ĐẠI HỌC THÁI NGUYÊN
TR- ỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

MÃ VĂN LAI

NGHIÊN CỨU VÀ PHÁT TRIỂN PHƯƠNG PHÁP RÚT GỌN CHỮ KÍ SỐ

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

THÁI NGUYÊN - NĂM 2014

MỤC LỤC

DANH MỤC CÁC CHỮ VIẾT TẮT

$\omega_n(\alpha)$	Là bậc của số nguyên α
$x \| y$	Nối độ dài bit của x và y
Gcd(x, y)	Ước số chung lớn nhất của x và y
Lcm(x, y)	Bội số chung nhỏ nhất của x và y
ECC	Elliptic Curve Cryptography – Mật mã trên đường cong Elliptic
ECES	Elliptic Curve Encrypt Scheme
ECDSA	Elliptic Curve Digital Signature Algorithm – Thuật toán chữ kí số trên đường cong Elliptic
MD5	Message – Digest algorithm 5 hàm băm mật mã tiêu chuẩn 128 bít
SHA	(Secure Hash Algorithm hay thuật giải băm an toàn
RSA	Rivest – Shamir – Adleman
Z_m	Vành thương hữu hạn m

DANH MỤC CÁC HÌNH VẼ

MỞ ĐẦU

Mật mã (Cryptography) là ngành khoa học là ngành nghiên cứu các kỹ thuật toán học nhằm cung cấp các dịch vụ bảo vệ thông tin. Đây là ngành khoa học quan trọng, có nhiều ứng dụng trong đời sống xã hội. Ngày nay, các ứng dụng mã hóa và an toàn thông tin đang được sử dụng ngày càng phổ biến trong các lĩnh vực khác nhau trên thế giới, từ các lĩnh vực an ninh, quốc phòng… cho đến các lĩnh vực dân sự như thương mại điện tử, ngân hàng…

⇨ *Vai trò của mật mã trong các giải pháp an toàn thông tin – đề cập đến vấn đề nghiên cứu và ứng dụng mật mã để bảo vệ thông tin.*

Trong mật mã vấn đề bảo mật luôn đi đôi với vấn đề xác thực thông tin, đặc biệt trong hệ thống mật mã khóa công khai vấn đề xác thực là vô cùng quan trọng. Để giải quyết được vấn đề xác thực, trong thực tế có một giải pháp kỹ thuật vừa đơn giản vừa hiệu quả là sử dụng chữ ký số. Việc sử dụng chữ ký số ngày càng có nhiều ứng dụng trong thực tế, không chỉ giới hạn trong Ngành Mật Mã mà còn được áp dụng trong một số lĩnh vực vô cùng quan trọng như trong lĩnh vực Chính phủ điện tử, Thương mại điện tử,… để xác thực người gửi, nội dung và nguồn gốc thông tin, chống chối từ.

⇨ *Vai trò của các thuật toán chữ ký số dựa trên các ứng dụng rộng rãi của chúng.*

Việc nghiên cứu, tối ưu và phát triển các lược đồ chữ ký số luôn được đặt ra trong thực tiễn (nhằm phát triển các lược đồ chữ ký số tối ưu, hoặc các lược đồ phù hợp cho các ứng dụng phát triển thực tiễn).

⇨ *Việc nghiên cứu và phát triển các lược đồ chữ ký số mới – một trong những mục tiêu chính được đặt ra trong thực tiễn nhằm nâng cao tính độc lập trong xây dựng các giải pháp an toàn thông tin.*

Trong thực tế, một yêu cầu rất quan trọng được đăt ra khi tối ưu và phát triển các lược đồ chữ ký số ứng dụng trong các môi trường hạn chế về băng thông và tài nguyên là các lược đồ chữ ký số với chiều dài chữ ký số ngắn (Giải quyết bài toán làm sao cho độ dài chữ ký tối thiểu nhất có thể mà không thể giả mạo chữ ký được).

⇨ *Việc nghiên cứu và phát triển các lược đồ chữ ký số rút gọn thể hiện tính khoa học và thực tiễn cao.*

Kết quả nghiên cứu của đề tài nhằm góp phần định hướng và tự phát triển các lược đồ chữ ký số có khả năng ứng dụng trong thực tiễn.

Mục tiêu của đề tài:

Nghiên cứu các giải pháp xây dựng và khả năng ứng dụng chữ ký số trong bảo vệ an toàn thông tin.

- Mật mã khóa công khai;
- Hàm băm mật mã;
- Các kiểu chữ ký số;
- Các ứng dụng của chữ ký số.

Nghiên cứu các cơ sở toán học, mô hình xây dựng và đánh giá các lược đồ chữ ký số.

- Chữ ký số dựa trên tính khó của bài toán phân tích một số nguyên lớn ra các thừa số nguyên tố;
- Chữ ký số dựa trên tính khó của bài toán logarit rời rạc;
- Chữ ký số dựa trên tính khó của bài toán logarit rời rạc trên các điểm nhánh của vành Elliptic.

Phát triển phương pháp rút gọn chữ ký số dựa trên tính khó của bài toán phân tích một số nguyên lớn ra các thừa số nguyên tố.

Xây dựng lược đồ rút gọn chữ ký số mới và biến thể của nó. Đánh giá độ an toán của các lược đồ đề xuất dựa trên các phương trình chứng minh đã được công nhận trên thế giới.

Xây dựng các chương trình mô phỏng và đánh giá kết quả nghiên cứu cần đạt được.

Cấu trúc của luận văn gồm 3 chương:

Chương 1: Tổng quan về mật mã khóa công khai và chữ ký số

Chương 2: Các cơ sở toán học và mô hình xây dựng các lược đồ chữ ký số

Chương 3: Phát triển phương pháp rút gọn chữ ký số.

Chương 1
TỔNG QUAN VỀ MẬT MÃ KHOÁ CÔNG KHAI VÀ CHỮ KÝ SỐ

1.1. Tổng quan về mật mã

1.1.1. An toàn và bảo mật thông tin

Khi nhu cầu trao đổi thông tin dữ liệu ngày càng lớn và đa dạng, các tiến bộ về điện tử - viễn thông và công nghệ thông tin không ngừng được phát triển ứng dụng để nâng cao chất lượng và lưu lượng truyền tin thì các quan niệm ý tưởng và biện pháp bảo vệ thông tin dữ liệu cũng được đổi mới. Bảo vệ an toàn thông tin dữ liệu là một chủ đề rộng, có liên quan đến nhiều lĩnh vực và trong thực tế có thể có rất nhiều phương pháp được thực hiện để bảo vệ an toàn thông tin dữ liệu. Các phương pháp bảo vệ an toàn thông tin dữ liệu có thể được quy tụ vào ba nhóm sau:

- Bảo vệ an toàn thông tin bằng các biện pháp hành chính
- Bảo vệ an toàn thông tin bằng các biện pháp kỹ thuật (phần cứng).
- Bảo vệ an toàn thông tin bằng các biện pháp thuật toán (phần mềm).

Ba nhóm trên có thể được ứng dụng riêng rẽ hoặc phối kết hợp. Môi trường khó bảo vệ thông tin nhất và cũng là môi trường đối phương dễ xâm nhập nhất đó là môi trường mạng và truyền tin. Biện pháp hiệu quả nhất và kinh tế nhất hiện nay trên mạng truyền tin và mạng máy tính là biện pháp thuật toán.

An toàn thông tin bao gồm những nội dung sau:

- Tính bí mật: Tính kín đáo riêng tư của thông tin
- Tính xác thực của thông tin, bao gồm xác thực đối tác (bài toán nhận dạng), xác thực thông tin trao đổi
- Tính trách nhiệm: Đảm bảo người gửi thông tin không thể thoái thác trách nhiệm về thông tin mà mình đã gửi.

Để đảm bảo an toàn thông tin dữ liệu trên đường truyền tin và trên mạng máy tính có hiệu quả thì điều trước tiên là phải lường trước hoặc dự đoán trước các khả năng không an toàn, khả năng xâm phạm, các sự cố rủi ro có thể xảy ra đối với thông tin dữ liệu được lưu trữ và trao đổi trên đường truyền tin cũng như trên mạng. Xác định càng chính xác các nguy cơ nói trên thì càng quyết định được tốt các giải pháp để giảm thiểu các thiệt hại. Có hai loại hành vi xâm phạm thông tin dữ liệu đó

là: *vi phạm chủ động và vi phạm thụ động*. Vi phạm thụ động chỉ nhằm mục đích cuối cùng là nắm bắt được thông tin (đánh cắp thông tin). Việc làm đó có khi không biết được nội dung cụ thể nhưng có thể dò ra được người gửi, người nhận nhờ thông tin điều khiển giao thức chứa trong phần đầu các gói tin. Kẻ xâm nhập có thể kiểm tra được số lượng, độ dài và tần số trao đổi. Vì vậy vi phạm thụ động không làm sai lệch hoặc hủy hoại nội dung thông tin dữ liệu được trao đổi.Vi phạm thụ động thường khó phát hiện nhưng có thể có những biện pháp ngăn chặn hiệu quả. Vi phạm chủ động là dạng vi phạm có thể làm thay đổi nội dung, xóa bỏ, làm trễ, sắp xếp lại thứ tự hoặc làm lặp lại gói tin tại thời điểm đó hoặc sau đó một thời gian. Vi phạm chủ động có thể thêm một số thông tin ngoại lai để làm sai lệch thông tin trao đổi. Vi phạm chủ động dễ phát hiện nhưng để ngăn chặn thì khó khăn hơn nhiều. Một thực tế là không có một biện pháp bảo vệ an toàn thông tin dữ liệu nào là an toàn tuyệt đối. Một hệ thống dù được bảo vệ chắc chắn đến đâu cũng không thể đảm bảo là an toàn tuyệt đối.

1.1.2. Mật mã học

Mật mã học bao gồm hai lĩnh vực: mã hóa (cryptography) và thám mã (cryptanalysis-codebreaking) trong đó:

- Mã hóa: nghiên cứu các thuật toán và phương thức để đảm bảo tính bí mật và xác thực của thông tin (thường là dưới dạng các văn bản lưu trữ trên máy tính). Các sản phẩm của lĩnh vực này là các hệ mật mã, các hàm băm, các hệ chữ ký số, các cơ chế phân phối, quản lý khóa và các giao thức mật mã:

- Thám mã: Nghiên cứu các phương pháp phá mã hoặc tạo mã giả. Sản phẩm của lĩnh vực này là các phương pháp thám mã, các phương pháp giả mạo chữ ký, các phương pháp tấn công các hàm băm và các giao thức mật mã.

Trong giới hạn của luận văn này tác giả chủ yếu vào tìm hiểu một số hệ mã hóa, các hàm băm, các hệ chữ ký số. Như thế mã hóa có thể được định nghĩa đơn giản như sau:

Định nghĩa 1.1

Mã hóa (cryptography) là một ngành khoa học của các phương pháp truyền tin bảo mật. Trong tiếng Hy Lạp, "Cryto" (krypte) có nghĩa là che dấu hay đảo lộn, còn "Graphy" (grafik) có nghĩa là từ.

Người ta quan niệm rằng: những từ, những ký tự của văn bản gốc có thể hiểu được sẽ cấu thành nên bản rõ (P – Plaintext), thường thì đây là các đoạn văn bản trong một ngôn ngữ nào đó; còn những từ, những ký tự ở dạng bí mật không thể hiểu được thì được gọi là bản mã (C – Ciphertext).

a. Vai trò của hệ mật mã

Các hệ mật mã phải thực hiện được các vai trò sau:

- Hệ mật mã phải che dấu được nội dung của văn bản rõ (Plain Text) để đảm bảo sao cho chỉ người chủ hợp pháp của thông tin mới có quyền truy cập thông tin (Secrety), hay nói cách khác là chống truy cập không đúng quyền hạn.

- Tạo các yếu tố xác thực thông tin, đảm bảo thông tin lưu hành trong hệ thống đến người nhận hợp pháp là xác thực (Authenticity).

- Tổ chức các sơ đồ chữ ký số, đảm bảo không có hiện tượng giả mạo, mạo danh để gửi thông tin trên mạng.

Ưu điểm lớn nhất của bất kỳ hệ mật mã nào đó là có thể đánh giá được độ phức tạp tính toán mà "kẻ địch" phải giải quyết bài toán để có thể lấy được thông tin của dữ liệu đã được mã hóa. Tuy nhiên mỗi hệ mật mã có một số ưu và nhược điểm khác nhau, nhưng nhờ đánh giá được độ phức tạp tính toán mà ta có thể áp dụng các thuật toán mã hóa khác nhau cho từng ứng dụng cụ thể tùy theo từng yêu cầu về độ an toàn.

b. Các thành phần của một hệ mật mã:

Một hệ mật mã là một bộ 5 (P, C, K, E, D) thỏa mãn các điều kiện sau:

- P là một tập hợp hữu hạn các bản rõ (Plain Text), nó được gọi là không gian bản rõ.

- C là tập các hữu hạn các bản mã (Crypto), nó còn được gọi là không gian các bản mã. Mỗi phần tử của C có thể nhận được bằng cách áp dụng phép mã hóa E_k lên một phần tử của P, với $k \in K$.

- K là tập hữu hạn các khóa hay còn gọi là không gian khóa. Đối với mỗi phần tử k của K được gọi là một khóa (Key). Số lượng của không gian khóa phải đủ lớn để "kẻ địch" không đủ thời gian để thử mọi khóa có thể (phương pháp vét cạn).