**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI**

**PHÂN HIỆU TẠI THÀNH PHỐ HỒ CHÍ MINH**



**BÁO CÁO AN TOÀN BẢO MẬT THÔNG TIN**

**ĐỀ TÀI:**

**MÃ HÓA VÀ GIẢI MÃ VỚI THUẬT TOÁN DES**

Sinh viên thực hiện:

PHẠM HUỲNH HẢI YẾN - 5951071125

VÕ THỊ DIỆU THƯƠNG - 5951071105

LÊ THỊ TƯỜNG VI - 5951071119

Lớp: CQ.59.CNTT

Khoá: 59

TP. Hồ Chí Minh, năm 2021

**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI**

**PHÂN HIỆU TẠI THÀNH PHỐ HỒ CHÍ MINH**



**BÁO CÁO AN TOÀN BẢO MẬT THÔNG TIN**

**ĐỀ TÀI:**

**MÃ HÓA VÀ GIẢI MÃ VỚI THUẬT TOÁN DES**

Sinh viên thực hiện:

PHẠM HUỲNH HẢI YẾN - 5951071125

VÕ THỊ DIỆU THƯƠNG - 5951071105

LÊ THỊ TƯỜNG VI - 5951071119

Lớp: CQ.59.CNTT

Khoá: 59

TP. Hồ Chí Minh, năm 2021

**TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**

**PHÂN HIỆU TẠI THÀNH PHỐ HỒ CHÍ MINH Độc lập – Tự do – Hạnh phúc**

# **LỜI CẢM ƠN**

Lời đầu tiên em xin gửi lời cảm ơn chân thành đến quý thầy, cô giáo trong **Bộ**

**môn Công nghệ thông tin – Phân hiệu Trường Đại học Giao thông vận tải.**

Những người đã truyền dạy, đã trang bị cho em kho tàng kiến thức về bầu trời công

nghệ thông tin rộng lớn.

Ở đây, em không chỉ học được kiến thức về sách vở mà em còn học được các

bài học, kỷ năng sống trước khi tạm biệt mái trường đại học thân yêu này và tiến ra

biển đời mênh mông rộng lớn.

Trong quá trình học tập và tìm hiểu em đã nỗ lực rất nhiều với mong muốn hoàn

thành bài tập lớn một cách tốt nhất, nhưng sẽ không tránh khỏi những thiếu sót. Em mong thầy, cô có thể thông cảm và cho em những ý kiến, đóng góp để em có thể hoàn thành bài tập lớn của nhóm một cách trọn vẹn.

Sau cùng, em xin kính chúc Quý Thầy Cô lời chúc sức khoẻ, luôn hạnh phúc và thành công hơn nữa trong công việc cũng như trong cuộc sống.

Em xin chân thành cảm ơn!

# **NHẬN XÉT CỦA GIÁO VIÊN**

**Tp. Hồ Chí Minh, ngày … tháng 07 năm 2021**

**Giáo viên hướng dẫn**

**MỤC LỤC**

[**LỜI CẢM ƠN 3**](#_Toc76593972)

[**NHẬN XÉT CỦA GIÁO VIÊN 4**](#_Toc76593973)

[**MỤC LỤC 5**](#_Toc76593974)

[**DANH MỤC HÌNH ẢNH 6**](#_Toc76593975)

[**DANH MỤC BẢNG 7**](#_Toc76593976)

[**CHƯƠNG 1: MỞ ĐẦU 8**](#_Toc76593977)

[**1.1 Hướng tiếp cận của đề tài. 8**](#_Toc76593978)

[**1.2 Mục tiêu nghiên cứu. 8**](#_Toc76593979)

[**1.3 Phương pháp nghiên cứu. 8**](#_Toc76593980)

[**CHƯƠNG 2: GIỚI THIỆU 9**](#_Toc76593981)

[**2.1 An toàn bảo mật thông tin và mật mã học 9**](#_Toc76593982)

[2.1.1 Giới thiệu về an toàn bảo mật thông tin 9](#_Toc76593983)

[2.1.2 Mật mã học 9](#_Toc76593984)

[2.1.3 Ứng dụng của an toàn bảo mật thông tin và mật mã học 9](#_Toc76593985)

[**CHƯƠNG 3: MÃ HÓA VÀ GIẢI MÃ VỚI THUẬT TOÁN DES 10**](#_Toc76593986)

[**3.1 Tổng quan về thuật toán DES 10**](#_Toc76593987)

[3.1.1 Khái niệm 10](#_Toc76593988)

[3.1.2 Mô tả sơ đồ mã hoá DES 10](#_Toc76593989)

[3.1.3 Hóa vị IP và hoán bị ngược IP-1 12](#_Toc76593990)

[3.1.4 Thuật toán sinh khóa con 14](#_Toc76593991)

[3.1.5 Mô tả hàm f 16](#_Toc76593992)

[3.1.6 Hàm(ánh xạ) mở rộng E 17](#_Toc76593993)

[3.1.7 Mô tả hộp S - Box 18](#_Toc76593994)

[3.1.8 Mô tả hộp P - Box 21](#_Toc76593995)

[**3.2 Ưu nhược điểm của DES 22**](#_Toc76593996)

[3.2.1 Ưu điểm 22](#_Toc76593997)

[3.2.2 Nhược điểm 22](#_Toc76593998)

[**CHƯƠNG 4: DEMO 23**](#_Toc76593999)

[**4.1 Giao diện demo 23**](#_Toc76594000)

[**TÀI LIỆU THAM KHẢO** 26](#_Toc76594001)

# **DANH MỤC HÌNH ẢNH**

[*Hình 3.1: Sơ đồ chuẩn háo dữ liệu DES 10*](#_Toc76593824)

[*Hình 3.2: Sơ đồ mã hóa DES 11*](#_Toc76593825)

[*Hình 3.3: Sơ đồ cấu trúc 1 vòng DES 14*](#_Toc76593826)

[*Hình 3.4: Sơ đồ tạo khóa con của DES 15*](#_Toc76593827)

[*Hình 3.5: Sơ đồ hàm mở rộng E 18*](#_Toc76593828)

[*Hình 4.1: Giao diện mã hóa DES 23*](#_Toc76593829)

[*Hình 4.2: Giao diện kết quả mã hóa 24*](#_Toc76593830)

[*Hình 4.3: Giao diện kết quả giải mã 25*](#_Toc76593831)

# **DANH MỤC BẢNG**

[*Bảng 3.1 : Bảng hoán vị IP* 14](#_Toc76553868)

[*Bảng 3.2: Bảng hoán vị IP-1* 14](#_Toc76553869)

[*Bảng 3.3: Bảng PC-1* 16](#_Toc76553870)

[*Bảng 3.4: Bảng dịch bit tại các vòng lặp của DES* 17](#_Toc76553871)

[*Bảng 3.5: Bảng trật tự nén PC-2* 17](#_Toc76553872)

[*Bảng 3.6: Hộp S1* 20](#_Toc76553873)

[*Bảng 3.7: Hộp S2* 20](#_Toc76553874)

[*Bảng 3.8: Hộp S3* 21](#_Toc76553875)

[*Bảng 3.9: Hộp S4* 21](#_Toc76553876)

[*Bảng 3.10: Hộp S5* 21](#_Toc76553877)

[*Bảng 3.11: Hộp S6* 21](#_Toc76553878)

[*Bảng 3.12: Hộp S7* 22](#_Toc76553879)

[*Bảng 3.13: Hộp S8* 22](#_Toc76553880)

[*Bảng 3.14: Bảng hoán vị(Hộp P-Box)* 22](#_Toc76553881)

# **MỞ ĐẦU**

## Hướng tiếp cận của đề tài.

* Nghiên cứu và hiểu được cách thức mã hóa, giải mã của thuật toán DES.
* Tiến hành kiểm tra và chạy thử ứng dụng

## Mục tiêu nghiên cứu.

* Xây dựng, phát triển ứng dụng mã hóa, giải mã của thuật toán DES.

## Phương pháp nghiên cứu.

* Tìm hiểu và khai thác các dữ liệu, tài liệu liên quan đến thuật toán DES

Tiến hành xây dựng UI cho ứng dụng sử dụng thuật toán DES.

## Phân công công việc.

* Tìm hiểu thông tin lí thuyết, tài liệu: Yến 34%, Thương 33%, Vi 33%.
* Xây dựng chương trình : Yến 40%, Thương - Vi: 30%.
* Thực hiện báo cáo: Yến – Thương – Vi : 33%.

# **GIỚI THIỆU**

## An toàn bảo mật thông tin và mật mã học

### Giới thiệu về an toàn bảo mật thông tin

An toàn bảo mật thông tin là bảo vệ an toàn thông tin dữ liệu cá nhân, tổ chức nhằm tránh khỏi sự ” đánh cắp, ăn cắp” bởi những kẻ xấu hoặc tin tặc. Trải qua nhiều thế kỷ hàng loạt các giao thức (protocol) và các cơ chế (mechanism) đã được tạo ra để đáp ứng nhu cầu bảo về thông tin khi mà nó được truyền tải trên các phương tiện. Tính an toàn về mặt vâṭ lý của thông tin là hạn chế vì có thể bị xem trộm, sao chép …… Vì thế điều cần thiết đối với một xã hội mà thông tin phát triển là các phương tiện, phương pháp đảm bảo an toàn bảo mật thông tin độc lập với các phương tiện, phương pháp lưu trữ vận chuyển thông tin bằng cách vật lí. Phương tiện, phương pháp đó chính là mật mã học - ngành khoa học lịch sử lâu đời dựa trên nền tảng các thuật toán số học, toán học, xác suất và các môn khoa học khác.

Một hệ thống thông tin được xem là an toàn khi đảm bảo ít nhất ba mục tiêu cơ bản: tính bí mật, tính toàn vẹn, tính sẵn sàng. Ngoài ra còn có các mục tiêu khác như: tính không thể chối cãi, tính xác thực.

### Mật mã học

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

Mật mã học bao gồm hai lĩnh vực:

* Mã hóa: nghiên cứu các thuật toán và phương thức để đảm bảo tính bí mật và xác thực của thông tin (thường là dưới dạng các văn bản lưu trữ trên máy tính). Các sản phẩm của mã hóa 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.
* Thám mã: Nghiên cứu các phương pháp phá mã hoặc tạo mã giả. Sản phẩm của lĩnh vực này là các phương pháp thám mã, các phương pháp giả mạo chữ ký, các phương pháp tấn công các hàm băm và các giao thức mật mã.

### Ứng dụng của an toàn bảo mật thông tin và mật mã học

Ngày nay khó có thể tìm thấy các ứng dụng trên máy tính lại không sử dụng tới các thuật toán và các giao thức mật mã học. Từ các ứng dụng cho các máy tính cá nhân (Desktop Applications) cho tới các chương trình hệ thống như các hệ điều hành (Operating Systems) hoặc các ứng dụng mạng như Yahoo Messenger, các hệ cơ sở dữ liệu đều sử dụng các thuật toán mã hóa mật khẩu dùng bằng một hệ mã hoặc một hàm băm. Đặc biệt với sự phát triển mạnh mẽ của thương mại điện tử các mô hình chữ ký điện tử ngày càng đóng vai trò tích cực cho một môi trường an toàn cho người sử dụng.

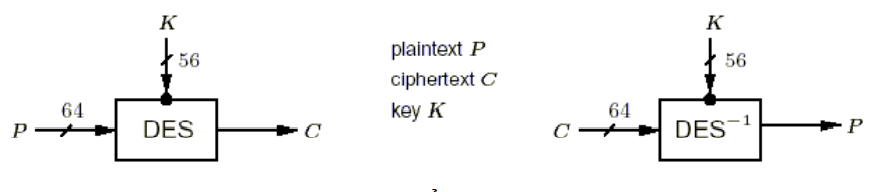
# **MÃ HÓA VÀ GIẢI MÃ VỚI THUẬT TOÁN DES**

## Tổng quan về thuật toán DES

### Khái niệm

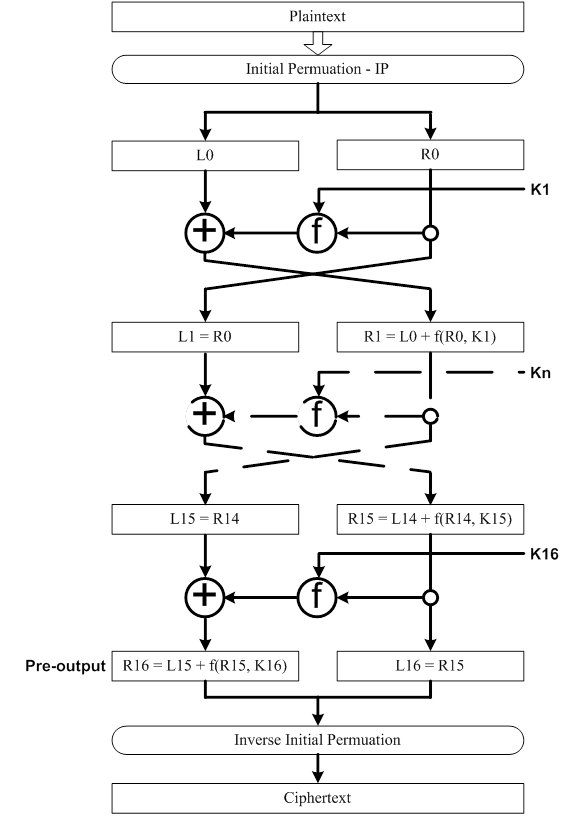
* DES là viết tắt của Data Encryption Standard hay còn gọi là tiêu chuẩn Mã hóa dữ liệu.
* Là phương pháp mật mã hóa được FIPS(Tiêu chuẩn Xử lý Thông tin Liên bang) chọn làm chuẩn chính thức năm 1976.
* Hiện nay DES được xem là không đủ an toàn cho nhiều ứng dụng do độ dài khóa tương đối ngắn(56 bit).

### Mô tả sơ đồ mã hoá DES



*Hình 3.1: Sơ đồ chuẩn háo dữ liệu DES*

DES là thuâṭ toán mã hóa với input là khối 64 bit, output cũng là khối 64 bit. Khóa mã hóa có độ dài 64 bit, thực ra chính xác hơn là 56 bit khóa + 8 bit (chia hết cho 8 có thể sử dụng là các bit kiểm tra tính chẵn lẻ).



*Hình 3.2: Sơ đồ mã hóa DES*

Thuật toán thực hiêṇ 16 vòng. Từ khóa input K, 16 khóa con 48 bit Ki sẽ được sinh ra, mỗi khóa cho một vòng thực hiện trong quá trình mã hóa. Trong mỗi vòng, 8 ánh xạ riêng biệt chuyển đổi 6 bit thành 4 bit bằng cách tách block 6 bit thành hai phần. Phần thứ nhất là tổ hợp của bit đầu tiên và bit cuối cùng của block để tạo thành 2 bit chọn hàng của bảng S, bảng S có 4 hàng được đánh số từ 0 đến 3 theo thứ tự từ trên xuống. Phần thứ 2 là 4 bit còn lại dùng để chọn cột của bảng S, bảng S có 16 cột được đánh số từ 0 đến 15 theo thứ tự từ trái qua phải.Như vậy, với mỗi block 8 bit ta chọn được 1 giá trị trong bảng S. Giá trị này nằm trong khoảng từ 0 đến 15 sẽ được quy đổi thành chuỗi nhị phân 4 bit tương ứng. Các chuỗi nhị phân có được sau khi chuyển đổi từ S1 đến S8 sẽ được ghép lại theo thứ tự từ trái qua phải để tạo thành một giá trị 32 bit.

Bản rõ 64 bit sẽ được sử dụng chia thành hai nữa L0 và R0. Các vòng có chức năng giống nhau, nhận input là Li-1 và Ri-1 từ vòng trước và sinh ra output là các xâu 32 bit Li và Ri như sau:

**Li = Ri-1;**

**Ri = Li-1 ⊕ f(Ri-1, Ki)**

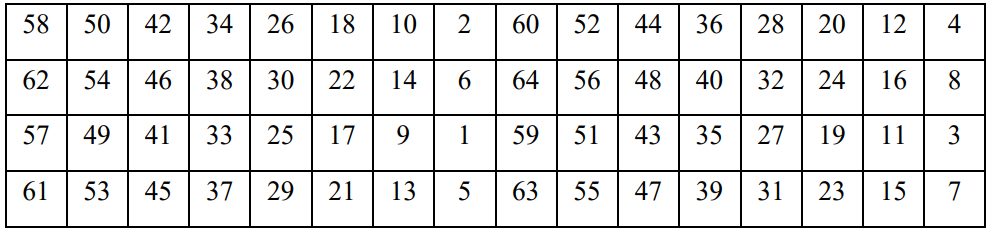
Với f(Ri-1, Ki) = P( S( E(Ri-1) ⊕ Ki ))

Trong đó:

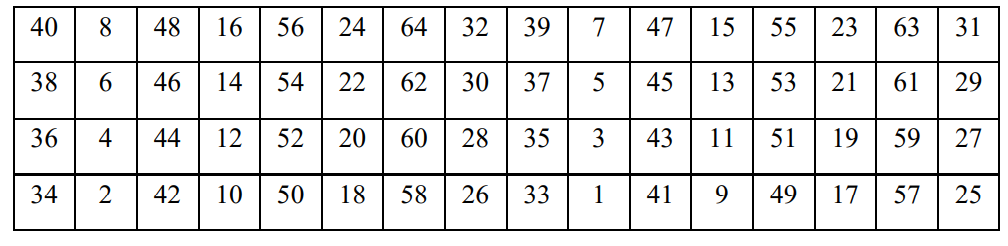
* + Là ký hiệu của phép tuyển loại trừ (XOR) của hai xâu bit theo modulo 2.
  + Hàm f là một hàm phi tuyến.
  + E là hoán vi ̣mở rộng ánh xạ Ri-1 từ 32 bit thành 48 bit.
  + P là hoán vi ̣cố định khác của 32 bit.

Một hoán vi ̣bit khởi đầu (IP) được sử dụng cho vòng đầu tiên, sau vòng cuối cùng nữa trái và nữa phải đổi cho nhau và cuối cùng xâu kết quả sẽ được hoán vi ̣bit lần cuối bởi hoán vi ̣ngược của IP (IP-1 ). Quá trình giải mã diễn ra tương tự nhưng với các khoá con ứng dụng vào các vòng trong theo thứ tự ngược lại. Có thể hình dung đơn giản là phần bên phải trong mỗi vòng sẽ thực hiện một tính toán thay thế phụ thuộc khóa trên mỗi một 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 khoá 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 vi ̣và gán cho hai biến 28 bit C và D, và sau đó trong 16 vòng lặp cả 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.

### Hóa vị IP và hoán bị ngược IP-1

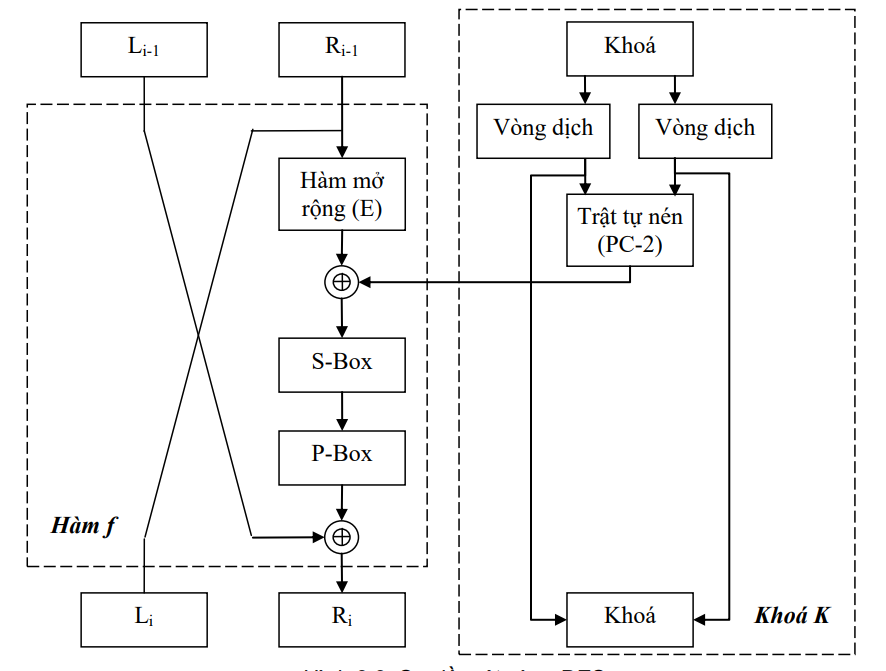


*Bảng 3.1 : Bảng hoán vị IP*



*Bảng 3.2: Bảng hoán vị IP-1*

Hoán vị ngược IP-1 bước cuối cùng để tạo ra giá trị mã hóa. Giá trị của lần lặp mã hóa cuối cùng sẽ được hoán vị khởi tạo đảo IP-1 và tạo ra giá trị mã hóa plaintext.

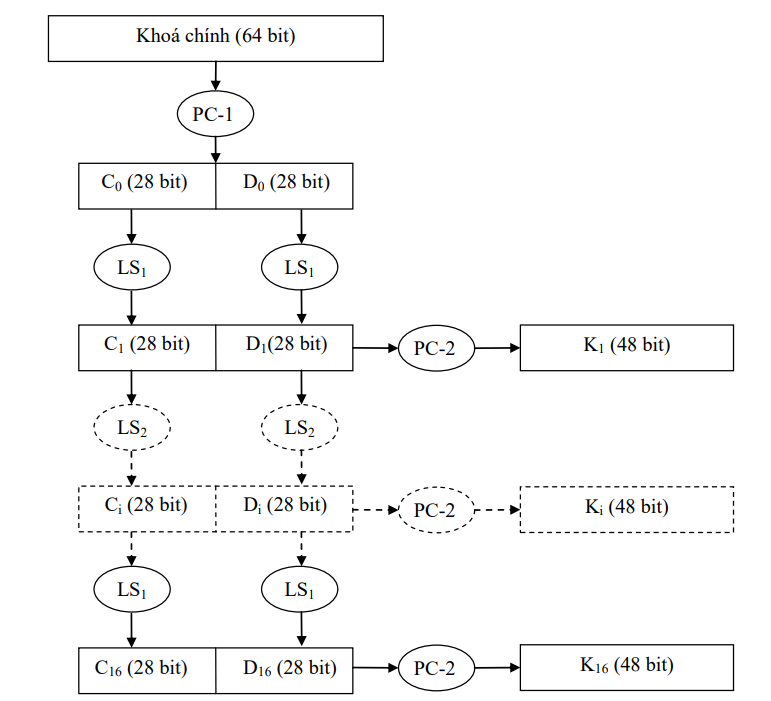


*Hình 3.3: Sơ đồ cấu trúc 1 vòng DES*

Hai hoán vị IP và IP-1 không có ý nghĩa gì về mặt mật mã mà nhằm tạo điều kiện cho việc “chip hoá” thuật toán DES.

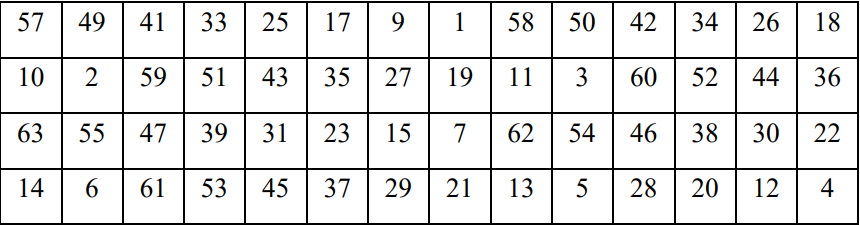
### Thuật toán sinh khóa con

DES có 16 vòng chạy thuật toán như nhau nhưng với 16 khóa con khác nhau. Các khoá con đều đƣợc sinh ra từ khoá chính của DES bằng một thuật toán sinh khoá con. Khoá chính K (64 bit) đi qua 16 bước biến đổi, tại mỗi bước một khoá con được sinh ra với độ dài 48 bit.



*Hình 3.4: Sơ đồ tạo khóa con của DES*

Đầu tiên, từ 64 bit ban đầu của khóa, 56 bit được chọn 8 bit còn lại bị loại bỏ. Sau đó 56 bit này lại được trích lấy 48 bit để sinh ra khóa cho 16 vòng của DES.



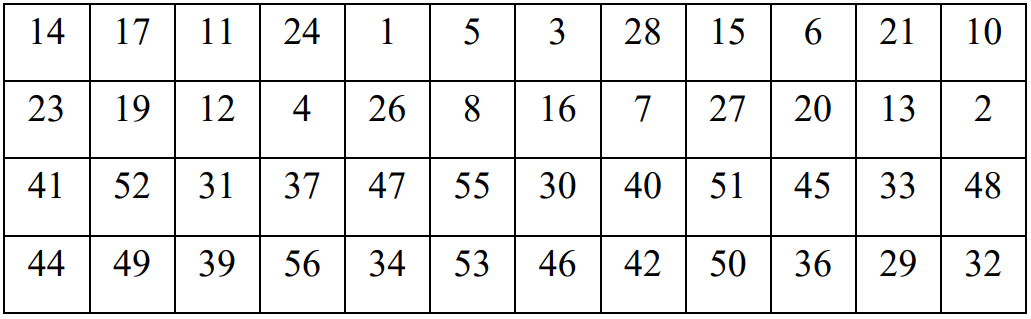
*Bảng 3.3: Bảng PC-1*

Sau đó 56 bit thu được được chia làm hai phần bằng nhau là C và D mỗi phần được xử lý độc lập. Sau mỗi chu trình, mỗi phần được dịch đi 1 hoặc 2 bit (tùy thuộc từng chu trình, nêu đó là chu trình 1,2,9,16 thì đó là dịch 1 bit, còn lại thì sẽ được dịch 2 bit).

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

*Bảng 3.4: Bảng dịch bit tại các vòng lặp của DES*

Các khóa con 48 bit được tạo thành bởi thuật toán lựa chọn 2 (PC-2) gồm 24 bit từ mỗi phần. Vì cách hoán vị này của các bit được chọn như một tổ hợp con của các bit nên được gọi là “hoán vị nén” hay “trật tự nén”.



*Bảng 3.5: Bảng trật tự nén PC-2*

Quá trình dịch khiến cho các khóa con sử dụng các bit khác nhau của khóa chính, mỗi bit được sử dụng trung bình ở 14 trong tổng số 16 khóa con.

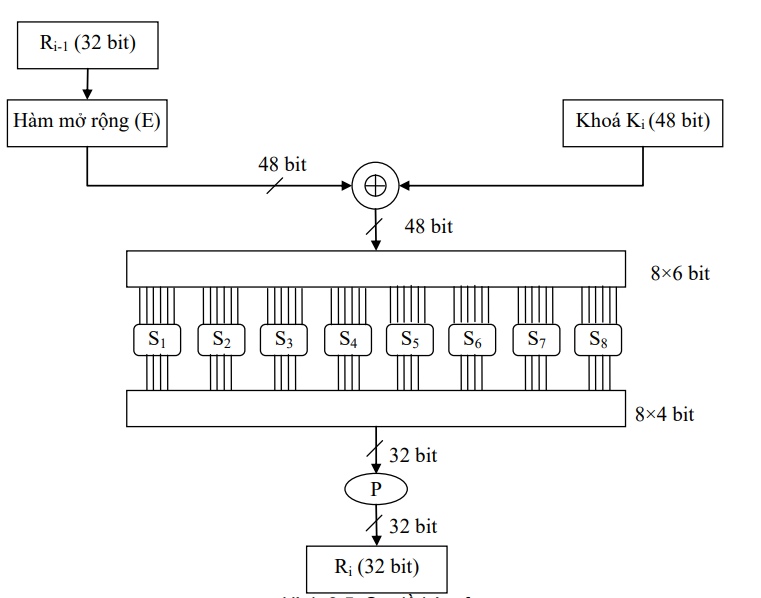
Quá trình tạo khóa con khi thực hiện giải mã cũng diễn ra tương tự nhưng các khóa con được tạo theo thứ tự ngược lại. Ngoài ra sau mỗi chu trình, khóa sẽ được dịch phải thay vì dịch trái như khi mã hóa.

### Mô tả hàm f

Hàm f(Ri-1,Ki) là một hàm có hai biến vào:

* Biến thứ nhất Ri-1 là một xâu bit có độ dài 32 bit,
* Biến thứ hai khoá Ki  là một xâu bít có độ dài 48 bit.

Đầu ra của f là một xâu bit có độ dài 32 bit. Hàm f có thể là hàm bất kỳ tuy nhiên vì nguồn gốc “sức mạnh” của DES nằm trong hàm f nên việc chọn hàm f phải cẩn thận để tránh bị phá mã một cách dễ dàng.



Hàm f hoạt động trên khối 32 bit và bao gồm bốn giai đoạn:

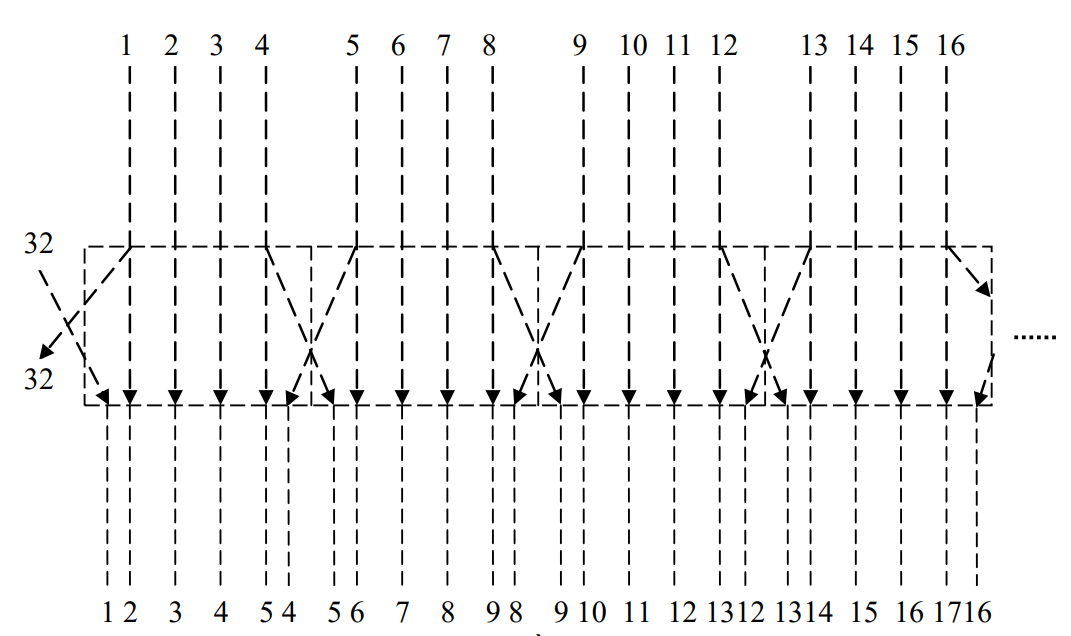
1. Mở rộng: 32 bit đầu vào được mở rộng thành 48 bit sử dụng thuật toán hoán vị mở rộng (*expansion permutation*) với việc nhân đôi một số bit. Giai đoạn này được ký hiệu là E trong sơ đồ.
2. Trộn khóa: 48 bit thu được sau quá trình mở rộng được XOR với khóa con. Mười sáu khóa con 48 bit được tạo ra từ khóa chính 56 bit theo một chu trình tạo khóa con (*key schedule*) đã miêu tả ở phần trước.
3. Thay thế: 48 bit sau khi trộn được chia làm 8 khối con 6 bit và được xử lý qua hộp thay thế S-box. Đầu ra của mỗi khối 6 bit là một khối 4 bit theo một chuyển đổi phi tuyến được thực hiện bằng một bảng tra. Khối S-box đảm bảo phần quan trọng cho độ an toàn của DES. Nếu không có S-box thì quá trình sẽ là tuyến tính và việc thám mã sẽ rất đơn giản.
4. Hoán vị: Cuối cùng, 32 bit thu được sau S-box sẽ được sắp xếp lại theo một thứ tự cho trước (còn gọi là P-box). Kết quả P(C) sẽ là kết quả của hàm f(Ri-1, Ki), và cũng chính là Ri cho vòng sau.

### Hàm(ánh xạ) mở rộng E

Hàm mở rộng (E) sẽ tăng độ dài của 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 khoá K để thực hiện việc cộng modulo XOR.
  + Cho kết quả dài hơn để có thể nén trong suốt quá trình thay thế.

Tuy nhiên, cả hai mục đích này đều 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 khoá.



*Hình 3.5: Sơ đồ 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 2 và 3 tương ứng với 1 bit ở đầu ra.

### Mô tả hộp S - Box

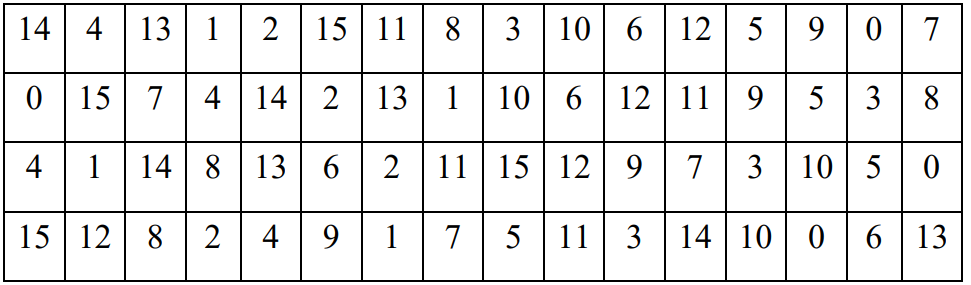
Đối với sơ đồ mã hoá DES, mọi tính toán đều là tuyến tính, tức là việc tính phép tuyển loại trừ XOR của hai đầu ra cũng giống với phép tuyển loại trừ XOR của hai đầu vào rồi tính toán đầu ra. Chỉ duy nhất có các tính toán với hộp S là phi tuyến. Chính vì vậy các hộp S-Box (chứa đựng các thành phần phi tuyến của hệ mật) là quan trọng nhất đối với độ mật của hệ mã, chính các hộp S tạo nên sự hỗn loạn (confusion) và sự khuếch tán (diffusion) của DES. Năm 1976, NSA đã đưa ra tiêu chuẩn thiết kế hộp S như sau:

* Mỗi hàng trong mỗi hộp S là một 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. 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 1 2 3 4 5 4 5 6 7 8 9 8 9 10 11 12 1312 1314 15 16 1716 32
* Đối với hộp S bất kỳ và với đầu vào x (một xâu bit có độ dài bằng 6) bất kỳ, thì S(x) và S(x ⊕ 001100) phải khác nhau ít nhất là 2 bit.

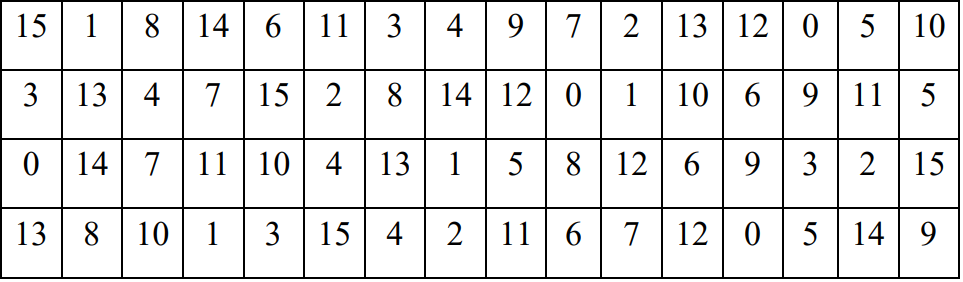
NSA cũng tiết lộ 3 thuộc tính của hộp S, những thuộc tính này đảm bảo tính confusion và diffusion của thuật toán:

* Các bit vào luôn phụ thuộc không tuyến tính với các bit ra.
* Sửa đổi ở một bit vào làm thay đổi ít nhất là hai bit ra.
* Khi một bit vào được giữ cố định và 5 bit còn lại cho thay đổi thì hộp S thể hiện một tính chất được gọi là “phân bố đồng nhất” so sánh số lượng bit số 0 và 1 ở các đầu ra luôn ở mức cân bằng. Tính chất này khiến cho việc phân tích theo lý thuyết thống kê để tìm cách phá hộp S là vô ích.

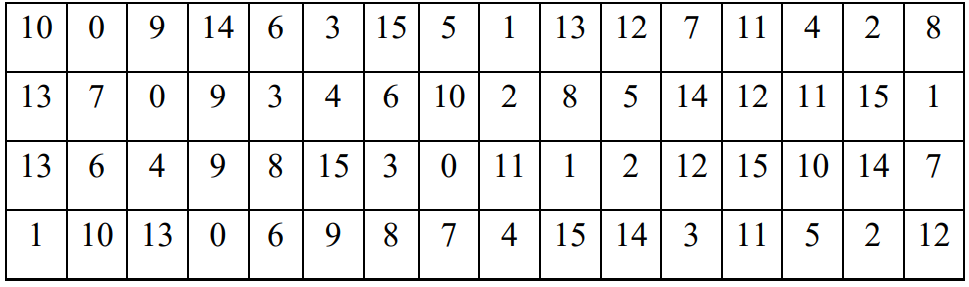
Sau khi cộng modulo với khoá K, kết quả thu được chuỗi 48 bit chia làm 8 khối đưa vào 8 hộp S-Box. Mỗi hộp S-Box có 6 bit đầu vào và 4 bit đầu ra (tổng bộ nhớ yêu cầu cho 8 hộp S-Box chuẩn DES là 256 bytes). Kết quả thu được là một chuỗi 32 bit tiếp tục vào hộp P-Box.



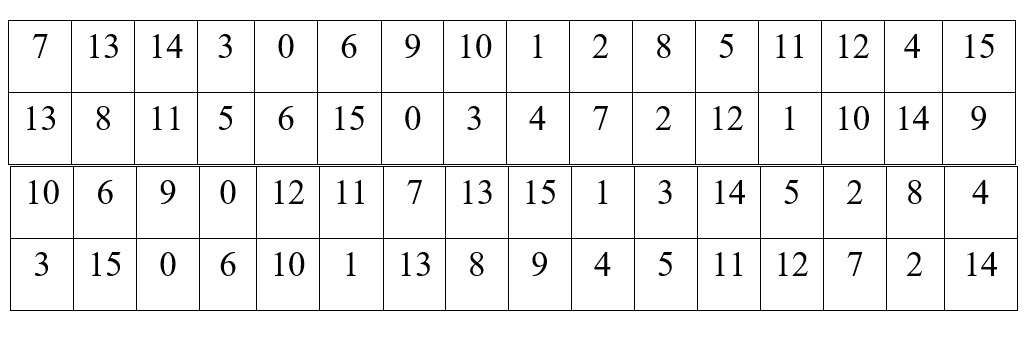
*Bảng 3.6: Hộp S1*



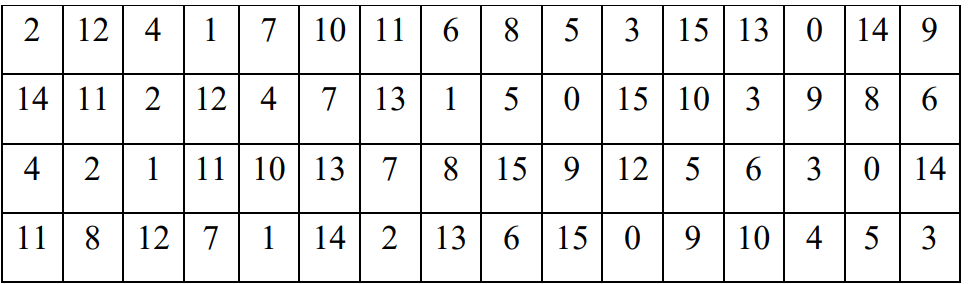
*Bảng 3.7: Hộp S2*



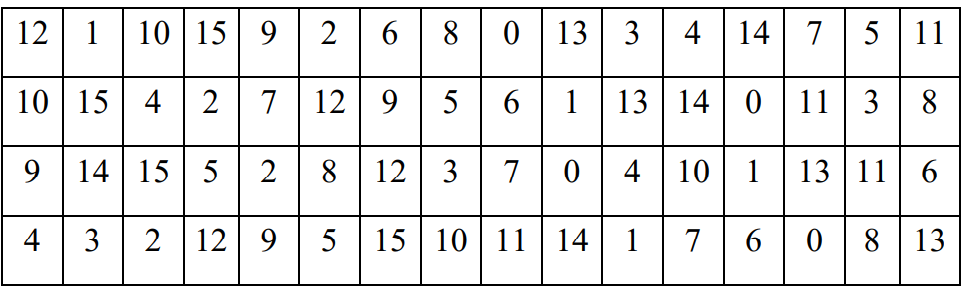
*Bảng 3.8: Hộp S3*



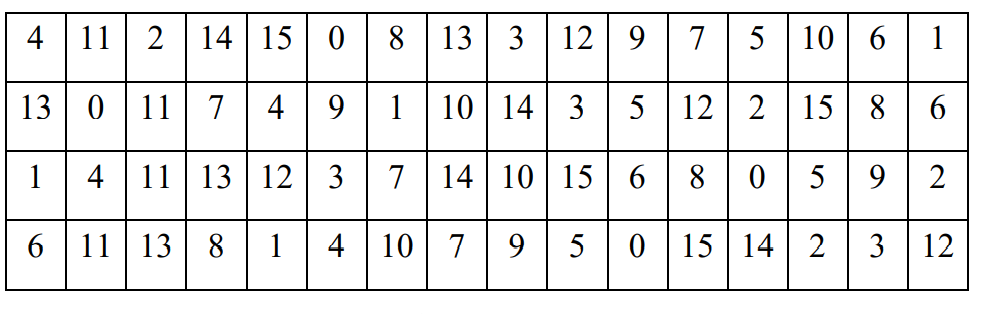
*Bảng 3.9: Hộp S4*



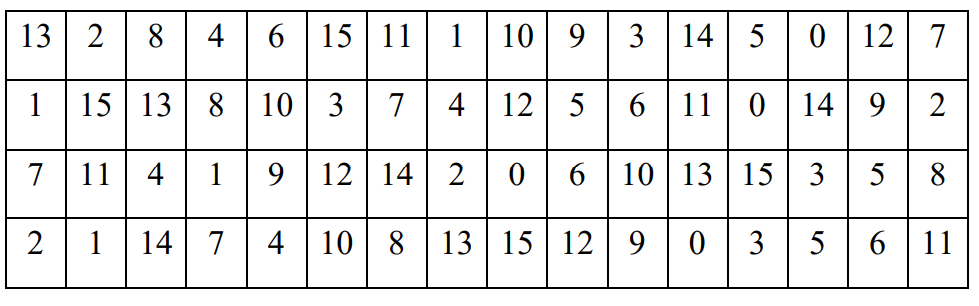
*Bảng 3.10: Hộp S5*



*Bảng 3.11: Hộp S6*



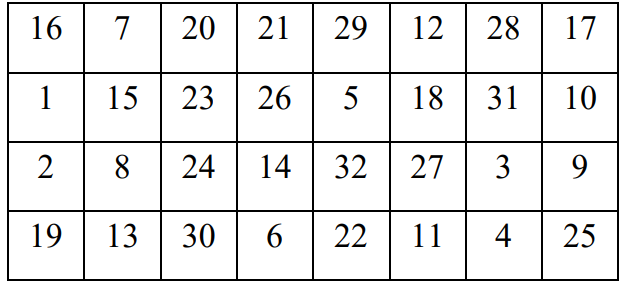
*Bảng 3.12: Hộp S7*



*Bảng 3.13: Hộp S8*

### Mô tả 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 hai lần hay bị bỏ qua. Hộp P-Box thực chất chỉ làm chức năng sắp xếp đơn thuần theo bảng sau:



*Bảng 3.14: Bảng hoán vị(Hộp P-Box)*

## Ưu nhược điểm của DES

### Ưu điểm

* Thuật toán mã hoá DES tốc độ mã hoá dữ liệu rất nhanh.

### Nhược điểm

* DES có kích cỡ của không gian khoá 256 là quá nhỏ, không đủ an toàn, cho nên những máy có mục đích đặc biệt có thể sẽ bẻ gãy và dò ra khoá rất nhanh.

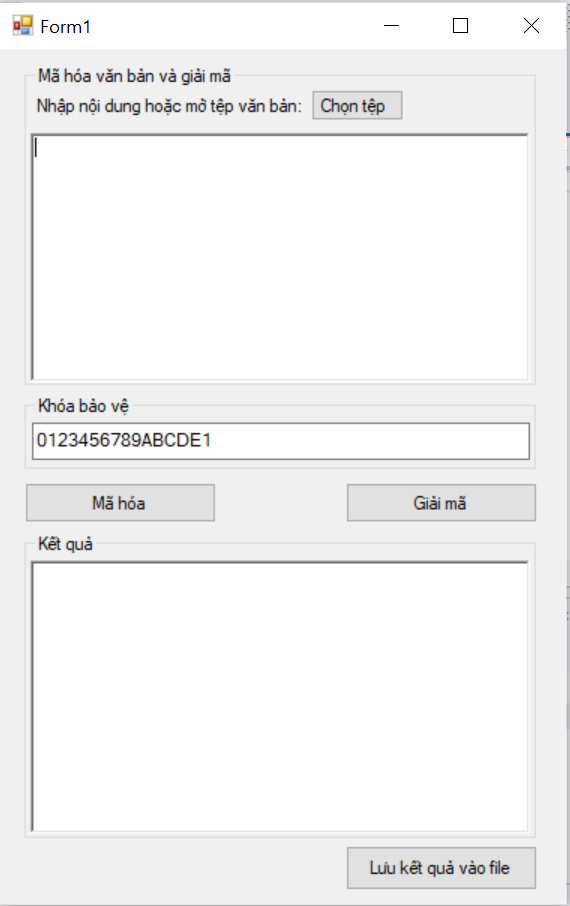
# **XÂY DỰNG CHƯƠNG TRÌNH**

## Bài toán đặt ra

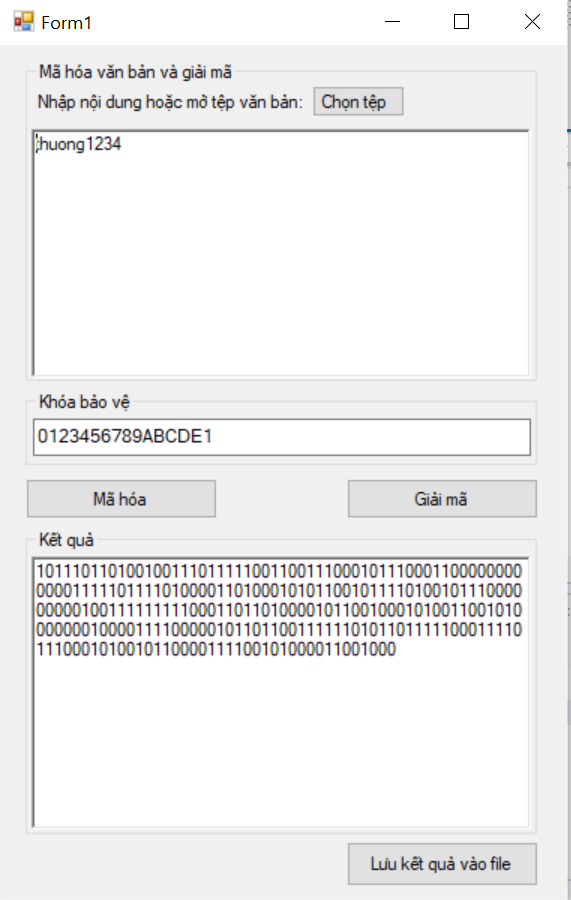
Viết chương trình mã hóa và giãi mã văn bản với thuật toán mã hóa DES. Chương trình có thể thực hiện các chức năng sau:

* Cho phép nhập văn bản vào hệ thống.
* Cho phép nhập khóa bảo vệ văn bản.
* Cho phép ghi File và mở File.

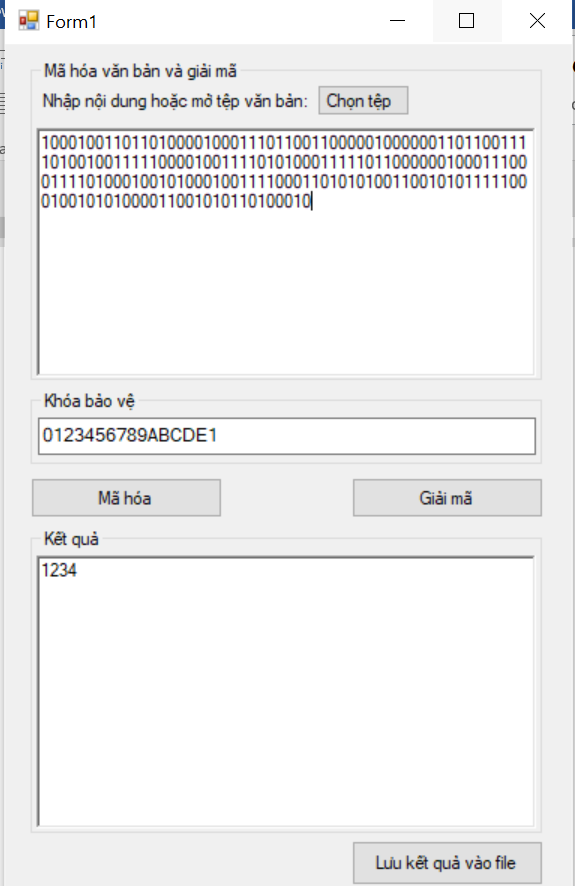
## Giao diện demo



*Hình 4.1: Giao diện mã hóa giải mã DES*



*Hình 4.2: Giao diện kết quả mã hóa*



*Hình 4.3: Giao diện kết quả giải mã*

# **TÀI LIỆU THAM KHẢO**

[1] <https://nguyenquanicd.blogspot.com/>

[2] <https://thuvientvc.files.wordpress.com/>

[3]