ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

VĂN THỊ THU THỊNH

LÔGARIT RỜI RẠC VÀ MẬT MÃ CÔNG KHAI

Chuyên ngành: TOÁN ỨNG DỤNG
Mã số: 60.46.01.12

LUẬN VĂN THẠC SĨ TOÁN HỌC

NGƯỜI HƯỚNG DẪN KHOA HỌC:
TS. VŨ MẠNH XUÂN

THÁI NGUYÊN – 2014

MỤC LỤC

LỜI CẢM ƠN

Sau một thời gian nghiên cứu tìm hiểu, em đã hoàn thành luận văn thạc sỹ toán học chuyên ngành toán ứng dụng với đề tài: ***" Lôgarit rời rạc và mật mã công khai".***

Lời đầu tiên em xin bày tỏ lòng biết ơn sâu sắc tới thầy giáo **TS. Vũ Mạnh Xuân** đã tận tình hướng dẫn em trong suốt quá trình nghiên cứu và thực hiện đề tài. Em cũng xin chân thành cảm ơn quý thầy cô khoa Toán – tin trường Đại học Khoa học – Đại học Thái Nguyên, các đồng nghiệp và các bạn học trong lớp đã hướng dẫn, truyền đạt kiến thức, tạo mọi điều kiện giúp đỡ cho em trong suốt thời gian theo học và thực hiện luận văn này.

Qua việc nghiên cứu và hoàn thành luận văn, em đã có thêm nhiều kiến thức bổ ích trong chuyên môn cũng như phương pháp luận nghiên cứu khoa học. Trong khuôn khổ của một luận văn, chắc chắn chưa đáp ứng được đầy đủ những vấn đề đặt ra. Vì điều kiện nghiên cứu còn hạn chế, nên mặc dù đã cố gắng rất nhiều nhưng luận văn không tránh khỏi những thiếu sót. Em rất mong nhận được sự đóng góp ý kiến, phê bình quý báu của các nhà khoa học, các thầy cô và các bạn đồng nghiệp.

Một lần nữa em xin chân thành cảm ơn !

Thái Nguyên, tháng 09 năm 2014

Học viên

Văn Thị Thu Thịnh

MỞ ĐẦU

Bài toán logarit rời rạc trong Z_p là đối tượng trong nhiều công trình nghiên cứu và được xem là bài toán khó nếu p được chọn cẩn thận. Bài toán này có nhiều ứng dụng sâu sắc trong nhiều hướng khác nhau của toán học, vật lý học,…đặc biệt bài toán logarit rời rạc là cơ sở để xây dựng hệ mã khóa công khai. Đây là dạng bài toán một chiều: bài toán lấy lũy thừa có thể tính toán hiệu quả theo thuật toán bình phương và nhân, song bài toán ngược tìm số mũ thì lại không dễ như vậy.

Đề tài này nhằm nghiên cứu về bài toán logarit rời rạc và tìm hiểu ứng dụng của nó trong một vài hệ mã công khai: hệ mã RSA, hệ mã Elgamal, chữ kí Elgamal và hệ mã đường cong Elliptic.

Luận văn được trình bày trong 2 chương ngoài phần mởp đầu và kết luận.

Chương 1 gồm những kiến thức cơ sở để nhằm phục vụ cho chương 2, bao gồm những kiến thức liên quan về về hệ mật mã, hệ mã công khai và bài toán logarit rời rạc.

Chương 2 tác giả trình bày những kiến thức cơ bản về hệ mã RSA, hệ mã Elgamal, chữ kí điện tử Ellgamal, hệ mã đường cong Elliptic. Chương này cũng trình bày một số ví dụ cụ thể để minh họa.

Mặc dù đã có nhiều cố gắng, song luận văn mới chỉ dừng ở mức trình bày hệ thống các kiến thức như trên và tính toán trên một số ví dụ cụ thể, phần ứng dụng thực tế còn hạn chế.

CHƯƠNG I : KIẾN THỨC CƠ SỞ

Chương 1 trình bày những kiến thức cơ sở khái quát về mật mã, khái niệm về hệ mật mã, hệ mã công khai, bài toán lôgarit rời rạc và một số thuật toán lôgarit rời rạc. Những kiến thức trình bày trong chương này được trích dẫn ở tài liệu sau: Mã hoá thông tin: Cơ sở toán học và ứng dụng - Phạm Huy Điển, Hà Huy Khoái (2003) - NXB Đại Học Quốc Gia, Lý thuyết mật mã và an toàn thông tin - Phan Đình Diệu (2002) - NXB Đại Học Quốc Gia Hà Nội, Giáo trình an toàn dữ liệu – Khoa công nghệ thông tin - Trịnh Nhật Tiến - NXB Đại Học Quốc Gia Hà Nội.

1.1. KHÁI QUÁT VỀ MẬT MÃ, MÃ CÔNG KHAI

1.1.1. Khái quát về mật mã

1.1.1.1. Giới thiệu

Mật mã đã được con người sử dụng từ lâu đời. Các hình thức mật mã sơ khai đã được tìm thấy từ khoảng bốn nghìn năm trước trong nền văn minh Ai Cập cổ đại. Trải qua hàng nghìn năm lịch sử, mật mã đã được sử dụng rộng rãi ở khắp nơi trên thế giới từ Đông sang Tây để giữ bí mật cho việc giao lưu thông tin trong nhiều lĩnh vực hoạt động giữa con người và các quốc gia, đặc biệt trong các lĩnh vực quân sự, chính trị, ngoại giao. Mật mã trước hết là một loại hoạt động thực tiễn, nội dung chính của nó là để giữ bí mật thông tin. Ví dụ muốn gửi một văn bản từ một người gửi A đến một người nhận B, A phải tạo cho văn bản đó một bản mã mật tương ứng và thay vì gửi văn bản rõ thì A chỉ gửi cho B bản mã mật, B nhận được bản mã mật và khôi phục lại văn bản rõ để hiểu được thông tin mà A muốn gửi cho mình. Do văn bản gửi đi thường được chuyển qua các con đường công khai nên người ngoài có thể "lấy trộm" được, nhưng vì đó là bản mật mã nên không đọc hiểu được. Còn A có thể tạo ra bản mã mật và B có thể giải bản mã mật thành bản rõ để hiểu

được là do hai người đã có một thoả thuận về một chìa khoá chung, chỉ với khoá chung này thì A mới tạo được bản mã mật từ bản rõ và B mới khôi phục được bản rõ từ bản mã mật. Khoá chung đó được gọi là khoá mật mã. Để thực hiện được một phép mật mã, ta còn cần có một thuật toán biến bản rõ cùng với khoá mật mã thành bản mã mật và một thuật toán ngược lại biến bản mật cùng với khoá mật mã thành bản rõ. Các thuật toán đó được gọi tương ứng là thuật toán lập mã và thuật toán giải mã. Các thuật toán này thường không nhất thiết phải giữ bí mật, mà cái luôn cần được giữ bí mật là khoá mật mã. Trong thực tiễn, có những hoạt động ngược lại với hoạt động bảo mật là khám phá bí mật từ các bản mã "lấy trộm" được, hoạt động này thường được gọi là mã thám hay phá khoá.

1.1.1.2. Các khái niệm cơ sở

Mật mã là một lĩnh vực khoa học chuyên nghiên cứu về các phương pháp và kỹ thuật đảm bảo an toàn và bảo mật trong truyền tin liên lạc với giả thiết sự tồn tại của các thế lực thù địch, những kẻ muốn ăn cắp thông tin để lợi dụng và phá hoại. Tên gọi trong tiếng Anh, Cryptology được dẫn giải nguồn gốc từ tiếng Hy lạp, trong đó kryptos nghĩa là "che dấu", logos nghĩa là "từ ngữ". Cụ thể hơn, các nhà nghiên cứu lĩnh vực này quan tâm xây dựng hoặc phân tích (để chỉ ra điểm yếu) các giao thức mật mã (cryptographic protocols), tức là các phương thức giao dịch có đảm bảo mục tiêu an toàn cho các bên tham gia (với giả thiết môi trường có kẻ đối địch, phá hoại).

Ngành Mật mã (cryptology) thường được quan niệm như sự kết hợp của 2 lĩnh vực con:

1. Sinh, chế mã mật (cryptography): nghiên cứu các kỹ thuật toán học nhằm cung cấp các công cụ hay dịch vụ đảm bảo an toàn thông tin.

2. Phá giải mã (cryptanalysis): nghiên cứu các kỹ thuật toán học phục vụ phân tích phá mật mã và hoặc tạo ra các đoạn mã giản nhằm đánh lừa bên

nhận tin. Hai lĩnh vực con này tồn tại như hai mặt đối lập, "đấu tranh để cùng phát triển" của một thể thống nhất là ngành khoa học mật mã (cryptology). Tuy nhiên, do lĩnh vực thứ hai (cryptanalysis) ít được phổ biến quảng đại nên dần dần, cách hiểu chung hiện nay là đánh đồng hai thuật ngữ cryptography và cryptology. Theo thói quen chung này, hai thuật ngữ này có thể dùng thay thế nhau. Thậm chí cryptography là thuật ngữ ưa dùng, phổ biến trong mọi sách vở phổ biến khoa học, còn cryptology thì xuất hiện trong một phạm vi hẹp của các nhà nghiên cứu học thuật thuần túy. Mặc dù trước đây hầu như mật mã và ứng dụng của nó chỉ phổ biến trong giới hẹp, nhưng với sự phát triển vũ bão của công nghệ thông tin và đặc biệt là sự phổ biến của mạng internet, các giao dịch có sử dụng mật mã đã trở nên rất phổ biến. Chẳng hạn, ví dụ điển hình là các giao dịch ngân hàng trực tuyến hầu hết đều được thực hiện qua mật mã. Ngày nay, kiến thức ngành mật mã là cần thiết cho các cơ quan chính phủ, các khối doanh nghiệp và cả cho cá nhân. Một cách khái quát, ta có thể thấy mật mã có các ứng dụng như sau:

- Với các chính phủ: bảo vệ truyền tin mật trong quân sự và ngoại giao, bảo vệ thông tin các lĩnh vực tầm cỡ lợi ích quốc gia.
- Trong các hoạt động kinh tế: bảo vệ các thông tin nhạy cảm trong giao dịch như hồ sơ pháp lý hay y tế, các giao dịch tài chính hay các đánh giá tín dụng…
- Với các cá nhân: bảo vệ các thông tin nhạy cảm, riêng tư trong liên lạc với thế giới qua các giao dịch sử dụng máy tính hoặc kết nối mạng.

1.1.1.3. Khái niệm hệ mật mã

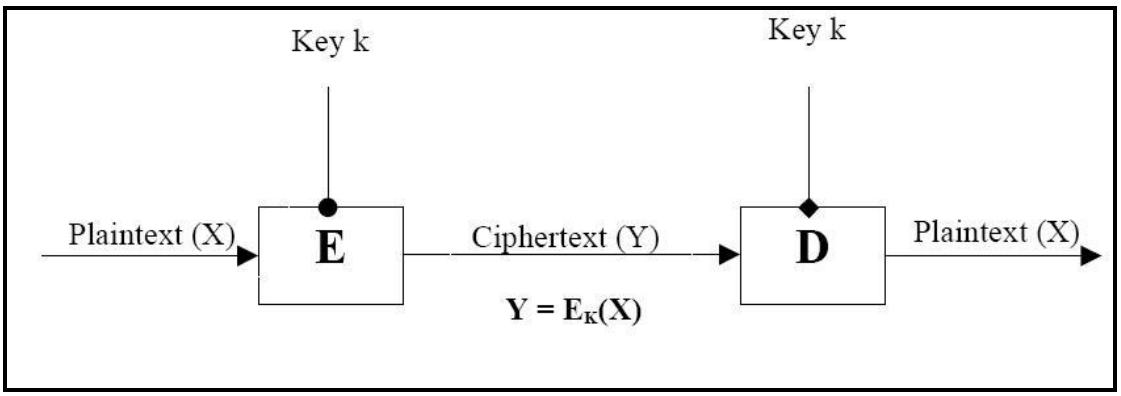
Hệ mật mã được định nghĩa là một bộ năm (P, C, K, E, D), trong đó:

1. P là tập hữu hạn các các bản rõ có thể.
2. C tập hữu hạn các bản mã có thể.
3. K là tập hữu hạn các khoá có thể.

4. E là tập các hàm lập mã.

5. D là tập các hàm giải mã. Với mỗi k ∈ K, có một hàm lập mã $e_k \in E$, $e_k : P \rightarrow C$ và một hàm giải mã $d_k \in D$, $d_k: C \rightarrow P$ sao cho

$d_k(e_k(x)) = x$, $x \in P$



Hình 1.1: Quá trình mã hoá và giải mã

- Một thông báo thường được tổ chức dưới dạng bản rõ.
- Người gửi sẽ làm nhiệm vụ mã hóa bản rõ, kết quả thu được gọi là bản mã.
- Bản mã này được gửi đi trên một đường truyền tới người nhận, sau khi nhận được bản mã người nhận giải mã nó để tìm hiểu nội dung.
- Dễ dàng thấy được công việc trên khi sử dụng định nghĩa hệ mật mã:

$e_k(P) = C$ và $d_k(C) = P$.

1.1.1.4. Những yêu cầu đối với hệ mật mã

Một hệ mật mã phải cung cấp một mức cao về độ tin cậy, tính toàn vẹn, sự không từ chối và sự xác thực.

- Độ tin cậy: cung cấp sự bí mật cho các thông báo và dữ liệu được lưu bằng việc che dấu thông tin sử dụng các kĩ thuật mã hóa.
- Tính toàn vẹn: cung cấp sự bảo đảm với tất cả các bên rằng thông báo còn lại không thay đổi từ khi tạo ra đến khi người nhận mở nó ra.
- Tính không từ chối: có thể cung cấp một cách xác nhận rằng tài liệu đã đến từ ai đó ngay cả khi họ cố gằng từ chối nó.
- Tính xác thực: cung cấp hai dịch vụ:

+ Đầu tiên là nhận dạng nguồn gốc của một thông báo và cung cấp một vài sự bảo đảm rằng nó là đúng sự thật.

+ Thứ hai là kiểm tra đặc tính của người đang trong một hê thống và sau đó tiếp tục kiểm tra đặc tính của họ trong trường hợp ai đó cố gắng đột nhiên kết nối và giả dạng người sử dụng.

1.1.2. Khái quát về hệ mã công khai

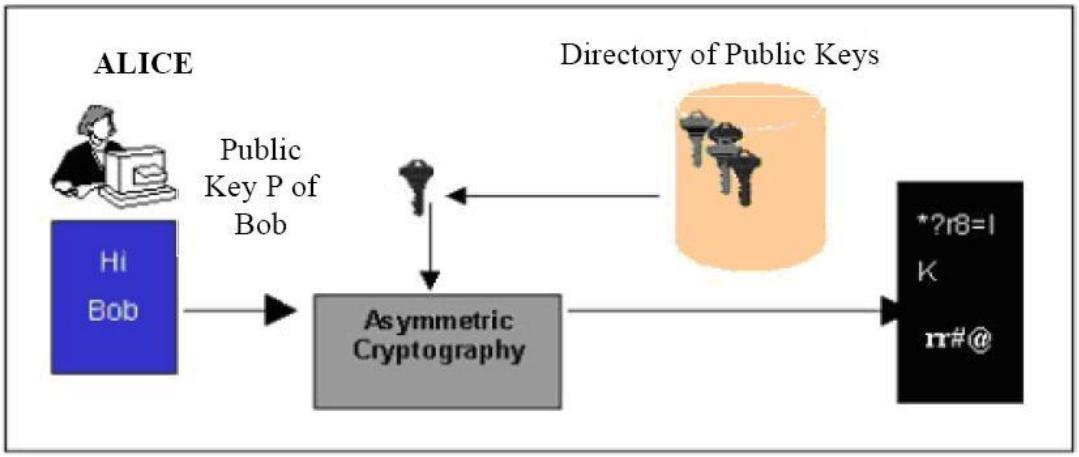
1.1.2.1. Mã đối xứng và mã công khai

Mã đối xứng được dùng để chỉ các hệ mã mà trong đó khi biết khóa lập mã ta có thể tìm được khóa giải mã một cách dễ dàng. Đồng thời việc giải mã cũng đòi hỏi thời gian như việc lập mã. Các hệ mã thuộc loại này có thời gian lập mã và giải mã tương đối nhanh vì thế các hệ mã đối xứng thường được sử dụng để mã hóa những dữ liệu lớn. Nhưng các hệ mã đối xứng yêu cầu phải giữ bí mật hoàn toàn về khóa lập mã.

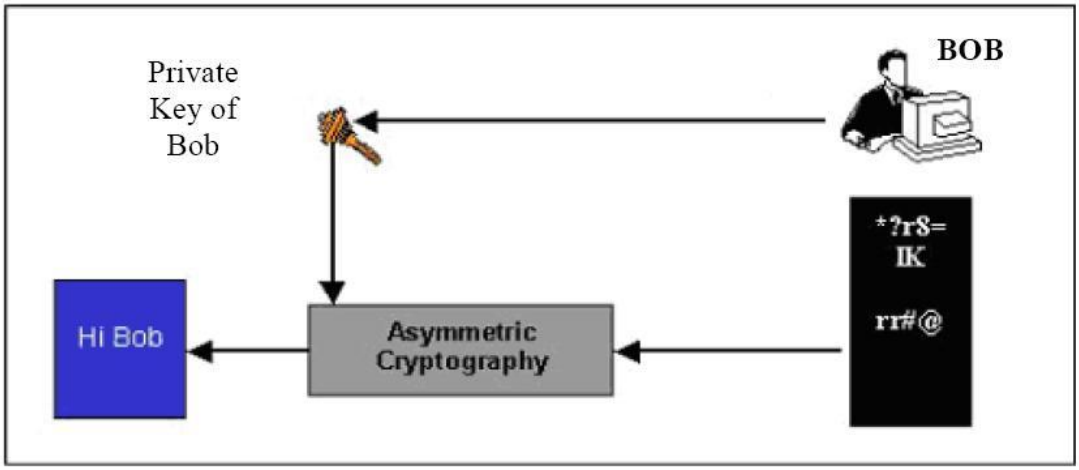
Để giải quyết vấn đề phân phối và thoả thuận khoá của mật mã khoá đối xứng, năm 1976 Diffie và Hellman đã đưa ra khái niệm về hệ mật mã khoá công khai và một phương pháp trao đổi công khai để tạo ra một khoá bí mật chung mà tính an toàn được bảo đảm bởi độ khó của một bài toán toán học cụ thể (là bài toán tính "lôgarit rời rạc"). Hệ mật mã khoá công khai hay còn được gọi là hệ mật mã phi đối xứng sử dụng một cặp khoá, khoá mã hoá còn gọi là khoá công khai (public key) và khoá giải mã được gọi là khoá bí mật hay khóa riêng (private key). Trong hệ mật này, khoá mã hoá khác với khoá giải mã. Về mặt toán học thì từ khoá công khai rất khó tính được khoá riêng. Biết được khoá này không dễ dàng tìm được khoá kia. Khoá giải mã được giữ bí mật trong khi khoá mã hoá được công bố công khai. Một người bất kỳ có thể sử dụng khoá công khai để mã hoá tin tức, nhưng chỉ có người nào có đúng khoá giải mã mới có khả năng xem được bản rõ.

Người gửi A sẽ mã hoá thông điệp bằng khóa công khai của người nhận B và người nhận B sẽ giải mã thông điệp với khoá riêng tương ứng của mình.

Quá trình này được mô tả trong hình 1.2 và 1.3.



Hình 1.2: Mã hoá thông điệp sử dụng khoá công khai P



Hình 1.3: Giải mã thông điệp sử dụng khoá riêng của người nhận

Có nhiều hệ thống khoá công khai được triển khai rộng rãi như hệ RSA, hệ Elgamal sử dụng giao thức trao đổi khoá Diffie-Hellman và nổi lên trong những năm gần đây là hệ mã đường cong Elliptic. Trong số các hệ mật mã trên thì hệ RSA là hệ được cộng đồng chuẩn quốc tế và công nghiệp chấp nhận rộng rãi trong việc thực thi mật mã khoá công khai.

Việc phát minh ra phương pháp mã công khai tạo ra một cuộc "cách mạng" trong công nghệ an toàn thông tin điện tử. Nhưng thực tiễn triển khai