HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

PHAN ĐỨC TUÂN

NGHIÊN CỨU HỆ MẬT ELGAMAL TRÊN TRƯỜNG ĐA THỨC

LUẬN VĂN THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

HÀ NỘI - 2020

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

PHAN ĐỨC TUÂN

NGHIÊN CỨU HỆ MẬT ELGAMAL TRÊN TRƯỜNG ĐA THỨC

CHUYÊN NGÀNH : **HỆ THỐNG THÔNG TIN**

MÃ SỐ: **8.48.01.04**

LUẬN VĂN THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

NGƯỜI HƯỚNG DẪN KHOA HỌC: GS. NGUYỄN BÌNH

HÀ NỘI - 2020

LỜI CẢM ƠN

Lời đầu tiên, tôi xin gửi lời cảm ơn sâu sắc nhất đến thầy GS. Nguyễn Bình, đã tận tâm, tận lực hướng dẫn, định hướng cho tôi, đồng thời cũng đã cung cấp nhiều tài liệu và tạo điều kiện thuận lợi trong suốt quá trình học tập và nghiên cứu để tôi hoàn thành luận văn này.

Tôi xin chân thành cảm ơn đến các thầy, cô bộ môn trong khoa Hệ Thống Thông Tin, Học Viện Bưu Chính Viễn Thông cùng với lãnh đạo nhà trường đã nhiệt tình giảng dạy và truyền đạt những kiến thức, kinh nghiệm quý giá trong suốt quá trình học tập và rèn luyện tại trường.

Do kiến thức và thời gian có hạn nên luận văn sẽ không tránh khỏi những thiếu sót nhất định. Tôi rất mong nhận được những sự góp ý quý báu của thầy cô, đồng nghiệp và bạn bè.

Xin chân thành cảm ơn!.

Hà Nội, ngày 15 tháng 05 năm 2020

Học viên thực hiện

Phan Đức Tuân

LỜI CAM ĐOAN

Tôi xin cam kết các kết quả đạt được trong luận văn "**Nghiên cứu hệ mật ElGamal trên trường đa thức**" do tôi thực hiện dưới sự hướng dẫn của **GS. Nguyễn Bình.**

Trong toàn bộ nội dung nghiên cứu luận văn, các vấn đề được trình bày đều là những tìm hiểu và nghiên cứu của cá nhân tôi hoặc là trích dẫn các nguồn tài liệu và một số trang web đều được đưa ra ở phần Tài liệu tham khảo.

Tôi xin cam đoan những lời trên là sự thật và chịu mọi trách nhiệm trước thầy cô và hội đồng bảo vệ luận văn thạc sĩ .

Hà Nội, ngày 15 tháng 05 năm 2020

Học viên thực hiện

Phan Đức Tuân

MỤC LỤC

DANH MỤC THUẬT NGỮ, CHỮ VIẾT TẮT

STT	Từ viết tắt	Tiếng Anh	Tiếng Việt
1	AES	Advanced Encryption Standard	Chuẩn mã hóa dữ liệu dạng khối
2	DES	Data Encryption Standard	Chuẩn mã hóa dữ liệu
3	F	Field	Trường
4	G	Group	Nhóm
5	GF	Galois Field	Trường Galois
6	ID		Chỉ danh người dùng trên mạng
7	R	Ring	Vành
8	RSA	Rivest, Shamir and Adlenman	Giải thuật mã hóa khóa công khai
9	UCLN	Gcd	Ước chung lớn nhất
10	Z		Tập số nguyên

DANH MỤC CÁC BẢNG BIỂU

DANH MỤC HÌNH VẼ

MỞ ĐẦU

1. Tính cấp thiết của đề tài

Cùng với sự phát triển của công nghệ thông tin và truyền thông, mạng máy tính đang trở thành một phương tiện điều hành thiết yếu trong mọi lĩnh vực hoạt động của xã hội. Việc trao đổi thông tin và dữ liệu trong môi trường mạng ngày càng trở lên phổ biến và đang dần thay thế các phương thức truyền tin trực tiếp. Khi ngày càng nhiều thông tin được trao đổi thì nhu cầu về bảo mật thông tin được đặt ra trong nhiều ngành và nhiều lĩnh vực. Các tài liệu, văn bản đều được mã hóa và xử lý trên máy tính truyền đi trong môi trường mạng internet là không an toàn. Do đó yêu cầu có một cơ chế, giải pháp để bảo vệ sự an toàn và bí mật của thông tin ngày càng cần thiết và không thể thiếu. Mật mã học chính là ngành khoa học để giải quyết vấn đề này. Hầu như mọi ứng dụng đều sử dụng các thuật toán mã hóa thông tin.

Hệ mật mã ra đời nhằm đảm bảo các dịch vụ an toàn cơ bản trên như: hệ mật mã với khóa sở hữu riêng (Private Key Cryptosystems), hệ mã với khóa bí mật (Secret Key Cryptosystem), hệ mã hóa truyền thống (Conventional Cryptosystem) đều là những hệ mật mã sử dụng mã hóa khóa đối xứng, hệ mật mã hóa khóa công khai. Hệ mật mã khóa công khai cho phép người sử dụng trao đổi các thông tin mà không cần trao đổi khóa chung bí mật. Hệ mã hóa khóa công khai thiết kế sao cho khóa giải mã khác với khóa mã hóa và ngược lại. Tức là hai khóa này có quan hệ với nhau về toán học nhưng không thể suy diễn được ra nhau. Một trong những thuật toán mã hóa khóa công khai được phát triển dựa trên Hệ mật mã ElGamal cho phép giải quyết các yêu cầu bảo mật thông tin, đồng thời việc xác thực về nguồn gốc và tính toàn vẹn của thông tin. Luận văn sẽ trình bày về hệ mật ElGamal trên trường đa thức. Giải quyết bài toán hệ ElGamal trên vành đa thức với hai lũy đẳng nguyên thủy.

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 nhằm nghiên cứu về bài toán Logarit rời rạc và ứng dụng giải quyết bài toán hệ mật ElGamal trên vành đa thức với hai lũy đẳng nguyên thủy.

2. Mục tiêu, đối tượng, phạm vi và phương pháp nghiên cứu

Mục tiêu nghiên cứu: Tìm hiểu bài toán Logarit rời rạc và hoạt động của hệ mật ElGamal. Tìm hiểu hệ mật ElGamal trên trường đa thức

Đối tượng và phạm vi nghiên cứu: Hệ mật ElGamal là đối tượng nghiên cứu của đề tài. Từ đó sẽ xây dựng hệ mật ElGamal trên vành đa thức với hai lũy đẳng nguyên thủy

Phương pháp nghiên cứu

** Phương pháp lý thuyết*

- Tìm hiểu nghiên cứu về mật mã, cơ sở toán học

- Tìm hiểu bài bài toán Logarit rời rạc và hệ mật ElGamal, thủ tục trao đổi khóa Diffie-Hellman, phương pháp che dấu dữ liệu

- Lý thuyết chung về hệ mật khóa công khai từ đó đưa ra phương pháp che dấu dữ liệu mới của hệ mật ElGamal

** Phương pháp thực nghiệm*

- Hệ mật vẫn giữ nguyên cấu trúc trao đổi khóa Diffie-Hellman.

- Trình bày kiểu che dấu dữ liệu theo phương pháp nhân và phương pháp cộng của hệ mật ElGamal.

3. Cấu trúc luận văn

Luận văn được tác giả trình bày 3 chương có phần mở đầu, danh mục từ viết tắt, phần kết luận, mục lục, phần tài liệu tham khảo. Các nội dung cơ bản của luận văn được trình bày theo cấu trúc như sau:

Chương 1: Kiến thức cơ sở

Trong chương này, luận văn trình bày khái quát về mật mã học, các khái niệm trong toán học mà các hệ mã hóa thường sử dụng như modulo, nhóm, vành , trường.

Chương 2: Bài toán Logarit rời rạc

Tập trung nghiên cứu về bài toán Logarit rời rạc như bài toán Logarit trên trường hữu hạn , trường số thực, các phương pháp giải bài toán Logarit rời rạc .

Chương 3: Hệ mật ElGamal trên trường đa thức

Tập trung nghiên cứu hệ mật ElGamal cổ điển và đưa ra đánh giá của hệ mật, xây dựng hệ mật ElGamal trên trường đa thức, giải bài toán hệ mật ElGamal trên vành đa thức với hai lũy đẳng nguyên thủy.

CHƯƠNG 1. KIẾN THỨC CƠ SỞ

1.1. Khái quát về mật mã học

1.1.1. Giới thiệu về mật mã học

Mật mã học là ngành khoa học ứng dụng toán học vào việc biến đổi thông tin thành một dạng khác với mục đích che dấu nội dung, ý nghĩa thông tin cần mã hóa. Đây là một ngành quan trọng và có nhiều ứng dụng trong đời sống xã hội. Ngày nay, các ứng dụng mã hóa và bảo mật thông tin đang được sử dụng ngày càng phổ biến hơn trong các lĩnh vực khác nhau trên thế giới, từ các lĩnh vực an ninh, quân sự, quốc phòng…, cho đến các lĩnh vực dân sự như thương mại điện tử, ngân hàng…

Cùng với sự phát triển của khoa học máy tính và Internet, các nghiên cứu và ứng dụng của khoa học mật mã ngày càng trở nên đa dạng hơn, mở ra nhiều hướng nghiên cứu chuyên sâu vào từng lĩnh vực ứng dụng đặc thù với những đặc trưng riêng. Ứng dụng của khoa học mật mã không chỉ đơn thuần là mã hóa và giải mã thông tin mà còn bao gồm nhiều vấn đề khác nhau cần được nghiên cứu và giải quyết: chứng thực nguồn gốc nội dung thông tin (kỹ thuật chữ ký điện tử), chứng nhận tính xác thực về người sở hữu mã khóa (chứng nhận khóa công cộng), các quy trình giúp trao đổi thông tin và thực hiện giao dịch điện tử an toàn trên mạng... Những kết quả nghiên cứu về mật mã cũng đã được đưa vào trong các hệ thống phức tạp hơn, kết hợp với những kỹ thuật khác để đáp ứng yêu cầu đa dạng của các hệ thống ứng dụng khác nhau trong thực tế, ví dụ như hệ thống bỏ phiếu bầu cử qua mạng, hệ thống đào tạo từ xa, hệ thống quản lý an ninh của các đơn vị với hướng tiếp cận sinh trắc học, hệ thống cung cấp dịch vụ multimedia trên mạng với yêu cầu cung cấp dịch vụ và bảo vệ bản quyền sở hữu trí tuệ đối với thông tin số...

1.1.2. Vấn đề về mã hóa

Mật mã học là một lĩnh vực liên quan với các kỹ thuật ngôn ngữ và toán học để

đảm bảo an toàn thông tin, cụ thể là trong thông tin liên lạc.

Hiện nay có nhiều kĩ thuật mật mã khác nhau, mỗi kĩ thuật có ưu và nhược điểm riêng. Tùy theo yêu cầu của môi trường ứng dụng ta dùng kĩ thuật này hay kĩ thuật khác.

Mật mã cổ điển chủ yếu dùng để che dấu dữ liệu. Với mật mã hiện đại ngoài khả năng che dấu dữ liệu, còn dùng để thực hiện: Ký số, tạo giao diện thông điệp, giao thức bảo toàn dữ liệu, xác thực thực tế….

Theo nghĩa hẹp, mật mã dùng để bảo mật dữ liệu, người ta quan niệm: Mật mã học là môn khoa học nghiên cứu mật mã: tạo mã và phân tích mã (thám mã).

Mật mã đảm bảo những tính chất sau:

- Tính bí mật (Bảo mật): Thông tin không bị lộ đối với người không được phép nhận
- Tính toàn vẹn (Bảo toàn): Ngăn chặn hay hạn chế việc bổ sung, loại bỏ và sửa chữa dữ liệu không được phép.
- Tính xác thực (Chứng thực): Xác thực đúng thực thể cần kết nối, giao dịch. Xác thực đúng thực thể có trách nhiệm về nội dung thông tin.
- Tính sẵn sàng: Thông tin sẵn sàng cho người dùng hợp pháp.

Thám mã (phá mã) là tìm những điểm yếu hoặc không an toàn trong phương thức mật mã hóa. Thám mã có thể được thực hiện bởi những kẻ tấn công, nhằm làm hỏng hệ thống, hoặc bởi những người thiết kế ra hệ thống (hoặc những người khác) với ý định đánh giá độ an toàn của hệ thống.

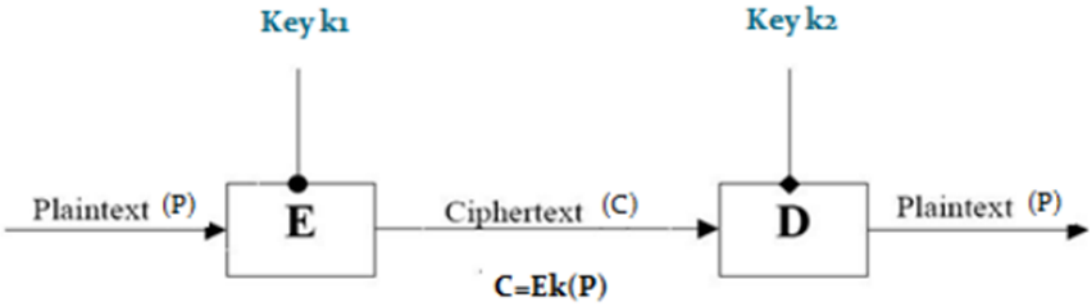
Hệ mã hóa là dùng một quy tắc nhất định để mã hóa thông tin. Hệ mã hóa được định nghĩa là một bộ năm thành phần (P,C,K,E,D) thỏa mãn các tính chất sau:

- P (Plaintext) là tập hợp hữu hạn các bản rõ có thể.
- C (Ciphertext) là tập hợp hữu hạn các bản mã có thể.
- K (Key) là tập hợp các bản khóa có thể.
- E (Encrytion) là tập hợp các quy tắc mã hóa có thể.

- D (Decrytion) là tập hợp các quy tắc giải mã có thể.

Quá trình mã hóa được tiến hành bằng cách áp dụng hàm toán học E lên thông tin P (được biểu diễn dưới dạng số) để trở thành thông tin đã mã hóa C.

Quá trình giải mã được tiến hành ngược lại: áp dụng hàm D lên thông tin C để được thông tin đã giải mã.



Hình 1. Quá trình mã hóa và giải mã

Có hai loại mã hóa: Mã hóa khóa đối xứng và mã hóa khóa bất đối xứng

Hệ mật mã đối xứng (hay còn gọi là mật mã khóa bí mật): là những hệ mật dùng chung một khóa cả trong quá trình mã hóa dữ liệu và giải mã dữ liệu. Do đó khóa phải được giữ bí mật tuyệt đối. Một số thuật toán nổi tiếng trong mã hóa đối xứng là DES, Triple DES (3DES), AES …

Hệ mật mã bất đối xứng (hay còn gọi là mật mã khóa công khai): Các hệ mật này dụng chung một khóa để mã hóa sau đó dùng một khóa khác để giải mã, nghĩa là khóa để mã hóa và giải mã là khác nhau. Các khóa này tạo nên từng cặp chuyển đổi ngược nhau và không có khóa nào có thể suy được từ khóa kia. Khóa dùng để mã hóa có thể công khai nhưng khóa dùng để giải mã phải giữ bí mật. Do đó trong thuật toán này có hai loại khóa: Khóa để mã hóa được gọi là khóa công khai – Public Key, khóa để giải mã được gọi là khóa bí mật – Private Key. Một số thuật toán mã hóa công khai nổi tiếng: Diffle-Hellman, RSA, ElGamal,…

Trong mô hình mật mã cổ điển mà cho tới nay vẫn còn được nghiên cứu Alice (người gửi) và Bob (người nhận) bằng cách chọn một khóa bí mật K. Sau đó Alice dùng khóa K để mã hóa theo luật e_k và Bod dùng chung khóa K đó để giải mã theo

luật giải d_k. Trong hệ mật này d_k hoặc e_k dễ dàng nhận được vì quá trình giải mã tương tự như quá trình mã hóa nhưng thủ tục khóa thì ngược lại. Nhược điểm lớn của hệ mật này là nếu để lộ e_k thì làm cho hệ thống mất an toàn, chính vì vậy chúng ta cần tạo ra cho hệ mật này một kênh an toàn. Ý tưởng xây dựng một hệ mật khóa công khai là tìm ra một hệ mật có khả năng tính toán được d_k khi biết được e_k. Khi Alice (người gửi) chuyển bản tin cho Bob (người nhận) thì chỉ có duy nhất Bob mới có thể giải được bản tin này bằng cách sử dụng luật giải mã bí mật d_k.

Để giải quyết vấn đề phân phối và thỏa thuận khóa, năm 1976 Diffie và Hellman đã đưa ra khái niệm về hệ mật mã khóa công khai và phương pháp trao đổi công khai để tạo ra một khóa bí mật chung. Tính an toàn của hệ mật được đảm bảo bởi độ khó một bài toán học cụ thể (bài toán Logarit rời rạc). Hệ mật mã khóa công khai còn được gọi là hệ mật mã phi đối xứng sử dụng một cặp khóa: khóa công khai(public key) và khóa bí mật(private key). Khóa công khai dùng để mã hóa còn khóa bí mật dùng để giải mã.

Mật mã hóa khóa công khai là một dạng mật mã hóa cho phép người sử dụng trao đổi các thông tin mật mà không cần phải trao đổi các khóa chung bí mật trước đó, 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). Trong mật mã hóa khóa công khai, khóa cá nhân phải được giữ bí mật trong khi khóa công khai được phổ biến công khai. Trong hai khóa, một dùng để mã hóa và khóa còn lại dùng để giải mã. Điều quan trọng đối với hệ thống là không thể tìm ra khóa bí mật nếu chỉ biết khóa công khai. Hệ thống mật mã hóa khóa công khai có thể sử dụng với các mục đích: Mã hóa, tạo Chữ ký số, Thỏa thuận khóa, cho phép thiết lập khóa dùng để trao đổi thông tin mật giữa hai bên. Các kỹ thuật mật mã hóa khóa công khai đòi hỏi khối lượng tính toán nhiều hơn các kỹ thuật mã hóa khóa đối xứng nhưng có nhiều ưu điểm nên được áp dụng trong nhiều ứng dụng.

1.2. Cơ sở toán học

1.2.1. Modulo số học

Modulo số học đã và đang dần trở lên quan trọng trong lĩnh vực mật mã. Lý thuyết modulo số học được sử dụng trong các thuật toán mã hóa khóa công khai như thuật toán RSA và Diffie-Hellman, các thuật toán khóa đối xứng như AES, DES. Ưu điểm chính của việc sử dụng modulo số học là nó cho phép chúng ta thực hiện phép nhân nhanh hơn. Ví dụ với phép toán phức tạp, việc tính toán đa thức đó (nhân đa thức) với một lượng số nguyên lớn thì việc sử dụng modulo số học sẽ làm giảm thời gian tính toán của phép toán lớn này. Áp dụng vào ứng dụng sửa mã lỗi, bằng việc sử dụng lý thuyết modulo số học mỗi chữ số của mã được liên kết đến các phần tử của trường hữu hạn.

Toán tử modulo (mod n) ánh xạ tới tất cả các số nguyên trong tập {0, 1, 2, ….,(n-1)} và tất cả các phép toán số học được thực thi trong tập hợp này. Kỹ thuật này được gọi là modulo số học.

Tập các số nguyên và các số nguyên khác 0 của mod n được ký hiệu bởi Z_n và Z^*_n.

Ví dụ: Cộng và nhân modulo trên modulo 23

Giả sử, 12 + 20 = (12 + 20) mod 23 = 32 mod 23 = 9 vì 32 chia cho 23 dư 9

Tương tự phép nhân, 8x9 = 72 mod 23 = 3, vì 72 chia cho 23 dư 3

1.2.2. Nhóm, vành và trường

Trong đại số trừu tượng, chúng ta làm việc với các tập mà các phần tử được thao tác một cách đại số. Ví dụ, chúng ta có thể nói rằng bằng cách kết hợp hai phần tử của một tập theo nhiều cách khác nhau, ta có thể tạo ra được phần tử thứ ba của tập hợp. Tất cả các phép toán sẽ tuân theo một số quy tắc cụ thể được định nghĩa trong tập. Một số định nghĩa:

Nhóm:

Một nhóm ký hiệu là {G, •}, là một tập G các phần tử và một phép kết hợp 2 ngôi • thỏa mãn các điều kiện sau:

+ Tính đóng: $\forall a,b \in G: a \bullet b \in G$
+ Tính kết hợp: $\forall a,b \in G: (a \bullet b) \bullet c = a \bullet (b \bullet c)$
+ Phần tử đơn vị: $\exists e \in G: a \bullet e = e \bullet a = a, \forall a \in G$
+ Phần tử nghịch đảo: $\forall a \in G, \exists! a' \in G: a \bullet a' = a' \bullet a = e$

Ví dụ: Tập số nguyên Z và phép cộng số nguyên là một nhóm. Phần tử đơn vị là 0. Với a ∈ Z thì nghịch đảo của a là –a. Tập Z có vô hạn phần tử nên nhóm này được gọi là nhóm vô hạn.

+ Tính giao hoán : $\forall a,b \in G : a \bullet b = b \bullet a$

Một nhóm được gọi là cyclic nếu có 1 hoặc nhiều phần tử mà có thể sinh ra tất cả các phần tử trong nhóm, hay có nói cách khác: $\exists g \in G, \forall a \in G, \exists k, a=g^k$

Ví dụ: p là số nguyên tố và (Z^*_p, x) là nhóm cyclic.

Nhóm cyclic (Z^*_7, x) với p = 7, số phần tử của nhóm là 6. Ta có, phần tử 3 và 5 là phần tử sinh của nhóm $Z^*_7 = \{1,2,3,4,5,6\}$ các lũy thừa của 3 modulo 7 là :

$1 = 3^6, 2 = 3^2, 3 = 3^1, 4 = 3^4, 5 = 3^5, 6 = 3^3$

Vành :

Một vành R, ký hiệu {R, + , x} là một tập các phần tử và hai phép kết hợp 2 ngôi, gọi là phép cộng và phép nhân, nếu các tính chấy sau được thỏa mãn:

+ R là một nhóm giao hoán theo phép cộng
+ Tính đóng đối với phép nhân: $\forall a,b \in R : ab \in R$ (viết tắt thay cho dấu x)
+ Tính kết hợp đối với phép nhân: $\forall a,b,c \in R\ (ab)c = a(bc)$
+ Tính phân phối giữa phép cộng và phép nhân: $\forall a,b,c \in R$

$$(a + b)c = ac + bc$$

$$a(b + c) = ab + ac$$

Tóm lại, trong một vành, chúng ta có thể thực hiện các phép cộng trừ, nhân mà không ra khỏi vành (kết quả các phép toán cộng, trừ, nhân thuộc R)

Một vành được gọi là vành giao hoán nếu có thêm tính giao hoán đối với phép nhân:

+ Tính giao hoán với phép nhân: $\forall a,b \in R: ab = ba$

Một vành được gọi là miền nguyên(integral domain) nếu đó là vành giao hoán và có thêm hai tính chất sau:

+ Tồn tại phần tử đơn vị phép nhân: $a1 = 1a = a$
+ Liên quan giữa phép nhân và phần tử đơn vị phép cộng:

Nếu $ab = 0$ thì $a = 0$ hay $b = 0$

Trường:

Một trường, ký hiệu {F, + , x} là một tập các phần tử và hai phép kết hợp 2 ngôi, gọi là phép cộng và phép nhân, nếu các tính chất sau được thỏa mãn:

+ F là một miền nguyên (thỏa mãn các tính chất trên của nhóm và vành)
+ Tồn tại phần tử nghịch đảo của phép nhân:

$$\forall a \in F \; a \neq 0 \; \exists a^{-1} \in F: aa^{-1} = 1$$

Ngắn gọn, trong một trường, chúng ta có thể thực hiện các phép cộng, trừ nhân chia mà không ra khỏi trường. Định nghĩa phép chia là $a/b = a(b^{-1})$

1.2.3. Trường hữu hạn GF(p)

Dựa vào phép toán modulo, chúng ta xây dựng một tập Z_n như sau:

Cho một số nguyên n: $Z_n = \{0,1,2 \ldots\ldots, n-1\}$

Tương tự tập số nguyên Z, trên tập Z_n ta định nghĩa các phép cộng và nhân như sau: $\forall a,b,c \in Z_n$

+ Phép cộng: $c = a + b$ => phép cộng trong số học thường

Nếu $c \equiv (a + b) \bmod n$ => phép cộng trong Z_n

+ Phép nhân: c = a.b nếu c ≡ (a.b) mod n

Dễ thấy rằng tập Z_n cùng với phép cộng trên thõa mãn các tính chất của một nhóm giao hoán với phần tử đơn vị của phép cộng là 0

Bên cạnh đó, tập Z_n cùng với phép cộng và phép nhân trên thỏa mãn các tính chất của một miền nguyên với phần tử đơn vị của phép nhân là 1

Ví dụ: Với n = 7 thì phép nhân và phép cộng là như sau:

Bảng 1: Bảng phép cộng và phép nhân trên Z_7

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

x	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Tuy nhiên không phải tập Z_n nào cũng thỏa mãn tính chất mọi phần tử khác 0 của Z_n phải có phần tử nghịch đảo của phép nhân. Chỉ có với những n là số nguyên tố thì Z_n mới thỏa mãn tính chất phần tử nghịch đảo. Ví dụ với n = 8 thì không thỏa mãn và n = 7 thì thỏa mãn.

Ta dùng thuật toán Euclid mở rộng để tìm phần tử nghịch đảo phép nhân trong tập Z_n.

Như vậy với n là số nguyên tố thì tập Z_n trở thành một trường hữu hạn mà ta gọi là trường Galois. Ký hiệu Z_n thành Z_p với p là số nguyên tố. Ký hiệu trường hữu hạn trên là GF(p).

1.2.4. Số học đa thức và trường hữu hạn GF(2^n)

1.2.4.1. Phép toán đa thức thông thường

Trong đại số, chúng ta định nghĩa một đa thức bậc n ($n \geq 0$) dưới dạng

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$$

Trong đó $a_i \in R$, $a_n \neq 0$ được gọi là các hệ số. và ta cũng định nghĩa các phép cộng, trừ nhân đa thức như sau:

Cho $f(x) = \sum_{i=0}^{n} a_i x^i$ $\quad$ $g(x) = \sum_{i=0}^{n} b_i x^i$

+ Phép cộng: $f(x) + g(x) = \sum_{i=0}^{\max(m,n)} (a_i + b_i) x^i$
+ Phép nhân : $f(x) \times g(x) = \sum_{i=0}^{m+n} c_i x^i$ với $c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_k$
+ Phép trừ $f(x) - g(x) = \sum_{i=0}^{m+n} (a_i - b_i) x^i$

Trong 3 phép toán trên ta giả định $a_i = 0$ *nếu* $i > n$ *và* $b_i = 0$ *nếu* $i > m$

Phép chia đa thức f(x) cho g(x) cũng tương tự như phép chia số nguyên gồm một đa thức thương q(x) và một đa thức dư r(x). r(x) có bậc nhỏ hơn g(x)

$$\frac{f(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)}$$

$$f(x) = q(x) \times g(x) + r(x)$$

Ví dụ : $f(x) = x^3 + x^2 + 2$, $\quad g(x) = x^2 - 2x + 2$

- $f(x) + g(x) = x^3 + 2x^2 - x + 3$
- $f(x) - g(x) = x^3 + x + 1$
- $f(x) \times g(x) = x^5 + 3x^2 - 2x + 2$

- $f(x)/g(x)$: đa thức phần thương $q(x) = x + 2$ và đa thức phần dư $r(x) = x$

Với các phép toán cộng và nhân như trên thì tập các đa thức (mỗi đa thức là một phần tử của tập) tạo thành một vành, với phần tử đơn vị của phép cộng là đa thức e(x) = 0 và phần tử đơn vị của phép nhân là đa thức d(x) = 1

Tuy nhiên tập các đa thức trên không tạo thành một trường vì không tồn tại phần nghịch đảo của phép nhân.

+ Đa thức trên tập Z_p

Xem xét tập các đa thức W_p có hệ số thuộc trường Z_p.

$$W_p = \left\{ f(x) = \sum_{i=0}^{n} a_i x^i \quad với\ n \geq 0, a_i \in Z_p, a_n \neq 0 \right\}$$

Trên tập W_p ta định nghĩa các phép cộng trừ, nhân, chia như sau :

$$f(x) = \sum_{i=0}^{n} a_i x^i \qquad g(x) = \sum_{i=0}^{m} b_i x^i$$

+ Phép cộng : $f(x) + g(x) = \sum_{i=0}^{\max(m,n)} (a_i + b_i) x^i$
+ Phép nhân : $f(x) \times g(x) = \sum_{i=0}^{m+n} c_i x^i$ với $c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_k$
+ Phép trừ : $f(x) - g(x) = \sum_{i=0}^{m+n} (a_i - b_i) x^i$
+ Phép chia : $f(x) / g(x)$ *có đa thức thương là q(x) và đa thức dư là r(x)*

Trong đó các phép toán $a_i + b_i,\ a_i b_i, a_i - b_i, a_i / b_i$ được định nghĩa trong tập Z_p

Ví dụ : Xét trường $Z_2 = \{0,1\}$

$$f(x) = x^7 + x^5 + x^4 + x^3 + x + 1\,,\ g(x) = x^3 + x + 1$$

- $f(x) + g(x) = x^7 + x^5 + x^4$
- $f(x) - g(x) = x^7 + x^5 + x^4$

- $f(x) \times g(x) = x^{10} + x^4 + x^2 + 1$
- $f(x)/g(x) = q(x) = x^4 + 1$ và $r(x) = 0$

Trong ví dụ trên có thể xem g(x) và q(x) là đa thức ước số của đa thức f(x). f(x)= g(x).q(x). Những đa thức f(x) như vậy được gọi là đa thức không tối giản. Đa thức tối giản là đa thức chỉ có ước số là đa thức 1 và chính nó (khái niệm tối giản tương tự như khái niệm số nguyên tố trong tập số tự nhiên)

Ví dụ (Xét trường Z_2)

- $x^3 + x + 1$ là đa thức tối giản
- $x^4 + 1$ không phải là đa thức tối giản vì $x^4 + 1 = (x + 1)(x^3 + x^2 + x + 1)$

Tương tự như khái niệm ước số chung lớn nhất của 2 số tự nhiên, chúng ta cũng có khái niệm ước số chung lớn nhất của 2 đa thức. Khái niệm lớn ở đây là bậc lớn, ví dụ $x^3 + 1$ lớn hơn $x^2 + x + 1$

Ví dụ : Xét trong trường Z_2, USCLN của hai đa thức $a(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ và $b(x) = x^4 + x^2 + x + 1$ là $c(x) = x^3 + x^2 + 1$

Tương tự như để tìm USCLN của hai số nguyên, chúng ta có thể sửa đổi thuật toán Euclid để tìm USCLN của hai đa thức

```
/**Thuật toán Euclid tính gcd (a(x), b(x))**/
EUCLID (a(x), b(x))
A(x) = a(x); B(x) = b(x);
While B(x) <> 0 do
R(x) = A(x) mod B(x)
A(x) = B(x);
B(x) = R(x);
End while
Return A(x);
```

1.2.4.2. Trường hữu hạn GF(2^n)

Tương tự như việc xây dựng tập Z_p dùng phép modulo p với p là số nguyên tố, trong phần này ta sẽ xây dựng một tập W_{pm} các đa thức dùng phép modulo đa thức.

Chọn một đa thức m(x) là đa thức tối giản trên Z_p có bậc là n. Tập W_{pm} bao gồm các đa thức trên Z_p có bậc nhỏ hơn n. Như vậy các đa thức thuộc W_{pm} có dạng.

$$f(x) = \sum_{i=0}^{n-1} a_i x^i \; với \; a_i \in Z_p = \{0,1,2 \ldots., p-1\}$$

Tập W_{pm} có p^n phần tử

Ví dụ:

p =3, n = 2 tập W_{pm} có 9 phần tử: *{0,1,2,x,x+1,x+2,2x, 2x+1,2x+2}*

p =2, n = 3 tập W_{pm} có 8 phần tử: *{0,1, x,x+1,x^2,x^2 + 1, x^2+x,x^2+x+1}*

Ta định nghĩa lại phép cộng và phép nhân đa thức như sau:

+ phép cộng, tương tự như phép cộng trên W_p
+ phép nhân, cũng tương tự như phép nhân trên W_p và kết quả cuối cùng được modulo với m(x) để bậc của kết quả nhỏ hơn n.

Vì m(x) là đa thức tối giản nên tương tự như số học modulo, các phần tử trong W_{pm} tồn tại phần tử nghịch đảo của phép nhân:

$$\forall f(x) \in W_{pm}, \exists f^{-1}(x) \in W_{pm}: f(x)f^{-1}(x) = 1$$

Do tồn tại phần tử nghịch đảo , nên ta có thể thực hiện được phép chia trong tập W_{pm} như sau: $f(x)/g(x) = f(x)g^{-1}(x)$

Lúc này W_{pm} thỏa mãn các tính chất của một trường hữu hạn và ta ký hiệu trường hữu hạn này là GF(p^n). Trong mã hóa, chúng ta chỉ quan tâm đến p = 2 tức trường đa thức hữu hạn GF(2^n) trên Z_2.

Ví dụ xét GF(2^3) chọn đa thức bất khả quy $m(x) = x^2 + x + 1$, bảng dưới thể hiện phép cộng và phép nhân.

Bảng 2: Phép cộng và phép nhân trên trường hữu hạn với đa thức $x^2 + x + 1$

+	0	1	x	x + 1	x^2	$x^2 + 1$	$x^2 + x$	x^2+x+1
0	0	1	x	x + 1	x^2	$x^2 + 1$	$x^2 + x$	x^2+x+1
1	1	0	x + 1	x	$x^2 + 1$	x^2	x^2+x+1	$x^2 + x$
x	x	x + 1	0	1	$x^2 + x$	x^2+x+1	x^2	$x^2 + 1$
x + 1	x + 1	x	1	0	x^2+x+1	$x^2 + x$	$x^2 + 1$	x^2
x^2	x^2	$x^2 + 1$	$x^2 + x$	x^2+x+1	0	1	x	x + 1
$x^2 + 1$	$x^2 + 1$	x^2	x^2+x+1	$x^2 + x$	1	0	x + 1	x
$x^2 + x$	$x^2 + x$	x^2+x+1	x^2	$x^2 + 1$	x	x + 1	0	1
x^2+x+1	x^2+x+1	$x^2 + x$	$x^2 + 1$	x^2	x + 1	x	1	0

x	0	1	x	x + 1	x^2	$x^2 + 1$	$x^2 + x$	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	x + 1	x^2	$x^2 + 1$	$x^2 + x$	x^2+x+1
x	0	x	x^2	$x^2 + x$	x + 1	1	x^2+x+1	$x^2 + 1$
x + 1	0	x + 1	$x^2 + x$	$x^2 + 1$	x^2+x+1	x^2	1	x
x^2	0	x^2	x + 1	x^2+x+1	$x^2 + x$	x	$x^2 + 1$	1
$x^2 + 1$	0	$x^2 + 1$	1	x^2	x	x^2+x+1	x + 1	$x^2 + x$
$x^2 + x$	0	$x^2 + x$	x^2+x+1	1	$x^2 + 1$	x + 1	x	x^2
x^2+x+1	0	x^2+x+1	$x^2 + 1$	x	1	$x^2 + x$	x^2	x + 1

Để tìm phần tử nghịch đảo của phép nhân đa thức, ta cũng sử dụng thuật toán

*/*Euclid mở rộng tương tự như tìm nghịch đảo trong tập Z_p */*

Thuật toán Euclid mở rộng trả về 2 giá trị

Gcd (m(x), b(x))

Nếu gcd(m(x), b(x)) = 1; trả về $b^{-1}(x)$ mod m(x)

Extended_euclid(m(x),b(x))

A1(x) = 1; A2(x) = 0; A3(x) = m(x);

B1(x) = 0; B2(x) = 1; B3(x) = b(x)

while (B3(x) <>0) AND (B3(x)<> 1) do

Q(x) = phần thương của A3(x) /B3(x);

T1(x) = A1(x) – Q(x)B1(x)

T2(x) = A2(x) – Q(x)B2(x)

T3(x) = A3(x) – Q(x)B3(x)

A1(x) = B1(x) ; A2(x) = B2(x) ; A3(x) = B3(x) ;

B1(x) = T1(x); B2(x) = T2(x); B3(x) = T3(x);

End while

If B3(x) = 0 then return A3(x) ; no inverse;

If B3(x) = 1 then return 1; B2(x);

1.2.4.3. GF(2^n) trong mã hóa

Khi thực hiện mã hóa đối xứng hay công khai, bản rõ và bản mã là các con số, việc mã hóa và giải mã có thể quy về việc thực hiện các phép cộng, trừ, nhân, chia. Do đó bản rõ và bản mã phải thuộc một trường nào đó để việc tính toán không ra khỏi trường. Việc quy bản rõ và bản mã về trường số thực không phải là phương án hiệu quả vì tính toán trên số thực tốn kém nhiều thời gian. Máy tính chỉ hiệu quả khi tính toán trên các số nguyên dưới dạng byte hay bit. Do đó trường Z_p là một phương án được tính đến. Tuy nhiên trường Z_p đòi hỏi p phải là một số nguyên tố, trong khi đó nếu biểu diễn bản rõ bản mã theo bít thì số lượng phần tử có dạng 2^n lại không phải là số nguyên tố. Ví dụ, xét tập các phần tử được biểu diễn bởi các số nguyên 8 bit, như vậy có 256 phần tử. Tuy nhiên Z_{256} lại không phải là một trường. Nếu ta chọn trường Z_{251} thì chỉ sử dụng được các số từ 0 đến 250, các số từ 251 đến 255 không tính toán được.

Trong bối cảnh đó, việc sử dụng trường GF(2^n) là một phương án phù hợp vì trường GF(2^n) cũng có 2^n phần tử. Ta có thể ánh xạ giữa một hàm đa thức trong GF(2^n) thành một số nhị phân tương ứng bằng cách lấy các hệ số của đa thức tạo thành dãy bít $a_{n-1}a_{n-2}\ldots.a_1a_0$.

Ví dụ xét trường GF(2^3) với đa thức bất khả quy $m(x) = x^3 + x + 1$ tương ứng với số nguyên 3 bít như sau:

Đa thức trong GF(2^3)	Số nguyên tương ứng	Thập lục phân
0	000	0
1	001	1
x	010	2
x + 1	011	3
x^2	100	4
$x^2 + 1$	101	5
$x^2 + x$	110	6
x^2+x+1	111	7

Bảng phép cộng và bảng phép nhân tương ứng là:

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	0	1	2	3
5	5	4	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1

x	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	3	1	7	5
3	0	3	6	5	7	4	1	2
4	0	4	3	7	6	2	5	1
5	0	5	1	4	2	7	3	6
6	0	6	7	1	5	3	2	4

7	7	6	5	4	3	2	1	0

7	0	7	5	2	1	6	4	3

Bảng nghịch đảo của phép cộng và phép nhân:

a		-a		a^{-1}	
Dạng đa thức	Dạng số	Dạng đa thức	Dạng số	Dạng đa thức	Dạng số
0	0	0	0	-	-
1	1	1	1	1	1
x	2	x	2	$x^2 + 1$	5
x + 1	3	x + 1	3	$x^2 + x$	6
x^2	4	x^2	4	x^2+x+1	7
$x^2 + 1$	5	$x^2 + 1$	5	x	2
$x^2 + x$	6	$x^2 + x$	6	x + 1	3
x^2+x+1	7	x^2+x+1	7	x^2	4

Ngoài ra nếu xét bảng phép nhân của Z_8

x	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Thì phân bố tần xuất các số không đều. Ta có bảng so sánh sau:

Số nguyên	1	2	3	4	5	6	7
Xuất hiện trong Z_8	4	8	4	12	4	8	4
Xuất hiện trong GF(2^3)	7	7	7	7	7	7	7

Vì vậy nếu dùng GF(2^3) thì sẽ thuận lợi hơn cho mã hóa, tránh việc sử dụng tần suất để phá mã.

CHƯƠNG 2: BÀI TOÁN LOGARIT RỜI RẠC

2.1. Tổng quan về bài toán Logarit rời rạc

Bài toán Logarit rời rạc là sự tiếp nối của phép tính Logarit trên trường số thực vào các nhóm hữu hạn. Với hai số thực x,y và cơ số a>0, a#0, nếu $a^x - y = 0$ thì x được gọi là Logarit cơ số a của y, ký hiệu $x = \log_a y$.

Logarit rời rạc là bài toán khó (chưa biết một thuật toán hiệu quả nào), trong khi bài toán ngược lũy thừa rời rạc lại không khó (có thể sử dụng thuật toán bình phương và nhân). Tình trạng này giống như tình hình giữa bài toán thừa số nguyên và phép nhân các số nguyên. Chúng đều có thể dùng để xây dựng cấu trúc cho một hệ mật mã.

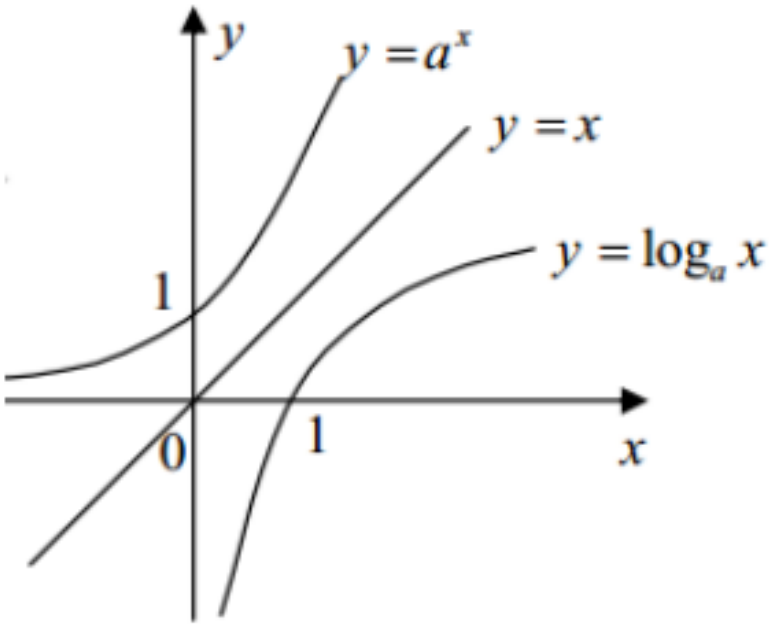
Người ta thường chọn nhóm G trong mật mã Logarit rời rạc là nhóm cyclic (Z^*_p) chẳng hạn như mật mã ElGamal, trao đổi khóa Diffie – Hellman và chữ kí số ElGamal.

Ngoài ra còn có mật mã sử dụng Logarit rời rạc trong nhóm con cyclic của các đường elliptic trên trường hữu hạn gọi là mật mã đường cong elliptic

2.2. Bài toán Logarit trên trường số thực R

+ Bài toán thuận: Hàm số $y = a^x$ với $a,x \in R$ việc tính toán hàm mũ này có thể được thực hiện dễ dàng bằng thuật toán nhân và bình phương.

+ Bài toán ngược: Phép tính ngược của hàm mũ chính là hàm Logarit $y = \log_a x$, việc tính toán hàm ngược Logarit này khó khăn hơn nhiều so với hàm thuận. Tuy nhiên, cả hai phép mũ và Logarit đều là các hàm đồng biến cho nên có thể xác định giá trị tương đối của hàm Logarit như hình dưới đây:



Hình 2. Logarit trên trường số thực

Một số tính chất của hàm Logarit.

+ $y = \log_a bc = \log_a b + \log_a c$

+ $y = \log_a \frac{b}{c} = \log_a b - \log_a c$

+ $\log_a 1 = 0$

+ $y = \log_a x^{-1} = -\log_a x$

2.3. Bài toán Logarit trên trường hữu hạn

Xét với vành đa thức Z_p^* với p là số nguyên tố thì theo định lý nếu p là số nguyên tố thì Z là một trường (Z_p = GF(2)).

Tập tất cả các phần tử khác không của trường sẽ tạo nên một nhóm nhân cyclic Z_p^*

$Z_p^* = Z_p / \{0\} = \{1,2,...,p-1\}$

+ Bài toán thuận : $y = a^x \bmod p$, $(a,x \in Z_p^*)$

Ví dụ : Xét p = 19, a = 2 ta có các giá trị $y = a^x$ như trong bảng dưới đây

Bảng 3: Các giá trị của $y = 2^x \bmod 19$ trên Z^*_{19}

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2^x	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1

Chú ý :

+ Nếu a là một phần tử nguyên thủy thì a^x sẽ đi qua tất cả các phần tử của nhóm.

+ Nếu a là phần tử nguyên thủy thì a^i cũng là nguyên thủy với (i,p-1) = 1 (p là số nguyên tố).

Trong ví dụ trên, các giá trị của i thỏa mãn (i,18) = 1 là i = (1,5,7,11,13,17). Số lượng các giá trị của i bằng giá trị hàm φ(p-1).

$N_i = \varphi(p-1) = \varphi(18) = 6$

Cách tính hàm Phi-Eulet φ như sau:

$\varphi(1) = 1$ và $\varphi(n) = (p-1)p^{k-1}$ với n là lũy thừa bậc k của số nguyên tố p. Nếu m và n là hai số nguyên tố cùng nhau thì $\varphi(mn) = \varphi(m) . \varphi(n)$

Nếu $n = p_1^{k1} . p_2^{k2} \ldots\ldots p_r^{kr}$ trong đó các p_j là các số nguyên tố phân biệt thì

$\varphi(n) = n \prod (1 - 1/p)$ với p|n

Như vậy trong Z^*_{19} có 6 phần tử nguyên thủy:

$2 = 2^i$; $13 = 2^5$; $14 = 2^7$; $15 = 2^{11}$; $3 = 2^{13}$; $10 = 2^{17}$

Các phần tử nguyên thủy này tạo thành các cặp nghịch đảo như sau:

$(2,10) \leftrightarrow 2 = 10^{-1}$

$(13,3) \leftrightarrow 13 = 3^{-1}$

$(14,15) \leftrightarrow 14 = 15^{-1}$

+ Bài toán ngược: $y = \log_2 x$, $(a,x \in Z^*_p)$

Từ bảng trên ta tính được giá trị hàm $\log_2 x$ như sau :

Bảng 4: Các giá trị $\log_2 x \pmod{19}$ trên Z^*_{19}

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2^x	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
$\log_2 x$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

Vì $2^{18} = 1$ nên $\log_2 1 = 18$

Một số tính chất của hàm Logarit rời rạc a^{-1}

+ $y = \log_a bc = (\log_a b + \log_a c) \bmod p - 1$

+ $y = \log_a \frac{b}{c} = (\log_a b - \log_a c) \bmod p - 1$

+ $\log_a{}^{-1} x = -\log_a x = p - 1 - \log_a x$

+ $\log_a 1 = 0 = p - 1$ (vì coi $0 = p - 1$)

Nhận xét : Từ hai bảng trên ta thấy hai hàm thuận và ngược đều không phải là hàm đồng biến, khi biết bài toán thuận thì mới tìm được bài toán ngược. Do đó việc giải bài toán ngược giống bài toán vét cạn, phải thử lần lượt các trường hợp.

Việc xác định Logarit của một phần tử bất ký trong trường hợp là bài toán khó giải.

Bài toán thuận :

Cho Z^*_p với p là số nguyên tố, a là một phần tử nguyên thủy ($a \in Z^*_p$)

Yêu cầu tìm $y = \log_a x$ với $a, x \in Z^*_p$.

Nhận xét: $\forall x \in Z^*_p$ thì :

- Bài toán có nghiệm khi a là một phần tử nguyên thủy
- Bài toán có thể không có nghiệm khi a là phần tử bất kỳ

Ví dụ **:**Với trường hợp p = 19 ta đã tính được 6 phần tử nguyên thủy như trong bảng trên. Ta sẽ đi tìm bài toán Logarit rời rạc với cơ số 6 phần tử nguyên thủy này.

Tuy nhiên ta có thể áp dụng tính chất của hàm Logarit rời rạc để tính Logarit với cơ số là các cặp số nghịch đảo.

$log_a^{-1}x = - log_a x = p – 1 – log_a x$ *hay* $log_a^{-1}x + log_a x = p - 1$

Tức là (2,10) là cặp số nghịch đảo, khi đó $\log_{10}x = p - 1 – \log_2 x = 18 – \log_2 x$

Tương tự (13,3) và (14,15) là các cặp nghịch đảo nên $\log_3 x = 18 – \log_{13} x$ và $\log_{15} x = 18 – \log_{14} x$

Với quy tắc như trên có thể tính được các giá trị lograrit như trong bảng dưới đây :

Bảng 5: Bài toán Logarit rời rạc trên Z^*_{19}

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2^x	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
$\log_2 x$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9
$\log_{10} x$	18	17	5	16	2	4	12	15	10	1	6	3	13	11	7	14	8	9
13^x	13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
$\log_{13} x$	18	11	17	4	14	10	12	15	16	7	6	3	1	5	13	8	2	9
$\log_3 x$	18	7	1	14	4	8	6	3	2	11	12	15	17	13	5	10	16	9
14^x	14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
$\log_{14} x$	18	13	7	8	10	2	6	3	14	5	12	15	11	1	17	16	4	9
$\log_{15} x$	18	5	11	10	8	16	12	15	4	13	6	3	7	17	1	2	14	9

Có thể tính 13^x thông qua 2^x như sau :

Ta thấy $13 = 2^5$ do đó $13^x = 2^{5x} \pmod{19}$. Tương tự có thể tính được $14^x = 2^{7x}$

2.4. Logarit rời rạc trong trường Galois

Cố định số nguyên tố p, số tự nhiên $n > 1$, đặt $q = p^n$. Giả sử a là phần tử sinh của nhóm cyclic F(q)*. Ta muốn giải phương trình $a^x = b$ trong trường F(q). Để làm điều này ta sử dụng các thuật toán với một cơ sở nhân tử. Ta xem thuật toán index-caculus sau :

Ý tưởng của thuật toán này là từ đẳng thức :

$$\prod_{i=1}^{m} x_i = \prod_{j=1}^{n} y_j$$

Các phần tử x_i, y_j nằm trong trường hữu hạn Z_p thì

$$\sum_{i=1}^{m} log_a x_i \equiv \sum_{j}^{n} log_a y_j (mod\ p-1)$$

Phương pháp đơn giản để tạo ra biểu thức trên – chọn phần tử bất kỳ g ϵ Z_p, tính u = a^g (mod p) và bằng cách lựa chọn chúng ta thử tìm số thỏa mãn điều kiện sau :

$$u = \prod p_i$$

Từ trên ta có thuật toán sau :

Thuật toán index – calculus

Input: cho hai số a và b.

Output: Tìm $\log_a b$

Bước 1. (Tính toán ban đầu). Trường F(q) đồng cấu với $F_p[x]/f(y)$, với $f(y) \in F_p[x]$ là đa thức đa thức bất khả quy bậc n. Cho nên bất kỳ thành phần của trường F_q được biểu diễn dưới dạng đa thức bậc không vượt quá n-1. Và nhân các đa thức như vậy sẽ rút gọn theo modulo f(y), điều này chúng ta đã tìm hiểu ở trường số. Phần tử $a_1 = a^{(q-1)(p-1)}$ có bậc là p -1 và tạo thành F_q*

Bước 2. (Lựa chon cơ sở nhân tử). Cơ sở nhân tử B ∈ F_q thành lập từ tất cả các đa thức g bất khả quy bậc không lớn hơn t, t là một số tham số, t < n

Bước 3. (Tìm biểu thức) Lựa chọn ngẫu nhiên m ≤ 1 , m ≤ q-2 , ta tìm các giá trị sao cho thỏa mãn biểu thức

$$a^m \equiv c_0 \prod_{g \in B} g^{a_g(m)}\ (mod\ f(y))$$

Với c_0 ∈ F_p từ đây tìm ra được biểu thức

$$m = log_a c_0 + \sum_{g \in B} \alpha_a(m) log_a g (mod\ q - 1)$$

ở đây $\log_a c_0$ ta đã biết, $\log_a g$ ta chưa biết độ lớn.

Bước 4. (Tìm thuật toán cho các phần tử của cơ sở nhân tử). Khi tìm ở bước 3 số lượng đủ lớn của biểu thức, ta giải hệ phương trình tuyến tính trong vành Z_{p-1} và tìm ra $\log_a g$

Bước 5. (Tìm Logarit riêng.) Ta tìm một giá trị của m sao cho:

$$b \times a^m \equiv c_1 \prod_{g \in B} g^{\beta_g} \big(mod\ f(x)\big)\ \ c_1 \in F_q$$

Từ đây tìm ra giá trị cần tìm

$$log_a b \equiv -m + log_a c_1 + \sum_{g \in B} \beta_q log_a g\ (mod\ q - 1)$$

2.5. Các phương pháp giải bài toán Logarit rời rạc

2.5.1. Thuật toán vét cạn

Đây là thuật toán tự nhiên nhất và kém hiệu quả nhất để tính Logarit rời rạc. Người ta cứ thử tính α^0, α^1, α^2, … cho đến khi nào đạt được β thì thôi. Phương pháp này đòi hỏi O(n) phép toán nhân với n là cấp của α và do đó không hiệu quả khi n lớn và rõ ràng là hàm mũ thực sự theo logn.

2.5.2. Thuật toán bước đi lớn bước đi nhỏ (Baby-step giant-step)

Giả sử m = [$\sqrt{n}$] với n là cấp của α .

Thuật toán bước đi lớn bước đi nhỏ là sự thoả hiệp giữa thời gian và bộ nhớ của phương pháp vét cạn và dựa trên quan sát sau là nếu $\beta = \alpha^x$ thì chúng có thể viết x = im + j với $0 \le i,j < m$. Từ đó $\alpha^x = \alpha^{im} \alpha^j$ hay $\beta (\alpha^{-m})^i = \alpha^j$. Vậy nên người ta có thể lập bảng (j, α^j) với $0 \le j < m$.

Sau đó lần lượt tính $\beta (\alpha^{-m})^{-i}$ với i lần lượt chạy từ 0 đến m – 1 và tra trong bảng (j, α^j) chừng nào có được đẳng thức $\beta (\alpha^{-m})^i = \alpha^j$ thì dừng lại.

Thuật toán này đòi hỏi không gian lưu trữ là O($\sqrt{n}$) phần tử nhóm và đòi hỏi O($\sqrt{n}$) phép nhân để xây dựng và O($\sqrt{n}$ logn) phép so sánh để sắp xếp. Ngoài ra nó cũng cần O($\sqrt{n}$) phép toán nhân và O($\sqrt{n}$) phép toán tra bảng. Tựu chung là nó có thời gian chạy O($\sqrt{n}$) phép toán nhóm.

2.5.3. Thuật toán Pohlig – Hellman

Thuật toán này tận dụng lợi thế của phân rã của cấp n của nhóm G. Giả sử phân rã của n = $p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$ là phân rã nguyên tố của n. Nếu x = $\log_\alpha \beta$ thì cách tiếp cận này xác định x_i = x mod $p_i^{e_i}$ với 1 ≤ i ≤ r và sau đó sử dụng thuật toán Gauss làm việc với định lý phần dư Trung Hoa để tìm ra x mod n.

Mỗi số x_i được tính theo các chữ số $l_0, l_1, \ldots, l_{e_i - 1}$ trong biểu diễn p_i phân rã của $x_i = l_0 + l_1 p_1 + \ldots + l_{e_i - 1}\, p^{e^i - 1}$ với $0 \le l_j \le p_i - 1$. Giả sử bước thứ j chúng ta đã tính được $l_0, l_1, \ldots, l_{j-1}$. Do đó chúng ta tính được $\gamma = \alpha^{l_0 + l_1 p_i + \ldots + l_{j-1} p_i^{j-1}}$ và $\overline{\alpha} = \alpha^{n/p_i}$. Do đó $\overline{\beta} = (\beta / \gamma)^{n/p_i^{j+1}} = (\overline{\alpha})^{l_j}$. Từ đây l_j được tính Logarit rời rạc theo cơ số $\overline{\alpha}$ của $\overline{\beta}$.

Khi biết trước phân rã của n thì thời gian chạy của thuật toán Pohlig – Hellman sẽ là O($\sum_{i=1}^{r} e_i (\log n + \sqrt{p_i})$ các phép toán nhóm. Thuật toán này chỉ thực sự hiệu quả khi ước lượng nguyên tố p_i của n tương đối nhỏ hay n là số nguyên mịn.

Các thuật toán trên đây cho thấy một điều là chúng đều chạy trong thời gian hàm mũ thực sự theo số bit đầu vào. Chính vì vậy mà chúng là không hiệu quả khi tấn công bài toán Logarit rời rạc.

2.5.4. Thuật toán tính chỉ số (Index-Calculus)

Thuật toán tính chỉ số là thuật toán mạnh nhất được biết đến khi đem tấn công bài toán Logarit rời rạc. Không phải nhóm nào cũng có thể áp dụng thuật toán tính chỉ số nhưng nếu áp dụng được thì nó cho chúng ta thời gian chạy là hàm tiểu mũ.

Thuật toán tính Logarit rời rạc đối với nhóm cyclic:

Đầu vào: Phần tử sinh α của nhóm cyclic G có cấp n và phần tử $\beta \in$ G.

Đầu ra: Logarit rời rạc y = $\log_\alpha \beta$.

Chọn cơ sở phân tích S: Chọn tập con S = {p_1, p_2, …, p_t } của G sao cho "một tỷ lệ đáng kể" của tất cả các phần tử của G có thể được biểu diễn hiệu quả như là tích của các phần tử của S.

1. Chọn các quan hệ tuyến tính liên quan đến Logarit của các phần tử của S.

   1.1 Chọn số ngẫu nhiên k, $0 \le k \le n-1$ và tính α^k .

   1.2 Thử biểu diễn α^k thành tích các phần tử trong S:

$$\alpha^k = \prod_{i=1}^{t} p_i^{c_i} \text{ , } c_i \ge 0$$

   Nếu thành công thì lấy Logarit cả hai vế của đẳng thức trên để đạt được quan hệ tuyến tính:

$$k = \sum_{i=1}^{t} c_i log_\alpha p_i \ (mod\ n)$$

   2.3 Lặp lại các bước 2.1 và 2.2 chừng nào t + c các quan hệ như trên đạt được (c là số tự nhiên nhỏ chẳng hạn c = 10 sao cho hệ phương trình đã cho với t + c phương trình sẽ có nghiệm duy nhất với xác xuất cao).

2. Tìm các Logarit của các phương trình trong S: Tính theo mod n giải hệ phương trình có t + c phương trình với t ẩn số giống như trên tại bước 2 để đạt được $\log_\alpha p_i$, với $1 \le i \le t$.

3. Tính y:

   3.1 Chọn số nguyên ngẫu nhiên k, $0 \le i \le k \le n-1$ và tính $\beta.\alpha^k$.

   3.2 Cố gắng biểu diễn $\beta.\alpha^k$ thàn tích của các phần tử trong S:

$$\beta.\alpha^{k} = \prod_{i=1}^{t} p_i^{d_i}$$

Nếu cố gắng không đạt kết quả thì lặp lại bước 4.1. Ngược lại, lấy Logarit cả hai vế của đẳng thức thu được để đạt được :

$$\log_{\alpha} \beta = \left(\prod_{i=1}^{t} d_i \log_{\alpha} p_i - k \right) \bmod n$$

Và do đó chúng ta có được kết quả của thuật toán là:

$$y = \left(\sum_{i=1}^{t} d_i \log_{\alpha} p_i - k \right) \bmod n .$$

2.5.4.1. Tính chỉ số trên GF(p)

Đối với trường GF(p) với số nguyên tố thì cơ sở phân tích được chọn sẽ là t số nguyên tố đầu tiên. Quan hệ phân rã trên cơ sở phân tích được sinh ra bằng cách tính α^{k} mod p và sử dụng phép chia thông thường để kiểm tra xem số nguyên này có là tích của các số nguyên tố trong S hay không.

Ví dụ: Thuật toán tính Logarit rời rạc trên Z^{*}_{229} với p = 229. Phần tử sinh α = 6 có cấp n = 228. Xét trường hợp β = 13. Khi $\log_6 13$ được tính như sau đây sử dụng kỹ thuật tính chỉ số:

1. Cơ sở phân tích được chọn là 5 số nguyên tố đầu tiên S = {2, 3, 5, 7, 11}.
2. Sáu quan hệ sau đây liên quan đến các phần tử của cơ sở phân tích đã đạt được:

   $6^{100} \bmod 229 = 180 = 2^2.3^2.5$

   $6^{18} \bmod 229 = 176 = 2^4.11$

   $6^{12} \bmod 229 = 165 = 3.5.11$

   $6^{62} \bmod 229 = 154 = 2.7.11$

   $6^{143} \bmod 229 = 198 = 2.3^2.11$

   $6^{206} \bmod 229 = 210 = 2.3.5.7$

Các quan hệ này mang lại 6 phương trình sau đây liên quan đến các phần tử

trong cơ sở phân tích:

$100 = 2\log_6 2 + 2\log_6 3 + \log_6 5 \pmod{228}$

$18 = 4\log_6 2 + \log_6 11 \pmod{228}$

$12 = \log_6 3 + \log_6 5 + \log_6 11 \pmod{228}$

$62 = \log_6 2 + \log_6 7 + \log_6 11 \pmod{228}$

$143 = \log_6 2 + 2\log_6 3 + \log_6 11 \pmod{228}$

$206 = \log_6 2 + \log_6 3 + \log_6 5 + \log_6 7 \pmod{228}$

3. Giải hệ phương trình tuyến tính có sáu phương trình với năm ẩn số chúng ta thu được lời giải $\log_6 2 = 21$, $\log_6 3 = 208$, $\log_6 5 = 98$, $\log_6 7 = 107$ và $\log_6 11 = 162$.

4.Giả sử số nguyên k = 77 được chọn thì vì rằng $\beta.\alpha^k = 13.6^{77} \bmod 229 = 147 = 3.7^2$

và suy ra rằng: $\log_6 13 = (\log_6 3 + 2\log_6 7 - 77) \bmod 228 = 117$.

2.5.4.2. Tính chỉ số trên GF(2^n)

Các phần tử của trường hữu hạn $F_{2^n}^*$ được biểu diễn thành các đa thức trên $Z_2[x]$ có bậc cao nhất là n – 1 với phép nhân được thực hiện modulo một đa thức bất khả quy f(x) có bậc n trên $Z_2[x]$. Cơ sở phân tích S được chọn là tập các đa thức bất khả quy trên $Z_2[x]$ có bậc cao nhất là một cận b nào đó. Quan hệ phân tích được sinh bằng cách tính α^k mod f(x) và sử dụng phép chia thông thường để kiểm tra xem đa thức này có là tích của các đa thức trong S không.

Ví dụ: Thuật toán tính Logarit trên $F_{2^7}^*$. Đa thức $f(x) = x^7 + x + 1$ bất khả quy trên Z_2. Từ đó các phần tử của trường hữu hạn GF(2^7) có cấp 128 được biểu diễn là một tập của tất cả các đa thức trên $Z_2[x]$ có bậc cao nhất là 6 với các phép nhân được thực hiện modulo f(x). Cấp của $F_{2^7}^*$ là $n = 2^7 - 1 = 127$ và $\alpha = x$ là phần tử sinh của $F_{2^7}^*$. Giả sử $\beta = x^4 + x^3 + x^2 + x + 1$. Khi đó $y = \log_\alpha \beta$ có thể được tính như sau sử dụng kỹ thuật tính chỉ số:

1. Cơ sở phân tích được chọn là tập tất cả các đa thức bất khả quy trên $Z_2[x]$ có bậc cao nhất là 3: S = {x, x + 1, $x^2 + x + 1$, $x^3 + x + 1$, $x^3 + x^2 + 1$ }
2. Năm quan hệ sau đây liên quan đến các phần tử của cơ sở phân tích đã đạt được:

   $x^{18} \mod f(x) = x^6 + x^4 = x^4(x+1)^2$

   $x^{103} \mod f(x) = x^6 + x^5 + x^4 + x = x(x+1)^2(x^3 + x^2 + 1)$

   $x^{72} \mod f(x) = x^6 + x^5 + x^3 + x^2 = x^2(x+1)^2(x^2 + x + 1)$

   $x^{45} \mod f(x) = x^5 + x^2 + x + 1 = (x+1)^2(x^3 + x + 1)$

   $x^{121} \mod f(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x^3 + x + 1)(x^3 + x^2 + 1)$

   Để cho thuận tiện chúng ta kí hiệu $p_1 = \log_x x$, $p_2 = \log_x(x+1)$, $p_3 = \log_x(x^2 + x + 1)$, $p_4 = \log_x(x^3 + x + 1)$, $p_5 = \log_x(x^3 + x^2 + 1)$. Sau đó chúng ta có các phương trình:

   $18 = 4p_1 + 2p_2 \pmod{127}$

   $103 = p_1 + 2p_2 + p_3 \pmod{127}$

   $72 = 2p_1 + 2p_2 + p_3 \pmod{127}$

   $45 = 2p_2 + 2p_4 \pmod{127}$

   $121 = p_4 + p_3 \pmod{127}$
3. Giải hệ phương trình tuyến tính gồm năm phương trình và năm ẩn số chúng ta thu được $p_1 = 1$, $p_2 = 7$, $p_3 = 56$, $p_4 = 34$ và $p_5 = 90$.
4. Giả sử k = 66 được chọn thì vì rằng:

$$\beta\alpha^k = (x^4 + x^3 + x^2 + x + 1)x^{66} \bmod f(x) = x^5 + x^3 + x = x(x^2 + x + 1)^2$$

Và từ đây suy ra rằng:

$$\log_x(x^4 + x^3 + x^2 + x + 1) = (p_1 + 2p_3 - 66) \bmod 127 = 47$$

Nếu chúng ta biểu diễn hàm thời gian chạy của thuật toán A với đầu vào là các phần tử của trường hữu hạn GF(q) như sau đây:

$$L_q[\alpha, c] = o(\exp((c + o(1))(\ln q)^q (\ln \ln q)^{1-\alpha})$$

Với c là hằng số dương và α là hằng số thoả mãn $0 < \alpha < 1$ thì A khi đó là thuật toán thời gian tiểu hàm mũ. Khi $\alpha = 0$ thì $L_q[0,c]$ là đa thức theo lnq còn khi $\alpha = 1$ thì $L_q[1,c]$ là đa thức q và như vậy nó là mũ thực sự theo lnq.

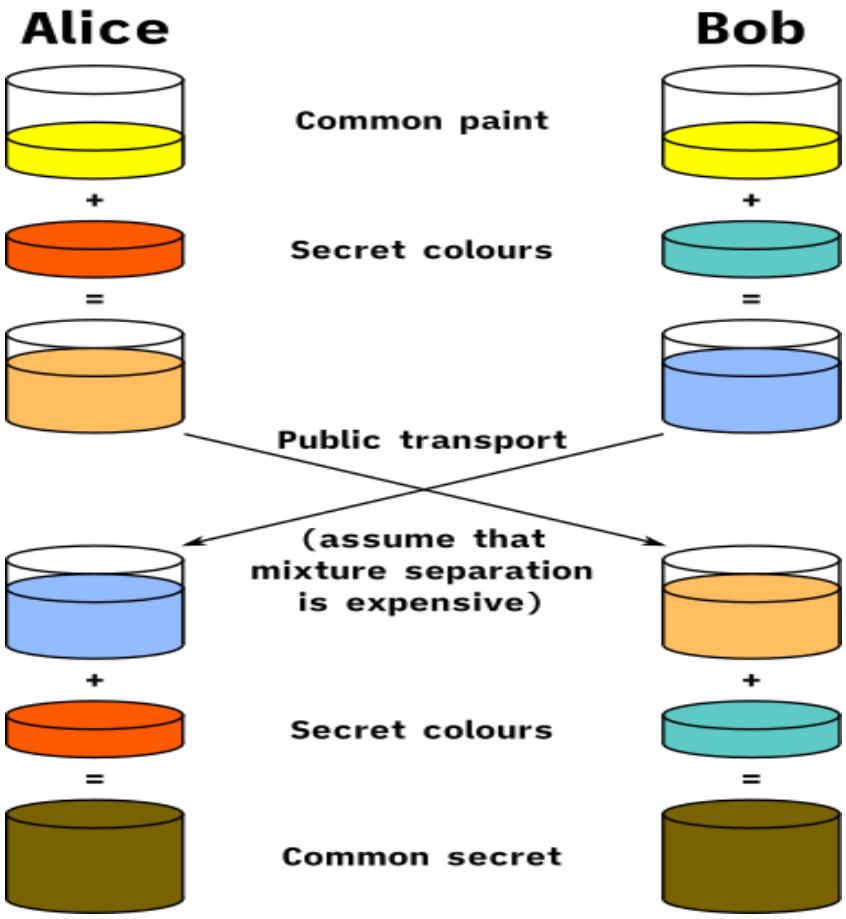
Thuật toán chỉ số trên GF(q) trong cả hai trường hợp q = p với p nguyên tố và $q = 2^n$ đều có thời gian chạy kỳ vọng là $L_q[\frac{1}{2},c]$ với c>0 là hằng số. Thời gian chạy kỳ vọng của thuật toán tính chỉ số là tiểu hàm mũ tốt hơn so với các thuật toán thời gian chạy là hàm mũ thực sự trước đây nhưng chưa phải là tốt nhất cả về lý thuyết và thực hành hiện nay.

Người ta tìm ra những thuật toán là biến thể của thuật toán tính chỉ số theo nghĩa sử dụng những kỹ thuật toán học và môi trường tính toán đặc biệt để thiết kế thành các thuật toán có thời gian chạy tốt hơn về lý thuyết và thực hành. Một loại thuật toán như vậy chính là thuật toán sàng trường số với thời gian chạy là $L_q[\frac{1}{3},c]$ với q = p nguyên tố và c = 1.923.

CHƯƠNG 3: HỆ MẬT ELGAMAL TRÊN TRƯỜNG ĐA THỨC

3.1. Trao đổi khóa Diffie Hellman

Trao đổi khoá Diffie Hellman là sơ đồ khoá công khai đầu tiên được đề xuất bởi Diffie và Hellman năm 1976 cùng với khái niệm khoá công khai. Sau này được biết đến bởi James Ellis (Anh), người đã đề xuất bí mật năm 1970 mô hình tương tự. Đây là phương pháp thực tế trao đổi công khai các khoá mật. Sự ra đời của giao thức trao đổi khoá Diffie – Hellman được xem là bước mở đầu cho lĩnh vực mã khoá công khai. Nó thúc đẩy việc nghiên cứu đề xuất các mã khoá công khai.



Hình 3. Trao đổi khóa Diffie-Hellman

3.1.1. Bài toán Diffie Hellman:

Cho một nhóm các Cyclic hữu hạn G và các phần tử

- Không thể dùng để trao đổi mẩu tin bất kỳ.
- Tuy nhiên nó có thể thiết lập khoá chung.
- Chỉ có hai đối tác biết đến.
- Giá trị khoá phụ thuộc vào các đối tác (và các thông tin về khoá công khai và khoá riêng của họ).
- Dựa trên phép toán lũy thừa trong trường hữu hạn (modulo theo số nguyên tố hoặc đa thức) là bài toán dễ.
- Độ an toàn dựa trên độ khó của bài toán tính Logarit rời rạc là bài toán khó.

3.1.2. Khởi tạo Diffie Hellman

- Mọi người dùng thỏa thuận dùng tham số chung:
  - Số nguyên tố rất lớn q hoặc đa thức.
  - α là căn nguyên tố của mod q.
- Mỗi người dùng (A chẳng hạn) tạo khoá của mình:
  - Chọn một khoá mật (số) của A: $x_A < q$
  - Tính khoá công khai của A: $Y_A = \alpha^{x_A} \mod q$
  - Mỗi người dùng thông báo công khai khoá của mình Y_A.

3.1.3. Trao đổi khoá Diffie Hellman

- Khoá phiên dùng chung cho hai người sử dụng A, B là K_{AB}

  $K_{AB} = \alpha^{x_A x_B} \mod q$

  $= Y_A^{x_B} \mod q$ (mà **B** có thể tính)

  $= Y_B^{x_A} \mod q$ (mà **A** có thể tính)

- K_{AB} được sử dụng như khoá phiên trong sơ đồ khoá riêng giữa A và B

- A và B lần lượt trao đổi với nhau, họ có khoá chung K_{AB} cho đến khi họ chọn khoá mới.
- Kẻ thám mã cần x, do đó phải giải tính Logarit rời rạc.

Ví dụ:

Hai người sử dụng Alice & Bob muốn trao đổi khoá phiên:

- Đồng ý chọn số nguyên tố q = 353 và α = 3

- Chọn các khoá mật ngẫu nhiên:

A chọn x_A = 97, B chọn x_B =233

- Tính các khoá công khai:

$Y_A = 3^{97} \bmod 353 = 40$ (Alice)

$Y_B = 3^{233} \bmod 353 = 248$ (Bob)

- Tính khoá phiên chung:

$K_{AB} = Y_B^{x_A} \bmod 353 = 248^{97} = 160$ (Alice)

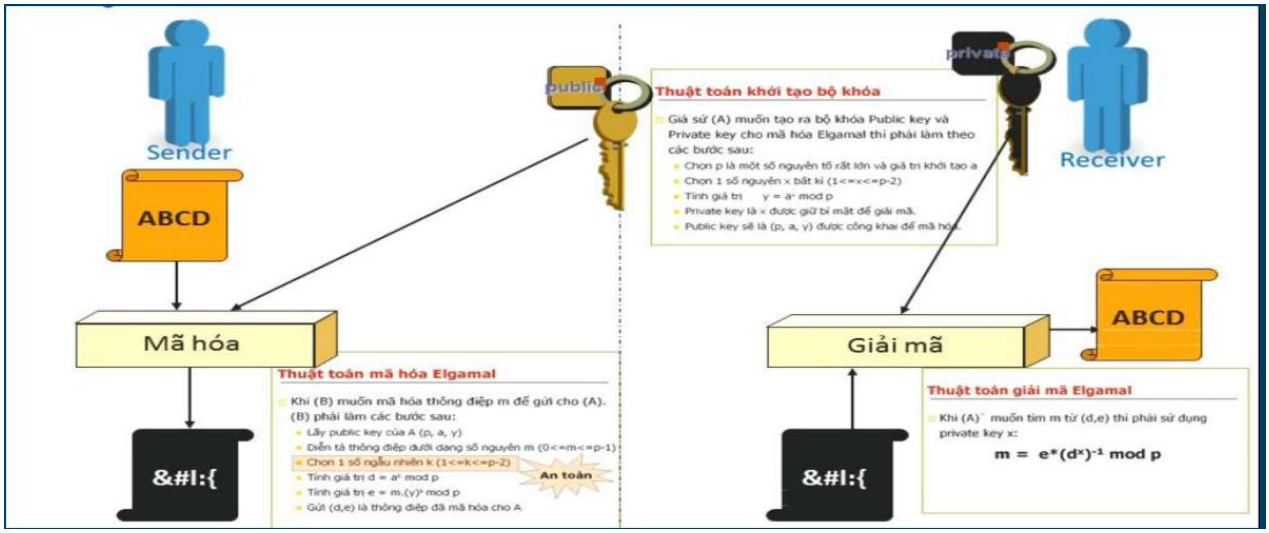
$K_{AB} = Y_A^{x_B} \bmod 353 = 40^{233} = 160$ (Bob)

3.2. Hệ mật ElGamal [3,Tr 294]

3.2.1. Giới thiệu

Hệ mã ElGamal là một hệ mật mã công khai. Hệ mã này dựa trên bài toán Logarit rời rạc. Tính an toàn của hệ mã này dựa vào độ phức tạp của bài toán loogarit.

Hệ ElGamal là một biến thể của sơ đồ phân phối khóa Diffie Hellman, được đưa ra năm 1985. So với hệ mã RSA , hệ ElGamal không có nhiều rắc rối về vấn đề bản quyền sử dụng.



Hình 4. Hệ mật ElGamal

3.2.2. Thủ tục tạo khóa

Mỗi bên liên lạc A, B tạo cho mình một cặp khóa công khai và khóa bí mật như sau:

1. Chọn số nguyên tố đủ lớn p sao cho sao cho bài toán logarit rời rạc trong Z_p là khó giải.
2. Cho g ϵ Z_p* là phần tử nguyên thủy
3. Chọn khóa bí mật x là số ngẫu nhiên sao cho 1< x < p - 1. Tính khóa công khai y theo công thức: $y = g^x \pmod p$
4. Sử dụng ba giá trị (p, g, y) làm khóa công khai của người nhận và gửi chúng cho người sử dụng cần mã hóa thông tin bí mật gửi cho mình.

3.2.3. Mã hóa hệ ElGamal

Giả sử B cần gửi bản tin M cho A, B sẽ thực hiện các bước sau:

1. B nhận khóa công khai của A: (p, g, y)

2. B chọn số nguyên k ngẫu nhiên với 1 < k < p – 1 và tính giá trị theo công thức :

$$\begin{cases} \gamma = g^k \ mod \ p \\ \delta = M(g^a)^k \ mod \ p \end{cases}$$

Giả sử bản tin đã được biểu thị dưới dạng một số nguyên M trong dải (1,…,p-1) Phép tính mũ được tính bằng thuật toán nhân và bình phương theo modulo

3. B gửi bản mã C = (γ , δ) cho A

Ta nhận thấy bản mã C được ghép từ γ , δ nên nó có độ dài bit bằng 2 lần độ dài của M, đây là nhược điểm của hệ mật này.

3.2.4. Giải mã hệ ElGamal

A nhận bản mã C từ B và tiến hành giải mã theo các bước sau:

1. A sử dụng khóa bí mật a để tính:

$$\gamma^{p-1-a} \bmod p = g^{-ak} \bmod p \text{ (Vì } \gamma^{p-1-a} = (g^k)^{-a} \text{)}$$

2. A khôi phục bản rõ bằng cách tính:

$$\delta\, \gamma^{p-1-a} \bmod p = M\, g^{ak}\, g^{-ak} = M$$

3.2.5. Tính đúng đắn của thuật toán mật mã hệ ElGamal

Thuật toán mật mã ElGamal hoàn toàn là đúng đắn. Với cách khôi phục bản tin ban đầu M bằng cách :

$$\delta\, \gamma^{p-1-a} \bmod p = M\, g^{ak}\, g^{-ak} = M$$

Như vậy, bản rõ nhận được sau giải mã chính là bản rõ ban đầu M.

3.2.6. Ví dụ

Cho hệ mã ElGamal có p = 347, g = 23, a = 67.

Ta tính $y = g^a \bmod p = 23^{67} \bmod 347 = 77$, từ đó suy ra khóa công khai là (p, g, y) = (347, 23, 77) và khóa bí mật là: a = 67.

Để mã hóa thông điệp ký tự “o”, ta chuyển nó thành số, chẳng hạn có thể lấy tương ứng các chữ cái “a” đến “z” với các số từ 0 đến 25 thì “o” ứng với 14.

Với M = 14 ta chọn số ngẫu nhiên k, chẳng hạn k = 54 rồi tính

$\gamma = g^k \bmod p = 23^{54} \bmod 347 = 278$.

Tiếp tục tính $\delta = M.y^k \bmod p = 14.77^{54} \bmod 347 = 59$.

Vậy bản mã gửi đi sẽ là (278, 59).

Khi người nhận nhận được bản mã (278, 59) sẽ tiến hành tính như sau: Tính $\gamma^a \bmod p = 278^{67} \bmod 347 = 29$ rồi tính $Z^{-1} = 29^{-1} \bmod 347 = 12$ Tiếp tục tính $\delta .y^{-a} \bmod p = (59. 12) \bmod 347 = 14$.

Do đã thỏa thuận trước về việc chuyển đổi ký tự nên người nhận đọc lại được ký tự "o" là bản rõ ban đầu.

Ta có nhận xét là khi giải mã, người nhận không hề biết số ngẫu nhiên k mà người gửi dùng để mã hóa. Điều đó cũng có nghĩa là với cùng một khóa, cùng một bản rõ có thể có nhiều bản mã khác nhau mà người nhận vẫn giải mã đúng.

3.2.7. Thám mã hệ ElGamal

Hệ mật ElGamal sẽ bị phá vỡ nếu khóa mật x hoặc k có thể tính được. Để tính được x hoặc k, cần phải giải một trong hai bài toán logarit rời rạc, tuy nhiên việc giải bài toán logarit rời rạc này là việc khó.

Chúng ta có hai thuật toán để giải bài toán Logarit rời rạc

- Thuật toán Shanks
- Thuật toán Pohlig – Hellman

Thuật toán Shanks

Thuật toán này có tên gọi khác là thuật toán thời gian – bộ nhớ. Tư tưởng của thuật toán là nếu ta có đủ bộ nhớ thì có thể sử dụng bộ nhớ đó để giảm thời gian thực hiện của thuật toán.

Input: Số nguyên tố p, phần tử nguyên thủy a của Z^*_p, số nguyên tùy ý

Output: Cần tìm a sao cho $y = a \bmod p$

Thuật toán:

Gọi $m = [(p-1)^{1/2}]$ (lấy phần nguyên)

1.Tính $a^{mj} \bmod p$ với $0 \leq j \leq m-1$.

2.Sắp xếp các cặp (j, a^{mj} mod p) theo a^{mj} mod p và lưu vào danh sách L1.

3.Tính ya^{-i} mod p, $0 \leq i \leq m-1$.

4.Sắp xếp các cặp (i, ya^{-i} mod p) theo ya^{-i} mod p và lưu vào danh sách L2.

5.Tìm trong hai danh sách L1 và L2 xem có tồn tại cặp (j, a^{mj} mod p) và (i, ya^{-i} mod p) mà a^{mj} mod p = ya^{-i} mod p .

6. Tính x = (mj + i) mod (p -1)

3.3. Hệ mật ElGamal trên trường đa thức

Dựa trên các hệ thống an toàn và cấu trúc có sẵn để xây dựng hệ mật ElGamal với hai lũy đẳng nguyên thủy. Chúng ta sửa đổi kiểu che giấu dữ liệu đó là theo phương pháp nhân và phương pháp cộng. Cũng giống như hệ mật ElGamal trong trường nguyên tố Z_p nhưng chúng đơn giản hơn về mặt tính toán.

Kiểu che dấu dữ liệu có nhiều cách, kiểu che giấu gốc của hệ mật là che giấu kiểu nhân. Vậy chúng ta có thể thêm kiểu che giấu dữ liệu theo kiểu cộng. Cộng sẽ dễ hơn về tính toán nhưng về mặt an toàn sẽ kém hơn.

Vành đa thức với hai lũy đẳng nguyên thủy bất khả quy có dạng $Z_2[x]/(1+x)g(x)$ với g(x) là đa thức bất khả quy nguyên thủy với bậc m

Các nhóm nhân của vành bao gồm:

+ $\{x^i \text{ mod } (1+x)g(x)\}$ i = 1, $2^m - 1$
+ $\{(x+g(x))^i \text{ mod } (1+x)g(x)$
+ g(x)
+ 0

3.3.1 . Hệ mã ElGamal theo phương pháp cộng trên vành đa thức với hai lũy đẳng

3.3.1.1. Tạo khóa

Trong hệ mã hóa ElGamal này, các khóa công khai và khóa bí mật được tạo ra như sau:

Bước 1: A chọn vành đa thức với hai lũy đẳng nguyên thủy bất khả quy $Z_2[x]/(1+x)g(x)$

Bước 2: A chọn $\alpha(x)$ là đa thức bất nguyên thủy khả quy

Bước 3: A chọn khóa bí mật a là số ngẫu nhiên sao cho $1< a < 2^m - 1$. Tính khóa công khai A(x) theo công thức $\alpha^a(x) \bmod (1+x)g(x)$

4. A sử dụng ba giá trị ($Z_2[x]/(1+x)g(x)$, $\alpha(x)$, A(x)) làm khóa công khai của người nhận và gửi chúng cho người sử dụng cần mã hóa thông tin bí mật gửi cho mình.

3.3.1.2. Mã hóa

Giả sử B có đoạn thông tin M(x) cần gửi cho A.

Khi đó để gửi bản tin M(x) cho A, sẽ thực hiện các bước như sau:

Bước 1: B chọn số ngẫu nhiên b thỏa mãn $1< a < 2^m - 1$, sau đó B tính giá trị $\gamma(x)$ theo công thức:

$$\gamma(x) = \alpha^b(x) \bmod (1+x)g(x).$$

Sử dụng khóa công khai của A để tính:

$$\delta(x) = (M(x) + A^b(x)) \bmod (1+x)g(x).$$

Bước 2: B gửi bản mã gồm ($\gamma(x)$, $\delta(x)$) đến A

3.3.1.3. Giải mã

Để khôi phục bản rõ ban đầu M(x) từ bản mã ($\gamma(x)$, $\delta(x)$) nhận được, A sử dụng khóa bí mật a của mình để tính toán và thực hiện các bước như sau:

$$M(x) = \delta(x) + \gamma^a(x) \bmod (1+x)g(x)$$

$$= [M(x) + A^b(x) + \gamma^a(x)] \bmod (1+x)g(x)$$

$$= [M(x) + \alpha^{ab}(x) + \alpha^{ab}(x)] \bmod (1+x)g(x)$$

$$= M(x)$$

3.3.1.4. Ví dụ

Tao khóa

Bước 1: A chọn trường đa thức $Z_2[x]/(1+x).(x^4+x+1)$

Bước 2: A chọn đa thức bất khả quy nguyên thủy $\alpha(x) = x^3+x+1$

Bước 3: A chọn khóa bí mật a = 4 là số ngẫu nhiên. Tính khóa công khai

$$A(x) = (x^3+x+1)^4 \mod (1+x).(x^4+x+1) = x^3 + x^2 + 1$$

Bước 4: A sử dụng ba giá trị ($Z_2[x]/(1+x).(x^4+x+1)$, x^3+x+1, x^3+x^2+1) làm khóa công khai của người nhận và gửi chúng cho B

Mã hóa

Giả sử B muốn gửi bản tin $M(x) = x^4 + x^2 + 1$ cho A

Bước 1: B chọn b = 5 và tính $\gamma(x) = (x^3+x+1)^5 = x^4+x^2+1$

B sử dụng khóa công khai của A để tính: $\delta(x) = (x^4 + x^2 + 1) + (x^3 + x^2 + 1)^5 = 0$

Bước 2: B gửi bản mã $c = [\gamma(x),\delta(x)]$ cho A

Giải mã

A nhận bản mã c và tính $M(x) = \gamma^a(x) + \delta(x)$

$$= (x^4+x^2+1)^4 + 0 = x^4+x^2+1$$

3.3.2. Hệ mã ElGamal theo phương pháp nhân trên vành đa thức với hai lũy đẳng

3.3.2.1. Tạo khóa

Trong hệ mã hóa ElGamal này, các khóa công khai và khóa bí mật được tạo ra như sau:

Bước 1: A chọn vành đa thức với hai lũy đẳng nguyên thủy bất khả quy $Z_2[x]/(1+x)g(x)$

Bước 2: A chọn $\alpha(x)$ là đa thức bất nguyên thủy khả quy

Bước 3: A chọn khóa bí mật a là số ngẫu nhiên sao cho $1< a < 2^m - 1$. Tính khóa công khai $A(x) = \alpha^a(x) \mod (1+x)g(x)$

Bước 4: A sử dụng ba giá trị ($Z_2[x]/(1+x)g(x)$, $\alpha(x)$, $A(x)$) làm khóa công khai của người nhận và gửi chúng cho người sử dụng cần mã hóa thông tin bí mật gửi cho mình.

3.3.2.2. Mã hóa

Giả sử B có đoạn thông tin M(x) cần gửi cho A.

Khi đó để gửi bản tin M(x) cho A, sẽ thực hiện các bước như sau:

Bước 1: B chọn số ngẫu nhiên b thỏa mãn $1< a < 2^m - 1$, sau đó B tính giá trị $\gamma(x)$ theo công thức:

$$\gamma(x) = \alpha^b(x) \bmod (1+x)g(x).$$

Sử dụng khóa công khai của A để tính:

$$\delta(x) = M(x).A^b(x) \bmod (1+x)g(x).$$

Bước 2: B gửi bản mã gồm $(\gamma(x), \delta(x))$ đến A

3.3.2.3. Giải mã

Để khôi phục bản rõ ban đầu M(x) từ bản mã $(\gamma(x), \delta(x))$ nhận được, A sử dụng khóa bí mật a của mình để tính toán và thực hiện các bước như sau:

$$\begin{aligned} M(x) &= \delta(x) .(\gamma^a(x))^{-1} \bmod (1+x)g(x) \\ &= (M(x).A^b(x).\gamma^a(x)) \bmod (1+x)g(x) \\ &= M(x).\alpha^{ab}(x).\alpha^{-ab}(x) \bmod (1+x)g(x) \\ &= M(x) \end{aligned}$$

3.3.2.4. Ví dụ

Tạo khóa

Bước 1: A chọn trường đa thức $Z_2[x]/(1+x).(x^4+x+1)$

Bước 2: A chọn đa thức bất khả quy nguyên thủy: $\alpha(x) = x^3+x+1$

Bước 3: A chọn khóa bí mật a =4. Tính khóa công khai

$A(x) = (x^3+x+1)^4 \bmod (1+x).(x^4+x+1) = x^3 + x^2 + 1$

Bước 4: A sử dụng ba giá trị $(Z_2[x]/(1+x).(x^4+x+1), x^3+x+1, x^3+x^2+1)$ làm khóa công khai và gửi chúng cho B

Mã hóa

Giả sử B muốn gửi bản tin $M(x) = x^4 + x^2 + 1$ cho A

Bước 1: B chọn b = 5 và tính $\gamma(x) = \alpha^5(x) = (x^3+x+1)^5 = x^4+x^2+1$

Sử dụng khóa công khai của A và tính:

$\delta(x) = M(x).A^b(x) = M(x).\alpha^{ab}(x) = (x^4+x^2+1)(x^3+x^2+1)^{20} = x^2+x+1$

Bước 2: B gửi bản mã $c = [\gamma(x),\delta(x)] = [x^4+x^2+1, x^2+x+1]$ cho A

Giải mã

A nhận bản mã c và tính:

$M(x) = \delta(x).\gamma^{-a}(x) = (x^2 + x + 1)(x^2 + x + 1) = (x^4+x^2+1)$

3.3.3. Độ an toàn

Hệ thống ElGamal dựa trên bài toán Logarit rời rạc. Tính an toàn của nó tùy thuộc vào độ phức tạp của bài toán Logarit rời rạc

Trong bài toán về hệ ElGamal

+ p là số nguyên tố, a là phần tử nguyên thủy của Z^*_p (p và a là cố định)

+ Bài toán Logarit rời rạc có thể được phát biểu như sau: Tìm 1 số mũ x duy nhất ($0< x < p -1$) sao cho $a^x = y \bmod p$, với y thuộc Z^*_p cho trước.

+ Bài toán có thể giải được bằng phương pháp vét cạn (tức duyệt tất cả phần tử x để tìm x thỏa mãn. Bài toán có độ phức tạp là O(p). Vấn đề đặt ra là nếu p rất lớn thì để thực hiện phương pháp này phải cần thời gian rất lớn, do đó không khả thi để tìm ra x. Hệ mật an toàn, khó bị thám mã giải mã.

KẾT LUẬN

Luận văn nghiên cứu giải quyết bài toán về mã hóa, giải quyết bài toán ElGamal trên trường đa thức. Từ việc giải quyết bài toán là nền tảng cho nhiều ứng dụng trong thực tế như dịch vụ thương mại điện tử, chữ ký số, cá thể hóa thẻ trong ngân hàng, bầu cử …

Luận văn đã đạt được một số kết quả chính sau:

- Tìm hiểu về bài toán Logarit rời rạc, một số thuật toán giải bài toán Logarit rời rạc.
- Tìm hiểu các phương pháp che dấu dữ liệu trên vành Z_p, Z_p^*, từ đó ứng dụng vào hệ mật ElGamal trên trường đa thức
- Nghiên cứu về hệ mật ElGamal trên trường đa thức với hai lũy đẳng nguyên thủy và lấy ví dụ minh họa cụ thể

1. Hạn chế

- Dung lượng bộ nhớ dành cho việc lưu trữ khóa lớn
- Tốc độ mã hóa chậm do phải xử lý và tính toán giá trị lớn, để hệ mật được an toàn thì tham số bậc của đa thức phải đủ lớn. Do bậc đa thức càng lớn thì độ phức tạp của bài toán logarit càng lớn.

2. Hướng phát triển

- Ứng dụng chữ ký số, dịch vụ thương mại.
- Kết hợp kiểu che dấu dữ liệu khác an toàn hơn và tốc độ nhanh hợn
- Tìm hiểu hệ mật ElGamal trên vành đa thức với nhiều hơn 2 lũy đẳng nguyên thủy

DANH MỤC CÁC TÀI LIỆU THAM KHẢO

[1] Nguyễn Bình, Giáo trình Mật mã học, Học viện Công nghệ Bưu chính Viễn thông.

[2] Phan Đình Diệu. Lý thuyết mật mã và an toàn thông tin – NXB Đại học Quốc gia Hà Nội - 2006

[3] Hồ Thuần (2000), Giáo trình Lý thuyết mật mã và an toàn dữ liệu, Đại học Bách Khoa Hà Nội

[3] A.J Menezes all Handbook of applied cryptography CRC Press 1998

[4] Crypttography and Network Security Principles and Practices, 4th Edition – William Stallings – Prentice Hall – 2005

[5] D Stinson Cryptography CRC Press 1995

[6] E.R Berlekamp Algebraic coding Theory McGraw Hill book company 1968

[7] W.W Peterson Error correcting codes The M.I.T.Press 1961

[8] http://vi.wikipedia.org/wiki/Lôgarit_rời_rạc

[9] https://vi.wikipedia.org/wiki/Trao_đổi_khóa_Diffie-Hellman