TRƯỜNG Đại Học Công Nghệ TP. HCM

Khoa Công Nghệ Thông Tin

**ĐỒ ÁN MÔN HỌC**

****

**ĐỀ TÀI:**

Xây Dựng Hệ Thống Bảo Mật:

1.Dùng phần mềm chạy hệ mã Rail Fence

2.Lựa chọn hệ mã bất kì chạy bằng tay

3.Triển khai dịch vụ bảo mật mạng IpSec(Công cụ mã hóa Rivest)

GVHD: Đặng Hồng Hiệp

SVTH: Nguyễn Minh Kha

MSSV: 1711060451

TPHCM, ngày 27 tháng 6 năm 2020

**LỜI NHẬN XÉT**

**Lời Cảm Ơn**

Chúng em chân thành cảm ơn Ban Giám Hiệu nhà trường và Khoa Công Nghệ Thông Tin và Viện Công Nghệ Việt Nhật đã tạo điều kiện để em có thể thực hiện đề tài này.

Chúng em chân thành cảm ơn thầy Đặng Hồng Hiệp đã giúp đỡ, dẫn dắt và định hướng em suốt thời gian thực hiện đồ án.

Sau quá trình thực hiện nghiên cứu đề tài, chúng em học được nhiều điều bổ ích. Chúng em hy vọng rằng, những điều chúng em được học, được biết sẽ là hành trang củng cố thêm cho chúng em không chỉ về kiến thức mà còn kinh nghiệm cho việc làm sau này.

Mục Lục

[Danh Mục Các Ký Hiệu và Chữ Viết Tắt 1](#_Toc22235)

[Chương 1.Dùng phần mềm chạy hệ mã Rail Fence 1](#_Toc29424)

[1. Hệ mã Rail Fence 1](#_Toc26422)

[2. Dùng phần mềm chạy hệ mã Rail Fence 1](#_Toc32003)

[2.1 Phương pháp mã hóa 1](#_Toc16173)

[2.1 Chạy mã 1](#_Toc7087)

[2.1.1 Thiết kế Form 1](#_Toc21527)

[2.1.2 Hàm xử lí sự kiện mã hóa 2](#_Toc23623)

[2.1.3 Hàm xử lí sự kiện giải mã 3](#_Toc7660)

[2.1.4 Kết quả thử nghiệm 3](#_Toc16142)

[Chương 2. Lựa chọn hệ mã bất kì chạy bằng tay 4](#_Toc2920)

[1. Hệ mã ViGenere 4](#_Toc12617)

[2. Phương pháp mã hóa 4](#_Toc4171)

[3. Giải mã 5](#_Toc27904)

[Chương 3.Triển khai dịch vụ bảo mật mạng IpSec(Công cụ mã hóa Rivest) 6](#_Toc26274)

[1. Ipsec là gì? 6](#_Toc5035)

[2. Cách thức hoạt động của IPsec là gì? 6](#_Toc9011)

[TÀI LIỆU THAM KHẢO 8](#_Toc17245)

[Các nguồn tài liệu tham khảo: 8](#_Toc32397)

# Danh Mục Các Ký Hiệu và Chữ Viết Tắt

Bản rõ ( Plaintext): thông báo gốc cần chuyển, được ghi bằng hình ảnh, âm thanh, chữ số, chữ viết…

Bản mật/Bản mã ( Ciphertext): “ngụy trang” bản rõ thành một dạng khác để người “ngoài cuộc” không thể đọc được

Mật mã hóa/lập mã ( Encryption): quá trình biến đổi bản rõ thành bản mật

Giải mật mã/giải mã ( Decryption): quá trình biến đổi bản mật thành bản rõ

Hệ mã (Cryptosystem): một phương pháp ngụy trang bản rõ. Nghệ thuật tạo ra và sử dụng các hệ mật mã được gọi là thuật mật mã hóa hay mật mã học (Cryptography )

Phân tích mã/thám mã (Cryptanalysis): nghệ thuật phá các hệ mật mã

# Chương 1.Dùng phần mềm chạy hệ mã Rail Fence

## Hệ mã Rail Fence

Rail Fence cipher Mã Rail Fence còn được gọi là mã zig zag là một hình thức của mã chuyển vị. Thông điệp được viết lần lượt từ trái qua phải trên các cột(rail) của một hàng dào tưởng tượng theo đường chéo từ trên xuống dưới. Theo đường chéo từ dưới lên khi đạt tới cột thấp nhất.Và khi đạt tới cột cao nhất, lại viết theo đường chéo từ trên xuống. Cứ lặp đi lặp lại như thế cho đến khi viết hết toàn bộ nội dung của thông điệp.

VD:

-Bản rõ:HUTECHTECHNOLOGY

-Key:2

-Bản mã:HTCTCNLGUEHEHOOY

## Dùng phần mềm chạy hệ mã Rail Fence

### Phương pháp mã hóa

Thông điệp được viết lần lượt từ trái qua phải trên các cột (rail) của một

hàng dào tưởng tượng theo đường chéo từ trên xuống dưới.

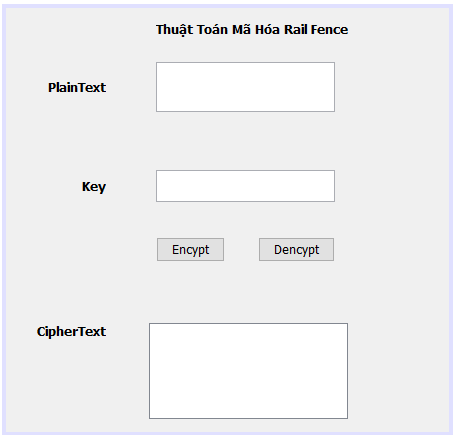
 Theo đường chéo từ dưới lên khi đạt tới cột thấp nhất.

 Và khi đạt tới cột cao nhất, lại viết theo đường chéo từ trên xuống. Cứ lặp

đi lặp lại như thế nào cho đến khi viết hết toàn bộ nội dung của thông điệp.

### Chạy mã

#### Thiết kế Form



Hình 2.2 .1 Thiết kế Form

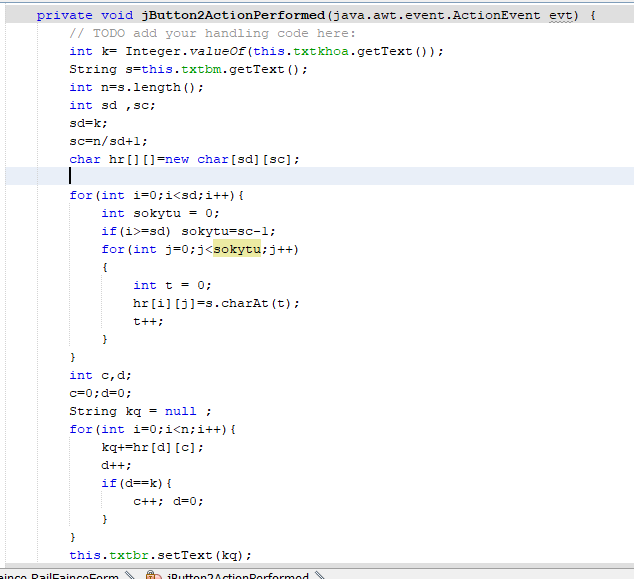
#### Hàm xử lí sự kiện mã hóa



Hình 2.2 2 Mã Hóa

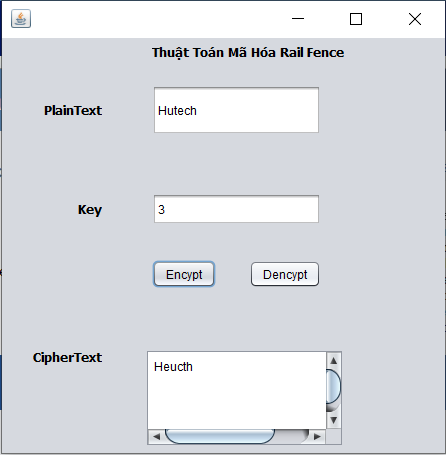
#### 

#### Hàm xử lí sự kiện giải mã



Hình 2.2 3 Giải Mã

#### Kết quả thử nghiệm



Hình 2.2 4 Kết Quả Th

# Lựa chọn hệ mã bất kì chạy bằng tay

## Hệ mã ViGenere

Mật mã Vigenere còn gọi là mật mã nhiều bảng mã. Ưu điểm của

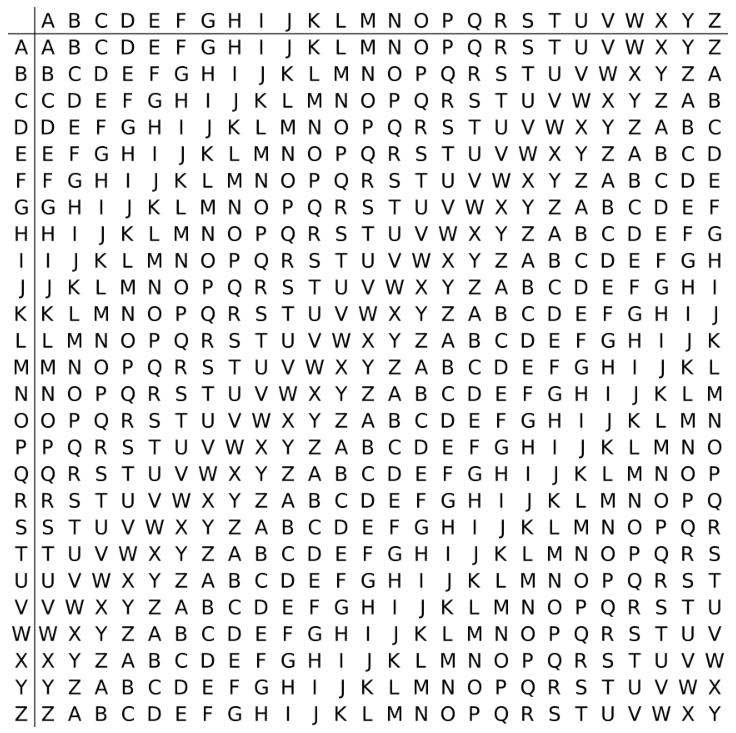
mã này là việc sử dụng 26 bảng mã khác nhau. Do đó mà không bị phá trong

một thời gian dài. Ngoài ra mã này còn hỗ trợ việc sử dụng từ khóa vô cùng

tiện lợi.

## Phương pháp mã hóa

Trong mã hóa Vigenère thì ra sẽ sử dụng một bảng để làm phép dịch, và một chuỗi khóa gọi là *key*



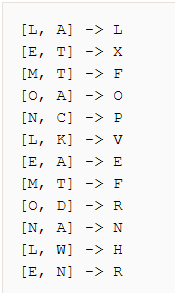
Ví dụ ta có một chuỗi cần mã hóa như sau:

Bản rõ: ATTACKATDAWN

Và key dùng để mã hóa là “LEMON”. Trước hết ta sẽ nhân chuỗi LEMON này lên để nó có cùng độ dài với chuỗi cần mã hóa:

Key: LEMONLEMONLE

Áp dụng với key LEMONLEMONLE và chuỗi ATTACKATDAWN bên trên:



ta được chuỗi LXFOPVEFRNHR.

=> Bản mã:LXFOPVEFRNHR

## 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 gía trị là ký tự trong chuỗi đã mã hóa. Ký tự trong cột đó chính là ký tự của chuỗi ban đầu.

# Chương 3.Triển khai dịch vụ bảo mật mạng IpSec(Công cụ mã hóa Rivest)

## Ipsec là gì?

Kiến trúc IP Security (viết tắt là IPsec) bao gồm một bộ các giao thức được phát triển để đảm bảo tính toàn vẹn, bảo mật và xác thực truyền dữ liệu qua mạng IP cho [máy tính](https://fptshop.com.vn/may-tinh-xach-tay" \o "máy tính" \t "https://fptshop.com.vn/tin-tuc/thu-thuat/_blank). Mặc dù tính linh hoạt của các tiêu chuẩn IPsec đã thu hút sự quan tâm của khu vực thương mại điện, tính linh hoạt này cũng dẫn đến việc xác định một số vấn đề với các giao thức vì sự phức tạp của chúng. Cũng như các hệ thống an ninh khác, việc bảo dưỡng kém có thể dễ dẫn tới sự thất bại của hệ thống bảo mật IPSec này.

IPsec có thể được sử dụng trong ba lĩnh vực bảo mật khác nhau: mạng riêng ảo (Private Virtual Network hoặc VPN), bảo mật cấp ứng dụng và bảo mật định tuyến. Vào thời điểm này, IPsec được sử dụng chủ yếu trong các ứng dụng vượt tường lửa VPN. Khi được sử dụng trong bảo mật định tuyến, IPsec không phải là giải pháp hoàn chỉnh và phải được kết hợp với các biện pháp bảo mật khác để có hiệu quả, gây cản trở việc triển khai IPSec trong các lĩnh vực này.

## Cách thức hoạt động của IPsec là gì?

IPsec có hai chế độ hoạt động, chế độ vận chuyển (transport) và chế độ phân luồng (tunnel). Khi hoạt động trong chế độ vận chuyển, các máy chủ nguồn và đích phải trực tiếp thực hiện tất cả các thao tác mã hoá. Dữ liệu được mã hóa được gửi qua một kết nối được tạo ra với công nghệ L2TP. Dữ liệu (bản mã) được tạo ra bởi máy chủ lưu trữ nguồn và được lấy từ máy chủ đích. Phương thức hoạt động này thiết lập tính an toàn từ đầu đến cuối đường truyền.

Khi IPsec hoạt động ở chế độ phân luồng, các cổng đặc biệt thực hiện quá trình xử lý mật mã ngoài các máy chủ nguồn và đích. Ở đây, nhiều ‘đường hầm” được tạo ra theo hàng loạt giữa các cổng kết nối gateway, thiết lập an ninh theo dạng gateway-to-gateway.

Khi sử dụng một trong hai chế độ này, điều quan trọng là phải cung cấp tất cả các cổng thông tin gateway khả năng xác minh rằng một gói tin là thực và để tiến hành mã hóa và giải mã tập tin ở cả hai đầu kết nối. Bất kỳ gói tin không hợp lệ phải được bỏ.

Hai loại mã hoá gói dữ liệu (DPE) được yêu cầu khi sử dụng công nghệ IPsec: Authentication Header (AH) và Encapsulating Security Payload (ESP). Các loaij mã hóa này cung cấp bảo mật cấp độ mạng cho dữ liệu được truyền đi bằng IPsec.

Chuẩn mã hóa AH cung cấp tính xác thực và toàn vẹn của gói tập tin chuyển đi. Việc xác thực được thực hiện thông qua các chức năng kỹ thuật được gọi là MAC (mã xác thực tin nhắn). Công nghệ mã hóa này này cũng cấm sửa đổi bất hợp pháp và có tùy chọn cung cấp bảo mật chống phản chiếu, hoặc thiết lập sự bảo mật giữa nhiều máy chủ, nhiều gateway, hoặc nhiều host và gateway.

Mã hóa ESP cung cấp công nghệ mã hóa, đóng gói dữ liệu và bảo mật dữ liệu. Tính bảo mật dữ liệu được cung cấp thông qua mã hóa khóa đối xứng. Tuy vào mục đích mà những kỹ sư mạng sẽ thiết kế xem hạ tầng của họ nên sử dụng loại bảo mật nào cho IPsec của họ.

# TÀI LIỆU THAM KHẢO

Các nguồn tài liệu tham khảo:

1. <https://kiendt.me/2017/11/01/vigenere-cipher/>
2. <https://thuvientvc.files.wordpress.com/2015/08/chuong1-tongquanatbmtt.pdf>
3. <https://vnnic.vn/ipv6/congnghe/giao-th%E1%BB%A9c-b%E1%BA%A3o-m%E1%BA%ADt-ipsec-trong-ipv6>
4. [http://www.nguyenduccuong.com/TaiLieu/BaoMatHTTT/BMHHTTC2%20madoixung.pdf](http://www.nguyenduccuong.com/TaiLieu/BaoMatHTTT/BMHHTTC2 madoixung.pdf)
5. <https://fptshop.com.vn/tin-tuc/thu-thuat/khai-niem-ipsec-la-gi-58963>