ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

DƯƠNG THỊ HOÀI THU

NGHIÊN CỨU GIẢI PHÁP XÂY DỰNG VÀ PHÁT TRIỂN CHỮ KÝ SỐ DÙNG TRONG CÁC CƠ QUAN TỈNH THÁI NGUYÊN

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Thái Nguyên, 2012

LỜI CẢM ƠN

Để hoàn thành chương trình cao học và viết luận văn này, tôi đã nhận được sự hướng dẫn, giúp đỡ và góp ý nhiệt tình của quý thầy cô trường Đại học Công nghệ thông tin - Truyền thông, Đại học Thái Nguyên.

Trước hết, tôi xin chân thành cảm ơn đến quí thầy cô trường Đại học Công nghệ thông tin - Truyền thông, đặc biệt là những thầy cô đã tận tình dạy bảo cho tôi suốt thời gian học tập tại trường.

Tôi xin gửi lời biết ơn sâu sắc đến thầy giáo TS. Nguyễn Văn Tảo người đã dành rất nhiều thời gian, tâm huyết và sự tận tình giúp đỡ, hướng dẫn cho tôi trong suốt quá trình nghiên cứu và giúp tôi hoàn thành luận văn.

Tôi xin bày tỏ lòng biết ơn tới gia đình, bạn bè và những người thân đã động viên khích lệ tinh thần và giúp đỡ để tôi hoàn thành luận văn này.

Mặc dù tôi đã có nhiều cố gắng hoàn thiện luận văn bằng tất cả sự nhiệt tình và năng lực của mình, tuy nhiên không thể tránh khỏi những thiếu sót, rất mong nhận được những đóng góp quí báu của quí thầy cô và các bạn.

Thái Nguyên, ngày 20 tháng 9 năm 2012

Học viên

Dương Thị Hoài Thu

LỜI CAM ĐOAN

Tôi xin cam đoan, toàn bộ nội dung liên quan tới đề tài được trình bày trong luận văn là bản thân tôi tự tìm hiểu và nghiên cứu, dưới sự hướng dẫn khoa học của Thầy giáo TS. Nguyễn Văn Tảo.

Các tài liệu, số liệu tham khảo được trích dẫn đầy đủ nguồn gốc. Tôi xin chịu trách nhiệm về lời cam đoan của mình.

Học viên thực hiện

Dương Thị Hoài Thu

MỤC LỤC

MỞ ĐẦU 1
1.1 CÁC KHÁI NIỆM CƠ BẢN 2
1.2 MỘT SỐ KHÁI NIỆM TOÁN HỌC CƠ SỞ 3
1.2.1 Phép đồng dư 3
1.2.2 Hàm phi-Euler 3
1.2.3 Định lý Femat và các mở rộng 4
1.2.4 Định lý Trung Quốc về phần dư 4
1.3 GIỚI THIỆU HỆ MÃ KHÓA CÔNG KHAI 5
1.4 HỆ MẬT MÃ RSA 7
1.4.1 Quá trình tạo khóa, mã hóa và giải mã 8
1.4.2 Độ an toàn của hệ RSA 9
1.5 HỆ MẬT MÃ ELGAMAL 10
1.5.1 Quá trình tạo khóa, mã hóa, giải mã 11
1.5.2 Độ an toàn của mật mã ElGamal: 12
CHƯƠNG 2 - CHỮ KÝ SỐ 13
2.1 GIỚI THIỆU CHUNG VỀ CHỮ KÝ SỐ 13
2.1.1 Khái niệm về chữ ký số: 13
2.1.2 Các ưu điểm của chữ ký số: 13
2.1.3 Phân loại chữ ký số: 15
2.1.4 Sơ đồ tổng quan của một hệ thống chữ ký số 16
2.2 CHỮ KÝ SỐ VÀ HÀM BĂM 17
2.2.1 Khái niệm về hàm băm: 17
2.2.2 Hàm băm MD5 (Message-Digest algorithm 5) 17
2.3 CHỮ KÝ SỐ DÙNG MẬT MÃ KHÓA CÔNG KHAI 20
2.3.1 Sơ đồ chữ ký số RSA 20
2.3.2 Sơ đồ chữ ký ElGamal 22

2.3.3 Chuẩn chữ ký số..... 25
2.4 XÁC THỰC VÀ CÁC PHƯƠNG PHÁP XÁC THỰC 28
2.4.1 Vấn đề xác thực: 28
2.4.2 Các phương pháp xác thực: 29
2.5 TRIỂN KHAI CHỮ KÝ SỐ TRONG THỰC TẾ 31
CHƯƠNG 3. ỨNG DỤNG MÃ HÓA VÀ CHỮ KÝ SỐ TRONG TRAO ĐỔI VĂN BẢN 35
3.1. MÔ HÌNH HỆ THỐNG..... 35
3.2 XÂY DỰNG CÁC MÔĐUN..... 36
3.2.1 Tạo khóa: 36
3.2.2 Mã hóa và tạo chữ ký cho file tài liệu: 37
3.2.3 Giải mã và xác thực chữ ký: 39
3.3 GIAO DIỆN MỘT SỐ CHỨC NĂNG CHÍNH CỦA CHƯƠNG TRÌNH.
..... 41

DANH MỤC CÁC KÝ HIỆU, CÁC CHỮ VIẾT TẮT

CA: Certificate Authority

FIPS: Federal information Processing Standard

MAC: Message Digest

NIST: National Institute Of Standards Anh Technology

RSA: Rivest, Shamir, Adleman

DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ

Hình 1.1 : Mô hình mật mã khóa công khai

Hình 2.1: Hàm MAC

Hình 3.1: Sơ đồ quá trình tạo khóa

Hình 3.2 : Sơ đồ quá trình ký và mã hóa file dữ liệu

Hình 3.3: Sơ đồ quá trình xác thực chữ ký và giải mã file dữ liệu

MỞ ĐẦU

Trong sự phát triển của xã hội loài người, kể từ khi có sự trao đổi thông tin, an toàn thông tin trở thành một nhu cầu gắn liền với nó như hình với bóng. Đặc biệt trong thời đại mà thương mại điện tử đang lên ngôi thì việc có được các công cụ đầy đủ để đảm bảo cho sự an toàn trao đổi thông tin liên lạc là vô cùng cần thiết. Chính vì vậy mà chữ ký số ra đời với nhiều tính năng ưu việt, chữ ký số sẽ giải quyết vấn đề toàn vẹn dữ liệu và là bằng chứng chống chối bỏ trách nhiệm trên nội dung đã ký, giúp cho các doanh nghiệp, tổ chức cá nhân yên tâm với các giao dịch điện tử của mình trong môi trường internet. Việc ứng dụng chữ ký số sẽ đem lại cho doanh nghiệp, tổ chức rất nhiều lợi ích như: Tiết kiệm chi phí giấy tờ, thời gian luân chuyển trong hoạt động quản lý công văn, giấy tờ, thư điện tử; giúp thúc đẩy nhanh các giao dịch qua mạng trong khi vẫn đảm bảo độ an toàn và bảo mật thông tin. Ngày nay, chữ ký số đóng một vai trò quan trọng trong kế hoạch phát triển Thương mại điện tử và Chính phủ điện tử ở nước ta.

Tại tỉnh Thái Nguyên việc áp dụng chữ ký số trong các giao dịch điện tử, các dịch vụ hành chính công chưa được triển khai thực hiện do còn gặp nhiều khó khăn, đặc biệt trong việc trong việc xây dựng cơ sở hạ tầng để phù hợp với tình hình thực tế tại tỉnh. Với mục đích nghiên cứu, tìm hiểu và vận dụng các kiến thức đã học được trong chương trình cao học để giải quyết một số vấn đề thực tiễn, tôi chọn đề tài "Nghiên cứu giải pháp xây dựng và phát triển chữ ký số dùng trong các cơ quan tỉnh Thái Nguyên"

CHƯƠNG 1 –HỆ MẬT MÃ KHOÁ CÔNG KHAI

1.1 CÁC KHÁI NIỆM CƠ BẢN

Khái niệm chung về mật mã

Hệ mật mã hiện đại thường gồm 5 thành phần (P,C, K, E, D) trong đó:

P: tập hợp hữu hạn các bản rõ có thể

C: tập hợp hữu hạn các bản mã có thể

K: tập hợp các bản khóa có thể

E: tập hợp các qui tắc mã hóa có thể

D: tập hợp ác qui tắc giải mã có thể

Nội dung cần mã hóa thể hiện dưới dạng bản rõ (P). Người sử dụng qui tắc (E) và khóa (K) mã hóa bản rõ (P), kết quả thu được gọi là bản mã ($E_K(P) = C$). Bản mã này được gửi đi trên một đường truyền tới người nhận, sau khi nhận được mã (C) người nhận sử dụng qui tắc (D) và khóa (K) giải mã để có thể biết được nội dung thông điệp gốc ($D_K(C) = P$).

Hàm một chiều:

Cho các tập hữu hạn S và T. Hàm một chiều:

f : S→T hàm khả nghịch thỏa:

1. f dễ thực hiện, nghĩa là cho $x \in S$, có thể dễ dàng tính được $y = f(x)$

2. f^{-1}, hàm ngược của f, khó thực hiện nghĩa là cho $y \in T$, rất khó tính được $x = f^{-1}(y)$.

3. f^{-1} có thể dễ tính được khi có thêm một số thông tin

- Một số ví dụ về hàm một chiều

+ Ví dụ 1: f: pq →n, là hàm một chiều với p và q là các số nguyên tố lớn. Thực vậy, ta có thể dễ thực hiện phép nhân p*q (độ phức tạp đa thức); nhưng tính f^{-1} thì lại là bài toán cực khó (đây chính là bài toán nổi tiếng phân tích ra thừa số nguyên tố - độ phức tạp mũ).

+ Ví dụ 2: $f_{g,N}$: x→ g^x mod N là hàm một chiều. Thực vậy, phép tính g^x mod N có độ phức tạp đa thức; nhưng tính f^{-1} lại là bài toán cực khó (đây chính là bài toán nổi tiếng: Bài toán logarithm rời rạc).

+ Ví dụ 3: $f_{k,N}$: x → x^k mod N là hàm một chiều, với N = p*q , p và q là các số nguyên tố lớn, kk' ≡ 1(mod Φ(N)). Thực vậy, phép tính x^k mod N có độ phức tạp đa thức, nhưng tính f^{-1} lại cực khó. Tuy nhiên, nếu biết k' thì có thể dễ dàng tính được f từ công thức $(x^k)^{k'}$= x [3].

1.2 MỘT SỐ KHÁI NIỆM TOÁN HỌC CƠ SỞ

1.2.1 Phép đồng dư

- Định nghĩa: Cho a và b là các số nguyên, a được gọi là đồng dư với b theo modulo n, ký hiệu a ≡ b (mod n) nếu số dư tìm được cho phép chia a và b cho n là bằng nhau. Số nguyên n được gọi là modulo của đồng dư.

- Một số tính chất của phép đồng dư:

- a ≡ a (mod n)
- Nếu a ≡ b (mod n) thì b ≡ a (mod n)
- Nếu a ≡ b (mod n) và b ≡ c (mod n) thì a ≡ c (mod n)
- Nếu a ≡ b (mod n), c ≡ d (mod n) thì a ± c ≡ b ± d (mod n), a.c ≡ b.d (mod n).

Như vậy, ta có khái niệm lớp tương đương như sau: Lớp tương đương của một số nguyên a là tập hợp các số nguyên đồng dư với a theo modulo n. Theo các tính chất 1,2,3 trên ta thấy: cho n cố định, các số đồng dư theo modulo n trong không gian Z được xếp vào một lớp đương đương.

1.2.2 Hàm phi-Euler

Định nghĩa: Cho n ≥1, đặt Φ(n) là tập các số nguyên trong khoảng [1,n] nguyên tố cùng nhau với n. Hàm φ như thế được gọi là hàm phi Euler.