TRƯỜNG ĐẠI HỌC MỎ - ĐỊA CHẤT

KHOA CÔNG NGHỆ THÔNG TIN

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



CƠ SỞ AN NINH MẠNG

TÌM HIỂU VỀ MẬT MÃ CỔ ĐIỂN

|  |  |
| --- | --- |
| Giảng viên hướng dẫn:  Sinh viên thực hiện:  Mã lớp học phần: 7080703-22 | ThS. Đào Anh Thư  1.Bùi Đức Thắng – 2121050765 (nhóm trưởng)  2.Trần Đức Vương – 2121050106  3.Hoàng Thắng Lợi – 2121051235  4.Lê Đình Đạt – 2121051332  5.Đào Trung Sơn – 2121050142 |

**Hà Nội –** **2023**

**MỤC LỤC**

[1. GIỚI THIỆU VỀ MẬT MÃ CỔ ĐIỂN 3](#_Toc151949738)

[1.1 Lịch sử phát triển 3](#_Toc151949739)

[1.2 Khái niệm liên quan 3](#_Toc151949740)

[2. MẬT MÃ KHÓA ĐỐI XỨNG 3](#_Toc151949741)

[2.1 Khái niệm cơ bản về mật mã 3](#_Toc151949742)

[2.2 Mật mã khóa đối xứng 4](#_Toc151949743)

[3. MẬT MÃ CỔ ĐIỂN VÀ MẬT MÃ HIỆN ĐẠI 6](#_Toc151949744)

[3.1 Sự phân biệt giữa mật mã cổ điển và mật mã hiện đại 6](#_Toc151949745)

[3.2 Sự tiến bộ trong mật mã hiện đại 8](#_Toc151949746)

[3.3 Ứng dụng của mật mã cổ điển và mật mã hiện đại trong thế giới hiện đại 9](#_Toc151949747)

[4. HỆ MẬT MÃ HOÁN VỊ 12](#_Toc151949748)

[4.1 Khái niệm và nguyên tắc hoạt động 12](#_Toc151949749)

[4.2 Ví dụ về hệ mật mã hoán vị 13](#_Toc151949750)

[5. Hệ mật mã Caesar 15](#_Toc151949751)

[5.1 Khái niệm 15](#_Toc151949752)

[5.2 Phương pháp mã hoá 15](#_Toc151949753)

[5.3 Ví dụ 16](#_Toc151949754)

[5.4 Đặc điểm 17](#_Toc151949755)

[6. HỆ MẬT MÃ VIGENÈRE 17](#_Toc151949756)

[6.1 Khái niệm và lịch sử 17](#_Toc151949757)

[6.2 Nguyên tắc hoạt động 18](#_Toc151949758)

[6.3 Điểm mạnh và yếu của hệ mật mã Vigenère 27](#_Toc151949759)

[7. HỆ MẬT MÃ PLAYFAIR 28](#_Toc151949760)

[7.1 Khái niệm và lịch sử 28](#_Toc151949761)

[7.2 Điểm mạnh và điểm yếu của hệ mật mã playfair 32](#_Toc151949762)

# 1. GIỚI THIỆU VỀ MẬT MÃ CỔ ĐIỂN

## 1.1 Lịch sử phát triển

Trong lịch sử phát triển của nhân loại, từ khi con người xuất hiện nhu cầu trao đổi thông tin với nhau thì nhu cầu giữ bí mật và đảm bảo tính an toàn của những thông tin đó cũng xuất hiện theo. Đó có thể là những thông tin quân sự quan trọng không thể để lộ ra cho kẻ thù, những âm mưu được ấp ủ, chỉ được thông báo cho những người liên quan, những ghi chép về kho báu hay thậm chí là thư từ cá nhân.​

​ Sự cần thiết của việc tìm ra một phương pháp đơn giản, hiệu quả để đảm bảo an toàn cho một thông điệp cần gửi đi chính là nguyên nhân của sự hình thành mật mã.​

​ Và cuộc chiến giữa một bên luôn muốn che giấu thông tin của mình còn một bên luôn muốn đọc được những thông tin đó đã thúc đẩy mật mã ngày càng phát triển.​

## 1.2 Khái niệm liên quan

**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.

Hai lĩnh vực con này tồn tại như hai mặt đối lập, “đấu tranh để cùng phát triển” của một thể thống nhất là ngành khoa học mật mã (cryptology). Tuy nhiên, do lĩnh vực thứ hai (cryptanalysis) ít được phổ biến quảng đại nên dần dần, cách hiểu chung hiện nay là đánh đồng hai thuật ngữ cryptography và cryptology. Theo thói quen chung này, hai thuật ngữ này có thể dùng thay thế nhau. Thậm chí cryptography là thuật ngữ ưa dùng, phổ biến trong mọi sách vở phổ biến khoa học, còn cryptology thì xuất hiện trong một phạm vi hẹp của các nhà nghiên cứu học thuật thuần túy.​

​

**Plaintext**: Văn bản ban đầu khi chưa được mã hóa, thường được gọi là bản rõ.​

​

**Ciphertext**: Văn bản sau khi đã được mã hóa, thường được gọi là bản mã.​

​

**Encrypt**: Hành động biến đổi bản rõ thành bản mã, sử dụng một thuật toán mã hóa nào đó.​

​

**Decrypt**: Hành động biển đổi bản mã thành bản rõ, sử dụng thuật toán giải mã tương ứng với thuật toán mã hóa đã được sử dụng để tạo ra bản mã.​

# 2. MẬT MÃ KHÓA ĐỐI XỨNG

## 2.1 Khái niệm cơ bản về mật mã

**Khái niệm :**

Mật mã khóa đối xứng (symmetric encryption) là phương pháp sử dụng chung một khóa bí mật để cả mã hóa và giải mã.

Khóa bí mật là thông tin quan trọng quyết định tính bảo mật của thông điệp. Chỉ cần thay đổi khóa, toàn bộ thuật toán mã hóa sẽ thay đổi.

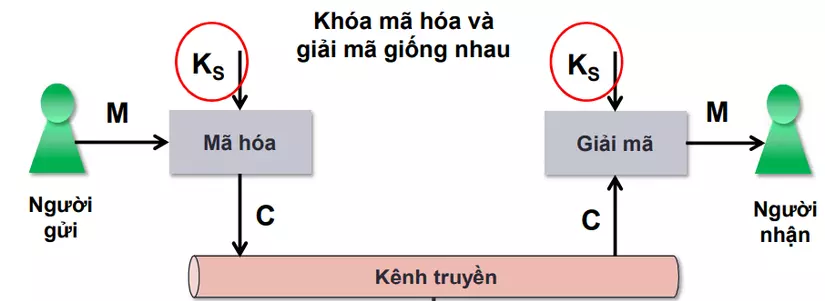
Các thành phần chính bao gồm: Thuật toán mã hóa (AES, DES, RC4...), khóa bí mật, thông điệp ban đầu và thông điệp đã mã hóa.

Quá trình mã hóa: Sử dụng thuật toán và khóa bí mật để biến đổi thông điệp thành dữ liệu khó hiểu.

Quá trình giải mã: Sử dụng chính xác cùng khóa bí mật và thuật toán ngược lại để phục hồi lại nội dung ban đầu.

Ưu điểm : Tính đơn giản, hiệu quả và thường dùng cho giao tiếp song phương.

Nhược điểm : khó quản lý và phân phối khóa bí mật an toàn.



## 2.2 Mật mã khóa đối xứng

**1. Nguyên tắc hoạt động**

Nguyên tắc hoạt động của mật mã hóa đối xứng là cùng sử dụng một khóa bí mật cho cả quá trình mã hóa và giải mã. Khóa này phải được lưu trữ bí mật và chỉ truy cập được bởi các bên tham gia giao tiếp.

Quá trình mã hóa: Bên gửi sử dụng khóa bí mật kết hợp với thuật toán mã hóa để biến đổi thông điệp thành dữ liệu mã hóa.

Quá trình truyền tải: Dữ liệu đã được mã hóa được truyền trên kênh truyền tải. Do đã được mã hóa nên người không phải là bên tham gia giao tiếp không thể đọc được nội dung.

Quá trình giải mã: Bên nhận cũng sử dụng chính xác cùng khóa bí mật để kết hợp với thuật toán giải mã ngược lại quá trình mã hóa, phục hồi lại nội dung ban đầu.

Nếu không sử dụng đúng khóa, dữ liệu sẽ không thể giải mã được.

1. **Sự cần thiết của khóa bí mật**

Khóa bí mật là thành phần quan trọng nhất quyết định tính bảo mật của thông điệp đã được mã hóa. Chỉ cần biết khóa mà không cần biết thuật toán, người ta có thể mã hóa và giải mã thông điệp.

Khóa bí mật xác định cách thức thuật toán áp dụng lên từng ký tự, xác định kết quả phép biến đổi cuối cùng. Chỉ cần thay đổi khóa, toàn bộ quá trình mã hóa sẽ thay đổi.

Bảo mật khóa là yếu tố quyết định tính bảo mật của việc truyền tải thông điệp mã hóa. Chỉ cần khóa bị lộ, kẻ tấn công có thể dễ dàng giải mã thông điệp.

Sự cần thiết của việc bảo mật khóa là khối lượng công việc đáng kể trong việc quản lý, trao đổi và lưu trữ khóa mã hóa một cách an toàn.

1. **Đặc điểm và ứng dụng**

- Đặc điểm :

+ Tính đơn giản: Ưu điểm lớn nhất là chỉ cần sử dụng 1 khóa duy nhất cho cả quá trình mã hóa và giải mã, thuật toán tương đối đơn giản so với mã khóa công khai.

+ Hiệu suất cao: Quá trình mã hóa và giải mã diễn ra rất nhanh do không cần thực hiện các phép toán tính toán phức tạp. Thích hợp cho truyền tải dữ liệu lớn.

+ Bảo mật vừa phải: Miễn là khóa được bảo mật tốt thì mức độ an toàn cao, tuy nhiên nguy cơ mất an toàn nếu khóa bị đánh cắp.

+ Tính bảo mật phụ thuộc hoàn toàn vào việc bảo vệ tính bí mật của khóa. Nếu khóa bị lộ sẽ dễ dàng giải mã thông điệp.

+ Khả năng mở rộng hạn chế do khó quản lý và phân phối khóa cho nhiều đối tượng.



- Ứng dụng :

+ Giao tiếp truyền thông trực tiếp: Mã hóa dữ liệu cuộc gọi trên GSM, kết nối di động 3G/4G, WLAN, Bluetooth, ZigBee.

+ Lưu trữ dữ liệu phân tán và bí mật: Mã hóa dữ liệu trên ổ cứng máy tính, thẻ nhớ di động, flash drive, hệ thống mạng SAN/NAS.

+ Mạng VPN/VLAN riêng: Tạo kênh truyền thông mã hóa an toàn giữa các nội bộ mạng riêng biệt trên Internet.

+ Cơ sở dữ liệu: Mã hóa các bảng dữ liệu nhạy cảm trong cơ sở dữ liệu.

+ E-commerce: Mã hóa thông tin thanh toán trực tuyến, giao dịch ngân hàng trên website, ứng dụng di động.

+ Quản lý tài liệu: Mã hóa tài liệu trong hệ thống quản lý tài liệu điện tử.  
  
**2.3.Ví Dụ**

Giả sử Alice muốn gửi một thông điệp bí mật cho Bob. Họ đã trước đó thống nhất sử dụng mã khoá đối xứng AES với khóa chia sẻ giữa họ là "SECRETKEY123".

Bước 1: Mã hóa thông điệp

Thông điệp của Alice: "Hello, Bob! Meet me at the park."

Alice sử dụng khóa đối xứng "SECRETKEY123" và thuật toán AES để mã hóa thông điệp.

Kết quả mã hóa được gửi cho Bob: "U2FsdGVkX1+uQvMw5y/5sGcbKlTb9u4B1gjG0Uk2N6A8K3DGJp9/pRXEgS0=".

Bước 2: Gửi thông điệp mã hóa

Alice gửi thông điệp mã hóa đến Bob thông qua kênh truyền thông.

Bước 3: Giải mã thông điệp

Bob nhận được thông điệp mã hóa từ Alice: "U2FsdGVkX1+uQvMw5y/5sGcbKl

Bob sử dụng khóa đối xứng "SECRETKEY123" và thuật toán AES để giải mã thông điệp.

Kết quả giải mã: "Hello, Bob! Meet me at the park."

# 3. MẬT MÃ CỔ ĐIỂN VÀ MẬT MÃ HIỆN ĐẠI

## 3.1 Sự phân biệt giữa mật mã cổ điển và mật mã hiện đại

* **Định nghĩa và khái niệm** cơ bản về mật mã cổ điển và mật mã hiện đại:

Mật mã cổ điển: Là hình thức mật mã được sử dụng từ thời cổ đại và trước sự ra đời của máy tính. Đây là những phương pháp mã hóa thông tin sử dụng các thuật toán cơ bản như thay thế, hoán đổi ký tự hay nhóm ký tự.

Mật mã hiện đại: Là hình thức mật mã được phát triển sau sự ra đời của máy tính và sử dụng các thuật toán phức tạp hơn, tích hợp các khái niệm toán học và khoa học máy tính.

* **Sự khác biệt** trong cách thức hoạt động và cấu trúc của mật mã cổ điển và mật mã hiện đại:

Mật mã cổ điển: Thường sử dụng các phương pháp đơn giản như thay thế, hoán đổi ký tự hay nhóm ký tự. Cấu trúc đơn giản và dễ hiểu, nhưng dễ bị giải mã bởi các phương pháp tấn công như phân tích tần số.

Mật mã hiện đại: Sử dụng các thuật toán phức tạp hơn như mã khóa công khai và mã khóa đối xứng. Cấu trúc phức tạp và khó hiểu, đòi hỏi kiến thức toán học và khoa học máy tính để xây dựng và giải mã

.

* **Ưu điểm và nhược điểm** của mật mã cổ điển và mật mã hiện đại:
* Mật mã cổ điển:

**Ưu điểm**: Dễ hiểu và triển khai, không yêu cầu sự phức tạp trong tính toán.

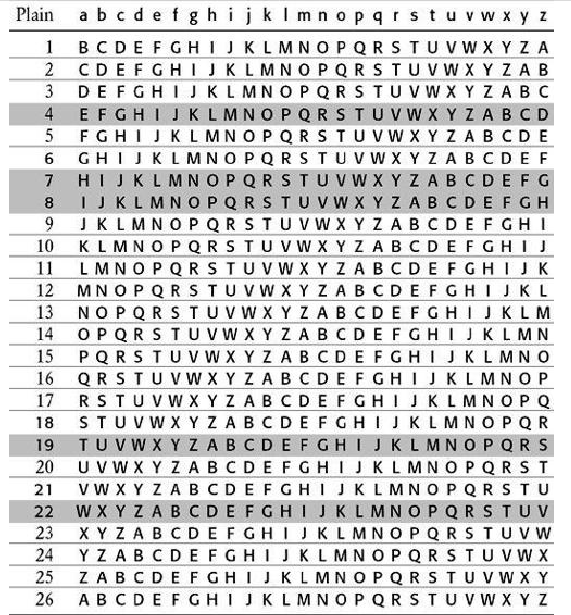
**Nhược điể**m: Dễ bị giải mã bởi các phương pháp tấn công thông thường, không đảm bảo độ bảo mật cao.

* Mật mã hiện đại:

**Ưu điểm**: Đảm bảo độ bảo mật cao hơn, khó bị giải mã bởi các phương pháp tấn công thông thường.

**Nhược điểm**: Đòi hỏi tính toán phức tạp, cần kiến thức chuyên sâu về toán học và khoa học máy tính để triển khai và giải mã.  
**Ví dụ** về các thuật toán mật mã cổ điển như Caesar, Vigenere và thuật toán mật mã hiện đại như RSA, AES:

* Mật mã cổ điển:



Ví dụ: Thuật toán Caesar - là phương pháp thay thế ký tự trong bản rõ bằng cách dịch chuyển chúng một số khoảng cố định trong bảng chữ cái.

Ví dụ: Thuật toán Vigenere - sử dụng một từ khoá để thay thế từng ký tự trong bản rõ bằng cách dịch chuyển chúng theo vị trí tương ứng trong từ khoá.

* Mật mã hiện đại:

Ví dụ: Thuật toán RSA - sử dụng cặp khóa công khai và khóa bí mật để mã hóa và giải mã thông tin. Sự bảo mật dựa trên tính khó giải mã của việc phân tích yếu to của số nguyên tố lớn.

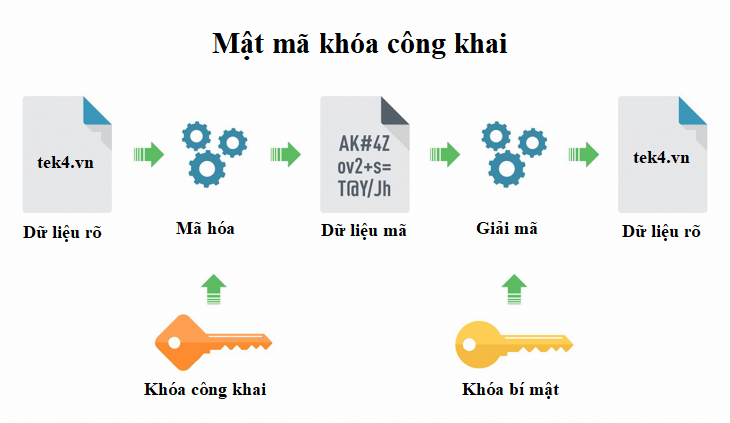
Ví dụ: Thuật toán AES - Advanced Encryption Standard là một thuật toán mật mã đối xứng tiêu chuẩn được sử dụng rộng rãi trong các ứng dụng mật mã hiện đại. Nó sử dụng các phép biến đổi không tuyến tính và thao tác trên các khối dữ liệu để đảm bảo tính bảo mật cao.

* **Tính ứng dụng và sự phát triển của mật mã cổ điển và mật mã hiện đại:**

Mật mã cổ điển: Hiện nay, mật mã cổ điển thường chỉ được sử dụng cho mục đích giả trí hoặc trong việc khôi phục lại các phương pháp mã hóa cổ điển để hiểu và nghiên cứu.

Mật mã hiện đại: Là hình thức mật mã phổ biến và được sử dụng rộng rãi trong các ứng dụng bảo mật thông tin như giao dịch ngân hàng trực tuyến, truyền thông an toàn, và bảo vệ dữ liệu cá nhân.

## 3.2 Sự tiến bộ trong mật mã hiện đại

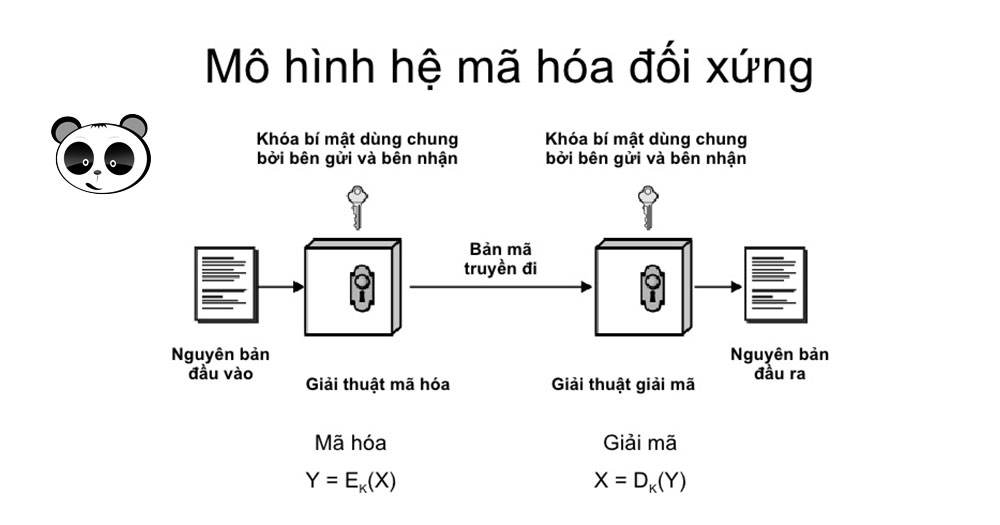
* **Mật mã khóa công khai:**

Mật mã khóa công khai, còn được gọi là mật mã không đối xứng, đã trải qua sự tiến bộ đáng kể trong thời gian gần đây. Đây là một hệ thống mật mã sử dụng hai khóa khác nhau: khóa công khai để mã hóa thông tin và khóa bí mật để giải mã. Sự tiến bộ trong mật mã khóa công khai đã tạo ra các thuật toán mã hóa mạnh hơn và bảo mật hơn, đảm bảo tính bí mật và toàn vẹn của dữ liệu.

Một trong những tiến bộ quan trọng trong mật mã khóa công khai là sự phát triển của thuật toán ECC (Elliptic Curve Cryptography). ECC sử dụng các tính chất của đường cong elliptic để tạo ra các khóa khác nhau, từ đó cung cấp tính bảo mật cao hơn so với các thuật toán truyền thống khác. Với cùng mức bảo mật, ECC sử dụng khóa ngắn hơn so với các thuật toán khác như RSA, điều này giúp tăng tốc độ mã hóa và giải mã thông tin và tiết kiệm tài nguyên hệ thống.

Ngoài ra, mật mã khóa công khai cũng đã phát triển các thuật toán mã hóa mới như RSA-OAEP (Optimal Asymmetric Encryption Padding), ECIES (Elliptic Curve Integrated Encryption Scheme) và GPG (Gnu Privacy Guard). Các thuật toán này đảm bảo tính bảo mật cao và đáng tin cậy khi áp dụng trong các ứng dụng bảo mật trực tuyến, giao dịch điện tử và trên các thiết bị di động.

* **Mật mã đối xứng hiện đại:**



Mật mã đối xứng, hay còn gọi là mật mã cổ điển, đã trải qua sự phát triển đáng kể để đáp ứng các yêu cầu bảo mật ngày càng cao trong thế giới kỹ thuật số. Mật mã đối xứng sử dụng cùng một khóa để mã hóa và giải mã thông tin. Sự tiến bộ trong mật mã đối xứng hiện đại đã tạo ra các thuật toán mã hóa mạnh mẽ và khó khăn trong việc giải mã thông tin.

Một trong những tiến bộ quan trọng nhất trong mật mã đối xứng hiện đại là sự phát triển của thuật toán AES (Advanced Encryption Standard). AES đã thay thế thuật toán DES (Data Encryption Standard) cũ kỹ và trở thành tiêu chuẩn mã hóa đối xứng hàng đầu. AES sử dụng các khối mã hóa có kích thước 128 bit, 192 bit hoặc 256 bit, tạo ra một hệ thống mã hóa mạnh mẽ và khó khăn trong việc giải mã thông tin.

Ngoài ra, mật mã đối xứng hiện đại cũng đã phát triển các thuật toán mã hóa mới như Twofish, Serpent và Camellia. Các thuật toán này cung cấp tính bảo mật cao và khả năng chống lại các cuộc tấn công từ các kỹ thuật tấn công tiên tiến như tấn công dựa trên bảng giá trị (table-based attacks) và tấn công phân tích thông tin (side-channel attacks).

## 3.3 Ứng dụng của mật mã cổ điển và mật mã hiện đại trong thế giới hiện đại

Mật mã, cả cổ điển và hiện đại, đóng vai trò vô cùng quan trọng trong việc bảo vệ thông tin và đảm bảo an ninh trong thế giới kỹ thuật số ngày nay. Các thuật toán và công nghệ mật mã đã được áp dụng rộng rãi trong nhiều lĩnh vực và ứng dụng, từ giao dịch điện tử, truyền thông, đến bảo vệ dữ liệu cá nhân. Dưới đây là một số ứng dụng phổ biến của mật mã cổ điển và mật mã hiện đại trong thế giới hiện đại:

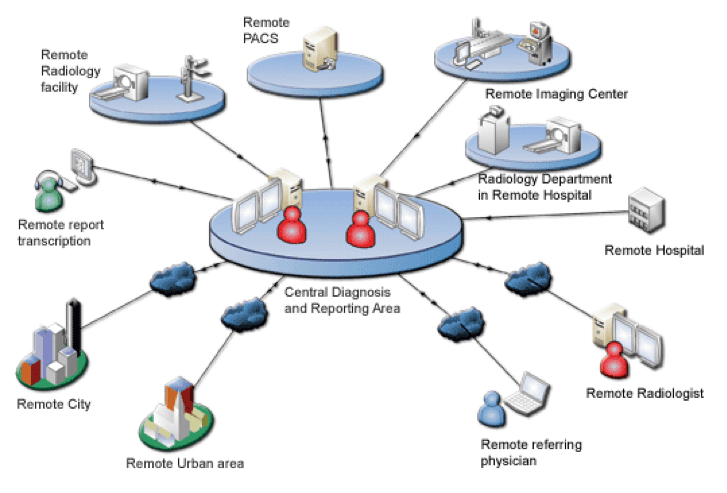
1. Bảo mật thông tin truyền tải:

Mật mã được sử dụng để bảo vệ thông tin truyền tải qua mạng internet và các kênh truyền thông khác. Mật mã đảm bảo tính bí mật và toàn vẹn của dữ liệu, ngăn chặn các cuộc tấn công từ việc nghe trộm, giả mạo và thay đổi thông tin. Việc áp dụng mật mã khóa công khai và mật mã đối xứng trong việc mã hóa và giải mã thông tin đã đảm bảo an toàn cho các giao dịch trực tuyến, email, các ứng dụng nhắn tin và truyền thông trực tuyến khác.

1. Bảo vệ dữ liệu cá nhân: Mật mã đóng vai trò quan trọng trong việc bảo vệ dữ liệu cá nhân và thông tin nhạy cảm. Sử dụng các thuật toán mật mã, dữ liệu được mã hóa trước khi được lưu trữ hoặc truyền tải, ngăn chặn việc truy cập trái phép và lộ thông tin cá nhân. Điển hình là việc sử dụng mật mã để bảo vệ thông tin tài khoản ngân hàng, thông tin thẻ tín dụng và các dữ liệu cá nhân trên các nền tảng trực tuyến như mạng xã hội, trang web mua sắm và các ứng dụng di động.



1. Bảo mật trong các ứng dụng điện toán đám mây: Với sự gia tăng của các dịch vụ điện toán đám mây, mật mã đóng vai trò quan trọng trong việc bảo mật dữ liệu và bảo vệ quyền riêng tư của người dùng. Các nhà cung cấp dịch vụ điện toán đám mây sử dụng mật mã để mã hóa dữ liệu của khách hàng, ngăn chặn việc truy cập trái phép và đảm bảo tính toàn vẹn của dữ liệu trong quá trình lưu trữ và truyền tải.
2. Bảo mật trong các thiết bị di động: Mật mã đóng vai trò quan trọng trong việc bảo mật thông tin trên các thiết bị di động như điện thoại di động và máy tính bảng. Các thuật toán mã hóa được sử dụng để bảo vệ dữ liệu cá nhân, thông tin thanh toán và các ứng dụng trên các thiết bị di động. Mật mã cũng được sử dụng để xác thực người dùng và bảo vệ quyền riêng tư trong việc sử dụng các ứng dụng di động.
3. Mật mã trong lĩnh vực y tế: Mật mã đóng vai trò quan trọng trong việc bảo vệ thông tin y tế và đảm bảo tính riêng tư của bệnh nhân. Các hệ thống mật mã được sử dụng để mã hóa và giải mã các hồ sơ y tế, thông tin về bệnh tật và kết quả xét nghiệm, đảm bảo rằng chỉ những người có quyền truy cập mới có thể xem và sửa đổi thông tin này. Việc sử dụng mật mã trong lĩnh vực y tế giúp ngăn chặn các vi phạm về quyền riêng tư và đảm bảo an toàn cho các thông tin nhạy cảm của bệnh nhân.



1. Bảo mật trong hệ thống định danh và xác thực: Mật mã đóng vai trò quan trọng trong việc định danh và xác thực người dùng trong các hệ thống trực tuyến. Các thuật toán mật mã được sử dụng để tạo ra các chứng chỉ số, mã thông báo và chữ ký số để xác minh danh tính của người dùng và đảm bảo tính toàn vẹn của thông tin. Việc sử dụng mật mã trong hệ thống định danh và xác thực giúp ngăn chặn các cuộc tấn công giả mạo và đảm bảo an toàn cho các giao dịch trực tuyến.
2. Bảo mật trong các ứng dụng IoT (Internet of Things): Với sự phát triển của IoT, mật mã đóng vai trò quan trọng trong việc bảo mật các thiết bị kết nối internet và dữ liệu được truyền tải qua mạng. Các thuật toán mã hóa được sử dụng để bảo vệ thông tin và ngăn chặn việc truy cập trái phép vào các thiết bị IoT, đảm bảo tính toàn vẹn và bảo mật của dữ liệu được truyền tải.



1. Bảo mật trong các ứng dụng blockchain: Mật mã đóng vai trò quan trọng trong việc bảo mật các giao dịch và dữ liệu trong các ứng dụng blockchain. Các thuật toán mật mã được sử dụng để tạo ra các chữ ký số và mã hóa dữ liệu trong quá trình giao dịch và lưu trữ trên blockchain. Mật mã đảm bảo tính toàn vẹn và bảo mật của dữ liệu trong hệ thống blockchain, ngăn chặn việc thay đổi và gian lận dữ liệu.

# HỆ MẬT MÃ HOÁN VỊ

## 4.1 Khái niệm và nguyên tắc hoạt động

* Khái niệm:

Cách hoán đổi vị trí của các ký tự trong văn bản gốc. Nguyên tắc hoạt động của hệ mật mã hoán vị dựa trên việc sắp xếp lại các ký tự theo một trật tự mới hoặc dựa trên một quy tắc cụ thể, để tạo ra một văn bản mã hoá không thể đọc được mà chỉ có thể giải mã thông qua việc áp dụng quy tắc hoán vị ngược lại.Hệ mật mã hoán vị là một phương pháp mã hóa thông tin bằng

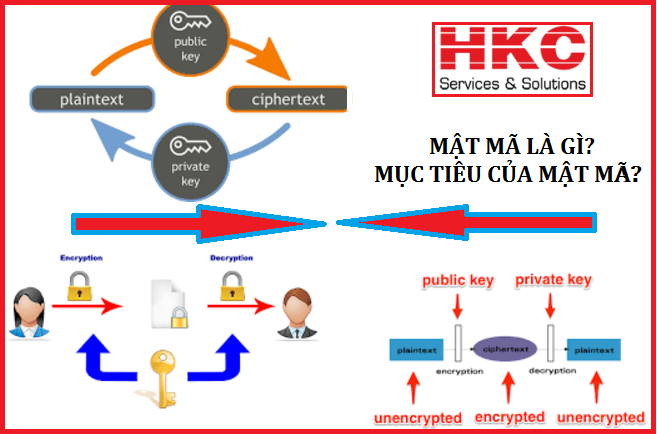
Có nhiều cách để thực hiện hoán vị trong hệ mật mã này. Một trong những cách phổ biến nhất là hoán vị theo một bảng chữ cái. Ví dụ, chúng ta có thể sắp xếp lại các chữ cái theo thứ tự ngược lại, từ Z đến A, hoặc theo một thứ tự ngẫu nhiên đã được xác định trước. Quy tắc hoán vị này sẽ được sử dụng để mã hóa và giải mã thông tin.

Ví dụ, giả sử chúng ta có một văn bản gốc là "HELLO WORLD". Nếu chúng ta sử dụng quy tắc hoán vị là sắp xếp các chữ cái theo thứ tự ngược lại, văn bản mã hoá sẽ trở thành "SVOOL DLOIR". Để giải mã văn bản này, chúng ta chỉ cần áp dụng quy tắc hoán vị ngược lại, tức là sắp xếp các chữ cái theo thứ tự bình thường, và kết quả sẽ là văn bản gốc "HELLO WORLD".

Hệ mật mã hoán vị có ưu điểm là đơn giản và dễ triển khai. Với quy tắc hoán vị đơn giản như sắp xếp các chữ cái theo một thứ tự cụ thể, không cần sử dụng khóa hay thuật toán phức tạp để mã hóa và giải mã thông tin. Điều này làm cho hệ mật mã hoán vị trở thành một lựa chọn phù hợp cho việc mã hóa thông tin trong các tình huống cần tính bảo mật thấp và đơn giản.

Tuy nhiên, hệ mật mã hoán vị cũng có nhược điểm. Do thông tin trong văn bản mã hoá chỉ bị hoán đổi vị trí mà không thay đổi nội dung, nên nó không cung cấp tính bảo mật cao. Nếu kẻ tấn công biết được quy tắc hoán vị hoặc có đủ kiến thức và công cụ để phân tích và phá vỡ quy tắc này, thông tin sẽ dễ dàng được giải mã. Do đó, hệ mật mã hoán vị thường được sử dụng kết hợp với các phương pháp mã hóa khác như mã hóa dịch chuyển, mã hóa thay thế hoặc mã hóa đảo ngược để tăng tính bảo mật và khó khăn trong việc giải mã.

**Nguyên tắc hoạt động :**



Trong các ứng dụng thực tế, hệ mật mã hoán vị được sử dụng rộng rãi trong việc bảo vệ thông tin nhạy cảm, chẳng hạn như trong quân sự, ngân hàng, điện toán và mạng, và còn nhiều ứng dụng khác. Mặc dù hệ mật mã hoán vị có thể đơn giản và dễ triển khai, nhưng để đảm bảo tính bảo mật cao, nó thường được kết hợp với các phương pháp mã hóa khác như mã hóa dịch chuyển, mã hóa thay thế hoặc mã hóa đảo ngược. Khi kết hợp các phương pháp này, thông tin sẽ trở nên khó hiểu hơn và khó bị phá vỡ.

Một ứng dụng phổ biến của hệ mật mã hoán vị là trong việc truyền tải thông tin qua mạng. Khi thông tin cần được bảo vệ trong quá trình truyền tải, hệ mật mã hoán vị có thể được sử dụng để mã hóa thông tin trước khi gửi đi, và người nhận sẽ giải mã để đọc thông tin. Điều này giúp đảm bảo tính bảo mật và ngăn chặn người không có quyền truy cập đọc được thông tin.

Trong quá trình mã hóa và giải mã, việc xác định quy tắc hoán vị là một yếu tố quan trọng. Nếu quy tắc hoán vị được tiết lộ hoặc bị gián đoạn, thông tin sẽ trở nên dễ dàng bị phá vỡ. Do đó, việc bảo vệ quy tắc hoán vị và chỉ cho người có quyền biết là vô cùng quan trọng để đảm bảo tính bảo mật của hệ mật mã hoán vị.

## 4.2 Ví dụ về hệ mật mã hoán vị

1. Mật mã Transposition (đảo vị):  
   Mật mã Transposition là một hình thức của hệ mật mã hoán vị, trong đó các ký tự của văn bản gốc được sắp xếp lại theo một quy tắc hoán vị cụ thể. Một ví dụ cụ thể về mật mã Transposition là mã hoán vị cột (Columnar Transposition). Quy tắc hoán vị này yêu cầu việc viết văn bản gốc thành các cột, rồi sau đó sắp xếp lại các cột theo một thứ tự cụ thể. Văn bản mã hoá sẽ là các ký tự trong các cột đã được sắp xếp lại.

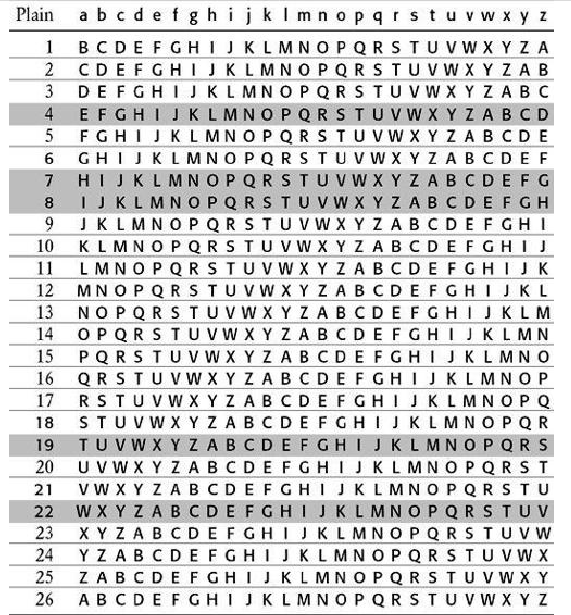
* Ví dụ, giả sử chúng ta có một văn bản gốc là "HELLO WORLD". Chúng ta sẽ viết văn bản này thành các cột, với số cột là một số nguyên dương đã được xác định trước. Đối với số cột là 3, việc viết văn bản sẽ trở thành:

H E L L O  
W O R L D

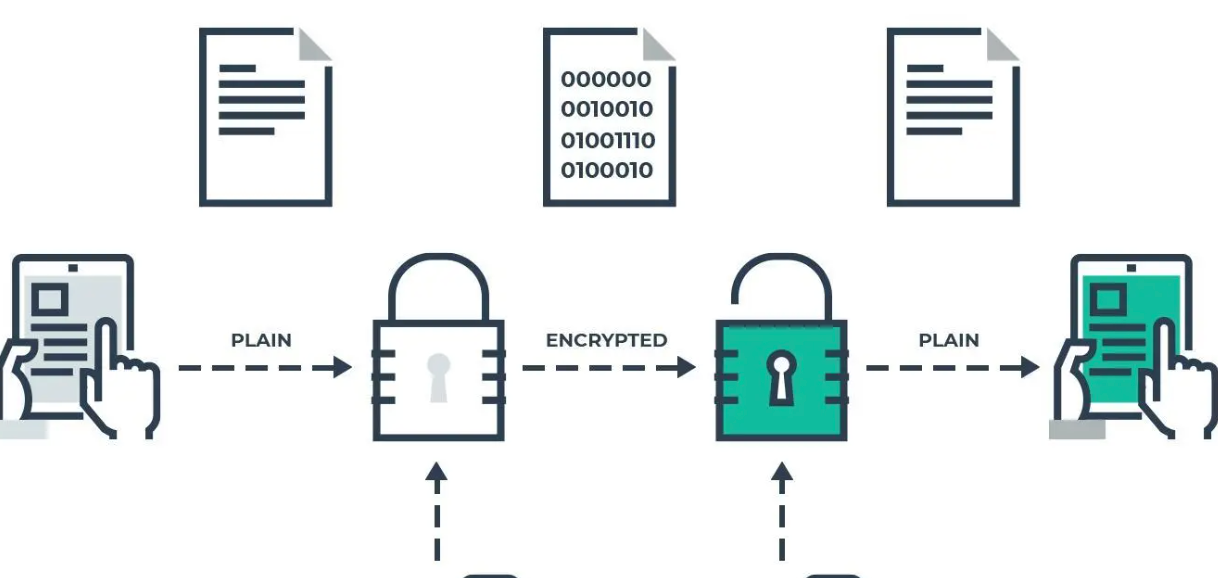
Sau đó, chúng ta sẽ sắp xếp lại các cột theo một thứ tự cụ thể, ví dụ như sắp xếp theo thứ tự từ trái qua phải. Văn bản mã hoá sẽ là:

HWOELLRLDO

Để giải mã thông tin, chúng ta chỉ cần áp dụng quy tắc hoán vị ngược lại, tức là sắp xếp lại các ký tự theo thứ tự ban đầu, và kết quả sẽ là văn bản gốc "HELLO WORLD".



1. Sự so sánh với mật mã khóa đối xứng:

  
 Hệ mật mã hoán vị và mật mã khóa đối xứng là hai hình thức mã hóa thông tin khác nhau. Mật mã khóa đối xứng sử dụng một khóa để mã hóa và giải mã thông tin, trong đó cùng một khóa được sử dụng cả cho quá trình mã hóa và giải mã. Trong khi đó, hệ mật mã hoán vị không sử dụng khóa và chỉ dựa vào quy tắc hoán vị để mã hóa và giải mã thông tin.

Sự khác biệt quan trọng nhất giữa hai hệ mật mã này là tính bảo mật. Mật mã khóa đối xứng có tính bảo mật cao hơn so với hệ mật mã hoán vị. Với mật mã khóa đối xứng, việc giải mã thông tin chỉ có thể thực hiện được nếu có khóa chính xác. Ngược lại, hệ mật mã hoán vị có tính bảo mật thấp hơn, vì thông tin có thể dễ dàng bị phá vỡ nếu quy tắc hoán vị được tiết lộ hoặc bị gián đoạn.

Mật mã khóa đối xứng cũng có thể hỗ trợ việc mã hóa và giải mã các khối dữ liệu lớn hơn, trong khi hệ mật mã hoán vị thường được sử dụng để mã hóa thông tin nhỏ hơn. Do đó, mật mã khóa đối xứng thường được ưu tiên sử dụng trong các ứng dụng cần bảo mật cao và mã hóa dữ liệu lớn.

Tuy nhiên, hệ mật mã hoán vị vẫn có ứng dụng trong nhiều lĩnh vực, như trong việc mã hóa và giải mã dữ liệu nhỏ, truyền thông tin qua mạng, hay trong việc bảo mật thông tin cá nhân nhỏ gọn. Mật mã hoán vị có thể được sử dụng như một phần trong các hệ mật mã phức tạp hơn, để tăng cường tính bảo mật và đa dạng hóa quá trình mã hóa.

# 5. Hệ mật mã Caesar

## 5.1 Khái niệm

Trong mật mã học, mật mã Caesar (Xê da), còn gọi là mật mã dịch chuyển, là một trong những mật mã đơn giản và được biết đến nhiều nhất. Hệ mã Caesar là một hệ mã hóa thay thế đơn âm, làm việc trên bẳng chữ cái tiếng Anh 26 ký tự. Đó là một dạng của mật mã thay thế, trong đó mỗi ký tự trong văn bản được thay thế bằng một ký tự cách nó một đoạn trong bảng chữ cái để tạo thành bản mã.

## 5.2 Phương pháp mã hoá

Thay thế mỗi ký tự bằng một ký tự khác cách nhau một khoảng cách nhất định trong bảng chữ cái.

Đối với bảng mã tiếng anh ( ABCDEFGHI. .. ), nếu độ dịch là 3, A sẽ được thay bằng D, B sẽ được thay bằng E, …, W sẽ thay bằng Z, X sẽ thay bằng A, Y sẽ thay bằng B và Z thay bằng C. Phương pháp được đặt tên theo Caesar, vị hoàng đế đã sử dụng nó liên tục trong việc làm.

A diagram of a diagram of a number of letters

Description automatically generated

## 5.3 Ví dụ

Giả sử chúng ta có thông điệp gốc là "HELLO" và chúng ta muốn mã hóa nó bằng Mật mã Caesar với phép dịch chuyển 3 bước:

Bước 1: Xác định thông điệp gốc và số bước dịch chuyển:

Thông điệp gốc: "HELLO"

Số bước dịch chuyển: 3

Bước 2: Thực hiện phép dịch chuyển trên từng ký tự trong thông điệp:

Ký tự "H" dịch chuyển 3 bước: "K"

Ký tự "E" dịch chuyển 3 bước: "H"

Ký tự "L" dịch chuyển 3 bước: "O"

Ký tự "L" dịch chuyển 3 bước: "O"

Ký tự "O" dịch chuyển 3 bước: "R"

A grid of letters in red and blue

Description automatically generated

Thông điệp đã mã hóa là "KHOOR".

Vậy, thông điệp "HELLO" đã được mã hóa thành "KHOOR" bằng Mật mã Caesar với phép dịch chuyển 3 bước.

## 5.4 Đặc điểm

Đơn giản: Mật mã Caesar là một hệ mật mã đơn giản và dễ hiểu. Việc thực hiện và hiểu cách hoạt động của nó không đòi hỏi kiến thức chuyên sâu về mật mã.

Dịch chuyển theo số bước cố định: Mật mã Caesar dịch chuyển mỗi ký tự trong thông điệp theo một số bước cố định trong bảng chữ cái. Số bước này được gọi là "khóa" và xác định quy tắc dịch chuyển.

Chu kỳ: Trong bảng chữ cái tiếng Anh, có tổng cộng 26 chữ cái. Do đó, Mật mã Caesar có chu kỳ là 26. Nghĩa là nếu ta dịch chuyển một ký tự quá giới hạn của bảng chữ cái, nó sẽ quay trở lại ký tự đầu tiên của bảng chữ cái.

Dễ bị phá vỡ: Mật mã Caesar rất dễ bị phá vỡ bởi kẻ tấn công thông qua phương pháp thử và sai. Vì chỉ có 26 khả năng dịch chuyển, kẻ tấn công có thể thử tất cả các khả năng để tìm ra khóa và giải mã thông điệp.

Khả năng tăng cường bảo mật: Mật mã Caesar có thể được cải tiến bằng cách sử dụng việc dịch chuyển theo một khóa ngẫu nhiên hoặc kết hợp của nhiều phép dịch chuyển. Điều này làm cho việc phá mật mã trở nên khó khăn hơn và tăng tính bảo mật của hệ thống.

Sử dụng trong mục đích giáo dục: Mật mã Caesar thường được sử dụng như một ví dụ đơn giản để giới thiệu các khái niệm cơ bản về mật mã và quy trình mã hóa/giải mã.

# 6. HỆ MẬT MÃ VIGENÈRE

## 6.1 Khái niệm và lịch sử

1. Khái niệm

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

- Hệ mật mã Vigenère là một loại mật mã truyền thống hoặc mật mã đối xứng, được phát minh vào thế kỷ 16 bởi Blaise de Vigenère, một nhà ngôn ngữ học và nhà kryptografie người Pháp. Hệ mật mã Vigenère hoạt động dựa trên việc thay đổi thông điệp ban đầu thành một thông điệp mã hóa bằng cách sử dụng một khóa, thường là một từ hoặc cụm từ bất kỳ.

2. Lịch sử

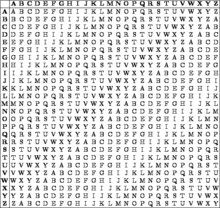
- Phát minh ban đầu: Hệ mật mã Vigenère được phát minh vào cuối thế kỷ 16, khoảng năm 1585, bởi Blaise de Vigenère, người Pháp. Anh ấy viết về phương pháp này trong cuốn sách của mình có tựa đề "Le Traité des Chiffres" (Treatise on Ciphers), nơi anh mô tả cách thực hiện mã hóa và giải mã thông điệp bằng cách sử dụng một chuỗi khóa.

- Đặt tên Vigenère: Hệ mật mã này được đặt tên theo người phát minh, Blaise de Vigenère. Tên "Vigenère" trở thành tên gọi chung cho loại mật mã này.

- Sự phát triển và ứng dụng: Hệ mật mã Vigenère đã được sử dụng rộng rãi trong lịch sử và đã trải qua nhiều phiên bản và biến thể. Nó được sử dụng trong giao tiếp quân sự và chính trị và đã đóng một vai trò quan trọng trong việc bảo mật thông tin trong thời kỳ trước khi các hệ mật mã mạnh mẽ hơn được phát triển.

- Giả mã và phân tích: Hệ mật mã Vigenère đã trải qua nhiều cuộc thử thách và nghiên cứu phân tích trong lịch sử. Trong thế kỷ 19, người ta đã phát triển các phương pháp phân tích để phá vỡ các thông điệp được mã hóa bằng Vigenère, và điều này đã dẫn đến nhận thức về các hạn chế về bảo mật của nó.

- Không còn được sử dụng cho mục đích bảo mật cao cấp: Ngày nay, Hệ mật mã Vigenère không còn được sử dụng cho mục đích bảo mật cao cấp vì nó dễ bị phá vỡ bằng các phương pháp phân tích thống kê và các công cụ máy tính hiện đại. Tuy nhiên, nó vẫn là một phần quan trọng của lịch sử mật mã và là một ví dụ tiêu biểu cho các mật mã đối xứng cổ điển.

**Top of Form**

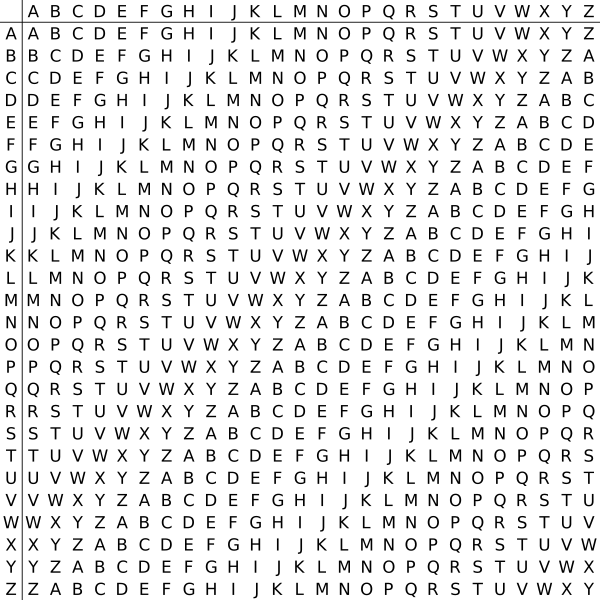
## 6.2 Nguyên tắc hoạt động

- Nguyên tắc hoạt động của Hệ mật mã Vigenère dựa trên việc sử dụng một chuỗi khóa để mã hóa và giải mã thông điệp.

**Cách 1: Dùng bảng** Vigenère

- Sau đây là vài chuẩn bị nho nhỏ cho hệ mật mã Vigenère hoạt động.

+ Đầu tiên, là bảng Vigenère thường là một bảng 26x26, trong đó hàng và cột của bảng chứa các ký tự trong bảng chữ cái tiếng Anh (A-Z).



+ Tiếp theo, chuẩn bị số liệu bao gồm:

* M : tư liệu cần mã hóa
* K : khóa ( 1 xâu kí tự)

+ Yêu cầu: đưa ra được chuỗi kí tự sau mã hóa C

\*Trường hợp khóa K ngắn hơn tư liệu cần mã hóa M, chúng ta có 2 cách:

1. Lặp khóa: gấp đôi khóa K đến bao giờ bằng với tư liệu M
2. Khóa tự động: Autokey = K + M sao cho Autokey = M

Nguyên lí hoạt động: với mỗi kĩ tự ở tư liệu cần mã hóa M, tương ứng với 1 kí tự ở khóa K, chúng ta sẽ dóng vào trong bảng Vigenère, dóng trùng ở đâu thì kí tự đó chính là kĩ tự sau mã hóa, lần lượt như vậy cho đến hết tất cả các kí tự của tư liệu M, qua khóa K ta sẽ được 1 tư liệu mới C có mã hóa là K.

**Ví dụ 1**

Input: + Chuỗi kí tự M = A L L W O R K A N D N O P L A Y M A

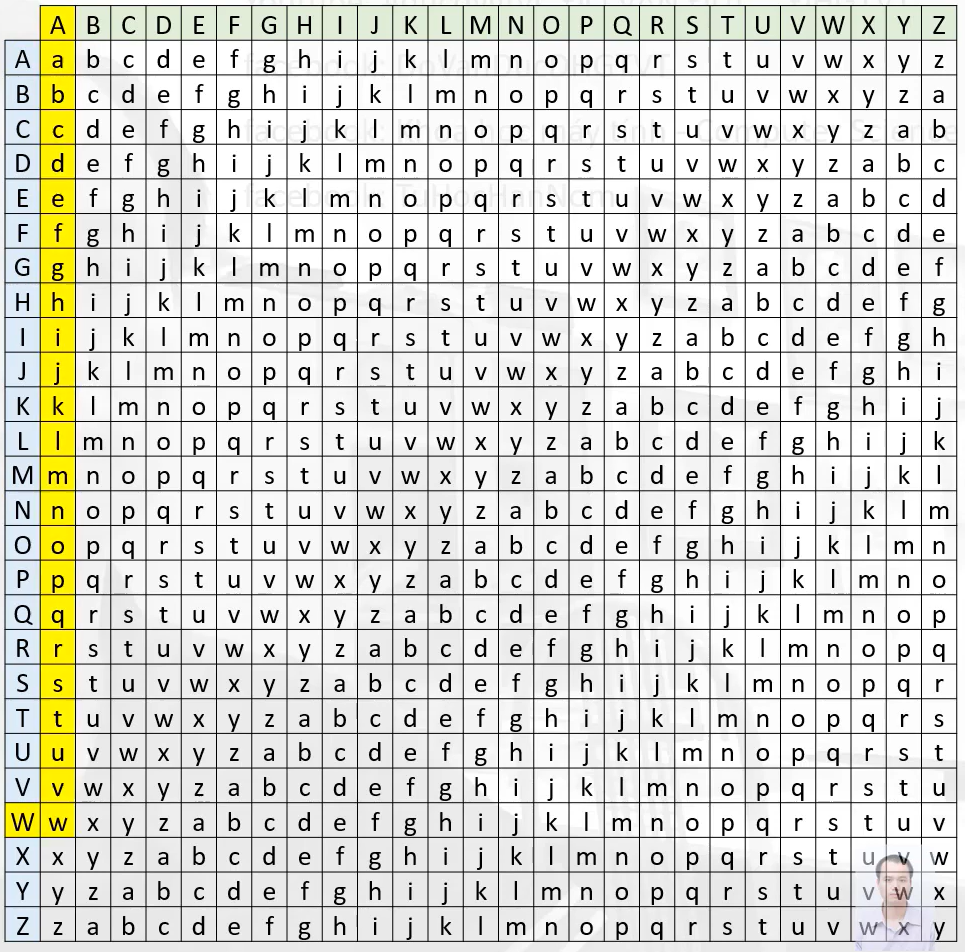
+ Khóa K = W H E N I N R O

* M = A L L W O R K A N D N O P L A Y M A
* K = W H E N I N R O W H E N I N R O W H

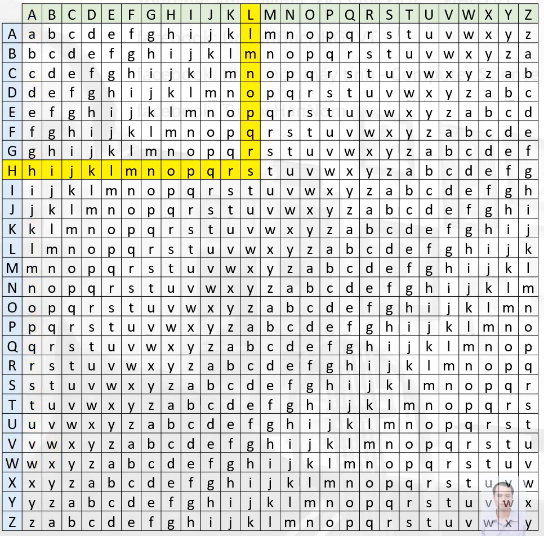
( Kí tự đỏ: được lặp lần 1 của khóa, kí tự xanh là được lặp lần 2 của khóa)

Kí tự đầu tiên A được mã hóa qua W, dóng vào bảng chúng ta được chữ W

* M = A L L W O R K A N D N O P L A Y M A
* K = W H E N I N R O W H E N I N R O W H
* C = W



- Tiếp tục như vậy, kí tự tiếp theo L được mã hóa qua H, dóng vào bảng ta được kí tự S

* M = A L L W O R K A N D N O P L A Y M A
* K = W H E N I N R O W H E N I N R O W H
* C = W S

- Tiếp tục kí tự tiếp theo, L được mã hóa qua E, dóng vào bảng ta được kí tự P

* M = A L L W O R K A N D N O P L A Y M A
* K = W H E N I N R O W H E N I N R O W H
* A screenshot of a crossword

  Description automatically generatedC = W S P

-Tương tự như vậy ta có kí tự sau mã hóa C :

* M = A L L W O R K A N D N O P L A Y M A
* K = W H E N I N R O W H E N I N R O W H
* C = W S P J W E B O J K R B X Y R M I H

**Ví dụ 2:** Cho chuỗi kí tự A = CHAOCACBAN, và khóa

K = XINCHAO, tìm chuối kí tự B sau mã hóa.

- Đầu tiên ta chó chuỗi kí tự A, và khóa K, số kí tự của khóa K ít hơn của chuỗi kí tự A nên chúng ta sẽ gấp đôi khóa K và lấy bằng với số kí tự của chuỗi A.

+ A = C H A O C A C B A N

+K = X I N C H A O X I N

- Ánh xạ vào bảng ta có:

+ A = C H A O C A C B A N

+K = X I N C H A O X I N

+B = Z P N Q J A Q Y I A

**Ví dụ 3:** Cho chuỗi kí tự A = ANNINHMANG, và khóa

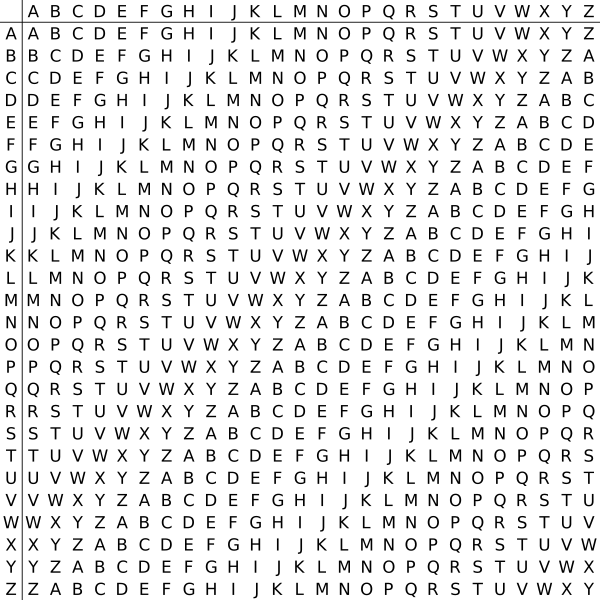
K = FAMILY , tìm chuối kí tự B sau mã hóa.

- A = A N N I N H M A N G

- K = F A M I L Y F A M I

- Ánh xạ vào bảng ta được

- B = F N Z Q Y F R A Z O



**Cách 2:** Ánh xạ lên số theo bảng số:

A yellow and black grid with numbers

Description automatically generated

- Input:

+ Khóa K gồm m kí tự

+ Chuỗi kí tự cần mã hóa M gồm n kí tự

- Output

+ Chuỗi kí tự C sau mã hóa

- Nguyên lí hoạt động:

+ Ánh xạ lên bảng số, chúng ta sẽ chuyển đổi hết các kí tự qua số theo bảng số bên trên và theo m kí tự 1 lần

+ Tiếp theo đó chúng ta cộng các giá trị của M và K sau khi ánh xạ lại

(TH: nếu số cộng lại lớn hơn hặc bằng 26, chúng ta sẽ trừ đi 26)

+ Sau khi cộng xong chúng ta được một dãy số tương ứng với n kí tự

+ Cuối cùng chúng ta chỉ cần ánh xạ lại vào bảng đổi lại từ số qua chữ là chúng ta đã có được 1 đoạn mã hóa bằng phương pháp mã hóa Vigenère

- Tiếp tục với ví dụ trên ta có:

M = A L L W O R K A N D N O P L A Y M A

K = W H E N I N R O

- Ánh xạ qua bảo số ta được:

K = 22 7 4 13 8 13 17 14 ( m = 8 )

M = 0 11 11 22 14 17 10 0

13 3 13 14 15 11 0 24

12 0

Sau khi cộng lại ta được bảng sau:

A grid of numbers with black lines

Description automatically generated

Những giá trị lớn hơn hặc bằng 26 ta tiến hành trừ đi 26 đơn vị:

A grid of numbers with black lines

Description automatically generated

- Sau khi cộng xong ta được xâu kí tự :

C = 22 18 15 35 22 30 27 14 35 10 17 27 23 24 17 38 34 7

C = 22 18 15 9 22 4 1 14 9 10 17 1 23 24 17 12 8 7

-Ánh xạ lại vào bảng ta được:

C = 22 18 15 9 22 4 1 14 9 10 17 1 23 24 17 12 8 7

C = W S P J W E B O J K R B X Y R M I H

Tương tự như đáp án của cách 1

Ví dụ 2: Cho xâu kí tự X = DAIHOCMODIACHAT, khóa

K = CONGNGHE (m = 8)

- Sắp xếp X theo 1 hàng có m = 8 kí tự ta được

X = D A I H O C M O

D I A C H A T

K = C O N G N G H E



- Ánh xạ vào bảng số ta được :

X = 3 0 8 7 14 2 12 14

3 8 0 2 7 0 19

K = 2 14 13 6 13 6 7 4

- Cộng hai dãy vào và trừ đi 26 ( nếu lớn hơn 26 ) ta được

Y = 5 14 21 13 1 8 19 18

5 22 13 8 20 6 0

- Ánh xạ vàng bảng số 1 lần nữa ta được:



Y = F O V N B I J S

F W N I U G A

- Ví dụ 3: Cho xâu kí tự A = C H A O T A M B I E T

Khóa K = H E T



- Ánh xạ bảng số ta được:

A = 2 7 0

14 19 0

12 1 8

4 19

K = 7 4 19

B = 9 11 19

21 23 19

19 5 1

11 23

B = J L T

V X T

T F B

L X

## 6.3 Điểm mạnh và yếu của hệ mật mã Vigenère

- Điểm mạnh của Hệ Mật Mã Vigenère:

* Dài hạn: Hệ mật mã Vigenère khá mạnh trong ngắn hạn và đối với việc mã hóa thông điệp ngắn. Nó có thể ngăn chặn việc đoán đúng thông điệp nếu không có đủ dữ liệu mã hóa.
* Dễ thay đổi khóa: Việc thay đổi khóa làm cho việc mã hóa trở nên khó khăn hơn cho người tấn công. Người sử dụng có thể thay đổi khóa theo một thang đo thời gian hoặc một sự kiện cụ thể.
* Dễ triển khai: Vigenère dễ triển khai mà không cần nhiều tài nguyên tính toán và phức tạp.

- Sự Yếu của Hệ Mật Mã Vigenère:

* Khóa ngắn hạn: Nếu khóa ngắn và không được thay đổi đều đặn, Vigenère trở nên yếu. Người tấn công có thể sử dụng các kỹ thuật tần số để phân tích thông điệp đã mã hóa.
* Bảng Vigenère: Bảng Vigenère tạo ra một mẫu chu kỳ trong quá trình mã hóa, điều này làm cho việc phân tích trở nên dễ dàng hơn cho kẻ tấn công.
* Dễ bị tấn công bằng phân tích tần số: Do sự lặp lại chu kỳ của khóa, Vigenère có thể bị tấn công bằng phân tích tần số. Kẻ tấn công có thể xác định độ dài của chu kỳ và các khóa con.
* Không phù hợp cho bảo mật cao cấp: Vigenère không đáp ứng được nhu cầu bảo mật cao cấp trong thời đại hiện đại, khi có các phương pháp mã hóa mạnh mẽ hơn, như mã hóa đối xứng AES hay RSA.

# 7. HỆ MẬT MÃ PLAYFAIR

## 7.1 Khái niệm và lịch sử

1. Khái niệm

- Mật mã Playfair là một hệ mã hóa nhiều chữ, giảm bớt tương quan giữa văn bản mã hóa và nguyên bản bằng cách mã hóa đồng thời nhiều chữ cái của nguyên bản.

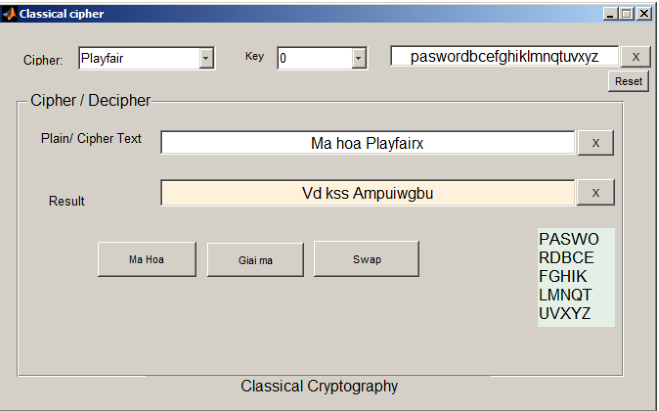
- Một trong những đặc điểm quan trọng của hệ mã hóa Playfair là ma trận Playfair, là một bảng 5x5 chứa 025 ký tự (thường loại bỏ "J" và thay thế bằng "I" để có đủ 26 chữ cái). Ma trận này được sử dụng để ánh xạ các cặp ký tự từ thông điệp gốc thành cặp ký tự đã mã hóa.

B. Nguyên tắc hoạt động

- Hệ mã hóa Playfair hoạt động bằng cách chia thông điệp thành các cặp ký tự (bổ sung "X" nếu cần thiết để tạo cặp chẵn, thêm vào giữa các kí tự trùng), sau đó ánh xạ từng cặp ký tự thành các cặp ký tự mã hóa sử dụng ma trận Playfair. Quá trình này làm thay đổi thông điệp ban đầu và tạo ra thông điệp đã mã hóa.

- Ánh xạ vào bảng 5x5 chứa 25 kí tự trong bảng chữ cái (thường bỏ “J” hoặc “I” để đủ 25 chữ cái) xếp các kí tự có trong khóa Key vào bảng trước, xếp từ trái qua phải, từ trên xuống dưới, những kí tự trùng, đã xếp sẽ bị bỏ qua. Sau khi xếp xong khóa Key vào bảng ta xếp lại các kí tự trong bảng chữ cái lần lượt từ A – Z, những kĩ tự nào trùng với khóa Key thì bỏ qua.

- Trong ánh xạ, chúng ta ánh xạ từ trái qua phải, từ trên xuống dưới và nếu trong trường hợp chéo tạo thành hình chữ nhật ta ánh xạ theo đường chéo còn lại (ưu tiên hàng ngang).



**-Ví dụ 1:**

- Cho xâu kí tự M = HELLOONEANDALL và khóa K = THEDIEIS

Tìm sâu kí tự sau mã hóa C

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | K |
| L | M | N | O | P | Q | R | S | T | U |
| V | W | X | Y | Z |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

- Đầu tiên chúng ta có 1 bảng 5x5, và bảng chữ cái (đã lược bỏ J) như trên hình.

- Tiếp theo đó, ta điền lần lượt các kí tự từ khóa Key vào bảng 5x5 trước rồi các kí tự còn lại của bảng 25 chữ cái, sau khi điền khóa Key ta được

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | K |
| L | M | N | O | P | Q | R | S | T | U |
| V | W | X | Y | Z |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| T | H | E | D | I |
| S | A | B | C | F |
| G | K | L | M | N |
| O | P | Q | R | U |
| V | W | X | Y | Z |

- Sau khi điền các kí tự của khóa Key vào bảng, ta tiếp tục điền các kí tự còn lại ta được- Tiếp theo, ta chia các kí tự ở chuỗi cần mã hóa ra từng cặp, nếu lẻ hoặc trùng thì thêm kí tự “X” vào sau giữa kí tự trùng và sau cùng kí tự lẻ

M = HE LX LO ON EA ND AL LX

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| T | H | E | D | I |
| S | A | B | C | F |
| G | K | L | M | N |
| O | P | Q | R | U |
| V | W | X | Y | Z |

- Sau đó chúng ta sẽ dóng vào bảng 5x5:

- Cặp đầu tiên là HE cùng nằm trên 1 hàng ngang, theo quy tắc thì H =>E, E=>D, sau mã hóa ta được HE=>ED

- Ta được cặp kí tự kết quả đầu tiên ở C = ED

- Tiếp tục là LX, 2 kí tự nằm trên cùng 1 hàng dọc, vậy ta sẽ di chuyển lùi xuống 1 dòng, ta được L=>Q, vì kí tự X ở cuối nên X=>E, sau mã hóa LX=>QE

- C = ED QE

- Cặp tiếp theo LO, là 2 đỉnh của hình chữ nhật, mã hóa ta sẽ lấy 2 đỉnh còn lại L=>G, O=>Q (chúng ta sẽ lấy hàng ngang của kí tự trong TH 2 kí tự tạo thành hình tứ giác), LO=>GQ

- C = ED QE GQ

- Tương tự với các cặp khác ta có

C = ED QE GQ UG HB MI BK QE

**-Ví dụ 2:**

- Cho xâu kí tự M = EMBUONNGUQUA và khóa K = DATELINE

Tìm sâu kí tự sau mã hóa C

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | K |
| L | M | N | O | P | Q | R | S | T | U |
| V | W | X | Y | Z |

M = EM BU ON NG UQ UA

C = CS FR HF IH PR QL

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| D | A | T | E | L |
| I | N | B | C | F |
| G | H | K | M | O |
| P | Q | R | S | U |
| V | W | X | Y | Z |

**Ví dụ 3:**

- Cho xâu kí tự M = VIDUCUOICUNG và khóa K = EMBUONNGU

Tìm sâu kí tự sau mã hóa C

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | K |
| L | M | N | O | P | Q | R | S | T | U |
| V | W | X | Y | Z |

M = VI DU CU OI CU NG

C = XF CO KC BL KC GA

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| E | M | B | U | O |
| N | G | A | C | D |
| F | H | I | K | L |
| P | Q | R | S | T |
| V | W | X | Y | Z |

## 7.2 Điểm mạnh và điểm yếu của hệ mật mã playfair

1. **Sử dụng ma trận Playfair**: Ma trận Playfair là một phần quan trọng của hệ mật mã Playfair và tạo ra một phép biến đổi phức tạp giữa các ký tự. Điều này làm cho việc phân tích thông điệp đã mã hóa trở nên khó khăn hơn so với các hệ mật mã dịch chuyển đơn giản.
2. **Khá hiệu quả đối với tấn công tần số**: Hệ mật mã Playfair khá hiệu quả trong việc đối phó với tấn công tần số, bởi vì nó làm thay đổi phân phối tần số của các ký tự trong thông điệp. Điều này làm cho việc phân tích tần số trở nên khó khăn hơn đối với kẻ tấn công.
3. **Dễ triển khai**: Mật mã Playfair dễ triển khai và thực hiện mà không đòi hỏi nhiều tài nguyên tính toán hoặc kiến thức cao cấp về toán học.

**Điểm Yếu của Hệ Mật Mã Playfair**:

1. **Sự phụ thuộc vào khóa**: Mật mã Playfair dựa vào việc xây dựng ma trận Playfair dựa trên một khóa. Nếu khóa không được chọn cẩn thận, thông điệp có thể dễ bị tấn công.
2. **Khả năng phân tích từ điển**: Mật mã Playfair không thể đối phó hiệu quả với các tấn công từ điển, nơi kẻ tấn công tìm kiếm thông điệp đã mã hóa trong từ điển của các thông điệp thông thường đã biết.
3. **Không đáp ứng bảo mật cao cấp**: Mật mã Playfair không đáp ứng được nhu cầu bảo mật cao cấp trong thời đại hiện đại, khi có các phương pháp mã hóa mạnh mẽ hơn, như AES, RSA, hoặc các biến thể của chúng.