ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN THỊ MINH HUỆ

SỐ GIẢ NGUYÊN TỐ VÀ ỨNG DỤNG

LUẬN VĂN THẠC SĨ TOÁN HỌC

THÁI NGUYÊN - 2017

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN THỊ MINH HUỆ

SỐ GIẢ NGUYÊN TỐ 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, người đã đặt vấn đề nghiên cứu, dành nhiều thời gian hướng dẫn và tận tình giải đáp những thắc mắc của tác giả trong suốt quá trình làm 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 Cao học Toán khóa 9B (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 Quang Trung, Huyện Thủy Nguyên, 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

$\left[\frac{b}{n}\right]$	ký hiệu Jacobi
$\pi(n)$	số các số nguyên tố nhỏ hơn hoặc bằng n
mod p	modulo p
$a \mid b$	b là bội của a
$a \equiv b \pmod{p}$	a đồng dư với b theo modulo p
$\gcd(a,b)$	ước chung lớn nhất của hai số nguyên a và b
$\sum_{i=1}^{m} a_i$	ký hiệu tổng $a_1 + a_2 + \cdots + a_m$
$\prod_{i=1}^{m} b_i$	ký hiệu tích $b_1 b_2 \cdots b_m$

Mở đầu

Có thể nói, Lý thuyết số là một ngành khoa học sớm nhất của nhân loại. Trước những năm 70 của thế kỷ XX, Lý thuyết số được coi là một ngành thuần túy lý thuyết, và thậm chí người ta còn ca ngợi vẻ đẹp của nó vì nó xa rời thực tiễn!

Tuy nhiên, như Issac Newton từng nói : "Không có gì gần với thực tiễn hơn là một lý thuyết đẹp", Lý thuyết số lại trở thành một ngành gần thực tiễn nhất, ứng dụng nhất, vì những ảnh hưởng lớn lao và bất ngờ của nó đến nhiều ngành, chẳng hạn như Lý thuyết mật mã. Trong lĩnh vực Lý thuyết mật mã, *mật mã hóa 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). Các kiến thức toán học được sử dụng ở đây là các mối quan hệ, các tính chất của số nguyên tố (prime), số giả nguyên tố (pseudoprime) và nhiều khía cạnh khác của Lý thuyết số.

Trong Lý thuyết số, *số giả nguyên tố* là một hợp số nguyên dương thỏa mãn nhiều quan hệ như các số nguyên tố. Nếu ta tìm được một quan hệ nào đó (ví dụ như đồng dư thức trong định lý Fermat bé) sao cho số các hợp số thoả mãn quan hệ đó là "rất ít" so với các số nguyên tố, thì những số giả nguyên tố xét theo quan hệ đó có thể sử dụng để tìm ra những số *nguyên tố xác suất*, tức là những số mà về mặt lý thuyết, có thể là hợp số với một xác suất rất nhỏ.

Luận văn này có một mục đích, một mặt là tìm hiểu sơ lược về cơ sở Toán học của Lý thuyết mật mã, mặt khác, là tìm hiểu một số loại số giả nguyên tố được nhiều người quan tâm.

Ngoài các phần Mở đầu, Kết luận, Tài liệu tham khảo, nội dung của luận văn được trình bày trong hai chương:

- *Chương 1. Số giả nguyên tố trong lý thuyết mật mã khóa công khai*. Trong chương này chúng tôi trình bày các kiến thức cơ sở về các số giả nguyên tố trong lý thuyết mật mã khóa công khai bao gồm cơ sở toán học của lý thuyết mật mã và độ phức tạp của việc sinh số nguyên tố lớn.

- *Chương 2. Một số loại số giả nguyên tố*. Chương này dành để trình bày về một số loại số giả nguyên tố quan trọng bao gồm số giả nguyên tố Fermat, số giả nguyên tố mạnh, số giả nguyên tố Euler, số giả nguyên tố Catalan.

Tác giả hy vọng rằng, bản luận văn này có thể làm tài liệu tham khảo hữu ích cho những ai quan tâm đến Lý thuyết số và các vấn đề ứng dụng thực tiễn, ví dụ như mật mã, và nó cũng có thể được làm tài liệu bồi dưỡng học sinh khá giỏi, tài liệu tham khảo về Lý thuyết số.

Thái Nguyên, ngày 20 tháng 5 năm 2017

Tác giả

Nguyễn Thị Minh Huệ

Chương 1

Số giả nguyên tố trong lý thuyết mật mã khóa công khai

1.1 Cơ sở toán học của lý thuyết mật mã khoá công khai

Trong mục này, chúng ta sẽ thảo luận về việc áp dụng phân tích nhân tử và kiểm tra tính nguyên tố trong mật mã.

Trong mật mã chúng ta tìm cách truyền một tin nhắn bí mật m, chẳng hạn từ Alice cho Bob theo cách mà Oscar là người chặn tín hiệu không thể đọc được tin. Ý tưởng là phải đưa ra một khoá mã hoá Φ, là một hàm toán học biến m thành $r := \Phi(m)$ để gửi. Số r là những ký tự mà dường như vô nghĩa để cho Oscar không thể thông dịch và Bob có thể giải mã bằng cách tính $\Psi(r)$, trong đó $\Psi = \Phi^{-1}$. Cho tới gần đây (trước 1977), hiểu biết về khoá mã hoá Φ có thể cho phép Oscar xác định khoá giải mã Ψ, và do đó việc giữ bí mật khoá mã hoá Φ là một việc vô cùng quan trọng và thường là một nhiệm vụ khó khăn.

Nếu Oscar được cho một khoá mã hoá thì anh ta dễ dàng xác định khoá giải mã bằng cách đảo ngược những gì đã làm để mã hoá. Tuy nhiên, năm 1976, Diffie và Hellman , bằng cách đưa ra hệ mã mũ, dường như đã tạo ra khoá công khai Φ, theo đó Oscar có thể nhìn thấy nhưng không thể xác

định $\Psi = \Phi^{-1}$. Nếu việc này khả thi, Alice có thể quên đi khó khăn của việc giữ khoá bí mật.

Trong hệ thống mã hoá khoá công khai ngày nay, các khó khăn trong việc xác định Ψ từ Φ có xu hướng dựa trên một bài toán khó chưa giải được, thường là các bài toán mà ngay cả những người giỏi nhất như Gauss và các nhà toán học sau này đều không giải được, ví dụ như bài toán phân tích nhân tử. Bây giờ chúng ta nghiên cứu các hệ thống mật mã khoá công khai nổi tiếng nhất.

1.1.1 Hệ mã khoá RSA

Năm 1977, Ron Rivest, Adi Shamir và Len Adleman đề xuất một hệ thống mật mã khoá công khai, là trung tâm của nhiều hệ thống bảo mật máy tính ngày nay. Ý tưởng là Bob lấy hai số nguyên tố lớn $p < q$, tính tích của chúng $n = pq$, và xác định hai số nguyên d và e thoả mãn $de \equiv 1(\pmod{(p-1)(q-1)})$ (việc này dễ dàng). Khoá công khai, mà Alice sử dụng, sẽ bao gồm số n và khoá mã hoá e, trong khi đó Bob giữ khoá giải mã d bí mật (tức là giữ p và q). Ta giả sử tin nhắn m là một số nguyên thuộc $[1, n-1]$. Để mã hoá m, Alice tính $r := \Phi(m) \equiv m^e \pmod{n}$, với $\Phi(m) \in [1, n-1]$, có thể dễ dàng tính được. Để giải mã Bob tính $\Psi(r) := r^d \pmod{n}$, với $\Psi(r) \in [1, n-1]$. Sử dụng Định lý Euler (cho tích của p và q) ta có thể dễ dàng kiểm tra $m^{de} \equiv m \pmod{n}$, và do đó $\Psi = \Phi^{-1}$.

Oscar biết n, và nếu ông có thể phân tích nhân tử n, thì ông cũng có thể dễ dàng xác định Ψ, do đó độ bảo mật của hệ thống RSA phụ thuộc vào độ khó của việc phân tích nhân tử. Như đã nói ở trên, việc này vượt xa những gì khả thi ngày nay nếu chúng ta lấy p và q là các số nguyên tố có chứa

nhiều hơn 200 chữ số. Ta sẽ thấy rằng, việc tìm số nguyên tố (xác suất) lớn như vậy rất dễ dàng bằng cách sử dụng các số giả nguyên tố, vấn đề sẽ thảo luận trong luận văn.

1.1.2 Vấn đề lấy căn bậc hai modulo n

Từ Định lý Euler ta biết rằng, nếu ta có thể tìm được căn bậc hai b của 1 mod n mà khác ± 1, thì điều này chứng tỏ rằng n là hợp số. Thực vậy, từ b suy ra phép phân tích nhân tử của số lẻ n với:

$$\gcd(b-1,n)\gcd(b+1,n) = \gcd(b^2-1,n) = n \tag{1.1}$$

(do $b^2 \equiv 1 \pmod{n}$) trong đó $\gcd(b-1,n)$ và $\gcd(b+1,n)$ nhỏ hơn n (vì $b \not\equiv 1$ hay $-1 \pmod{n}$), kéo theo $1 < \gcd(b-1,n), \gcd(b+1,n) < n$ và do đó (1.1) là phép phân tích nhân tử không tầm thường của n.

Một cách tổng quát hơn ta giả sử rằng cho trước hợp số lẻ n với ít nhất hai nhân tử nguyên tố phân biệt, Oscar có một hàm f_n sao cho nếu a là một bình phương $\pmod{n}$, thì $f_n(a)^2 \equiv a \pmod{n}$. Sử dụng f_n, Oscar có thể dễ dàng phân tích nhân tử n (với thời gian đa thức ngẫu nhiên), vì nếu ông lấy các số nguyên b trong khoảng $[1,n-1]$ một cách ngẫu nhiên thì $\gcd(f_n(b^2)-b,n)$ là một nhân tử không tầm thường của n với điều kiện $b \not\equiv f_n(b^2)$ hay $-f_n(b^2) \pmod{n}$; vì có ít nhất bốn căn bậc hai của $b^2 \pmod{n}$, xác suất đây là một phép phân tích nhân tử của n là lớn hơn hoặc bằng $1/2$.

Sử dụng ý tưởng này, Rabin xây dựng một hệ thống mật mã khoá công khai mà về bản chất việc phá khoá khó như tìm phân tích nhân tử của n.