

TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI

**KHOA CÔNG NGHỆ THÔNG TIN**

------🙙🕮🙛-------



**BÁO CÁO THỰC NGHIỆM**

Học phần: An ninh mạng

**Chủ đề**: **Chữ ký số Elgmal và ứng dụng trong xác thực tính toàn vẹn của dữ liệu**

.

Giáo viên hướng dẫn: TS. Phạm Văn Hiệp

Nhóm sinh viên thực hiện:

1. Nguyễn Bá Thuận Mã SV: 2022603360

2. Đỗ Tuấn Đạt Mã SV: 2022602884

3. Nguyễn Văn Dũng Mã SV: 2023601938

4. Nguyễn Mạnh Hùng Mã SV: 2021608268

5. Lê Đăng Dương Mã SV: 2021607148

Mã Lớp học phần: 20241IT6070001

Nhóm: 2

Hà Nội - Năm 2024

**MỤC LỤC**

Danh mục các từ viết tắt…

Danh mục hình ảnh…

Danh mục bảng biểu…

…Các chương, các đề mục trong báo cáo…

Bảng phân công công việc (theo file mẫu, in ra và kẹp vào báo cáo)..

**Lời nói đầu**

Trước đây, khi công nghệ máy tính chưa phát triển, vấn đề an toàn và bảo mật thông tin thường được thực hiện thông qua các biện pháp thủ công để đảm bảo tính toàn vẹn và bí mật của dữ liệu. Các biện pháp như đóng dấu và ký niêm phong một bức thư để kiểm tra tính nguyên vẹn, mã hóa thông điệp để bảo vệ nội dung chỉ dành cho người gửi và người nhận, hoặc lưu giữ tài liệu trong két sắt tại nơi được bảo vệ nghiêm ngặt là những ví dụ điển hình.

Ngày nay, với sự phát triển vượt bậc của công nghệ, đặc biệt là sự bùng nổ của Internet và các thiết bị thông minh, vấn đề an toàn và bảo mật thông tin trở nên cấp bách hơn bao giờ hết. Việc trao đổi và lưu trữ một lượng lớn dữ liệu trên môi trường số đặt ra những thách thức to lớn, đòi hỏi các phương pháp bảo mật hiện đại để đảm bảo dữ liệu không bị sửa đổi hoặc giả mạo. Trong số đó, chữ ký số đóng vai trò quan trọng, không chỉ giúp xác thực danh tính người gửi mà còn đảm bảo tính toàn vẹn của dữ liệu trong quá trình truyền tải.

Chữ ký số ElGamal, dựa trên nguyên lý mật mã khóa công khai, là một trong những phương pháp được sử dụng phổ biến để xác thực tính toàn vẹn của dữ liệu. Với tính năng bảo mật cao và khả năng ứng dụng linh hoạt, thuật toán này đã trở thành công cụ hữu hiệu trong nhiều lĩnh vực, từ giao dịch điện tử đến quản lý tài liệu số.

Trong báo cáo này, nhóm em đã nghiên cứu về chữ ký số ElGamal và ứng dụng của nó trong việc xác thực tính toàn vẹn của dữ liệu. Báo cáo được tổ chức thành 3 chương:

* Chương 1: Tổng quan về đề tài nghiên cứu.
* Chương 2: Kết quả nghiên cứu và triển khai ứng dụng.
* Chương 3: Kết luận và bài học kinh nghiệm.

Nhóm em xin gửi lời cảm ơn chân thành tới thầy Phạm Văn Hiệp, giảng viên hướng dẫn nhóm thực hiện đề tài trong khuôn khổ học phần An ninh mạng. Với sự hướng dẫn tận tình của thầy, nhóm em đã cố gắng hoàn thành tốt nội dung báo cáo. Tuy nhiên, do hạn chế về kinh nghiệm và thời gian, không thể tránh khỏi những thiếu sót trong quá trình thực hiện. Vì vậy, nhóm rất mong nhận được những ý kiến đóng góp quý báu từ thầy cô và các bạn để có thể tiếp tục cải thiện và hoàn thiện hơn.

**Chương 1: Tổng quan**

* 1. Tổng quan về An ninh mạng

Thuật toán mã hóa ElGamal là một thuật toán quan trọng trong lĩnh vực an ninh mạng, vậy nên trước tiên chúng ta cần hiểu rõ khái niệm an ninh mạng là gì, cũng như các vấn đề liên quan đến lĩnh vực này.

Thứ nhất, an ninh mạng là một lĩnh vực quan trọng và không thể thiếu trong kỹ thuật và công nghệ. Nó bao gồm các biện pháp bảo vệ hệ thống, mạng máy tính và dữ liệu khỏi các mối đe dọa như truy cập trái phép, tấn công, đánh cắp hoặc phá hoại thông tin. An ninh mạng đóng vai trò quan trọng trong việc bảo vệ hệ thống thông tin của cá nhân, tổ chức và cả quốc gia trước các nguy cơ ngày càng tinh vi trong môi trường số.

Thứ hai, với sự phát triển nhanh chóng của Internet và các công nghệ kỹ thuật số, an ninh mạng trở thành một vấn đề cấp bách, đặc biệt trong bối cảnh nhiều hoạt động kinh doanh, giao dịch và trao đổi thông tin được thực hiện trực tuyến. Các vấn đề liên quan đến an ninh mạng bao gồm:

* Mã hóa dữ liệu:  
  Mã hóa dữ liệu là một trong những phương pháp quan trọng nhất để bảo vệ thông tin trên môi trường mạng. Quá trình mã hóa chuyển đổi dữ liệu gốc thành một định dạng khác, chỉ có thể giải mã bằng khóa thích hợp, giúp bảo vệ dữ liệu khỏi truy cập trái phép. Các thuật toán mã hóa phổ biến bao gồm DES, AES, RSA và ElGamal.
* Xác thực danh tính và chữ ký số:  
  Chữ ký số là một cơ chế xác thực giúp đảm bảo tính toàn vẹn và nguồn gốc của dữ liệu. Chữ ký số không chỉ chứng minh tài liệu hoặc thông điệp đến từ người gửi hợp lệ mà còn đảm bảo rằng dữ liệu không bị sửa đổi trong quá trình truyền tải.
* Quản lý và bảo mật khóa:  
  Trong an ninh mạng, quản lý khóa là một yếu tố quan trọng để đảm bảo sự an toàn của dữ liệu mã hóa. Quản lý khóa bao gồm việc tạo, lưu trữ, phân phối và thu hồi các khóa mã hóa, đảm bảo rằng chỉ những người có thẩm quyền mới có thể sử dụng các khóa này.
* Phát hiện và phòng chống tấn công mạng:  
  Các hệ thống an ninh mạng phải có khả năng phát hiện và ngăn chặn các cuộc tấn công, chẳng hạn như tấn công từ chối dịch vụ (DDoS), xâm nhập trái phép, tấn công phishing hoặc ransomware. Điều này đòi hỏi sự kết hợp của các công cụ và giải pháp, từ tường lửa đến các hệ thống phát hiện xâm nhập (IDS).
* Quản lý truy cập và danh tính:  
  Đảm bảo rằng chỉ những người dùng được ủy quyền mới có quyền truy cập vào các hệ thống và tài nguyên quan trọng là một phần không thể thiếu của an ninh mạng. Việc này bao gồm xác thực đa yếu tố (MFA) và sử dụng các hệ thống quản lý danh tính để giám sát và kiểm soát quyền truy cập.
* Kiểm thử và đánh giá bảo mật:  
  Kiểm thử bảo mật là một quy trình cần thiết để đánh giá các lỗ hổng và điểm yếu của hệ thống trước khi chúng bị kẻ xấu khai thác. Các phương pháp như kiểm thử xâm nhập (penetration testing) và quét lỗ hổng được áp dụng để cải thiện độ an toàn của hệ thống mạng.

Những vấn đề trên cho thấy tầm quan trọng của an ninh mạng trong việc bảo vệ các hệ thống và dữ liệu quan trọng. Trong bối cảnh này, thuật toán mã hóa công khai ElGamal nổi lên như một công cụ hữu ích không chỉ trong việc mã hóa dữ liệu mà còn trong việc xác thực và bảo vệ tính toàn vẹn thông tin trên môi trường mạng.

* 1. Các kiến thức cơ sở (kiến thức cơ sở về toán học, thuật toán, ngôn ngữ lập trình…)

Để nghiên cứu và triển khai thuật toán mã hóa ElGamal và ứng dụng trong xác thực tính toàn vẹn dữ liệu, chúng ta cần dựa vào các kiến thức nền tảng thuộc nhiều lĩnh vực khác nhau. Các kiến thức cơ sở này bao gồm:

### 1. Kiến thức cơ sở về toán học

* Lý thuyết số:  
  Lý thuyết số là nền tảng quan trọng để hiểu cách hoạt động của thuật toán ElGamal. Các khái niệm như số nguyên tố, số nguyên tố lớn, tính chất modulo, và luỹ thừa modulo đóng vai trò thiết yếu trong việc mã hóa và giải mã.
* Logarit rời rạc (Discrete Logarithm):  
  Thuật toán ElGamal dựa vào bài toán logarit rời rạc, một bài toán toán học khó giải trong thực tế, để đảm bảo tính bảo mật. Hiểu được bài toán này giúp chúng ta đánh giá được độ an toàn của thuật toán.

### 2. Kiến thức về thuật toán và cấu trúc dữ liệu

* Thuật toán mã hóa công khai:  
  Thuật toán ElGamal thuộc nhóm mã hóa công khai, do đó, cần hiểu rõ cách hoạt động của các thuật toán mã hóa công khai khác như RSA để so sánh và nắm bắt đặc điểm chung.
* Thuật toán nhân nhanh và luỹ thừa modulo:  
  Do ElGamal yêu cầu xử lý các số rất lớn, các thuật toán tối ưu như nhân nhanh và luỹ thừa modulo hiệu quả là rất quan trọng để giảm thời gian tính toán.
* Thuật toán sinh số nguyên tố:  
  Việc sinh ra các số nguyên tố lớn đóng vai trò quan trọng trong việc thiết lập khóa của thuật toán. Hiểu các phương pháp sinh số nguyên tố như thử chia, kiểm tra Miller-Rabin, hoặc các thuật toán sinh số ngẫu nhiên là cần thiết.

### 3. Kiến thức về ngôn ngữ lập trình

* Lập trình cơ bản:  
  Kỹ năng lập trình là yêu cầu không thể thiếu để triển khai thuật toán ElGamal. Các khái niệm như biến, hàm, vòng lặp, và xử lý lỗi là nền tảng để xây dựng chương trình.
* Lập trình với số lớn:  
  Do thuật toán ElGamal hoạt động trên các số lớn, cần sử dụng thư viện hỗ trợ hoặc các kỹ thuật lập trình tối ưu để xử lý hiệu quả. Ví dụ, các thư viện như BigInteger trong Java hoặc System.Numerics.BigInteger trong C#.
* Ngôn ngữ lập trình áp dụng:  
  Thuật toán ElGamal có thể được triển khai bằng nhiều ngôn ngữ lập trình như Python, Java, C++, hoặc C#. Hiểu rõ cú pháp và thư viện hỗ trợ của ngôn ngữ được sử dụng là một yêu cầu quan trọng.

### 4. Kiến thức về hệ thống và an ninh mạng

* Hệ thống mã hóa và quản lý khóa:  
  Hiểu cách mã hóa công khai tích hợp với các hệ thống quản lý khóa (Public Key Infrastructure - PKI) là cần thiết để ứng dụng thuật toán vào các hệ thống thực tế.
* Chữ ký số:  
  Do ứng dụng của thuật toán ElGamal liên quan đến việc tạo và xác thực chữ ký số, cần hiểu quy trình tạo chữ ký, kiểm tra chữ ký, và các tiêu chuẩn phổ biến như RSA, DSA để so sánh và tối ưu hóa.

### 5. Kiến thức bổ trợ khác

* Kỹ năng đọc hiểu và nghiên cứu tài liệu:  
  Việc nghiên cứu các tài liệu chuyên ngành về mật mã học, thuật toán, và các tiêu chuẩn mã hóa là rất cần thiết để áp dụng lý thuyết vào thực tế.
* Kiến thức về kiểm thử phần mềm:  
  Để đảm bảo chương trình hoạt động chính xác, cần có kỹ năng kiểm thử mã nguồn (unit testing) và kiểm tra hiệu suất của thuật toán trong các trường hợp thực tế.

Những kiến thức trên là nền tảng để triển khai thành công thuật toán mã hóa ElGamal và các ứng dụng liên quan trong lĩnh vực an ninh mạng.

* 1. Nội dung nghiên cứu (trình bày lý do và các nội dung nghiên cứu…)

Trong bối cảnh phát triển nhanh chóng của công nghệ thông tin và việc lưu trữ, truyền tải dữ liệu trên các nền tảng trực tuyến ngày càng trở nên phổ biến, vấn đề bảo mật và xác thực tính toàn vẹn của dữ liệu là một yêu cầu quan trọng đối với mọi hệ thống. Một trong những phương pháp được ứng dụng rộng rãi để đảm bảo tính toàn vẹn và bảo mật của dữ liệu là chữ ký số. Thuật toán chữ ký số ElGamal, với tính bảo mật dựa trên bài toán logarit rời rạc, đã trở thành một trong những lựa chọn hiệu quả cho việc xác thực và bảo vệ tính toàn vẹn của thông tin.

Với mục tiêu nghiên cứu và ứng dụng thuật toán chữ ký số ElGamal, nhóm chúng em đã tiến hành các nghiên cứu sau:

### 1. **Lý do nghiên cứu**

Chữ ký số ElGamal đóng vai trò quan trọng trong việc bảo vệ tính toàn vẹn của dữ liệu, đặc biệt trong các giao dịch điện tử, hệ thống chứng thực, và bảo mật thông tin. Việc đảm bảo tính toàn vẹn và xác thực của thông tin trong môi trường mạng là cực kỳ quan trọng, giúp ngăn chặn việc sửa đổi hoặc giả mạo thông tin. Nghiên cứu về thuật toán ElGamal giúp hiểu rõ cơ chế bảo mật của chữ ký số và áp dụng nó để bảo vệ dữ liệu trong thực tế.

### 2. **Các nội dung nghiên cứu**

Để thực hiện nghiên cứu về chữ ký số ElGamal và ứng dụng của nó trong xác thực tính toàn vẹn của dữ liệu, nhóm chúng em đã tập trung vào các nội dung chính sau:

* Tìm hiểu về chữ ký số ElGamal: Nghiên cứu nguyên lý hoạt động của thuật toán chữ ký số ElGamal, bao gồm các bước tạo khóa, ký và xác minh chữ ký, cũng như các vấn đề bảo mật liên quan đến thuật toán này.
* Quy trình tạo khóa công khai và khóa bí mật: Nghiên cứu cách lựa chọn các tham số an toàn như số nguyên tố lớn pp và cơ sở sinh gg, từ đó tính toán khóa công khai và khóa bí mật đảm bảo an toàn cho việc ký và xác minh chữ ký.
* Thuật toán ký và xác minh chữ ký: Tìm hiểu chi tiết cách thực hiện các phép toán trong quá trình ký và xác minh chữ ký, bao gồm việc sử dụng khóa bí mật để ký và khóa công khai để xác minh tính toàn vẹn của dữ liệu.
* Ứng dụng thực tế của chữ ký số ElGamal trong xác thực tính toàn vẹn: Nghiên cứu và thực hiện chương trình mẫu để minh họa ứng dụng chữ ký số ElGamal trong việc xác thực tính toàn vẹn của dữ liệu trong các hệ thống thông tin, như các giao dịch điện tử, hệ thống bảo mật email, và các ứng dụng truyền thông khác.
* Kiểm thử và tối ưu hóa thuật toán: Kiểm thử và đánh giá hiệu quả của thuật toán trong các tình huống thực tế, sửa lỗi và tối ưu hóa chương trình để đạt được hiệu quả cao nhất trong việc bảo vệ tính toàn vẹn của dữ liệu.

Những nội dung nghiên cứu trên sẽ giúp nhóm chúng em hiểu rõ hơn về chữ ký số ElGamal, ứng dụng thực tế của nó, đồng thời cung cấp một công cụ hữu ích để bảo vệ tính toàn vẹn của dữ liệu trong các hệ thống thông tin hiện đại.

**Chương 2: Kết quả nghiên cứu**

**( Hùng, Đỗ Đạt hạn thứ 7 tuần này)**

* 1. Nghiên cứu, tìm hiểu hệ mã hóa khóa công khai (hoặc “hệ mã hóa khóa bí mật” tùy theo từng đề tài).
  2. Chữ ký số và ứng dụng trong thực tế
  3. Nghiên cứu, tìm hiểu về … (Đề tài về nội dung gì thì trình bày về vấn đề đó, Nội dung thuật toán)

Ví dụ: Nghiên cứu, tìm hiểu về hệ mật mã Elgamal

## 2.1. Giới thiệu tổng quan

### 2.1.1. Chữ ký điện tử

● Chữ ký điện tử (Electronic Signature) là thông tin đi kèm theo dữ liệu (văn bản, hình ảnh, âm thanh, …) nhằm mục đích xác định chủ nhân của dữ liệu và xác nhận sự chấp thuận của người đó đối với nội dung dữ liệu đã ký.

● Chữ ký điện tử cũng giống như chữ viết tay, tức là chữ ký điện tử được dùng để xác nhận lời hứa hay cam kết của người nào đó và sau đó không thể chối bỏ được.

● Chữ ký điện tử không đòi hỏi phải sử dụng giấy mực mà nó gắn đặc điểm nhận dạng của người ký vào một bản cam kết nào đó. Như vậy, chữ ký điện tử sẽ chứng thực định danh người gửi và bảo vệ sự toàn vẹn dữ liệu.

● Chữ ký điện tử được sử dụng trong các giao dịch số. Xuất phát từ thực tế, chữ ký điện tử cần đảm bảo chức năng xác định được người chủ của một dữ liệu nào đó: văn bản, âm thanh, hình ảnh, … của dữ liệu đó có bị thay đổi hay không.

● Thông thường chữ ký của một người trên tài liệu thường đặt ở cuối bản tin để xác nhận nguồn gốc hay trách nhiệm của người ký với tài liệu đó. Với tài liệu đã được “số hóa” nếu chữ ký đặt ở cuối bản tin thì việc sao chép “chữ ký số” là dễ dàng và tính toàn vẹn dữ liệu sẽ không được đảm bảo. Vậy một “chữ ký số” đặt cuối tài liệu “số hóa” không thể chịu trách nhiệm đối với toàn bộ nội dung văn bản. “Chữ ký số” thể hiện trách nhiệm đối với toàn bộ tài liệu phải là chữ ký được ký trên từng bit của tài liệu đó. Tuy nhiên, chữ ký số cũng không thể ký trên bất kỳ tài liệu nào với độ dài tùy ý, vì như vậy chữ ký số sẽ có độ dài rất lớn. Với tài liệu dài người ta ký trên đại diện của nó mà đại diện này được tạo ra từ hàm băm.

● Chữ ký thông thường người ta kiểm tra bằng cách so sánh với chữ ký xác thực khác. Đây không phải phương pháp an toàn vì nó có thể giả mạo. Với chữ ký số, người ta có thể kiểm tra thông qua thuật toán kiểm tra công khai.Bất kỳ ai cũng có thể kiểm tra được chữ ký số. Việc dùng một lược đồ chữ ký an toàn sẽ ngăn chặn được khả năng giả mạo bởi nó sẽ đảm bảo ba yêu cầu:

○ Xác thực

○ Toàn vẹn dữ liệu

○ Không thể thoái thác trách nhiệm

● Bản thân bức điện, văn bản gửi đi cần chứa thông tin thay đổi liên tục (chẳng hạn như ngày tháng) để đảm bảo văn bản không bị dùng lại vì bản sao tài liệu được ký bằng chữ ký số đồng nhất với bản gốc

● Lợi ích của việc sử dụng chữ ký điện tử:

○ Giảm thời gian

○ Giảm chi phí

○ Bảo mật thông tin

### 2.1.2. Tính pháp lý của chữ ký điện tử

Để xác định tính pháp lý của 3 loại chữ ký điện tử gồm: Chữ ký số, chữ ký scan và chữ ký hình ảnh, doanh nghiệp có thể căn cứ vào các văn bản pháp luật sau đây:

● Luật Giao dịch điện tử năm 2005.

● Nghị định 130/2018/NĐ-CP ngày 27/9/2018 của Chính Phủ quy định chi tiết thi hành Luật Giao dịch điện tử năm 2005.

● Nghị định số 52/2013/NĐ-CP ngày 16/5/2013 của Chính phủ về thương mại điện tử.

● BLDS 2015 điều chỉnh tất cả các loại giao dịch và hợp đồng, bao gồm cả các giao dịch và hợp đồng được ký kết bằng chữ ký sống và các giao dịch và hợp đồng được ký kết thông qua phương tiện điện tử.

Theo Luật Giao dịch điện tử 2005, chữ ký điện tử có giá trị pháp lý nếu:

● Phương pháp tạo chữ ký điện tử cho phép xác minh người ký và chứng tỏ sự chấp thuận của người ký đối với nội dung hợp đồng.

● Phương pháp tạo chữ ký điện tử là đủ tin cậy, phù hợp với mục đích mà hợp đồng được khởi tạo và gửi đi.

Như vậy, theo các quy định của pháp luật hiện hành, pháp luật Việt Nam mới có quy định về chữ ký số, chưa có nhiều văn bản hướng dẫn cụ thể về hiệu lực của hợp đồng được ký kết bằng hình thức scan hay chữ ký hình ảnh. Do đó, khi tìm hiểu về khung pháp lý cho chữ ký điện tử sử dụng trên hợp đồng điện tử, doanh nghiệp có thể căn cứ vào các văn bản pháp luật quy định về chữ ký số để áp dụng.

Chữ ký số Elgamal là một phương pháp chữ ký số dựa trên bài toán logarith rời rạc, được phát triển bởi Taher Elgamal vào năm 1985. Phương pháp này cung cấp tính bảo mật cao nhờ độ khó trong việc giải bài toán logarith rời rạc và được sử dụng trong nhiều hệ thống bảo mật hiện đại. Dưới đây là bản tóm tắt về lược đồ chữ ký số Elgamal:

Bước 1: Khởi tạo khóa

1. Chọn tham số nhóm:
   * Chọn một số nguyên tố lớn ppp sao cho bài toán logarith rời rạc trên là khó giải quyết.
   * Chọn một phần tử sinh g trong nhóm .
2. Tạo khóa:
   * Chọn một số ngẫu nhiên bí mật xxx (1<x<p−1), đây là khóa bí mật.
   * Tính y= mod p, đây là khóa công khai.

Khóa bí mật: x  
 Khóa công khai: (p,g,y)

Bước 2: Ký

Để ký một thông điệp m:

1. Chọn ngẫu nhiên k sao cho 1<k<p−1 và gcd (k, p−1) = 1
2. Tính:
   * r = mod  p
   * s=(m−x\*r) \* mod (p−1),  
      trong đó là nghịch đảo modular của k modulo p−1.
3. Chữ ký là cặp (r,s).

Bước 3: Xác thực

Để xác thực chữ ký (r,s) cho thông điệp m:

1. Kiểm tra r thỏa mãn 1<r<p. Nếu không, chữ ký không hợp lệ.
2. Tính:
   * = \* mod p,
   * = mod p.
3. Nếu = ​, chữ ký được xác nhận là hợp lệ.

Đặc điểm quan trọng

* Bảo mật cao: Dựa trên độ khó của bài toán logarith rời rạc, không có thuật toán hiệu quả nào hiện tại có thể giải bài toán này khi các tham số đủ lớn.
* Tính ngẫu nhiên: Mỗi lần ký một thông điệp, giá trị kkk được chọn ngẫu nhiên, đảm bảo rằng mỗi chữ ký là duy nhất ngay cả với cùng một thông điệp.
* Hiệu quả: Dễ dàng triển khai trong các hệ thống thực tế.

Ưu điểm của chữ ký số Elgamal

* Độ bảo mật cao: Khó phá vỡ nếu p lớn và g được chọn đúng cách.
* Thích hợp cho nhiều ứng dụng: Dùng trong các hệ thống yêu cầu bảo mật cao như giao dịch tài chính, trao đổi thông tin nhạy cảm.

Nhược điểm của chữ ký số Elgamal

* Chữ ký dài: Chữ ký là cặp (r,s), dẫn đến dung lượng lớn hơn so với RSA.
* Yêu cầu xử lý phức tạp hơn: Quá trình tính toán cần nhiều bước hơn RSA, nhất là khi chọn ngẫu nhiên k.

### 2.1.3. Hàm băm SHA

Giới thiệu sơ lược về hàm băm mật mã:

Hiểu theo nghĩa đơn giản, hàm băm là hàn cho tương ứng một mảng dữ liệu lớn với một mảng dữ liệu nhỏ hơn mà được dùng rộng rãi trong nhiều ứng dụng tin học, không chỉ phạm vi mật mã.

Trong mã hóa hàm băm được xem như là ảnh đại diện thu gọn của một dãy bit có độ dài hữu hạn tùy ý và được sử dụng để nhận diện cho chuỗi bit đó, kế hợp công cụ để tạo chữ ký số, cá hàm băm được dùng cho việc đảm bảo tính toàn vẹn của dữ liệu.

Định nghĩa:

- Hàm băm (Hash Function) là một hàm toán học chuyển đổi một thông điệp đầu vào có độ dài bất kỳ thành một dãy bit có độ dài quy định(tùy thuộc vào thuật toán hàm băm). Dãy bit này được gọi là thông điệp rút gọn, hay giá trị băm, đại diện cho thông điệp ban đầu

- Hàm băm là hàm một chiều mà neesy đưa một lượng dữ liệu bất kì qua hàm này sẽ cho ra một chuỗi số có độ dài cố định ở đầu ra

- hàm h(X) được gọi là hàm băm khi nó thỏa mãn 2 điều kiện sau:

+ Nén gọn: hàm h(x) tương ứng có chiều dài cố định n>0

+ Dễ tính toán: với mọi điều kiện chuỗi vit đầu vào x có chiều dài hữu hạn tùy ý,h(X) được tính toán dễ dàng.

Một hàm băm lý tưởng có các tính chất sau:

- Tính kháng tiền ảnh: với mọi đầu ra y cho trước không thể tìm được bất kỳ giá trị đầu vào x sao cho h(x) = y

- Tính kháng tiền ảnh thứ 2: Với mọi điều kiện vào x cho trước y=h(X), không thể tính toán để tìm ra được x’≠ sao cho h(x’) = h(x)

- Tính kháng xung đột: Không thể tính toán để tìm được 2 giá trị đầu vào x’ và x phân biệt sao cho h(x) = h(x’)

\* Phân loại hàm băm mật mã:

Dựa trên tham biến đầu vào của các hàm băm, các hàm băm mật mã được phân thành 2 lớp

- Lớp các hàm băm sử dụng khóa, chẳng hạn như Mac: nhận hai giá trị đầu vào

+ Thông điệp cần tính giá trị hàm băm

+ Khóa bí mật để băm văn bản theo đúng chuẩn quy định

- Lớp các hàm băm không sử dụng khóa:chỉ nhận vào một giá trị duy nhất là thông điệp

Trong lớp các hàm băm không sử dụng khóa thì MDCs. Lớp này lại chia thành các lớp nhỏ hơn

● Hàm băm một chiều: các hàm trong lớp này đều thảo mã tính chất là với mọi mã băm biết trước không thể tính toán được chuỗi bit đầu vào có mã băm bằng với mã băm đã cho

● Hàm băm kháng xung đột: các hàm trong lớp này thỏa mãn tính chất không thể tính toán để tìm ra hai chuỗi có cùng giá trị băm SHA hay thuật toán băm bảo mật là một họ những thuật toán băm mật mã do viện tiêu chuẩn và công nghệ Quốc gia (NIST) công bố thuộc tiêu chuẩn xử lý thông tin Liên Bang Hoa Kỳ (FIPS)[6,8,9]. Hiện tại có ba thuật toán SHA1, SHA2, SHA3 được định nghĩa.

Dưới đây là các thuật toán băm SHA:

- SHA 1

- SHA 2 (SHA - 224; SHA - 256; SHA - 384; SHA - 512)

- SHA 3 (SHA3 – 224; SHA3 – 256; SHA3 – 384; SHA3 – 512)

\* SHA1 & SHA2

Đối với SHA 1 và SHA – 256, thông điệp mở rộng được phân tích thành N khối 512 bitsM(1), M(2), …, M(N) . Do đó 512 bits của khối dữ liệu đầu vào có thể được thể hiện bằng 16 từ 32 – bits, M0 (i) chứa 32 bits đầu của khối thông điệp i, M1 (i) chứa 32 bits kế tiếp…

Đối với SHA 384, SHA – 512 thông điệp mở rộng được phân tích thành N khối 1024 bits M(1), M(2),.., M(N). Do đó 1024 bits của khối dữ liệu ban đầu vào có thể được thể hiện bằng 16 từ 64 bits, M0 (i) chứa 64bit đầu của khối thông điệp i, M1 (i) chứa 64 bits kế tiếp… M16 (i) chứa 64 bits cuối cùng.

Trước khi thực hiện băm, với mỗi thuật toán băm an toàn, giá trị băm ban đầu H (0) phải được thiết lập. Kích thước và số lượng từ trong H (0) tùy thuộc vào kích thước thông điệp rút gọn.

Các cặp thuật toán SHA – 224 và SHA – 256; SHA – 384 và SHA – 512 có các thao tác thực hiện giống nhau, chỉ khác nhau về số lượng bits kết quả của thông điệp rút gọn. Nói cách khác, SHA -224 sử dụng 224 bits đầu tiên trong kết quả thông điệp rút gọn sau khi áp dụng thuật toán SHA – 256. Tương tự SHA – 384 và SHA – 512 sử dụng 384 bits/512 bits đầu tiên trong kết quả thông điệp rút gọn.

\*Hàm băm SHA3

Thuật toán SHA -3 bao gồm:

Bốn dạng hàm băm mật mã là: SHA 3 -224, SHA3 – 256, SHA3 – 384, SHA3 – 512.

Hai dạng hàm băm mở rộng là: SHAKE-128, SHAKE- 256.

## 2.2. Nội dung thuật toán

### 2.2.1. Thuật toán sinh khóa Elgamal

1. Chọn tham số nhóm:

o Chọn một số nguyên tố lớn ppp sao cho bài toán logarith rời rạc trên ​ là khó giải quyết.

o Chọn một phần tử sinh ggg trong nhóm , nghĩa là g sinh ra tất cả các phần tử trong nhóm.

2. Sinh khóa bí mật và khóa công khai:

o Chọn một số nguyên xxx ngẫu nhiên (1<x<p−1), gọi là khóa bí mật.

o Tính y= mod p, gọi là khóa công khai.

3. Kết quả:

o Khóa bí mật: x.

o Khóa công khai: (p,g,y).

Lưu ý:

1. Kích thước p cần đủ lớn để đảm bảo tính bảo mật.
2. x phải được bảo mật và không tiết lộ, vì nó là yếu tố quyết định tính an toàn của hệ thống.

### 2.2.2. Thuật toán sinh chữ ký ElgamalĐể ký một thông điệp m, thực hiện các bước sau: 1. Chọn hàm băm: o Sử dụng một hàm băm an toàn, ví dụ: SHA-256, để ánh xạ thông điệp mmm thành giá trị băm h(m). 2. Tính giá trị băm của thông điệp: o h(m)=SHA−256(m). 3. Chọn số ngẫu nhiên: o Chọn một số nguyên ngẫu nhiên kkk sao cho 1<k<p−1 và gcd(k,p−1)=1. o kkk phải được thay đổi mỗi lần ký để đảm bảo tính ngẫu nhiên và bảo mật. 4. Tính chữ ký:

o Tính r = mod  p  
o Tính s=(h(m)−x\*r) \* mod (p−1), trong đó là nghịch đảo modular của k modulo (p−1).  
5. Kết quả:  
 o Chữ ký của m là cặp (r,s).

### 2.2.3. Thuật toán chứng thực chữ số Elgamal

Để kiểm tra tính hợp lệ của chữ ký (r,s) với thông điệp m:  
1. Xác định giá trị băm của thông điệp:  
o Tính h(m)=SHA−256(m).  
  
 2. Kiểm tra điều kiện hợp lệ của r:  
  
 o Nếu 1<r< p, tiếp tục, nếu không, chữ ký không hợp lệ.  
3. Tính giá trị kiểm tra:  
o Tính = \* mod p.  
o Tính = mod p.  
4. So sánh giá trị:  
o Nếu = ​, chữ ký hợp lệ.  
o Nếu ≠ ​, chữ ký không hợp lệ.  
Ý nghĩa các bước:  
1. Tính ngẫu nhiên:  
o Giá trị k thay đổi mỗi lần ký, đảm bảo rằng mỗi chữ ký đều khác nhau ngay cả khi thông điệp giống nhau.  
2. Hàm băm:  
o Sử dụng hàm băm (SHA-256) để đảm bảo rằng bất kỳ thay đổi nào trong thông điệp sẽ dẫn đến chữ ký khác biệt hoàn toàn.  
3. Bảo mật:  
 o Chữ ký chỉ có thể được tạo bởi người giữ khóa bí mật x, nhưng bất kỳ ai có khóa công khai (p,g,y) đều có thể xác minh tính hợp lệ.  
Quá trình này đảm bảo rằng chỉ có bên gửi có khóa bí mật mới có thể tạo ra chữ ký hợp lệ cho thông điệp, và người nhận có thể xác minh tính toàn vẹn của thông điệp đã được ký.  
Thêm vào đó, việc sử dụng hàm băm (ví dụ: SHA-256) đảm bảo tính duy nhất của chữ ký đối với mỗi thông điệp và bất kỳ thay đổi nhỏ nào trong thông điệp cũng sẽ dẫn đến một giá trị băm khác.  
Với việc bổ sung mục này, bạn có thể hoàn chỉnh mô tả về quá trình hoạt động của hệ thống RSA, bao gồm cả quá trình sinh khóa, sinh chữ ký và chứng thực chữ ký.

## 2.3.

### 2.3.1. Phương pháp tấn công

1. Tấn công dạng 1: Tìm cách xác định khóa bí mật  
1.1. Xác định khóa bí mật thông qua thông tin bị lộ:  
  
 - Nếu trong quá trình tạo khóa, các giá trị bí mật như p, g, hoặc x (khóa bí mật của người ký) bị lộ ra, kẻ tấn công có thể dễ dàng tái tạo chữ ký giả.  
- Giải pháp:  
o Quá trình tạo khóa phải được thực hiện trong môi trường bảo mật.  
  
 o Phải bảo mật chặt chẽ khóa bí mật x, đồng thời xóa các dữ liệu nhạy cảm sau khi sử dụng.  
1.2. Tấn công dựa trên phân tích logarit rời rạc:  
  
 - Kẻ tấn công cố gắng giải bài toán logarit rời rạc để tính toán giá trị x từ  
  
 y= mod p, trong đó g là cơ sở và p là số nguyên tố lớn.  
- Giải pháp:  
o Chọn giá trị p và g đủ lớn, thường là trên 2048 bit, để đảm bảo rằng việc giải logarit rời rạc là bất khả thi trong thời gian thực.  
1.3. Sử dụng các tham số có tính toán dễ bị khai thác:  
- Nếu p−1 có các ước nguyên tố nhỏ, kẻ tấn công có thể sử dụng thuật toán Pollard’s Rho để phân tích và tìm khóa bí mật.  
- Giải pháp:  
  
 o Chọn p sao cho p−1 có các ước nguyên tố lớn, tránh trường hợp dễ bị khai thác.  
2. Tấn công dạng 2: Giả mạo chữ ký (không cần khóa bí mật)  
  
 1. Tấn công dựa trên việc sử dụng lại giá trị k:  
  
 - Nếu người ký sử dụng lại giá trị k (số ngẫu nhiên trong quá trình tạo chữ ký), kẻ tấn công có thể khai thác thông tin này để tính khóa bí mật x.  
- Giải pháp:  
  
 o Đảm bảo rằng mỗi lần ký đều sử dụng một giá trị k ngẫu nhiên mới.  
  
 2. Tấn công thông qua lựa chọn giá trị k không thích hợp:  
  
 - Nếu k không thỏa mãn gcd(k, p−1)=1, kẻ tấn công có thể tính ngược được khóa bí mật hoặc làm mất tính an toàn của chữ ký.  
- Giải pháp:  
  
 o Luôn kiểm tra điều kiện gcd(k, p−1)=1 trước khi sử dụng giá trị k.  
3. Tấn công trên đường truyền:  
- Kẻ tấn công có thể giả mạo chữ ký bằng cách bắt gói tin, thay đổi chữ ký hoặc thông điệp.  
- Giải pháp:  
o Sử dụng cơ chế mã hóa an toàn để bảo vệ chữ ký và thông điệp trong quá trình truyền tải.  
o Kết hợp các biện pháp xác thực để đảm bảo tính toàn vẹn.

### 2.3.2. Đánh giá mức độ phức tạp thuật toán

- Phức tạp tính toán của tạo cặp khóa:  
o Phụ thuộc vào bài toán logarit rời rạc.  
o Độ phức tạp: O(), trong đó kkk là số bit của ppp.  
- Phức tạp tính toán của tạo chữ ký số:  
o Phép toán lũy thừa modulo: O().  
o Phép toán ngẫu nhiên kkk: O(k).  
o Tổng độ phức tạp: O().  
- Phức tạp tính toán của xác minh chữ ký số:  
o Phép toán lũy thừa modulo: O().  
o Phép toán so sánh: O(1).  
o Tổng độ phức tạp: O().

### 2.3.3. **Ưu nhược điểm**

- Ưu điểm:  
+ Tính bảo mật cao:  
o Dựa trên bài toán logarit rời rạc, rất khó để giải quyết trong thời gian thực nếu các tham số được chọn đúng cách.  
+ Tính linh hoạt:  
o Có thể áp dụng cho nhiều loại dữ liệu khác nhau, bao gồm văn bản, hình ảnh, và dữ liệu nhị phân.  
+ Hiệu quả:  
o Việc tạo và xác minh chữ ký có tốc độ nhanh hơn một số thuật toán khác, như RSA.  
- Nhược điểm:  
+ Kích thước chữ ký lớn:  
o Chữ ký ElGamal thường lớn hơn các chữ ký của thuật toán RSA, gây ra tốn kém về lưu trữ và băng thông.  
  
 + Sử dụng lại giá trị **kk**k dẫn đến rủi ro:  
o Việc sử dụng lại hoặc chọn **kk**k không ngẫu nhiên có thể làm lộ khóa bí mật.  
+ Chi phí tính toán cao:  
o Dù nhanh hơn RSA trong một số trường hợp, ElGamal vẫn có chi phí tính toán đáng kể đối với các hệ thống lớn.

**2.3.4. Hướng phát triển**- Tính khả thi của chủ đề nghiên cứu: Với những kiến thức đã được giảng viên cung cấp sẵn trong quá trình học tập, đồng thời với những kinh nghiệm, kiến thức tổng hợp về các học phần đã được học từ trước, việc thực hiện đề tài là hoàn toàn khả thi. Tuy nhiên, không chỉ bao gồm những kiến thức đã được dạy, sinh viên cũng cần phải tìm tòi, tham khảo các loại tài liệu khác nhau để đưa ra được kết quả cuối cùng một cách hoàn thiện và đạt được các yêu cầu mà bài toán đưa ra.  
- Thuận lợi, khó khăn trong quá trình nghiên cứu:  
+ Thuận lợi:  
o Có được những kiến thức cơ bản thực hiện đề tài được giảng viên cung cấp trước đó.  
o Có đủ thời gian nghiên cứu để triển khai đề tài được giao.  
o Giao tiếp, trao đổi giữa các thành viên trong nhóm rất tốt.  
+ Khó khăn:  
o Cần học thêm nhiều kiến thức bên ngoài để xây dựng được một chương trình với giao diện hoàn chỉnh.  
- Hướng phát triển và mở rộng của đề tài:  
+ Cá nhân hóa: Kết hợp với lưu trữ dữ liệu bằng hệ quản trị dữ liệu để tang tính bảo mật, thêm chức năng đăng nhập tài khoản để cá nhân hóa cho từng người đồng thời giúp cho phần mềm có thể sử dụng cho nhiều người  
 + Phát triển phần mềm cho nhiều người sử dụng: Không chỉ cho một người sử dụng, phần mềm có thể phát triển thêm để ứng dụng có thể gửi và nhận thông tin từ các tài khoản khác nhau. Gửi thông tin cho người ta muốn gửi thông qua mã định danh cá nhân tài khoản của người dùng mà ta muốn gửi cung cấp.  
+ Triển khai đa nền tảng: biến chương trình đã thực hiện xây dựng và chạy được trên đa nền tảng, giúp việc truyền tải thông tin không chỉ trên một loại thiết bị mà có thể thực hiện trên loại thiết bị khác nhau.  
+ Xây dựng cổng thông tin trao đổi thông tin giữa các cơ quan, tổ chức với nhau.  
+ Kết hợp với các phần mềm ứng dụng khác để xác nhận người dùng, tính toàn vẹn của dữ liệu và trách nhiệm của mỗi bên như trong các phần mềm với các hoạt động: mua bán, đặt hàng trực tuyến; thanh toán trực tuyến; giao dịch online; giao dịch ngân hàng; giao dịch email; …

2.4. Thiết kế chương trình, cài đặt thuật toán. Dương, Dũng (Hạn: thứ 5 tuần sau)

* Thiết kế kịch bản chương trình
* Giới thiệu ngôn ngữ lập trình sử dụng để cài đặt thuật toán.
* Cài đặt thuật toán, giao diện chương trình (theo từng ngôn ngữ)

**Chương 3: Kết luận và bài học kinh nghiệm**

* 1. Kiến thức kỹ năng đã học được trong quá trình thực hiện đề tài.
  2. Bài học kinh nghiệm
  3. Đề xuất về tính khả thi của chủ đề nghiên cứu, những thuận lợi, khó khăn …

**Tài liệu tham khảo**

(Sắp xếp theo ngôn ngữ: Việt, Anh, Pháp, Đức, Nga…)

[1]. Nguyễn Xuân Dũng, *Bảo mật thông tin – Mô Hình và ứng dụng*, NXB thống kê, 2009.

[2]. Bùi Doãn Khanh, Nguyễn Đình Thúc, *Mã hóa thông tin – Lý thuyết và ứng dụng*, NXB Lao động xã hội, 2011.

[3]. William Stallings**,** *Cryptography and Network Security Principles and Practices***,** Fourth Edition, Prentice Hall, 2005.

…

[n]. <http://www.hhs.com>

(thời gian truy cập: 15h00, ngày 27/10/2024)

**Phụ lục 1: Chương trình Java**

**Phụ lục 2: Chương trình C#**

**Quy định trình bày báo cáo:**

Lề trên: 2,5 cm Lề dưới: 2 cm

Lề trái: 3,5 cm lề phải: 2 cm

Nội dung báo cáo trình bày: căn đều lề 2 bên

Phông chữ: Time New Roman

Cỡ chữ: 13 (hoặc 14)

Dãn dòng: Multiple 1.3

Các đoạn báo cáo căn đều 2 bên

Đánh số trang ở giữa, phía trên đầu mỗi trang giấy (phần Header)

Số lượng trang báo cáo: từ 40 - 60 trang