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

TRƯƠNG HÀ DIỆP

NGHIÊN CỨU TÌM HIỂU HỆ MÃ HÓA ĐỒNG CẤU VÀ ỨNG DỤNG

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

THÁI NGUYÊN - 2016

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

TRƯƠNG HÀ DIỆP

NGHIÊN CỨU TÌM HIỂU HỆ MÃ HÓA ĐỒNG CẤU VÀ ỨNG DỤNG

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 HỒ VĂN CANH

THÁI NGUYÊN - 2016

LỜI CAM ĐOAN

Tôi xin cam đoan luận văn **"*Nghiên cứu tìm hiểu hệ mã hóa đồng cấu và ứng dụng*"** là công trình nghiên cứu của cá nhân tôi tìm hiểu, nghiên cứu dưới sự hướng dẫn của TS Hồ Văn Canh. Các kết quả là hoàn toàn trung thực, toàn bộ nội dung nghiên cứu của luận văn, các vấn đề được trình bày đều là những tìm hiểu và nghiên cứu của chính cá nhân tôi hoặc là được trích dẫn từ các nguồn tài liệu được trích dẫn và chú thích đầy đủ.

TÁC GIẢ LUẬN VĂN

Trương Hà Diệp

LỜI CẢM ƠN

Học viên xin bày tỏ lời cảm ơn chân thành tới tập thể các thầy cô giáo Viện công nghệ thông tin, các thầy cô giáo Trường Đại học Công nghệ thông tin và truyền thông - Đại học Thái Nguyên đã mang lại cho học viên kiến thức vô cùng quý giá và bổ ích trong suốt quá trình học tập chương trình cao học tại trường. Đặc biệt học viên xin bày tỏ lòng biết ơn sâu sắc tới thầy giáo TS Hồ Văn Canh đã định hướng khoa học và đưa ra những góp ý, gợi ý, chỉnh sửa quý báu, quan tâm, tạo điều kiện thuận lợi trong quá trình nghiên cứu hoàn thành luận văn này.

Cuối cùng, học viên xin chân thành cảm ơn các bạn bè đồng nghiệp, gia đình và người thân đã quan tâm, giúp đỡ và chia sẻ với học viên trong suốt quá trình học tập.

Do thời gian và kiến thức có hạn nên luận văn chắc không tránh khỏi những thiếu sót nhất định. Học viên rất mong nhận được những sự góp ý quý báu của thầy cô và các bạn.

Thái Nguyên, ngày 28 tháng 12 năm 2016

HỌC VIÊN

Trương Hà Diệp

MỤC LỤC

MỤC CÁC HÌNH VẼ, ĐỒ THỊ

DANH MỤC BẢNG BIỂU

MỞ ĐẦU

1. Đặt vấn đề

Để đảm bảo các thông tin quan trọng liên quan đến Quốc phòng, An ninh và Thương mại, người ta sử dụng công nghệ mật mã. Có hai loại hệ mật mã được dùng là mật mã khóa đối xứng và mật mã khóa bất đối xứng (Asymmetric key). Hệ thống mật mã bất đối xứng chủ yếu được sử dụng trong môi trường chữ ký số (digital signatures), trong xác thực và trong việc trao đổi các khóa mã đối xứng (symmetric keys). Mật mã đối xứng đóng vai trò quan trọng trong lĩnh vực bảo mật dữ liệu. Mật mã đối xứng có hai loại chính là mật mã hiện đại như mật mã DES (Data Enecryption Standard), mật mã AES (Advanced Encryption Standard), mật mã IDEA (International Data Encryption Algorithm)… và mật mã truyền thống. Mật mã truyền thống rất đơn giản và thuận lợi mà thế giới đã sử dụng hàng thế kỷ trước. một nhược điểm cơ bản của mật mã truyền thống là độ bảo mật không cao vì không gian khóa thường quá nhỏ.

Mục đích của đề tài luận văn là nghiên cứu thuật toán mã hóa trên cơ sở kết hợp các mật mã truyền thống thành một hệ mật mã có độ bảo mật cao hơn nhiều trên cơ sở đánh giá tính ngẫu nhiên của nó bằng kỹ thuật của lý thuyết thống kê toán học.

2. Đối tượng và phạm vi nghiên cứu

Đề tài luận văn sẽ nghiên cứu và trình bày phương pháp tạo ra một thuật toán mã hóa từ các thuật toán mật mã truyền thống nhưng có độ bảo mật cao hơn.

3. Hướng nghiên cứu của đề tài

Đề tài luận văn tập trung tìm hiểu hệ mật mã đồng cấu, trên cơ sở đó xây dựng một hệ mật mã đồng cấu sử dụng các hệ mật mã truyền thống, đưa ra một phương pháp khắc phục được những lỗ hổng về độ an toàn của các hệ mật mã này.

4. Những nội dung nghiên cứu chính

Luận văn gồm 3 chương.

Chương 1: Mật mã cổ điển và hệ mật mã đồng cấu

Chương 2: Hệ mật mã DES và hệ mật IDEA

Chương 3: Phương pháp mã hóa tự đồng cấu mở rộng không gian khóa cho các mã cổ điển