**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ ĐÔNG Á**

**KHOA: CÔNG NGHỆ THÔNG TIN**



**BÀI TẬP LỚN**

**HỌC PHẦN: <TÊN HỌC PHẦN>**

**Chủ đề …: <Tên chủ đề>**

**Đề tài số …: <Tên đề tài>**

|  |  |  |
| --- | --- | --- |
| **Sinh viên thực hiện** | **Lớp** | **Khóa** |
| **Nguyyễn Thanh Hải** | **DCCNTT13.10.7** | **K13** |
| **Hoàng Minh Quang** | **DCCNTT13.10.7** | **K13** |
|  | **DCCNTT13.10.7** | **K13** |
|  | **DCCNTT13.10.7** | **K13** |
|  | **DCCNTT13.10.7** | **K13** |

**Bắc Ninh, năm 2024**

**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ ĐÔNG Á**

**KHOA: CÔNG NGHỆ THÔNG TIN**

**BÀI TẬP LỚN**

**HỌC PHẦN: <TÊN HỌC PHẦN>**

**Chủ đề …: <Tên chủ đề>**

**Đề tài số …: <Tên đề tài>**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STT** | **Sinh viên thực hiện** | **Mã sinh viên** | **Điểm bằng số** | **Điểm bằng chữ** |
| **1** |  |  |  |  |
| **2** |  |  |  |  |
| **3** |  |  |  |  |
| **4** |  |  |  |  |
| **5** |  |  |  |  |

|  |  |
| --- | --- |
| **CÁN BỘ CHẤM 1**  *(Ký và ghi rõ họ tên)* | **CÁN BỘ CHẤM 2**  *(Ký và ghi rõ họ tên)* |

# MỤC LỤC

Contents

[MỤC LỤC 3](#_Toc178450732)

[CHƯƠNG 1: TỔNG QUAN VỀ MÃ HÓA VÀ GIẢI MÃ 5](#_Toc178450733)

[1.1 Giới Thiệu về Mã Hóa và Giải Mã: 5](#_Toc178450734)

[1.2 Các Phương Pháp Mã Hóa Cơ Bản 5](#_Toc178450735)

[1.3 Ý Nghĩa của Mã Hóa và Giải Mã 6](#_Toc178450736)

[1.4 Các khái niệm liên quan khác 7](#_Toc178450737)

[1.5 Các thành phần của hệ mật mã 8](#_Toc178450738)

[1.6 Phân loại hệ mật mã 9](#_Toc178450739)

[1.7 Tiêu chuẩn đánh giá hệ mật mã 11](#_Toc178450740)

[CHƯƠNG 2: MÃ HÓA AFFINE CIPHER 13](#_Toc178450741)

[2.1 Cơ sở lý thuyết của mã hóa Affine Cipher: 13](#_Toc178450742)

[2.2 Mô Hình Toán Học 14](#_Toc178450743)

[2.3Tính Chất và Đặc Điểm. 16](#_Toc178450744)

[2.4 Các Yếu Tố Ảnh Hưởng Đến Tính Bảo Mật 17](#_Toc178450745)

[2.5 Phương Pháp Tấn Công: 17](#_Toc178450746)

[CHƯƠNG 3: XÂY DỰNG ỨNG DỤNG MÃ HÓA AFFINE TRONG TRUYỀN NHẬN THÔNG TIN 18](#_Toc178450747)

[3.1 Mục Tiêu Xây Dựng. 18](#_Toc178450748)

[3.2 Phân Tích Yêu Cầu 18](#_Toc178450749)

[3.3 Thiết Kế Ứng Dụng Mã Hóa Affine cho Tin Nhắn Văn Bản 19](#_Toc178450750)

[3.4 Thực Hiện Mã Hóa và Giải Mã 20](#_Toc178450751)

[3.5 Tích Hợp với Hệ Thống Truyền Thông 23](#_Toc178450752)

[3.6 Đánh Giá và Hiệu Chỉnh 26](#_Toc178450753)

[CHƯƠNG 4: THỰC NGHIỆM VÀ ĐÁNH GIÁ 27](#_Toc178450754)

[4.1 Xây Dựng và Thực Hiện Các Thí Nghiệm: 27](#_Toc178450755)

[4.2 Các Bài Toán Thực Nghiệm 27](#_Toc178450756)

[4.3 Phân Tích Kết Quả 31](#_Toc178450757)

[4.4 Kết Luận và Đề Xuất 33](#_Toc178450758)

[Kết luận 35](#_Toc178450759)

[CHƯƠNG 5: TỔNG KẾT 36](#_Toc178450760)

[5.1 Kết Quả Đạt Được 36](#_Toc178450761)

[5.2 Khó Khăn và Hạn Chế 36](#_Toc178450762)

[5.3 Hướng Phát Triển 36](#_Toc178450763)

[Kết Luận 37](#_Toc178450764)

[Tài Liệu Tham Khảo 38](#_Toc178450765)

# CHƯƠNG 1: TỔNG QUAN VỀ MÃ HÓA VÀ GIẢI MÃ

## 1.1 Giới Thiệu về Mã Hóa và Giải Mã:

Lịch Sử của Mã Hóa và Giải Mã

**Thời kỳ cổ đại**: Mã hóa đã được sử dụng từ thời kỳ cổ đại để bảo vệ thông tin. Một trong những phương pháp mã hóa sớm nhất là mã hóa Caesar, được Julius Caesar sử dụng để bảo vệ các thông điệp quân sự của ông. Phương pháp này thay đổi mỗi ký tự trong thông điệp bằng cách dịch chuyển nó một số vị trí nhất định trong bảng chữ cái.

**Thế kỷ 19 và 20**: Với sự phát triển của các chiến tranh thế giới, mã hóa và giải mã trở nên rất quan trọng trong các chiến lược quân sự. Các phương pháp như mã hóa Vigenère, mã hóa Enigma, và các máy mã hóa cơ học được phát triển để bảo vệ thông tin.

**Kỷ nguyên số**: Với sự phát triển của công nghệ máy tính, mã hóa đã trở thành một lĩnh vực quan trọng trong an ninh mạng. Các thuật toán mã hóa hiện đại như AES (Advanced Encryption Standard) và RSA (Rivest-Shamir-Adleman) được phát triển để đảm bảo bảo mật thông tin trong thế giới số.

**Mật mã học**: Gắn liền với quá trình mã hóa nghĩa là chuyển đổi thông tin từ dạng "có thể hiểu được" thành dạng "không thể hiểu được" và ngược lại là quá trình giải mã là việc chuyển bản tin đã được mã hóa về bản tin gốc bằng khóa giải mã . Quá trình mã hóa và giải mã được đặc trưng bởi hình sau:

## 1.2 Các Phương Pháp Mã Hóa Cơ Bản

**Mã Hóa Thay Thế (Substitution Cipher)**: Là phương pháp thay thế mỗi ký tự trong thông điệp bằng một ký tự khác theo một quy tắc nhất định. Ví dụ: mã hóa Caesar và mã hóa Vigenère. Có 4 kỹ thuật thay thế sau đây:

**Thay thế đơn (A simple substitution cipher)**

**Thay thế đồng âm (A homophonic substitution cipher)**

**Thay thế đa mẫu tự (A polyalphbetic substitution cipher)**

**Thay thế đa sơ đồ (A polygram substitution cipher)**

**Mã Hóa Hoán Đổi (Transposition Cipher)**: Là phương pháp thay đổi vị trí của các ký tự trong thông điệp mà không thay đổi chính ký tự đó. Ví dụ: mã hóa ma trận.

**Mã Hóa Affine**: Là một loại mã hóa thay thế mà mỗi ký tự được mã hóa bằng công thức affine (hàm bậc nhất). Phương pháp này sử dụng hai khóa (a và b) để mã hóa và giải mã.

**Mã Hóa Đối Xứng (Symmetric Encryption)**: Sử dụng cùng một khóa để mã hóa và giải mã thông tin. Các thuật toán như DES (Data Encryption Standard) và AES là ví dụ điển hình.

**Mã Hóa Bất Đối Xứng (Asymmetric Encryption)**: Sử dụng hai khóa khác nhau - một khóa công khai để mã hóa và một khóa riêng tư để giải mã. RSA là một ví dụ điển hình.

**Mã Hóa Hòa Tan (Stream Cipher) và Mã Hóa Khối (Block Cipher)**: Stream cipher mã hóa dữ liệu từng bit hoặc byte một, trong khi block cipher mã hóa dữ liệu theo từng khối cố định.

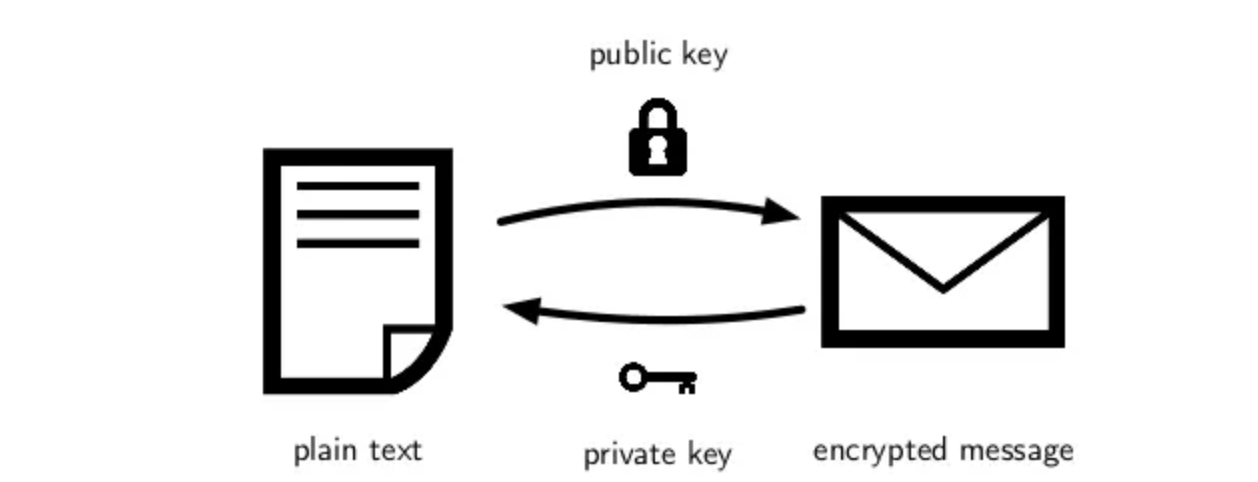
## 1.3 Ý Nghĩa của Mã Hóa và Giải Mã

**Bảo mật thông tin**: Mã hóa là quá trình chuyển đổi thông tin từ dạng dễ hiểu thành dạng không thể đọc được mà không có khóa giải mã. Điều này giúp bảo vệ thông tin khỏi bị truy cập trái phép và đảm bảo rằng chỉ những người có quyền mới có thể truy cập vào thông tin đó.

**Xác thực và Toàn vẹn**: Mã hóa cũng giúp xác thực danh tính của người gửi và đảm bảo rằng thông tin không bị thay đổi trong quá trình truyền tải. Điều này rất quan trọng trong các giao dịch trực tuyến và các hệ thống an ninh mạng.

**Bảo vệ quyền riêng tư**: Trong thời đại số, bảo vệ quyền riêng tư cá nhân là rất quan trọng. Mã hóa giúp bảo vệ dữ liệu cá nhân và thông tin nhạy cảm khỏi bị đánh cắp hoặc lạm dụng.

## 1.4 Các khái niệm liên quan khác



**Bản rõ (Plaintext)**: Dạng ban đầu của thông báo.

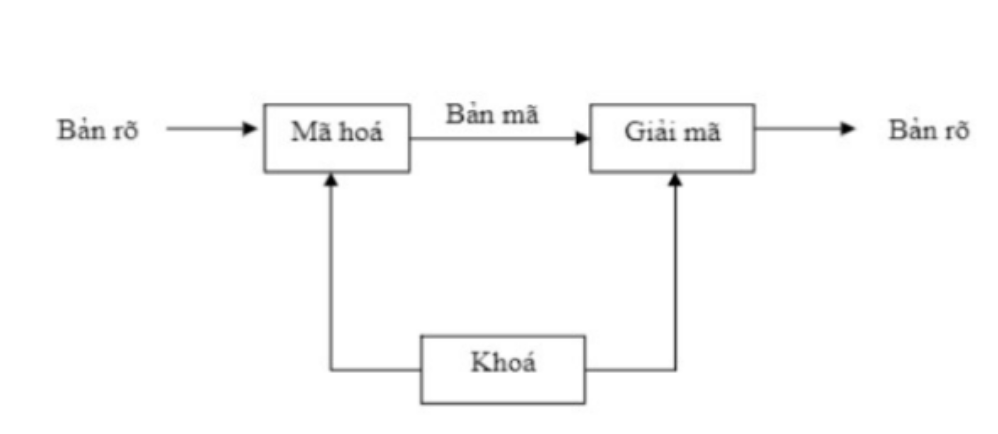
**Bản mã (Ciphertext):** Dạng mã của bản rõ ban đầu.

**Khóa (Key):** thông tin tham số dùng để mã hóa.

**Mã hóa (Encryption):** Quá trình biến đổi thông tin từ dạng bản rõ sang bản mã bằng khóa hoặc không cần khóa.

**Giải mã (Decryption):** Quá trình ngược lại biến đổi thông tin từ dạng bản mã sang bản rõ

## 1.5 Các thành phần của hệ mật mã



**Việc mã hóa hay giải mã theo quy tắc nhất định** : quy tắc đó được gọi là hệ mật mã. Định nghĩa : Một hệ mật là một bộ 5 (P,C,K,E,D) thoả mãn các điều kiện sau:

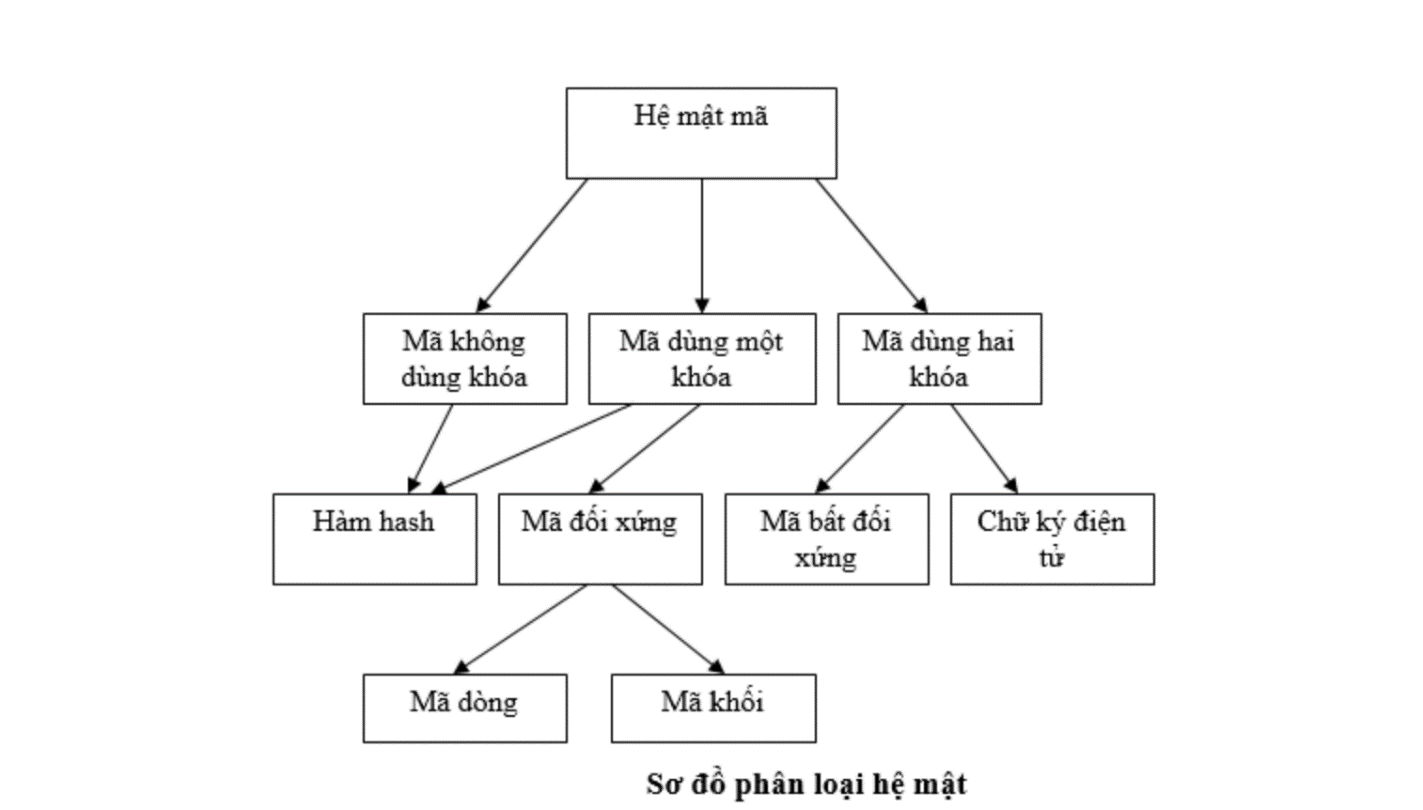
**P:** là một tập hợp hữu hạn các bản rõ (PlainText), nó được gọi là không gian bản rõ.

**C là tập các hữu hạn các bản mã** (Crypto), nó còn được gọi là không gian các bản mã. Mỗi phần tử của C có thể nhận được bằng cách áp dụng phép mã hoá Ek lên một phần tử của P, với k ∈ K.

**K là tập hữu hạn các khoá** hay còn gọi là không gian khoá. Đối với mỗi phần tử k của K được gọi là một khoá (Key). Số lượng của không gian khoá phải đủ lớn để “kẻ địch”: không có đủ thời gian để thử mọi khoá có thể(phương pháp vét cạn).

Đối với mỗi k ∈ K có một quy tắc mã eK: P → C và một quy tắc giải mã tương ứng dK ∈ D. Mỗi eK: P → C và dK: C → P là những hàm mà: dK (eK(x))=x với mọi bản rõ x ∈ P

## 1.6 Phân loại hệ mật mã



Có nhiều cách phân loại hệ mật mã, và chúng có thể được phân loại theo các tiêu chí khác nhau. Dưới đây là phân loại hệ mật mã theo cách truyền khóa, thời gian ra đời, và phương pháp mã hóa:

*Phân loại theo cách truyền khóa.*

**Hệ mật mã đối xứng (Mật mã khóa bí mật)**

**Đặc điểm**: Sử dụng cùng một khóa cho cả quá trình mã hóa và giải mã dữ liệu.

**Yêu cầu**: Khóa phải được giữ bí mật tuyệt đối để đảm bảo an toàn cho thông tin.

**Hệ mật mã bất đối xứng (Mật mã khóa công khai)**

**Đặc điểm**: Sử dụng hai khóa khác nhau cho mã hóa và giải mã. Một khóa (khóa công khai) dùng để mã hóa, và khóa còn lại (khóa bí mật) dùng để giải mã.

**Yêu cầu**: Khóa công khai có thể được công bố, nhưng khóa bí mật cần được giữ kín. Các khóa này tạo thành các cặp chuyển đổi ngược nhau và không thể suy ra khóa này từ khóa kia.

*Phân loại theo thời gian ra đời*

**Mật mã cổ điển**

**Đặc điểm**: Các hệ mật mã đã được phát triển trước năm 1970.

**Mật mã hiện đại**

**Đặc điểm**: Các hệ mật mã được phát triển sau năm 1970.

**3. Phân loại theo cách thức mã hóa**

**Mã dòng**

**Đặc điểm**: Mã hóa từng bit hoặc byte của dữ liệu một cách liên tục. Mỗi bit hoặc byte được mã hóa bằng một khóa sinh ra từ hàm sinh khóa, được gọi là dòng khóa.

**Mã khối**

**Đặc điểm**: Mã hóa dữ liệu theo từng khối cố định. Mỗi khối dữ liệu được mã hóa bằng cùng một khóa.

Những phân loại này giúp hiểu rõ hơn về cách các hệ mật mã hoạt động và ứng dụng của chúng trong bảo mật thông tin.

## 1.7 Tiêu chuẩn đánh giá hệ mật mã

Để đánh giá một hệ mật mã người ta thường đánh giá thông qua các tính chất sau:

*Độ an toàn:*

Một hệ mật được đưa vào sử dụng điều đầu tiên phải có độ an toàn cao. Ưu điểm của mật mã là có thể đánh giá được độ an toàn thông qua độ an toàn tính toán mà không cần phải cài đặt. Một hệ mật được coi là an toàn nếu để phá hệ mật mã này phải dùng n phép toán. Mà để giải quyết n phép toán cần thời gian vô cùng lớn, không thể chấp nhận được. Một hệ mật mã được gọi là tốt thì nó cần phải đảm bảo các tiêu chuẩn sau:

Chúng phải có phương pháp bảo vệ mà chỉ dựa trên sự bí mật của các khoá, công khai thuật toán.

Khi cho khoá công khai eK và bản rõ P thì chúng ta dễ dàng tính được eK(P) = C. Ngược lại khi cho dK và bản mã C thì dễ dàng tính được dK(M)=P. Khi không biết dK thì không có khả năng để tìm được M từ 16 C, nghĩa là khi cho hàm f: X → Y thì việc tính y=f(x) với mọi x ∈ X là dễ còn việc tìm x khi biết y lại là vấn đề khó và nó được gọi là hàm một chiều.

Bản mã C không được có các đặc điểm gây chú ý, nghi ngờ . Khi đánh giá hệ mật mã chúng ta phải chú ý đến tốc độ mã và giải mã. Hệ mật tốt thì thời gian mã và giải mã nhanh.

*Phân phối khóa:*

Một hệ mật mã phụ thuộc vào khóa, khóa này được truyền công khai hay truyền khóa bí mật. Phân phối khóa bí mật thì chi phí sẽ cao hơn so với các hệ mật có khóa công khai. Vì vậy đây cũng là một tiêu chí khi lựa chọn hệ mật mã

**1.8 Phạm Vi Nghiên Cứu:**

**Nội Dung Nghiên Cứu:** Nghiên cứu và phân tích mã hóa và giải mã Affine trong ứng dụng truyền nhận thông tin, tập trung vào việc hiểu cơ chế hoạt động và áp dụng trong các hệ thống truyền thông số.

**Giới Hạn Nghiên Cứu:** Nghiên cứu sẽ không bao gồm các phương pháp mã hóa hiện đại như AES hoặc RSA, cũng như các ứng dụng không liên quan đến truyền thông số, chẳng hạn như mã hóa trong bảo mật phần cứng.

**Lý Do Chọn Phạm Vi:** Mã hóa Affine là một phương pháp cơ bản và dễ hiểu, phù hợp để nghiên cứu các nguyên tắc cơ bản của mã hóa và giải mã trong truyền thông số. Việc tập trung vào phương pháp này giúp làm sáng tỏ những nguyên lý cơ bản mà không bị phân tâm bởi các kỹ thuật mã hóa phức tạp hơn.

# CHƯƠNG 2: MÃ HÓA AFFINE CIPHER

## 2.1 Cơ sở lý thuyết của mã hóa Affine Cipher:

Công Thức Mã Hóa và Giải Mã, Mô Hình Toán Học

Mã hóa Affine là một phương pháp mã hóa thay thế đơn giản nhưng hiệu quả, sử dụng các phép toán số học trong một hệ thống modulo. Dưới đây là các nguyên tắc cơ bản, công thức mã hóa và giải mã, cũng như mô hình toán học của mã hóa Affine.

*Công Thức Mã Hóa và Giải Mã*

**Mã Hóa**

Để mã hóa một ký tự x (biểu diễn dưới dạng số nguyên) thành ký tự y công thức mã hóa Affine được sử dụng là:

|  |
| --- |
| y=(a\*x+b) mod m |

Trong đó:

* a và b là các khóa bí mật, với aaa phải là số nguyên nguyên tố với m (tức là a và m phải là số nguyên tố với nhau, ký hiệu là gcd(a,m)=1
* x là giá trị số của ký tự cần mã hóa (thường được chuyển đổi từ ký tự sang số theo bảng chữ cái, ví dụ: 'A' = 0, 'B' = 1, ..., 'Z' = 25 cho bảng chữ cái tiếng Anh).
* m là kích thước của bảng ký tự (ví dụ: 26 cho bảng chữ cái tiếng Anh).

**Giải Mã**

Để giải mã ký tự y thành ký tự gốc x, công thức giải mã Affine được sử dụng là:

|  |
| --- |
| x=a-1. (y –b) mod m |

Trong đó:

* a-1 là nghịch đảo của a modulo m. Nghịch đảo này là số nguyên a-1 sao cho a. a-1 ≡ 1 mod m . Nghịch đảo này có thể được tính bằng thuật toán Euclid mở rộng.

## 2.2 Mô Hình Toán Học

Mã hóa Affine hoạt động trong không gian số học modulo. Đây là cách mô hình hóa và tính toán trong phương pháp mã hóa này:

1. **Bảng Chữ Cái và Không Gian Modulo:**
   * Mã hóa Affine làm việc với một bảng chữ cái có m ký tự, thường là 26 ký tự trong bảng chữ cái tiếng Anh. Mỗi ký tự được ánh xạ thành một số nguyên từ 0 đến m−1.
2. **Nhóm Toán Học:**
   * Mã hóa Affine sử dụng các phép toán trong một nhóm toán học, cụ thể là nhóm các số nguyên modulo m với phép nhân và phép cộng. Nhóm này phải có tính chất là "nhóm Abel" (nhóm cộng).
3. **Khóa và Nghịch Đảo:**
   * Để đảm bảo mã hóa và giải mã chính xác, a phải là số nguyên nguyên tố với m. Điều này đảm bảo rằng phép toán modulo có thể được thực hiện mà không gặp phải vấn đề không khả thi trong giải mã.
   * Nghịch đảo a-1 là rất quan trọng cho quá trình giải mã. Nghịch đảo modulo có thể được tính bằng thuật toán Euclid mở rộng, đảm bảo rằng mỗi giá trị a có một giá trị nghịch đảo duy nhất.

*Ví Dụ Minh Họa*

Giả sử bạn sử dụng bảng chữ cái tiếng Anh (26 ký tự) với khóa a = 5 và b = 8:

Để mã hóa ký tự 'A' (với giá trị số là 0):

y=(5.0+8) mod 26 = 8

Ký tự mã hóa tương ứng là 'I'.

Để giải mã ký tự 'I' (với giá trị số là 8):

Tính nghịch đảo của a 5 modulo 26. Nghịch đảo là 21

x=21 . (8 –8) mod 26 = 0

Ký tự giải mã tương ứng là 'A'.

## 2.3Tính Chất và Đặc Điểm.

*Đặc Điểm của Mã Hóa Affine*

**1. Đơn Giản và Dễ Thực Hiện:**

* Mã hóa Affine rất đơn giản và dễ thực hiện nhờ vào công thức toán học cơ bản. Chỉ cần thực hiện phép nhân, phép cộng, và phép modulo để mã hóa và giải mã thông tin.

**2. Tính Tương Quá Tương Đương (Inversibility):**

* Mã hóa Affine là một phương pháp mã hóa một-một, nghĩa là mỗi ký tự gốc được ánh xạ đến một ký tự mã hóa duy nhất, và ngược lại. Điều này cho phép phục hồi thông tin gốc từ thông tin mã hóa một cách chính xác.

**3. Đối Xứng:**

* Mã hóa và giải mã đều sử dụng các phép toán toán học cơ bản với khóa bí mật. Việc này đồng nghĩa với việc quy trình mã hóa và giải mã là tương tự nhau, với một khóa bí mật (a và b) cần được bảo vệ.

**4. Số Lượng Ký Tự Có Thể Mã Hóa:**

* Mã hóa Affine hoạt động trong không gian modulo, thường là bảng chữ cái hoặc một tập hợp các ký tự. Số lượng ký tự có thể mã hóa phụ thuộc vào giá trị của m, ví dụ, bảng chữ cái tiếng Anh có m=26 ký tự.

## 2.**4** Các Yếu Tố Ảnh Hưởng Đến Tính Bảo Mật

**1. Khóa Bí Mật (a và b):**

* **Khóa a**: Để mã hóa Affine an toàn, a phải là một số nguyên nguyên tố với m. Nếu không, một số ký tự có thể ánh xạ đến cùng một ký tự mã hóa, làm giảm tính bảo mật.
* **Khóa b**: Khóa b là một giá trị được thêm vào trong quá trình mã hóa. Khóa này không ảnh hưởng đến tính bảo mật theo cách cơ bản nhưng vẫn cần được giữ bí mật để bảo vệ thông tin.

**2. Kích Thước Bảng Ký Tự (m):**

* Kích thước bảng ký tự m có ảnh hưởng đến tính bảo mật của mã hóa. Mã hóa Affine trong bảng chữ cái tiếng Anh (26 ký tự) có thể dễ dàng bị phá vỡ bằng phương pháp phân tích tần suất, vì phân phối tần suất của các ký tự trong văn bản mã hóa vẫn giữ nguyên.

**3. Phân Tích Tần Suất:**

* Do mã hóa Affine là một loại mã hóa thay thế, tần suất xuất hiện của các ký tự trong văn bản mã hóa có thể phản ánh tần suất xuất hiện của các ký tự trong văn bản gốc. Điều này làm cho mã hóa Affine dễ bị tấn công bằng phương pháp phân tích tần suất.

**4. Tính Toàn Vẹn:**

* Mã hóa Affine không cung cấp tính toàn vẹn của dữ liệu, nó chỉ bảo vệ tính bảo mật. Do đó, các phương pháp mã hóa hiện đại thường kết hợp mã hóa với các phương pháp bảo mật khác để đảm bảo toàn vẹn và chứng thực thông tin.

## 2.****5 Phương Pháp Tấn Công:****

**Tấn Công Phân Tích Tần Suất:** Như đã đề cập, mã hóa Affine dễ bị tấn công bằng phương pháp phân tích tần suất. Kẻ tấn công có thể phân tích tần suất xuất hiện của các ký tự trong văn bản mã hóa để xác định các quy tắc mã hóa và giải mã.

**Tấn Công Brute Force:** Vì số lượng khóa có thể là hạn chế (dựa trên kích thước của bảng ký tự và các giá trị của a và b), kẻ tấn công có thể thực hiện tấn công brute force để thử tất cả các kết hợp khóa có thể.

# **CHƯƠNG** 3: XÂY DỰNG ỨNG DỤNG MÃ HÓA AFFINE TRONG TRUYỀN NHẬN THÔNG TIN

## ****3.1 Mục Tiêu Xây Dựng.****

**Bảo Vệ Nội Dung Tin Nhắn:** Đảm bảo rằng các tin nhắn văn bản được bảo mật thông qua mã hóa trước khi gửi đi và có thể giải mã khi nhận.

**Đơn Giản Hóa Quy Trình:** Cung cấp một phương pháp mã hóa và giải mã đơn giản và dễ dàng tích hợp vào các hệ thống tin nhắn hiện có.

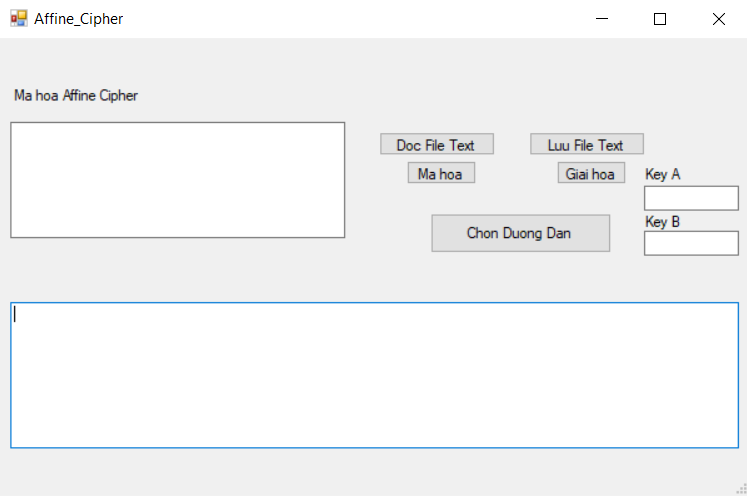
## ****3.2 Phân Tích Yêu Cầu****

**Tính Chính Xác và An Toàn:** Đảm bảo rằng thông điệp mã hóa có thể được giải mã chính xác bởi người nhận mà không bị thay đổi.

**Hiệu Suất:** Đánh giá thời gian mã hóa và giải mã để đảm bảo không làm giảm hiệu suất của hệ thống truyền thông.

## ****3.3 Thiết Kế Ứng Dụng Mã Hóa Affine cho Tin Nhắn Văn Bản****

**Xây Dựng Giao Diện Người Dùng (UI):**



**Nhập Tin Nhắn:** Cung cấp một ô nhập để người dùng gõ tin nhắn cần mã hóa.

**Nhập Khóa Mã Hóa:** Cung cấp các ô nhập để người dùng nhập khóa bí mật (a và b).

**Hiển Thị Kết Quả:** Hiển thị tin nhắn đã mã hóa và tin nhắn giải mã.

**Xử Lý Dữ Liệu:**

**Mã Hóa:** Áp dụng thuật toán mã hóa Affine để mã hóa tin nhắn khi người dùng nhấn nút gửi.

**Giải Mã:** Áp dụng thuật toán giải mã Affine để giải mã tin nhắn khi người dùng nhận.

## 3.4 ****Thực Hiện Mã Hóa và Giải Mã****

**Giả sử mã hóa và giải mã thông điệp "HELLO" sử dụng mã hóa Affine với các khóa:**

**Sử dụng bảng chữ cái tiếng Anh với m = 26., a=5 và b=8.**

***Mã Hóa Tin Nhắn:***

**Bước 1: Chuyển đổi các ký tự thành giá trị số**

**Sử dụng bảng chữ cái tiếng Anh:**

**A = 0, B=1, C = 2,... Z = 25**

**Vì vậy:**

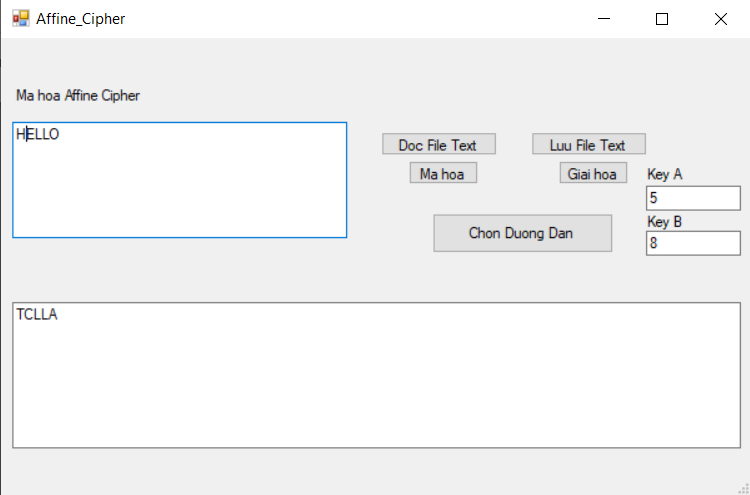
**H=7**

**E=4**

**L=11**

**O = 14**

**Thông điệp "HELLO" trở thành các số: 7, 4, 11, 11, 14**



***Giải Mã Tin Nhắn:***

Bước 1: Tính nghịch đảo của a modulo 771

Để giải mã, cần tỉnh nghịch đảo của a modulo m. Đối với a = 5 và m = 26, nghịch đảo a-1 được tỉnh bằng thuật toán Euclid mở rộng hoặc bằng cách thử nghiệm.

Nghịch đảo của 5 modulo 26 là 21, vì: 5 . 21 mod 26 = 105 mod 26 = 1

Bước 2: Áp dụng công thức giải mã

Công thức giải mã Affine là:

|  |
| --- |
| x = a-1 . (y - b) mod m |

Áp dụng với a-1 = 21 và b = 8:

• Giải mã T (17): x=21.(17-8) mod 26=21.9 mod 26=189 mod 26 = 7 (H= 7)

• Giải mã C (2): x=21.(2-8) mod 26=21.(-6) mod 26=126 mod 26 = 4 (E = 4)

• Giải mã L (11): x=21.(11-8) mod 26=21.3 mod 26=63 mod 26 = 11 (L = 11)

• Giải mã L (11): x=21.(11-8) mod 26 = 11 (L = 11)

• Giải mã A (0): x=21.(0-8) mod 26=21.(-8) mod 26=-168 mod 26=14 (0 = 14)

Thông điệp sau khi giải mã trở lại là "HELLO".

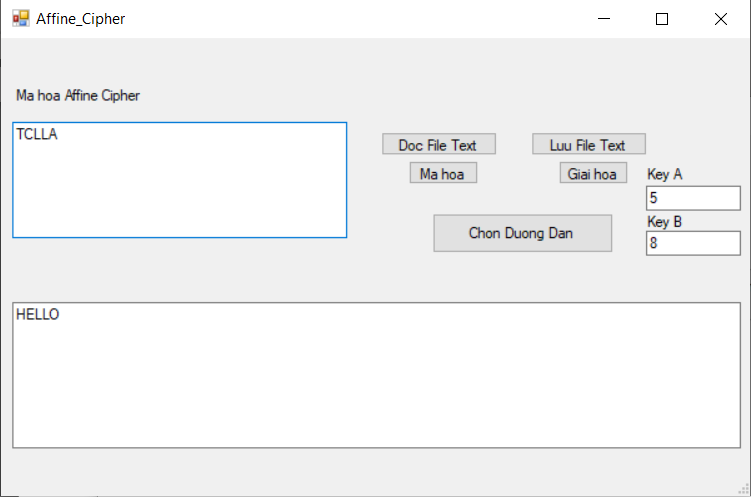
Tóm Tắt

Thông điệp gốc: "HELLO"

Khóa mã hóa: a = 5,b = 8

Thông điệp mã hóa: "TCLLA"

Thông điệp giải mã: "HELLO"

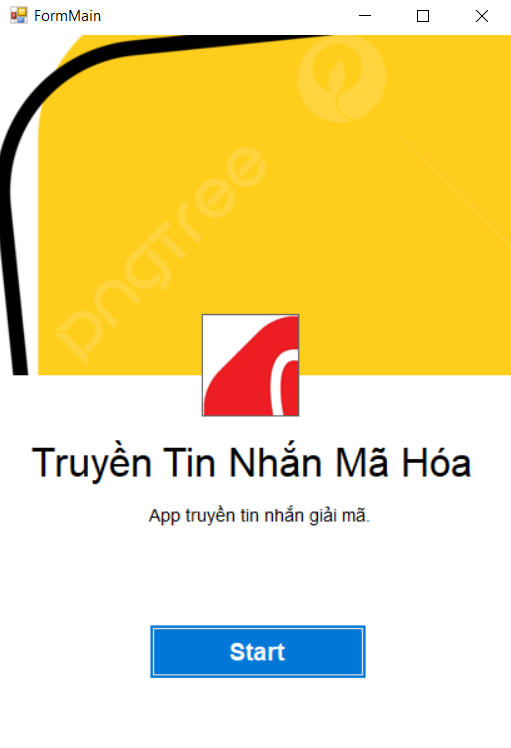


## ****3.5 Tích Hợp với Hệ Thống Truyền Thông****

**Kết Nối với Các Ứng Dụng Tin Nhắn:**

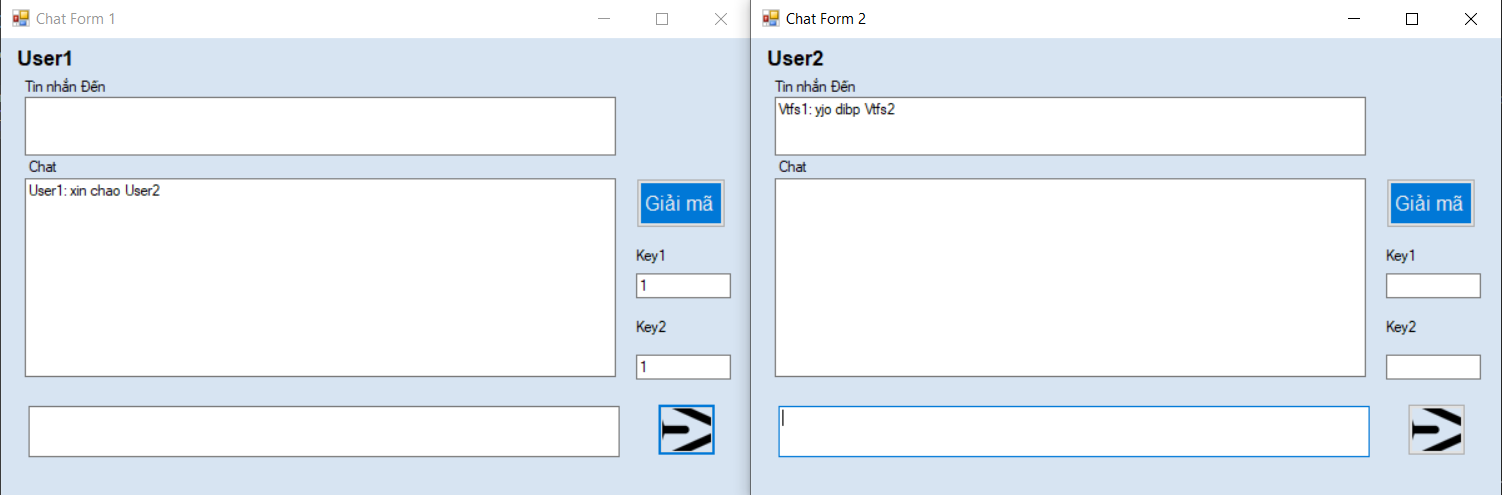
Tích hợp ứng dụng mã hóa Affine vào hệ thống tin nhắn để mã hóa và giải mã tin nhắn khi gửi và nhận.

Ứng dụng truyền tin nhắn mã hóa

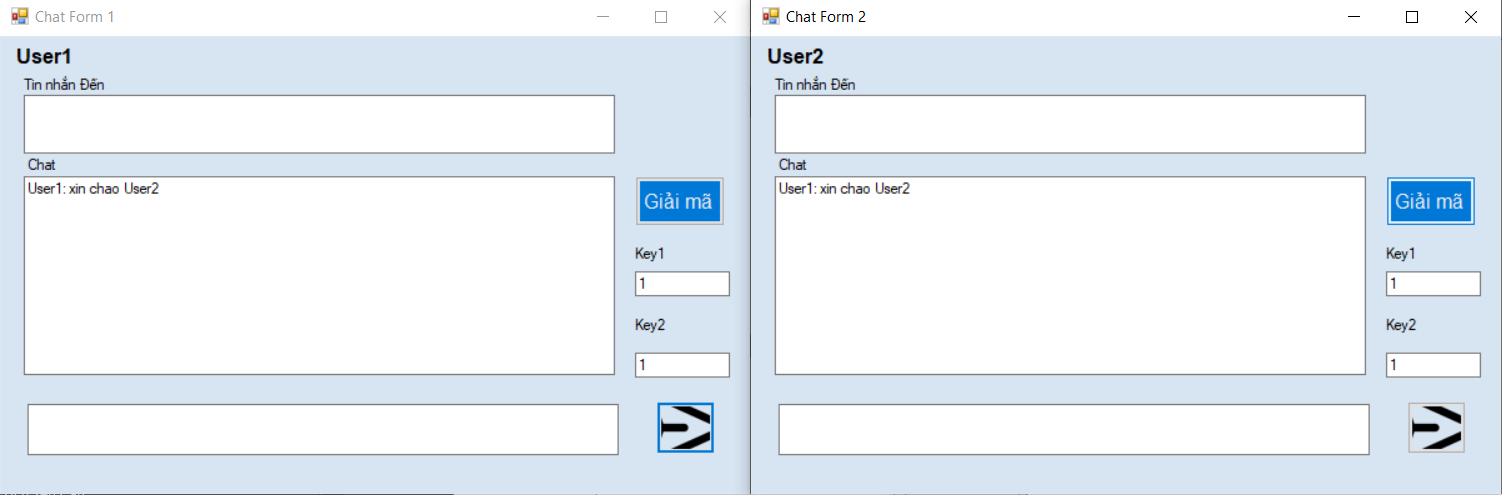


Form chat dụng chat giữa 2 người dùng User1 và User2

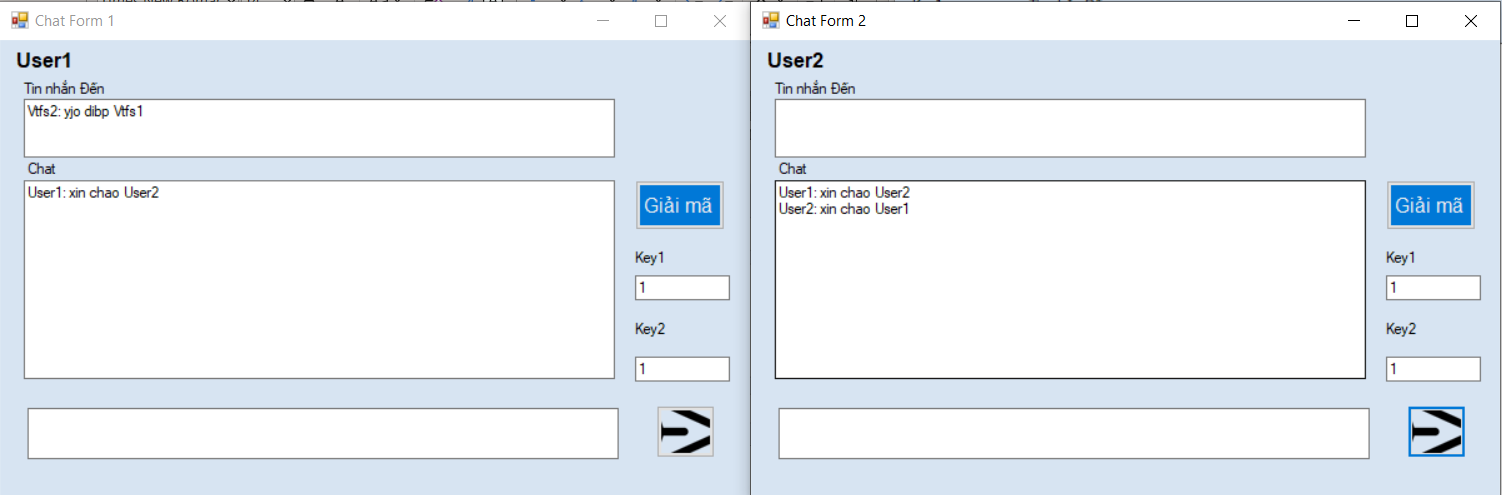
User1 gửi tin nhắn đến User2



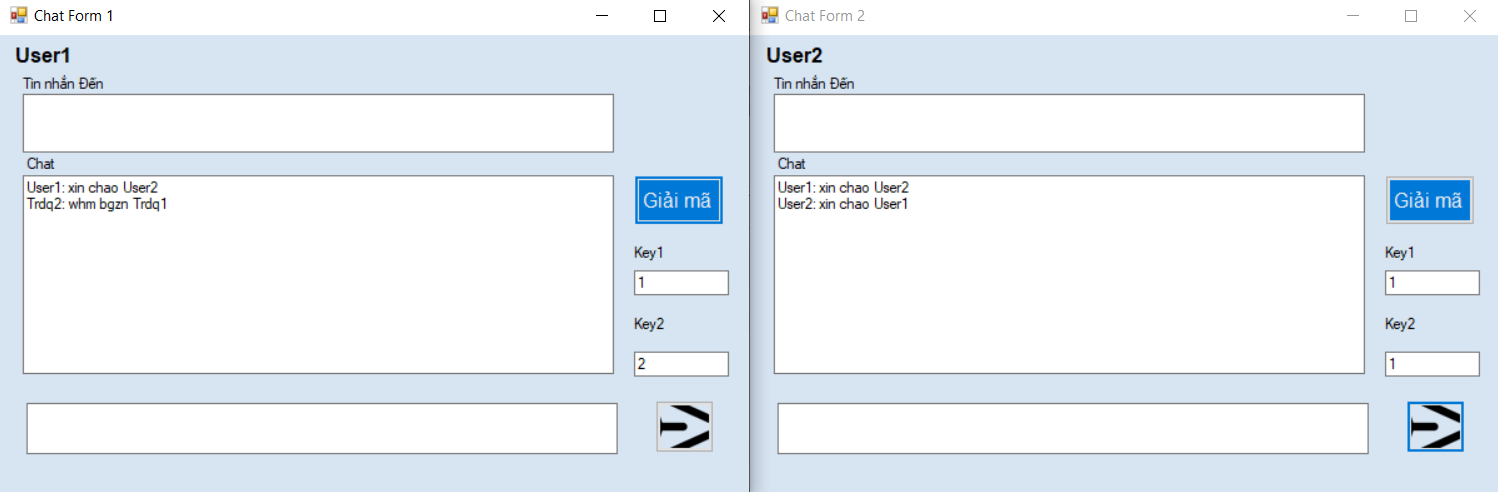
User2 giải mã đúng khóa



User2 gửi tin nhắn đến User1



User1 giải mã sai khóa.



## ****3.6 Đánh Giá và Hiệu Chỉnh****

**3.6.1 Đánh Giá Tính Chính Xác và Hiệu Suất**

**Kiểm tra tính chính xác**:  
Ứng dụng mã hóa Affine Cipher đã được kiểm tra kỹ lưỡng để đảm bảo rằng tất cả các tin nhắn sau khi mã hóa đều có thể giải mã chính xác mà không xảy ra lỗi. Các cặp khóa khác nhau (key1, key2) được sử dụng để xác định độ tin cậy của quá trình mã hóa và giải mã. Đặc biệt, các trường hợp như ký tự đặc biệt, khoảng trắng và tin nhắn dài đã được thử nghiệm nhằm đảm bảo tính ổn định và độ chính xác của ứng dụng.

**Đánh giá hiệu suất**:  
Hiệu suất của ứng dụng cũng được đánh giá để đảm bảo hoạt động mượt mà và nhanh chóng. Trong các bài kiểm tra với tin nhắn ngắn và trung bình, ứng dụng hoạt động ngay lập tức. Tuy nhiên, với tin nhắn dài, thời gian xử lý có thể bị kéo dài, điều này dẫn đến việc xem xét các cải tiến về hiệu năng. Tính năng brute force (thử mọi khả năng khóa) cũng được kiểm tra kỹ lưỡng để đảm bảo rằng nó hoạt động hiệu quả trong việc tìm khóa đúng.

**3.6.2 Cải Thiện và Tinh Chỉnh**

**Sửa lỗi**:  
Sau quá trình kiểm tra, một số lỗi nhỏ liên quan đến xử lý ký tự đặc biệt và định dạng tin nhắn đã được phát hiện và sửa chữa. Điều này đảm bảo rằng ứng dụng có thể xử lý mọi loại tin nhắn mà không phát sinh lỗi. Ngoài ra, các lỗi về logic trong giải mã cũng được tinh chỉnh để đảm bảo kết quả trả về luôn chính xác.

# CHƯƠNG 4: THỰC NGHIỆM VÀ ĐÁNH GIÁ

## ****4.1 Xây Dựng và Thực Hiện Các Thí Nghiệm:****

Để đánh giá hiệu quả của thuật toán mã hóa Affine, việc thực hiện các thí nghiệm là rất quan trọng. Dưới đây là cách tổ chức các thí nghiệm và các bài toán thực nghiệm để kiểm tra và đánh giá thuật toán mã hóa Affine.

**Mục Tiêu của Thí Nghiệm**

**Xác Minh Tính Đúng Đắn:** Đảm bảo rằng thuật toán mã hóa và giải mã hoạt động chính xác.

**Đánh Giá Tính Bảo Mật:** Đánh giá mức độ bảo mật của mã hóa Affine trong các tình huống thực tế.

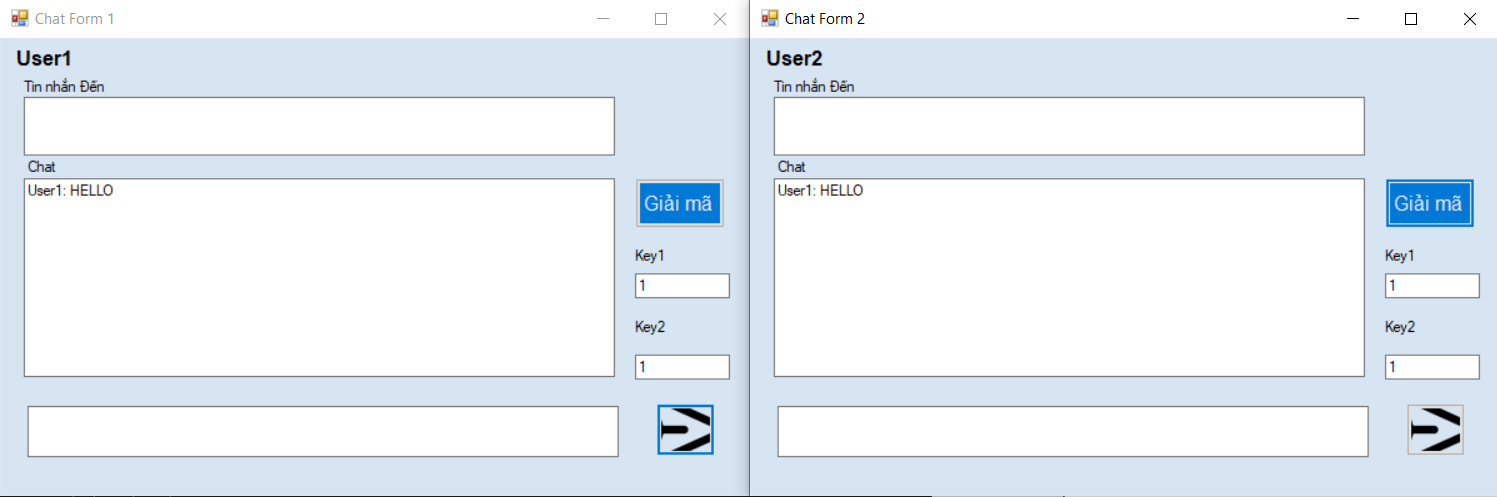
**Đo Hiệu Suất:** Đo lường hiệu suất của thuật toán trong các điều kiện khác nhau.

## ****4.2 Các Bài Toán Thực Nghiệm****

***Kiểm Tra Đúng Đắn Của Thuật Toán***

**Bài Toán 1: Mã Hóa và Giải Mã Đơn Giản**

Chọn một thông điệp đơn giản (ví dụ: "HELLO") và thực hiện mã hóa và giải mã bằng thuật toán Affine.

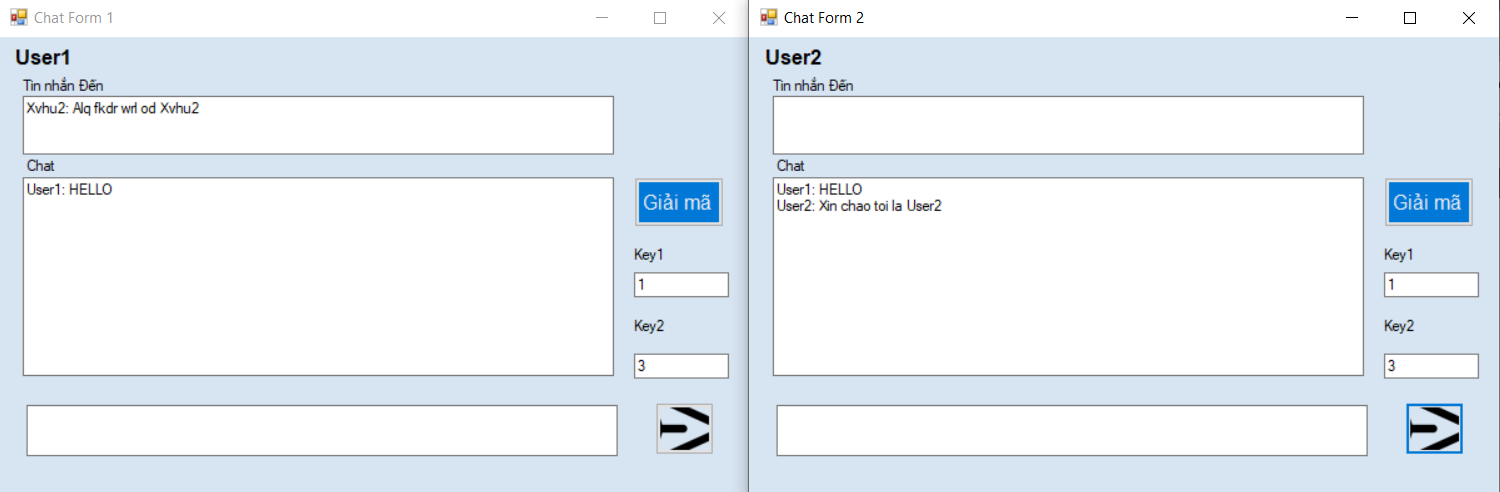


So sánh kết quả giải mã với thông điệp gốc xác minh thông điệp bảo toàn thông tin.

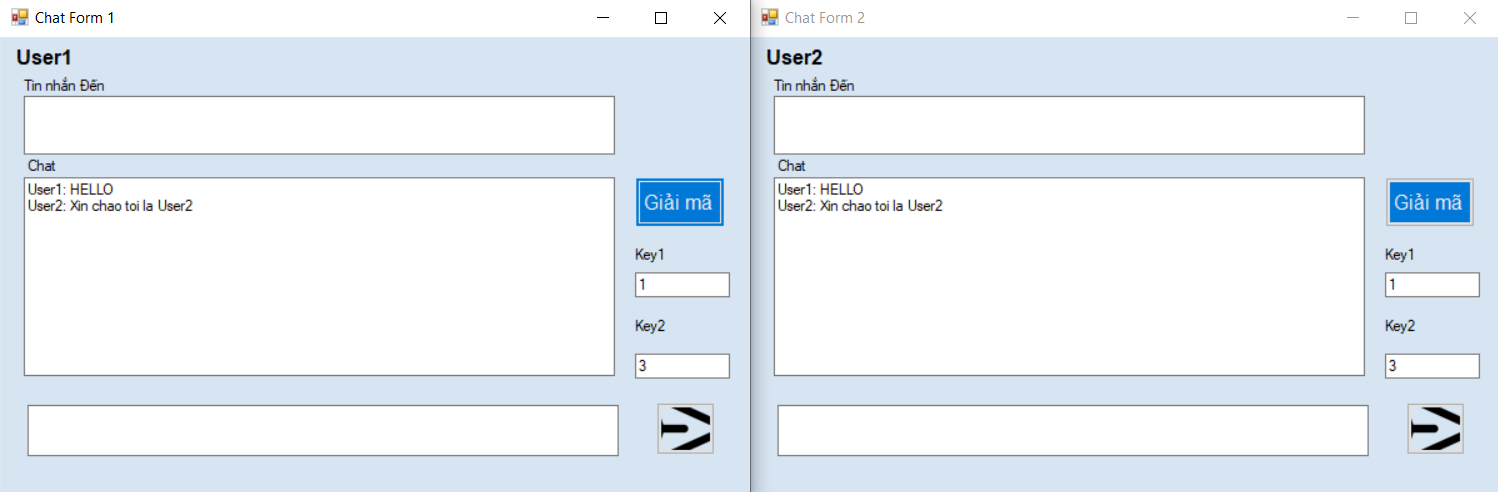
**Bài Toán 2: Kiểm Tra Với Các Khóa Khác Nhau**

Thực hiện mã hóa và giải mã với nhiều cặp khóa (a, b) khác nhau để đảm bảo rằng thuật toán hoạt động đúng với các giá trị khóa khác nhau.

User2 gửi tin nhắn đến User1 với khóa là (1,3)



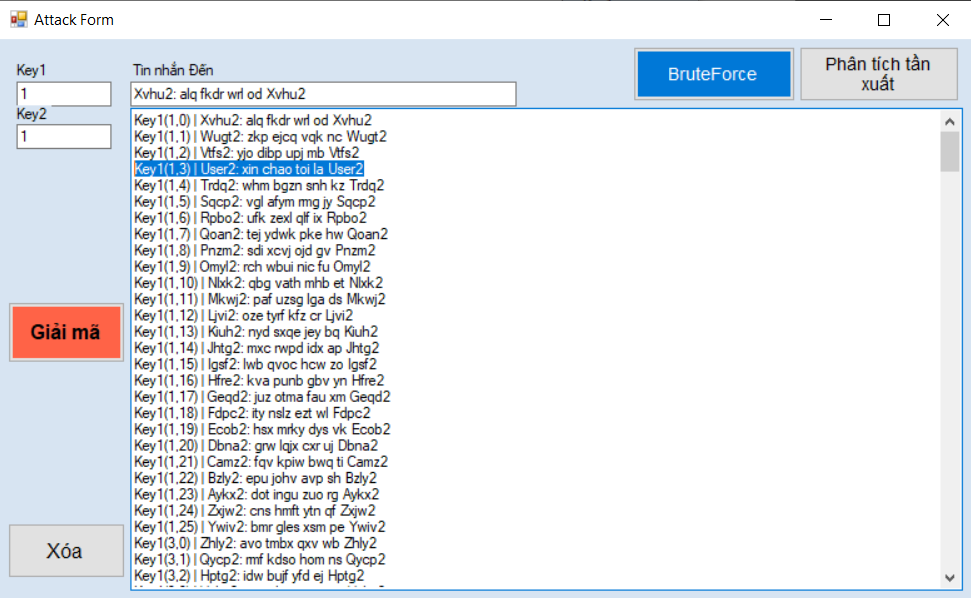
User1 giải mã tin nhắn với khóa là (1,3)



***Đánh Giá Tính Bảo Mật***

**Bài Toán 3: Phân Tích Tấn Công Brute-Force**

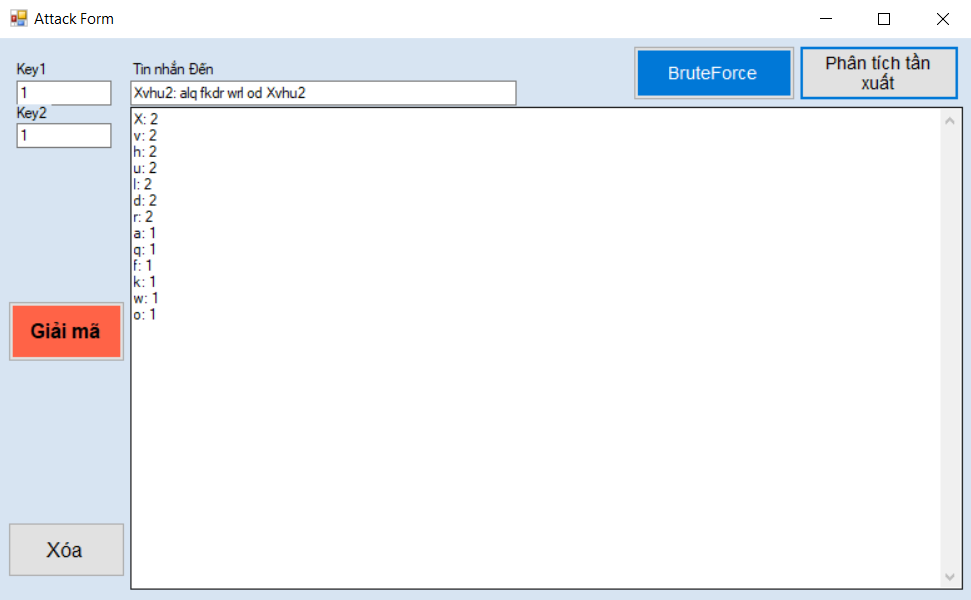
Thực hiện tấn công brute-force để tìm khóa bí mật. Đánh giá độ khó và thời gian cần thiết để phá mã.



Tấn công Brute-Force dễ dàng giải mã tin nhắn dù không biết khóa, khả năng bảo mật không cao.

**Bài Toán 4: Phân Tích Tần Suất Ký Tự**

Mã hóa một thông điệp dài và phân tích tần suất ký tự trong thông điệp mã hóa.

Khả năng chống tần suất ký tự còn hạn chế, nhưng kẻ tấn công không thể dễ dàng giải mã với tấn công phân tích tần xuất.

## ****4.3 Phân Tích Kết Quả****

**Đánh Giá Kết Quả Kiểm Tra Đúng Đắn**

1. **Xác Minh Kết Quả Thực Nghiệm**

**Xác minh tính đúng đắn**:  
Trong suốt quá trình kiểm tra, các bài toán thực nghiệm đều được thiết lập để đánh giá tính đúng đắn của quá trình mã hóa và giải mã trong ứng dụng. Tất cả các trường hợp thử nghiệm đều trả về kết quả chính xác như mong đợi, đảm bảo rằng thông tin sau khi mã hóa và giải mã không bị mất hoặc sai lệch. Các thử nghiệm bao gồm cả các tin nhắn ngắn và dài, với ký tự đặc biệt, chữ số và khoảng trắng. Mỗi tin nhắn đều được mã hóa thành chuỗi ký tự mã hóa chính xác và sau đó được giải mã về nguyên gốc một cách thành công.

**Kết quả thực nghiệm**:  
Các bài kiểm tra không chỉ nhằm xác minh tính chính xác trong quá trình mã hóa và giải mã mà còn kiểm tra sự ổn định của hệ thống khi xử lý các dữ liệu phức tạp hơn. Với tất cả các trường hợp thử nghiệm, hệ thống đều hoạt động đúng như dự kiến mà không có lỗi về logic hay dữ liệu.

2. **Đánh Giá Tính Chính Xác Của Mã Hóa và Giải Mã**

**Mã hóa và giải mã tin nhắn**:  
Các kiểm tra đã chứng minh rằng quá trình mã hóa và giải mã của Affine Cipher diễn ra một cách chính xác, không có hiện tượng mất mát thông tin khi tin nhắn được chuyển đi và trở lại qua quá trình giải mã. Dữ liệu được chuyển đi giữa các bên liên quan qua ứng dụng đều giữ nguyên trạng thái, không bị biến đổi ngoài ý muốn. Điều này cho thấy tính đúng đắn và ổn định của thuật toán Affine Cipher trong việc xử lý tin nhắn.

**Không mất hay thay đổi thông tin**:  
Mọi tin nhắn, sau khi được mã hóa, được truyền đi và sau đó giải mã tại điểm nhận một cách chính xác, đảm bảo rằng không có thông tin nào bị mất hay thay đổi trong quá trình này. Các thử nghiệm với nhiều loại dữ liệu khác nhau, từ chữ cái đến ký tự đặc biệt và số, đều cho ra kết quả chính xác. Điều này xác nhận rằng ứng dụng có khả năng bảo toàn dữ liệu tốt trong suốt quá trình xử lý và truyền tải.

**Đánh Giá Kết Quả Đánh Giá Tính Bảo Mật**

1. **Phân Tích Kết Quả Từ Tấn Công Brute-force và Phân Tích Tần Suất**

**Tấn công brute-force**:  
Trong quá trình thử nghiệm, ứng dụng đã cho phép người dùng sử dụng tấn công brute-force để giải mã tin nhắn khi không biết trước các khóa mã hóa. Kết quả cho thấy, mặc dù phương pháp brute-force có thể tìm ra khóa đúng, nhưng thời gian để tìm được khóa tăng đáng kể với độ dài tin nhắn và độ phức tạp của hệ thống khóa. Tuy nhiên, với các cặp khóa ngắn và tin nhắn ngắn, brute-force trở nên dễ dàng và nhanh chóng, làm giảm độ an toàn của hệ thống trong những trường hợp này.

**Phân tích tần suất**:  
Ứng dụng cũng được kiểm tra qua phương pháp phân tích tần suất, một kỹ thuật thường được sử dụng để tấn công các mã hóa thay thế như Affine Cipher. Qua các thử nghiệm, phân tích tần suất cho thấy tính dễ tổn thương của mã hóa Affine trước những dạng tấn công này, đặc biệt khi dữ liệu đủ lớn để người tấn công có thể nhận ra mô hình xuất hiện của các ký tự. Kết quả nhấn mạnh rằng Affine Cipher không phải là lựa chọn tối ưu nếu không có các biện pháp bảo vệ bổ sung.

2. **So Sánh Với Tiêu Chuẩn Bảo Mật và Phương Pháp Mã Hóa Khác**

**So sánh với các tiêu chuẩn bảo mật**:  
Khi so sánh với các phương pháp mã hóa hiện đại như AES (Advanced Encryption Standard) hoặc RSA (Rivest–Shamir–Adleman), Affine Cipher cho thấy sự yếu kém về mặt bảo mật. Affine Cipher thuộc nhóm mã hóa thay thế cổ điển, dễ bị tấn công bởi các kỹ thuật brute-force hoặc phân tích tần suất, điều này khiến nó kém an toàn hơn nhiều so với các phương pháp mã hóa hiện đại, vốn sử dụng các thuật toán phức tạp với độ dài khóa lớn và tính toán cao hơn.

**Đánh giá khả năng áp dụng**:  
Dù Affine Cipher đơn giản và dễ triển khai, nhưng trong môi trường yêu cầu bảo mật cao, nó không thể so sánh được với các tiêu chuẩn mã hóa hiện đại. AES, với khả năng sử dụng khóa dài và tính ngẫu nhiên cao trong quy trình mã hóa, gần như không thể bị phá vỡ qua brute-force. Tương tự, RSA dựa trên độ khó của bài toán phân tích số nguyên tố, cung cấp mức độ bảo mật cao hơn rất nhiều.

## ****4.4 Kết Luận và Đề Xuất****

**Tóm Tắt Kết Quả Thí Nghiệm:**

Tổng hợp các kết quả từ các bài toán thực nghiệm.

**Đơn giản và Dễ thực hiện**: Mã hóa Affine rất đơn giản để thực hiện và giải mã. Điều này làm cho nó dễ sử dụng trong các tình huống không yêu cầu bảo mật cao, chẳng hạn như trong các bài học lịch sử về mật mã học.

**Kém An Toàn**: Mã hóa Affine có những điểm yếu rõ rệt về bảo mật:

**Dễ bị tấn công Phân tích Tần suất**: Vì mã hóa Affine là một dạng mã hóa thay thế, mỗi ký tự trong văn bản gốc sẽ được thay thế bằng một ký tự khác theo một quy tắc cố định. Điều này làm cho phân phối tần suất của các ký tự trong văn bản đã mã hóa tương tự như phân phối tần suất của các ký tự trong văn bản gốc, tạo điều kiện cho các phương pháp phân tích tần suất tấn công.

**Số lượng khóa hạn chế**: Số lượng khóa có thể dùng trong mã hóa Affine là tương đối nhỏ. Nếu m là kích thước của bảng mã, thì có thể có ít nhất ϕ(m) lựa chọn cho a (trong đó ϕ là hàm Euler), và bất kỳ giá trị nào cho b. Ví dụ, trong bảng chữ cái tiếng Anh (26 ký tự), có 12 lựa chọn cho a và 26 cho b, tổng cộng là 312 lựa chọn khóa, điều này không đủ để chống lại các tấn công kiểm tra toàn bộ khóa.

**Không có Tính Nâng Cao**: Mã hóa Affine không có các tính năng nâng cao như tính kháng đối đầu hoặc mã hóa đa lần (multi-round encryption), điều này làm giảm đáng kể tính bảo mật của nó so với các phương pháp mã hóa hiện đại hơn như AES.

**Đề Xuất Cải Tiến:**

1. Tăng độ phức tạp của khóa

* **Vấn đề hiện tại**: Thuật toán Affine sử dụng hai khóa a và b với giá trị nhỏ (thường nằm trong phạm vi của bảng chữ cái), khiến nó dễ bị tấn công brute-force do không gian khóa hạn chế.
* **Cải tiến**: Tăng phạm vi lựa chọn khóa a và b, hoặc kết hợp nhiều khóa trong quá trình mã hóa, ví dụ như dùng khóa theo các vòng lặp, tăng số lượng biến đổi mỗi khi mã hóa một ký tự.

2. **Kết hợp với các kỹ thuật mã hóa khác**

* **Vấn đề hiện tại**: Mã hóa Affine dễ bị tấn công bằng phân tích tần suất vì sự ánh xạ giữa ký tự gốc và ký tự mã hóa là tuyến tính.
* **Cải tiến**: Kết hợp Affine với các kỹ thuật mã hóa khác, chẳng hạn như XOR với một dãy số ngẫu nhiên, để tăng cường tính an toàn. Điều này sẽ phá vỡ mối quan hệ trực tiếp giữa ký tự gốc và ký tự mã hóa.

3. **Thay đổi bảng chữ cái**

* **Vấn đề hiện tại**: Thuật toán Affine hoạt động trên một bảng chữ cái cố định, chẳng hạn như bảng chữ cái tiếng Anh với 26 ký tự.
* **Cải tiến**: Sử dụng bảng chữ cái động, nghĩa là thay đổi bảng chữ cái dựa trên một số yếu tố ngẫu nhiên hoặc khóa người dùng. Điều này sẽ làm phức tạp quá trình phân tích tần suất.

4. **Thêm bước hoán vị sau khi mã hóa**

* **Vấn đề hiện tại**: Mã hóa Affine chỉ thực hiện biến đổi tuyến tính dựa trên phép nhân và cộng.
* **Cải tiến**: Sau bước mã hóa bằng Affine, thêm một bước hoán vị (permutation) các ký tự trong thông điệp để tăng độ phức tạp và giảm nguy cơ bị tấn công phân tích.

Các Chỉ số Bảo mật

1. **Khả năng Chống Tấn Công Phân Tích Tần Suất**: Như đã đề cập, do mã hóa Affine không thay đổi phân phối tần suất của các ký tự, nó dễ bị tấn công phân tích tần suất. Các ký tự phổ biến trong văn bản gốc vẫn giữ tần suất tương tự trong văn bản mã hóa.
2. **Khả năng Kháng Tấn Công Brute-Force**: Với số lượng khóa hạn chế, mã hóa Affine có thể dễ dàng bị phá vỡ bằng cách thử tất cả các khóa khả dĩ (brute-force attack). Đây là một vấn đề nghiêm trọng đối với bảo mật của phương pháp này.
3. **Khả năng Chống Tấn Công Vào Ký Tự (Known-Plaintext Attack)**: Nếu kẻ tấn công biết một số ký tự trong văn bản gốc và văn bản mã hóa tương ứng, họ có thể giải mã toàn bộ văn bản hoặc xác định khóa mã hóa bằng cách giải quyết hệ phương trình tuyến tính đơn giản.

## Kết luận

Mã hóa Affine, dù đơn giản và dễ triển khai, không đủ mạnh để bảo vệ thông tin trong các tình huống yêu cầu bảo mật cao. Hiệu quả của nó chủ yếu giới hạn trong các ứng dụng học thuật, giáo dục hoặc trong các bối cảnh không đòi hỏi bảo mật nghiêm ngặt. Các chỉ số bảo mật như khả năng chống tấn công phân tích tần suất và khả năng kháng tấn công brute-force cho thấy mã hóa Affine không đủ mạnh để chống lại các phương pháp tấn công hiện đại

# ****CHƯƠNG 5: TỔNG KẾT****

Trong suốt quá trình phát triển ứng dụng mã hóa Affine cho truyền nhận thông tin, nhóm chúng em đã hoàn thành được các mục tiêu đề ra. Ứng dụng cho phép người dùng có thể gửi tin nhắn được mã hóa và giải mã dựa trên thuật toán mã hóa Affine, giúp bảo vệ thông tin trong quá trình truyền tải.

## ****5.1 Kết Quả Đạt Được****

Ứng dụng đã hoàn thành các chức năng chính như sau:

**Mã hóa và giải mã tin nhắn**: Sử dụng thuật toán Affine, tin nhắn được mã hóa và giải mã một cách chính xác dựa trên hai khóa (a và b).

**Giao diện người dùng thân thiện**: Ứng dụng cung cấp giao diện đơn giản, dễ sử dụng, với các tính năng gửi và nhận tin nhắn rõ ràng.

**Chức năng tấn công brute-force**: Khi khóa không được biết trước, người dùng có thể sử dụng chức năng brute-force để tìm khóa đúng, giúp tăng tính tương tác và mở rộng ứng dụng cho các tình huống phân tích, tấn công mã hóa.

**Tính bảo mật**: Ứng dụng đã đảm bảo tính an toàn cho tin nhắn trong suốt quá trình truyền thông tin giữa hai bên thông qua việc mã hóa tin nhắn.

## ****5.2 Khó Khăn và Hạn Chế****

Mặc dù ứng dụng đã đạt được nhiều kết quả tích cực, vẫn còn một số khó khăn và hạn chế:

**Khóa yếu trong mã hóa Affine**: Một số khóa có thể dễ dàng bị tấn công bằng phương pháp brute-force, làm giảm tính bảo mật của ứng dụng.

**Hiệu suất brute-force**: Khi sử dụng brute-force để tìm khóa, thời gian giải mã có thể bị kéo dài đáng kể đối với các tập hợp khóa lớn.

**Giao diện**: Mặc dù giao diện đã hoàn thiện, nhưng một số chức năng có thể được trình bày tốt hơn để tăng tính thân thiện với người dùng.

## ****5.3 Hướng Phát Triển****

Trong tương lai, ứng dụng có thể được cải tiến theo các hướng sau:

**Tích hợp các thuật toán mã hóa mạnh hơn**: Thay vì chỉ sử dụng mã hóa Affine, có thể tích hợp thêm các thuật toán mã hóa khác như RSA hoặc AES để nâng cao tính bảo mật.

**Tăng cường tính năng bảo mật**: Có thể áp dụng thêm các cơ chế kiểm soát truy cập hoặc xác thực để đảm bảo rằng chỉ những người dùng được phép mới có thể giải mã tin nhắn.

**Cải tiến giao diện người dùng**: Tăng cường trải nghiệm người dùng bằng cách cải thiện giao diện, thêm các hướng dẫn sử dụng chi tiết và trực quan hơn.

## ****Kết Luận****

Quá trình xây dựng ứng dụng mã hóa Affine trong truyền nhận thông tin đã giúp chúng em hiểu rõ hơn về mã hóa Affine cũng như các kỹ thuật mã hóa khác. Ứng dụng có thể đáp ứng nhu cầu bảo mật cơ bản trong truyền thông tin giữa hai bên, đồng thời cũng mở ra nhiều cơ hội phát triển và nghiên cứu thêm về bảo mật thông tin trong tương lai.

# Tài Liệu Tham Khảo

[1] <https://tek4.vn/khoa-hoc/cau-truc-du-lieu-va-thuat-toan/he-mat-affine>

(Tham khảo ngày 19 tháng 9 năm 2024 )

[2] <https://vi.wikipedia.org/wiki/M%E1%BA%ADt_m%C3%A3_Affine>

(Tham khảo ngày 19 tháng 9 năm 2024 )