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

TÓM TẮT LUẬN VĂN THẠC SĨ

HÀ NỘI - NĂM 2020

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: GS.Nguyễn Bình

Phản biện 1: ……

Phản biện 2: ……..

Luận văn sẽ được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông

Vào lúc: ..... giờ ..... ngày ..... tháng .... năm .....

Có thể tìm hiểu luận văn tại:

- Thư viện của Học viện Công nghệ Bưu chính Viễn thông.

MỞ ĐẦU

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.. 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.

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 sử dụng 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. Một trong những thuật toán mã hóa khóa công khai được phát triển dự 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.

Đề tài nhằm nghiên cứ 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.

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

Chương 2 Bài toán Logarit rời rạc

Chương 3. Hệ mật ElGamal trên trường đa thức

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…

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.

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.

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.

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

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 dụng một khóa khác để giải mã, nghĩa là khóa để mã hóa và giải mã là khác nhau.

1.2 Cơ sở toán học

1.2.1 Modulo số học

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.

1.2.2 Nhóm, vành và trường

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: $\forall a \in G, \exists! a' \in G: a \bullet a' = a' \bullet a = e$
+ 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: $\exists g \in G, \forall a \in G, \exists k, a=g^k$

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 Abel 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: $\forall a,b,c \in R$

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

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

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

+ Tồn tại phần tử đơn vị phép nhân: $a1 = 1a = a$

+ Liên quan giữa phép nhân và phần tử đơn vị phép cộng:

Nếu $ab = 0$ thi $a = 0$ 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:

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

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

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

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

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)

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

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

+ Đa thức trên tập Z_p

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

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

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

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

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

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.

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

Tập W_{pm} có p^n phần tử

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.

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 $a_{n-1}a_{n-2}\ldots.a_1a_0$.

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 Logarith 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.

2.2 Bài toán Logarith 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.

Một số tính chất của hàm Logarithm.

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

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

+ $\log_a 1 = 0$

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

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 xyclic Z^*_p

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

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

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).

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

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 $0 = p - 1$)

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 :

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 $B \in F_q$ 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 $m \leq 1$, $m \leq q-2$, ta tìm các giá trị sao cho thỏa mãn biểu thức

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

Với $c_0 \in F_p$ từ đây tìm ra được biểu thức

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

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:

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

Từ đây tìm ra giá trị cần tìm

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

2.5 Các phương pháp giải bài toán Logarith rời rạc

2.5.1 Thuật toán vét cạn

Đây là thuật toán tự nhiên nhất và kém hiệu quả nhất để tính Logaritth rời rạc. Người ta cứ thử tính α^0, α^1, α^2, … cho đến khi nào đạt được β thì thôi

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.

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 $x_i = x \bmod p_i^{e_i}$ với $1 \le i \le r$ và sau đó sử dụng thuật toán Gauss làm việc với định lý phần dư Trung Hoa để tìm ra x mod n.

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 Logarith 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.

2.4.5.1.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.

2.4.5.2.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.

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 cộng. Nó thúc đẩy việc nghiên cứu đề xuất các mã khoá công khai.

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 Logarith 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: $y_A = \alpha^{X_A} \bmod q$.
  - Mỗi người dùng thông báo công khai khoá của mình y_A.

3.1.2 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)

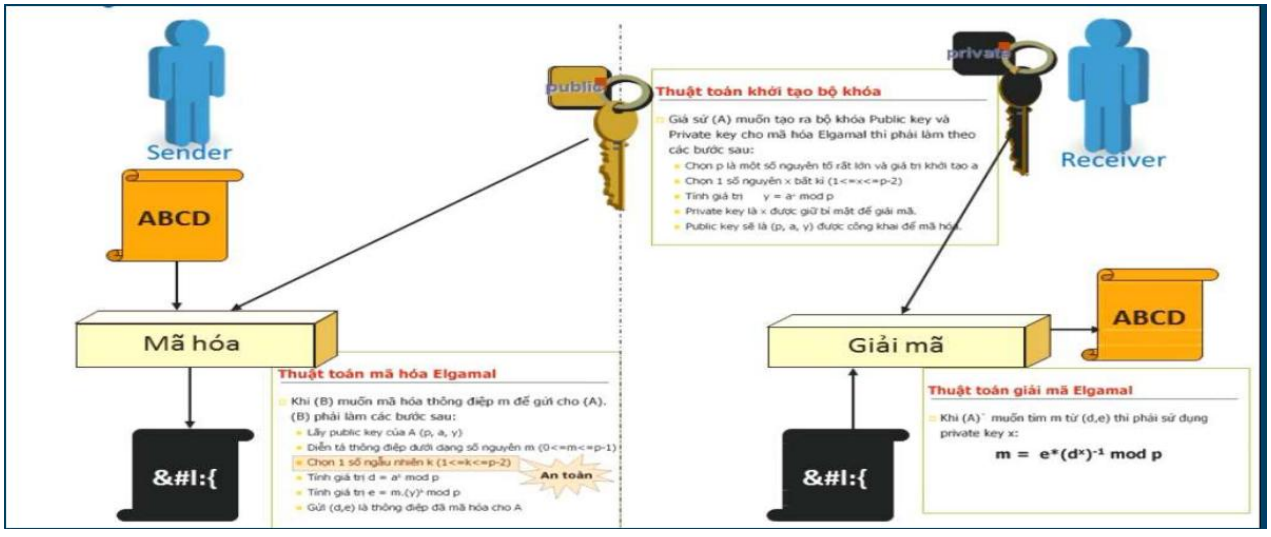
- K_{AB} được sử dụng như khoá phiên trong sơ đồ khoá riêng giữa A và B
- A và B lần lượt trao đổi với nhau, họ có khoá chung K_{AB} cho đến khi họ chọn khoá mới.
- Kẻ thám mã cần x, do đó phải giải tính Logarith rời rạc.

3.2 Hệ mật Elgamal

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 Logarit.

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



Hình 1. 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 lôgarit 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 :

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

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:

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

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 loogarit rời rạc, tuy nhiên việc giải bài toán lôgarit 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 mod p

Thuật toán:

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

1.Tính a^{mj} mod 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 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

+ $\{x^i \text{ mod } (1+x)g(x)\}$ 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

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 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 đã đạt được một số kết quả sau:

- Nghiên cứu về bài toán Logarit rời rạc, một số thuật toán giải bài toán Logarit rời rạc.

- Nghiên cứu về hệ mật elgamal trên trường đa thức với hai lũy đẳng nguyên thủy và lấy ví dụ minh họa cụ thể

- 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