|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **BAN CƠ YẾU CHÍNH PHỦ**  **HỌC VIỆN KỸ THUẬT MẬT MÃ**  **KHOA: AN TOÀN THÔNG TIN**  **&**  **IMG_256**  **BÁO CÁO MÔN**  **CƠ SỞ LÝ THUYẾT MẬT MÃ**  **----------------------------------------------------------**  **HỆ MẬT MÃ KHOÁ CHẠY**     |  |  | | --- | --- | | **Giảng viên:** | **Tống Anh Tuấn** | | **Sinh viên thực hiện:** | **Trần Cao Minh Bách AT150204**  **Vũ Thị Ánh AT150504**  **Trần Thị Dung AT150310**  **Nguyễn Thị Huyền AT150325** |   **Hà Nội, 2021** |

Mục lục

[LỜI MỞ ĐẦU 1](#_Toc81167328)

[Chương 1: Tổng quan mật mã 2](#_Toc81167329)

[1.1 Tổng quan về mật mã 2](#_Toc81167330)

[1.2 Hệ mật cổ điển 2](#_Toc81167331)

[1.2.1 Một số định nghĩa 2](#_Toc81167332)

[1.2.2 Các hệ mật thay thế đa biểu 3](#_Toc81167333)

[1.2.3 Hệ Vigenere Cipher 3](#_Toc81167334)

[1.2.4 Các hệ mật thay thế không tuần hoàn 3](#_Toc81167335)

[Chương 2: Hệ mã khoá chạy 4](#_Toc81167336)

[2.1 Tính chất 4](#_Toc81167337)

[2.2 Cơ chế hoạt động 4](#_Toc81167338)

[2.2.1 Giải thuật 4](#_Toc81167339)

[2.3 Hệ mã khoá chạy biểu diễn bằng ngôn ngữ lập trình ( Sử dụng ngôn ngữ Python) 6](#_Toc81167340)

[a. Mã hoá 6](#_Toc81167341)

[b. Giải mã 7](#_Toc81167342)

[2.3 Xây dựng App trên cơ sở đã xây dựng 8](#_Toc81167343)

[2.3.1 Giao diện 8](#_Toc81167344)

[2.3.2 Hoạt động 9](#_Toc81167345)

[2.4 Ứng dụng 11](#_Toc81167346)

[2.5 Hạn chế 11](#_Toc81167347)

[Chương 3: Kết luận 12](#_Toc81167348)

# LỜI MỞ ĐẦU

Với các bộ mã đi trước và việc thám mã ngày càng tốt, việc sử dung một bộ mã với khoá K dễ đoán là điều cực kì bất lợi. Vì vậy, dựa theo bộ mã Vigenere, chính Vigenere cũng đã đề xuất một loại khoá tự động sinh cho bằng độ dài bản tin. Từ đó, hệ mã khoá chạy ra đời. Việc ra đời hệ mã khoá này, giúp cho việc bảo mật thông tin được đảm bảo hơn tại thời điểm ấy. Chúng ta sẽ cùng đi tìm hiểu nó trong tài liệu này!

# Chương 1: Tổng quan mật mã

## Tổng quan về mật mã

Mật mã là một lĩnh vực khoa học chuyên nghiên cứu về các phương pháp và kỹ thuật đảm bảo an toàn và bảo mật trong truyền tin liên lạc, với giả thiết sự tồn tại của các thế lực thù địch, những kẻ muốn ăn cắp thông tin để lợi dụng và phá hoại. Tên gọi trong tiếng Anh, Cryptology được dẫn giải nguồn gốc từ tiếng Hy lạp, trong đó kryptos nghĩa là “che dấu”, logos nghĩa là “từ ngữ”. Cụ thể hơn, các nhà nghiên cứu lĩnh vực này quan tâm xây dựng hoặc phân tích (để chỉ ra điểm yếu) các giao thức mật mã (cryptographic protocols), tức là các phương thức giao dịch có đảm bảo mục tiêu an toàn cho các bên tham gia (với giả thiết môi trường có kẻ đối địch, phá hoại).

Ngành Mật mã (cryptology) thường được quan niệm như sự kết hợp của 2 lĩnh vực con:

* + - Sinh, chế mã mật (cryptography): nghiên cứu các kỹ thuật toán học nhằm cung cấp các công cụ hay dịch vụ đảm bảo an toàn thông tin
    - Phá giải mã (cryptanalysis): nghiên cứu các kỹ thuật toán học phục vụ phân tích phá mật mã và/hoặc tạo ra các đoạn mã giản nhằm đánh lừa bên nhận tin.

## Hệ mật cổ điển

### Một số định nghĩa

Mật mã khóa đối xứng là một loại sơ đồ mã hóa trong đó một khóa giống nhau sẽ vừa được dùng để mã hóa, vừa được dùng để giải mã các tệp tin. Phương pháp mã hóa thông tin này đã được sử dụng khá phổ biến từ nhiều thập kỷ với mục đích tạo ra cách thức liên lạc bí mật giữa chính phủ với quân đội. Ngày nay, các thuật toán khóa đối xứng được ứng dụng rộng rãi trên nhiều hệ thống máy tính khác nhau, nhằm tăng cường bảo mật cho dữ liệu.

* Bản rõ (plaintext-M): bản tin được sinh ra bởi bên gửi
* Bản mật (ciphertext-C): bản tin che giấu thông tin của bản rõ, được gửi tới bên nhận qua một kênh không bí mật
* Khóa (Ks): nó là giá trị ngẫu nhiên và bí mật được chia sẻ giữa các bên trao đổi thông tin và được tạo ra từ:
  + Bên thứ 3 được tin cậy tạo và phân phối tới bên gửi và bên nhận
  + Hoặc, bên gửi tạo ra và chuyển cho bên nhận

### Các hệ mật thay thế đa biểu

* + - * Yếu điểm của các mã pháp đơn biểu là phân bố tần suất của chúng phản ánh phân bố của bảng chữ cái cơ sở. Một mã pháp an toàn hơn về mặt mật mã sẽ thể hiện phân bố bằng phẳng hơn, điểu này sẽ không cho kẻ thám mã chút thông tin nào.
* Một hướng khác làm tăng độ an toàn cho mã trên bảng chữ là sử dụng nhiều bảng chữ để mã. Mỗi chữ sẽ được mã bằng bất kì chữ nào trong bản mã tùy thuộc vào ngữ cảnh khi mã hóa. Làm như vậy để trải bằng tần suất các chữ xuất hiện trong bản mã. Do đó làm mất bớt cấu trúc của bản rõ được thể hiện trên bản mã và làm cho mã thám đa bảng khó hơn.
* Độ dài khoá là chu kì lặp của các bản chữ. Độ dài càng lớn và nhiều chữ kahcs nhau được sử dụng trong từ khoá thì càng khó thám mã

### Hệ Vigenere Cipher

* Tác giả: Blaise de Vigènere (1523 – 1596)
* Đây là dạng mã thay thế đa biểu đơn giản nhất.
* Ý tưởng:
  + Sử dụng một loạt mã Caesar khác nhau dựa trên các kí tự của một từ khóa phụ thuộc vào vị trí của chữ đó trong bản rõ và được lấy trong từ khoá theo thứ tự tương ứng

### Các hệ mật thay thế không tuần hoàn

Vigenere đề xuất hệ mật khoá tự sinh

1. **Định nghĩa:**

Việc sử dụng nhiều bản chữ cái để không thể nhận diện được phân bố và không có mẫu trong suốt đối với việc lựa chọn một bảng chữ cái tại một điểm cụ thể.

1. **Ý tưởng hệ mã khoá chạy:**

• Từ khoá được nối tiếp bằng chính bản rõ, sau đó sử dụng mã Vigenere để mã

• Khi biết từ khoá, giải được một số chữ của bản rõ rồi dùng chúng giải nốt phần còn lại

• Sự cải tiến này gây mất khái niệm chu kỳ.

1. **Ứng dụng:**

• Áp dụng trong việc mã hoá thông tin.

# Chương 2: Hệ mã khoá chạy

## 2.1 Tính chất

Hệ mã khoá chạy có nhiều đặc điểm và tính chất giống với mật mã Vigenere. Sự khác biệt gữa hai hệ này là ở cách chọn khoá để mã hoá. Với hệ mã Vigenere, nó sử dụng một khoá ngắn và lặp lại cho bằng với chiều dài của bản rõ. Trong khi đó, hệ mã khoá chạy thì sử dụng một khoá dài, chẳng hạn như một đoạn trích từ một cuốn sách, hoặc có thể là chính từ bản rõ, nối tiếp vào khoá ban đầu. Điều này giúp cho khoá không bao giờ lặp lại, khiến cho việc phân tích mật mã trở nên khó khăn hơn.

## 2.2 Cơ chế hoạt động

### 2.2.1 Giải thuật

- Input: Thông điệp đưa vào ở bản rõ hoặc là bản mã hoá và Khoá

- Output: Thông điệp được mã hoá hoặc là bản rõ

**a. Mã hoá**

**Bước 1:** Tạo khoá

* Gán thêm vào khoá ban đầu những kí tự từ bản rõ đến khi nào chiều dài của khoá và bản rõ là bằng nhau

**Bước 2:** Xác định vị trí

* Từng kí tự ở bản rõ và key tương ứng vị trí thứ [ i ] sẽ được so với vị trí trong bảng mã được sử dụng

**Bước 3:** Mã hoá

* Từng kí tự ở bản rõ và bản mã sau khi được lấy vị trí, sẽ được mã hoá theo công thức:
  + Ci = (Pi + Ki) mod 26

**Bước 4:** Thu thông điệp mã hoá hoàn chỉnh

**b. Giải mã**

**Bước 1:** Giải mã cho chuỗi có độ dài bằng khoá

* Từng kí tự vị của bản mã hoá và khoá tại vị trí thứ [ i ] được xác định trong bảng mã
* Từ các vị trí trên, các kí tự bản rõ sẽ được giải mã theo công thức:
  + Pi  = (Ci – Ki) mod 26

**Bước 2:** Tạo khoá

* Lúc này ta thu được các kí tự của bản rõ, lần lượt ta nối chúng vào chuỗi khoá trên

**Bước 3:** Lặp lại quá trình của bước 1 và bước 2 đến khi nhận được bản rõ có chiều dài bằng với bản mã hoá

**Bước 4:** Lúc này ta thu được thông điệp hoàn chỉnh của thông điệp ban đầu

**VD:**

* Bản mã được sử dụng: abcdefghijklmnopqrstuvwxyz
* Input:
  + Plaintext: toilasinhvien
  + Key: attt
* Output: thbetgqyhnqru

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Key | a | t | t | t | t | o | i | l | a | s | i | n | h |
| Plaintext | t | o | i | l | a | s | i | n | h | v | i | e | n |
| Ciphertext | t | h | b | e | t | g | q | y | h | n | q | r | u |

## 2.3 Hệ mã khoá chạy biểu diễn bằng ngôn ngữ lập trình ( Sử dụng ngôn ngữ Python)

### a. Mã hoá

Text

Description automatically generated

### b. Giải mã

Text

Description automatically generated

## 2.3 Xây dựng App trên cơ sở đã xây dựng

### 2.3.1 Giao diện

Graphical user interface, application

Description automatically generated

### 2.3.2 Hoạt động

a. Mã hoá:

* Bản mã được sử dụng: abcdefghijklmnopqrstuvwxyz
* Input:
  + Plaintext: toilasinhvien
  + Key: attt
* Output: thbetgqyhnqru

Graphical user interface, application

Description automatically generated

b. Giải mã:

* Bản mã được sử dụng: abcdefghijklmnopqrstuvwxyz
* Input:
  + Plaintext: avavtgxkvwznnewvd
* Key: thoi tiet
* Output: homnaytroinangdep

Graphical user interface, application, Teams

Description automatically generated

2.4 Ứng dụng

Hệ mã khoá chạy để sử dụng trong mã hoá cơ bản, tính bảo mật của hệ mã khoá chạy là cao. Với khoá được chọn ngẫu nhiên và bản rõ đủ dài, thì việc phá khoá là rất khó khăn.

## 2.5 Hạn chế

Tuy vấn đề của các hệ mã trước được giải quyết, nhưng không có sự hoàn hảo. Hệ mã khoá chạy cũng vậy. Vì khoá được sử dụng là từ chính bản rõ, hoặc được lấy từ một văn bản ngẫu nhiên, entropy của mỗi kí tự là thấp. Từ đó việc thám mã có thể xảy ra. Khi đó người thám mã có thể xác định một phần của văn bản và xác định thử các trường hợp của bản rõ, nếu nó là một đoạn văn bản dễ dàng để hiểu thì đấy có thể là bản rõ cần tìm tại phần đó của văn bản. Từ đó, người thám mã có thể mở rộng để có thể xác định tiếp tục các phần sau của bản mã, từ đó hoàn toàn có thể suy ra được bản rõ hoàn chỉnh.

# Chương 3: Kết luận

* Hiện nay có rất nhiều loại mã khác, cũng như là các loại hàm băng có tính bảo mật cao hơn rất nhiều và bên cạnh đó là vấn đề bảo đảm ba tính chất của an toàn thông tin (tam giác CIA).
* Tuy độ khó khi phá khoá là vậy, nhưng việc sử dụng brute force để tấn công cũng không thể loại trừ và mọi thứ đều chỉ mang tính tương đối.