

ĐẠI HỌC THÁI NGUYÊN  
TR- ỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

**NGUYỄN THIÊN PHI**

**TÌM HIỂU MẬT MÃ HỘP TRẮNG  
(WHITEBOX CRYPTOGRAPHY) VÀ ỨNG DỤNG  
TRONG HỆ THỐNG THU PHÁT THÔNG TIN SỐ**

**LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH**

**THÁI NGUYÊN - NĂM 2014**

ĐẠI HỌC THÁI NGUYÊN  
TR- ỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

NGUYỄN THIÊN PHI

**TÌM HIỂU MẬT MÃ HỘP TRẮNG  
(WHITEBOX CRYPTOGRAPHY) VÀ ỨNG DỤNG  
TRONG HỆ THỐNG THU PHÁT THÔNG TIN SỐ**

**LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH**

**Chuyên ngành: KHOA HỌC MÁY TÍNH**

**Mã số: 60 48 01**

**Người hướng dẫn khoa học: PGS.TS. TRỊNH NHẬT TIẾN**

**Thái Nguyên, 2014**

## LỜI CAM ĐOAN

Học viên xin cam đoan, toàn bộ nội dung liên quan tới đề tài được trình bày trong luận văn là bản thân học viên tự tìm hiểu và nghiên cứu, dưới sự hướng dẫn khoa học của thầy PGS.TS.Trịnh Nhật Tiến.

Các tài liệu, số liệu tham khảo được trích dẫn đầy đủ nguồn gốc. Học viên xin chịu hoàn toàn trách nhiệm và chịu mọi hình thức kỷ luật theo quy định cho lời cam đoan của mình.

*Thái Nguyên, 29 tháng 09 năm 2014*

**Học viên thực hiện**

**Nguyễn Thiên Phi**

## LỜI CẢM ƠN

Luận văn này được thực hiện tại trường Đại học Công nghệ Thông tin và Truyền thông - Đại học Thái Nguyên dưới sự hướng dẫn của thầy PGS. TS. Trịnh Nhật Tiến.

Trước tiên, Học viên xin được bày tỏ lòng cảm ơn và sự kính trọng của mình đến các thầy, cô giáo đã tận tình truyền đạt các kiến thức quý báu cho học viên trong suốt quá trình học tập.

Đặc biệt học viên xin bày tỏ lòng biết ơn sâu sắc tới thầy PGS.TS. Trịnh Nhật Tiến, người định hướng, hướng dẫn học viên trong quá trình thực hiện luận văn này, những lời động viên chỉ bảo giúp học viên vượt qua những khó khăn để học viên hoàn thành tốt luận văn của mình. Bên cạnh những kiến thức khoa học, thầy giáo đã giúp học viên nhận ra những bài học về phong cách học tập, làm việc và những kinh nghiệm sống quý báu.

Nhân dịp này, học viên cũng xin gửi lời cảm ơn đến gia đình, bạn bè, đồng nghiệp và những người thân đã tạo điều kiện giúp đỡ, động viên, trợ giúp về tinh thần, vật chất để học viên hoàn thành luận văn này.

## MỤC LỤC

LỜI CAM ĐOAN .....	i
LỜI CẢM ƠN .....	ii
MỤC LỤC .....	iii
DANH MỤC HÌNH .....	v
DANH MỤC TỪ VIẾT TẮT .....	vii
MỞ ĐẦU .....	1
1. Lý do chọn đề tài .....	1
2. Đối tượng và phạm vi nghiên cứu .....	2
3. Hướng nghiên cứu của đề tài .....	3
4. Những nội dung nghiên cứu chính .....	3
5. Phương pháp nghiên cứu .....	3
6. Ý nghĩa khoa học và thực tiễn của đề tài .....	4
CHƯƠNG 1. VẤN ĐỀ AN TOÀN TRONG HỆ THỐNG THU PHÁT THÔNG TIN SỐ .....	5
1.1. HỆ THỐNG THU PHÁT THÔNG TIN SỐ .....	5
1.1.1. Các khái niệm cơ bản .....	5
1.1.2. Những thách thức về an toàn bảo mật .....	6
1.2. PHƯƠNG PHÁP MÃ HOÁ KHỐI .....	6
1.2.1. Mật mã học .....	6
1.2.2. Mã hóa khối .....	8
1.2.3. Một số cách tấn công vào hệ mã hóa hiện đại .....	16
1.3. MÃ HÓA HỘP TRẮNG TRÊN NỀN MÃ HÓA KHỐI .....	18
1.3.1. Giới thiệu về mã hóa hộp trắng .....	18
1.3.2. Các khái niệm cơ bản .....	19
1.3.3. Đề xuất sử dụng mật mã hộp trắng .....	21

CHƯƠNG 2. MÃ HÓA RIJNDAEL VÀ MÃ HOÁ HỘP TRẮNG AES.....	21
2.1. PHƯƠNG PHÁP MÃ HÓA RIJNDAEL .....	22
2.1.1. Giới thiệu.....	22
2.1.2. Quy trình mã hóa.....	22
2.1.3. Phát sinh khóa của mỗi chu kỳ.....	34
2.2. KỸ THUẬT XÂY DỰNG MÃ HÓA HỘP TRẮNG.....	42
2.2.1. Khái niệm và các ký hiệu trong mô tả thuật toán. ....	42
2.2.2. Kỹ thuật mã hóa hộp trắng trên AES .....	43
2.2.3. Hiệu suất của mật mã hộp trắng.....	51
CHƯƠNG 3. CHƯƠNG TRÌNH MÃ HÓA HỘP TRẮNG AES VÀ ỨNG DỤNG TRONG HỆ THỐNG IPTV .....	54
3.1. BÀI TOÁN THỰC TẾ.....	54
3.2. SET TOP BOX VÀ GIẢI PHÁP HIỆN NAY.....	55
3.3. SỬ DỤNG MÃ HÓA HỘP TRẮNG MỀM HÓA SET-TOP BOX....	57
3.3.1. Cài đặt chương trình mã hóa trên AES .....	57
3.3.2. Đề xuất mềm hóa Set-top box.....	66
3.3. NHẬN XÉT .....	68
KẾT LUẬN.....	70
TÀI LIỆU THAM KHẢO.....	71

## DANH MỤC HÌNH

Hình 1.1 Quá trình truyền tin trong hệ thống thông tin số.....	5
Hình 1.2 Mô hình cơ bản của truyền tin bảo mật .....	7
Hình 1.3 Cấu trúc thuật toán Feistel dùng trong DES .....	10
Hình 1.4 Hàm F (F-function) dùng trong DES .....	11
Hình 1.5 Mô tả thuật toán tạo khóa con cho các chu trình .....	13
Hình 1.6 Biến đổi của hàm SubBytes .....	14
Hình 1.7 Biến đổi của hàm ShiftRows.....	15
Hình 1.8 Biến đổi của hàm MixColumns .....	15
Hình 1.9 Biến đổi của hàm AddRoundKey .....	16
Hình 1.10 Phương pháp Entropy Attack.....	17
Hình 1.11 Mô hình hộp đen truyền thống.....	19
Hình 1.12 Kẻ thù công tấn công trong mô hình hộp trắng .....	20
Hình 1.13 Mô hình Mật mã hộp trắng .....	20
Hình 2.1. Biểu diễn dạng ma trận trạng thái ( $N_b = 6$ ) và mã khóa ( $N_k = 4$ )..	23
Hình 2.2 Quy trình mã hóa Rijndael .....	24
Hình 2.3 Thuật toán Mã hóa và giải mã Rijndael .....	26
Hình 2.4 Thao tác SubBytes tác động trên từng byte của trạng thái .....	27
Hình 2.5 Bảng thay thế S-box qua phép biến đổi SubBytes.....	28
Hình 2.6 Thao tác ShiftRows tác động trên từng dòng của trạng thái.....	28
Hình 2.7 Giá trị di số $\text{shift}(r, N_b)$ .....	29
Hình 2.8 Các thao tác MixColumns tác động lên mỗi cột của trạng thái .....	31
Hình 2.9 Các thao tác AddRoundKey tác động lên mỗi cột của trạng thái....	34
Hình 2.10 Bảng mã khóa mở rộng và cách xác định mã khóa của chu kỳ .....	36
Hình 2.11 Thao tác InvShiftRows tác động lên từng dòng của state.....	38
Hình 2.12 Bảng thay thế S-box qua phép biến đổi InvSubBytes .....	40

Hình 2.13 Cấu trúc mỗi bảng tra cứu sau khi biến đổi .....	43
Hình 2.14 Khối MC.....	45
Hình 2.15 Bảng loại IV .....	46
Hình 2.16 Bảng loại II.....	47
Hình 2.17 Bảng loại III .....	49
Hình 2.18 Bảng loại Ia .....	50
Hình 2.19 Bảng loại Ib .....	51
Hình 3.1 Minh họa việc phân chia bảng thành 2 phần dạng 1.....	59
Hình 3.2 Minh họa việc phân chia bảng thành 2 phần dạng 2.....	60
Hình 3.3 Giao diện viết chương trình DEV C++ .....	64
Hình 3.4 Giao diện phần mềm mã hóa hộp trắng .....	65
Hình 3.5 Phần mềm mã hóa hộp trắng thực hiện mã hóa .....	66
Hình 3.6 Phần mềm mã hóa hộp trắng thực hiện giải mã.....	66
Hình 3.7 Sơ đồ khối phần mềm thay thế Set-top box.....	68



## DANH MỤC TỪ VIẾT TẮT

- AES** : Advanced Encryption Standard
- DES** : Data Encryption Standard
- DVD** : Digital Video Disc
- FIPS** : Federal Information Processing Standards
- FP** : Final permutation
- IBM** : *International Business Machines*
- ICME** : *International Congress on Mathematical Education*
- IP** : Initial permutation
- IPTV** : Internet Protocol Television
- NIST** : National Institute of Standards and Technology
- NSA** : *National Security Agency*
- STB** : *Set-top box*

## MỞ ĐẦU

### 1. Lý do chọn đề tài

Không thể phủ nhận lợi ích của sự phát triển của Internet, nó là động lực thúc đẩy phát triển của xã hội. Giúp chúng ta trao đổi, nắm bắt thông tin một cách nhanh chóng. Nhiều hoạt động của chúng ta như đọc báo, mua bán hay thậm chí giao khoản có thể thông qua Internet. Những hoạt động truyền tin này đều tiềm ẩn nguy cơ về bảo mật thông tin. Sự đảm bảo an toàn thông tin ảnh hưởng đến sự phát triển xã hội, như nhiều bản nhạc, bộ phim có thể được chuyển đổi dưới dạng số và chia sẻ một cách nhanh chóng mà không phải trả một loại phí nào cho tác giả. Vâng, đây chính là vấn đề bản quyền cũng vấn đề này rất nhiều văn bản đã ra đời nhằm bảo vệ quyền sở hữu trí tuệ và chất xám của tác giả một cách mạnh mẽ. Mới đây nhất nhà nước đã ban hành Thông tư số 07/2012/TTLT-BTTTT-BVHTTDL, ngày 19-6 giữa Bộ Thông tin - Truyền thông và Bộ Văn hóa - Thể thao và Du lịch (VH-TT-DL).

Thực hiện Thông tư số 07/2012/TTLT-BTTTT-BVHTTDL, các doanh nghiệp cung cấp dịch vụ internet, viễn thông, lưu trữ trực tuyến, mạng xã hội... là nguồn khởi đầu đăng tải, truyền đưa hoặc cung cấp nội dung thông tin số (tác phẩm, cuộc biểu diễn, bản ghi âm, ghi hình, chương trình phát sóng) qua mạng viễn thông và internet mà không được phép của chủ thể quyền; sửa chữa, cắt xén, sao chép nội dung thông tin số dưới bất kỳ hình thức nào mà không được phép của chủ thể quyền thì sẽ phải chịu trách nhiệm bồi thường thiệt hại theo quy định của pháp luật về sở hữu trí tuệ và pháp luật khác có liên quan.

Mặc dù Thông tư có nhiều quy định chặt chẽ hơn đối với việc vi phạm bản quyền trên mạng Internet song nhiều doanh nghiệp cung cấp dịch vụ, người dùng vẫn rất băn khoăn về khả năng thực thi của nó khi vẫn còn tồn tại nhiều rào cản, vướng mắc.