ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC CNTT & TT THÁI NGUYÊN

Trương Mạnh Cường

LUẬN VĂN THẠC SỸ KHOA HỌC MÁY TÍNH

NGHIÊN CỨU CÁC THUẬT TOÁN MÃ HÓA KHÓA CÔNG KHAI VÀ ỨNG DỤNG TRONG CHỮ KÝ ĐIỆN TỬ

Chuyên ngành: KHOA HỌC MÁY TÍNH

Mã số: 60 48 01

THÁI NGUYÊN - 2014

ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC CNTT & TT THÁI NGUYÊN

Trương Mạnh Cường

LUẬN VĂN THẠC SỸ KHOA HỌC MÁY TÍNH

NGHIÊN CỨU CÁC THUẬT TOÁN MÃ HÓA KHÓA CÔNG KHAI VÀ ỨNG DỤNG TRONG CHỮ KÝ ĐIỆN TỬ

GIÁO VIÊN HƯỚNG DẪN
PGS.TS BÙI THẾ HỒNG

THÁI NGUYÊN - 2014

MỤC LỤC

DANH MỤC CÁC CHỮ TIẾNG ANH VIẾT TẮT

NIST	National Institute of Standards and Technology
RSA	R. Rivest, A. Shamir, L. Adleman
MITM	Man-In-The-Middle attack
MD	Message-Digest algorithm
SHA	Secure Hash Algorithm
MAC	Message Authentication Code
PKCS	Public Key Cryptography Standards

DANH MỤC CÁC HÌNH

MỞ ĐẦU

1. Lý do nghiên cứu đề tài

Bảo mật thông tin luôn là nhu cầu cần thiết trong các lĩnh vực tình báo, quân sự, ngoại giao, thông tin thương mại. Bảo mật thông tin cũng là một vấn đề đã được nghiên cứu từ xưa đến nay.

Bảo mật thông tin là duy trì tính bảo mật, tính toàn vẹn, tính sẵn sàng. Tính bảo mật là đảm bảo thông tin chỉ được tiếp cận bởi những người được cấp quyền trao đổi thông tin. Tính toàn vẹn của thông tin là bảo vệ sự chính xác, hoàn chỉnh của thông tin và thông tin chỉ được thay đổi bởi những người được cấp quyền. Tính sẵn sàng của thông tin là những người được quyền sử dụng có thể truy xuất thông tin khi họ cần. Để đảm bảo được các yêu cầu về thông tin trên thì rất nhiều người trong nước và thế giới đang tập trung nghiên cứu và tìm mọi giải pháp để đảm bảo an toàn, an ninh cho các giao dịch điện tử trên máy tính.

Giao dịch điện tử ở Việt Nam hiện nay đã và đang được quan tâm. Những giao dịch điện tử xuất hiện cùng với sự phổ dụng của máy tính và mạng Internet. Đã có những luật, văn bản dưới luật cho lĩnh vực an toàn thông tin trong giao dịch điện tử như: Quốc hội thông qua luật thương mại, luật giao dịch điện tử... Thủ tướng Chính phủ đã ban hành Quyết định số 1073/QĐ-TTg ngày 12/7/2010 phê duyệt kế hoạch tổng thể phát triển thương mại điện tử giai đoạn 2010 – 2015...

Cùng với xu thế chung của đất nước, cũng là yêu cầu đặt ra với chính công việc của mình, học viên đã chọn đề tài về an toàn thông tin, mà ở đây cụ thể là áp dụng các thuật toán mã hóa khóa công khai, hàm băm, chữ ký điện tử, làm mục tiêu nghiên cứu. Mong muốn những tìm tòi của mình có thể xây dựng được ứng dụng phục vụ cho cơ quan, đơn vị nơi học viên công tác.

2. Hướng nghiên cứu đề tài

- Nghiên cứu các giải thuật mã hóa khóa công khai.
- Nghiên cứu về chữ ký điện tử, tìm hiểu về hàm băm và các giải thuật về hàm băm.

- Cài đặt thử nghiệm một giải thuật sinh chữ ký điện tử.

3. Đối tượng nghiên cứu

- Một số thuật toán sinh khóa công khai, khóa bí mật;
- Một số hàm băm thường sử dụng hiện nay;
- Chữ ký điện tử.

4. Phương pháp nghiên cứu đề tài

- Tìm hiểu dựa trên cơ sở lý thuyết, các thuật toán hay về sinh khóa công khai, khóa bí mật đã có từ trước. So sánh để thấy những ưu điểm, những hạn chế của từng thuật toán.
- Từ cơ sở đó có thể cải tiến, hoặc triển khai ứng dụng cài đặt một giải thuật tối ưu nhất vào thực tiễn.
- Trong quá trình triển khai ứng dụng nêu lên những hạn chế của đề tài và những khó khăn trong thực hiện đề tài.
- Đề xuất hướng phát triển của đề tài trong thời gian tới.

5. Cấu trúc của luận văn

Ngoài phần mở đầu và kết luận đề tài có cơ cấu gồm 3 chương:

Chương 1 : Tổng quan về các thuật toán mã hóa khóa công khai

Chương 2: Hàm băm và chữ ký điện tử

Chương 3: Xây dựng ứng dụng.

CHƯƠNG 1. TỔNG QUAN VỀ CÁC THUẬT TOÁN MÃ HÓA KHÓA CÔNG KHAI

1.1 Khái niệm mã hóa khóa công khai

1.1.1 Mật mã hóa khóa đối xứng

Trong mật mã học, các thuật toán khóa đối xứng (symmetric key algorithms) là một lớp các thuật toán mật mã hóa trong đó các khóa dùng cho việc mật mã hóa và giải mã có quan hệ rõ ràng với nhau (có thể dễ dàng tìm được một khóa nếu biết khóa kia).

Khóa dùng để mã hóa có liên hệ một cách rõ ràng với khóa dùng để giải mã có nghĩa chúng có thể hoàn toàn giống nhau, hoặc chỉ khác nhau nhờ một biến đổi đơn giản giữa hai khóa. Trên thực tế, các khóa này đại diện cho một bí mật được phân hưởng bởi hai bên hoặc nhiều hơn và được sử dụng để giữ gìn sự bí mật trong kênh truyền thông tin

Thuật toán đối xứng có thể được chia ra làm hai thể loại, mật mã luồng (stream ciphers) và mật mã khối (block ciphers). Mật mã luồng mã hóa từng bit của thông điệp trong khi mật mã khối gộp một số bit lại và mật mã hóa chúng như một đơn vị. Cỡ khối được dùng thường là các khối 64 bit. Những thuật toán mã hóa khóa đối xứng nổi tiếng là DES và AES.

Các thuật toán đối xứng thường không được sử dụng độc lập. Trong thiết kế của các hệ thống mật mã hiện đại, cả hai kiểu mật hóa khóa đối xứng và khóa bất đối xứng thường được sử dụng phối hợp để tận dụng các ưu điểm của chúng.

1.1.2 Mật mã hóa khóa công khai

Là một dạng mật mã hóa cho phép người sử dụng trao đổi các thông tin mật mà không cần phải trao đổi các khóa chung bí mật trước đó. Điều này được thực hiện bằng cách sử dụng một cặp khóa có quan hệ toán học với nhau là khóa công khai và khóa cá nhân (hay khóa bí mật).

Thuật ngữ "mật mã hóa khóa bất đối xứng" thường được dùng đồng nghĩa với "mật mã hóa khóa công khai" mặc dù hai khái niệm không hoàn toàn tương đương. Có những thuật toán mật mã khóa bất đối xứng không có

tính chất khóa công khai và bí mật như đề cập ở trên mà cả hai khóa (cho mã hóa và giải mã) đều cần phải giữ bí mật.

Trong mật mã hóa khóa công khai, khóa cá nhân phải được giữ bí mật trong khi khóa công khai được phổ biến công khai. Trong 2 khóa, một dùng để mã hóa và khóa còn lại dùng để giải mã. Điều quan trọng đối với hệ thống là không thể tìm ra khóa bí mật nếu chỉ biết khóa công khai.

Hệ thống mật mã hóa khóa công khai có thể sử dụng với các mục đích:

- **Mã hóa**: giữ bí mật thông tin và chỉ có người có khóa bí mật mới giải mã được.
- **Tạo chữ ký số**: cho phép kiểm tra một văn bản có phải đã được tạo với một khóa bí mật nào đó hay không.
- **Thỏa thuận khóa**: cho phép thiết lập khóa dùng để trao đổi thông tin mật giữa 2 bên.

Thông thường, các kỹ thuật mật mã hóa khóa công khai đòi hỏi khối lượng tính toán nhiều hơn các kỹ thuật mã hóa khóa đối xứng nhưng những lợi điểm mà chúng mang lại khiến cho chúng được áp dụng trong nhiều ứng dụng.

Có thể hình dung hệ mật này tương tự như sau. A đặt một vật vào một hộp kim loại và rồi khoá nó lại bằng một khoá số do B để lại. Chỉ có B là người duy nhất có thể mở được hộp vì chỉ có người đó mới biết tổ hợp mã của khoá số của mình.

Thuật toán mã hóa công khai là thuật toán được thiết kế sao cho khóa mã hóa là khác so với khóa giải mã. Mà khóa giải mã hóa không thể tính toán được từ khóa mã hóa. Khóa mã hóa gọi là khóa công khai (public key), khóa giải mã được gọi là khóa riêng (private key).