

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

TRƯỜNG 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

TRƯỜNG 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

|   |     |
|---|-----|
| LỜI CAM ĐOAN .....  | i   |
| LỜI CẢM ƠN .....  | ii  |
| MỤC LỤC.....  | iii |
| MỤC CÁC HÌNH VẼ, ĐỒ THỊ .....                                   | vi  |
| MỞ ĐẦU.....   | 1   |
| CHƯƠNG 1 .....  | 3   |
| MẬT MÃ CỔ ĐIỂN VÀ HỆ MẬT MÃ ĐỒNG CẤU .....                      | 3   |
| 1.1 Khái quát hệ mật mã .....                                   | 3   |
| 1.1.1 Khái niệm.....  | 3   |
| 1.1.2 Định nghĩa.....   | 3   |
| 1.1.3 Những yêu cầu đối với hệ mật mã .....                     | 4   |
| 1.2 Một số hệ mật mã đơn giản .....                             | 5   |
| 1.2.1 Mã dịch vòng ( shift cipher).....                         | 5   |
| 1.2.1.1 Định nghĩa (modulo): <i>Định nghĩa về đồng dư</i> ..... | 5   |
| 1.2.1.2 Định nghĩa mã dịch vòng:.....                           | 6   |
| 1.2.2 Mã thay thế (MTT) .....                                   | 7   |
| 1.2.3 Mã Anffine .....  | 8   |
| 1.2.3.1 Định lý (đồng dư thức) .....                            | 9   |
| 1.2.3.2 Định nghĩa (hàm Euler) .....                            | 9   |
| 1.2.3.3 Định nghĩa (phần tử nghịch đảo trong phép nhân).....    | 10  |
| 1.2.4 Mã Vigenere.....  | 13  |
| 1.2.5 Mật mã Hill.....  | 14  |
| 1.2.5.1 Khái niệm.....  | 14  |

|   |           |
|---|-----------|
| 1.2.5.2 Định nghĩa (ma trận đơn vị) .....             | 14        |
| 1.2.5.3 Định nghĩa (Định thức của ma trận) .....      | 15        |
| 1.2.5.4 Định lý (ma trận nghịch đảo).....             | 15        |
| 1.2.5.5 Định nghĩa mật mã Hill .....                  | 15        |
| 1.2.6 Mã hóa hoán vị.....                             | 15        |
| 1.2.7 Thám mã .....                                   | 17        |
| 1.3 Các phương pháp mã hóa đối xứng .....             | 17        |
| 1.3.1 Hệ mã hóa DES .....                             | 17        |
| 1.3.2 Hệ mã hóa AES .....                             | 19        |
| 1.3.3 Hệ mã hóa IDEA.....                             | 19        |
| 1.4 Hệ mã hóa đồng cấu.....                           | 21        |
| 1.4.1 Định nghĩa.....                                 | 21        |
| 1.4.1.1 Định nghĩa đồng cấu trong toán học .....      | 21        |
| 1.4.1.2 Định nghĩa hệ mã hoá đồng cấu .....           | 21        |
| 1.4.2 Hệ mã hoá đồng cấu cộng.....                    | 21        |
| 1.4.3 Hệ mã hoá đồng cấu nhân.....                    | 22        |
| <b>CHƯƠNG 2. HỆ MẬT MÃ DES VÀ HỆ MẬT MÃ IDEA.....</b> | <b>23</b> |
| 2.1 Hệ mật mã DES .....                               | 23        |
| 2.1.1 Mô tả hệ mật .....                              | 23        |
| 2.1.2 Quá trình mã hóa .....                          | 24        |
| 2.1.2.1 Giai đoạn 1: Cách tính biến $x_0$ .....       | 24        |
| 2.1.2.2 Giai đoạn 2.....                              | 25        |
| 2.1.2.3 Giai đoạn 3.....                              | 32        |
| 2.1.2.4 Ví dụ.....                                    | 32        |
| 2.1.3 Quá trình giải mã .....                         | 36        |
| 2.1.3.1 Thuật toán .....                              | 37        |

|   |           |
|---|-----------|
| 2.1.3.2 Chứng minh thuật toán .....                                       | 37        |
| 2.1.4 Ưu nhược điểm của hệ mật DES .....                                  | 39        |
| 2.1.4.1 Ưu điểm.....  | 39        |
| 2.1.4.2 Nhược điểm của DES .....  | 39        |
| 2.1.5 Độ an toàn của DES .....  | 41        |
| 2.1.5.1 Các đặc trưng an toàn cơ bản của một hệ mã khối.....              | 41        |
| 2.1.5.2 Độ an toàn của DES trước một vài phương pháp tấn công phá mã..... | 42        |
| 2.2 Hệ mật IDEA .....   | 43        |
| 2.2.1 Mô tả hệ mật IDEA.....  | 43        |
| 2.2.2 Các phép toán sử dụng trong IDEA.....                               | 43        |
| 2.2.3 Mã hoá và giải mã trong IDEA.....                                   | 45        |
| 2.2.3.1 Mã hoá.....   | 45        |
| 2.2.4 Quá trình làm việc của một Modul .....                              | 51        |
| <b>CHƯƠNG 3 NGHIÊN CỨU PHƯƠNG PHÁP MÃ HÓA TỰ ĐỒNG</b>                     |           |
| <b>CẤU MỞ RỘNG KHÔNG GIAN KHÓA CHO CÁC MÃ CỔ ĐIỂN .</b>                   | <b>55</b> |
| 3.1 Mở đầu .....  | 55        |
| 3.2 Nội dung phương pháp .....  | 55        |
| 3.2.1 Khái niệm, định nghĩa.....  | 55        |
| 3.2.2 Thuật toán mã hóa.....  | 55        |
| 3.2.3. Ví dụ.....   | 55        |
| 3.2.4 Thuật toán giải mã .....  | 59        |
| 3.3 Đánh giá độ an toàn của thuật toán.....                               | 61        |
| 3.4 Đề xuất hướng ứng dụng trong thực tế.....                             | 62        |
| <b>4. KẾT LUẬN HƯỚNG NGHIÊN CỨU .....</b>                                 | <b>63</b> |
| <b>TÀI LIỆU THAM KHẢO .....</b>   | <b>64</b> |

## MỤC CÁC HÌNH VẼ, ĐỒ THỊ

|   |    |
|---|----|
| Hình 1.1. Kênh liên lạc .....   | 4  |
| Hình 1.2 Mã dịch vòng.....  | 6  |
| Hình 1.3 Mã thay thế.....   | 7  |
| Hình 1.4. Mã hóa Anffine.....   | 12 |
| Hình 1.5. Phương pháp mã hóa Vigenere.....  | 13 |
| Hình 1.6. Mật mã Hill.....  | 15 |
| Hình 1.7 Mã hoán vị.....  | 16 |
| Hình 2.1 Biểu diễn dãy 64 bit $x$ thành 2 thành phần $L$ và $R$ .....                   | 23 |
| Hình 2.2 Quy trình phát sinh dãy $L_i R_i$ từ dãy $L_{i-1} R_{i-1}$ và khóa $K_i$ ..... | 24 |
| Hình 2.3 Sơ đồ của hàm mở rộng .....  | 25 |
| Hình 2.4 Sơ đồ tạo khóa con.....  | 26 |
| Hình 2.5 Hàm $f$ .....  | 28 |
| Hình 2.6 Quá trình mã hóa DES .....   | 32 |
| Hình 2.7 Sơ đồ giải mã .....  | 38 |
| Hình 2.8 Cấu trúc Multiplication/Additio (MA) .....                                     | 44 |
| Hình 2.9 Cấu trúc IDEA .....  | 45 |
| Hình 2.10 Cấu trúc một modul (Modul 1).....   | 46 |
| Hình 2.11 Hàm biến đổi của IDEA .....   | 47 |
| Hình 2.12 Mã hoá và giải mã trong IDEA.....   | 49 |
| Hình 2.13 Cấu trúc một modul (Modul 1).....   | 51 |
| Hình 3.1: Mã hóa thông điệp .....   | 59 |
| Hình 3.2: Giải mã thông điệp.....   | 61 |



**DANH MỤC BẢNG BIỂU**

|  |    |
|--|----|
| Bảng 2.2 Bảng chọn E bit .....           | 26 |
| Bảng 2.3 Hoán vị $IP^{-1}$ .....         | 27 |
| Bảng 2.5 Hoán vị PC - 2 .....            | 27 |
| Bảng 2.7 8 hộp S-Box.....                | 31 |
| Bảng 2.8 Phép hoán vị P .....            | 31 |
| Bảng 2.9 16 vòng lặp mã .....            | 36 |
| Bảng 2.10 Các khóa yếu của DES .....     | 40 |
| Bảng 2.11 Các khóa nửa yếu của DES ..... | 40 |

## 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 Encryption 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