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

-------o0o-------

ĐỖ XUÂN TRƯỜNG

THOẢ THUẬN KHOÁ TRONG AN TOÀN VÀ BẢO MẬT THÔNG TIN

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Thái Nguyên, 2015

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

-------o0o-------

ĐỖ XUÂN TRƯỜNG

THOẢ THUẬN KHOÁ TRONG AN TOÀN VÀ BẢO MẬT THÔNG TIN

Chuyên ngành: KHOA HỌC MÁY TÍNH
Mã số : 60.48.01

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

NGƯỜI HƯỚNG DẪN KHOA HỌC
PGS. TS ĐỖ TRUNG TUẤN

Thái Nguyên, 2015

MỤC LỤC

CAM KẾT

Tài liệu được sử dụng trong luận văn được thu thập từ các nguồn kiến thức hợp pháp, có trích dẫn nguồn tài liệu tham khảo. Chương trình sử dụng mã nguồn mở, có xuất xứ.

Dưới sự giúp đỡ nhiệt tình và chỉ bảo chi tiết của giáo viên hướng dẫn, tôi đã hoàn thành luận văn của mình. Tôi xin cam kết luận văn này là của bản thân tôi làm và nghiên cứu, không hề trùng hay sao chép của bất kỳ ai.

Thái Nguyên, ngày tháng năm 2015

Tác giả

Đỗ Xuân Trường

LỜI CẢM ƠN

Để hoàn thành chương trình cao học và viết luận văn này, em đã nhận được sự giúp đỡ và đóng góp nhiệt tình của các thầy cô trường Đại học Công nghệ thông tin và Truyền thông, Đại học Thái Nguyên.

Trước hết, em xin chân thành cảm ơn các thầy cô trong khoa Đào tạo sau đại học, đã tận tình giảng dạy, trang bị cho em những kiến thức quý báu trong suốt những năm học qua.

Đặc biệt em xin gửi lời tri ân sâu sắc đến PGS.TS Đỗ Trung Tuấn - người đã dành nhiều thời gian, công sức và tận tình hướng dẫn cho em trong suốt quá trình hình thành và hoàn chỉnh luận văn.

Xin chân thành cảm ơn gia đình, bạn bè đã nhiệt tình ủng hộ, giúp đỡ, động viên cả về vật chất lẫn tinh thần trong thời gian học tập và nghiên cứu.

Trong quá trình thực hiện luận văn, mặc dù đã rất cố gắng nhưng cũng không tránh khỏi những thiếu sót. Kính mong nhận được sự cảm thông và tận tình chỉ bảo của các thầy cô và các bạn.

Thái Nguyên, ngày tháng năm 2015

Tác giả

Đỗ Xuân Trường

DANH MỤC CÁC TỪ VIẾT TẮT

C	(Cypto): Tập hợp hữu hạn các bản mã
C/S	Khách/ chủ
CA	Chứng thực số, certificate authority
CSDL	Cơ sở dữ liệu
CERT	Computer Emegency Response
DES	Khóa Data Encryption Standard
ID	Định danh
KDC	Key Distribution Center
Key	Khóa
Key Agreement Protocol	Giao thức thỏa thuận khóa
Key Exchange	Trao đổi khóa
MTI	Giao thức trao đổi khóa do Matsumoto, Takashima và Imai đề xuất
PIN	Postal Index Number
P	Plain Text (Tập hợp các bản rõ có thể)
PKI	Hạ tầng khóa công khai
Public key	Khóa công khai
RSA	Hệ thống mã và chứng thực do Ron Rivest, Adi Shamir, và Leonard Adleman đề xuất
STS	Station to station
TA	Trust Authority
TMDT	Thương mại điện tử
TVP	Time variant parameter

DANH MỤC HÌNH VẼ VÀ BẢNG BIỂU

MỞ ĐẦU

Hiện nay, ở các nước phát triển cũng như đang phát triển, mạng máy tính và Internet đang ngày càng đóng vai trò thiết yếu trong mọi lĩnh vực hoạt động của xã hội và nó trở thành phương tiện làm việc trong các hệ thống thì nhu cầu bảo mật thông tin được đặt lên hàng đầu. Nhu cầu này không chỉ có ở các bộ máy An ninh, Quốc phòng, Quản lý Nhà nước, mà đã trở thành cấp thiết trong nhiều hoạt động kinh tế xã hội như: Tài chính, ngân hàng, thương mại…thậm chí trong cả một số hoạt động thường ngày của người dân (Thư điện tử, thanh toán tín dụng,…). Do ý nghĩa quan trọng này mà những năm gần đây công nghệ mật mã và an toàn thông tin đã có những bước tiến vượt bậc và thu hút sự quan tâm của các chuyên gia trong nhiều lĩnh vực khoa học, công nghệ.

Quản lý khóa có vai trò cực kỳ quan trọng đối với an ninh của các hệ thống dựa trên mật mã.

Rất nhiều yếu tố quan trọng góp phần trong việc quản lý khóa thành công lại không thuộc về phạm vi của mật mã học mà lại thuộc về lĩnh vực quản lý. Chính điều này lại làm cho việc thực hiện thành công chính sách quản lý khóa thêm phức tạp. Cũng vì nguyên nhân này mà phần lớn các tấn công vào các hệ thống mật mã là nhằm vào cách thức quản lý khóa hơn là tấn công vào các kỹ thuật mật mã.

Luận văn sẽ nghiên cứu và xác định rõ vai trò của khóa trong các giải pháp bảo mật và an toàn thông tin. Trên cơ sở nghiên cứu và phân tích các giải pháp an toàn khóa trong việc phân phối, thoả thuận, chuyển vận khóa, cũng như các phương thức quản lý nhằm mang lại hiệu quả cao nhất trong quá trình thực hiện các giao thức đó.