TRƯỜNG ĐẠI HỌC MỎ - ĐỊA CHẤT
KHOA CÔNG NGHỆ THÔNG TIN
BỘ MÔN HỆ THỐNG THÔNG TIN và TRI THỨC

Báo cáo Sinh hoạt học thuật

Đề tài

Nghiên cứu, phân tích thuật toán mã hóa trong An toàn và bảo mật Hệ thống thông tin

Người thực hiện: Dương Chí Thiện

Hà Nội , Tháng 6 năm 2021

MỤC LỤC

Lời nói đầu

Ngày nay với sự phát triển của công nghệ thông tin việc ứng dụng các công nghệ máy tính trở nên vô cùng phổ cập và cần thiết . Sự ra đời và tiến bộ của nó là bước ngoặt trong lịch sử phát triển của xã hội , đưa thế giới từ kỉ nguyên công nghiệp sang kỷ nguyên thông tin và phát triển kinh tế tri thức .Công nghệ mạng máy tính đã mang lại lợi ích to lớn chúng được áp dụng trong hầu hết các công việc trong mọi lĩnh vực : chính trị , quân sự , quốc phòng ....

Sự xuất hiện Internet cho phép mọi người có thể truy cập , chia sẻ và khai thác thông tin một cách dễ dàng và hiệu quả . Các công nghệ E-mail cho phép mọi người có thể gửi thư cho người khác cũng như nhận thư ngay trên máy tính của mình. Gần đây cũng có công nghệ E-business cho phép thực hiện các hoạt động thương mại trên máy tính . Việc ứng dụng các mạng cục bộ trong các tổ chức , công ty hay trong một quốc gia là rất phong phú . Các hệ thống chuyển tiền của các ngân hàng có thể chuyển hàng tỷ dô la qua hệ thống của mình .Các thông tin về kinh tế , chính trị , khoa học xã hội được trao đổi rộng rãi .

Tuy nhiên lại nảy sinh vấn đề về an toàn thông tin .Đó cũng là một quá trình tiến triển hợp logic : khi những vui thích ban đầu về một siêu xa lô thông tin bạn nhất định nhận thấy không chỉ cho phép bạn truy cập vào nhiều nơi trên thế giới ,Internet còn cho phép nhiều người không mời mà tự ý ghé thăm máy tính của bạn .Thật vậy, Internet có những kỹ thuật tuyệt vời ch phép mọi người truy cập, khai thác , chia sẻ thông tin .Nhưng nó cũng là nguy cơ chính dẫn đến thông tin của bạn bị hư hỏng hoặc phá hủy hoàn toàn .

Có những thông tin vô cùng quan trọng mà việc bị mất hay bị làm sai lệch có thể ảnh hưởng tới các tổ chức , các công ty hay cả một quốc gia .Các thông tin về an ninh quốc gia , bí mật kinh doanh hay các thông tin tài chính là mục tiêu của các tổ

chức tình báo nước ngoài về chính trị hay công nghiệp hoặc kẻ cắp nói chung. Bọn chúng có thể làm mọi việc có thể có được những thông tin quý giá . Thử tưởng tượng nếu có kẻ xâm nhập đc vào hệ thống chuyển tiền của các ngân hàng dó sẽ chịu những thiệt hại to lớn có thể dẫn tới phá sản .Chưa kể nếu hệ thống

Không chỉ số lượng các cuộc tấn công tăng lên nhanh chóng, mà các phương pháp tấn công cũng liên tục được hoàn thiện. Điều đó một phần do các nhân viên quản trị hệ thống được kết nối với Internet ngày càng đề cao cảnh giác. Cũng theo CERT, những cuộc tấn công thời kỳ 1988-1989 chủ yếu đoán tên người sử dụng-mật khẩu (UserID-password) hoặc sử dụng một số lỗi của các chương trình và hệ điều hành (security hole) làm vô hiệu hệ thống bảo vệ, tuy nhiên các cuộc tấn công vào thời gian gần đây bao gồm cả các thao tác như giả mạo địa chỉ IP, theo dõi thông tin truyền qua mạng, chiếm các phiên làm việc từ xa (telnet hoặc rlogin).

Để vừa bảo đảm tính bảo mật của thông tin lại không làm giảm sự phát triển của việc trao đổi thông tin quảng bá trên toàn cầu thì một giải pháp tốt nhất là mã hoá thông tin. Có thể hiểu sơ lược mã hoá thông tin là che đi thông tin của mình làm cho kẻ tấn công nếu chặn được thông báo trên đường truyền thì cũng không thể đọc được và phải có một giao thức giữa người gửi và người nhận để có thể trao đổi thông tin, đó là các cơ chế mã và giải mã thông tin.

Ngày nay thì việc mã hoá đã trở nên phổ cập. Các công ty phần mềm lớn trên thế giới đều có nghiên cứu và xây dựng các công cụ, thuật toán mã hoá để áp dụng cho thực tế. Mỗi quốc gia hay tổ chức đều có những cơ chế mã hoá riêng để bảo vệ hệ thống thông tin của mình.

Một người quản trị hệ thống không hiểu về khía cạnh an toàn và yêu cầu của hệ thống và vô tình cho phép người dùng khác truy nhập vào thư mục chứa các thông tin hệ thống. Người dùng phát hiện ra họ có thể có được các thông tin hệ thống và

có thể dùng nó phục vụ cho lợi ích của mình. Thật tai hại nếu các vấn đề trên xảy ra, nó có thể ảnh hưởng không chỉ lợi ích cá nhân mà còn ảnh hưởng tới lợi ích của tập đoàn, có khi là quốc gia.

Vậy nên vấn đề bảo mật thông tin ngày càng trở lên cần thiết và được sử dụng rất nhiều trong các công ty, tập đoàn, ban bộ…Vì đó các hệ mã hóa mang lại lợi ích rất lớn và đóng vai trò không thể thiếu trong đời sống công nghệ thông tin. Trong bài này, tôi xin giới thiệu với các bạn một số hệ mã hóa như: Caesar, mã thay thế, mã dịch vòng…và đặc biệt hệ về hệ mã hóa Vigenere nổi tiếng. Hệ mã hóa này được phát minh vào thế kỷ thứ 16 và được viết đầu tiên bởi nhà ngoại giao Pháp Blaise de Vigenère và là một kiểu của mã hóa thay thế được xem xét là chưa từng bị phá vỡ trong suốt 4 thế kỷ và nó được sử dụng phổ biến rộng rãi cho việc mã hóa những dữ liệu được truyền qua hệ thống điện tín trong suốt thế kỷ 19.

Chương I : NGÀNH KHOA HỌC MẬT MÃ

1.1.Lịch sử ra đời của ngành khoa học mật mã

Mật mã học là một lĩnh vực liên quan đến các kỹ thuật ngôn ngữ và toán học để đảm bảo an toàn thông tin, cụ thể là trong thông tin liên lạc.

Mật mã học có lịch sử lâu dài và đầy màu sắc. Nói chung, những dạng sớm nhất của cách viết bí mật (ngày nay gọi chung là mật mã hóa cổ điển) chỉ cần có bút và giấy. Hai phạm trù chính của mật mã cổ điển là mật mã hoán vị, trong đó người ta sắp xếp lại trật tự các chữ cái của thông điệp, và mật mã thay thế, trong đó người ta thay thế có hệ thống các chữ cái hay các nhóm chữ cái bằng các chữ cái hay các nhóm chữ cái khác. Văn bản được mật mã hóa bằng mật mã cổ điển có xu hướng lộ ra các thông tin thống kê nhất định về văn bản thường. Bằng cách sử dụng các thông tin này, mật mã cổ điển rất dễ bị dò ra (ví dụ bằng phân tích tần suất). Mật mã cổ điển vẫn còn được phổ biến tới ngày nay, chủ yếu thông qua việc giải các ô đố chữ (xem tài liệu viết bằng mật mã).

Các thiết bị và các kỹ thuật khác nhau đã được sử dụng để mật mã hóa. Một trong những thiết bị sớm nhất có lẽ là gậy mật mã (tiếng Hy Lạp: σκυτάλη). Trong nửa đầu thế kỷ XX, một số thiết bị cơ khí đã được phát minh để thực hiện mật mã hóa, bao gồm rotor machines — nổi tiếng nhất là máy Enigma được người Đức sử dụng trong Đại chiến thế giới 2. Mật mã thực hiện bằng các máy móc này đã tăng độ phức tạp lên đáng kể đối với công việc phân tích mã.

Với sự ra đời của máy tính kỹ thuật số và điện tử học thì các mật mã cực kỳ phức tạp đã có thể được thực hiện. Đặc trưng của mật mã máy tính là chúng thực hiện trên các chuỗi nhị phân, không giống như trong các mô hình mật mã hóa cổ điển và cơ học (chỉ sử dụng bảng chữ cái với khoảng 26 ký tự-phụ thuộc vào từng

ngôn ngữ). Mật mã máy tính cũng có khả năng chịu đựng việc phân tích mật mã tốt hơn; rất ít các mật mã như thế dễ bị tổn thương chỉ bởi kiểu tấn công biết bản mã.

Các nghiên cứu rộng rãi có tính học thuật về mật mã hóa hiện đại là tương đối gần đây — nó chỉ được bắt đầu trong cộng đồng mở kể từ những năm thập niên 1970 với các chi tiết kỹ thuật của DES (viết tắt trong tiếng Anh của Data Encryption Standard tức Tiêu chuẩn Mật mã hóa Dữ liệu) và sự phát minh ra RSA. Kể từ đó, mật mã hóa đã trở thành công cụ được sử dụng rộng rãi trong liên lạc và bảo mật máy tính.

Cũng giống như các bài học thu được từ trong lịch sử của nó, các nhà mật mã hóa cũng rất thận trọng khi nhắc đến tương lai. Định luật Moore thông thường được nhắc đến khi nói về độ lớn khóa, và các hiệu ứng tiềm năng của máy tính lượng tử cũng đã được nói.

1.2.Tổng quan và các khái niệm về khoa học mật mã

Khoa học mật mã (cryptology) gồm:

- Mật mã học (cryptography): là khoa học nghiên cứu cách ghi bí mật thông tin nhằm biến đổi bản rõ thành bản mã.
- Phân tích mật mã (cryptanalysis): nghiên cứu cách phá các hệ mật nhằm phục hồi bản rõ ban đầu từ bản mã, nghiên cứu các nguyên lí và phương pháp giải mã mà không biết khóa.
  - Có 3 phương pháp tấn công cơ bản của thám mã:
    - •Tìm khóa vét cạn
    - •Phân tích thống kê
    - •Phân tích toán học

Mật mã là một ngành khoa học chuyên nghiên cứu các phương pháp truyền tin bí mật. Mật mã bao gồm : Lập mã và phá mã. Lập mã bao gồm hai quá trình: mã hóa và giải mã.

Để bảo vệ thông tin trên đường truyền người ta thường biến đổi nó từ dạng nhận thức được sang dạng không nhận thức được trước khi truyền đi trên mạng, quá trình này được gọi là mã hoá thông tin (encryption), ở trạm nhận phải thực hiện quá trình ngược lại, tức là biến đổi thông tin từ dạng không nhận thức được (dữ liệu đã được mã hoá) về dạng nhận thức được (dạng gốc), quá trình này được gọi là giải mã. Đây là một lớp bảo vệ thông tin rất quan trọng và được sử dụng rộng rãi trong môi trường mạng.Để bảo vệ thông tin bằng mật mã người ta thường tiếp cận theo hai hướng:

- Theo đường truyền (Link_Oriented_Security).
- Từ nút đến nút (End_to_End).

Theo cách thứ nhất thông tin được mã hoá để bảo vệ trên đường truyền giữa hai nút mà không quan tâm đến nguồn và đích của thông tin đó. Ởđây ta lưu ý rằng thông tin chỉđược bảo vệ trên đường truyền, tức là ở mỗi nút đều có quá trình giải mã sau đó mã hoá để truyền đi tiếp, do đó các nút cần phải được bảo vệ tốt.

Ngược lại theo cách thứ hai thông tin trên mạng được bảo vệ trên toàn đường truyền từ nguồn đến đích. Thông tin sẽđược mã hoá ngay sau khi mới tạo ra và chỉđược giải mã khi vềđến đích. Cách này mắc phải nhược điểm là chỉ có dữ liệu của người ung thì mới có thể mã hóa được còn dữ liệu điều khiển thì giữ nguyên để có thể xử lý tại các nút.

1.2.1 . Các khái niệm cơ bản liên quan tới khoa học mật mã

Mật mã học (Cryptography) là ngành khoa học nghiên cứu về việc đảm bảo an toàn thông tin.Đây là một ngành quan trọng và có nhiều ứng dụng trong đời sống

xã hội. Ngày nay , các ứng dụngmax hóa và bảo mật thông tin đang được sử dụng ngày càng phổ biến hơn trong các lĩnh vực khác nhau trên thế giới , từ các lĩnh vữ an ninh-quốc phòng cho tới các lĩnh vực dân sự như thương mại điện tử , ngân hàng ,...

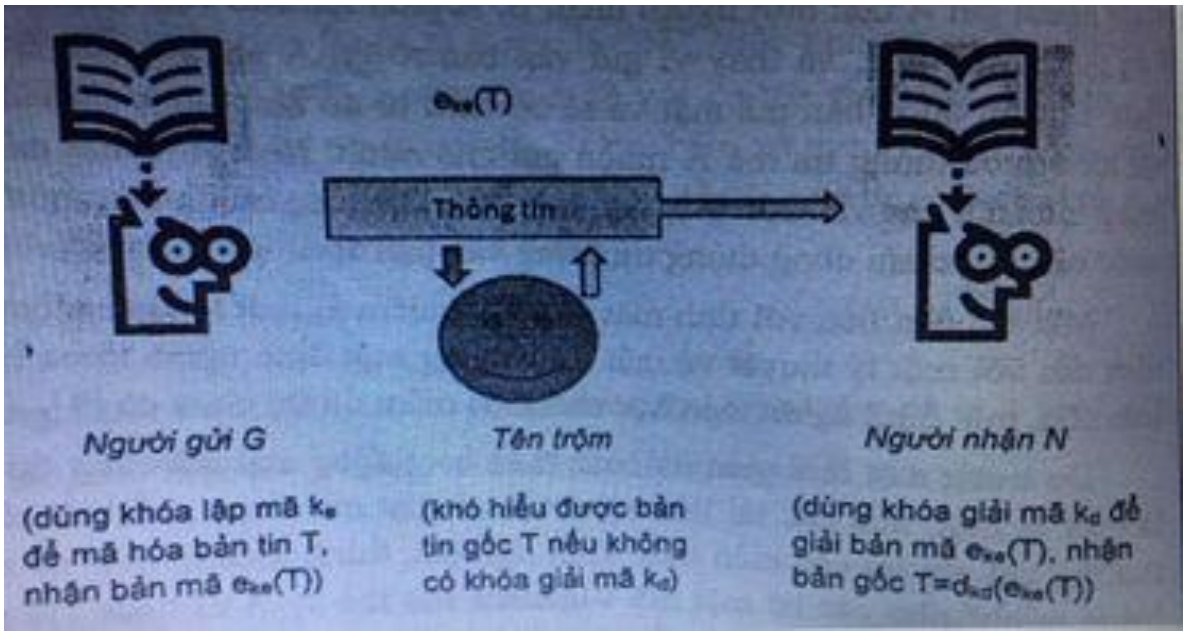
Thám mã (cryptanalysis): nghiên cứu cách phá các hệ mật nhằm phục hồi bản rõ ban đầu từ bản mã, nghiên cứu các nguyên lí và phương pháp giải mã mà không biết khóa. Có 3 phương pháp tấn công cơ bản của thám mã:

- Tìm khóa vét cạn
- Phân tích thống kê
- Phân tích toán

1.2.1.1.Mã hóa và giải mã

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 gải mã được đặc trưng bởi hình sau :



Quá trình truyền tin mật

1.2.1.2.Khóa mã hóa

Khóa là một đoạn thông tin điều khiển hoạt động của thuật toán mật mã hóa. Nói một cách khác, khóa là thông tin để cá biệt hóa quá trình mã hóa cũng như giải mã. Khóa cũng được sử dụng trong các thuật toán khác trong mật mã học như thuật toán tạo chữ ký số hay hàm băm mật mã.

Với một thuật toán được thiết kế tốt, mã hóa cùng một văn bản với các khóa khác nhau sẽ cho ra các bảng mã hoàn toàn khác nhau. Tương tự, khi giải mã với khóa sai thì kết quả sẽ cho ra một bản rõ hoàn toàn ngẫu nhiên. Trong trường hợp khóa bị thất lạc thì không thể phục hồi lại bản rõ ban đầu với điều kiện là thuật toán đảm bảo chất lượng và độ dài khóa đủ lớn.

1.2.1.3.Che giấu thông tin

Để đảm bảo an toàn thông tin lưu trữ trong máy tính hay bảo đảm An toàn thông tin trên đường truyền tin , người ta phải che giấu các thông tin này .

Che giấu thông tin là thay đổi hình dạng gốc làm cho người đọc khó nhận biết được thông tin gốc

Giấu thông tin là cất giấu thông tin trong ản tin khác làm cho người đọc khó nhận ra có thông tin đã giấu .

1.2.1.4.Thuật toán lập mật mã và giải mật mã

Để lập mật mã hay thực hiện được phép mã hóa , ta còn cần có một thuật toán biến bản rõ , cùng vs khóa mật mã , thành bản mã mật , và một thuật toán ngược , biến bản mã mật , cùng khóa mật mã , thành bản rõ . Các thuật toán đó được gọi tương ứng là thuật toán lập mật mã / mã hóa và các thuật toán giả mã mật mã / giải mã . Các thuật toán này thường không nhất thiết phải giữ bí mật , mà cái cần được giữ tuyệt mật luôn luôn là khóa mật mã .

1.2.1.5.Mã hóa và phá khóa

Trong thục tiễn , đã hoạt đọng bảo mật thì cũng có hoạt động ngược lại là khám phá bí mật từ các bản mã mật "lấy trộm" được, ta thương gọi hoạt động này là mã thám , hoạt động này quan trọng không kém gì hoạt động bảo mật .vì các thuật toán lập mật mã và giải mật mã không nhất thiết là bí mật , nên mã thám thường được tập trung vào việc tìm khóa mật mã , do đó cũng có người gọi công việc là phá khóa .

Bài toán mã hóa cơ bản là bài toán tìm khóa mật mã K (hay khóa giải mã Kd) để giải bài toán đó , giả thiết người thám mã biết thông tin về sơ đồ hệ mật mã được dùng , kể cả các phép lập mã và giải mã tổng quát E và D . Ngoài ra , thám mã có thể biết thêm một sô thông tin khác , tùy theo những thông tin được biết thêm này mà có thể phân loại bài toán thám mã thành các bài toán cụ thể :

- Bài toán thám mã chỉ biết bản mã : là bàu toán phổ biến nhất , khi người thám mã chỉ biết một bản mật mã Y .
- Bài toán thám mã khi chỉ biết bản rõ : người thám mã biets một bản mật mã Y cùng với bản rõ tưng ứng với X;
- Bài toán thám mã khi có bản rõ được chọn : người thám mã có thển chọn một bản rõ X ,và biết bản mật mã tuonge ứng Y . điều này có thể xảy ra khi người thám mã chiếm được tạm thời máy lập mã
- Bài toán thám mã khi có bản mã được chọn : người thám mã có thể chọn một bản mật mã Y , và biết bản rõ tương ứng X. điều này có thể xảy ra khi một người thám mã tham chiếm được tạm thời máy giải mã .

1.2.1.6.Các khái niệm liên quan khác

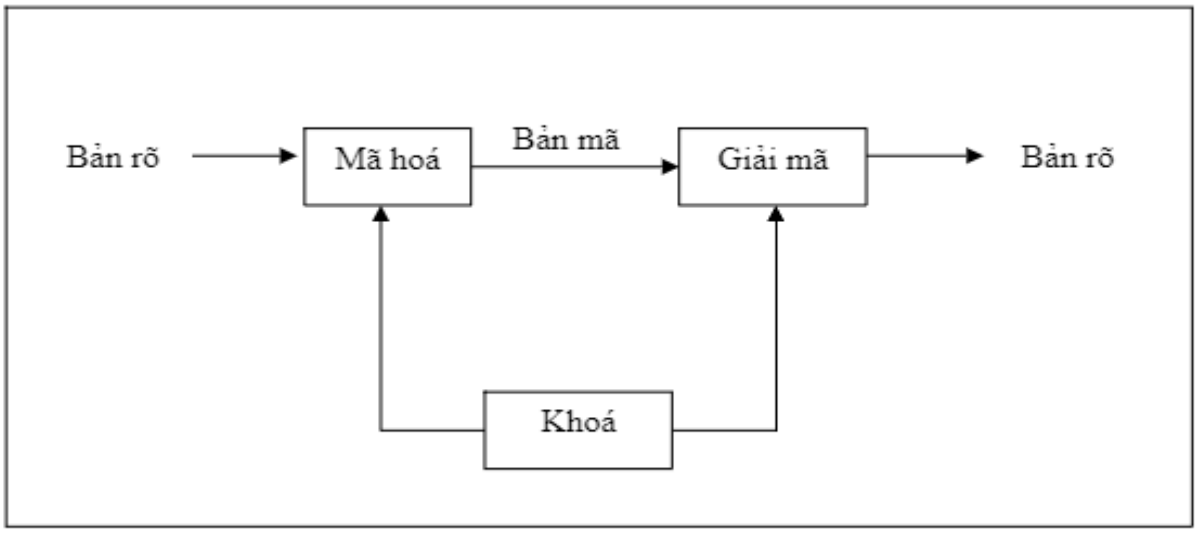
- Bản rõ (Plaintext): Dạng ban đầu của thông báo
- Bản mã (Ciphertext): Dạng mã của bản rõ ban đầu
- Khóa (Key): thông tin tham số dùng để mã hóa Mã hóa
- (Encryption): Quá trình biến đổi thông tin từ dạng bản rõ sang bản mã bằng khóa hoặc không cần khóa
- Giải mã (Decryption): Quá trình ngược lại biến đổi thông tin từ dạng bản mã sang bản rõ

1.3.Các thành phần của một 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 "kẻđịch: 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 e_K: P → C và một quy tắc giải mã tương ứng d_K∈ D. Mỗi e_K: P → C và d_K: C → P là những hàm mà: d_K (e_K(x))=x với mọi bản rõ x ∈ P.



Mã hoá với khoá mã và khoá giải giống nhau

1.4. Phân loại hệ mật mã

Có nhiều cách để phân loại hệ mật mã. Dựa vào cách truyền khóa có thểphân các hệ mật mã thành hai loại:

- Hệ mật đối xứng (hay còn gọi là mật mã khóa bí mật): là những hệ mật dung chung một khoá cả trong quá trình mã hoá dữ liệu và giải mã dữ liệu. Do đó khoá phải được giữ bí mật tuyệt đối.
- Hệ mật mã bất đối xứng (hay còn gọi là mật mã khóa công khai) : Hay còn gọi là hệ mật mã công khai, các hệ mật này dùng một khoá để mã hoá sau đó dùng một khoá khác để giải mã, nghĩa là khoá để mã hoá và giải mã là khác nhau. Các khoá này tạo nên từng cặp chuyển đổi ngược nhau và không có khoá nào có thể suy được từ khoá kia. Khoá dùng để mã hoá có thể công khai nhưng khoá dùng để giải mã phải giữ bí mật.

Ngoài ra nếu dựa vào thời gian đưa ra hệ mật mã ta còn có thể phân làm hai loại: Mật mã cổđiển (là hệ mật mã ra đời trước năm 1970) và mật mã hiện đại (ra đời sau năm 1970). Còn nếu dựa vào cách thức tiến hành mã thì hệ mật mã còn được chia làm hai loại là mã dòng (tiến hành mã từng khối dữ liệu, mỗi khối lại dựa vào các khóa khác nhau, các khóa này được sinh ra từ hàm sinh khóa, được gọi là dòng khóa) và mã khối (tiến hành mã từng khối dữ liệu với khóa như nhau)

1.5.Các tính chất cơ bản của quá trình bảo mật và mã hóa

Hệ mật mã giúp đảm bảo các tính chất sau của thông tin :

- Tính bí mật (confidentiality/privacy): tính chất này đảm bảo thông tin chỉ được hiểu bởi những ai biết chìa khóa bí mật.
- Tính toàn vẹn (integrity): tính chất này đảm bảo thông tin không đổi mà không bị phát hiện. Tính chất này không đảm bảo thông tin không đổi, nhưng một khi nó bị nghe lén hoặc thay đổi thì người nhận được thông tin có thể biết được là thông tin đã bị nghe lén hoặc thay đổi. Các hàm một chiều(one- way function) như MD5, SHA-1, MAC...được dùng để đảm bảo tính toàn vẹn cho thông tin.

- Tính xác thực (authentication): người gửi (hoặc người nhận) có minh đúng họ. Người ta có thể dụng một password, một challenge dự thuật toán mã hóa hoặc một bí mật chia sẻ giữa hai người để xác thực. Sự xác thực này có thể thực hiện một chiều (one-way) hoặc hai chiều (multual authen
- Tính không chối bỏ (non-repudiation): người gửi hoặc nhận sau này không thể chối bỏ việc đã gửi hoặc nhận thông tin. Thông thường điều thực hiện thông qua một chữ ký điện tử (electronic signature).
- Tính nhận dạng (identification): người dùng của một hệ thống, một tài nguyên sở hữu một chứng minh thư (identity) như là một chìa khó (primary key). identity này sẽ xác định những chức năng của người dùn cho phép của người dùng cũng như các thuộc tính liên quan.

1.6. 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:

a, Độ an toàn: Một hệ mật được đưa vào sử dụng điều đầu tiên phải có độan toàn cao. Ưu điểm của mật mã là có thểđánh 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

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. b, Tốc độ mã và giải mã: 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.

c, 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 sẽcao hơn so với các hệ mật có khóa công khai. Vì vậy đây cũng là một tiêu chí khi lựa chọn hệ mật mã.

Chương II : HỆ MẬT MÃ VIGENERE

2.1.HỆ MÃ HÓA ĐỐI XỨNG

Mã hóa cổ điển là phương pháp mã hóa đơn giản nhất xuất hiện đầu tiên trong lịch sử ngành mã hóa. Thuật toán đơn giản và dễ hiểu. Những phương pháp mã hóa này là cơ sở cho việc nghiên cứu và phát triển thuật toán mã hóa đối xứng được sử dụng ngày nay.

Mọi thuật toán cổ điển đều là mã khóa đối xứng, vì ở đó thông tin về khóa được chia sẻ giữa người gửi và người nhận. Mã đối xứng là kiểu duy nhất trước khi phát minh ra khóa công khai (hệ mã không đối xứng) vào những năm 1970.

Mật mã đối xứng sử dụng cùng một khóa cho việc mã hóa và giải mã. Có thể nói Mã đối xứng là mã một khóa hay mã khóa riêng hay mã thỏa thuận.

Hiện nay các Mã đối xứng và công khai tiếp tục phát triển và hoàn thiện. Mã công khai ra đời hỗ trợ mã đối xứng chứ không thay thế nó, do đó mã đối xứng đến nay vẫn được sử dụng rộng rãi.

Có ba phương pháp chính trong mật mã khoá bí mật (mật mã khoá riêng hay mật mã cổ điển):

- Hoán vị
- Thay thế
- Xử lý bit (chủ yếu nằm trong các ngôn ngữ lập trình)
- Ngoài ra còn có phương pháp hỗn hợp thực hiện kết hợp các phương pháp trên mà điển hình là chuẩn mã dữ liệu (DES –Data Encryption Standard) của Mỹ.

Hệ mật mã khóa đối xứng được sử dụng rất sớm nên được gọi là hệ mật mã khóa đối xứng _cổ điển . Bản mã hay bản rõ đều là dãy chữ số la-tinh . Việc lập mã và giải mã được thực hiện theo nguyên tắc :

- Lập mã : thực hiện theo các bước sau

Bước 1 : nhập bản rõ kí tự : RÕ_CHỮ

Bước 2 : chuyển bản RÕ_CHỮ thành RÕ_SỐ

Bước 3 : chuyển RÕ_SỐ thành MÃ_SỐ

Bước 4 : chuyển MÃ_SỐ thành MÃ_CHỮ

- Giải mã : thực hiện theo các bước sau

Bước 1 : nhập bản rõ kí tự : MÃ_CHỮ

Bước 2 : chuyển bản MÃ_CHỮ thành MÃ_SỐ

Bước 3 : chuyển MÃ_SỐ thành RÕ_SỐ

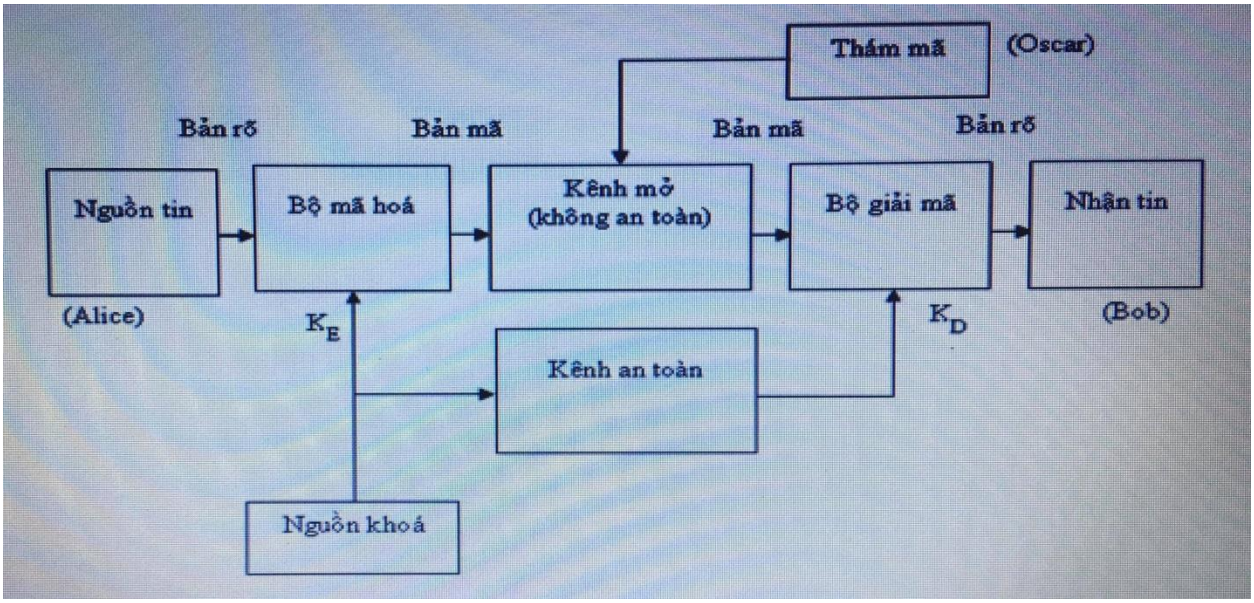
Bước 4 : chuyển RÕ_SỐ thành RÕ_CHỮ

Để chuyển từ CHỮ sang SỐ hay ngược lại từ số trở về chữ , người ta theo một quy ước nào đó , ví dụ chữ cái thay bằng số theo modulo 26. Các tập kí tự bản rõ và bản mã thường dùng là các tập kí tự của ngôn ngữ thông thường như tiếng việt , tiếng anh

Ta có bản chữ cái thay bằng số theo modulo 26 :

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M
13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Sơ đồ khối của hệ truyền tin mật :



2.2.HỆ MẬT MÃ VIGENERE

2.2.1.Nguồn gốc ra đời

Mật mã Vigernere là một phương pháp mã hóa chữ văn bản tiếng Anh, lần đầu tiên được mô tả bởi Giovan Battista Bellaso vào năm 1553. Phương pháp mã hóa mật mã Vigenère dễ hiểu và dễ thực hiện, nhưng chỉ đến năm 1863 với nhiều nỗ lực suốt ba thế kỷ, Friedrich Kasiski mới xuất bản một phương pháp chung để giải mã mật mã Vigernere.

2.2.2.Khái niệm

Mật mã là một ngành khoa học biến đổi các thông điệp trở nên vô nghĩa đối với những người không có quyền được biết nội dung của thông điệp. Có nhiều thuật toán đã đc phát minh từ xa xưa.

Thuật toán Vigenere là 1 trong những thuật toán mật mã cổ điển, thuật toán thực hiện trên nguyên lý dịch chuyển vị trí của kí tự trong bảng Alphabet. Số vị trí dịch chuyển phụ thuộc vào khoá đc dùng để mật mã

Mật mã Vigernere là tập hợp các quy tắc thay thế chữ cái đơn trong bảng chữ cái tiếng Anh qua việc sử dụng 26 mật mã Caesar với các bước dịch chuyển từ 0 đến 25 tương ứng từ chữ ‘a’ đến chữ ‘z’.

Mã Vigernere là hệ mật trong đó P=C=K=(Z26)^m và m là độ dài khóa , với c,p ϵ (Z26)m , ta định nghĩa :

$$c_k(p)=c_k(c_1,c_2,....,c_m)=(p_1+k_1,p_2+k_2,...,p_m+k_m)$$

$$p_k(\ p)=d_k(p_1,p_2,.....,p_m)=(c_1-k_1,c_2-k_2,....,c_m-k_m)$$

Trong đó : tất cả các phép toán thực hiện trong z26

p là bản mã

c là bản rõ

k là khóa với mỗi k=(k1,k2,..km)ϵK

Ý tưởng : Chia chuỗi cần mã hóa thành các đoạn có độ dài m và mã hóa theo đoạn. Mã thế đa bảng đơn gian nhất là mã Vigenere.

Thực chất quá trình mã hóa Vigenere là việc tiến hành đồng thời dùng nhiều mã Ceaser cùng một lúc trên bản rõ với nhiều khóa khác nhau . Khóa cho mỗi chữ cái dùng để mã phụ thuộc vào vị trí của chữ đó trong bản rõ và được lấy trong từ khóa theo thứ tự tương ứng.

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M
13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Bảng chữ cái theo số với moldun 26

2.3.Mã hóa

Giả sử khóa là một chuỗi chữ cái có độ dài m được viết dưới dạng K= k_1 ,k_2 , k_3 ,.k_m .Trong đó k_i nhận giá trị nguyên từ 0 đến 25.

Ta chia bản rõ thành các chuỗi có độ dài m .Mỗi chữ thứ i trong chuỗi chỉ định dùng bảng chữ thứ i với tịnh tiến k_i giống như trong Caeser.

Hiểu theo cách khác , ta lấy giá trị số tương ứng của các kí tự trong bản rõ **cộng** với các kí tự số đã được chia theo độ dài m củ khóa k sẽ thu đc các kí tự số của bản mã tương ứng . Cuối cùng đem kí tự số của bản mã ra đối chiếu với "*bảng chữ cái theo số với moldun 26* "để nhận được bản mã chữ tương ứng).

Công thức mã hóa :

$$Ci = (Pi + Ki) \bmod 26 \text{ , với } i = 1,\ldots\ldots m$$

2.4 .Giải mã

Trên thực tế khi mã ta có thể sử dụng lần lượt các bảng chữ cái lăp lại từ đầu sau m chữ của bản rõ . Vì thế nhiều bảng chữ khác nhau , nên cùng một chữ ở vị trí khác nhau sẽ có các bước nhảy khác nhau , làm cho tần suất các chữ trong bản mã dãn tương đối đều.

Giải mã đơn giản là quá trình làm ngược lại của mã hóa . Nghĩa là dùng bản mã và khóa với bảng chữ tương ứng , nhưng với mỗi chữ sư dụng bước nhảy lùi về lại đầu.

Hiểu theo cách khác , ta lấy giá trị số tương ứng của các kí tự trong bản mã **trừ** với các kí tự số đã được chia theo độ dài m của khóa k sẽ thu đc các kí tự số của bản rõ tương ứng . Cuối cùng đem kí tự số của bản rõ ra đối chiếu với "*bảng chữ cái theo số với moldun 26* "để nhận được bản mã chữ tương ứng).

Công thức giải mã :

$$Pi = (Ci – Ki) \bmod 26 \text{ , với } i = 1,.....m$$

2.5 .Ví dụ

Mã hóa và giải mã bản rõ ‘’WELCOMETOVIETNAM‘’ dùng mã Vegernere với khóa là k = HANOI.

Giải :

Ta có bản rõ : "WELCOMETOVIETNAM"

P_i	W	E	L	C	O	M	E	T	O	V	I	E	T	N	A	M
	22	4	11	2	14	12	4	19	14	21	8	4	19	13	0	12

Áp dụng công thức : **$Ci = (Pi + Ki) \bmod 26$, với i = 1,.....m**

Sau đó chia chuỗi thành các đoạn có độ dài m=5 và CỘNG mỗi đoạn với dãy (7 ,0 ,13 ,14 ,8) , ta có kết quả cho bởi bảng:

P_i	W	E	L	C	O	M	E	T	O	V	I	E	T	N	A	M
	22	4	11	2	14	12	4	19	14	21	8	4	19	13	0	12
K_i	H	A	N	O	I	H	A	N	O	I	H	A	N	O	I	H
	7	0	13	14	8	7	0	13	14	8	7	0	13	14	8	7
	3	4	24	16	22	19	4	6	2	3	15	4	6	1	8	19
C_i	D	E	Y	Q	W	T	E	G	C	D	P	E	G	B	I	T

Bản mã thu được là : “DEYQWTEGCDPEGBIT”

Bản mã : “DEYQWTEGCDPEGBIT” với C_i tương ứng là :

C_i	D	E	Y	Q	W	T	E	G	C	D	P	E	G	B	I	T
	3	4	24	16	22	19	4	6	2	3	15	4	6	1	8	19

Áp dụng công thức : **$Pi = (Ci – Ki) \bmod 26$, với i = 1,…..m**

Sau đó chia chuỗi thành các đoạn có độ dài m=5 và TRỪ mỗi đoạn với dãy (7 ,0 ,13 ,14 ,8) , ta có kết quả cho bởi bảng:

C_i	D	E	Y	Q	W	T	E	G	C	D	P	E	G	B	I	T
	3	4	24	16	22	19	4	6	2	3	15	4	6	1	8	19
K_i	H	A	N	O	I	H	A	N	O	I	H	A	N	O	I	H
	7	0	13	14	8	7	0	13	14	8	7	0	13	14	8	7
	22	4	11	2	14	12	4	19	14	21	8	4	19	13	0	12
P_i	W	E	L	C	O	M	E	T	O	V	I	E	T	N	A	M

Bản mã thu được là : “WELCOMTOVIETNAM ”

Chương III: CÁC ĐẶC TRƯNG CỦA HỆ MẬT VIGENERE

3.1. Đặc tính của hệ mật Vigenere

Trong phương pháp mã hóa bằng thay thế cũng như các trường hợp đặc biệt của phương pháp này (mã hóa bằng dịch chuyển, mã hóa Affine,…), ứng với một khóa k được chọn, mỗi phần tử x € P được ánh xạ vào duy nhất một phần tử y € C. Nói cách khác, ứng với mỗi khóa k € K, một song ánh được thiết lập từ P vào C.

Khác với hướng tiếp cận này, phương pháp Vigenere sử dụng một từ khóa có độ dài m. Có thể xem như phương pháp mã hóa Vigenere Cipher bao gồm m phép mã hóa bằng dịch chuyển được áp dụng luân phiên nhau theo chu kỳ.

Không gian khóa K của phương pháp Vigenere Cipher có số phần tử là n m , lớn hơn hẳn phương pháp số lượng phần tử của không gian khóa K trong phương pháp mã hóa bằng dịch chuyển. Do đó, việc tìm ra mã khóa không để giải mã thông điệp đã được mã hóa sẽ khó khăn hơn đối với phương pháp mã hóa bằng dịch chuyển.

3.2.Độ an toàn của hệ mật Vigenere

Độ an toàn tương đối cao

Như vậy có chữ mã khác nhau cho cùng một chữ của bản rõ .Suy ra tần xuất của các chữ bị phẳng , nghĩa là tần suất xuất hiện các chữ trên bản mã tương đối đều nhau.Tuy nhiên chưa mất hoàn toàn , do độ dài khóa có hạn nên có thể tạo nên chu kì vòng lặp.

Kẻ thám mã bắt đầu từ tần suất của chữ để xem có phải đây là mã đơn biểu hay không . Nếu khóa gồm m ký tự khác nhau , mỗi kí tự được ánh xạ vào trong m ký tự có thể, do đó hệ mã này được gọi là hệ thay thế đa biểu . Như vậy , số khóa (độ dài m) có thể có trong hệ mã vigenere là 26m . Nếu dùng phương pháp“ tấn công vét cạn ”, thám mã phải kiểm tra 26m=308915776 ; duyệt toàn bộ chừng ấy khóa để thám mã bằng cách tính thủ công thì khó , nhưng nếu dùng máy tính đủ mạnh thì cũng không đến nỗi khó lắm

3.3.Ưu điểm và nhược điểm

3.3.1.Ưu điểm

- Tốc độ cao và dễ thực hiện.
- Để đảm bảo độ bền của mật mã sử dụng độ dài khóa nhỏ

3.3.2.Nhược điểm

- Do dùng chung khóa để mã hóa và giải mã => nếu bị mất hoặc bị đánh cắp bởi hacker sẽ bị lộ thông tin, bảo mật không cao.
- Cần kênh mật để chia sẻ khóa bí mật giữa các bên => Làm sao để chia sẻ một cách an toàn ở lần đầu tiên.
- Để đảm bảo liên lạc an toàn cho tất cả mọi người trong một nhóm gồm n người => cần tổng số lượng lớn khóa là n(n-1)/2
- Khó ứng dụng trong các hệ thống mở.
- Không có khả năng sử dụng cho chữ ký số, chứng chỉ.
- Không thể dùng cho mục đích xác thực hay mục đích chống thoái thác được.
- Và để khắc phục những nhược điểm đó thì hệ mật mã khóa bất đối xứng (hay còn gọi là hệ mật mã khóa công khai) đã ra đời

Chương 4 Code Hệ mật mã Vigenere

Chương trình nguồn được viết bởi Ngôn ngữ Java

```
package KiTu26;
import java.util.Scanner;
public class Vigenere {
        public static String P="";
        public static String K="";
         public static String C="";
         public char SoSangKiTu(int n){
              char t=' ';
              if(n == 0)
                   t = 'A';
              else if(n == 1)
                   t = 'B';
              else if(n == 2)
                   t = 'C';
              else if(n == 3)
                   t = 'D';
              else if(n == 4)
                   t = 'E';
              else if(n == 5)
                   t = 'F';
              else if(n == 6)
                   t = 'G';
              else if(n == 7)
```

```
        t = 'H';
    else if(n == 8)
        t = 'I';
    else if(n == 9)
        t = 'J';
    else if(n == 10)
        t = 'K';
    else if(n == 11)
        t = 'L';
    else if(n == 12)
        t = 'M';
    else if(n == 13)
        t = 'N';
    else if(n == 14)
        t = 'O';
    else if(n == 15)
        t = 'P';
    else if(n == 16)
        t = 'Q';
    else if(n == 17)
        t = 'R';
    else if(n == 18)
        t = 'S';
    else if(n == 19)
        t = 'T';
```

```
    else if(n == 20)
        t = 'U';
    else if(n == 21)
        t = 'V';
    else if(n == 22)
        t = 'W';
    else if(n == 23)
        t = 'X';
    else if(n == 24)
        t = 'Y';
    else if(n == 25)
        t = 'Z';
    return t;
}
public int KiTuSangSo (char c){
    int t=0;
    if(c == 'A')
        t = 0;
    else if(c == 'B')
        t = 1;
    else if(c == 'C')
        t = 2;
    else if(c == 'D')
        t = 3;
    else if(c == 'E')
```

```
        t = 4;
    else if(c == 'F')
        t = 5;
    else if(c == 'G')
        t = 6;
    else if(c == 'H')
        t = 7;
    else if(c == 'I')
        t = 8;
    else if(c == 'J')
        t = 9;
    else if(c == 'K')
        t = 10;
    else if(c == 'L')
        t = 11;
    else if(c == 'M')
        t = 12;
    else if(c == 'N')
        t = 13;
    else if(c == 'O')
        t = 14;
    else if(c == 'P')
        t = 15;
    else if(c == 'Q')
        t = 16;
```

```
        else if(c == 'R')
            t = 17;
        else if(c == 'S')
            t = 18;
        else if(c == 'T')
            t = 19;
        else if(c == 'U')
            t = 20;
        else if(c == 'V')
            t = 21;
        else if(c == 'W')
            t = 22;
        else if(c == 'X')
            t = 23;
        else if(c == 'Y')
            t = 24;
        else if(c == 'Z')
            t = 25;
        return t;
    }
    public int[] Chuoi_So(String str){
        int[] t = new int[str.length()];
        for(int i = 0;i<str.length();i++){
            t[i] = KiTuSangSo(str.charAt(i));
        }
```

```
        return t;
    }
    public String So_Chuoi(int[]t){
        String str ="";
        for(int i = 0;i<t.length;i++){
            str += SoSangKiTu(t[i]);
        }
        return str;
    }
    public String MaHoa(){
        System.out.println("Chuoi can ma hoa:"+P);
        System.out.println("Khoa:"+K);
        P = P.toUpperCase();
        K = K.toUpperCase();
        int []p = Chuoi_So(P);
        //InSo(p);
        int []k = Chuoi_So(K);
        //InSo(k);
        int []kq = new int[P.length()];
        for(int i=0,j=0;i<P.length();i++){
            kq[i] = (p[i]+k[j])% 26;
            j = ++j%K.length();
        }
        //InSo(kq);
        C = So_Chuoi(kq);
```

```
    return C;
}
public String GiaiMa(){
    int []c = Chuoi_So(C);
    //InSo(c);
    int []k = Chuoi_So(K);
    //InSo(k);
    int []kq = new int[C.length()];
    for(int i=0,j=0;i<C.length();i++){
        kq[i] = (c[i]-k[j])% 26;
        if(kq[i]<0)
            kq[i] = (c[i]+(26-k[j]))% 26;
        j = ++j%K.length();

    }               //InSo(kq);
    String str = So_Chuoi(kq);
    return str;
}
public void InSo(int[]t){
    for(int i=0;i<t.length;i++)
        System.out.print(" "+t[i]);
    System.out.println();
}
public static void main(String[] args) {
    @SuppressWarnings("resource")
```

```
        Scanner sc = new Scanner(System.in);
    Vigenere t= new Vigenere();
    System.out.println("Nhap vao ban ro : "+P);
    P = sc.nextLine();
    System.out.println("Nhap vao khoa k :"+K);
     K = sc.nextLine();
    System.out.println("Chuoi ma hoa:"+t.MaHoa());
    System.out.println("Ban ma can giai ma : "+C);
            System.out.println("Chuoi giai ma:"+t.GiaiMa());
} }
```

Chương 5 Kết luận

Như vậy , các chữ mã khác nhau có thể cho cùng một chữ của bản rõ . Suy ra tần suất của các chữ cái là phẳng , nghĩa là tần suất xuất hiện các chữ trên bản mã tương đối đều nhau . Tuy nhiên chưa mất hoàn toàn , do độ dài của khóa có hạn nên có thể tạo nên chu kì vòng lặp . Kẻ thám mã bắt đầu từ tần suất của chữ để xem đây có phải là mã đơn chữ cái hay không. Giả sử đây là mã đa vần đa chữ cái,khi đó ta xác định số chữ cái trong từ khóa và lần tìm từng chữ . Như vậy cần tăng độ dài từ khóa để tăng số chữ cái dùng khi mã để "là " tần xuất của các chữ cái . Rõ ràng rằng , nếu độ dài của khóa mã mà bằng độ dài của bản mã thì hệ mã hóa này trở nên bền vững , thêm vào đó nếu khóa mã không phải là một dây các từ khóa có quy luật mà là một dãy giả ngẫu nhiên thì người ta đã chứng minh được loại mã hóa này cho đến nay được đánh giá là hệ mật mã không thể phá vở .

Vì vậy , hệ mã hóa Vigenere vẫn được sử dụng phổ biến rộng rãi cho việc mã hóa những dữ liệu được truyền qua hệ thống tin điện.