**KHOA CÔNG NGHỆ THÔNG TIN**
**ĐẠI HỌC THÁI NGUYÊN**

**NGUYỄN NGỌC TRUNG**

# CÁC THUẬT TOÁN TỐI ƯU HÓA TRONG BẢO MẬT THÔNG TIN

**CHUYÊN NGÀNH : KHOA HỌC MÁY TÍNH**
**MÃ SỐ : 60.48.01**

## LUẬN VĂN THẠC SĨ KHOA HỌC NGÀNH CÔNG NGHỆ THÔNG TIN

**NGƯỜI HƯỚNG DẪN KHOA HỌC**
**PGS.TSKH. NGUYỄN XUÂN HUY**

**Thái Nguyên 03/2008**

## LỜI CẢM ƠN

Tôi xin gửi lời cảm ơn tới Khoa CNTT – ĐHTN, nơi các thầy cô đã tận tình truyền đạt các kiến thức quý báu cho tôi trong suốt quá trình học tập. Xin cảm ơn Ban chủ nhiệm khoa và các cán bộ đã tạo điều kiện tốt nhất cho chúng tôi học tập và hoàn thành đề tài tốt nghiệp của mình.

Đặc biệt, tôi xin gửi tới PGS. TSKH Nguyễn Xuân Huy, thầy đã tận tình chỉ bảo tôi trong suốt quá trình thực hiện đề tài lời cảm ơn và biết ơn sâu sắc nhất. Bên cạnh những kiến thức khoa học, thầy đã giúp tôi nhận ra những bài học về phong cách học tập, làm việc và những kinh nghiệm sống quý báu.

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

**Thái Nguyên, ngày 10 tháng 11 năm 2008**

**Nguyễn Ngọc Trung**

## 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 **PGS. TSKH Nguyễn Xuân Huy.**

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

***Học viên thực hiện***

**Nguyễn Ngọc Trung**

# MỤC LỤC

Trang

# DANH MỤC CÁC KÝ HIỆU, CÁC CHỮ VIẾT TẮT

| | |
|---|---|
| CRT | Chinese Remainder Theorem |
| DES | Data Encryption Standard |
| RSA | Rivest ShamirAdleman |
| GCD | Great Comon Divisor |
| FFT | Fast Fourier Transform |

# DANH MỤC CÁC BẢNG

Trang

# DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ

Trang

# MỞ ĐẦU

## 1. Lý do chọn đề tài

Các hệ mã công khai như RSA thực hiện tính toán với các số nguyên lớn hàng trăm chữ số. Độ phức tạp trong việc giải mã các hệ mã này tỉ lệ thuận với độ lớn của các số nguyên tham gia vào việc tạo khóa mã hóa và khóa công khai. Do đó để hệ mã an toàn, cần tăng kích thước của các số nguyên.

Mặt khác, khi kích thước của các số nguyên cần xử lý lớn thì thời gian xử lý của chương trình mã hóa cũng tăng lên.

Thông tin cần mã hóa ngày càng đa dạng và có khối lượng lớn, đòi hỏi hệ mã giảm thiểu thời gian xử lý.

Các công cụ và giải thuật nhằm bẻ khóa các hệ mật mã được cải tiến đòi hỏi hệ mã cần được nâng cấp tính bảo mật.

Tuy nhiên, việc nghiên cứu và triển khai các nâng cấp trong việc tối ưu hóa về mặt thuật toán trong các phép xử lý số học của các hệ mã còn hạn chế trong phạm vi các chương trình độc quyền.

Để hỗ trợ giải quyết các vấn đề trên, đề tài này tập trung vào việc xây dựng một số thuật toán tối ưu hóa nhằm tăng hiệu quả các phép tính toán thực hiện với số nguyên lớn.

Các kết quả của đề tài sẽ được ứng dụng trong việc hỗ trợ cho các phép xử lý số học của các hệ mã. Từ đó làm tăng tốc độ xử lý và tính bảo mật của các hệ mã.

Từ tính cấp thiết của vấn đề tối ưu hóa các hệ mã công khai, đồng thời được sự hướng dẫn và gợi ý của PGS.TSKH Nguyễn Xuân Huy tôi đã chọn đề tài cho luận văn tốt nghiệp Cao học ngành khoa học máy tính là:

**“Các thuật toán tối ưu hóa trong bảo mật thông tin”.**

## 2. Mục đích và nhiệm vụ

- ***Mục tiêu***
  - ***Về học thuật:***

    Đề tài này tập trung vào việc xây dựng một số thuật toán tối ưu hóa nhằm tăng hiệu quả các phép tính toán thực hiện với số nguyên lớn.
  - ***Về phát triển và triển khai ứng dụng:***

    Các kết quả của đề tài sẽ được ứng dụng trong việc hỗ trợ cho các phép xử lý số học với số nguyên lớn trong các hệ mã. Từ đó làm tăng tốc độ xử lý và tính bảo mật của các hệ mã.
- ***Nhiệm vụ***

  - Nghiên cứu các quá trình thực hiện mã hóa và giải mã của các hệ mã công khai.
  - Tìm hiểu các thuật toán xử lý số học được dùng trong các hệ mã.
  - Phát hiện các giải thuật tính toán cần tối ưu hóa.
  - Thực hiện đưa ra giải pháp tối ưu hóa các giải thuật này.
  - Ứng dụng trong một hệ mã cụ thể.
  - So sánh với kết quả thực thi của hệ mã khi chưa thực hiện tối ưu hóa.

## 3. Phương pháp nghiên cứu

- Nghiên cứu dựa trên việc tìm hiểu các giải thuật xử lý với số nguyên lớn của các hệ mã. Cụ thể là hệ mã hóa RSA, từ kết quả nghiên cứu có được sẽ định hướng lựa chọn thuật toán nào cần tối ưu hóa.

- Thực hiện việc tối ưu hóa các giải thuật bằng cách tối ưu các phép xử lý với số học lớn. Thao tác này sử dụng kết hợp các phương pháp tính toán với số học nhằm tăng hiệu năng của từng bước xử lý.

- Thu thập các tài liệu đã xuất bản, các bài báo trên các tạp chí khoa học và các tài liệu trên mạng Internet có liên quan đến vấn đề đang nghiên cứu.

- Tìm hiểu, vận dụng và kế thừa các thuật toán và qui trình mã đã công bố kết quả.

- Thực nghiệm cài đặt ứng dụng để minh họa các vấn đề trình bày trong đề tài.

**4. Đối tượng và phạm vi nghiên cứu**

◆ ***Đối tượng nghiên cứu*** **:**

Các hệ mật mã khóa công khai, trong đó hệ mật mã RSA được sử dụng làm đối tượng nghiên cứu chính của đề tài nhằm phát hiện các phép xử lý toán học cần tối ưu. Từ các kết quả thu được bước đầu đề tài đưa ra một cách xây dựng thử nghiệm hệ mã RSA áp dụng các kết quả tối ưu hóa.

◆ ***Phạm vi nghiên cứu***

Đề tài thực hiện việc tối ưu hóa với một số phép tính toán với số nguyên lớn.

Ứng dụng thử nghiệm trong một hệ mã nhằm so sánh hiệu năng xử lý của hệ mã trước và sau khi tối ưu.

Đề tài giới hạn trong phạm vi nghiên cứu để đưa ra giải pháp, việc triển khai ứng dụng thực tiễn cần có thêm các điều kiện về thời gian và quy mô.

**5. Ý nghĩa khoa học và thực tiễn của luận văn**

◆ ***Ý nghĩa khoa học***

- Trình bày các kiến thức toán học cơ bản, lý thuyết độ phức tạp của thuật toán, các thuật toán thường dùng trong các hệ mật mã khoá công khai.

- Trình bày các phương pháp mật mã gồm: Phương pháp mã hoá khóa bí mật và phương pháp mã hoá khóa công khai. Với phương pháp mã hóa khóa công khai thì tập trung vào các thuật toán mã hóa RSA. Với phương pháp mã hóa khóa bí mật chỉ giới thiệu sơ lược để so sánh với phương pháp mã hóa khóa công khai.

- Tối ưu các phép xử lý số học với số nguyên lớn là một yêu cầu cần thiết trong việc xây dựng các hệ mã hóa có tốc độ xử lý và độ an toàn cao.

◆ ***Ý nghĩa thực tiễn***

- Cài đặt hoàn chỉnh các giải thuật xử lý số học với số nguyên lớn cỡ hàng trăm chữ số.