hàng… Với sự phát triển ngày càng nhanh chóng của Internet và các ứng dụng giao dịch điện tử trên mạng, nhu cầu bảo vệ thông tin trong các hệ thống và ứng dụng điện tử ngày càng được quan tâm và có ý nghĩa hết sức quan trọng. Cùng với sự phát triển của khoa học máy tính, các nghiên cứu và ứng dụng của các chuẩn mã hóa ngày càng trở nên đa dạng hơn.

Hiện nay, có nhiều phương pháp mã hóa, mỗi phương pháp có ưu, nhược điểm riêng. Tùy theo yêu cầu của môi trường ứng dụng mà người ta có thể dùng phương pháp này hay phương pháp kia. Có những môi trường cần phải an toàn tuyệt đối bất kể thời gian và chi phí. Có những môi trường lại cần giải pháp "dung hòa" giữa bảo mật và chi phí. Vấn đề bảo đảm an toàn cho các hệ thống thông tin là một trong những vấn đề quan trọng cần cân nhắc trong suốt quá trình thiết kế, thi công, vận hành và bảo dưỡng hệ thống thông tin.

Các hệ thống mã hóa được chia thành hai loại: hệ mã hóa khóa đối xứng (việc giải mã và mã hóa sử dụng chung một khóa) và hệ mã hóa công khai (mã hóa và giải mã dùng khóa khác nhau). Trong phạm vi luận văn của mình, tác giả tập trung vào nghiên cứu hệ mã hóa khoá đối xứng (mã hóa khóa bí mật), tập trung vào các thuật toán mã hóa cổ điển, chuẩn mã hóa dữ liệu DES và chuẩn mã hoá nâng cao AES.

Hệ mã hóa công khai có nhược điểm là tốc độ mã hóa và giải mã rất chậm, do vậy chỉ phù hợp sử dụng trong trao đổi khóa, trong khi đó hệ mã hóa đối xứng có tốc độ xử lý nhanh hơn rất nhiều và phù hợp với nhu cầu xử lý số lượng lớn tài liệu. Dựa trên thực tế về yêu cầu mã hóa tại trung tâm kỹ thuật tài liệu nghiệp vụ có đặc điểm đa dạng về thể loại và số lượng. Chính vì vậy tác giả đã lựa chọn nghiên cứu và ứng dụng giải pháp mã hóa đối xứng cho bài toán thực tế nơi tác giả đang công tác.

CHƯƠNG 1: CÁC KHÁI NIỆM CƠ BẢN VỀ AN TOÀN BẢO MẬT THÔNG TIN

Nội dung chính của chương 1 trình bày một số khái niệm cơ bản về vấn đề an toàn và bảo mật thông tin, khái niệm về hệ mật mã và cơ sở toán học về lý thuyết đồng dư. Các yêu cầu chính của một hệ thống mã hóa, khái niệm về thám mã làm cơ sở cho việc nghiên cứu các hệ mã hóa trong chương 2. Các kiến thức này được tham khảo trong các tài liệu [1, 2, 3, 4].

1.1. Tổng quan về an toàn và bảo mật thông tin

1.1.1. Khái niệm chung

Từ xưa đến nay thông tin luôn là yếu tố quan trọng trong các hoạt động của đời sống con người. Trong thời đại ngày nay, các phương thức truyền đạt thông tin ngày càng đa dạng và phát triển. Với sự ra đời của máy tính và mạng máy tính, việc trao đổi thông tin đã trở lên dễ dàng hơn, nhanh chóng hơn, đa dạng hơn. Nhưng kèm theo đó là các nguy cơ xâm phạm thông tin cũng ngày càng tăng.

Khi nhu cầu trao đổi thông tin dữ liệu ngày càng lớn và đa dạng, các tiến bộ về điện tử - viễn thông và công nghệ thông tin không ngừng được phát triển ứng dụng để nâng cao chất lượng và lưu lượng truyền tin thì các quan niệm ý tưởng và biện pháp bảo vệ thông tin dữ liệu cũng được đổi mới. Bảo vệ an toàn thông tin dữ liệu là một chủ đề rộng, có liên quan đến nhiều lĩnh vực và trong thực tế có thể có rất nhiều phương pháp được thực hiện để bảo vệ an toàn thông tin dữ liệu. Các phương pháp bảo vệ an toàn thông tin dữ liệu có thể được tổng kết vào ba nhóm sau:

- Bảo vệ an toàn thông tin bằng các biện pháp hành chính.
- Bảo vệ an toàn thông tin bằng các biện pháp kỹ thuật (phần cứng).
- Bảo vệ an toàn thông tin bằng các biện pháp thuật toán (phần mềm).

Ba nhóm trên có thể được ứng dụng riêng rẽ hoặc phối kết hợp. Môi trường khó bảo vệ an toàn thông tin nhất và cũng là môi trường đối phương dễ xâm nhập nhất đó là môi trường mạng và truyền tin. Biện pháp hiệu quả nhất và kinh tế nhất hiện nay trên mạng truyền tin và mạng máy tính là biện pháp thuật toán.

An toàn thông tin bao gồm các nội dung sau:

- Tính bí mật: tính kín đáo riêng tư của thông tin.