**TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI**

**PHÂN HIỆU THÀNH PHỐ HỒ CHÍ MINH**

**BỘ MÔN CÔNG NGHỆ THÔNG TIN**



**BÁO CÁO TIỂU LUẬN**

**MÔN: AN TOÀN BẢO MẬT THÔNG TIN**

**ĐỀ TÀI:**

**MÃ HOÁ VÀ GIẢI MÃ VĂN BẢN VỚI THUẬT TOÁN VIGENERE**

Sinh viên thực hiện : VÕ TẤN ĐÀO

Mã sinh viên : 5951071011

Lớp : CQ.59.CNTT

*TP Hồ Chí Minh, năm 2021*

**TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI**

**PHÂN HIỆU THÀNH PHỐ HỒ CHÍ MINH**

**BỘ MÔN CÔNG NGHỆ THÔNG TIN**



**BÁO CÁO TIỂU LUẬN**

**MÔN: AN TOÀN BẢO MẬT THÔNG TIN**

**ĐỀ TÀI:**

**MÃ HOÁ VÀ GIẢI MÃ VĂN BẢN VỚI THUẬT TOÁN VIGENERE**

Sinh viên thực hiện : VÕ TẤN ĐÀO

Mã sinh viên : 5951071011

Lớp : CQ.59.CNTT

*TP Hồ Chí Minh, năm 2021*

|  |  |
| --- | --- |
| **TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI**  **PHÂN HIỆU TẠI THÀNH PHỐ HỒ CHÍ MINH** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**  **Độc lập – Tự do – Hạnh phúc** |

# **NHIỆM VỤ BÁO CÁO TIỂU LUẬN**

BỘ MÔN: **CÔNG NGHỆ THÔNG TIN**

-------\*\*\*-------

**Mã sinh viên:** 5951071011 **Họ tên SV:** Võ Tấn Đào

**Khóa:** 59 **Lớp:** CQ.59.CNTT

1. **Tên đề tài:**

MÃ HOÁ VÀ GIẢI MÃ VĂN BẢN VỚI THUẬT TOÁN VIGENERE

1. **Mục đích, yêu cầu:**
   1. **Mục đích:**

Mã hóa với mục đích làm cho dữ liệu không thể đọc được bởi bất cứ ai, ngoại trừ những ai được cho chép đọc. Mã hóa sử dụng thuật toán và khóa để biến đổi dữ liệu từ hình thức đơn giản rõ ràng (plain hay cleartext), làm biến dữ liệu sang hình tức mật mã vô nghĩa (code hay ciphertext). Chỉ có những ai có thông tin giải mã thì mới giải mã được và đọc được dữ liệu.

* 1. **Yêu cầu:**
* **Yêu cầu công nghệ:**
  + Sử dụng ngôn ngữ lập trình C#.
  + Sử dụng công cụ Visual Studio.
* **Yêu cầu chức năng:**
* Cho phép nhập văn bản vào hệ thống
* Cho phép nhập khóa bảo vệ văn bản.
* Cho phép mở File và Ghi File.

1. **Nội dung và phạm vi đề tài**
   1. **Nội dung:**

* Tổng quan bài toán.
* Tổng quan về các công nghệ đang sử dụng.
* Khảo sát bài toán.
* Lập trình xây dựng.
* Kiểm thử và chạy thực nghiệm.
* Kết quả thu được
  1. **Phạm vi:**
     + Nghiên cứu công cụ Visual Studio và ngôn ngữ C#

1. **Công nghệ, công cụ và ngôn ngữ lập trình**
   * + Công cụ: Visual Studio.
     + Ngôn ngữ lập trình: C#.
2. **Các kết quả chính dự kiến sẽ đạt được và ứng dụng**
   * + Xây dựng ứng dụng mã hoá và giải mã văn bản với thuật toán Vigenere.

**Ngày ...... tháng ...... năm 2021**

**Trưởng BM Công nghệ Thông tin**

# **LỜI CẢM ƠN**

Lời đầu tiên em xin gửi lời cảm ơn chân thành đến quý thầy, cô giáo trong **Bộ môn Công nghệ thông tin – Phân hiệu Trường Đại học Giao thông vận tải.** Những người đã truyền dạy, đã trang bị cho em kho tàng kiến thức về bầu trời côngnghệ thông tin rộng lớn.

Ở đây, em không chỉ học được kiến thức về sách vở mà em còn học được các bài học, kỹ năng sống trước khi tạm biệt mái trường đại học thân yêu này và tiến ra biển đời mênh mông rộng lớn. Đặc biệt, em xin gửi lời cảm ơn chân thành và sâu sắc đến thầy **PHAN THANH HY**, người đã dạy em môn **AN TOÀN VÀ BẢO MẬT THÔNG TIN**

Trong quá trình học tập và tìm hiểu em đã nỗ lực rất nhiều với mong muốn hoàn thành project một cách tốt nhất, nhưng đời người sẽ có những thiếu sót không thể tránh khỏi, và với những người chưa chững chạc và trưởng thành như em thì sai lầm là không thể không mắc phải. Em mong thầy, cô bộ môn có thể thông cảm và cho em những ý kiến, đóng góp để em có thể hoàn thành tốt hơn về đồ án của mình một cách trọn vẹn để có cơ hội sửa chữa.

Sau cùng, em xin kính chúc Quý Thầy Cô trong **Bộ môn Công nghệ thông tin** lời chúc sức khoẻ, luôn hạnh phúc và thành công hơn nữa trong công việc cũng nhưtrong cuộc sống.

Em xin chân thành cảm ơn!

# 

# **NHẬN XÉT CỦA GIÁO VIÊN**

*Tp. Hồ Chí Minh, ngày … tháng … năm …*

Giảng viên hướng dẫn

Mục Lục:

[NHIỆM VỤ BÁO CÁO TIỂU LUẬN iii](#_Toc76462530)

[LỜI CẢM ƠN 5](#_Toc76462531)

[NHẬN XÉT CỦA GIÁO VIÊN 6](#_Toc76462532)

[MỞ ĐẦU 9](#_Toc76462533)

[1. Giới thiệu đề tài. 9](#_Toc76462534)

[2. Mục tiêu nghiên cứu: 9](#_Toc76462535)

[3. Phương pháp nghiên cứu 9](#_Toc76462536)

[CHƯƠNG 1: CƠ SỞ LÝ THUYẾT VÀ THUẬT TOÁN VIGENERE 10](#_Toc76462537)

[1.1. Lý thuyết cơ sở. 10](#_Toc76462538)

[**1.1.1.** **Mật mã.** 10](#_Toc76462539)

[**1.1.2.** **Mật mã cổ điển** 10](#_Toc76462540)

[1.2. Mật mã Vigenere 10](#_Toc76462541)

[**1.2.1.** **Khái niệm** 10](#_Toc76462542)

[**1.2.2.** **Mật mã Vigenere** 11](#_Toc76462543)

[**1.2.3.** **Phương pháp mã hoá Vigenere** 12](#_Toc76462544)

[CHƯƠNG 2: THỬ NGHIỆM ỨNG DỤNG 15](#_Toc76462545)

[2.1. Môi trường cài đặt 16](#_Toc76462546)

[2.2. Triển khai ứng dụng 16](#_Toc76462547)

[CHƯƠNG 3: KẾT LUẬN 17](#_Toc76462548)

**DANH MỤC HÌNH ẢNH**

[Hình 1. 1 – Bảng mật mã của Vigenere 11](#_Toc75853966)

[Hình 1. 2 – Bảng rõ 13](#_Toc75853967)

**DANH MỤC BẢN BIỂU**

[Bảng 1. 1 – Bảng chuỗi plaintext P và keyword K 13](#_Toc76462825)

[Bảng 1. 2 – Bảng chuỗi plaintext P và keyword K đã chuyển sang bảng rõ 14](#_Toc76462826)

[Bảng 1. 3 – Bảng mật mã 14](#_Toc76462827)

[Bảng 1. 4 – Bảng mã hoá và keyword 14](#_Toc76462828)

[Bảng 1. 5 – Bảng giải mã 14](#_Toc76462829)

[Bảng 1. 6 - Bảng tách ghép P&K theo AutoKey 15](#_Toc76462830)

# **MỞ ĐẦU**

1. **Giới thiệu đề tài.**

Như các bạn đã biết ngay từ xa xưa con người chúng ta đã biết truyền thông .Trong một thời đại không có điện thoại cũng chẳng có thư điện tử, bất kỳ ai muốn truyền thông tin riêng của mình đến một người nào khác ở nơi xa chỉ có một cách là viết nó lên mặt giấy rồi giao phó cho một người mang thư đi .Nếu chẳng may người mang thư đó ngờ là trong thư có những thông tin quý giá ,anh ta có thể bán đứng cho kẻ thù để kiếm được nhiều tiền hơn là đưa nó đến đúng địa chỉ .Nhiều bộ óc trong lịch sử đã phát minh ra các phương pháp sử dụng mật mã để giải quyết những thách thức trong việc bảo vệ dữ liệu . Jujius Caesar phát minh ra cách viết mật mã được gọi là hộp Caesar ; Mary , Nữ hoàng Scotland đã tạo ra mật mã thay thế và gởi đi những thông báo bí mật từ nhà tù ; nhà khoa học xuất sắc người Arập Abu Yusuf Ismail al-Kindi đã bảo vệ được những bí mật của mình bằng một mật mã thay thế tài tình sử dụng nhiều chữ cái khác nhau …..

Ngày nay , khi khoa học phát triển , mật mã cũng được sử dụng trong những hệ thống cần độ bảo mật cao như : Ngân hàng , bưu chính ,…. Những thuật toán mã hóa được phát triển ngày nhiều và có độ bảo mật cao hơn.

**Hướng tiếp cận của đề tài:**

* Nghiên cứu và hiểu được cách thức mã hoá và giải mã của thuật toán Vigenere.
* Tiến hành kiểm tra và chạy thử ứng dụng.

1. **Mục tiêu nghiên cứu:**

* Phát triển thành công ứng dụng mã hoá và giải mã văn bản với thuật toán Vigenere

1. **Phương pháp nghiên cứu**

* Tài liệu: Tìm hiểu và khai thác các tài liệu liên quan đến thuật toán Vigenere.
* Thực hành: Tiến hành xây dựng UI cho ứng dụng sau đó sử dụng thuật toán Vigenere.

# 

# **CHƯƠNG 1: CƠ SỞ LÝ THUYẾT VÀ THUẬT TOÁN VIGENERE**

* 1. **Lý thuyết cơ sở.**
     1. **Mật mã.**

Mật mã là tập hợp mọi phương pháp (hoặc quy tắc) biến đổi nào đó nhằm chuyển các thông báo (messages) dưới dạng nhận thức được nội dung (như chữ viết, tiếng nói, hình vẽ, hình ảnh…) thành dạng bí mật mà những người ngoài cuộc không hiểu được nội dung nếu họ không biết được phương pháp (hoặc quy tắc) biến đổi đó.

* + 1. **Mật mã cổ điển**

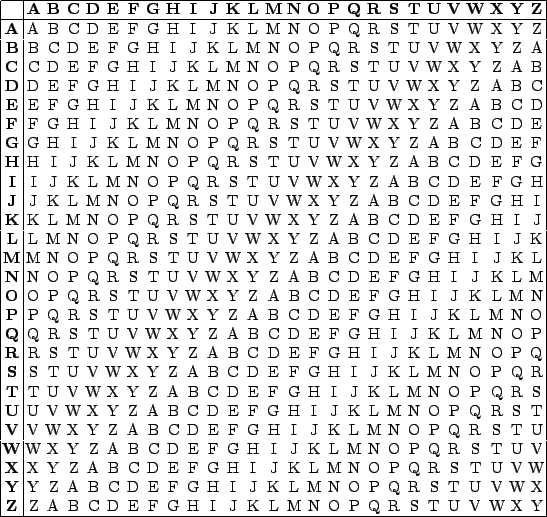
Trong mật mã học, mật mã học cổ điển là một dạng của mật mã học đã được sử dụng trong lịch sử phát triển của loài người nhưng ngày nay đã trở nên lạc hậu do các phương thức mã hóa này quá đơn giản và những kẻ tấn công có thể dễ dàng bẻ khóa thông qua nhiều phương thức như tấn công vét cạn (ví dụ như dùng máy tính thử hết mọi trường hợp) hay dựa trên tấn công thống kê (dựa trên tần suất xuất hiện của các chữ cái). Nói chung, mật mã học cổ điển hoạt động trên cơ sở bảng chữ cái (chẳng hạn các ký tự từ "A" tới "Z" trong tiếng Anh), và chúng được thực hiện bằng tay hay một số máy móc cơ khí đơn giản. Ngược lại, các mô hình mã hóa hiện đại sử dụng các máy tính hay các công nghệ số hóa khác, và hoạt động mã hóa dựa trên việc thay thế các bit hay byte. Các phương thức mã hóa cổ điển thông thường dễ bị tổn thương (phá mã) bởi các tấn công văn bản mã hóa, đôi khi thậm chí kẻ tấn công không cần biết các chi tiết cụ thể của hệ thống mã hóa, bằng cách sử dụng các công cụ như phân tích tần suất.

* 1. **Mật mã Vigenere**
     1. **Khái niệm**

Mật mã Vigenere là một phương pháp mã hóa văn bản bằng cách sử dụng xen kẽ một số phép mã hóa Caesar khác nhau dựa trên các chữ cái của một từ khóa. Nó là một dạng đơn giản của mật mã thay thế dùng nhiều bảng chữ cái.

* + 1. **Mật mã Vigenere**

Trong mật mã Vigenere, người ta dùng tất cả 26 bảng thế là sự thu được từ bảng gốc chữ cái tiếng Anh mà dịch đi từ 0-25 vị trí. Sự hoà trộn này có quy luật hoàn toàn xác định bởi khoá. Mỗi chữ của khoá sẽ xác định mỗi bảng thế được dùng.



Hình 1. 1 – Bảng mật mã của Vigenere

* + 1. **Phương pháp mã hoá Vigenere**

Ví dụ: Bài tập Cho chuỗi Plaintext P: “GIAO THONG VAN TAI”. Trình bày các bước mã hóa chuỗi đã cho với vigenere cipher. Biết rằng keyword K: “TANDAO”

* + - 1. **Giải mã và mã hoá theo cách truyền thống:**

**Mã hoá:**

* Bước 1: Điền Keyword dưới chuỗi Plaintext P và lặp lại ta có:

Hàng 1: G I A O T H O N G V A N T A I

Hàng 2: T A N D A O T A N D A O T A N

* Bước 2: Lấy một chữ cái ở hàng 2 ứng với một chữ cái ở hàng 1 và dựa vào bảng sau để tìm ra chữ cái tương ứng.

|  |  |  |
| --- | --- | --- |
| Cột | Hàng | Mã hoá |
| G | T | Z |
| I | A | I |
| A | N | N |
| O | D | R |
| T | A | T |
| H | O | V |
| O | T | H |
| N | A | N |
| G | N | T |
| V | D | Y |
| A | A | A |
| N | O | B |
| T | T | M |
| A | A | A |
| I | N | V |

**Giải mã:** Trước hết, ngoài mật mã thì ta còn cần từ khóa (lấy ví dụ như trên). Đầu tiên, ta lấy chữ cái đầu tiên của từ khóa (ở đây là chữ cái T), sau đó tìm chữ cái đó ở hàng ngang đầu tiên của bảng mã. Từ chữ cái tìm được, ta dóng xuống chữ cái cùng thứ tự của mã (ở đây là chữ cái L). Rồi ta di chuyển tới chữ cái tương ứng ở cột dọc đầu tiên từ trái sang phải. Dần dần ta sẽ giải hết mật mã.

* + - 1. **Mã hoá và giải mã theo cách lặp khoá:**

Plaintext(P) và Key(K):

* Mã hoá:
* = ( mod 26
* Giải mã:
* = ( mod 26

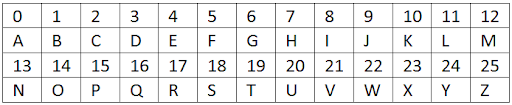
**Giải ví dụ:**

* Bước 1: Điền Keyword K dưới chuỗi Plaintext P và lặp lại ta có:

Hàng 1: G I A O T H O N G V A N T A I

Hàng 2: T A N D A O T A N D A O T A N

* Bước 2: Chuyển K và P theo bảng rõ



Hình 1. 2 – Bảng rõ

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| G | I | A | O | T | H | O | N | G | V | A | N | T | A | I |
| T | A | N | D | A | O | T | A | N | D | A | O | T | A | N |

Bảng 1. 1 – Bảng chuỗi plaintext P và keyword K

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6 | 8 | 0 | 14 | 19 | 7 | 14 | 13 | 6 | 23 | 0 | 13 | 19 | 0 | 8 |
| 19 | 0 | 13 | 3 | 0 | 14 | 19 | 0 | 13 | 13 | 0 | 14 | 19 | 0 | 13 |

Bảng 1. 2 – Bảng chuỗi plaintext P và keyword K đã chuyển sang bảng rõ

Cộng P và K theo module 26

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 25 | 8 | 13 | 17 | 19 | 21 | 7 | 13 | 19 | 10 | 0 | 1 | 19 | 0 | 21 |

Bảng 1. 3 – Bảng mật mã

* Bước 3: Từ bảng trên ta nhìn vào bảng rõ thì mật mã chuỗi Plaintext P: “GIAO THONG VAN TAI” và keyword K: “TANDAO” sẽ được mã hoá thành: **ZINRTVHNTYABMAV**
  + - Giải mã: Ta lấy bảng 1.3 và keyword sau đó trừ nhau theo module 26.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 25 | 8 | 13 | 17 | 19 | 21 | 7 | 13 | 19 | 10 | 0 | 1 | 19 | 0 | 21 |
| 19 | 0 | 13 | 3 | 0 | 14 | 19 | 0 | 13 | 13 | 0 | 14 | 19 | 0 | 13 |

Bảng 1. 4 – Bảng mã hoá và keyword

Trừ theo module 26

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6 | 8 | 0 | 14 | 19 | 7 | 14 | 13 | 6 | 23 | 0 | 13 | 19 | 0 | 8 |

Bảng 1. 5 – Bảng giải mã

* + - 1. **Mã hoá và giải mã theo AutoKey**

Đối với Vigenere Cipher thông thường như trên, thì ta sẽ lặp lại key để có độ dài bằng với độ dài chuỗi cần mã hoá, theo đó thì ta chỉ cần tra bảng mã là ra chuỗi encode cũng như decode. Tuy nhiên, để tăng độ khó cho chuỗi mã hoá, người ta sử dụng một phương pháp khác có tên gọi là Vigenère Cipher auto key, trong đó ta sẽ sử dụng key một lần duy nhất, ghép với chuỗi cần mã hoá để tạo ra key mới như sau:

**Mã hoá:**

* Bước 1: Tách hoặc thêm các dấu cách (space) trong key(K) để cùng form với chuỗi gốc.
* Bước 2: Sau đó ghép với chuỗi gốc và cắt cho độ dài bằng độ dài chuỗi gốc.
* Bước 3: So sánh với bảng mã và đưa ra chuỗi mã hoá.

**Ví dụ:**

* Ta thêm dấu cách vào trong chỗi P và key K, sau đó ghép chuỗi P và cắt cho bằng độ dài chuỗi gốc.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| G | I | A | O | T | H | O | N | G | V | A | N | T | A | I |
| T | A | N | D | A | O | G | I | A | O | T | H | O | N | G |

Bảng 1. 6 - Bảng tách ghép P&K theo AutoKey

* So sánh với bảng bảng mã *Hình 1. 1* ta được chuỗi mã hoá như sau: **ZINRTVUVGJTUHNO**

**Giải mã:** Để giải mã, ta sẽ lần ngược lại bảng mã thôi. Bắt đầu từ trái qua phải, với mỗi ký tự của key làm dòng, ta tìm cột mà khi dóng xuống ta có giá trị là ký tự trong chuỗi đã mã hóa. Ký tự trong cột đó chính là ký tự của chuỗi ban đầu.

**CHƯƠNG 2: THỬ NGHIỆM ỨNG DỤNG**

1. **Môi trường cài đặt**

Từ những cơ sở lý thuyết, phương pháp phân tích được đề cập ở chương 1. Em đã xây dựng và phát triển thành công ứng dụng trên môi trường Visual Studio, viết bằng ngôn ngữ lập trình C#.

1. **Triển khai ứng dụng**

# **CHƯƠNG 3: KẾT LUẬN**

* + - 1. **Kết quả đạt được**
* Về tri thức:

Trong suốt khoảng thời gian 2 tuần, em đã học được rất nhiều về kiến thức nền tảng, các phương pháp tìm và đọc tại liệu.

* Về ứng dụng:

Đã đạt được các yêu cầu đề về mã hoá Vigenere như:

* Cho phép nhập văn bản vào hệ thống.
* Cho phép nhập khóa bảo vệ văn bản.
* Cho phép mở File và Ghi File.
* Về con người: khoảng thời gian 2 tuần là khoảng thời gian đủ để em hoàn thành tiểu luận, mặc dù cũng gặp đôi chút khó khăn. Tuy nhiên em đã hoàn thành xong bài tiểu luận được giao.
  + - 1. **Hạn chế tồn tại**

Vì thời gian thực hiện đề tài cũng như kiến thức của bản thân là có giới hạn nên vẫn còn vài thiếu sót như: giao diện chưa đẹp măt, các phương pháp mã hoá chưa phong phú.

**TÀI LIỆU THAM KHẢO**

**[1**]. Mật mã Vigenère

[https://vi.wikipedia.org/wiki/Mật\_mã\_Vigenère](https://vi.wikipedia.org/wiki/M%E1%BA%ADt_m%C3%A3_Vigen%C3%A8re) truy cập vào lúc 11h32 2/6/2021

**[2].** Thám mật mã Vigenère

<http://antoanthongtin.vn/gp-mat-ma/tham-mat-ma-vigenere-106294> truy cập vào lúc 8h29 3/6/2021

**[3].** Mã hóa cổ điển - Mã hóa Vigenere

<https://www.youtube.com/watch?v=f0AmB_3cIAQ> truy cập vào lúc 22h45 5/6/2021