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

DANH MỤC HÌNH

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 các 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 quyềnthì 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.