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

NGUYỄN THỊ THỦY

TÌM HIỂU CHUẨN MẬT MÃ DỮ LIỆU DES (DATA ENCRYPTION STANDARD) VÀ ĐÁNH GIÁ ĐỘ AN TOÀN

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

THÁI NGUYÊN - 2014

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

NGUYỄN THỊ THỦY

TÌM HIỂU CHUẨN MẬT MÃ DỮ LIỆU DES (DATA ENCRYPTION STANDARD) VÀ ĐÁNH GIÁ ĐỘ AN TOÀN

Chuyên ngành: KHOA HỌC MÁY TÍNH
Mã số: 60 48 01

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

HƯỚNG DẪN KHOA HỌC: TS. HỒ VĂN CANH

THÁI NGUYÊN - 2014

LỜI CAM ĐOAN

Tôi xin cam đoan luận văn là công trình nghiên cứu của riêng cá nhân tôi, không sao chép của ai do tôi tự nghiên cứu, đọc, dịch tài liệu, tổng hợp và thực hiện. Nội dung lý thuyết trong trong luận văn tôi có sử dụng một số tài liệu tham khảo như đã trình bày trong phần tài liệu tham khảo. Các số liệu, chương trình phần mềm và những kết quả trong luận văn là trung thực và chưa được công bố trong bất kỳ một công trình nào khác.

Thái Nguyên, ... tháng .... năm 2014

Học viên thực hiện

Nguyễn Thị Thủy

LỜI CẢM ƠN

Để hoàn thành chương trình cao học và viết luận văn này, tôi đã nhận được sự hướng dẫn, giúp đỡ và góp ý nhiệt tình của quý thầy cô trường Đại học Công nghệ thông tin và Truyền Thông Thái Nguyên.

Trước hết, tôi xin chân thành cảm ơn đến quý thầy cô trường Đại học Công nghệ thông tin và Truyền thông Thái Nguyên, đặc biệt là những thầy cô đã tận tình dạy bảo cho tôi suốt thời gian học tại trường.

Tôi xin gửi lòng biết ơn sâu sắc đến Thầy giáo: **TS. Hồ Văn Canh** đã dành rất nhiều thời gian và tâm huyết hướng dẫn nghiên cứu và giúp tôi hoàn thành luận văn tốt nghiệp.

Nhân đây, tôi xin chân thành cảm ơn Ban giám hiệu trường Đại học Công nghệ thông tin và Truyền thông Thái Nguyên cùng quý thầy cô trong khoa Khoa học máy tính và khoa sau đại học đã tạo điều kiện để tôi học tập và hoàn thành tốt khoá học.

Mặc dù tôi đã có nhiều cố gắng hoàn thiện luận văn bằng tất cả sự nhiệt tình và năng lực của mình, tuy nhiên không thể tránh khỏi những thiếu sót, rất mong nhận được những đóng góp quý báu của quý thầy cô và các bạn.

Tôi xin thành cảm ơn !

Thái Nguyên, Ngày ……tháng…… năm 2014

Học viên

Nguyễn Thị Thủy

MỤC LỤC

DANH MỤC BẢNG BIỂU

DANH MỤC HÌNH VẼ

MỞ ĐẦU

Ngày nay, 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 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 ngày càng được đổi mới. Bảo vệ an toàn thông tin dữ liệu và 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.

Trong số các phương pháp đảm bảo an toàn thông tin thì phương pháp mật mã hoá (cryptography) được sử dụng rộng rãi và đảm bảo an toàn nhất. Tuy nhiên phương pháp mật mã hoá cũng có những nhược điểm quan trọng, nếu là phương pháp mật mã hoá không tốt (mặc dù việc quản lý khoá mã được giả thiết là an toàn) thì rất nguy hiểm. Vậy làm thế nào để đánh giá được chất lượng một hệ mật mã là tốt? Hiểu được tính cấp thiết và quan trọng nên tôi chọn đề tài "***Tìm hiểu chuẩn mật mã dữ liệu DES (Data Encryption Standard) và đánh giá độ an toàn***". Luận văn đóng góp một phần nhỏ vào việc nhìn nhận và đánh giá một hệ mật an toàn từ đó xây dựng các phương pháp bảo mật tốt hơn.

Luận văn gồm các chương sau:

- *Chương* 1: Tổng quan về bảo mật thông tin
- *Chương* 2: Tìm hiểu về chuẩn mật mã DES và đánh giá độ an toàn
- *Chương* 3: Chương trình mô phỏng thuật toán DES

CHƯƠNG 1
TỔNG QUAN VỀ BẢO MẬT THÔNG TIN

1.1 TỔNG QUAN VỀ AN TOÀN THÔNG TIN DỮ LIỆU

Trải qua nhiều thế kỷ hàng loạt các giao thức (Protocol) và cơ chế (Mechanism) đã được tạo ra để đáp ứng nhu cầu an toàn bảo mật thông tin khi nó được truyền tải trên các hệ thống truyền tin số. Thường thì các mục tiêu của an toàn bảo mật thông tin không thể đạt được nếu chỉ đơn thuần dựa vào các thuật toán toán học và các giao thức, mà để đạt được điều này đòi hỏi cần có các kỹ thuật mang tính thủ tục và sự tôn trọng mang tính điều luật. Chẳng hạn sự bí mật của các bức thư tay là do sự phân tán các lá thư đã có đóng dấu bởi dịch vụ thư tín đã được chấp nhận. Tính an toàn về mặt vật lý của các lá thư là hạn chế (nó có thể bị xem trộm) nên để đảm bảo sự bí mật của bức thư pháp luật đưa ra quy định: việc xem thư mà không được sự đồng ý của chủ nhân hoặc những người có thẩm quyền là phạm pháp và sẽ bị trừng phạt. Đôi khi mục đích của an toàn bảo mật thông tin lại đạt được nhờ chính phương tiện vật lý mang chúng, chẳng hạn như tiền giấy đòi hỏi phải được in bằng loại mực và giấy tốt để không bị làm giả.

Về mặt lý tưởng việc lưu giữ thông tin là không có nhiều thay đổi đáng kể qua thời gian. Ngày xưa thông tin thường được lưu và vận chuyển trên giấy tờ, trong khi giờ đây chúng được lưu dưới dạng số hoá và được vận chuyển bằng các hệ thống viễn thông (các hệ thống có dây hoặc không dây). Tuy nhiên sự thay đổi đáng kể đến ở đây chính là khả năng sao chép và thay đổi thông tin. Người ta có thể tạo ra hàng ngàn mẫu tin giống nhau và không thể phân biệt được nó với bản gốc. Với các tài liệu lưu trữ và vận chuyển trên giấy điều này khó khăn hơn nhiều. Và điều cần thiết đối với một xã hội mà thông tin hầu hết được lưu và vận chuyển trên các phương tiện điện tử chính là các phương tiện đảm bảo an toàn bảo mật thông tin độc lập với các phương tiện lưu trữ và vận chuyển vật lý của nó. Phương tiện đó chính là mật mã học, một ngành khoa học có lịch sử lâu đời dựa trên nền tảng các thuật toán toán học, số học, xác suất và các môn khoa học khác.