THÁI NGUYÊN - 2016
ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

TẠ THỊ HẰNG

SỐ NGUYÊN TỐ VÀ ỨNG DỤNG TRONG PHƯƠNG PHÁP CHỨNG MINH KHÔNG TIẾT LỘ THÔNG TIN

Chuyên ngành: Khoa học máy tính
Mã số: 60 48 0101

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

***Người hướng dẫn khoa học*: TS. Nguyễn Thị Hồng Minh**

THÁI NGUYÊN - 2016

Lời cam kết

Tài liệu được sử dụng trong luận văn được thu thập từ các nguồn kiến thức hợp pháp, có trích dẫn nguồn tài liệu tham khảo. Chương trình sử dụng mã nguồn mở, có xuất xứ.

Dưới sự giúp đỡ nhiệt tình và chỉ bảo chi tiết của giáo viên hướng dẫn, tôi đã hoàn thành luận văn của mình. Tôi xin cam kết luận văn này là của bản thân tôi làm và nghiên cứu, không hề trùng hay sao chép của bất kỳ ai.

Lời cảm ơn

Trước hết tôi xin gửi lời cảm ơn đến TS. Nguyễn Thị Hồng Minh, Phó Chủ nhiệm khoa Sau đại học, Đại học Quốc gia Hà Nội người đã hướng dẫn và giúp đỡ tôi rất nhiều trong suốt quá trình tìm hiểu nghiên cứu và hoàn thành khóa luận này. Sự hướng dẫn nhiệt tình của Tiến sĩ đã giúp tôi quyết tâm hoàn thành luận văn, qua đó bản thân tôi đã mở rộng hiểu biết về vấn đề bảo mật thông tin và các ứng dụng trong thự tế của nó.

Tôi cũng xin chân thành cảm ơn quý Thầy, Cô trong trường Đại học Công nghệ Thông tin & Truyền thông - Đại học Thái Nguyên; quý Thầy, Cô trong Viện Công nghệ thông tin đã tận tình truyền đạt kiến thức cho chúng tôi trong 2 năm học tập và nghiên cứu. Với vốn tiếp thu trong khóa học không chỉ là nền tảng cho quá trình nghiên cứu luận văn này mà còn là hành trang quý báu, nền tảng vững chắc để tôi tiếp tục nghiên cứu, hoạt động trong lĩnh vực công nghệ thông tin.

Cuối cùng xin cảm ơn gia đình, bạn bè, đồng nghiệp đã giúp đỡ và động viên tôi trong công việc và học tập cũng như trong quá trình thực hiện luận văn này.

Xin chúc mọi người luôn mạnh khoẻ, đạt được nhiều thành tích cao trong công tác, học tập và nghiên cứu khoa học!

Trân trọng cảm ơn!

Thái Nguyên, ngày 12 tháng 5 năm 2016

Tác giả

Tạ Thị Hằng

Danh mục viết tắt

Viết tắt	Giải thích
Đpcm	Điều phải chứng minh
CMKTTTT	Chứng minh không tiết lộ thông tin
UCLL	Ước chung lớn nhất
TTĐT	Thanh toán điện tử
CT	Cử Tri
KP	Kiểm Phiếu
TMĐT	Thương mại điện tử
GMR	Goldwasser, Micali và Rackoff
TT	Thông tin
BKP	Ban kiểm phiếu
CSDL	Cơ sở dữ liệu
BDK	Bàn Đăng Ký
BKP	Ban kiểm phiếu

Danh mục các hình và bảng

Hình 1.1: Sơ đồ quy trình bỏ lá phiếu điện tử……. 35
Hình 1.2: Sơ đồ giai đoạn đăng ký bỏ phiếu…… 36
Hình 1.3: Sơ đồ giai đoạn bỏ phiếu……. 38

Lời nói đầu

Ngày nay, công nghệ thông tin đang phát triển mạnh mẽ, Internet đã trở thành một phần không thể thiếu trong cuộc sống hàng ngày thì các hoạt động trao đổi thông tin, mua bán,…trên mạng Internet diễn ra thường xuyên và ngày phổ biến hơn. Chính vì vậy mà việc bảo mật, đảm bảo an toàn thông tin đang là nhu cầu cấp thiết. Trước các nhu cầu cấp thiết đó, lý thuyết về mật mã thông tin đã ra đời nhằm đảm bảo tính an toàn dữ liệu tại nơi lưu trữ cũng như khi dữ liệu đang được truyền trên mạng. Mật mã học là một trong những vấn đề quan trọng trong lĩnh vực bảo mật và an toàn thông tin.Trên thế giới mật mã học được ra đời từ thời La Mã cổ đại và ngày càng được nghiên cứu, phát triển đạt những thành tựu to lớn. Trong mật mã học thì vấn đề bảo mật luôn đi đôi với vấn đề xác thực thông tin, đặc biệt trong hệ thống mã hóa khóa công khai vấn đề xác thực là vô cùng quan trọng, để giải quyết vấn đề trên người ta đưa ra một cách giải quyết hiệu quả, đó là phương pháp chứng minh không tiết lộ thông tin. Với sự bùng nổ của mạng Internet hiên nay, mạng máy tính đang ngày càng đóng vai trò thiết yếu trong lĩnh vực hoạt động xã hội, và khi nó trở thành phương tiện điều hành các hệ thống thì nhu cầu bảo mật thông tin được đặt lên hàng đầu. Việc sử dụng phương pháp chứng minh không tiết lộ thông tin là một giải pháp hữu hiệu, ngày càng được ứng dụng nhiều trong thực tế, không chỉ giới hạn trong nghành công nghệ thông tin, mật mã học mà còn được áp dụng nhiều trong lĩnh vực khác như ngân hàng, viễn thông…”Chứng minh không tiết lộ thông tin (zero Knowledge Proofs” là phương pháp chứng minh không có nghĩa là “ không để lộ thông tin” mà là “để lộ thông tin ở mức thấp nhất” về sự vật, sự việc cần chứng minh. Với việc “không để lộ” người xác minh sẽ không có nhiều hiểu biết về sự vật, sự việc, họ chỉ thu được chút ít thông tin (coi như là không) về tính chất của nó nhưng vẫn đảm bảo được nhận thức về tính đúng của đối tượng cần xác minh.

Số nguyên tố, một phát minh kì diệu của con người, được quan tâm không chỉ bởi cộng đồng toán học mà cả cộng đồng tin học do tính chất đặc biệt của nó và cả những ứng dụng thực tế hiệu quả. Ứng dụng chính của số nguyên tố là trong lĩnh vực mã hóa (cryptography), trong đó chúng ta cần tạo ra những số nguyên tố với hàng trăm chữ số. Kiểm tra một số có phải số nguyên tố hay không, làm sao sinh được các số nguyên tố càng lớn càng tốt là những bài toán khá quan trọng trong khoa học máy tính.

Trong đề tài này em tập trung nghiên cứu về một số vấn đề liên quan tới số nguyên tố lớn và ứng dụng trong phương pháp chứng minh không tiết lộ thông tin (bỏ lá phiếu điện tử và tiền điện tử).

Bố cục luận văn gồm 3 chương. Chương 1 giới thiệu số nguyên tố và các bài toán liên quan và cách phân tích thừa số nguyên tố.Tiếp theo chương 2 trình bày về thuật toán kiểm tra số nguyên tố lớn và ứng dụng trong phương pháp chứng minh không tiết lộ thông tin như bỏ lá phiếu điện tử, tiền điện tử từ đó chúng tôi sẽ có những vị trí đặt trạm làm tiền đề cho chương 3 với thuật toán kiểm tra số nguyên tố lớn để ứng dụng trong bỏ lá phiếu điện tử. Chương 3 sẽ trình bày một số kết quả thực nghiệm để kiểm chứng hiệu quả của thuật toán trên hệ thống máy tính để kiểm tra và sinh số nguyên tố lớn, lồng ghép vào chương trình chứng minh không tiết lộ thông tin trong việc mô tả quá trình bỏ lá phiếu điện tử.

Chương 1: Số nguyên tố và các bài toán liên quan

1.1. Định nghĩa số nguyên tố

Số tự nhiên *p*, lớn hơn 1 gọi là số nguyên tố nếu như nó chỉ chia hết cho 1 và chính nó. Định lý cơ bản của số học nói rằng, bất kỳ số tự nhiên *n*, lớn hơn 1 có thể phân tích thành tích các số nguyên tố. Tức là một số tự nhiên n có thể biểu diễn dưới dạng sau:

$$n = p_1^{\alpha_1} ... p_k^{\alpha_k},$$

ở đây $p_1 < p_2 < ... < p_k$ - là các số nguyên tố khác nhau, $\alpha_1,...,\alpha_k \in N$.

1.2. Tính chất của số nguyên tố

Ký hiệu "$b \mid a$" nghĩa là *b* là ước của *a*, ký hiệu $a \vdots b$ nghĩa là *a* chia hết cho *b*.

- Ước tự nhiên khác 1 nhỏ nhất của một số tự nhiên là số nguyên tố.

Chứng minh: Giả sử $d \mid a$; *d* nhỏ nhất; $d \neq 1$.

Nếu d không nguyên tố $\Rightarrow$ $d = d_1.d_2$; $d_1, d_2 > 1$

$\Rightarrow d_1 | a$ với $d_1 < d$: mâu thuẫn với *d* nhỏ nhất. Vậy *d* là nguyên tố.

- Cho *p* là số nguyên tố; $a \in$ N; $a \neq 0$. Khi đó

  $(a,p) = p \Leftrightarrow (a \vdots p)$

  $(a,p) = 1 \Rightarrow (a \not\vdots p)$

- Nếu tích của nhiều số chia hết cho một số nguyên tố *p* thì có ít nhất một thừa số chia hết cho *p*.

- Ước số dương bé nhất khác 1 của một hợp số *a* là một số nguyên tố không vượt quá $\sqrt{a}$

- 2 là số nguyên tố nhỏ nhất và cũng là số nguyên tố chẵn duy nhất

- Tập hợp các số nguyên tố là vô hạn.

1.3. Sinh số nguyên tố và phân tích thừa số nguyên tố

1.3.1. Sinh số nguyên tố

Vậy làm sao chúng ta có thể tìm ra được các số nguyên tố trong số các số nguyên dương (hay số tự nhiên dương)? Trong tập hợp các số tự nhiên, có bao nhiêu số nguyên tố? Cho đến nay, người ta vẫn chưa biết được, bởi vì quy luật của nó rất khó tìm, giống như đứa trẻ bướng bỉnh vậy, nó nấp ở phía đông, chạy ở phía tây, thách thức các nhà toán học.

Có lẽ chúng ta cũng đã từng nghe đến phương pháp sàng lọc của nhà toán học Eratosthenes, dùng phương pháp này có thể tìm ra các số nguyên tố rất tiện lợi. Nó giống như là sàng lấy sỏi trong cát, sàng lọc lấy những số nguyên tố trong tập hợp số tự nhiên, bảng các số nguyên tố chính là được làm theo phương pháp này.

Thế nhưng, các nhà toán học chưa thỏa mãn với việc dùng phương pháp này để tìm ra số nguyên tố, bởi vì nó có chút mò mẫm nhất định, bạn không thể biết trước được số nguyên sẽ "sàng" ra số nào. Điều mà các nhà toán học muốn là tìm ra quy luật của số nguyên tố để nghiên cứu sâu hơn về nó.

Từ trong bảng các số nguyên tố, chúng ta có thể thấy chúng được phân bố như sau: từ 1 đến 1000 có 168 số nguyên tố; từ 1000 đến 2000 có 135 số; từ 2000 đến 3000 có 127 số; từ 3000 đến 4000 có 120 số; từ 4000 đến 5000 có 119 số. Khi số các số tự nhiên càng lớn thì tỉ lệ phân bố các số nguyên tố càng thưa. Số nguyên tố đã "hoá trang" cho mình rồi lẩn khuất trong các số tự nhiên, khiến việc tìm ra chúng trở nên khó khăn hơn.

Ví dụ, 101, 401, 601, 701 đều là số nguyên tố, nhưng 301 và 901 thì lại không phải. Có người thử tính như thế này: 12 + 1 + 41 = 43, 22 + 2 + 41 = 47, 32 + 3 + 41 = 53, ..., 392 + 39 + 41 = 1601. Có 39 số từ 43 cho đến 1601 đều là số nguyên tố, thế nhưng tiếp sau đó: 402 +40 +41 =1681 = 41 x 41 thì lại là một hợp số.