

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

ĐỖ QUỐC TRƯỜNG

**ĐẢM BẢO AN TOÀN THÔNG TIN TRÊN WEB SỬ DỤNG KỸ
THUẬT MÃ HÓA ỨNG DỤNG VÀO GỬI NHẬN CÔNG VĂN TÀI
LIỆU TRONG HỆ THỐNG MẠNG QUÂN SỰ**

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Thái Nguyên - 2020

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

ĐỖ QUỐC TRƯỜNG

**ĐẢM BẢO AN TOÀN THÔNG TIN TRÊN WEB SỬ DỤNG KỸ
THUẬT MÃ HÓA ỨNG DỤNG VÀO GỬI NHẬN CÔNG VĂN TÀI
LIỆU TRONG HỆ THỐNG MẠNG QUÂN SỰ**

Chuyên ngành: Khoa học máy tính

Mã số chuyên ngành: 8480101

**LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH
Người hướng dẫn khoa học: TS PHẠM THẾ QUẾ**

Thái Nguyên - 2020

LỜI CAM ĐOAN

Tôi xin cam đoan luận văn này là công trình nghiên cứu của chính bản thân, luận văn này hoàn toàn được hình thành và phát triển từ quan điểm của chính cá nhân tôi, dưới sự hướng dẫn chỉ bảo của TS Phạm Thế Quế. Các kết quả nghiên cứu trong luận văn là trung thực và chưa được công bố trong các công trình nào khác.

Học viên

Đỗ Quốc Trường

LỜI CẢM ƠN

Để hoàn thành luận văn “Đảm bảo an toàn thông tin trên web sử dụng kỹ thuật mã hóa ứng dụng vào gửi nhận công văn tài liệu trong hệ thống mạng Quân sự” học viên đã nhận được sự hướng dẫn và giúp đỡ nhiệt tình của nhiều tập thể và cá nhân.

Trước hết, học viên xin bày tỏ lòng biết ơn chân thành đến ban lãnh đạo cùng quý thầy cô trong khoa Công nghệ thông tin - Trường Đại học Công nghệ thông tin và truyền thông, Đại học Thái Nguyên đã tận tình dạy dỗ, truyền đạt kiến thức, kinh nghiệm và tạo điều kiện thuận lợi cho học viên trong suốt thời gian học tập và thực hiện đề tài.

Đặc biệt, xin bày tỏ lòng biết ơn sâu sắc đến thầy hướng dẫn TS. Phạm Thế Quế, người đã gợi cho học viên những ý tưởng về đề tài, đã tận tình hướng dẫn và giúp đỡ để đề tài được thực hiện và hoàn thành.

Tôi cũng xin cảm ơn cơ quan, bạn bè đồng nghiệp, gia đình và những người thân đã cùng chia sẻ, giúp đỡ, động viên, tạo điều kiện thuận lợi để tôi hoàn thành tốt nhiệm vụ học tập và hoàn thành bản luận văn.

Thái nguyên, ngày.... tháng.... năm 2020

Học viên

Đỗ Quốc Trường

MỤC LỤC

MỞ ĐẦU	06
Chương 1: TỔNG QUAN VỀ AN TOÀN THÔNG TIN VÀ BẢO MẬT TRÊN WEB	09
1.1. Quá trình phát triển của web	09
1.2. Quá trình phát triển của web	09
1.3. Các hiểm họa đối với an toàn thông tin trên web	09
1.3.1. Tấn công vào vùng ẩn	09
1.3.2. Can thiệp vào tham số trên URL.....	10
1.3.3. Tấn công dùng cookie	10
1.3.4. Các lỗ hổng bảo mật.....	10
1.3.5. Cấu hình không an toàn	10
1.3.6. Tràn bộ đệm	10
1.3.7. Tấn công từ chối dịch vụ DoS (Denial of Service).....	11
1.4. Các vấn đề bảo mật ứng dụng web	11
1.4.1. Giao thức IPSec.....	11
1.4.2. Giao thức SSL và TLS	11
1.4.3. Giao thức SET.....	14
1.4.4. So sánh giữa SET và SSL	16
1.5. An toàn thông tin trong môi trường web	17
1.5.1. Vấn đề an toàn thông tin	17
1.5.2. Chứng chỉ số và cơ chế xác thực	17
1.5.3. Chứng chỉ khóa công khai	21
1.6. Kết luận chương	25
Chương 2: MÃ KHÓA ĐỐI XỨNG, MÃ KHÓA CÔNG KHAI, CHỮ KÝ SỐ TRONG BẢO MẬT GỬI NHẬN CÔNG VĂN TÀI LIỆU GIỮA CÁC ĐƠN VỊ TRONG QUÂN SỰ	26
2.1. Mã khóa đối xứng	26
2.1.1. Định nghĩa.....	26

2.1.2. Chuẩn mã hóa dữ liệu DES	27
2.2. Mã khóa bất đối xứng (mã hóa khóa công khai)	32
2.2.1. Giới thiệu chung.....	32
2.2.2. Hệ mật mã RSA	35
2.2.3. Hàm băm	39
2.3. Chữ ký số	42
2.3.1. Khái niệm.....	42
2.3.2. Phân loại chữ ký số	43
2.3.3. Một số lược đồ chữ ký cơ bản.....	46
2.3.4. Quá trình ký và xác thực chữ ký số	51
2.3.5. Các phương pháp tấn công chữ ký điện tử	52
2.4. Bảo mật việc gửi nhận công văn tài liệu trong hệ thống Quân sự.....	52
2.4.1. Trình tự quản lý công văn tài liệu chuyển đi	53
2.4.2. Kiểm tra, đăng ký và đóng dấu công văn tài liệu	53
2.4.3. Trình tự quản lý công văn tài liệu đến	53
2.5. Kết luận chương	53
Chương 3: XÂY DỰNG CHƯƠNG TRÌNH BẢO MẬT GỬI NHẬN CÔNG VĂN TÀI LIỆU TRONG HỆ THỐNG MẠNG QUÂN SỰ	55
3.1. Hiện trạng về gửi nhận công văn tài liệu ở các đơn vị Quân sự.....	55
3.2. Bảo đảm an toàn thông tin trong đơn vị Quân sự	57
3.3. Cài đặt chương trình và thử nghiệm.....	59
3.4. Đánh giá kết quả thử nghiệm chương trình	63
KẾT LUẬN	64
KIẾN NGHỊ VÀ HƯỚNG PHÁT TRIỂN	65
TÀI LIỆU THAM KHẢO	66

DANH MỤC CÁC THUẬT NGỮ, TỪ VIẾT TẮT

Từ viết tắt	Tiếng anh	Nghĩa tiếng việt
CA	Certificate Authority	Cơ quan chứng thực chữ ký số
DS	Digital Signatures	Chữ ký số
DSA	Digital Signature Algorithm	Giải thuật ký điện tử
DES	Data Encryption Standard	Chuẩn mã hóa dữ liệu
DSS	Digital Signature Standard	Chuẩn chữ ký số
DoS	Denial of Service	Tấn công từ chối dịch vụ
FTP	File Transfer Protocol	Giao thức truyền tập tin
HTML	Hypertext Markup Language	Ngôn ngữ đánh dấu siêu văn bản
HTTP	Hypertext Transfer Protocol	Giao thức truyền siêu văn bản
LDAP	Lightweight Directory Access Protocol	Giao thức ứng dụng truy cập các cấu trúc thư mục
RSA	Rivest, Shamir and Adleman	Giải thuật mã hóa công khai
PKI	Public Key Infrastructure	Cơ sở hạ tầng khóa công khai
SHA	Secure Hash Algorithm	Giải thuật băm an toàn
SSL	Secure Socket Layer	Giao thức an ninh thông tin

Từ viết tắt	Tiếng anh	Nghĩa tiếng việt
SQL	Structured Query Language	Ngôn ngữ truy vấn
TCP/IP	Transmission Control Protocol/Internet Protocol	Một hệ thống các giao thức hỗ trợ việc truyền thông tin trên mạng
TLS	Transport Layer Security	Bảo mật tầng giao vận
URL	Uniform Resource Locator	Định vị tài nguyên thống nhất

DANH MỤC HÌNH VẼ

Hình 1.1: Mô hình hoạt động của web.....	09
Hình 1.2: Sử dụng SSL gửi và nhận trên internet.....	12
Hình 1.3: Sơ đồ hoạt động của SSL.....	14
Hình 1.4: Dùng mật khẩu để xác thực máy khách kết nối tới máy dịch vụ.....	18
Hình 1.5: Chứng thực của máy khách kết nối tới máy dịch vụ	20
Hình 1.6: Sơ đồ hoạt động của Hệ thống cấp chứng chỉ khóa công khai.....	22
Hình 1.7: Mô hình dây chuyền chứng thực	24
Hình 2.1: Sơ đồ mã hóa khóa đối xứng	26
Hình 2.2: Một vòng của DES.....	28
Hình 2.3: Hàm f của DES	29
Hình 2.4: Sơ đồ thuật toán tạo các khóa từ K1 đến K16	30
Hình 2.5: Sơ đồ mô tả chi tiết DES.....	31
Hình 2.6: Gửi nhận tài liệu mã hóa bất đối xứng.....	33
Hình 2.7: Sơ đồ mô tả chi tiết thuật toán RSA	37
Hình 2.8: Sơ đồ mô tả bản băm thông điệp.....	39
Hình 2.9: Đường đi đúng của thông tin	40
Hình 2.10: Thông tin bị lấy trộm và đã bị thay đổi trên đường truyền.....	40
Hình 2.11: Mô hình lược đồ chữ ký khôi phục thông điệp.....	46
Hình 2.12: Quá trình ký thông điệp	51
Hình 2.13: Mô hình lược đồ chữ ký khôi phục thông điệp.....	52
Hình 3.1: Sử dụng thiết bị lưu trữ di động để trao đổi tài liệu (USB).....	55
Hình 3.2: Sử dụng máy tính kết nối internet để gửi tài liệu.....	56
Hình 3.3: Chương trình gửi nhận công văn tài liệu đang triển khai	56
Hình 3.4: Giao diện tạo khóa	59
Hình 3.5: Giao diện gửi tài liệu.....	60
Hình 3.6: Giao diện lựa chọn các chế độ gửi tài liệu.....	60
Hình 3.7: Giao diện tài liệu đến khi gửi bảo mật và ký số	61
Hình 3.8: Giao diện giải mã tài liệu thành công	61
Hình 3.9: Giao diện xác thực chữ ký tài liệu thành công.....	62
Hình 3.10: Giao diện xác thực chữ ký tài liệu không thành công	62

MỞ ĐẦU

1. Đặt vấn đề

1.1. Sự cần thiết lựa chọn đề tài

Hiện nay tình hình an toàn thông tin số ở nước ta diễn biến phức tạp đe dọa nghiêm trọng đến ứng dụng công nghệ thông tin phục vụ phát triển kinh tế xã hội và đảm bảo Quốc phòng an ninh. Bảo mật và đảm bảo an toàn thông tin dữ liệu đang nhiều nhà khoa học tập trung nghiên cứu, là một chủ đề rộng có liên quan đến nhiều lĩnh vực, trong thực tế có thể có nhiều phương pháp được thực hiện để đảm bảo an toàn thông tin dữ liệu. Ngày nay, với sự phát triển nhanh chóng của hạ tầng truyền thông, người sử dụng dựa trên nền tảng này để truyền các thông tin trên mạng thì các nguy cơ xâm nhập vào các hệ thống thông tin, các mạng dữ liệu ngày càng gia tăng. Nhiều chuyên gia đang tập trung nghiên cứu và tìm mọi giải pháp để đảm bảo an toàn, an ninh cho hệ thống, đặc biệt là các hệ thống mạng máy tính trong Quân sự. Việc bảo mật cho hệ thống mạng máy tính có thể thực hiện theo nhiều phương diện, ở nhiều tầng khác nhau, bao gồm từ phương diện kiểm soát truy nhập vật lý vào hệ thống, thực hiện sửa chữa, cập nhật, nâng cấp hệ điều hành cũng như vá mọi lỗ hổng về an ninh, quản lý các hoạt động gửi nhận công văn và truyền tải văn bản trên mạng (Giám sát qua tường lửa, các bộ định tuyến Router, phát hiện và phòng ngừa sự xâm nhập,...) xây dựng các giải pháp bảo mật ở mỗi phần mềm để quản lý người dùng thông qua việc cấp quyền sử dụng, mật khẩu, mật mã, mã hóa dữ liệu để che giấu thông tin.

Trên thực tế hiện nay các chiến lược Quân sự Quốc phòng các phương án tác chiến, các bí mật về khoa học Quân sự cho đến các công văn tài liệu bí mật, tuyệt mật đều được tạo lập soạn thảo lưu trữ trên các máy tính. Do không kiểm soát được việc sử dụng các thiết bị lưu trữ di động như USB, thẻ nhớ, ổ cứng di động hay các thiết bị thu phát sóng như USB 3G, Wifi... nên tất cả các tài nguyên thông tin Quân sự đang nằm trên không gian mạng đều có thể bị lộ lọt, bị làm giả, bị chỉnh sửa... Nhận thức được vấn đề nêu trên nên em đã chọn đề tài: “Đảm bảo an toàn thông tin trên web sử dụng kỹ thuật mã hóa ứng dụng