CHỮ KÝ SỐ VÀ ỨNG DỤNG TRONG QUẢN LÝ VĂN BẢN ĐIỆN TỬ

Học viên: Phùng Thị Nguyệt
Đơn vị công tác: Trường THPT Trưng Vương – Văn Lâm – Hưng Yên
Email:nguyet1709@gmail.com

GVHD: Đoàn Văn Ban
Đơn vị công tác: Viện khoa học, viên công nghệ thông tin
Email: doanban@gmail.com

Từ khóa: Digit Signature, PEM(Privary Enhanced Mail),CRL(certificate revocation list), …

1. GIỚI THIỆU BÀI TOÁN

Trình bày lí do chọn đề tài, nội dung bài toán đặt ra?

- Cùng với sự phát triển của công nghệ thông tin và truyền thông, giao dịch điện tử đã và đang phát triển mạnh mẽ trên thế giới thay thế dần các giao dịch truyền thống. Rất nhiều nước có chủ trương vừa phát triển các hoạt động cung ứng dịch vụ điện tử, vừa xây dựng hệ thống pháp luật đầy đủ, minh bạch để đảm bảo giá trị pháp lý của các thông điệp điện tử và giao dịch điện tử. Tại Việt Nam, giao dịch điện tử đã được áp dụng tại các lĩnh vực thuế, hải quan, thương mại điện tử,...

- Theo kết quả khảo sát thương mại điện tử Việt Nam 2010 của Bộ Công thương, trong 7 trở ngại khiến thương mại điện tử chưa phát triển thì vấn đề an ninh, an toàn thông tin chiếm vị trí gần cao nhất (chỉ sau trở ngại về môi trường xã hội và tập quán kinh doanh). Một trong những giải pháp giải quyết vấn đề này đó là chữ ký số.

- Nội dung bài toán đặt ra:

Có một công văn trên sở, xác định xem công văn đó có đúng là của người trên sở gửi công văn đó xuống không?

2. NỘI DUNG LUẬN VĂN

Trình bày các giải pháp, các đóng góp chính của luận văn?

Các giải pháp bảo mật về an toàn thông tin:

- Phương pháp che giấu, bảo đảm toàn vẹn và xác thực thông tin.

Sử dụng các kỹ thuật: Mã hóa, Hàm băm, Giấu tin, Ký số, Thủy ký, Giao thức bảo toàn thông tin, Giao thức xác thực thông tin, ...

Luận văn trình bày kỹ thuật chữ ký số để bảo toàn, bảo mật thông tin.

3. KẾT LUẬN

Đưa ra các kết luận về nội dung luận văn

Luận văn trình bày sơ bộ về an toàn thông tin, các giải pháp về bảo mật an toàn thông tin, cơ sở toán học áp dụng trong hệ mã hoá. Chọn hệ mã hoá khoá công khai RSA để ứng dụng vào việc xây dựng chương trình tạo chữ ký số.

Luận văn trình bày hai lược đồ có ưu điểm nổi trội hơn và đang được ứng dụng rộng rãi hiện nay đó là lược đồ chữ ký RSA và lược đồ chữ ký chuẩn DSA/ DSS. Các thuật toán hàm băm MD5, SHA - 1 cũng đã được trình bày và đi sâu phân tích làm rõ bản chất của các thuật toán này trong việc ứng dụng để tạo ra chữ ký số. Luận văn trình bày

các vấn đề liên quan đến chứng chỉ số và trình bày chi tiết về chứng chỉ số X.509.

Trên cơ sở tìm hiểu và tập hợp lại một cách có hệ thống phần lý thuyết liên quan, Luận văn đã tạo được cơ sở lý thuyết cho việc xây dựng chương trình tạo chữ ký và chứng thực chữ ký. Chương trình ứng dụng này có thể được áp dụng tại bộ phận văn thư của các đơn vị thuộc Sở Giáo dục – Đào tạo tỉnh Hưng Yên. Chương trình thực hiện được các chức năng cơ bản của một hệ mã hoá như tạo cặp khoá công khai và khoá bí mật, ký vào văn bản để gửi đi và chứng thực chữ ký đã ký.

Các kiến nghị và định hướng nghiên cứu trong tương lai:

Hướng phát triển tiếp theo của đề tài là, phát triển mô hình theo hướng client – server, cần mở rộng thêm một số chức năng như mở rộng cơ sở dữ liệu, bảo mật qua mạng Lan, mạng internet,....