**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

**KHOA CÔNG NGHỆ THÔNG TIN**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**🙠**🕮**🙢**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



**BÀI TẬP LỚN**

**AN TOÀN VÀ BẢO MẬT THÔNG TIN**

***ĐỀ TÀI***

**Ứng dụng thật toán DES và lược đồ chia sẻ bí mật vào thi tuyển sinh**

**- - - - - - - - - - 🙞🕮🙜- - - - - - - - - -**

|  |  |  |
| --- | --- | --- |
| Giáo viên hướng dẫn | : | ThS. Trần Phương Nhung |

Lớp : **20221IT6001001**

**Nhóm : 01**

**Thành viên nhóm : Trần Bằng An -2019600136**

**Trần Trường Anh – 2019600823**

**Phạm Quốc Anh – 2020604668**

**Phạm Văn Đạt - 2019601321**

Hà Nội, 2022

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

**KHOA CÔNG NGHỆ THÔNG TIN**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**🙠**🕮**🙢**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



**BÀI TẬP LỚN**

**AN TOÀN VÀ BẢO MẬT THÔNG TIN**

***ĐỀ TÀI***

**Ứng dụng thật toán DES và lược đồ chia sẻ bí mật vào thi tuyển sinh**

**- - - - - - - - - - 🙞🕮🙜- - - - - - - - - -**

|  |  |  |  |
| --- | --- | --- | --- |
| Giáo viên hướng dẫn | | : | ThS. Trần Phương Nhung |
| Mã lớp | | : | **20221IT6001001** |
| Sinh viên thực hiện | | : |  |
|  | **Trần Bằng An -2019600136**  **Trần Trường Anh – 2019600823**  **Phạm Quốc Anh – 2020604668**  **Phạm Văn Đạt - 2019601321** | | |

Hà Nội, 2022

# MỤC LỤC

[MỤC LỤC 2](#_Toc60793420)

[DANH MỤC HÌNH VẼ 4](#_Toc60793421)

[DANH MỤC BẢNG BIỂU 4](#_Toc60793422)

[LỜI NÓI ĐẦU 5](#_Toc60793423)

[Chương 1: An toàn và bảo mật thông tin 7](#_Toc60793424)

[1.1. Tổng quan về an toàn và bảo mật thông tin 7](#_Toc60793425)

[1.1.1. Sự cần thiết của việc đảm bảo an toàn thông tin 7](#_Toc60793426)

[1.1.2. Khái niệm an toàn thông tin 7](#_Toc60793427)

[1.1.3. Các phương pháp bảo vệ thông tin 9](#_Toc60793428)

[1.2. An toàn thông tin bằng mật mã 10](#_Toc60793429)

[1.2.1. Mật mã và thông tin 10](#_Toc60793430)

[1.2.2. Hệ mật mã 12](#_Toc60793431)

[Chương 2: Chuẩn mã dữ liệu DES 17](#_Toc60793432)

[2.1. Hệ mã hóa khối DES 17](#_Toc60793433)

[2.1.1. Lịch sử của DES 17](#_Toc60793434)

[2.1.2. Mật mã khối 18](#_Toc60793435)

[2.2. Kỹ thuật hệ mã hóa DES 19](#_Toc60793436)

[2.3. Ưu nhược điểm 22](#_Toc60793437)

[2.3.1. Ưu điểm: 22](#_Toc60793438)

[2.3.2. Các yếu điểm của DES: 22](#_Toc60793439)

[2.4. Sơ đồ khối 26](#_Toc60793440)

[2.5. Thuật toán 28](#_Toc60793441)

[2.5.1. Quá trình mã hóa: 30](#_Toc60793442)

[2.5.2. Quá trình giải mã: 32](#_Toc60793443)

[2.5.3. Hàm F 32](#_Toc60793444)

[2.5.4. Quá trình tạo khóa con 33](#_Toc60793445)

[2.5.5. Hàm (ánh xạ) mở rộng (E) 35](#_Toc60793446)

[2.5.6. Hộp S – Box 37](#_Toc60793447)

[2.5.7. Hộp P-Box 38](#_Toc60793448)

[2.6. Lập mã DES 38](#_Toc60793449)

[2.7. Một vài kết luận về DES 42](#_Toc60793450)

[Chương 3: Bài toán chia sẻ bí mật 44](#_Toc60793451)

[3.1. Kỹ thuật Chia sẻ khóa bí mật (Secret Sharing) 44](#_Toc60793452)

[3.1.1. Khái niệm về chia sẻ bí mật 44](#_Toc60793453)

[3.1.2. Các sơ đồ chia sẻ bí mật 45](#_Toc60793454)

[3.2. Ứng dụng lược đồ chia sẻ bí mật của Lagrange để phân phối khóa 50](#_Toc60793455)

[3.3. Kết luận 51](#_Toc60793456)

[Chương 4: Áp dụng thuật toán DES và lược đồ chia sẻ bí mật vào thi tuyển sinh 53](#_Toc60793457)

[4.1. Bài toán ứng dụng 53](#_Toc60793458)

[4.2. Quy trình thực hiện giải bài toán 53](#_Toc60793459)

[4.2.1. Sơ đồ 53](#_Toc60793460)

[4.2.2. Các bước thực hiện 54](#_Toc60793461)

**Chương 5 : Kết quả nghiên cứu áp dụng thuật toán nội suy Lagrange để phân phối khóa ứng dụng lược đồ chia sẻ bí mật tuyển sinh.**

[KẾT LUẬN 59](#_Toc60793463)

# DANH MỤC HÌNH VẼ

[Ảnh 1.1: Các mức độ bảo vệ thông tin 10](#_Toc60793464)

[Ảnh 1.2: Thông tin gửi đi bị nghe lén 11](#_Toc60793465)

[Ảnh 1.3: Bảo vệ thông tin bằng mật mã 11](#_Toc60793466)

[Ảnh 1.4: Quá trình mã hóa và giải mã thông tin 12](#_Toc60793467)

[Ảnh 1.5: Sơ đồ mã hóa và giải mã bằng khóa riêng 15](#_Toc60793468)

[Ảnh 1.6: Sơ đồ mã hóa và giải mã bằng khóa công khai 15](#_Toc60793469)

[Ảnh 2.1: Sơ đồ khối chương trình DES 26](#_Toc60793470)

[Ảnh 2.2: Sơ đồ khối quá trình sinh khóa 27](#_Toc60793471)

[Ảnh 2.3: Sơ đồ mã hóa DES 29](#_Toc60793472)

[Ảnh 2.4: Sơ đồ một vòng DES 30](#_Toc60793473)

[Ảnh 2.5: Sơ đồ hàm F 33](#_Toc60793474)

[Ảnh 2.6: Sơ đồ tạo khóa con 34](#_Toc60793475)

[Ảnh 2.7: Sơ đồ của hàm mở rộng 36](#_Toc60793476)

[Ảnh 3.1: DES và quá trình phân phối khóa 51](#_Toc60793477)

[Ảnh 4.1: Sơ đồ quy trình bảo mật đề thi gửi từ nơi ra đề đến nơi tổ chức thi 54](#_Toc60793478)

[Ảnh 4.2: Chương trình mình họa 57](#_Toc60793479)

# DANH MỤC BẢNG BIỂU

[Bảng 2.1: Các khóa yếu của DES 23](#_Toc60793480)

[Bảng 2.2: Các khóa nửa yếu của DES 23](#_Toc60793481)

[Bảng 2.3: Hoán vị IP 31](#_Toc60793482)

[Bảng 2.4: . Hoán vị IP-1 31](#_Toc60793483)

[Bảng 2.5: Hoán vị PC-1 34](#_Toc60793484)

[Bảng 2.6: Bảng dịch bit tại các vòng lặp của DES 35](#_Toc60793485)

[Bảng 2.7: Hoán vị PC-2 35](#_Toc60793486)

[Bảng 2.8: Hàm mở rộng E 36](#_Toc60793487)

[Bảng 2.9: 8 hộp S-Box 38](#_Toc60793488)

[Bảng 2.10: Bảng hoán vị P 38](#_Toc60793489)

# LỜI NÓI ĐẦU

Với sự bùng nổ mạnh của công nghệ thông tin và sự phát triển của mạng Internet nên việc trao đổi thông tin trở nên dễ dàng hơn bao giờ hết. Tuy nhiên, phát sinh thêm một vấn đề ngày càng trở nên cấp bách và cần thiết về yêu cầu an toàn mạng, an ninh dữ liệu, bảo mật thông tin trong môi trường mạng cũng như trong thực tiễn.

Trên thế giới có nhiều quốc gia và nhà khoa học nghiên cứu vẫn đề bảo mật, đưa ra nhiều thuật toán giúp thông tin không bị đánh cắp hoặc nếu bị lấy cắp cũng không sử dụng được. Trong các giải pháp đó là an toàn thông tin bằng mật mã. Ở đề tài này nhóm em đề cập tới thuật toán mã hóa DES (Data Encryption Standard) từng được Liên bang Mỹ và nhiều quốc gia trên thế giới sử dụng. Tuy rằng DES hiện nay không còn được đánh giá cao về độ an toàn tuyệt đối, nhưng nó vẫn được ứng dụng trong nhiều lĩnh vực thực tiễn.

Bên cạnh mã hóa thông tin, lược đồ chia sẻ bí mật cũng được dùng để chia nhỏ thông tin trong quá trình truyền đi để đảm bảo an toàn dữ liệu. Sơ đồ chia sẻ bí mật thường được sử dụng để chia sẻ mật khẩu, khóa mã hóa trong đó có khóa mã hóa của DES.

Để ứng dụng 2 phương pháp trên vào thực tiễn, được sự hướng dẫn của cô Trần Phương Nhung, chúng em lựa chọn đề tài ***“Ứng dụng mã hóa bảo mật DES và lược đồ chia sẻ bí mật vào thi tuyển sinh”*** với mong muốn áp dụng kiến thức đã học, giải quyết bài toán bảo mật đề thi trong thi tuyển sinh.

Đề tài nhóm gồm 4 phần:

*Chương 1: An toàn vào bảo mật thông tin*. Phần này trình bày tổng quan về an toàn và bảo mật thông tin, các phương pháp mã hóa để bảo mật dữ liệu.

*Chương 2: Chuẩn dữ liệu DES*. Chương này nói về quá trình mã hóa và giải mã của hệ mật mã DES, các vấn đề xung quanh DES

*Chương 3: Sơ đồ chia sẻ bí mật*. Trong chương này trình bày về sơ đồ chia sẻ bí mật của Lagrange, phương thức chia sẻ và khôi phục khóa bí mật.

*Chương 4: Áp dụng thuật toán DES và lược đồ chia sẻ bí mật vào thi tuyển sinh.*

Đề tài được hoàn thành bằng sự cộng tác của các thành viên nhóm cùng sự hướng dẫn của cô Trần Phương Nhung. Nội dung đề tài được hoàn thành dựa trên những lý thuyết đã học về Chuẩn dữ liệu DES cùng nhiều tài liệu tham khảo khác tuy nhiên không tránh khỏi thiếu xót mong nhận thêm phản ánh và góp ý từ phía giảng viên và quý bạn đọc.

# An toàn và bảo mật thông tin

## Tổng quan về an toàn và bảo mật thông tin ( Trần Bằng An )

### Sự cần thiết của việc đảm bảo an toàn thông tin

Ngày nay sự xuất hiện của internet toàn cầu đã giúp cho việc trao đổi thông tin trở nên nhanh gọn, dễ dàng. Các phương thức chia sẻ dữ liệu qua mạng làm cho việc trao đổi, mua bán, chuyển tiền, … diễn ra mỗi ngày trên nền tảng số.

Tuy nhiên vấn đề mới lại phát sinh. Những thông tin đang nằm ở kho dữ liệu hay đang được truyền đi có thể bị trộm cắp, bị làm sai lệch, giả mạo. Điều này làm ảnh hưởng đến độ an toàn của thông tin nhạy cảm, tin mật, … có thể tác động lớn đến nhiều cá nhân, tổ chức, hay ác động đến an ninh quốc gia.

### Khái niệm an toàn thông tin

#### Khái niệm

Định nghĩa của an toàn thông tin được nêu ra từ nhiều nguồn khác nhau, chúng ta có thể hiểu theo nhiều cách sau: *An toàn thông tin nghĩa là thông tin được bảo vệ, các hệ thống và dịch vụ có khả năng chống lại những sự can thiệp, lỗi và những tai họa không mong đợi, các thay đổi tác động đến độ an toàn của hệ thống là nhỏ nhất. Hệ thống không an toàn là hệ thống tồn tại những điểm: thông tin bị rò rỉ ra ngoài, thông tin bị thay đổi,* ...

Giá trị thực sự của thông tin chỉ đạt được khi thông tin được cung cấp chính xác và kịp thời, hệ thống phải hoạt động chuẩn xác thì mới có thể đưa ra những thông tin có giá trị cao. *Mục tiêu của an toàn bảo mật trong công nghệ thông tin là đưa ra một số tiêu chuẩn an toàn và áp dụng các tiêu chuẩn an toàn này vào chỗ thích hợp để giảm bớt và loại trừ những nguy hiểm có thể xảy ra.* Ngày nay với kỹ thuật truyền nhận và xử lý thông tin ngày càng phát triển và phức tạp nên hệ thống chỉ có thể đạt tới một mức độ an toàn nào đó và không có một hệ thống an toàn tuyệt đối.

#### Các yêu cầu an toàn bảo mật thông tin

Ngày nay, với sự phát triển rất nhanh của khoa học công nghệ, các biện pháp tấn công ngày càng tinh xảo hơn, độ an toàn của thông tin có thể bị đe dọa từ nhiều nơi, theo nhiều cách khác nhau, chúng ta cần phải đưa ra các chính sách đề phòng thích hợp. Các yêu cầu cần thiết của việc bảo vệ thông tin và tài nguyên:

* *Đảm bảo bí mật (Bảo mật):* thông tin không bị lộ đối với người không được phép.
* *Đảm bảo tính tin cậy (Confidentiality):* Thông tin và tài nguyên không thể bị truy cập trái phép bởi những người không có quyền hạn.
* *Đảm bảo tính toàn vẹn (Integrity):* Thông tin và tài nguyên không thể bị sửa đổi, bị thay thế bởi những người không có quyền hạn.
* *Đảm bảo tính sẵn sàng (Availability):* Thông tin và tài nguyên luôn sẵn sàng để đáp ứng sử dụng cho người có quyền hạn.
* *Đảm bảo tính không thể chối bỏ (Non-repudiation):* Thông tin và tài nguyên được xác nhận về mặt pháp luật của người cung cấp.

#### Các nội dung an toàn thông tin

* *Nội dung chính:*
  + An toàn máy tính: là sự bảo vệ các thông tin cố định bên trong máy tính, là khoa học về bảo đảm an toàn thông tin trong máy tính
  + An toàn truyền tin: là sự bảo vệ thông tin trên đường truyền tin(thông tin được truyền từ hệ thống này sang hệ thống khác), là khoa học bảo đảm an toàn thông tin trên đường truyền tin.
* *Nội dung chuyên ngành:* 
  + An toàn dữ liệu (data security)
  + An toàn cơ sở dữ liệu (database security)
  + An toàn hệ điều hành (operation system security)
  + An toàn mạng máy tính (network security)

#### Các chiến lược bảo đảm an toàn thông tin

*Giới hạn quyền hạn tối thiểu (Last Privilege):*theo nguyên tắc này bất kỳ một đối tượng nào cùng chỉ có những quyền hạn nhất định đối với tài nguyên mạng.

*Bảo vệ theo chiều sâu (Defence In Depth):* Không nên dựa vào một chế độ an toàn nào dù cho chúng rất mạnh, mà nên tạo nhiều cơ chế an toàn để tương hỗ lẫn nhau.

*Nút thắt (Choke Point):* Tạo ra một “cửa khẩu” hẹp, và chỉ cho phép thông tin đi vào hệ thống của mình bằng con đường duy nhất chính là “cửa khẩu” này.

*Điểm nối yếu nhất (Weakest Link):*Chiến lược này dựa trên nguyên tắc: “ Một dây xích chỉ chắc tại mắt duy nhất, một bức tường chỉ cứng tại điểm yếu nhất”.

*Tính toàn cục:* Các hệ thống an toàn đòi hỏi phải có tính toàn cục của các hệ thống cục bộ.

*Tính đa dạng bảo vệ:* Cần phải sử dụng nhiều biện pháp bảo vệ khác nhau cho hệ thống khác nhau, nếu không có kẻ tấn công vào được một hệ thống thì chúng cũng dễ dàng tấn công vào các hệ thống khác.

### Các phương pháp bảo vệ thông tin

*Quyền truy nhập:* Là lớp bảo vệ trong cùng nhằm kiểm soát các tài nguyên của mạng và quyền hạn trên tài nguyên đó.

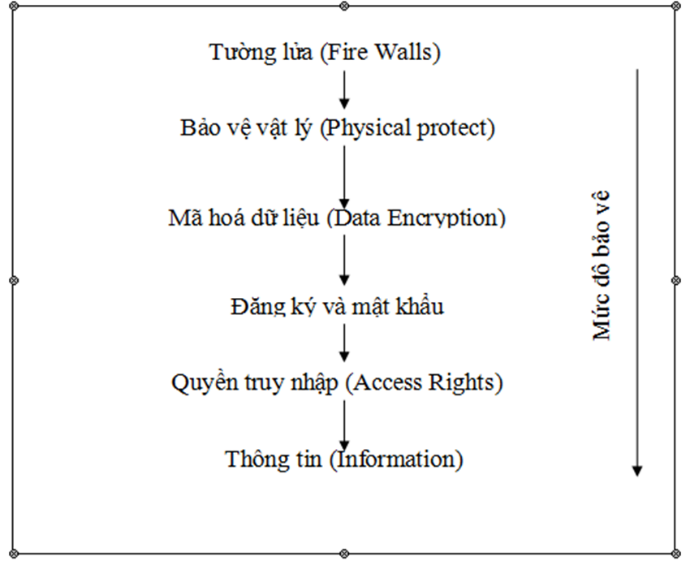
*Đăng ký tên /mật khẩu:* Thực ra đây cũng là kiểm soát quyền truy nhập, nhưng không phải truy nhập ở mức thông tin mà ở mức hệ thống.

*Mã hoá dữ liệu:* Dữ liệu bị biến đổi từ dạng nhận thức được sang dạng không nhận thức được theo một thuật toán nào đó và sẽ được biến đổi ngược lại ở trạm nhận (giải mã).

*Bảo vệ vật lý:* Ngăn cản các truy nhập vật lý vào hệ thống.

*Tường lửa:* Ngăn chặn thâm nhập trái phép và lọc bỏ các gói tin không muốn gửi hoặc nhận vì các lý do nào đó để bảo vệ một máy tính hoặc cả mạng nội bộ (intranet).

*Quản trị mạng:* Công tác quản trị mạng máy tính phải được thực hiện một cách khoa học. Toàn bộ hệ thống hoạt động bình thường trong giờ làm việc. Backup dữ liệu quan trọng theo định kỳ, có kế hoạch bảo trì định kỳ, bảo mật dữ liệu, phân quyền, …



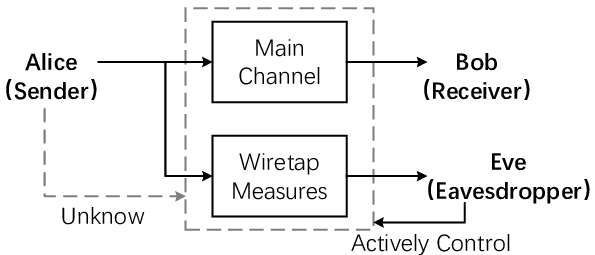
Ảnh .: Các mức độ bảo vệ thông tin

## An toàn thông tin bằng mật mã

### Mật mã và thông tin

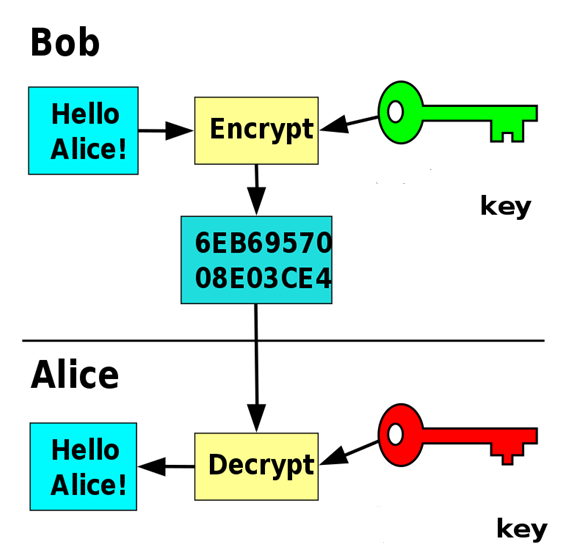
Mật mã là một ngành khoa học chuyên nghiên cứu các phương pháp truyền tin bí mật. Mật mã bao gồm : Lập mã và phá mã.

* *Lập mã* bao gồm hai quá trình: mã hóa và giải mã. Các sản phẩm của lĩnh vực này là các hệ mã mật , các hàm băm, các hệ chữ ký điện tử, các cơ chế phân phối, quản lý khóa và các giao thức mật mã.
* *Phá mã:* Nghiên cứu các phương pháp phá mã hoặc tạo mã giả. Sản phẩm của lĩnh vực này là các phương pháp phá mã , các phương pháp giả mạo chữ ký, các phương pháp tấn công các hàm băm và các giao thức mật mã.



Ảnh .: Thông tin gửi đi bị nghe lén

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 (decryption). Đây là một lớp bảo vệ thông tin rất quan trọng và được sử dụng rộng rãi trong môi trường mạng.



Ảnh .: Bảo vệ thông tin bằng mật mã

Để bảo vệ thông tin bằng mật mã người ta thường tiếp cận theo hai hướng:

* *Theo đường truyền (Link\_Oriented\_Security):* 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. Thông tin chỉ được 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.
* *Từ nút đến nút (End\_to\_End):* thông tin trên mạng được bảo vệ trên toàn đường truyền từ nguồn đến đích. Thông tin sẽ được mã hoá ngay sau khi mới tạo ra và chỉ được giải mã khi về đến đích. Cách này mắc phải nhược điểm là chỉ có dữ liệu của người dùng thì mới có thể mã hóa được còn dữ liệu điều khiển thì giữ nguyên để có thể xử lý tại các nút.

### Hệ mật mã

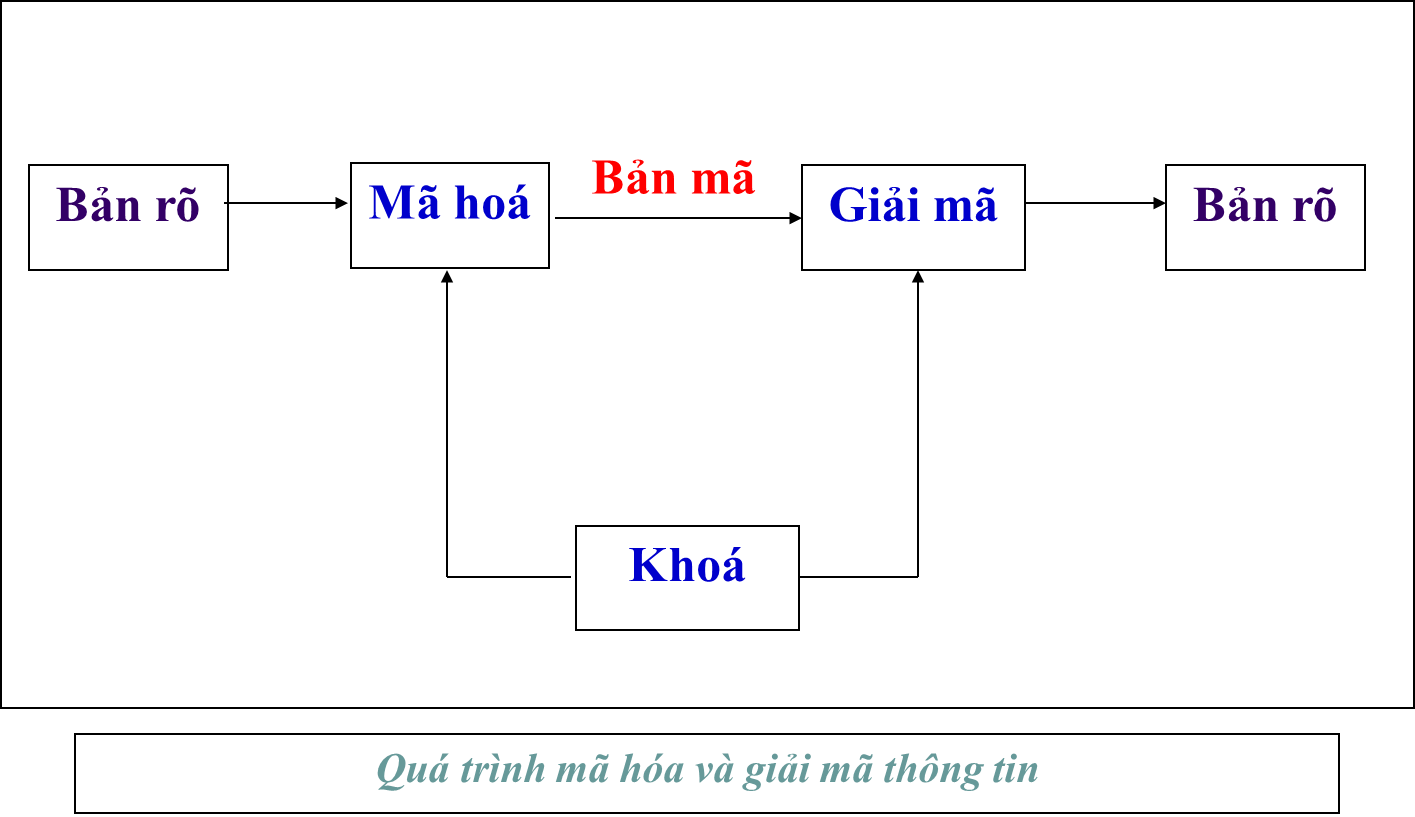
#### Vai trò của hệ mật mã

Các hệ mật mã phải thực hiện được các vai trò sau:

* Hệ mật mã phải che dấu được nội dung của văn bản rõ (PlainText) để đảm bảo sao cho chỉ người chủ hợp pháp của thông tin mới có quyền truy cập thông tin (Secrety), hay nói cách khác là chống truy nhập không đúng quyền hạn.
* Tạo các yếu tố xác thực thông tin, đảm bảo thông tin lưu hành trong hệ thống đến người nhận hợp pháp là xác thực (Authenticity).
* Tổ chức các sơ đồ chữ ký điện tử, đảm bảo không có hiện tượng giả mạo, mạo danh để gửi thông tin trên mạng.

Ưu điểm lớn nhất của bất kỳ hệ mật mã nào đó là có thể đánh giá được độ phức tạp tính toán mà “kẻ địch” phải giải quyết bài toán để có thể lấy được thông tin của dữ liệu đã được mã hoá. Tuy nhiên mỗi hệ mật mã có một số ưu và nhược điểm khác nhau, nhưng nhờ đánh giá được độ phức tạp tính toán mà ta có thể áp dụng các thuật toán mã hoá khác nhau cho từng ứng dụng cụ thể tuỳ theo yêu cầu về độ an toàn.

#### Mã hóa và giải mã thông tin



Ảnh .: Quá trình mã hóa và giải mã thông tin

* Mã hóa: Quá trình chuyển đổi dữ liệu gốc thành dữ liệu được mã hóa sao cho người khác không thể đọc hiểu được.
* Giải mã: Là quá trình ngược lại của mã hóa, biến đổi dữ liệu đã được mã hóa thành dạng gốc ban đầu.
* Bản mã: Tệp dữ liệu đã được mã hóa.

Một hệ thống mã hóa bao gồm các thành phần sau:

* PlainText : Bản tin sẽ được mã hóa hay bản tin gốc.
* CipherText : Bản tin đã được mã hóa hay bản tin mã.
* Thuật toán mã hóa và giải mã :
  + Encryption : quá trình chuyển bản tin gốc sang dạng mật mã.
  + Decryption : quá trình giải bản tin dạng mật mã trở về bản tin gốc.
  + Cách chọn khóa : giá trị toán học dùng để thực hiện mã hóa.

Nhiều phương pháp mã hóa đã được đưa ra dựa trên những giải thuật toán phức tạp, để tạo khó khăn cho những ai đó muốn phá mật mã mà không cần được ai trao chìa khóa. Nói tạo khó khăn là vì trên lý thuyết ta không thể nói việc tìm chìa khóa là vô phương. Nhưng nếu trở ngại đủ lớn để làm nản lòng kẻ gian thì đã là một mức độ an toàn tốt. Quá trình mã hóa và giải mã có thể được minh họa theo sơ đồ sau:

#### Các thành phần của một hệ mật mã

Một hệ mã mật là bộ 5 (P, C, K, E, D) thoả mãn các điều kiện sau:

* P là tập hữu hạn các bản rõ (PlainText), nó được gọi là không gian bản rõ chứa bản tin gốc ban đầu.
* C là tập hợp hữu hạn bản mã (Crypto), nó còn được gọi là không gian các bản mã. Một phần tử của C có thể nhận được bằng cách áp dụng phép mã hóa EK lên một phần tử 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 “kẻ địch” không có đủ thời gian thử mọi khoá có thể (phương pháp vét cạn).
* Đối với mỗi k ∈ K có một quy tắc mã eK: P → C và một quy tắc giải mã tương ứng dK ∈ D. Mỗi eK: P→ C và dK: C → P là những hàm mà:

dK (eK(x))=x với mọi bản rõ x ∈ P.

* Hàm giải mã dk chính là ánh xạ ngược của hàm mã hóa ek

#### Phân loại hệ mật mã

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

* Hệ mật đối xứng (hay còn gọi là mật mã khóa bí mật)
* Hệ mật mã bất đối xứng (hay còn gọi là mật mã khóa công khai)

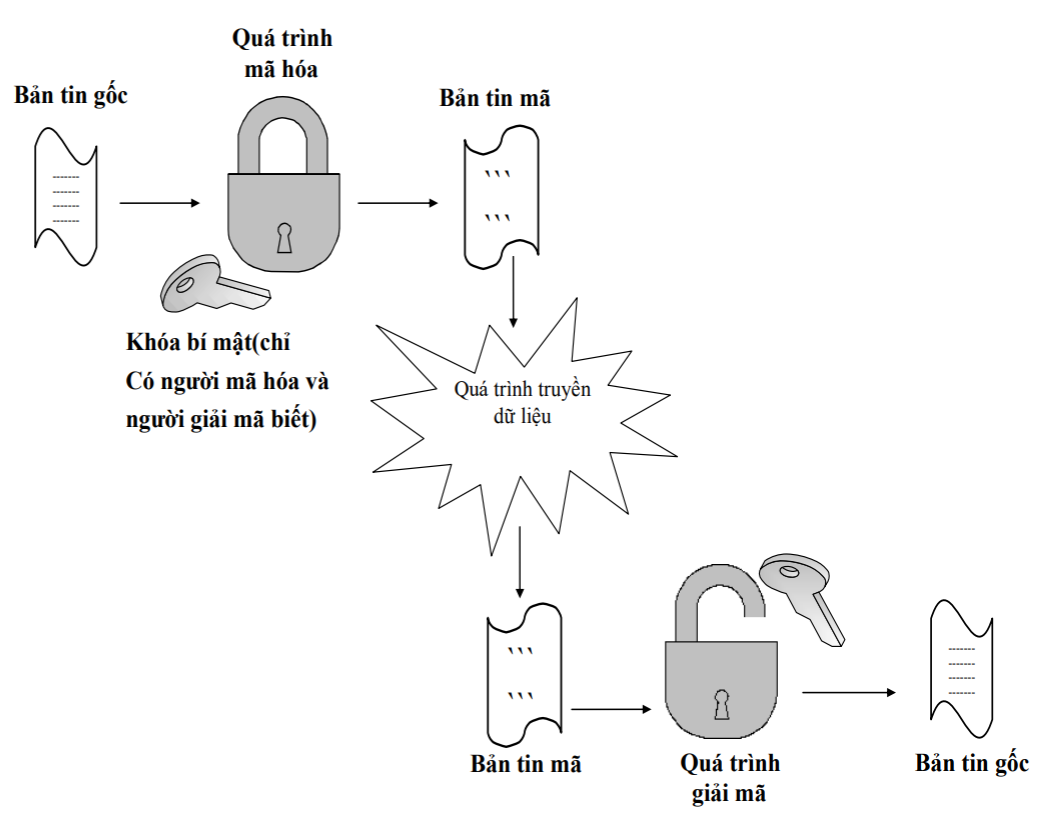
Ngoài ra nếu dựa vào thời gian đưa ra hệ mật mã ta còn có thể phân làm hai loại: Mật mã cổ điển (là hệ mật mã ra đời trước năm 1970) và mật mã hiện đại (ra đời sau năm 1970). Còn nếu dựa vào cách thức tiến hành mã thì hệ mật mã còn được chia làm hai loại là mã dòng (tiến hành mã từng khối dữ liệu, mỗi 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).

##### Mã hóa bằng khóa bí mật

Các hệ thống mã hóa với khóa bí mật còn được gọi là mã hóa bằng khóa riêng, mã hóa đối xứng sử dụng duy nhất một khóa cho cả quá trình mã hóa lẫn quá trình giải mã.

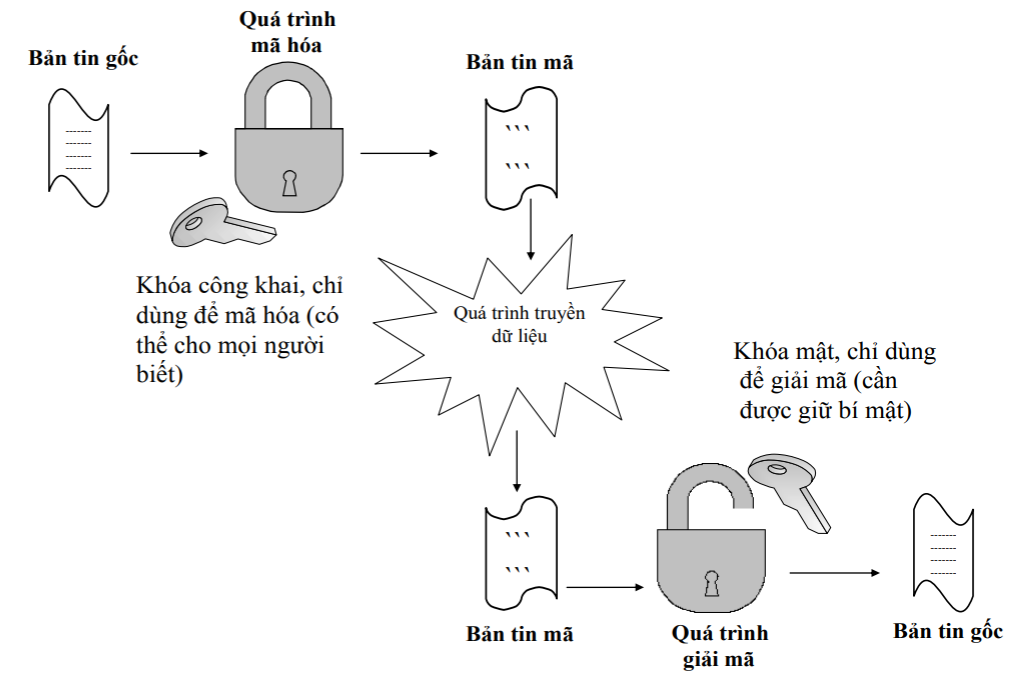
* Stream Algorithms/Stream Ciphers: các thuật toán hoạt động trên văn bản bình thường theo từng bit một.
* Block Algorithms/Block Ciphers : các thuật toán hoạt động trên văn bản theo các khối (32 bit, 64 bit, 128 bit, ...).
* Một số thuật toán đang được sử dụng rộng rãi hiện nay : DES, TripleDES, RC5, RC6, Rijndael ...

Quá trình mã hóa và giải mã bằng cách sử dụng khóa bí mật được minh họa như hình dưới đây:



Ảnh .: Sơ đồ mã hóa và giải mã bằng khóa riêng

##### Mã hóa bằng khóa công khai



Ảnh .: Sơ đồ mã hóa và giải mã bằng khóa công khai

Mã hóa bằng khóa công khai còn gọi là mã hóa bất đối xứng hay mã hóa bằng khóa chung. Sự khác biệt cơ bản giữa một hệ thống mã hóa bằng khóa bí mật với hệ thống mã hóa bằng khóa công khai là hệ thống mã hóa khóa công khai dùng hai khóa khác nhau để mã hóa và giải mã. Do đó, một bộ mã công khai sẽ bao gồm hai khóa: một khóa dành cho người mã hóa thường được công khai, và khóa còn lại dùng cho người giải mã thường được giữ bí mật. Như vậy, hệ thống mã hóa với khóa công khai cần có một quá trình sinh ra hai khóa để mã hóa và giải mã thông điệp. Các khóa này được xem như là một đôi:

* Public-key (khóa công khai): được phép công khai mà không phải chịu rủi ro về an toàn. Khóa này được dùng để mã hóa thông điệp.
* Private-key (khóa bí mật): không được để lộ. Mỗi thông điệp được mã hóa bằng public-key chỉ có thể giải mã bằng một khóa mật thích hợp.
* Một số thuật toán mã hóa công khai phổ biến : RSA, Diffie-Hellman KeyExchange Algorithm (dùng cho việc phân phối và trao đổi khóa).

Như vậy, với sự bùng nổ của mạng toàn cầu mọi hệ thống thông tin đều phải đương đầu với bài toán an toàn và bảo mật. Như đã trình bày, có nhiều chiến lược cũng như phương pháp bảo đảm bảo an toàn thông tin. Trong đó, an toàn thông tin bằng mật mã có vai trò pháp quan trọng và được ứng dụng rộng khắp không chỉ trong ngành công nghệ thông tin mà còn dùng để bảo mật những thông tin và tài liệu quan trọng ngoài đời. (Ví dụ như bảo mật đề thi trong tuyển sinh được đề cập đến trong chương sau)

## Chương trình demo ( Python )

Graphical user interface, application

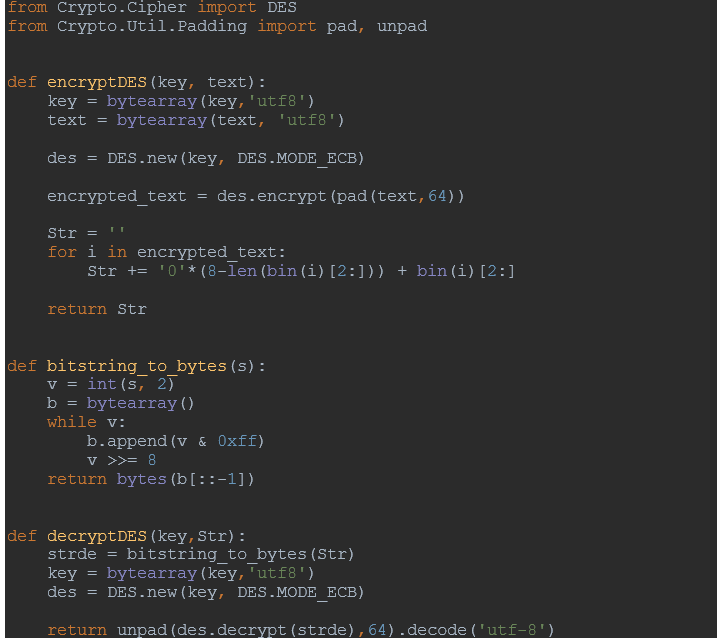
Description automatically generated

*Giao diện mã hóa*

Graphical user interface, text, application

Description automatically generated

*Giao diện giải mã*

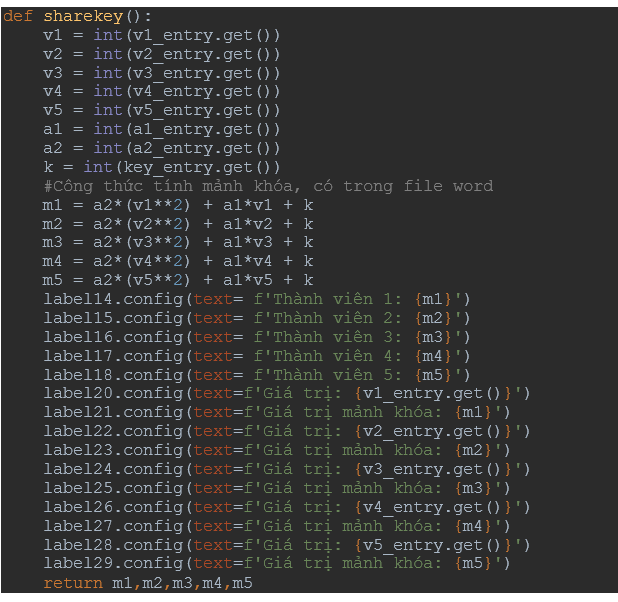
**

*Hàm mã hóa (encrypt) / giải mã (decrypt)*

Graphical user interface, application

Description automatically generated

*Giao diện chia sẻ khóa*



*Hàm chia sẻ khóa*

# Chuẩn mã dữ liệu DES

Như đã trình bày ở chương trước: mọi thông tin cần bảo vệ nên được mã hóa. Với sự phát triển của công nghệ, nhiều hệ mật mã khác nhau được ra đời từ các hệ mật mã truyền thống đến các hệ mật mã hiện đại. Từ những năm 70 của thế kỷ trước, các nhà khoa học đã nghiên cứa và tạo ra nhiều phương thức mật mã với tốc độ mã hóa rất nhanh chỉ cần giữ bí mật khóa mã (mã hóa đối xứng) và mã hóa được mọi dữ liệu tùy ý. Đó là một bước tiến vĩ đại của kỹ thuật mật mã .Trong đó mã DES (Data Encryption Standard) là một điển hình của bước tiến này.

## Hệ mã hóa khối DES (Trần Trường Anh)

### Lịch sử của DES

Vào những năm đầu thập kỷ 70, nhu cầu có một chuẩn chung về thuật toán mật mã đã trở nên rõ ràng. Các lý do chính là:

* Sự phát triển của công nghệ thông tin và của nhu cầu an toàn & bảo mật thông tin: sự ra đời của các mạng máy tính tiền thân của Internet đã cho phép khả năng hợp tác và liên lạc số hóa giữa nhiều công ty, tổ chức trong các dự án lớn của chính phủ Mỹ.
* Các thuật toán mã hóa cổ điển không thể đảm bảo được tính tin cậy đòi hỏi cao.
* Các thiết bị khác nhau đòi hỏi sự trao đổi thông tin mật mã thống nhất, chuẩn.

Một chuẩn chung cần thiết phải có với các thuộc tính như:

* Bảo mật ở mức cao.
* Thuật toán được đặc tả và hoàn toàn công khai, tức là tính bảo mật không được phép dựa trên những những đặc điểm của thuật toán mã hóa.
* Việc cài đặt phải dễ dàng để đem lại tính kinh tế.
* Phải mềm dẻo để áp dụng được cho muôn vàn nhu cầu ứng dụng.

Năm 1972, Viện tiêu chuẩn và công nghệ quốc gia Hoa kỳ (National Institute of Standards and Technology-NIST) đặt ra yêu cầu xây dựng một thuật toán mã hoá bảo mật thông tin với yêu cầu là dễ thực hiện, sử dụng được rộng rãi trong nhiều lĩnh vực và mức độ bảo mật cao. Năm 1974, IBM giới thiệu thuật toán Lucifer, thuật toán này đáp ứng hầu hết các yêu cầu của NIST. Sau một số sửa đổi, năm 1976, Lucifer được NIST công nhận là chuẩn quốc gia Hoa kỳ và được đổi tên thành Data Encryption Standard (DES).

DES là thuật toán mã hoá bảo mật được sử dụng rộng rãi nhất trên thế giới, tồn tại trong nhiều lĩnh vực như ngân hàng, thương mại, thông tin… và vẫn được tin dùng trong 2 thập kỷ sau đó, trước khi bị thay thế bởi AES.

### Mật mã khối

Các hệ mã hóa cổ điển đều có điểm đặc trưng là từng ký tự của bản rõ được mã hóa tách biệt. Điều này làm cho việc phá mã trở nên dễ dàng hơn. Chính vì vậy, trên thực tế người ta sử dụng một kiểu mật mã khác, trong đó từng khối ký tự của bản rõ được mã hóa cùng một lúc như là một đơn vị mã hóa đồng nhất. Trong kiểu mã hóa này, các tham số quan trọng là kích thước (độ dài) của mối khối và kích thước khóa.

*Điều kiện để mã hóa khối an toàn:*

* Kích thước khối phải đủ lớn để chống lại phương án tấn công bằng phương pháp thống kê. Tuy nhiên điều này sẽ dẫn đến thời gian mã hóa sẽ tăng lên.
* Không gian khóa, tức chiều dài khóa phải đủ lớn để chống lại phương án tấn công bằng vét cạn. Tuy nhiên khóa phải đủ ngắn để tạo khóa, phân phối và lưu trữ khóa được dễ dàng.

Khi thiết kế một hệ mã khối, phải đảm bảo hai yêu cầu sau:

* Sự hỗn loạn (confusion): sự phụ thuộc giữa bản rõ và bản mã phải thực sự phức tạp để gây khó khăn với việc tìm quy luật thám mã. Mối quan hệ này tốt nhất là phi tuyến.
* Sự khuếch tán (diffusion): Mỗi bit của bản rõ và khóa phải ảnh hưởng lên càng nhiều bit của bản mã càng tốt.

Trong khi sự hỗn loạn (confusion) được tạo ra bằng kỹ thuật thay thế thì sự khuếch tán (diffusion) được tạo ra bằng kỹ thuật hoán vị. Hệ mã hóa khối được xem xét trong tài liệu này đều thỏa mãn các yêu cầu đó.

Ngoài hệ mã hóa khối được trình bày trong tài liệu (DES) còn có rất nhiều các hệ ãm hóa khối khác đã phát triển qua thời gian (tại các quốc gia khác nhau và ứng dụng trong các lĩnh vực khác nhau), có thể kể ra như: Lucifer (1969), Madryga (1984), NewDES(1985), FEAL, REDOC, LOKI (1990), Khufu and Khafre (1990), RC2, RC4, IDEA (1990), MB, CA-1.1, Shipjack, GOST, CAST, ca, SAFER, 3-Way, Crab, SXAL8/MBAL, RC5, RC6, …

Đặc điểm chung của các hệ mã khối là quá trình mã hóa làm việc với khối dữ liệu (thường dạng xâu bit) có kích thước khác nhau (tối thiểu là 64 bit), khóa của các hệ mã cũng là một xâu bit có độ dài cố định (56 bit với DES, và các hệ mã khác là 128, 256 hoặc thậm chí là 512 bit). Tất cả các hệ mã này đều dựa trên lý thuyết của Shannon đưa ra năm 1949 và nếu mang mã hóa hai bản rõ giống nhau sẽ thu được cùng một bản mã. Hoạt động của các hệ mã khối thường được qua một số lần lặp, mỗi lần sẽ sử dụng một khóa con được sinh ra từ khóa chính.

## Kỹ thuật hệ mã hóa DES

Trong phương pháp DES, kích thước khối là 64 bit. DES thực hiện mã hóa dữ liệu qua 16 vòng lặp mã hóa, mỗi vòng sử dụng một khóa chu kỳ 48 bit được tạo ra từ khóa ban đầu có độ dài 56 bit. DES sử dụng 8 bảng hằng số S-box để thao tác

Quá trình mã hóa của DES có thể tóm tắt như sau : Biểu diễn thông điệp nguồn x∈ P bằng dãy 64 bit. Khóa k có 56 bit. Thực hiện mã hóa theo 3 giai đoạn :

1. Tạo dãy 64 bit x0 bằng cách hoán vị x theo hoán vị IP (Initial Permutation)

Biểu diễn x0 =IP(x)=L0R0, L0 gồm 32 bit bên trái của x0 .R0 gồm 32 bit bên phải của x0.

|  |  |
| --- | --- |
| L0 | R0 |

X0

**Hình 2.2 :** Biểu diễn dãy 64 bit x thành 2 thành phần L và R

2. Thực hiện 16 vòng lặp từ 64 bit thu được và 56 bit của khóa k (chỉ sử dụng 48 bit của khóa k trong mỗi vòng lặp). 64 bit kết quả thu được qua mỗi vòng lặp sẽ là đầu vào cho vòng lặp sau. Các cặp từ 32 bit Li, Ri (với 1 ≤ I ≤ 16 ) được xác định theo quy tắc sau:

Li=Ri-1

Ri=Li-1⊕ f(Ri-1, Ki)

Với ⊕ biểu diễn phép toán XOR trên hai dãy bit, K1, K2,...,K16 là các dãy 48 bit phát sinh từ khóa K cho trước ( Trên thực tế, mỗi khóa Ki được phát sinh bằng cách hoán vị các bit trong khóa K cho trước)

3. Áp dụng hoán vị ngược IP-1 đối với dãy bit R16L16, thu được từ y gồm 64 bit. Như vậy, y=IP-1 (R16L16)

Hàm f được sử dụng ở bước 2 là hàm số gồm 2 tham số: Tham số thứ nhất A là một dãy 32 bit , tham số thứ hai J là một dãy 48 bit. Kết quả của hàm f là một dãy 32 bit. Các bước xử lý của hàm f (A,J) như sau:

Tham số thứ nhất A (32 bit) được mở rộng thành dãy 48 bit được phát sinh từ A bằng cách hoán vị theo một thứ tự nhất định 32 bit của A, trong đó có 26 bit của A được lặp lại 2 lần trong E (A).

Li-1 Ri-1

Li  Ri

Ki

**Hình 2.3 :** Quy trình phát sinh dãy Li Ri  từ dãy Li-1 Ri-1 và khóa Ki

Thực hiện phép toán XOR cho hai dãy 48 bit E(A) và J, ta thu được một dãy 48 bit B. Biểu diễn B thành từng nhóm 6 bit như sau: B=B1 B2 B3 B4 B5 B6 B7 B8 Sử dụng 8 ma trận S1, S2, ..., S8 mỗi ma trận Si có kích thước 4x16 và mỗi dòng của ma trận nhận đủ 16 giá trị từ 0 đến 15. Xét dãy gồm 6 bit Bj= b1 b2 b3 b4 b5 b6, Sj(Bj) được xác định bằng giá trị của phần tử tại dòng r cột c của Sj, trong đó, chỉ số dòng r có biểu diễn nhị phân là b1 b6 , chỉ số cột c có biểu diễn nhị phân là b2 b3 b4 b5. Bằng cách này, ta xác định được các dãy 4 bit Cj=Sj(Bj), 1 ≤ j ≤ 8.

Tập hợp các dãy 4 bit Cj lại, ta có được dãy 32 bit C= C1 C 2 C3 C4 C5 C6 C7 C8. Dãy 32 bit thu được bằng cách hoán vị C theo một quy luật P nhất định chính là kết quả của hàm F(A,J).

Quá trình giải mã diễn ra tương tự nhưng với các khóa con ứng dụng vào các vòng theo thứ tự ngược lại

Có thể hình dung đơn giản là phần bên phải trong mỗi vòng (sau khi mở rộng input 32 bit thành 8 ký tự 6 bit – xâu 48 bit) sẽ thực hiện một tính toán thay thế phụ thuộc khóa trên mỗi ký tự trong xâu 48 bit, và sau đó sử dụng một phép chuyển bit cố định để phân bố lại các bit của các ký tự kết quả hình thành nên output 32 bit.

Các khóa con Ki (chứa 48 bit của K) được tính bằng cách sử dụng các bảng PC1 và PC2 (Permutation Choice 1 và 2). Trước tiên 8 bit ( K8, K16, …, K64) của K bị bỏ đi (áp dụng PC1). 56 bit còn lại được hoán vị và gán cho hai biến 28 bit C và D sẽ được quay 1 hoặc 2 bit, và các khóa con 48 bit Ki được chọn từ kết quả của việc ghép hai xâu với nhau.

Như vậy, ta có thể mô tả toàn bộ thuật toán sinh mã DES dưới dạng công thức như sau:

**Y = IP-1 • f16 • T • f15 • T • ... • f2 • T • f1 • IP(X)**

Trong đó :

- T mô tả phép hoán vị của các khối Li, RI (1 ≤ i ≤ 15).

- fi mô tả việc dùng hàm f với khóa Ki (1 ≤ i≤ 16)

## Chương trình demo ( PHP )

## Ưu nhược điểm ( Đinh Huy Đại )

### Ưu điểm:

- Có tính bảo mật cao

- Công khai, dễ hiểu

- Nó có thể triển khai trên thiết bị điện tử có kích thước nhỏ

### Các yếu điểm của DES:

#### Tính bù

Nếu ta ký hiệu  là phần bù của u (ví dụ : 0100101 là phần bù của 1011010) thì des có tính chất sau

y = DES (x,k) → = DES (  ,)

Cho nên nếu ta biết mã y được mã hóa từ thông tin x với khóa K thì ta suy được bản mã  được mã hóa từ bản rõ  với khóa . Tính chất này là một yếu điểm của DES bởi vì qua đó đối phương có thể loại bỏ đi một số khóa phải thử khi tiến hành thử giải mã theo kiểu vét cạn

#### Khóa yếu

Khóa yếu là các khóa mà theo thuật toán sinh khóa con thì tất cả 16 khóa con đều như nhau : K1=K2=... =K16. Điều đó khiến cho việc mã hóa và giải mã đối với khóa yếu là giống hệt nhau

Bảng .: Các khóa yếu của DES

|  |  |  |
| --- | --- | --- |
| **Khóa yếu (Hex)** | **C0** | **D0** |
| 0101 0101 0101 0101  FEFE FEFE FEFE FEFE  1F1F 1F1F 0E0E 0E0E  E0E0 E0E0 F1F1 F1F1 | {0}28  {1}28  {0}28  {1}28 | {0}28  {1}28  {1}28  {0}28 |

Đồng thời còn có 6 cặp khóa nửa yếu (semi-weak key) khác với thuộc tính như sau :

y= DES(x,k1) và y=DES(x,k2)

Nghĩa là với 2 khóa khác nhau nhưng mã hóa cùng một bản mã từ cùng một bản rõ :

Bảng .: Các khóa nửa yếu của DES

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| C0 | D0 | Semi-weak key(Hex) | | C0 | D0 |
| {01}14  {01}14  {01}14  {01}14  {0}28  {1}28 | {01}14  {10}14  {0}28  {1}28  {01}14  {01}14 | 01FE 01FE 01FE 01FE  1FE0 1FE0 1FE0 1FE0  01E0 01E0 01F1 01F1  1FFE 1FFE 0EFE 0EFE  011F 011F 010E 010E  E0FE E0FE F1FE F1FE | FE01 FE01 FE01 FE01  E01F E01F E01F E01F  E001 E001 F101 F101  FE1F FE1F FE0E FE0E  1F01 1F01 0E01 0E01  FEE0 FEE0 FEF1 EF1 | {10}14  {10}14  {10}14  {10}14  {0}28  {1}28 | {10}14  {01}14  {0}28  {1}28  {10}14  {10}14 |

#### DES có cấu trúc đại số

Với 64 bit khối bản rõ có thể được ánh xạ lên tất cả các vị trí của khối 64 bit khối bản mã trong 264 cách. Trong thuật toán DES, với 56 bit khóa có thể cho chúng ta 256 (khoảng 1017 ) vị trí ánh xạ. Với việc đa mã hóa thì không gian ánh xạ còn lớn hơn. Tuy nhiên điều này chỉ đúng nếu việc mã hóa DES là không cấu trúc

Với DES có cấu trúc đại số thì việc đa mã hóa sẽ được xem ngang bằng với việc đơn mã hóa. Ví dụ như có hai khóa bất kỳ K1 và K2 thì sẽ luôn được khóa K3 như sau :

EK2(EK1(X))=EK3(X)

Nói một cách khác, việc mã hóa DES mang tính chất “nhóm”, đầu tiên mã hóa bản rõ bằng khóa K1 sau đó là khóa K2 sẽ giống với việc mã hóa ở khóa K3. Điều này thực sự quan trọng nếu sử dụng DES trong đa mã hóa. Nếu một “nhóm” được phát với cấu trúc hàm quá nhỏ thì tính an toàn sẽ giảm.

#### Không gian khóa K

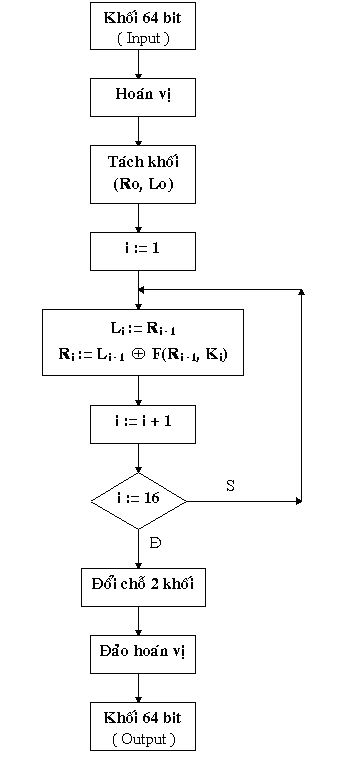
DES có 256 = 1017 khóa. Nếu chúng ta biết được một cặp “tin/mã” thì chúng ta có thể thử tất cả 1017 khả năng này để tìm ra khóa cho kết quả khớp nhất. Giả sử như một phép thử mất 10-6s, thì chúng sẽ mất 1011s, tức 7300 năm. Nhưng với các máy tính được chế tạo theo xử lý song song. Chẳng hạn với 107 con chip mã DES chạy song song thì bây giờ mỗi một con chipset chỉ phải chịu trách nhiệm tính toán với 1010 phép thử. Chipset mã DES ngày nay có thể xử lý tốc độ 4.5x107 bit/s tức có thể làm được hơn 105 phép mã DES trong một giây.

Vào năm 1976 và 1977, Dieffie và Hellman đã ước lượng rằng có thể chế tạo được một máy tính chuyên dụng để vét cạn không gian khóa DES trong ½ ngày với cái giá 20 triệu đô la. Năm 1984, chipset mã hóa DES với tốc độ mã hóa 256000 lần/giây. Năm 1987, đã tăng lên 512000 lần/giây. Vào năm 1993, Michael Wiener đã thiết kế một máy tính chuyên dụng với giá 1 triệu đô la sử dụng phương pháp vét cạn để giải mã DES trung bình trong vòng 3,5 giờ (và chậm nhất là 7 giờ).

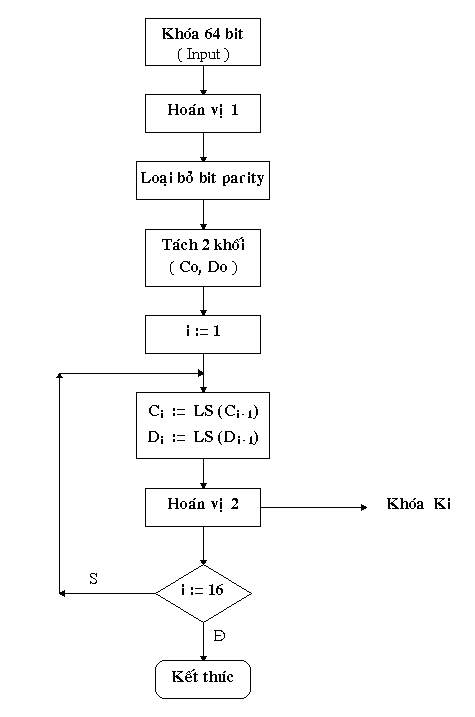
Đến năm 1990, hai nhà toán học người Do Thái – Biham và Shamir – đã phát minh ra phương pháp mã hóa vi sai (diferential cryptanalyis), đây là một kỹ thuật sử dụng những phỏng đoán khác nhau trong bản rõ để đưa ra những thông tin trong bản mã. Với phương pháp này, Biham và Shamir đã chứng minh rằng nó hiệu quả hơn cả phương pháp vét cạn.

Phá mã vi sai là thuật toán xem xét những cặp mã khóa khác nhau, đây là những cặp mã hóa mà bản mã của chúng là khác biệt. Người ta sẽ phân tích tiến trình biến đổi của những cặp mã này thông qua các vòng của DES khi chúng được mã hóa với cùng một khóa K. Sau đó sẽ chọn hai bản rõ khác nhau một cách ngẫu nhiên hợp lý nhất. Sử dụng sự khác nhau của kết quả bản mã và gán cho những khóa khác nhau một cách phù hợp nhất. Khi phân tích nhiều hơn những cặp bản mã, chúng ta sẽ tìm ra một khóa được xem là đúng nhất.

## Sơ đồ khối

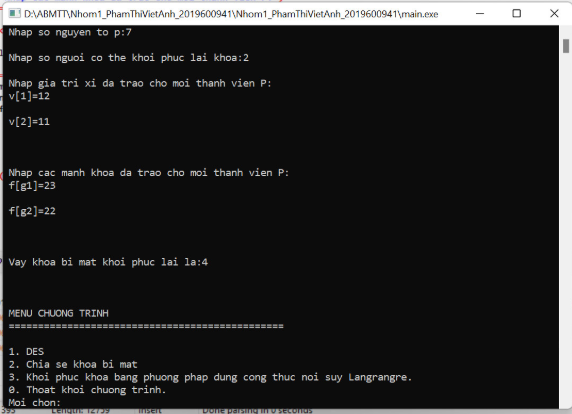


Ảnh .: Sơ đồ khối chương trình DES

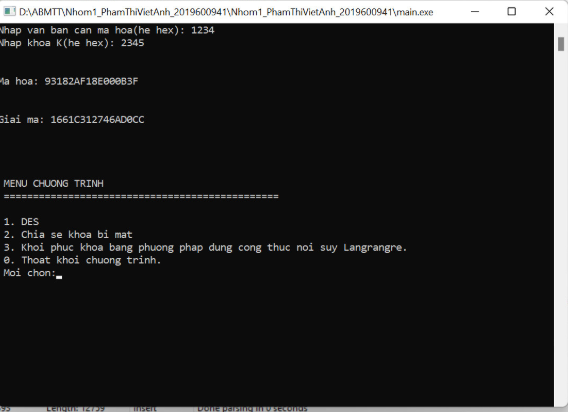


Ảnh .: Sơ đồ khối quá trình sinh khóa

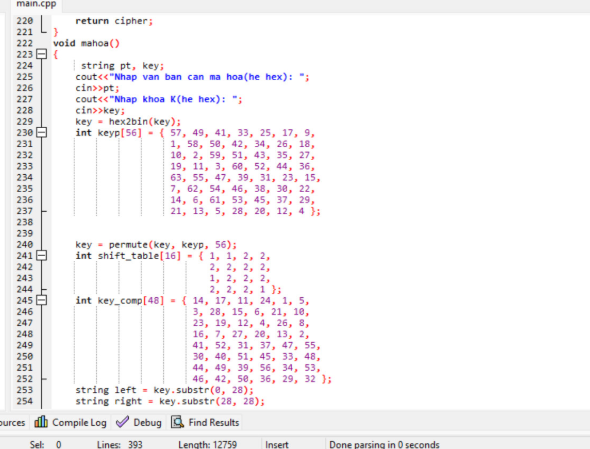
## Chương trình demo (C++)



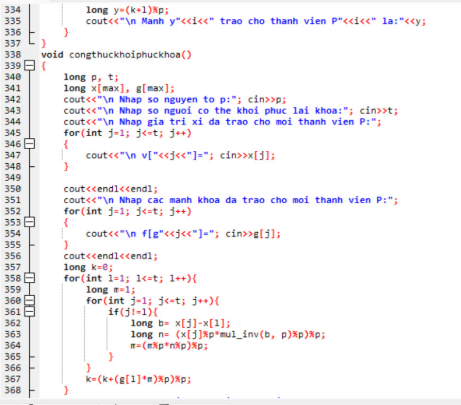
*Chia sẻ khóa*

**

*Giải mã / Mã Hóa*

**

*Hàm mã hóa*

**

*Hàm khôi phục khóa*

## Thuật toán ( Phạm Quốc Anh )

DES là thuật toán mã hóa khối, nó xử lý từng khối thông tin của bản rõ có độ dài xác định là 64 bit. Trước khi đi vào 16 chu trình chính, khối dữ liệu cần bảo mật được “bẻ” ra từng khối 64 bit, và từng khối 64 bit này sẽ được lần lượt đưa vào 16 vòng mã hóa DES để thực hiện

**Input:** bản rõ M = m1m2 … m64, là một khối 64 bit, khóa 64 bit K = k1k2 . . . k64 (bao gồm cả 8 bit chẵn lẻ, việc thêm bit chẵn lẻ sao cho các đoạn khóa 8 bit có số bit 1 là lẻ)

**Output:** bản mã 64 bit C = c1 c2 … c64

1. Sinh khóa con. Tính các khóa con theo thuật toán sinh khóa con
2. (L0,R0) ← IP (m1 m2 . . . m64) (sử dụng bản hoán vị IP để hoán vị các bit, kết quả nhận được chia thành 2 nửa là L0 = m58 m50 . . . m8, R0 = m57 m49 . . . m7)
3. Với i chạy từ i=1 đến 16 thực hiện:

Tính các Li và Ri theo công thức:

Li=Ri-1;

Ri=Li-1 ⊕ f(Ri-1) trong đó f ( Ri-1, Ki )=P ( S ( E ( Ri-1 ) ⊕ Ki ) );

Việc tính f ( Ri-1 ) = P ( S ( E ( Ri-1 ) ⊕ Ki ) ) được thực hiện như sau:

🟆 Mở rộng Ri-1 = r1r2 . .. r32 từ 32 bit thành 48 bit bằng cách sử dụng hoán vị mở rộng E.

T ← E ( Ri-1 ) . ( Vì thế T = r32 r1 r2 . . . r32 r1)

🟆 T’ ← T ⊕ Ki. Biểu diễn T’ như là các xâu gồm 8 ký tự 6 bit T’ = ( B1, . . . ,B8 )

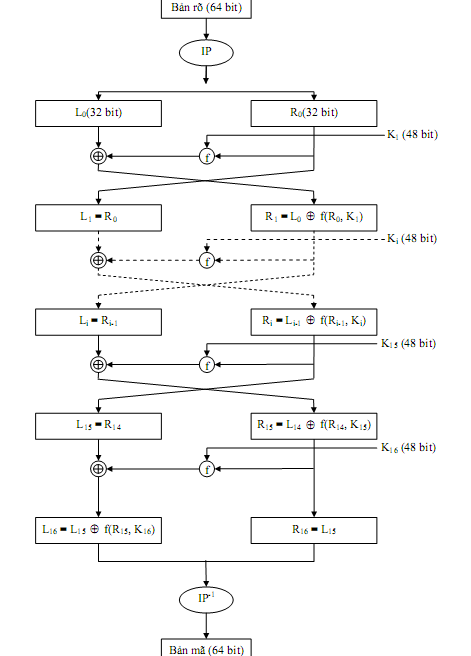
🟆 T’’ ← ( S1 ( B1 ) , S2 ( B2 ) , . . . , S8 ( B8 ) ). Trong đó Si ( Bi ) ánh xạ b1b2 . . . b6 thành các xâu 4 bit của phần tử thuộc hàng r và cột c của các bảng Si (S box) trong đó r = 2 \* b1 + b6 và c = b2 b3 b4 b5 là một số nhị phân từ 0 tới 15. Chẳng hạn S1 ( 011011) sẽ cho r = 1 và c = 3 và kết quả là 5 biểu diễn dưới dạng nhị phân là 0101.

🟆 T’’’ ← P ( T’’) trong đó P là hoán vị cố định để hoán vị 32 bit của

T’’ = t1 t2 . . . t32 sinh ra t16 t7 . . . t25

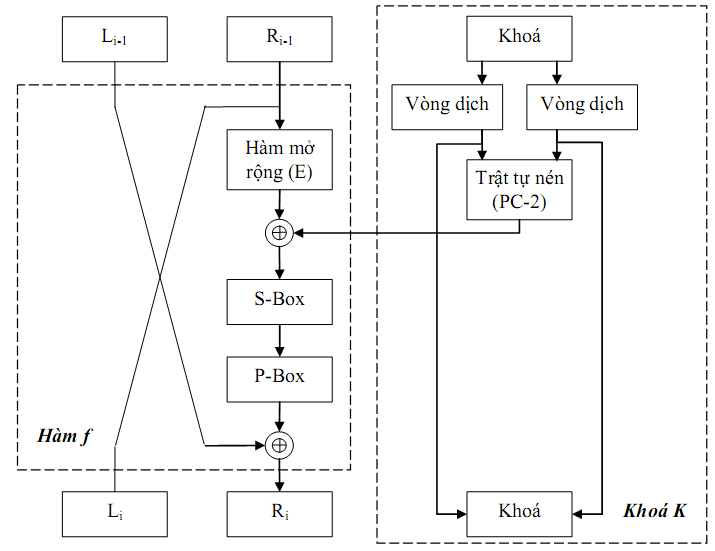
1. Khối từ b1 b2 . . . b64 ← ( R16, L16) ( đổi vị trí các khối cuối cùng L16, R16)

C ← IP-1 ( b1 b2 . . . b64) ( Biến đổi sử dụng IP-1, C = b40 b8 . . . b25).



Ảnh .: Sơ đồ mã hóa DES

### Quá trình mã hóa:

****

Ảnh .: Sơ đồ một vòng DES

Chia làm 3 giai đoạn:

#### Giai đoạn 1:

Với bản rõ cho trước x, 1 xâu x' sẽ được tạo ra bằng cách hoán vị các bit của x theo hoán vị ban đầu IP:

x'=IP(x)=L0 R0

L0:32 bit đầu

R0:32 bit cuối

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***Bộ chuyển vị IP*** | | | | | | | |
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 |
| 60 | 52 | 44 | 36 | 28 | 20 | 12 | 4 |
| 62 | 54 | 46 | 38 | 30 | 22 | 14 | 6 |
| 64 | 56 | 48 | 40 | 32 | 24 | 16 | 8 |
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 |
| 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 |
| 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 |

Bảng .: Hoán vị IP

#### Giai đoạn 2:

Tính toán 16 lần lập theo 1 hàm xác định. Ta sẽ tính LiRi (1≤ i ≤ 16) theo quy tắc:

Li=Ri-1  
 Ri = Li-1⊕ f (Ri-1, Ki)

Với: ⊕ là toán tử Xor, k1,k2,k3.....k16 là xâu bit độ dài 48 bit được tính qua hàm khoá K (thực tế thì Ki là 1 phép hoán vị bit trong K)

#### Giai đoạn 3:

Áp dụng hoán vị ngược IP-1 cho xâu bit R16 L16 ta thu được bản mã y:  
y = IP-1 (R16 L16)

+ Chú ý vị trí của R16 và L16.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Hoán vị nghịc đảo IP-1** | | | | | | | |
| 40 | 8 | 48 | 16 | 56 | 24 | 64 | 32 |
| 39 | 7 | 47 | 15 | 55 | 23 | 63 | 31 |
| 38 | 6 | 46 | 14 | 54 | 22 | 62 | 30 |
| 37 | 5 | 45 | 13 | 53 | 21 | 61 | 29 |
| 36 | 4 | 44 | 12 | 52 | 20 | 60 | 28 |
| 35 | 3 | 43 | 11 | 51 | 19 | 59 | 27 |
| 34 | 2 | 42 | 10 | 50 | 18 | 58 | 26 |
| 33 | 1 | 41 | 9 | 49 | 17 | 57 | 25 |

Bảng .: . Hoán vị IP-1

### Quá trình giải mã:

Do là 1 thuật toán đối xứng nên quá trình giải mã và mã hóa cũng gần giống nhau chỉ khác ở:

Li=Ri-1  
Ri = Li-1⊕ f (Ri-1, K16-i)

Khóa K của hàm F sẽ đi từ 16 ->0

### Hàm F

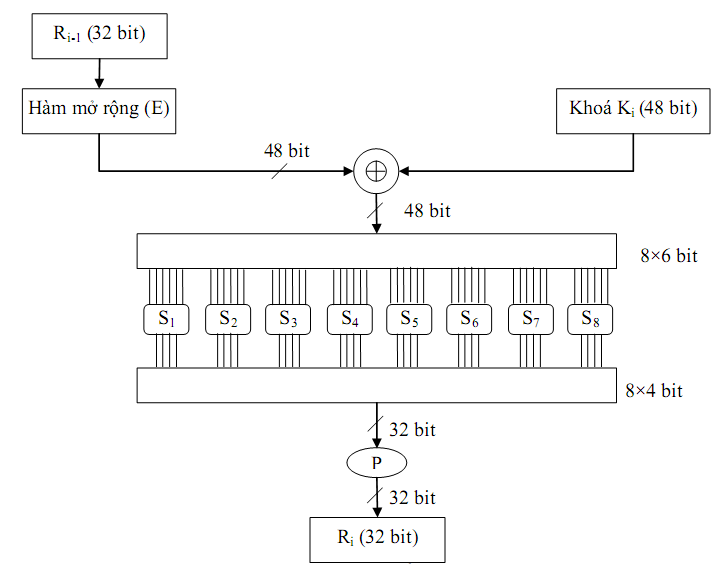
Đầu vào hàm f có 2 biến: biến 1: R là xâu bit có độ dài 32 bit, biến 2:K là xâu bit có độ dài 48 bit. Đầu ra của f là xâu bit có độ dài 32 bit.

- Biến thứ nhất Ri-1 được mở rộng thành một xâu bit có độ dài 48 bit theo một hàm mở rộng cố đinh E. Thực chất hàm mở rộng E ( Ri-1) là một hoán vị có lặp trong đó lặp lại 16 bit của Ri-1

- Tính E ( Ri-1 ) ⊕ Ki và viết kết quả thành 8 xâu 6 bit B1B2B3B4B5B6B7B8

- Đưa khối 8 bit Bi vào 8 bảng S1, S2, … .S8 ( được gọi là các hộp S-Box). Mỗi hộp S-Box là một bảng 4\*16 cố định có các cột từ 0 đến 15 và các hàng từ 0 đến 3. Với mỗi xâu 6 bit Bi = b1b2b3b4b5b6, ta tính được Si (B i) như sau: hai bit b1b6  xác định hàng r trong trong hộp Si, bốn bit b2b3b4b5 xác định cột c trong hộp S­i. Khi đó, Si (Bi) sẽ xác định phần tử Ci=Si ( r,c), phần tử này viết dưới dạng nhị phân 4 bit. Như vậy, 8 khối 6 bit Bi ( 1 ≤ i ≤ 8 ) sẽ cho ra 8 khối 4 bit Ci với ( 1 ≤ i ≤ 8 )

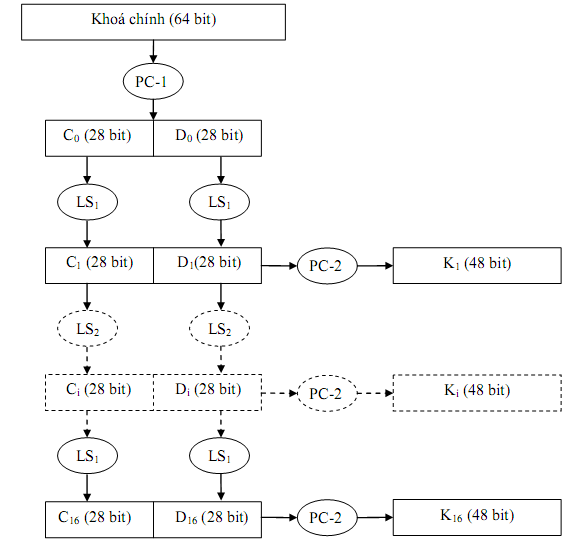
- Xâu bit C = C1C2C3C4C5C6C7C8 có độ dài 32 bit được hoán vị theo phép toán hoán vị P (hộp P-Box). Kết quả P(C) sẽ là kết quả của hàm f( Ri-1, K­i), và cũng chính Ri cho vòng sau



Ảnh .: Sơ đồ hàm F

### Quá trình tạo khóa con

- Mười sáu vòng lặp DES chạy cùng thuật toán như nhau nhưng với 16 khóa con khác nhau. Các khóa con đều được sinh ra từ khóa chính của DES bằng một thuật toán sinh khóa con.



Ảnh .: Sơ đồ tạo khóa con

K là xâu có độ dài 64 bit, một bit trong 8 bit của byte sẽ được lấy ra dùng để kiểm tra phát hiện lỗi( thường thì các bit này ở vị trí 8, 16, 24, ...,64) tạo ra chuỗi 56 bit. Sau khi bỏ các bit kiểm tra ta sẽ hoán vị chuối 56 bit, 2 bước trên được thực hiện thông qua hoá vị ma trận PC-1.

**Bảng trật tự khóa PC-1:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 | 58 | 50 | 42 | 34 | 26 | 18 |
| 10 | 2 | 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 | 60 | 52 | 44 | 36 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 | 62 | 54 | 46 | 38 | 30 | 22 |
| 14 | 6 | 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 | 28 | 20 | 12 | 4 |

Bảng .: Hoán vị PC-1

Ta chia PC-1 thành 2 phần:

C0: 28 bit đầu

D0: 28 bit cuối

Mỗi phần sẽ được xử lý 1 cách độc lập.

Ci=LSi(Ci-1)  
Di = LSi(Ci-1) với 1≤ i ≤ 16

+ LSi biểu diễn phép dịch bit vòng(cyclic shift) sang trái 1 hoặc 2 vị trí tuỳ thuộc vào i. Cyclic shift sang trái 1 bit nếu i=1, 2 , 9, 16 hoặc sang trái 2 bit nếu i thuộc các vị trí còn lại.

Ki=PC-2(CiDi).

+ Số bit dịch của các vòng:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Vòng lặp** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| **Số lần dịch trái** | 1 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 1 |

Bảng .: Bảng dịch bit tại các vòng lặp của DES

+ PC-2 là hoán vị cố định sẽ hoán vị chuỗi CiDi 56 bit thành chuỗi 48 bit.

**Bảng trật tự nén PC-2:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 14 | 17 | 11 | 24 | 1 | 5 | 3 | 28 | 15 | 6 | 21 | 10 |
| 23 | 19 | 12 | 4 | 26 | 8 | 16 | 7 | 27 | 20 | 13 | 2 |
| 41 | 52 | 31 | 37 | 47 | 55 | 30 | 40 | 51 | 45 | 33 | 48 |
| 44 | 49 | 39 | 56 | 34 | 53 | 46 | 42 | 50 | 36 | 29 | 32 |

Bảng .: Hoán vị PC-2

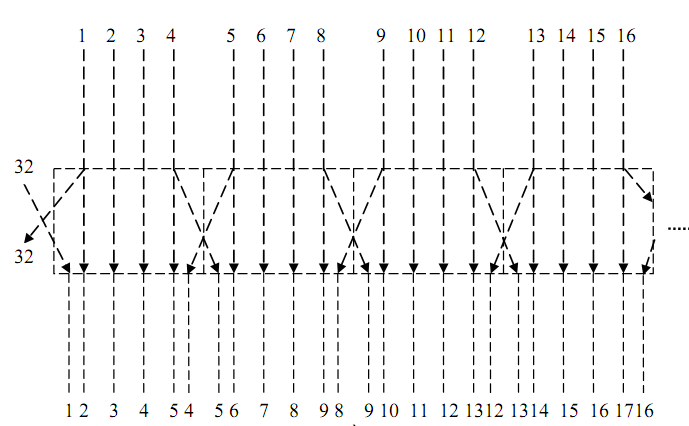
### Hàm (ánh xạ) mở rộng (E)

Hàm mở rộng (E) sẽ tăng độ dài từ Ri từ 32 bit lên 48 bit bằng cách thay đổi các thứ tự của các bit cũng như lặp lại các bit. Việc thực hiện này nhằm hai mục đích:

- Làm độ dài của Ri cùng cỡ với khóa K để thực hiện việc cộng modulo XOR.

- Cho kết quả dài hơn để có thể được nén trong suốt quá trình thay thế

Tuy nhiên, cả hai mục đích này nhằm một mục tiêu chính là bảo mật dữ liệu. Bằng cách cho phép 1 bit có thể chèn vào hai vị trí thay thế, sự phụ thuộc của các bit đầu ra với các bit đầu vào sẽ trải rộng ra. DES được thiết kế với điều kiện là mỗi bit của bản mã phụ thuộc vào mỗi bit của bản rõ và khóa.



Ảnh .: Sơ đồ của hàm mở rộng

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Hàm mở rộng E** | | | | | |
| 32 | 1 | 2 | 3 | 4 | 5 |
| 4 | 5 | 6 | 7 | 8 | 9 |
| 8 | 9 | 10 | 11 | 12 | 13 |
| 12 | 13 | 14 | 15 | 16 | 17 |
| 16 | 17 | 18 | 19 | 20 | 21 |
| 20 | 21 | 22 | 23 | 24 | 25 |
| 24 | 25 | 26 | 27 | 28 | 29 |
| 28 | 29 | 30 | 31 | 32 | 1 |

Bảng .: Hàm mở rộng E

Đôi khi nó được gọi là hàm E-Box, mỗi 4 bit của khối vào, bit thứ nhất và bit thứ tư tương ứng với 2 bit của đầu ra, trong khi bit thứ hai và ba tương ứng với 1 bit ở đầu ra

### Hộp S – Box

- Mỗi hàng trong mỗi hộp S là hoán vị của các số nguyên từ 0 đến 15

- Không có hộp S nào là hàm Affine hay tuyến tính đối với các đầu vào của nó

- Sự thay đổi của một bit đầu vào sẽ dẫn đến sự thay đổi ít nhất hai bit đầu ra

- Đối với hộp S bất kỳ và với đầu vào x ( một xâu bit có độ dài bằng 6 bit) bất kỳ, thì S(x) và S (x ⊕ 001100) phải khác nhau ít nhất là 2 bit

Sau khi cộng modulo với khóa K, kết quả thu được chuỗi 48 bit chia làm 8 khối đưa vào 8 hộp S-Box. Mỗi hộp S-Box có 6 bit đầu vào và 4 bit đầu ra ( tổng bộ nhớ yêu cầu cho 8 hộp S-Box chuẩn DES là 256 bytes). Kết quả thu được là một chuỗi 32 bit tiếp tục vào hộp P-Box

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S1** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 14  0  4  15 | | 4  15  1  12 | | 13  7  14  8 | | 1  4  8  2 | | 2  14  13  4 | | 15  2  6  9 | | 11  13  2  1 | | 8  1  11  7 | | 3  10  15  5 | | 10  6  12  11 | | 6  12  9  3 | | 12  11  7  14 | | 5  9  3  10 | | 9  5  10  0 | | 0  3  5  6 | 7  8  0  13 | |
| **S2** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 15  3  0  13 | 1  13  14  8 | | 8  4  7  10 | | 14  7  11  1 | | 6  15  10  3 | | 11  2  4  15 | | 3  8  13  4 | | 4  14  1  2 | | 9  12  5  11 | | 7  0  8  6 | | 2  1  12  7 | | 13  10  6  12 | | 12  6  9  0 | | 0  9  3  5 | | 5  11  2  14 | | | 10  5  15  9 |
| **S3** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 10  13  13  1 | 0  7  6  10 | | 9  0  4  13 | | 14  9  9  0 | | 6  3  8  6 | | 3  4  15  9 | | 15  6  3  8 | | 5  10  0  7 | | 1  2  11  4 | | 13  8  1  15 | | 12  5  2  14 | | 7  14  12  3 | | 11  12  5  11 | | 4  11  10  5 | | 2  15  14  2 | | | 8  1  7  12 |
| **S4** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 7  13  10  3 | 13  8  6  15 | | 14  11  9  0 | | 3  5  0  6 | | 0  6  12  10 | | 6  15  11  1 | | 9  0  7  13 | | 10  3  13  8 | | 1  4  15  9 | | 2  7  1  4 | | 8  2  3  5 | | 5  12  14  11 | | 11  1  5  12 | | 12  10  2  7 | | 4  14  8  2 | | | 15  9  4  14 |
| **S5** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2  14  4  11 | 12  11  2  8 | | 4  2  1  12 | | 1  12  11  7 | | 7  4  10  0 | | 10  7  13  14 | | 11  13  7  2 | | 6  1  8  13 | | 8  5  15  6 | | 5  0  9  15 | | 3  15  12  0 | | 15  10  5  9 | | 13  3  6  10 | | 0  9  3  4 | | 14  8  0  5 | | | 9  6  14  3 |
| **S6** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 12  10  9  4 | 1  15  14  3 | | 10  4  15  2 | | 15  2  5  12 | | 9  7  2  9 | | 2  12  8  5 | | 6  9  12  15 | | 8  5  3  10 | | 0  6  7  11 | | 13  1  0  14 | | 3  13  4  1 | | 4  14  10  7 | | 14  0  1  6 | | 7  11  13  0 | | 5  3  11  8 | | | 11  8  6  13 |
| **S7** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4  13  1  6 | 11  0  4  11 | | 2  11  11  13 | | 14  7  13  8 | | 15  4  12  1 | | 0  9  3  4 | | 8  1  7  10 | | 13  10  14  7 | | 3  14  10  9 | | 12  3  15  5 | | 9  5  6  0 | | 7  12  8  15 | | 5  2  0  14 | | 10  15  5  2 | | 6  8  9  3 | | | 1  6  2  12 |
| **S8** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 13  1  7  2 | 2  15  11  1 | | 8  13  4  14 | | 4  8  1  7 | | 6  10  9  4 | | 15  3  12  10 | | 11  7  14  8 | | 1  4  2  13 | | 10  12  0  15 | | 9  5  6  12 | | 3  6  10  9 | | 14  11  13  0 | | 5  0  15  3 | | 0  14  3  5 | | 12  9  5  6 | | | 7  2  8  11 |

Bảng .: 8 hộp S-Box

### Hộp P-Box

Việc hoán vị này mang tính đơn ánh, nghĩa là một bit đầu vào sẽ cho một bit ở đầu ra, không bit nào được sử dụng 2 lần hay bị bỏ qua. Hộp P-Box thực chất chỉ là chức năng sắp xếp đơn thuần theo bảng sau:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 16 | 7 | 20 | 21 | 29 | 12 | 28 | 17 |
| 1 | 15 | 23 | 26 | 5 | 18 | 31 | 10 |
| 2 | 8 | 24 | 14 | 32 | 27 | 3 | 9 |
| 19 | 13 | 30 | 6 | 22 | 11 | 14 | 25 |

Bảng .: Bảng hoán vị P

## Lập mã DES

Đây là ví dụ về việc sử dụng DES. Giả sử ta mã hóa bản rõ sau trong dạng thập lục phân(Hexadecimal) *0123456789ABCDEF* sử dụng khóa thập lục phân *133457799BBCDFF1*

Khóa trong dạng nhị phân không có các bit kiểm tra sẽ là :

00010010011010010101101111001001101101111011011111111000.

Áp dụng IP , ta nhận được L0 và R0 (trong dạng nhị phân)

|  |  |  |
| --- | --- | --- |
| **L0**  **L1 = R0** | **=**  **=** | **11001100000000001100110011111111**  **11110000101010101111000010101010** |

16 vòng lặp mã được thể hiện như sau:

|  |  |  |
| --- | --- | --- |
| **E(R0)**  **K1**  **E(R0) ⊕ K1**  **S-box output**  **f(R0,K1)**  **L2 = R1** | **=**  **=**  **=**  **=**  **=**  **=** | **011110100001010101010101011110100001010101010101**  **000110110000001011101111111111000111000001110010**  **011000010001011110111010100001100110010100100111**  **01011100100000101011010110010111**  **00100011010010101010100110111011**  **11101111010010100110010101000100** |

|  |  |  |
| --- | --- | --- |
| **E(R1)**  **K2**  **E(R1) ⊕ K2**  **S-box output**  **f(R1, K2)**  **L3 = R2** | **=**  **=**  **=**  **=**  **=**  **=** | **011101011110101001010100001100001010101000001001**  **011110011010111011011001110110111100100111100101**  **000011000100010010001101111010110110001111101100**  **11111000110100000011101010101110**  **00111100101010111000011110100011**  **11001100000000010111011100001001** |

|  |  |  |
| --- | --- | --- |
| **E(R2)**  **K3**  **E(R2) ⊕ K3**  **S-box output**  **f(R2, K3)**  **L4 = R3** | **=**  **=**  **=**  **=**  **=**  **=** | **111001011000000000000010101110101110100001010011**  **010101011111110010001010010000101100111110011001**  **101100000111110010001000111110000010011111001010**  **00100111000100001110000101101111**  **01001101000101100110111010110000**  **10100010010111000000101111110100** |

|  |  |  |
| --- | --- | --- |
| **E(R3)**  **K4**  **E(R3) ⊕ K4**  **S-box output**  **f(R3, K4)**  **L5 = R4** | **=**  **=**  **=**  **=**  **=**  **=** | **010100000100001011111000000001010111111110101001**  **011100101010110111010110110110110011010100011101**  **001000101110111100101110110111100100101010110100**  **00100001111011011001111100111010**  **10111011001000110111011101001100**  **011101110** |

|  |  |  |
| --- | --- | --- |
| **E(R4)**  **K5**  **E(R4) ⊕ K5**  **S-box output**  **f(R4, K5)**  **L6 = R5** | **=**  **=**  **=**  **=**  **=**  **=** | **101110101110100100000100000000000000001000001010**  **011111001110110000000111111010110101001110101000**  **110001100000010100000011111010110101000110100010**  **01010000110010000011000111101011**  **00101000000100111010110111000011**  **10001010010011111010011000110111** |
| **E(R5)**  **K6**  **E(R5) ⊕ K6**  **S-box output**  **f(R5, K6)**  **L7 = R6** | **=**  **=**  **=**  **=**  **=**  **=** | **110001010100001001011111110100001100000110101111**  **011000111010010100111110010100000111101100101111**  **101001101110011101100001100000001011101010000000**  **01000001111100110100110000111101**  **10011110010001011100110100101100**  **11101001011001111100110101101001** |

|  |  |  |
| --- | --- | --- |
| **E(R6)**  **K7**  **E(R6) ⊕ K7**  **S-box output**  **f(R6, K7)**  **L8 = R7** | **=**  **=**  **=**  **=**  **=**  **=** | **111101010010101100001111111001011010101101010011**  **111011001000010010110111111101100001100010111100**  **000110011010111110111000000100111011001111101111**  **00010000011101010100000010101101**  **10001100000001010001110000100111**  **00000110010010101011101000010000** |

|  |  |  |
| --- | --- | --- |
| **E(R7)**  **K8**  **E(R7) ⊕ K8**  **S-box output**  **f(R7, K8)**  **L9 = R8** | **=**  **=**  **=**  **=**  **=**  **=** | **000000001100001001010101010111110100000010100000**  **111101111000101000111010110000010011101111111011**  **111101110100100001101111100111100111101101011011**  **01101100000110000111110010101110**  **00111100000011101000011011111001**  **11010101011010010100101110010000** |

|  |  |  |
| --- | --- | --- |
| **E(R8)**  **K9**  **E(R8) ⊕ K9**  **S-box output**  **f(R8, K9)**  **L10 = R9** | **=**  **=**  **=**  **=**  **=**  **=** | **011010101010101101010010101001010111110010100001**  **111000001101101111101011111011011110011110000001**  **100010100111000010111001010010001001101100100000**  **00010001000011000101011101110111**  **00100010001101100111110001101010**  **00100100011111001100011001111010** |

|  |  |  |
| --- | --- | --- |
| **E(R9)**  **K10**  **E(R9) ⊕ K10**  **S-box output**  **f(R9, K10)**  **L11 = R10** | **=**  **=**  **=**  **=**  **=**  **=** | **000100001000001111111001011000001100001111110100**  **101100011111001101000111101110100100011001001111**  **101000010111000010111110110110101000010110111011**  **11011010000001000101001001110101**  **01100010101111001001110000100010**  **10110111110101011101011110110010** |

|  |  |  |
| --- | --- | --- |
| **E(R10)**  **K11**  **E(R10) ⊕ K11**  **S-box output**  **f(R10, K11)**  **L12 = R11** | **=**  **=**  **=**  **=**  **=**  **=** | **010110101111111010101011111010101111110110100101**  **001000010101111111010011110111101101001110000110**  **011110111010000101111000001101000010111000100011**  **01110011000001011101000100000001**  **11100001000001001111101000000010**  **11000101011110000011110001111000** |

|  |  |  |
| --- | --- | --- |
| **E(R11)**  **K12**  **E(R11) ⊕ K12**  **S-box output**  **f(R11, K12)**  **L13 = R12** |  | **011000001010101111110000000111111000001111110001**  **011101010111000111110101100101000110011111101001**  **000101011101101000000101100010111110010000011000**  **01111011100010110010011000110101**  **11000010011010001100111111101010**  **01110101101111010001100001011000** |

|  |  |  |
| --- | --- | --- |
| **E(R12)**  **K13**  **E(R12)⊕ K13**  **S-box output**  **f(R12, K13)**  **L14 = R13** | **=**  **=**  **=**  **=**  **=**  **=** | **001110101011110111111010100011110000001011110000**  **100101111100010111010001111110101011101001000001**  **101011010111100000101011011101011011100010110001**  **10011010110100011000101101001111**  **11011101101110110010100100100010**  **00011000110000110001010101011010** |

|  |  |  |
| --- | --- | --- |
| **E(R13)**  **K14**  **E(R13)⊕ K14**  **S-box output**  **f(R13, K14)**  **L15 = R14** | **=**  **=**  **=**  **=**  **=**  **=** | **000011110001011000000110100010101010101011110100**  **010111110100001110110111111100101110011100111010**  **010100000101010110110001011110000100110111001110**  **01100100011110011001101011110001**  **10110111001100011000111001010101**  **11000010100011001001011000001101** |

|  |  |  |
| --- | --- | --- |
| **E(R14)**  **K15**  **E(R14)⊕ K15**  **S-box output**  **f(R14, K15)**  **L16 = R15** | **=**  **=**  **=**  **=**  **=**  **=** | **111000000101010001011001010010101100000001011011**  **101111111001000110001101001111010011111100001010**  **010111111100010111010100011101111111111101010001**  **10110010111010001000110100111100**  **01011011100000010010011101101110**  **01000011010000100011001000110100** |

|  |  |  |
| --- | --- | --- |
| **E(R15)**  **K16**  **E(R15)⊕ K16**  **S-box output**  **f(R15, K16)**  **R16** | **=**  **=**  **=**  **=**  **=**  **=** | **001000000110101000000100000110100100000110101000**  **110010110011110110001011000011100001011111110101**  **111010110101011110001111000101000101011001011101**  **10100111100000110010010000101001**  **11001000110000000100111110011000**  **00001010010011001101100110010101** |

Cuối cùng , áp dụng IP-1 cho ta nhận được bản mã trong dạng thập lục phân như sau :

*85E813540F0AB405*

## Một vài kết luận về DES

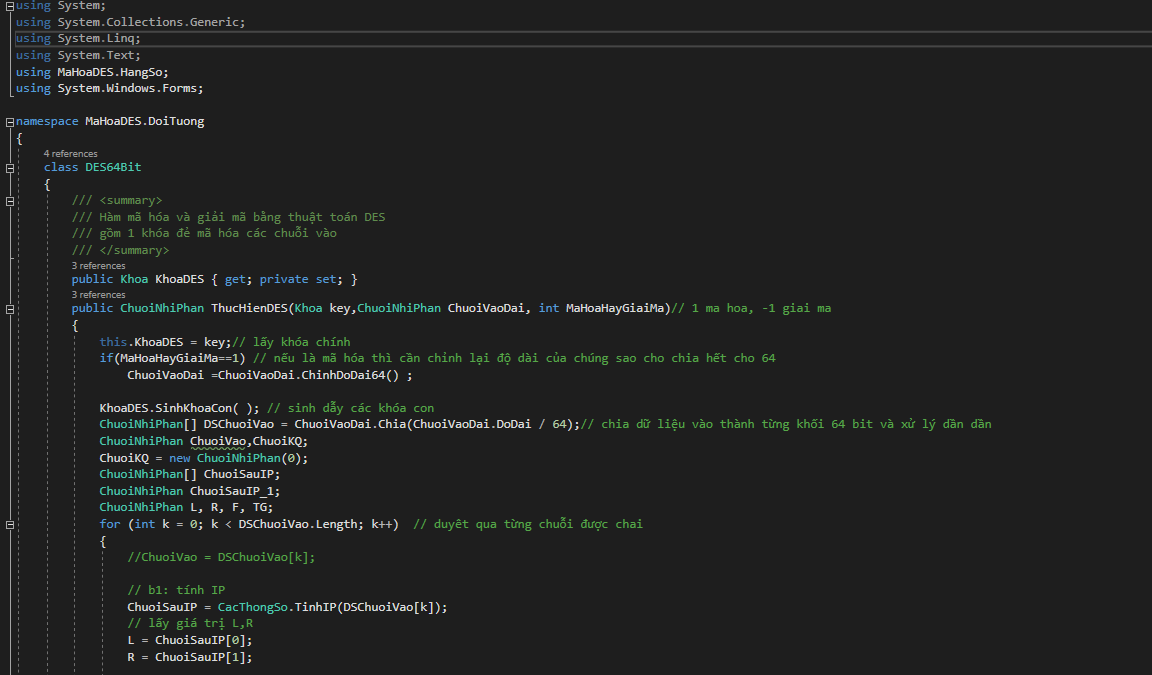
Ngay cả khi việc mô tả DES khá dài dòng thì DES được thực hiện rất hiệu quả trong cả phần cứng lẫn phần mền. Những tính toán số học duy nhất được thực hiện là phép XOR của các chuỗi bit. Việc mở rộng hàm E các hộp S, sự hoán vị IP và P, và việc tính toán k1, k2,…, k16 tất cả được thực hiện trong thời gian ngắn bởi bảng tìm kiếm trong phần mền hoặc cách nối dây cứng chúng vào môt mạch.

DES thường được dùng để mã hoá bảo mật các thông tin trong quá trình truyền tin cũng như lưu trữ thông tin. Một ứng dụng quan trọng khác của DES là kiểm tra tính xác thực của mật khẩu truy nhập vào một hệ thống (hệ thống quản lý bán hàng, quản lý thiết bị viễn thông…), hay tạo và kiểm tính hợp lệ của một mã số bí mật (thẻ internet, thẻ điện thoại di động trả trước), hoặc của một thẻ thông minh (thẻ tín dụng, thẻ payphone…).

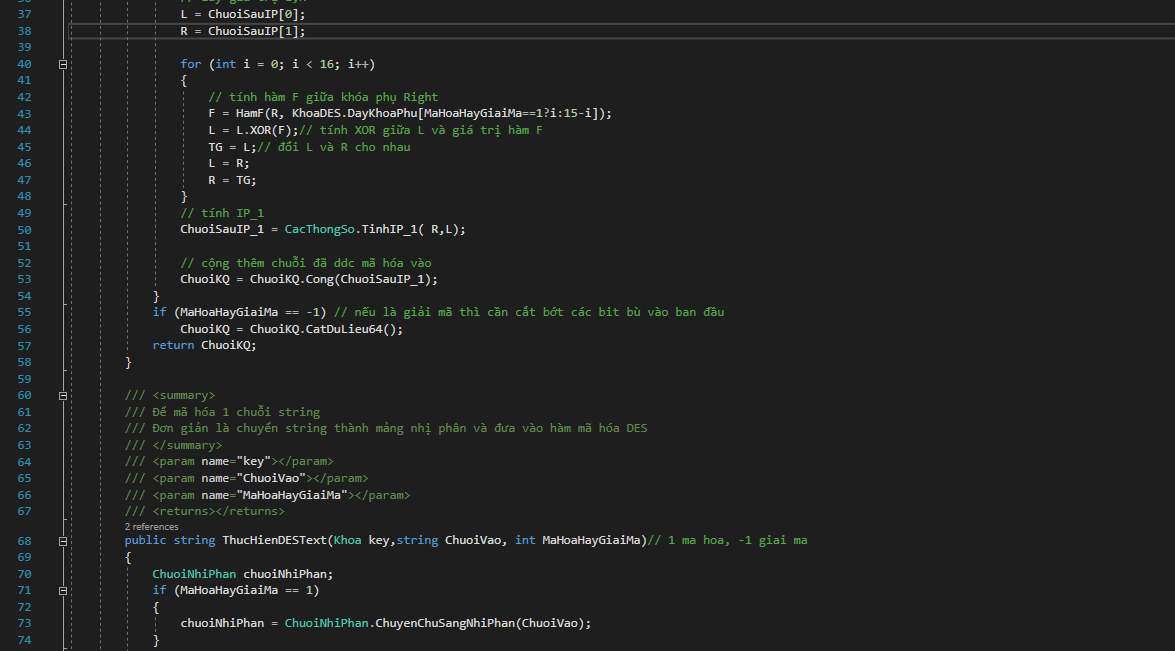
Để tăng độ an toàn, trong thực tế các hệ thống mã hóa sử dụng mã hóa DES mở rộng (3DES – TripleDES). Triple-DES chính là DES với hai chìa khoá 56 bit. Cho một bản tin cần mã hoá, chìa khoá đầu tiên được dùng để mã hoá DES bản tin đó, kết quả thu được lạI được cho qua quá trình giải mã DES nhưng với chìa khoá là chìa khoá thứ hai, bản tin sau qua đã được biến đổi bằng thuật toán DES hai lần như vậy lại được mã hoá DES với một lần nữa với chìa khoá đầu tiên để ra được bản tin mã hoá cuối cùng. Quá trình mã hoá DES ba bước này được gọi là Triple-DES.

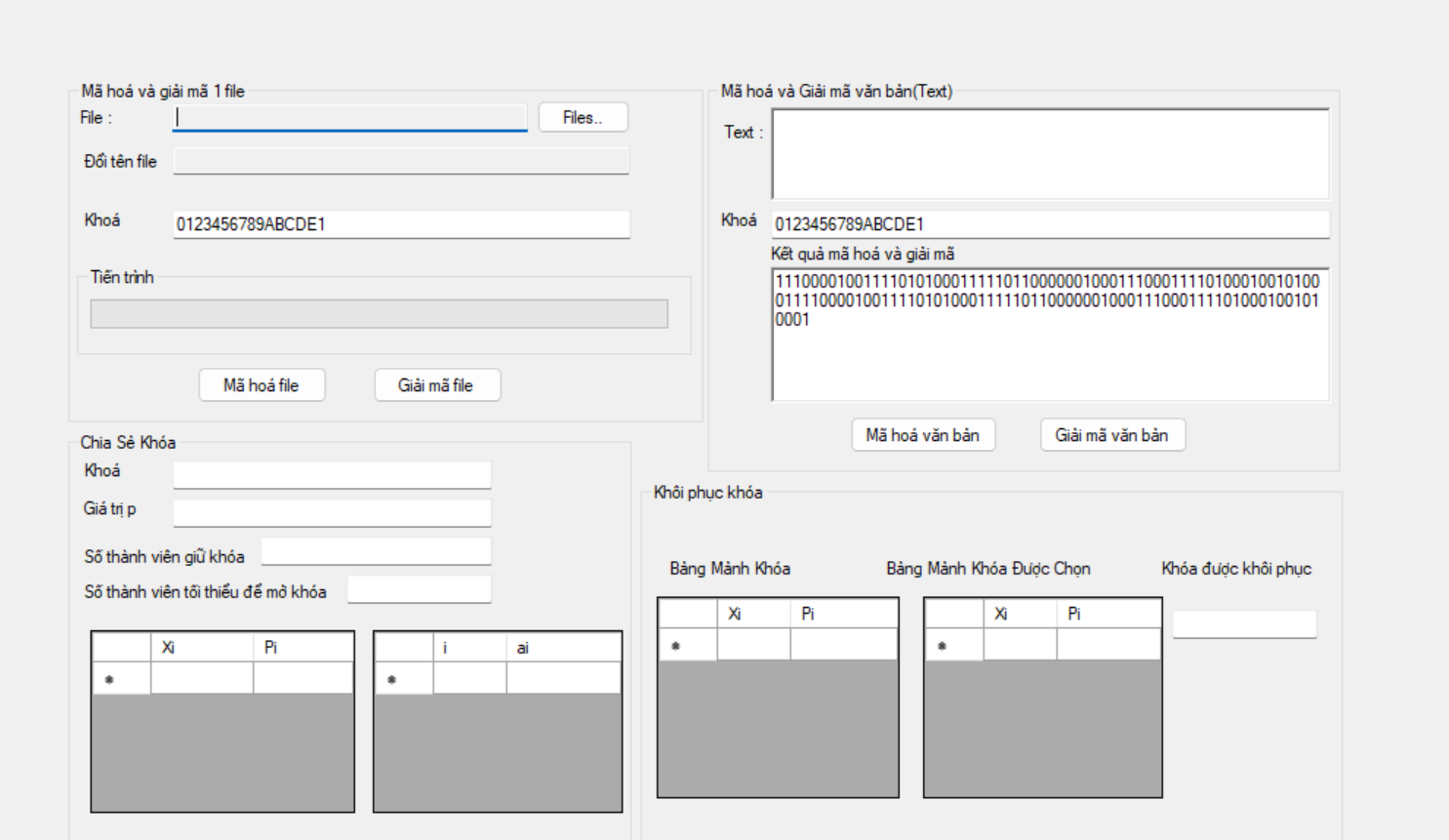
Hiện nay DES được xem là không đủ an toàn cho nhiều ứng dụng. Nguyên nhân chủ yếu là độ dài 56 bit của khóa là quá nhỏ. Khóa DES đã từng bị phá trong vòng chưa đầy 24 giờ. Đã có rất nhiều kết quả phân tích cho thấy những điểm yếu về mặt lý thuyết của mã hóa có thể dẫn đến phá khóa. Nâng cao hơn là TripleDES trên lý thuyết phương pháp này vẫn có thể bị phá. Gần đây DES đã được thay thế bằng AES (Advanced Encryption Standard, hay Tiêu chuẩn Mã hóa Tiên tiến).

## Chương trình demo (C#)



*Hàm Mã Hóa/Giải Mã*





*Giao diện chương trình*

# Bài toán chia sẻ bí mật

## Kỹ thuật Chia sẻ khóa bí mật (Secret Sharing) (Phạm Văn Đạt)

### Khái niệm về chia sẻ bí mật

Sơ đồ chia sẻ bí mật không phải là một lĩnh vực mới mẻ của an toàn bảo mật thông tin, nhưng hứa hẹn sẽ mang đến nhứng ứng dụng rộng khắp: khóa mã hóa , mã phóng tên lửa và số tài khoản ngân hàng, …

Sơ đồ chia sẻ bí mật chính là phương thức dùng đề chia một bí mật ra làm nhiều phần riêng biệt sau đó phân phối tới những người tham gia. Trong đó chỉ với số người được chỉ định trước mới có khả năng khôi phục bí mật bằng cách gộp những phần thông tin của họ, những người không được chỉ định sẽ không thu được bất kỳ thông tin gì về bí mật.

*Ý tưởng:* thông tin quan trọng cần bí mật, không nên trao cho một người nắm giữ, mà phải chia thông tin đó thành nhiều mảnh và trao cho mỗi người một hay một số mảnh. Thông tin gốc chỉ có thể được xem lại, khi mọi người giữ các mảnh thông tin đều nhất trí. Các mảnh thông tin được khớp lại để được thông gốc.

|  |  |
| --- | --- |
| - Thông tin cần giữ bí mật được chia thành nhiều mảnh: | |
| Thông tin bí mật | Các mảnh được chia sẻ |
| - Khi các mảnh được khớp lại sẽ cho ta thông tin ban đầu: | |
| Các mảnh cần để ghép lại thông tin | Thông tin bí mật được khôi phục |

*Yêu cầu:* để thực hiện công việc trên, phải sử dụng một sơ đồ gọi là Sơ đồ chia sẻ bí mật.

*Khái niệm chia sẻ bí mật:* Sơ đồ chia sẻ bí mật dùng để chia sẻ một thông tin cho m thành viên, sao cho chỉ những tập con hợp thức các thành viên mới có thể khôi phục lại thông tin bí mật, còn lại không ai có thể làm được điều đó.

*Ứng dụng:*

* Chia sẻ thông tin mật thành nhiều mảnh.
* Chia sẻ Passwod, khóa mật thành nhiều mảnh. Mỗi nơi, mỗi người hay mỗi máy tính cất giấu 1 mảnh.

*Các thành phần của sơ đồ chia sẻ bí mật:*

* Người phân phối bí mật (Dealer): Là người trực tiếp chia bí mật thành nhiều phần.
* Những người tham gia nhận dữ liệu từ Dealer (Participant), ký hiệu P.
* Nhóm có khả năng khôi phục bí mật (Acess structure): Là tập con của P trong đó có các tập con có khả năng khôi phục bí mật.

Ví dụ:Chìa khóa để mở két bạc là chìa khóa số được chủ két bạc D chia thành 3 mảnh khóa, có 3 thủ quỹ là P1, P2, P3. Mỗi thủ quỹ giữ một mảnh khóa. Chỉ có thủ quỹ P1 và P2 hoặc P2 và P3 hoặc P1 và P3 khi khớp 2 mảnh khóa của họ với nhau thì sẽ nhận được chìa khóa gốc để mở két bạc. Các tập con hợp thúc là các tập con có thể mở khóa: { P1, P2 }, { P2, P3}, {P1, P3}.

### Các sơ đồ chia sẻ bí mật

#### Sơ đồ chia sẻ bí mật sơ khai

Một sơ đồ chia sẻ bí mật đảm bảo tính bảo mật là sơ đồ trong đó bất kỳ người nào có ít hơn t phần dữ liệu (là số lượng đủ để khôi phục bí mật) không có nhiều thông tin hơn một người không có dữ liệu.

Xem xét sơ đồ chia sẻ bí mật sơ khai trong đó cụm từ bí mật “password” được chia thành các phần “pa­­­\_\_\_”, “\_ss\_\_\_”, “\_\_\_wo\_” và “\_\_\_\_rd”. Một người không có một trong các phần bí mật đó chỉ biết mật khẩu có 8 chữ cái. Người đó sẽ phải đoán mật khẩu đó từ 268 = 208 tỷ khả năng có thể xảy ra. Một người có một phần trong số 4 phần của mật khẩu đó sẽ phải đoán 6 chữ cái tương đương với 266 = 308 tỷ khả năng. Hệ thống này không phải là một sơ đồ chia sẻ bí mật an toàn bởi vì một người tham gia có ít hơn t phần dữ liệu thu được một phần đáng kể thông tin về bí mật. Trong một sơ đồ chia sẻ bí mật an toàn, mặc dù một người tham gia chỉ thiếu một phần dữ liệu cũng có thể sẽ đối mặt với 268 = 208 tỷ khả năng.

#### Sơ đồ chia sẻ bí mật của Shamir

Ý tưởng về sơ đồ ngưỡng giới hạn của Shamir dựa trên tính chất: Hai điểm có thể định nghĩa một đường thẳng, 3 điểm định nghĩa được 1 parabol, 4 điểm định nghĩa được một hình lập phương, cứ như thế một cách tổng quát cần n+1 điểm để định nghĩa một đa thức bậc n.

***Bài toán***:

Cho t, m là các số nguyên dương, t ≤ m. Một sơ đồ ngưỡng A(t, m) là một phương pháp phân chia khóa K cho một tập w thành viên (kí hiệu là P) sao cho t thành viên bất kì có thể tính được K nhưng không một nhóm (t-1) thành viên nào có thể làm được điều đó.

*Ví dụ* : có m = 3 thủ quỹ giữ két bạc. Hãy xây dựng hệ thống sao cho bất kì t = 2 thủ quỹ nào cũng có thể mở được két bạc, nhưng từng người một riêng rẽ thì không thể. Đó là sơ đồ ngưỡng A(2,3).

Giá trị K được chọn bởi một thành viên đặc biệt được gọi là người phân phối (D), D∉P.

D phân chia khóa K cho mỗi thành viên trong P bằng cách cho mỗi thành viên một thông tin cục bộ gọi là mảnh. Các mảnh được phân phát một cách bí mật để không thành viên nào biết được mảnh được trao cho các thành viên khác.

Một tập con các thành viên B P sẽ kết hợp các mảnh của họ để tính khóa K (cũng có thể trao các mảnh của mình cho một người đáng tin cậy để tính khóa hộ).

Nếu |B| ≥ t thì họ có khả năng tính được K.

Nếu |B| < t thì hị không thể tính được K.

Gọi P là tập các giá trị được phân phối khóa K: P = {pi : 1 ≤ i ≤ m}

K là tập khóa: tất cả các khóa K có thể

S tập mảnh: tập tất cả các mảnh có thể

* ***Khởi tạo:*** Chọn số nguyên tố p
  1. D chọn phần tử khác nhau, ≠ 0 trong Zp, (yêu cầu: , Tl: khác nhau, ≠ 0 trong Zp). D trao cho thành viên *Pi*. Giá trị là công khai.
* ***Phân phối mảnh khóa***

1. D chọn bí mật (ngẫu nhiên, độc lập) (*t – 1*) phần tử Zp là *a1, …, at* – 1.
2. Với *1 ≤ i ≤ m*, D tính: *yi = P(xi),*
3. Với *1 ≤ i ≤ m*, D sẽ trao mảnh *yi* cho *Pi*.

* ***Khôi phục khóa K từ t thành viên***

Giải hệ phương trình tuyến tính t ẩn, t phương trình

Vì *P(x) = K + a1 x1 + a2 x2 + …+ at-1 xt-1*

Các hệ số *K, a1, …, at-1* là các phần tử chưa biết của Zp, *a0 = K* là khóa.

Vì *yi j = P(xi j)*, nên ta có thể thu được t phương trình tuyến tính t ẩn *a0, a1, …, at-1*,

Nếu các phương trình độc lập tuyến tính thì sẽ có một nghiệm duy nhất và ta được giá trị khoá *a0 = K*.

#### Chia sẻ bí mật dựa trên ý tưởng của Lagrange

Giả sử ta có n thực thể A1,A2,…,An và có 1 người được ủy quyền B biết được toàn bộ khóa bí mật S N.

***Người được ủy quyền B thực hiện các bước sau:***

1. B chọn một số nguyên tố P đủ lớn sao cho: với
2. B tiếp theo chọn (2n – 1) số một cách ngẫu nhiên:
3. B xác định một đa thức với các hệ số *a1, …, at-1* trên :
4. Bây giờ B gửi Aj (một cách công khai) cặp coi như mảnh riêng của Aj.

***Khôi phục bí mật S:***

Tất cả n người A1, …, An có thể hợp tác lại để khôi phục lại bí mật S bằng cách:

Khi đó dễ dàng xác định được *S = g(0) (x = 0)*

Ta có định lý như sau:

Nếu n thực thể kết hợp với nhau thì có thể khôi phục bí mật S một cách có hiệu quả đó là: S = g(0) = f(0)

***Chứng minh:***

Thật vậy ,dễ thấy rằng g(x) là hàm nội suy Lagrange của hàm f(x) là một đa thức có cấp bé hơn n và g thỏa mãn điều kiện:g(vj)=f(vj) với 0 ≤ j < n.

Do đó, f – g là đa thức trên Zp có cấp bé hơn n, nhưng nó lại có ít nhất là n nghiệm khác nhau: là các số r thỏa mãn f(r) – g(r) = 0. Chứng tỏ rằng f(a) = g(a) với đặc biệt f(0) = g(0) = S. (ĐPCM)

*Ví dụ:*

*Ví dụ 1:* Có 3 người A1, A2, A3 muốn chia sẻ bí mật 472. Cho p = 1999 công khai. A chọn v1 = 626, v2 = 674, v3 = 93; a1 = 334, a2 = 223.

Tính

Áp dụng công thức trên ta có:

Ta lấy 3 cặp hợp lại sẽ xác định được S:

Áp dụng công thức ta được:

b0 = 1847

b1 = 793

b2 = 1359

*Ví dụ 2*:

Cho số nguyên tố p=342853815608923 (Đây là 1 số nguyên tố được lấy trong bảng các số nguyên tố từ cuốn “The Art of Programing” của Knut(Vol 2). Cho n=3, ta có: a1 =53958111706386; a2 =151595058245452;

v1 =111350135012507; v2 =207244959855905; v3 =20545949133543;

Giải sử bí mật là S = 151595058245452

Tính

Áp dụng công thức trên ta có:

Ta lấy 3 cặp hợp lại sẽ xác định được S:

Áp dụng công thức ta được:

b1 = 266921901220910

b2 = 129147516050688

b3 = 289638215946249

## Ứng dụng lược đồ chia sẻ bí mật của Lagrange để phân phối khóa

Như đã trình bày ở Chương 1: để bảo vệ thông tin của mình khi gửi cho người nhận người gửi thường chọn cách mã hóa thông tin bằng nhiều phương pháp khác nhau có thể phân loại ra thành Hệ mật mã khóa bia mật và Hệ mật mã khóa công khai. Trong cả 2 hệ mật mã này thì việc giữ bí mậy khóa mã hóa (cryptographic keys) là đặc biệt quan trọng. Khác với Hệ mã khóa công khai có thể dễ dàng chia sẻ khóa *publish key* giữa bên gửi và nhận thông tin thì Hệ mã khóa bí mật phải đặc biệt bảo mật khóa mã hóa vì nó quyết định cả quá trình mã hóa và giải mã.

Vậy làm thế nào để người gửi chia sẻ khóa mã hóa của hệ mã khóa bí mật cho người nhận có thể giải mã và đọc thông tin đã được gửi?

Phương pháp: Chúng ta sẽ sử dụng lược đồ chia sẻ bí mật để chia sẻ khóa thành nhiều mảnh để truyền đi trong các nút không dáng tin cậy. Khi nhận được các mảnh của chìa khóa người dùng sẽ ghép lại thành khóa hoàn chỉnh và có thể giải mã được thông tin. Vì mỗi mảnh khóa đều không thể suy ra khóa đã chia sẻ nên việc chia sẻ khóa sẽ là an toàn.

***Áp dụng bài toán: Phân phối khóa hệ mã DES***

Hệ mã DES với khóa 64 bit (trong đó chỉ có 56 bit được sử dụng để mã hóa và giải mã, 8 bit còn lại chỉ dùng cho việc kiểm tra) tương đương với 16 số hệ Hexa hay một số nguyên gồm 20 số thập phân. Con số bí mật này không quá lớn đối với bài toán chia sẻ bí mật nên việc tính toán là rất hiệu quả.

Để phân phối khóa của DES cho người nhận, ta sẽ lấy khóa gồm 20 số thập phân chia nhỏ thành chia nhỏ thành các cặp bằng sơ đồ chia sẻ bí mật của Lagrange. Sau đó, người nhận sau khi nhận được bản mã hóa và các mảnh sẽ khôi phục lại khóa để có thể giải mã.

Graphical user interface

Description automatically generated

Ảnh .: DES và quá trình phân phối khóa

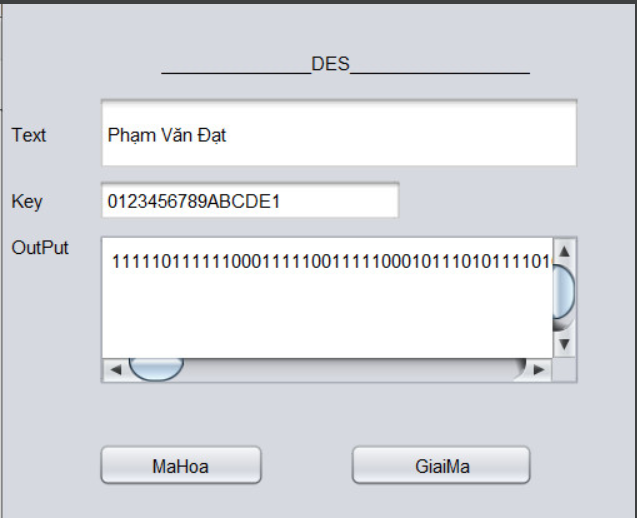
## Kết luận

Như vậy, Sơ đồ chia sẻ bí mật là một cách thức để chia sẻ các thông tin quan trọng (password, khóa mã hóa) được sử dụng trong thực tế như:

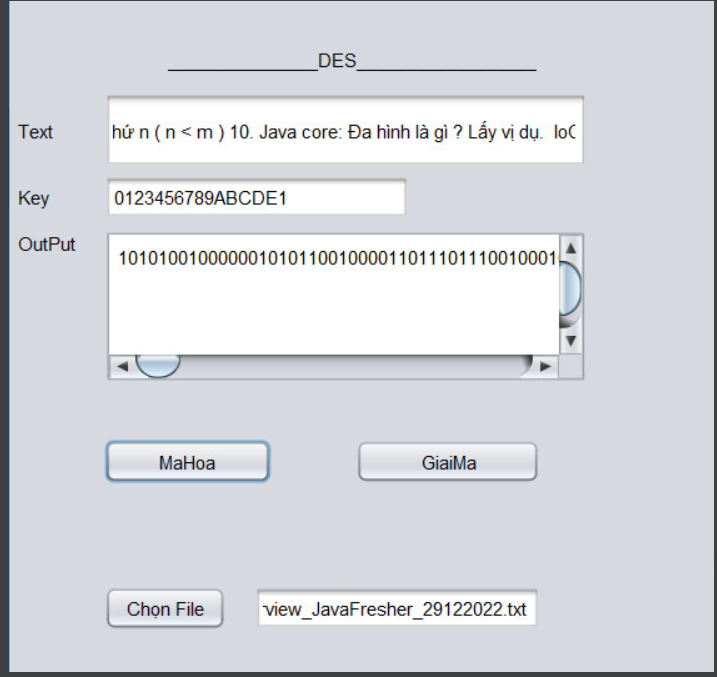
* Trong việc giữ khóa két bạc: Không nên trao khoá két bạc cho một người duy nhất. Khoá phải được chia nhỏ thành nhiều mảnh và trao cho mỗi thành viên một mảnh.
* Trong bỏ phiếu điện tử: Không thể tin hoàn toàn vào tất cả các thành viên Ban kiểm phiếu. Vì vậy, lá phiếu nên chia thành nhiều mảnh và trao cho mỗi Kiểm phiếu viên một mảnh của lá phiếu.
* Trong lưu trữ các khóa bí mật: Khoá bí mật và quan trọng không nên lưu trữ tại một Server. Nó phải được chia nhỏ và lưu trữ tại nhiều máy trạm.
* Trong thi tuyển sinh: Trong một kỳ thi, nơi ra đề và nơi tổ chức thi cách xa nhau, ta phải thực hiện việc chuyển đề thi từ nơi ra đề tới nơi tổ chức thi trên mạng máy tính sao cho đảm bảo về tính bảo mật. (Bài toán này sẽ được miêu tả chi tiết ở chương sau của tài liệu này.)

Ngoài ra nó còn là một phần quan trọng trong bảo mật thông tin và cũng được dùng trong việc xác thực người dùng.

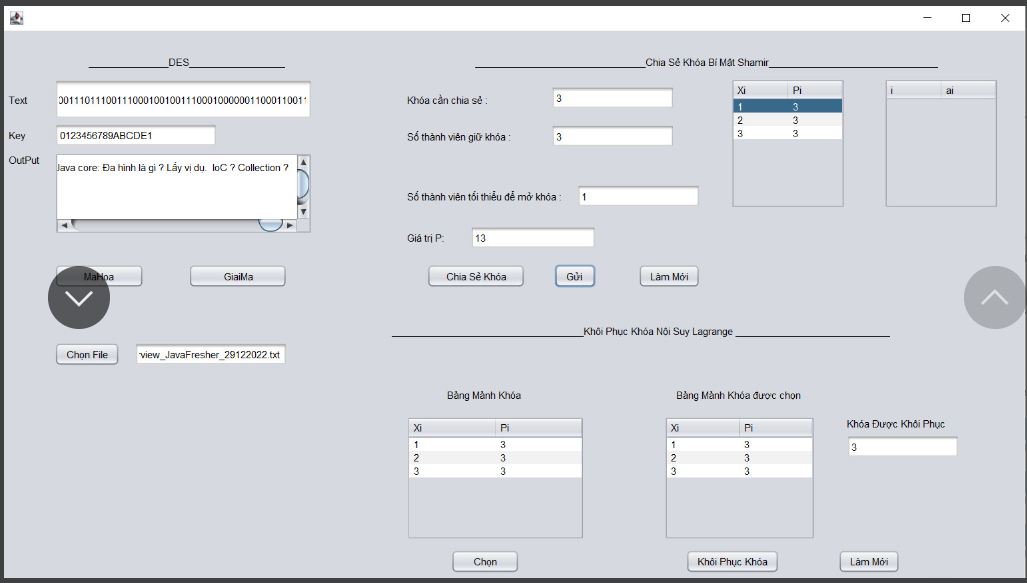
## Chương trình demo ( Java )



*Giao diện mã hóa / Giải Mã*

**

*Mã hóa / Giải mã File*

**

*Chia sẻ khóa*

# Kết quả nghiên cứu DES và lược đồ chia sẻ bí mật vào thi tuyển sinh

## Bài toán ứng dụng

Thuật toán mã hóa DES và sơ đồ chia sẻ bí mật được ứng dụng rất nhiều trong nhiều lĩnh vực khác nhau để đảm bảo an toàn thông tin khi trao đổi thông tin. Trong phần này ta nghiên cứu một ứng dụng trong việc chuyển đề thi tuyển sinh làm sao để giữ bí mật trước giờ phát đề cho thí sinh.

***- Bài toán:***

Trong một kỳ thi, nơi ra đề thi và nơi tổ chức thi ở cách xa nhau, ta phải thực hiện việc chuyển đề thi từ nơi ra đề tới nơi tổ chức trên mạng máy tính sao cho đảm bảo về tính bảo mật.

***- Ý tưởng giải quyết bài toán:***

Việc bảo mật đề thi là rất quan trọng, làm sao để vừa giao đề thi cho nơi tổ chức thi kịp thời mã vẫn không bị lộ đề thi trước giờ phát đề?

Để làm như vậy ta cần mã hóa đề thi (ở đây ta dùng thuật toán mã hóa DES với khóa mã hóa K) sau đó chuyển đề thi đã được mã hóa cho nơi tổ chức thi.

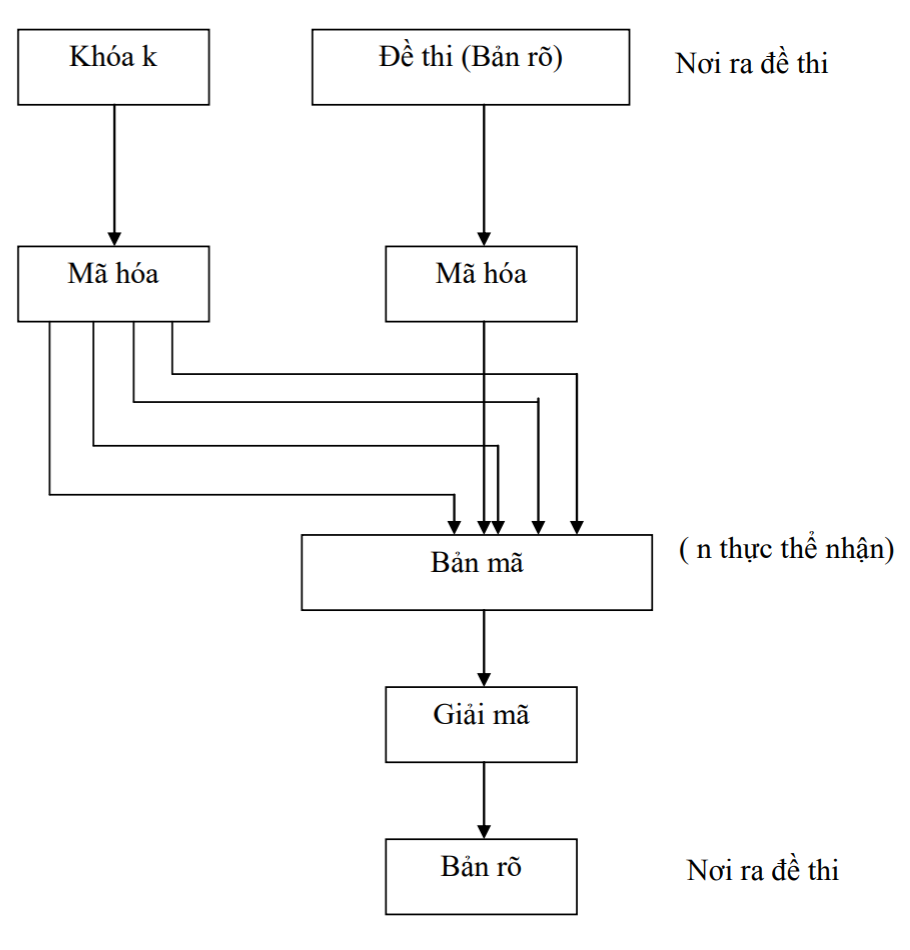
Về việc bảo mật khóa mã hóa: Dùng sơ đồ chia sẻ bí mật chia khóa K thành 2 khóa k1 và k2. Sau đó lần lượt gửi k1 và k2 cho nơi tổ chức. Nơi tổ chức sẽ dùng k1 và k2 để ghép lại khóa K sau đó tiến hành giải mã đề thi để được bản rõ ban đầu.

## Quy trình thực hiện giải bài toán

### Sơ đồ

Khóa DES gồm 56 bit, tương đương với một số nguyên gồm 20 chữ số thập phân. Con số bí mật nay không quá lớn đối với bài toán chia sẻ bí mật. Cho nên việc tính toán là rất hiệu quả.

Ứng dụng lược đồ chia sẻ bí mật của Lagrange để phân phối khóa đã được mô tả ở chương trước.



Ảnh .: Sơ đồ quy trình bảo mật đề thi gửi từ nơi ra đề đến nơi tổ chức thi

### Các bước thực hiện

Theo sơ đồ trên ta phải thực hiện theo các bước sau:

* Nơi ra đề thi:
  + Bản rõ (đề thi)
  + Mã hóa bản rõ
  + Tạo khóa k
  + Mã hóa khóa k
  + Gửi bản mã
* Nơi tổ chức thi:
  + Nhận bản mã và cặp (vj, f(vj))
  + Giải bản mã (sau khi nhận đủ các cặp khác từ người ra đề thi để xác định được khóa K).

*Mã hóa bản rõ (đề thi):* Bộ giáo dục dùng bảng mã ASCII mở rộng để chuyển bản rõ từ dạng kí tự sang Hexa sau đó dùng thuật toán DES để mã hóa.

*Tạo khóa k:* Dùng dãy kí tự dạng chữ hoặc dạng số, nhóm 8 kí tự thành 1 nhóm sau đó dùng 56 bit để mã hóa.

*Gửi bản tin:* Dựa vào lược đồ chia sẻ bí mật chia khóa k thành 2 mảnh rời nhau k1, k2 : k1 + k2 = k. Sau đó gửi k1 cho n thực thể (các địa chỉ thi). Quy định đến đúng giờ G vụ Đào tạo gửi nốt k2 cho n thực thể đó trên cơ sở k1, k2. Tất cả các nơi đều mở được đề và trao cho học sinh hoặc gửi cho học sinh thông qua máy tính để làm (qua mail đồng thời).

***Ví dụ:*** Tại nơi ra đề dùng khóa mã hóa là khóa K(64 bit) = ABCDEF0123456789HEX = 12379813738877118345DEC, lấy số nguyên tố p = 12764787846358441471 (theo https://primes.utm.edu/lists/small/small.html).

Sau khi dùng khóa K để mã hóa đề thi bằng thuật toán DES, Nơi ra đề sẽ thực hiện chia chìa khóa thành 2 phần (n=2) với:

v1 = 151595058245452 (tùy chọn)

v2 = 111350135012507 (tùy chọn)

a1 = 207244959855905 (tùy chọn)

- Quá trình tách khóa:

Tính

Áp dụng công thức trên ta có:

Sau đó cùng gửi đề thi đã mã hóa và *k1* cho các địa chỉ thi. Đến đúng giờ G vụ Đào tạo sẽ gửi nốt *k2* cho các điểm thi.

- Từ 2 cặp hợp lại sẽ xác định được K:

Áp dụng công thức ta được:

Từ đó ta tính được:

=> K = ABCDEF0123456789(HEX)

Khi đã có K, tai địa điểm thi sẽ có thể giải mã để mở được đề thi và tiến hành thi.

Như vậy, với thật toán DES và lược đồ chia sẻ bí mật có thể đảm bảo an toàn thông tin, không bị lộ đề thi, đảm bảo tính minh bạch của kỳ thi. Đây là một ứng dụng có hiệu quả cao trong thực tiễn.

## Thiết kế, cài đặt chương trình đề mô thuật toán

### Giao diện chương trình đề mô