ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN THỊ BÌNH

MỘT SỐ THUẬT TOÁN PHÂN TÍCH SỐ NGUYÊN HIỆN ĐẠI VÀ ỨNG DỤNG

LUẬN VĂN THẠC SĨ TOÁN HỌC

THÁI NGUYÊN - 2017

ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN THỊ BÌNH

MỘT SỐ THUẬT TOÁN PHÂN TÍCH SỐ NGUYÊN HIỆN ĐẠI VÀ ỨNG DỤNG

LUẬN VĂN THẠC SĨ TOÁN HỌC

Chuyên ngành: **Phương pháp Toán sơ cấp**

Mã số: **60 46 01 13**

NGƯỜI HƯỚNG DẪN KHOA HỌC

GS.TSKH. HÀ HUY KHOÁI

THÁI NGUYÊN - 2017

Mục lục

Lời cảm ơn

Luận văn này được thực hiện tại Trường Đại học Khoa học - Đại học Thái Nguyên và hoàn thành với sự hướng dẫn của GS.TSKH. Hà Huy Khoái (Trường Đại học Thăng Long, Hà Nội). Tác giả xin được bày tỏ lòng biết ơn chân thành và sâu sắc tới người hướng dẫn khoa học của mình đã dành nhiều công sức hướng dẫn để tác giả hoàn thành luận văn.

Tác giả xin trân trọng cảm ơn Ban Giám hiệu Trường Đại học Khoa học - Đại học Thái Nguyên, Ban Chủ nhiệm Khoa Toán-Tin, cùng các giảng viên đã tham gia giảng dạy, đã tạo mọi điều kiện tốt nhất để tác giả học tập và nghiên cứu.

Tác giả muốn gửi những lời cảm ơn tốt đẹp nhất tới tập thể Lớp B, cao học Toán khóa 9 (2015-2017) đã động viên và giúp đỡ tác giả rất nhiều trong suốt quá trình học tập.

Nhân dịp này, tác giả cũng xin chân thành cảm ơn Sở Giáo dục và Đào tạo Hải Phòng, Ban Giám hiệu và các đồng nghiệp ở Trường THPT Nguyễn Đức Cảnh, Huyện Kiến Thụy, Thành phố Hải Phòng đã tạo điều kiện cho tác giả hoàn thành tốt nhiệm vụ học tập và công tác của mình.

Cuối cùng, tác giả muốn dành những lời cảm ơn đặc biệt nhất đến bố mẹ và đại gia đình đã luôn động viên và chia sẻ những khó khăn để tác giả hoàn thành tốt luận văn này.

Danh sách kí hiệu

$\mathbb{Z}$	vành các số nguyên
$\mathbb{Q}$	trường các số hữu tỷ
$\mathbb{F}_p$	trường có p phần tử
$K[X]$	vành đa thức với hệ số trên trường K
$\lceil x \rceil$	trần của số x
$\deg P(X)$	bậc của đa thức $P(X)$
$\bmod p$	modulo p
$\gcd(P(X), Q(X))$	ước chung lớn nhất của $P(X)$ và $Q(X)$
$\exp(\cdot)$	hàm số mũ
$\gcd(a, b)$	ước chung lớn nhất của a và b
$a \mid b$	a là ước của b
$\lfloor N \rfloor$	sàn của số N
$\mathbb{F}[\alpha]$	trường mở rộng của trường $\mathbb{F}$

Mở đầu

Trước những năm 70 của thế kỷ XX, Số học thường được xem là một trong những ngành toán học thuần tuý, chỉ có ý nghĩa lý thuyết. Đối tượng nghiên cứu của Số học là các quy luật trong tập hợp số nguyên; các giả thuyết lớn tồn tại trong Số học thường là các giả thuyết về số nguyên tố. Thậm chí, có những nhà toán học cho rằng, vẻ đẹp của số học có được nhờ sự xa rời thực tiễn của nó.

Ngày nay, những ứng dụng lớn lao và bất ngờ của Số học vào mật mã cho ta thấy rằng quan niệm trên đã hoàn toàn thay đổi. Vẻ đẹp của Số học không chỉ thể hiện trong ý nghĩa "thuần tuý" của nó, mà cả trong những ứng dụng bất ngờ vào thực tiễn. Cách đây khoảng 30 năm, khó có thể hình dung được rằng, một số kết quả lý thuyết trong Số học lại làm nên một cuộc cách mạng trong bảo mật thông tin trong Lý thuyết mật mã. Cơ sở của những ứng dụng đó chính là Số học thuật toán, lĩnh vực nghiên cứu các thuật toán trong Số học. Trong lĩnh vực Lý thuyết mật mã, *mật mã khóa công khai* là một dạng mật mã 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). Cơ sở toán học của vấn đề này là việc phân tích các số tự nhiên và một số vấn đề liên

quan đến chúng.

Luận văn này có mục đích tìm hiểu sơ lược về cơ sở toán học của Lý thuyết mật mã, đồng thời phân tích sâu hơn các thuật toán phân tích số tự nhiên để làm cơ sở toán học cho ứng dụng. Ngoài các phần Mở đầu, Kết luận, Tài liệu tham khảo, nội dung của luận văn được trình bày trong hai chương:

- *Chương 1. Thám mã và một số thuật toán cổ điển phân tích số nguyên*. Trong chương này chúng tôi trình bày các kiến thức cơ sở về thám mã và sau đó là một số thuật toán cổ điển phân tích số nguyên, làm cơ sở so sánh và phát triển cho chương tiếp theo.

- *Chương 2. Một số thuật toán hiện đại phân tích số nguyên*. Đây là nội dung chính của luận văn. Chúng tôi sẽ trình bày một số thuật toán hiện đại phân tích số nguyên như thuật toán phân tích Pollard, phân tích dùng đường cong elliptic hoặc sàng trường số.

Thái Nguyên, ngày 10 tháng 7 năm 2017

Tác giả

Nguyễn Thị Bình

Chương 1

Thám mã và một số thuật toán cổ điển phân tích số nguyên

1.1 Thám mã và phân tích số nguyên

Phần này em sẽ trình bày về thám mã. Thám mã là một vấn đề phức tạp nên trong luận văn này em xin phép chỉ đề cập những vấn đề đơn giản nhất. Phần đầu trong trình bày chúng tôi dựa vào [2].

Thám mã (hay *phân tích mã* - cryptanalysis) là việc nghiên cứu các phương pháp "phá vỡ" bức màn ngụy trang văn bản (do việc mã hóa tạo nên) để có thể hiểu được nội dung văn bản.

Hiện nay, trên quan điểm thám mã, người ta phân các hệ mã thành ba loại:

- Loại đã bị phá;
- Loại chưa được nghiên cứu phân tích (vì còn mới, hoặc vì chưa được dùng rộng rãi);

- Loại đã được nghiên cứu nhưng chưa bị phá (RSA, IDEA, các hệ mã sử dụng logarit rời rạc, đường cong elliptic, . . .).

Có ba cách thông dụng trong việc chuyển hóa *văn bản mã* thành *văn bản gốc*:

- Ăn trộm, hối lộ, hoặc mua (với giá rất cao) để có được chìa khóa;
- Khai thác tính cẩu thả hoặc lỏng lẻo của người dùng khóa (ví dụ : có người hay dùng tên người thân để làm mật khẩu hoặc chìa khóa);
- Phân tích mã (tức là thám mã).

Bây giờ, ta sẽ thảo luận về một số phương pháp thám mã. Thực tế, thám mã sẽ phức tạp hơn nếu người ta không biết hệ mật mã đã được sử dụng. chúng ta giả sử người thám mã đã biết rõ hệ mật mã được sử dụng khi tiến hành phân tích mã. Mục đích là thiết kế được một hệ mật mã an toàn bảo mật.

Dưới đây ta sẽ liệt kê các loại tấn công vào hệ mật mã. Mức độ tấn công sẽ phụ thuộc vào hiểu biết của người thám mã đối với hệ mật mã được sử dụng :

- **Tấn công chỉ biết bản mã (ciphertext-only):** người thám mã chỉ có bản tin mã hóa.
- **Tấn công biết bản tin rõ (known plaintext):** người thám mã có bản tin rõ và bản mã.

- **Tấn công chọn bản tin rõ (chosen plaintext):** người thám mã tạm thời có quyền truy xuất tới bộ mã hóa, do đó người thám mã có khả năng chọn bản tin rõ và xây dựng bản mã tương ứng.

- **Tấn công chọn bản mã (chosen ciphertext):** người thám mã tạm thời có quyền truy xuất tới bộ giải mã, do đó anh ta có khả năng chọn bản mã và xây dựng lại bản tin rõ tương ứng.

Bây giờ ta sẽ liệt kê các phương pháp thám mã

1. *Thám mã tích cực* là việc thám mã sau đó tìm cách làm sai lạc các dữ liệu truyền, nhận hoặc các dữ liệu lưu trữ phục vụ mục đích của người thám mã.

2. *Thám mã thụ động* là việc thám mã để có được thông tin về bản tin rõ phục vụ mục đích của người thám mã.

3. *Thám mã affine.* Trong mật mã affine, đầu tiên bảng chữ cái của thông điệp cần mã hóa có kích thước m sẽ được chuyển thành các con số tự nhiên từ $0,\ldots,m-1$. Sau đó dùng một hàm modulo để mã hóa và chuyển thành bản mã. Hàm mã hóa cho một ký tự như sau:

$$e(x) = (ax+b) \pmod{m}$$

với m là kích thước của bảng chữ cái, a và b là khóa mã. Giá trị a được chọn sao cho a và m là nguyên tố cùng nhau.

Giả sử Trudy đã lấy được bản mã sau đây: