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

NGUYỄN CAO THẮNG

NGHIÊN CỨU, TÌM HIỂU KỸ THUẬT GIẤU TIN MẬT VÀ ỨNG DỤNG

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

Thái Nguyên - 2020

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

NGUYỄN CAO THẮNG

NGHIÊN CỨU, TÌM HIỂU KỸ THUẬT GIẤU TIN MẬT VÀ ỨNG DỤNG

Ngành: Công nghệ thông tin
Chuyên ngành: Khoa học máy tính
Mã số: 848 0101

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

NGƯỜI HƯỚNG DẪN KHOA HỌC: TS. HỒ VĂN CANH

Thái Nguyên - 2020

LỜI CAM ĐOAN

Học viên xin cam đoan luận văn này là công trình nghiên cứu thực sự của bản thân, dưới sự hướng dẫn khoa học của TS. Hồ Văn Canh.

Các số liệu, kết quả trong luận văn là trung thực và chưa từng được công bố dưới bất cứ hình thức nào. Tất cả các nội dung tham khảo, kế thừa của các tác giả khác đều được trích dẫn đầy đủ.

Em xin chịu trách nhiệm về nghiên cứu của mình.

Tác giả

Nguyễn Cao Thắng

LỜI CẢM ƠN

Học viên trân trọng cảm ơn sự quan tâm, tạo điều kiện và động viên của Lãnh đạo Đại học Công nghệ thông tin & Truyền thông, Đại học Thái Nguyên, các thầy cô Khoa Đào tạo sau đại học, các khoa đào tạo và các quý phòng ban Học viện trong suốt thời gian qua.

Học viên xin bày tỏ sự biết ơn sâu sắc tới TS. Hồ Văn Canh đã nhiệt tình định hướng, bồi dưỡng, hướng dẫn học viên thực hiện các nội dung khoa học trong suốt quá trình nghiên cứu, thực hiện luận văn.

Xin chân thành cảm ơn sự động viên, giúp đỡ to lớn từ phía Cơ quan đơn vị, đồng nghiệp và gia đình đã hỗ trợ học viên trong suốt quá trình triển khai các nội dung nghiên cứu.

Mặc dù học viên đã rất cố gắng, tuy nhiên, luận văn không tránh khỏi những thiếu sót. Học viên kính mong nhận được sự đóng góp từ phía Cơ sở đào tạo, quý thầy cô, các nhà khoa học để tiếp tục hoàn thiện và tạo cơ sở cho những nghiên cứu tiếp theo.

Xin trân trọng cảm ơn!

Thái Nguyên, tháng năm 2020

Học viên

Nguyễn Cao Thắng

MỤC LỤC

DANH MỤC TỪ VIẾT TẮT

Ký hiệu, viết tắt		**Ý nghĩa**
AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa tiên tiến
AN-QP		An ninh quốc phòng
CNSS	Committee on National Security Systems	Ủy ban hệ thống an ninh quốc gia
GCD	Greatest Common Divisor	Ước chung lớn nhất
HVS	Human Vision System	Kỹ thuật giấu tin phụ thuộc vào thị giác
HAS	Human Auditory System	Kỹ thuật giấu tin phụ thuộc vào thính giác
IT	Information Technology	Công nghệ thông tin
ISO	International Organization for Standardization	Tổ chức tiêu chuẩn hóa quốc tế
LSB	Laest Significant Bit	Bít có trọng số bé nhất
MSB	Most Significant Bit	Bit có trọng số lớn nhất
NIST	National Institute of Science and Technology	Viện công nghệ và tiêu chuẩn quốc gia Hoa Kỳ
RSA	Rivest - Shamir - Adlemal	Hệ mật mã RSA
CRT	Chinese Remainder Theorem	Định lý đồng dư Trung Hoa
$GF(P)$		Trường số hữu hạn P phần tử
$GF(2)$		Trường nhị phân
K		Tập hợp khóa mã
E		Thuật toán mã hóa

D		Thuật toán giải mã
P		Tập hợp các bản rõ
C		Tập hợp các bản mã
$\varphi(n)$		Hàm Phi_Ơle
(p,q)		Cặp số nguyên tố p và q
n		Số nguyên dương bất kỳ
x		Văn bản rõ thuộc P
y		Bản mã thuộc C
$k^{'}$		Thành phần khóa công khai
$k^{''}$		Thành phần khóa bí mật
s		Số nguyên tố Mersenne
r		Số nguyên lẻ

DANH MỤC HÌNH VẼ

DANH MỤC BẢNG BIỂU