



Nhom 1 Bao Cao BTL Atbmtt

Cơ bản công nghệ thông tin (Trường Đại học Công nghiệp Hà Nội)

**BỘ CÔNG THƯƠNG
TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**



BÀI TẬP LỚN

Môn: An toàn và bảo mật thông tin

Đề tài 1: Ứng dụng thuật toán DES và lược đồ chia sẻ bí mật vào thi tuyển sinh

CBHD: ThS. Trần Phương Nhung

Nhóm: 1

Thành viên nhóm:

1. Đoàn Nam Anh - 2021600078 (Trưởng nhóm)
2. Nguyễn Văn An - 2021601318 (Thư kí)
3. Trần Đức An - 2021601904
4. Dư Ngọc Ánh - 2021605184

Hà Nội - 2022

MỤC LỤC

Chương 1. Tổng quan	3
1.1. Mục tiêu đề tài.....	3
1.2. Nội dung nghiên cứu.....	4
1.3. Chủ đề nghiên cứu.....	4
1.4. Kiến thức bắt buộc.....	4
1.5. Lĩnh vực nghiên cứu.....	5
1.6. Phương pháp nghiên cứu.....	6
1.7. Tìm hiểu về ngôn ngữ lập trình.....	7
1.8. Cách thực hiện đề tài.....	7
Chương 2. Kết quả nghiên cứu	8
2.1 Giới thiệu.....	8
2.2 Nội dung thuật toán.....	8
2.3 Thiết kế, cài đặt chương trình đề mô thuật toán.....	10
2.3.1 Giao diện chương trình demo	10
2.4 Cài đặt và triển khai.....	10
2.5 Thực hiện bài toán.....	16
2.5.1 Phân công công việc	16
2.5.2 Đoàn Nam Anh và Nguyễn Văn An – Tìm hiểu hệ mật mã DES	17
2.5.3 Dư Ngọc Ánh – Nghiên cứu bài toán chia sẻ bí mật Lagrange	34
2.5.4 : Trần Đức An - Ứng dụng lược đồ chia sẻ bí mật của Lagrange để phân phối khóa	37
Chương 3. Phần kiến thức lĩnh hội và bài học kinh nghiệm	39
3.1 Nội dung đã thực hiện.....	39
3.2 Hướng phát triển.....	40
3.2.1 Xác định tính khả thi của đề tài	40
3.2.2 Những thuận lợi trong quá trình nghiên cứu.	40
3.2.3 Những khó khăn trong quá trình nghiên cứu	40
3.2.4 Hướng phát triển	41
Chương 4. Kết luận	41
1. Tìm hiểu lí thuyết về mật mã	41
2. Phần ứng dụng	41
Tài liệu tham khảo	42

Chương 1. Tổng quan

1.1. Mục tiêu đề tài

Hiện nay, với sự phát triển không ngừng của mạng máy tính, mỗi quốc gia đều có mạng riêng với rất nhiều mạng mang tính bộ phận trên phạm vi toàn cầu, người ta đã dùng mạng Internet một cách thông dụng. Các dịch vụ điện tử: thư điện tử, chuyển tiền, thương mại điện tử, chính phủ điện tử... đã được áp dụng rộng rãi.

Khi các ứng dụng trên mạng máy ngày càng trở lên phổ biến, thuận lợi và quan trọng thì yêu cầu về an toàn mạng, an ninh dữ liệu càng trở lên cấp bách và cần thiết.

Trên thế giới có rất nhiều quốc gia, nhiều nhà khoa học nghiên cứu về vấn đề bảo mật, đưa ra nhiều thuật toán với mục đích thông tin truyền đi không bị lấy cắp hoặc nếu bị lấy cắp thì cũng không thể sử dụng được. Trong đề tài của chúng em đưa ra một thuật toán đó là thuật toán DES (Data encryption standard) đây là thuật toán chuẩn của Mỹ, được Mỹ và nhiều nước trên thế giới sử dụng, thuật toán này đã được đưa vào sử dụng nhiều năm nhưng vẫn giữ được tính bảo mật của nó. Tuy nhiên với công nghệ phát triển như hiện nay thì thuật toán DES trở lên không được an toàn tuyệt đối nữa, người ta đã đưa ra thuật toán 3DES dựa trên nền tảng của thuật toán DES nhưng số bit được mã hóa tăng lên.

Mã hóa và các lược đồ chia sẻ bí mật có thể được ứng dụng trong rất nhiều lĩnh vực ví dụ: phát hành thẻ ATM trong ngân hàng, đấu thầu

từ xa, trong thi tuyển sinh, trong lĩnh vực quân sự... Trong đề tài của em đề cập tới một lĩnh vực đó là ứng dụng trong thi tuyển sinh.

Vấn đề thi tuyển sinh đại học ở nước ta trở thành gánh nặng cho ngành giáo dục và các ban ngành khác liên quan. Nó gây tổn hại về kinh tế, công sức không chỉ với các ban ngành tham gia tổ chức kì thi mà chính cả những sĩ tử dự thi cũng sẽ bị ảnh hưởng không nhỏ, đặc biệt khi kì thi này có sức nặng rất lớn lên cuộc đời và sự nghiệp của các em. Vì vậy để giảm thiểu những khâu không cần thiết và đảm bảo tính công bằng, chính xác cho kì thi, chúng em nghĩ rằng chúng ta nên ứng dụng công nghệ thông tin vào kì thi tuyển sinh này, cụ thể hơn ở đây là lược đồ chia sẻ bí mật và thuật toán DES để đảm bảo tính bảo mật và chính xác cho các thông tin nhạy cảm trong kì tuyển sinh như vị trí thi, ngày thi, đề thi,...

Phạm vi bài toán đề cập đến mật mã, thuật toán DES, lược đồ chia sẻ bí mật và ứng dụng của chúng trong việc bảo mật thông tin thi tuyển sinh.

1.2. Nội dung nghiên cứu

- Tìm hiểu mã hóa DES và các bước thực hiện mã hóa DES
- Tìm hiểu giải mã DES và các vấn đề liên quan đến DES
- Nghiên cứu bài toán chia sẻ bí mật của lagrange
- Ứng dụng lược đồ chia sẻ bí mật của lagrange để phân phối khóa
- Demo chương trình (Sử dụng ngôn ngữ C++)

- Demo chương trình (Sử dụng ngôn ngữ C#)
- Demo chương trình (Sử dụng ngôn ngữ Java)
- Demo chương trình (Sử dụng ngôn ngữ Python)
- Demo chương trình (Sử dụng ngôn ngữ JavaScript)

1.3. Chủ đề nghiên cứu

Ứng dụng thuật toán DES và lược đồ chia sẻ bí mật vào thi tuyển sinh thuộc lĩnh vực đảm bảo tính an toàn, toàn vẹn dữ liệu.

1.4. Kiến thức bắt buộc.

□ Kiến thức chuyên ngành

Yêu cầu có kiến thức về công nghệ thông tin, sử dụng thành thạo một số ngôn ngữ lập trình như C, C++, C#, Java, JavaScripts... Và đặc biệt am hiểu về an toàn bảo mật thông tin. Ngoài các kiến thức trên không thể bỏ qua yếu tố yêu thích với an toàn bảo mật thông tin và đam mê lập trình.

□ Kiến thức về hệ mã DES

- Đặc điểm của hệ mã hóa DES
- Thuật toán mã hóa, giải mã
- Ưu nhược điểm
- Cách tính hàm f

- Nắm vững được bài toán chia sẻ bí mật
- Sơ đồ chia sẻ bí mật
- Công thức nội suy Lagrange
- Phép nội suy đa thức

1.5. Lĩnh vực nghiên cứu.

Đề tài “*Ứng dụng thuật toán DES và lược đồ chia sẻ bí mật vào thi tuyển sinh*” thuộc lĩnh vực an toàn bảo mật thông tin.

Nghiên cứu các vấn đề liên quan đến thuật toán DES, mã hóa, giải mã DES, chia sẻ khóa theo phương thức chia sẻ bí mật Shamir, khôi phục khóa bằng phương pháp dùng công thức nội suy Lagrange, chia sẻ khóa bí mật và khôi phục khóa bằng mạch đơn điệu.

□ Kiến thức cơ bản về an toàn thông tin

- Biết phân biệt giữa dữ liệu và thông tin. Biết cách thức lưu trữ, vận chuyển dữ liệu và thông tin trong môi trường truyền thông.
- Hiểu các loại nguy cơ đối với dữ liệu: mất cắp, mất an toàn (safety) về vật lý (hư hỏng môi trường lưu giữ, các thảm họa - chiến tranh, thiên tai, cháy nổ), không đảm bảo an toàn thông tin trong khai thác, sử dụng.

- Hiểu nguồn gốc các nguy cơ đối với việc đảm bảo an toàn thông tin: từ nhân viên, các nhà cung cấp dịch vụ, từ các cá nhân bên ngoài. Hiểu khái niệm tội phạm mạng (cybercrime).
- Biết về các lỗ hổng bảo mật hệ thống: của hệ điều hành, hệ quản trị cơ sở dữ liệu, dịch vụ Internet. Biết các khái niệm và phương thức hoạt động của các thiết bị bảo mật.

❖ Các lĩnh vực an toàn thông tin

- Hiểu và phân biệt việc đảm bảo an toàn cho tổ chức như chính phủ, doanh nghiệp và đảm bảo an toàn cho cá nhân khi tham gia các hoạt động trên mạng.
- Biết các đặc trưng cơ bản của an toàn thông tin: tính mật, tính toàn vẹn, tính sẵn sàng, tính xác thực.
- Biết các quy định phổ biến về bảo vệ, gìn giữ và kiểm soát dữ liệu, sự riêng tư tại Việt Nam.
- Hiểu vai trò của các lĩnh vực liên quan đến an toàn dữ liệu: chính sách, tổ chức, biện pháp quản lý và các giải pháp công nghệ.
- Biết về tiêu chuẩn TCVN ISO/IEC 27001:2009. Biết một số chính sách cơ bản về an toàn thông tin và một số văn bản pháp luật về an toàn thông tin của Việt Nam. Hiểu tầm quan trọng của việc xây dựng và thi hành chính sách an toàn thông tin đối với việc ứng dụng CNTT.

1.6. Phương pháp nghiên cứu.

- Sử dụng các công cụ sau: Word, DevC, Visual Studio, ...
- Ngôn ngữ: C, C++, C#, Java, JavaScripts

1.7. Tìm hiểu về ngôn ngữ lập trình

- Với C, C++, C#, Java, JavaScripts.
 - + Tìm hiểu về hướng đối tượng
 - + Tìm hiểu về các kiểu dữ liệu, khai báo biến, vòng lặp, thao tác với chuỗi, mảng, constructor, method, object, class, cấp độ truy cập dữ liệu
 - + Nghiên cứu cách giải quyết bài toán
 - + Vận dụng kiến thức tìm hiểu thực hiện giải đề tài được giao

1.8. Cách thực hiện đề tài

- Tìm hiểu mã hóa DES và các bước thực hiện mã hóa DES
- Tìm hiểu giải mã DES và các vấn đề liên quan đến DES
- Nghiên cứu bài toán chia sẻ bí mật của lagrange
- Ứng dụng lược đồ chia sẻ bí mật của lagrange để phân phối khóa

Chương 2. Kết quả nghiên cứu

1.1 Giới thiệu

- Tên đề tài nghiên cứu: Ứng dụng thuật toán DES và lược đồ chia sẻ bí mật trong thi tuyển sinh.

Nội dung nghiên cứu

- Tìm hiểu mật mã DES
 - Nghiên cứu bài toán chia sẻ bí mật của Lagrange
 - Ứng dụng lược đồ chia sẻ bí mật của Lagrange để phân phối khóa
 - Demo chương trình
- Các bước thực hiện triển khai đề tài bao gồm:
- Nghiên cứu, tìm hiểu cách mã hóa và giải mã của hệ mật mã DES
 - Nghiên cứu bài toán chia sẻ bí mật của Lagrange, từ đó áp dụng lược đồ chia sẻ bí mật để phân phối khóa
 - Thiết kế và cài đặt chương trình demo thuật toán DES
- Hình thức sản phẩm: Sản phẩm bản mẫu
- Kết quả đạt được:
- Quyền báo cáo bài tập lớn
 - Chương trình demo thuật toán

1.2 Nội dung thuật toán

Về Mã hóa và giải mã DES

- Thuật toán hoán vị các bảng IP, IP-1, E, P, PC-1
- Thuật toán dịch bit sang trái
- Thuật toán chuyển cơ số
- Thuật toán chuyển mảng 1 chiều sang 2 chiều và ngược lại

Về thuật toán chia sẻ bí mật

Giai đoạn khởi tạo:

1. D chọn w phần tử khác nhau và khác 0 trong Z_p và kí hiệu chúng là: x_i , $1 \leq i \leq w$ ($w \geq p+1$).

Với $1 \leq i \leq w$, D cho giá trị x_i cho p_i . Các giá trị x_i là công khai.

Phân phối mảnh:

2. Giả sử D muốn phân chia khóa $k \in Z_p$. D sẽ chọn một cách bí mật (ngẫu nhiên và độc lập) $t-1$ phần tử Z_p , $a_1 \dots a_{t-1}$
3. Với $1 \leq i \leq w$, D tính $y_i = a(x_i)$, trong đó

$$a(x) = k + \sum_{i=1}^{t-1} a_i x^i \pmod{p}$$

4. Với $1 \leq i \leq w$, D sẽ trao mảnh y_i cho p_i

Về thuật toán khôi phục khóa theo công thức nội suy Lagrange

Tất cả n người A_1, A_2, \dots, A_n có thể hợp tác lại để khôi phục lại bí mật S bằng cách tính:

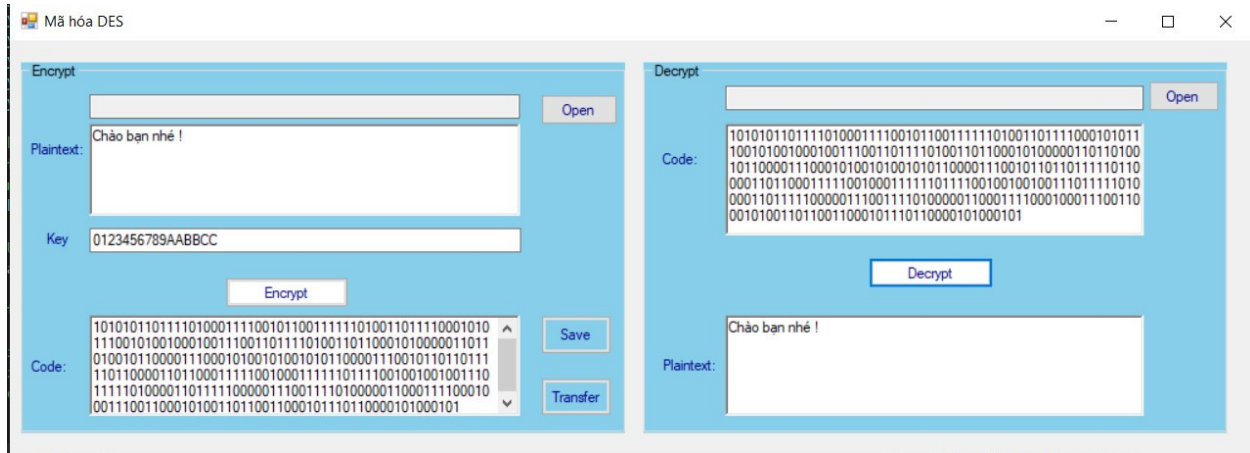
$$g(x) = \sum_{0 \leq j \leq n} f(v_j) \prod_{0 \leq i \leq n} (v_j - v_i)^{-1} (x - v_i) \pmod{p}$$

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

2.1.1

Giao diện chương

trình demo



Hình 1 : Giao diện chương trình như sau

Chức năng của chương trình gồm mã hóa và giải mã hệ mật mã DES

1.4 Cài đặt và triển khai

Giới thiệu công cụ:

Microsoft Visual Studio là một môi trường phát triển tích hợp (IDE) từ Microsoft. Microsoft Visual Studio còn được gọi là "Trình soạn thảo mã nhiều người sử dụng nhất thế giới ". Nó được sử dụng để phát triển chương trình máy tính cho Microsoft Windows, cũng như các trang web, các ứng dụng web và các dịch vụ web. Visual Studio sử dụng nền tảng phát triển phần mềm của Microsoft như Windows API, Windows Forms, Windows Presentation Foundation, Windows Store và Microsoft Silverlight. Nó có thể sản xuất cả hai ngôn ngữ máy và mã số quản lý.

Visual Studio bao gồm một trình soạn thảo mã hỗ trợ IntelliSense cũng như cải tiến mã nguồn. Trình gỡ lỗi tích hợp hoạt động cả về trình gỡ lỗi mức độ mã nguồn và gỡ lỗi mức độ máy. Công cụ tích hợp khác bao gồm một mẫu thiết kế các hình thức xây dựng giao diện ứng dụng, thiết kế web, thiết kế lớp và thiết kế giản đồ cơ sở dữ liệu. Nó chấp nhận các plug-in nâng cao các chức năng ở hầu hết các cấp bao gồm thêm hỗ trợ cho các hệ thống quản lý phiên bản (như Subversion) và bổ sung thêm bộ công cụ mới như biên tập và thiết kế trực quan cho các miền ngôn ngữ cụ thể hoặc bộ công cụ dành cho các khía cạnh khác trong quy trình phát triển phần mềm.



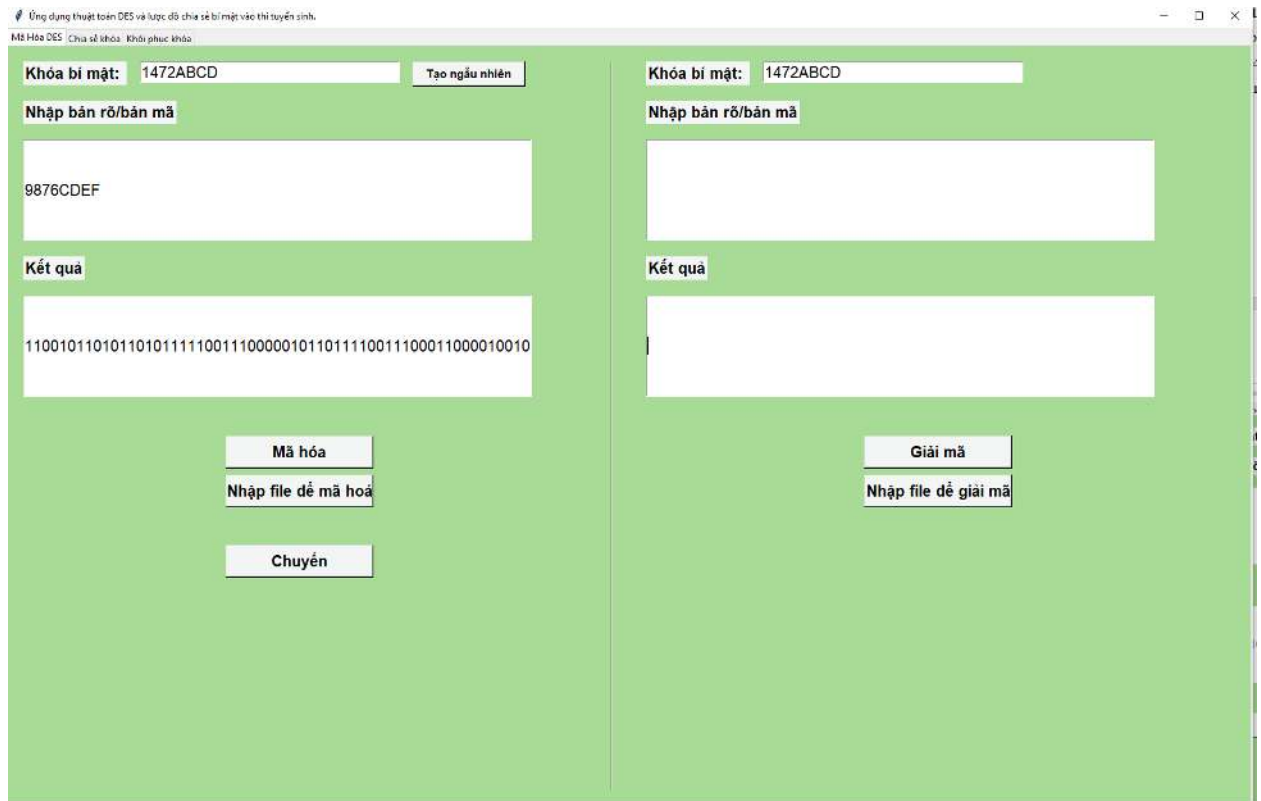
Hướng dẫn chạy chương trình Demo:

Chức năng 1: Mã hóa và giải mã chuỗi Hexa:

Nhập chuỗi bản rõ: 9876CDEF

Nhập Key: 1472ABCD

Sau đó nhấn mã hóa:



Bản Mã là :

```
11001011010110101111100111000001011011110011100011000010010110011110
0010010010000010111111110111000010111011010001101110001011111100010
0100100000101111111101110000101110110100011011100010111111000100100
1000001011111111011100001011101101000110111000101111110001001001000
0010111111110111000010111011010001101110001011111100010010010000010
1111111101110000101110110100011011100010111111000100100100000101111
1111101110000101110110100011011100010111111000100100100000101111111
101110000101110110100011011100010111
```

Ngược lại :

Ta nhập chuỗi bản Mã là :

```
11001011010110101111100111000001011011110011100011000010010110011110
0010010010000010111111110111000010111011010001101110001011111100010
```

0100100000101111111101110000101110110100011011100010111111000100100
 10000010111111111011100001011101101000110111000101111110001001001000
 00101111111110111000010111011010001101110001011111100010010010000010
 1111111101110000101110110100011011100010111111000100100100000101111
 1111101110000101110110100011011100010111111000100100100000101111111
 1011100001011101101000110111000101111110001001001000001011111111

Với khóa K dùng để mã hóa : 1472ABCD

Sau đó nhấn giải mã:

Bản Rõ nhận được đúng với ban đầu là 0123456798ABCDEF.

Tuy nhiên đây khóa K dùng để giải mã ngược với dãy khóa K dùng để mã hóa.

Đây là sự khác nhau giữa mã hóa và giải mã của hệ mật mã DES.

Chức năng 2: Mã hóa và giải mã chuỗi ký tự

Bản rõ là: Nhóm 1-ATBMTT

Khóa K: 5911BCDA

Nhấn mã hoá:

Ứng dụng thuật toán DES và lược đồ chia sẻ bí mật vào thí nghiệm sinh.

Mã Hóa DES Chia sẻ khóa Khôi phục khóa

Khóa bí mật: 5911BCDA **Tạo ngẫu nhiên**

Nhập bản rõ/bản mã

Nhóm 1-ATBMTT

Kết quả

10100100011100100011001001011011010000101010110111100110011

Mã hóa

Nhập file để mã hoá

Chuyển

Khóa bí mật:

Nhập bản rõ/bản mã

Kết quả

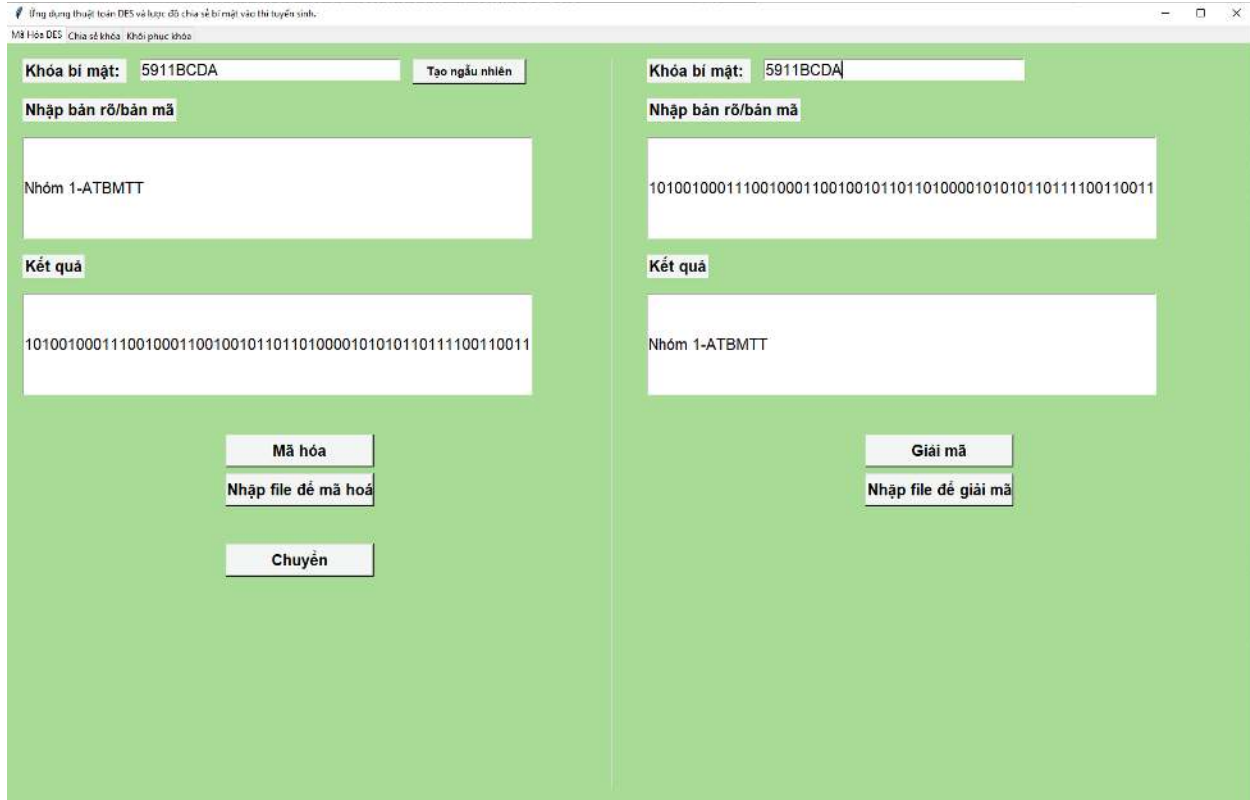
Giải mã

Nhập file để giải mã

Bản mã nhận được(như trong hình trên)

Ngược lại :

Ta xóa chuỗi bản rõ ban đầu đi. Sau đó nhấn giải mã.



Ta nhận lại được chuỗi bản rõ ban đầu nhập vào.

1.5 Thực hiện bài toán

1.5.1

Phân công công việc

Tên sinh viên	Tên công việc
Trần Đức An	Ứng dụng lược đồ chia sẻ bí mật của Lagrange để phân phối khóa
Đoàn Nam Anh	Tìm hiểu mật mã DES
Nguyễn Văn An	
Dư Ngọc Ánh	Nghiên cứu bài toán chia sẻ bí mật của Lagrange

1.5.2**Đoàn Nam Anh và****Nguyễn Văn An – Tìm hiểu hệ mật mã DES****1. Giới thiệu chung về DES**

- Sau những năm 70 của thế kỉ trước, các nhà toán học đã nghiên cứu và tạo ra nhiều phương thức mật mã với tốc độ mã hóa rất nhanh (hàng chục thậm chí hàng trăm kilo Byte trong một giây) và người ta chỉ cần giữ bí mật khóa mã và mã hóa được mọi dữ liệu tùy ý. Đó là một bước tiến vĩ đại của kĩ thuật mật mã. Trong đó mã DES (Data Encryption Standard) là một điển hình của bước tiến này.
- Ngày 13/5/1973 ủy ban quốc gia về tiêu chuẩn của Mỹ công bố yêu cầu về hệ mật mã áp dụng cho toàn quốc . Điều này đã đặt nền móng cho chuẩn mã hóa dữ liệu DES.
- Lúc đầu DES được công ty IBM phát triển từ hệ mã Lucifer, công bố vào năm 1975.
- Sau đó DES được xem như là chuẩn mã hóa dữ liệu cho các ứng dụng.

2. Đặc điểm của thuật toán DES

- DES là thuật toán mã hóa khối, độ dài mỗi khối là 64bit.
- Khóa dùng trong DES có độ dài toàn bộ là 64bit. Tuy nhiên chỉ có 56 bit thực sự được sử dụng; 8 bit còn lại chỉ dùng cho việc kiểm tra.
- DES xuất ra bản mã 64bit

- Thuật toán thực hiện 16 vòng
- Mã hóa và giải mã được sử dụng cùng 1 khóa

3. Mô tả thuật toán.

Thuật toán gồm 3 giai đoạn:

Giai đoạn 1:

Input: bản rõ x có độ dài 64 bit được hoán vị khởi tạo IP thu được chuỗi x_0 .

IP

$x \quad \checkmark \quad x_0 \text{ (64 bit)} = IP(x) = L_0.R_0$

L_0 : 32 bit đầu của x_0 .

R_0 : 32 bit cuối của x_0 .

Bộ chuyển vị IP: Hoán đổi vị trí các bit trong chuỗi đầu vào.

Output: $L_0 R_0$

Giai đoạn 2:

Input: $L_0 R_0$

Lặp 16 vòng

Cho $L_0 R_0 \quad \checkmark \quad \text{Vòng } i: L_i = R_{i-1}$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

Trong đó: K_i là khóa con có độ dài 48 bit.

$$1 \leq i \leq 16.$$

\oplus là phép XOR của 2 chuỗi bit.

Giống bit thì trả về 0

Khác bit thì trả về 1.

K_1 đến K_{16} lập nên một lịch khóa.

Output: $L_{16} R_{16}$.

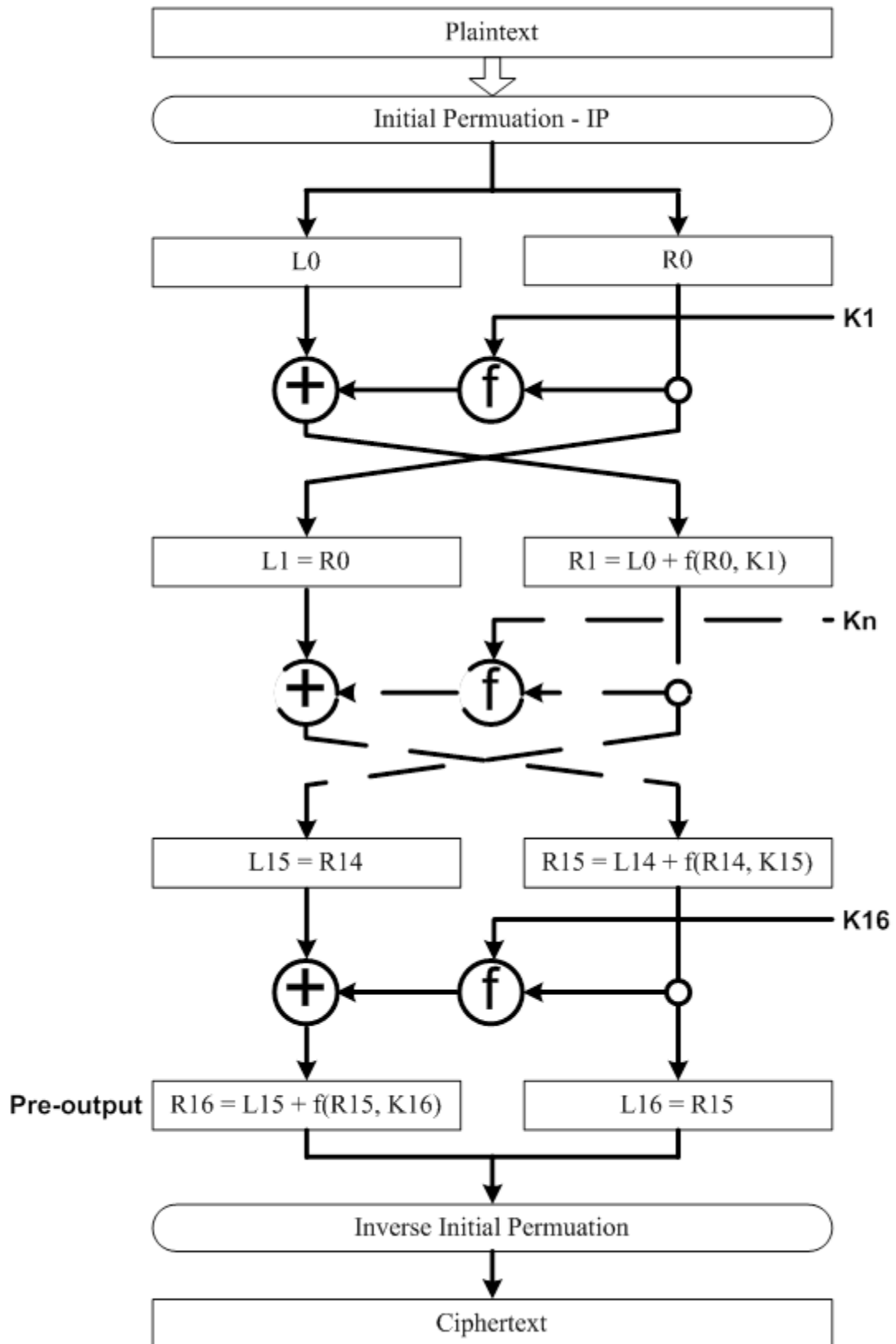
Giai đoạn 3:

Input: $L_{16} R_{16}$.

Tại vòng 16 đổi chỗ R_{16} và L_{16} cho nhau. Ghép R_{16} và L_{16} sau đó cho đi qua hoán vị nghịch đảo của hoán vị IP, thu được bản mã y có độ dài 64 bit.

IP^{-1}

$R_{16} L_{16} \quad \nabla \quad y \text{ (64 bit)}$



IP là một phép hoán vị vị trí của các ký tự trong mỗi từ 64 bit, từ vị trí thứ 1 đến vị trí thứ 64.

Cách hiểu là bit thứ nhất của $IP(x)$ là bit thứ 58 của từ x (có 64 bit), bit thứ hai của $IP(x)$ là bit thứ 50 của x, \dots

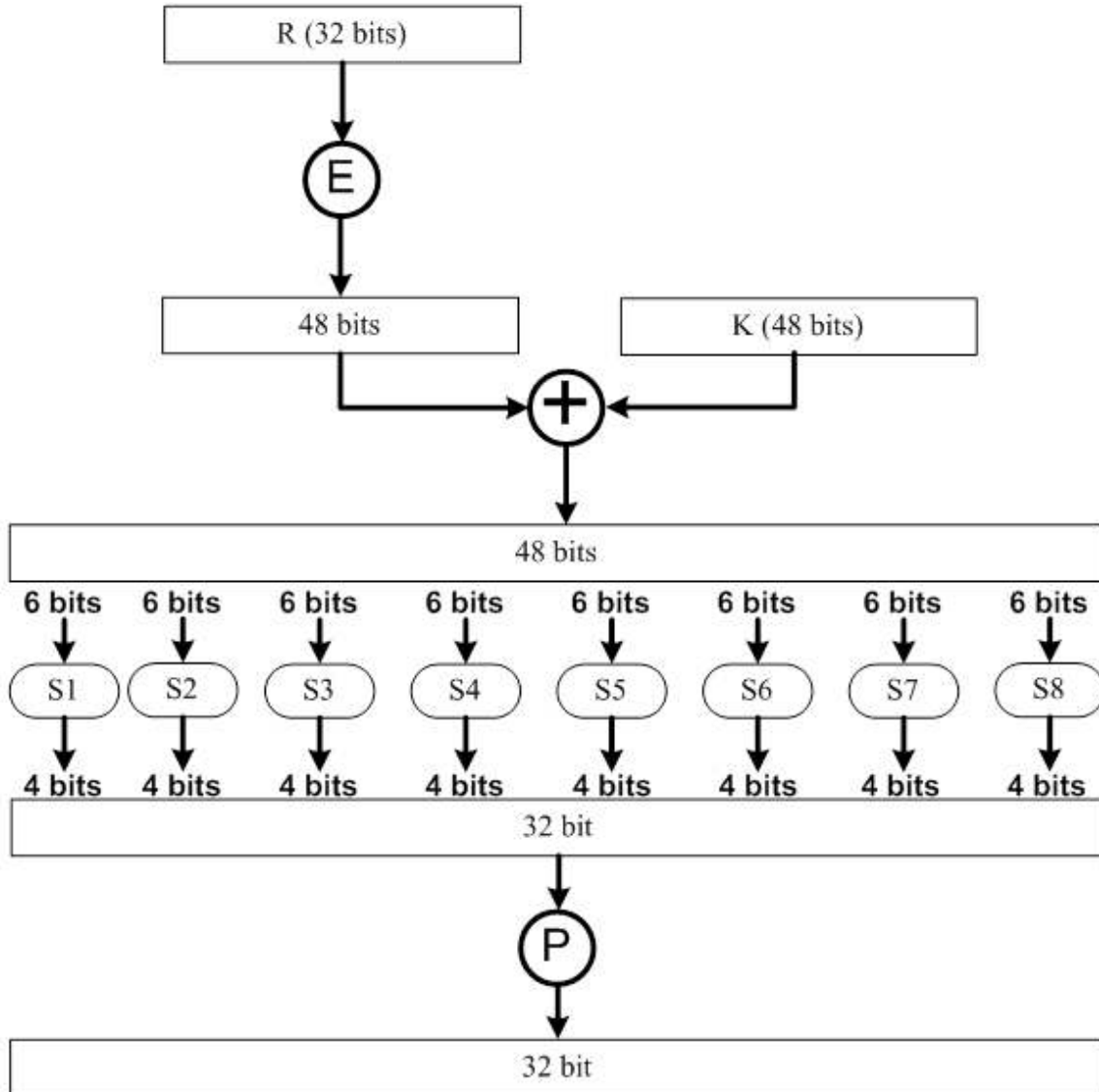
Bảng của phép hoán vị IP và IP^{-1}

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
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

4. Sơ đồ hàm f:

Hàm f lấy đầu vào là 2 từ: R có 32bit và K có 48 bit.

Kết quả đầu ra là từ $f(R,K)$ có 32bit, được xác định bởi sơ đồ sau đây:



- Đầu tiên ra cho R_i đi qua phép mở rộng E, biến $R_i(32) \rightarrow R_i(48)$
- Sau đó cộng bit với khóa K_i tương ứng.
- Kết quả tạo ra được khối B có độ dài 48 bit.
- Chia B thành 8 khối $B = B_1B_2B_3...B_8$. Mỗi khối độ dài 6bit
- Cho các khối B_i đi qua các hộp S_i tạo ra các C_i (4 bit)

- Ghép các khối C_i thành khối C sau đó cho qua P để tạo thành hàm $f(R,K)$ 32bit

Bảng hoán vị P :

P			
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
16	7	20	21

Giải thích các khối B_i và hộp S_i

- Hộp S_i là 1 bảng 4 hàng 16 cột. được đánh số từ 0
- Khối B_i có 6 bit. 2 bit gồm bit đầu và bit cuối tạo thành 1 số.
- Số đó là số thứ tự dòng
- 4 bit ở giữa tạo thành 1 số. Đó là vị trí cột.
- Chiều số dòng , số cột vào bảng S_i tương ứng sẽ tạo ra giá trị của khối C_i

Ví dụ: $B_1 = 011000$

- $b_1b_6 = 00 \rightarrow$ xác định dòng 0
- $b_2b_3b_4b_5 = 1100 \rightarrow$ xác định cột 12
- chiếu vào hộp S_1 với dòng 0 cột 12 sẽ ra 1 giá trị. Đổi giá trị đó về nhị phân sẽ ra giá trị của C_i

Các hộp $S_1 \dots S_8$ như sau:

Hộp S1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Hộp S2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

Hộp S5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

Hộp S6



12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

Hộp S7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

Hộp S8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

5. Phép mở rộng E

E là một phép hoán vị “mở rộng” theo nghĩa là nó biến mỗi từ R 32bit thành từ E(R) bằng cách hoán vị 32bit của R nhưng có 1 số cặp bit được lặp lại để E(R) thành 1 từ có 48 bit.

Cụ thể phép hoán vị “mở rộng” đó được cho bởi bảng sau đây:

E					
3	1	2	3	4	5
2					
4	5	6	7	8	9
8	9	1	11	1	1
		0		2	3

1	1	1	1	1	1
2	3	4	5	6	7
1	1	1	1	2	2
6	7	8	9	0	1
2	2	2	2	2	2
0	1	2	3	4	5
2	2	2	2	2	2
4	5	6	7	8	9
2	2	3	3	3	1
8	9	0	1	2	

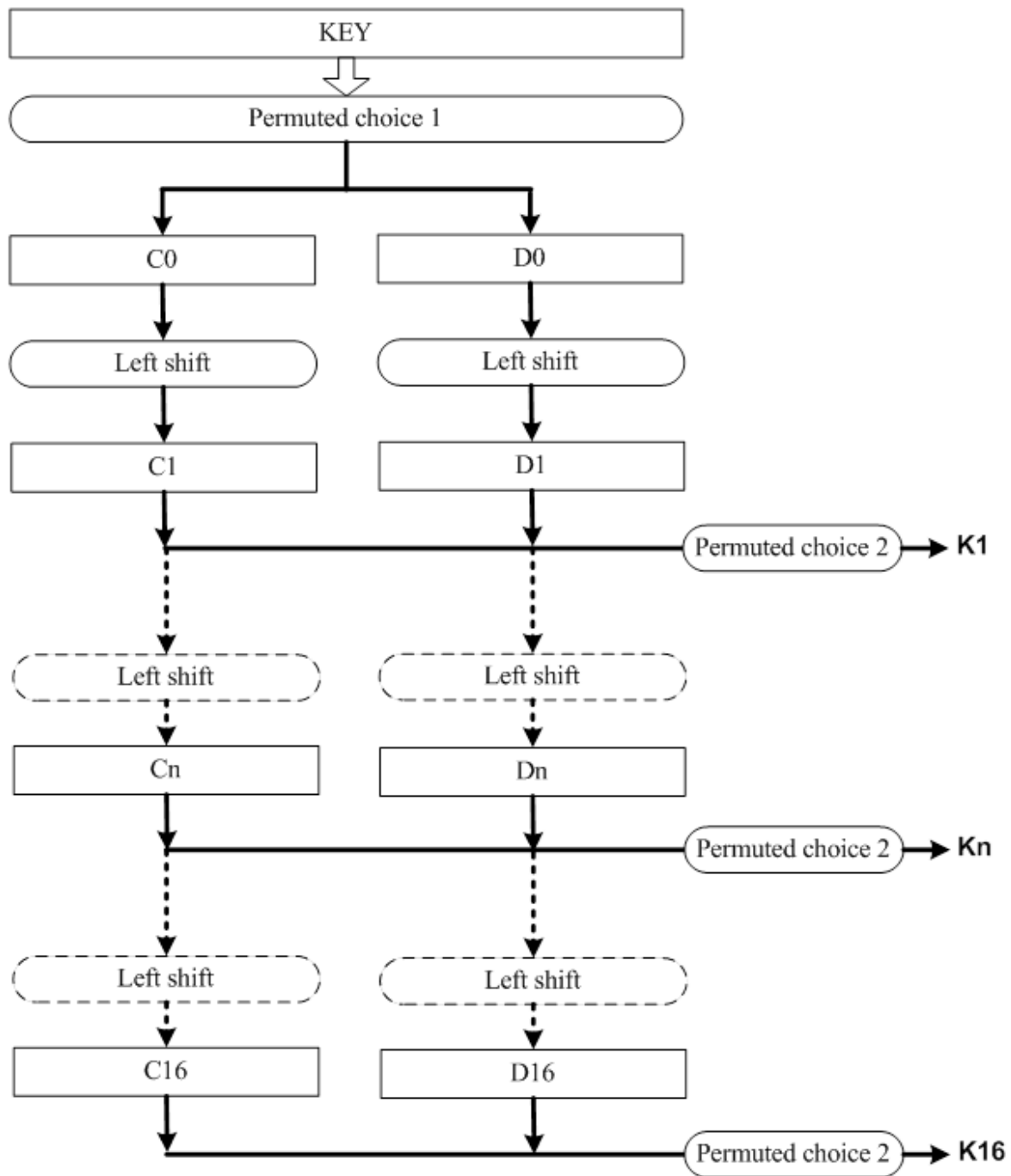
Theo định nghĩa đó, mỗi từ $R = a_1 a_2 a_3 \dots a_{31} a_{32}$ sẽ biến thành

$$E(R) = a_{32} a_1 a_2 a_3 a_4 a_5 a_4 a_5 a_6 a_7 a_8 a_9 \dots a_{32} a_1$$

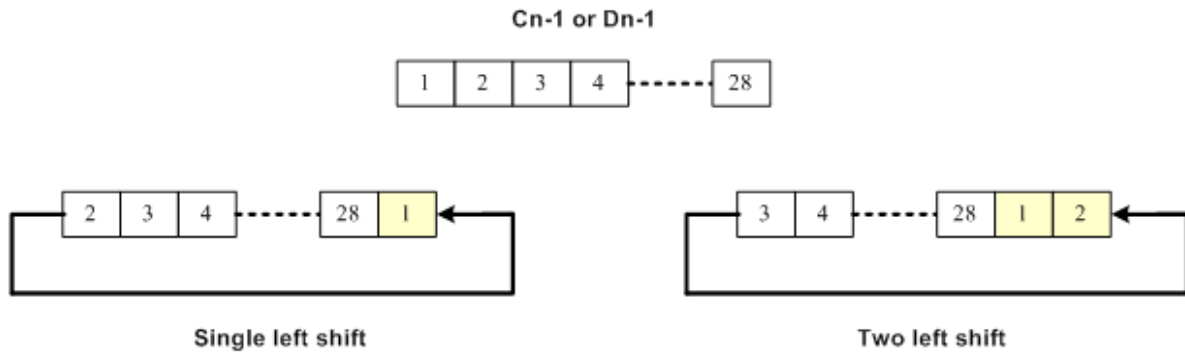
6. Tạo khóa K.

Khóa K(64bit) trong đó:

- 8 bit kiểm tra: 8,16,24,32,40,48,56,64
- 56 bit còn lại dùng để chế khóa.
- Cho K(56) đi qua PC-1.
- Tạo ra C_0 là 28 bit đầu
- D_0 là 28 bit sau.
- Tại mỗi vòng lặp I có: $C_i D_i$ là kết quả của phép dịch trái của các bit từ khối $C_{i-1} D_{i-1}$
- Trong đó: $i = 1, 2, 8, 16$ dịch trái 1 bit, các vòng còn lại dịch trái 2 bit.
- Cho hoán vị PC-2(C_i, D_i) để được khóa K_i



Thuật toán tính khóa vòng



Mô tả thuật toán dịch trái

Bảng PC-1:

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

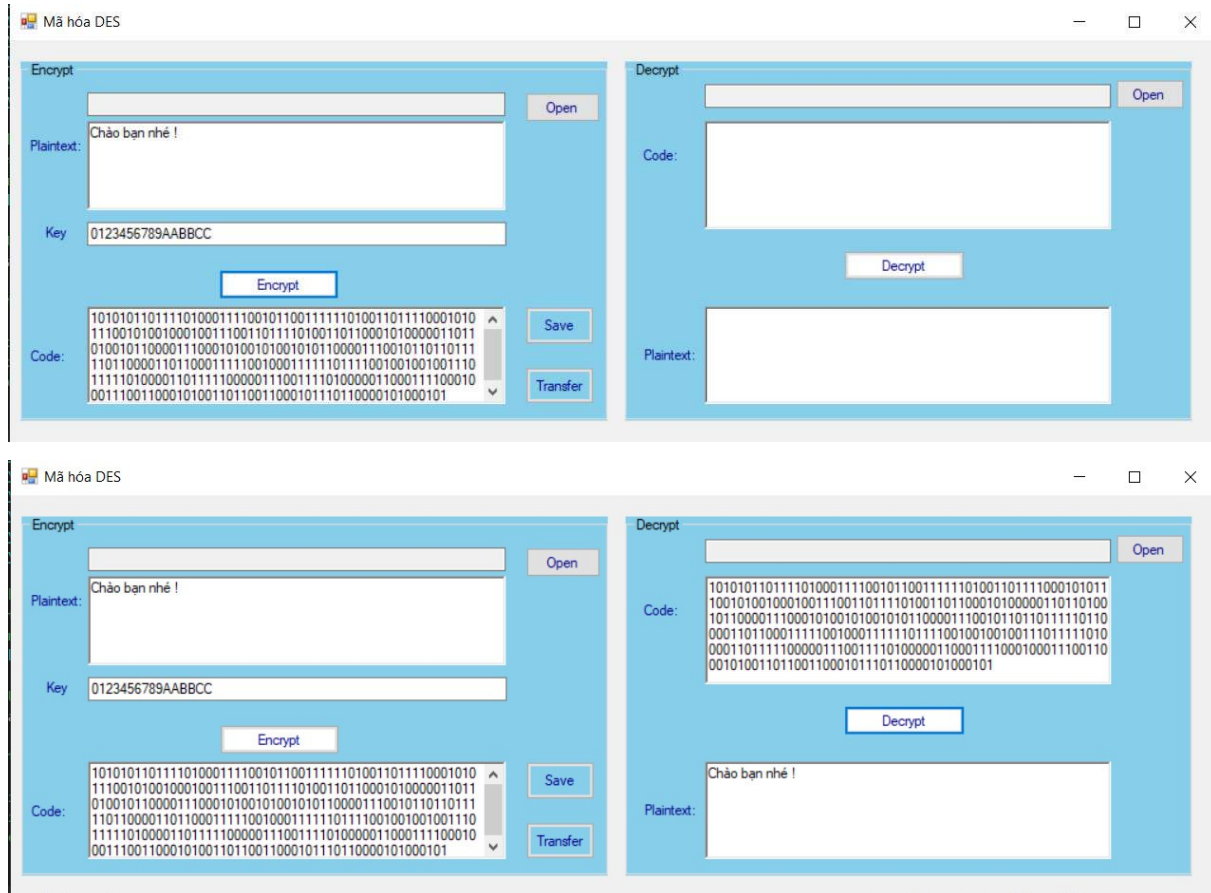
Bảng PC-2:

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

7. Giải mã

- DES là giải mã dùng chung 1 thuật toán vs mã hóa.
- Quá trình giải mã tương tự mã hóa. Tuy nhiên, khóa tại mỗi vòng lặp ngược lại với mã hóa. Tức là từ $K_{16} \rightarrow K_1$.

Chương trình demo bằng C# (Nguyễn Văn An)



Demo chương trình bằng ngôn ngữ Python (Đoàn Nam Anh)

Ứng dụng thuật toán DES và lược đồ chia sẻ bí mật vào thí tuyển sinh.

Mô Hình DES Chia sẻ khóa Khôi phục khóa

Khóa bí mật: 64928351 Tạo ngẫu nhiên

Nhập bản rõ/bản mã

Chào bạn nhé!

Kết quả

0001111100111000100111001100111101100011110111111100100100

Mã hóa

Nhập file để mã hoá

Chuyển

Khóa bí mật: 64928351

Nhập bản rõ/bản mã

0001111100111000100111001100111101100011110111111100100100

Kết quả

Chào bạn nhé!

Giải mã

Nhập file để giải mã

Ứng dụng thuật toán DES và lược đồ chia sẻ bí mật vào thí tuyển sinh.

Mô Hình DES Chia sẻ khóa Khôi phục khóa

Khóa cần chia sẻ 64928351

Giá trị P 41

Số thành viên giữ khóa: 5 Tạo khoá

Nhập giá trị của mỗi thành viên

Thành viên 1: 2

Thành viên 2: 8

Thành viên 3: 20

Thành viên 4: 25

Thành viên 5: 19

Chia sẻ khóa

Nhập 2 số bất kì thuộc vành Z_p

Số thứ nhất: 14 Số thứ hai: 16

Các mảnh khóa được chia cho các thành viên là

Thành viên thứ nhất: 64928443

Thành viên thứ hai: 64929487

Thành viên thứ ba: 64935031

Thành viên thứ tư: 64938701

Thành viên thứ năm: 64934393

Ứng dụng thuật toán DES và lược đồ chia sẻ bí mật vào thí nghiệm sinh.

Mã Họa DES Chia sẻ khóa Khôi phục khóa

Chọn ít nhất 3 thành viên để khôi phục khóa

<input checked="" type="checkbox"/> Thành viên 1:	Giá trị: 2	Giá trị mảnh khóa: 64928443
<input type="checkbox"/> Thành viên 2:	Giá trị: 8	Giá trị mảnh khóa: 64929487
<input checked="" type="checkbox"/> Thành viên 3:	Giá trị: 20	Giá trị mảnh khóa: 64935031
<input checked="" type="checkbox"/> Thành viên 4:	Giá trị: 25	Giá trị mảnh khóa: 64938701
<input type="checkbox"/> Thành viên 5:	Giá trị: 19	Giá trị mảnh khóa: 64934393

Khóa được khôi phục là: 64928351

Khôi phục khóa

Thoát chương trình

1.5.3

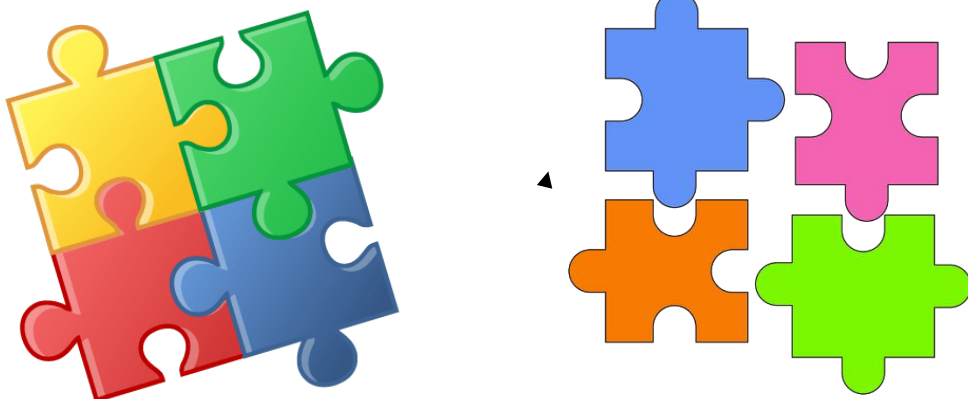
Dư Ngọc Ánh –

Nghiên cứu bài toán chia sẻ bí mật Langrange

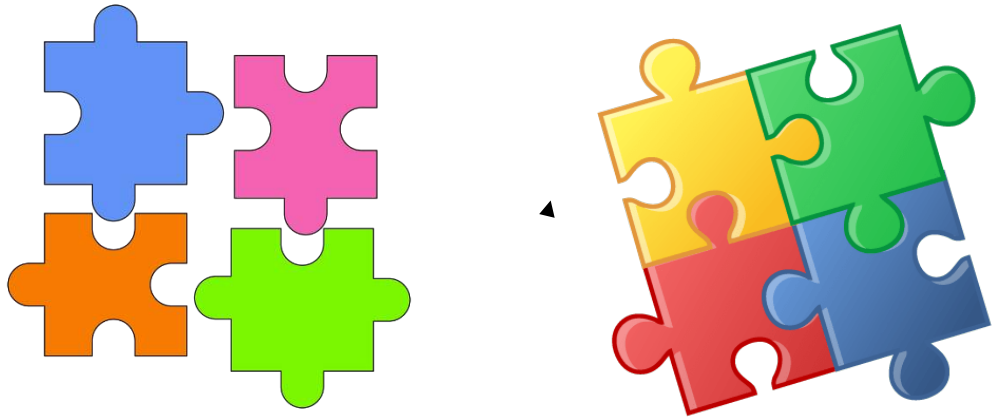
1.5.3.1 Khái niệm chia sẻ bí mật

Thông tin bí mật sẽ được chia thành nhiều mảnh. Các mảnh được chia ra sẽ trao cho các thành viên giữ (mỗi người giữ một hay một số mảnh). Thông tin có thể được xem lại nếu tất cả mọi người giữ mảnh đều đồng ý. Các mảnh sẽ được khớp lại để khôi phục lại tin gốc.

Thông tin bí mật chia thành nhiều mảnh và giao cho các thành viên.



Các mảnh được khớp lại để khôi phục lại tin gốc.



1.5.3.2 Sơ đồ chia sẻ bí mật

Bài toán thực tế: Trong một ngân hàng có một két phải mở hằng ngày. Ngân hàng sử dụng 3 thủ quỹ lâu năm nhưng họ không tin bất kì người nào. Bởi vậy họ cần thiết kế một hệ thống sao cho bất kì 2 thủ quỹ nào cũng có thể mở được két song riêng từng người một thì không thể mở được. Vấn đề này có thể được giải quyết bằng lược đồ chia sẻ bí mật.

1.5.3.2.1 Khái niệm sơ đồ chia sẻ bí mật

Sơ đồ chia sẻ bí mật là một phương thức để chia sẻ bí mật ra nhiều phần sau đó phân phối cho một tập hợp những người tham gia sao cho các tập con trong số những người này được chỉ thị, có khả năng khôi phục lại bí mật bằng cách kết hợp dữ liệu của họ.

Một sơ đồ chia sẻ bí mật là hoàn hảo, nếu bất kì một tập hợp những người tham gia mà không được chỉ định, sẽ không thu được thông tin về bí mật.

1.5.3.2.2 Định nghĩa

Cho t, w là các số nguyên dương, $t \leq w$. Một sơ đồ ngưỡng $A(t, w)$ 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.

Giá trị k được chọn bởi một thành viên đặc biệt được gọi là người phân phối (D). $D \notin P$.

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 mỗi thành viên khác. Một tập con các thành viên ($B \subseteq P$) 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 $|B| \geq t$ thì họ có khả năng tính được k . Nếu $|B| \leq t$ thì không thể tính được k .

Gọi P là tập các giá trị được phân phối khóa K : $P = \{ p_i: 1 \leq i \leq w \}$ K là tập khóa: tập tất cả các khóa có thể.

S tập mảnh: tập tất cả các mảnh có thể.

Sau đây là một sơ đồ ngưỡng được gọi là sơ đồ ngưỡng Shamir.

Giai đoạn khởi tạo:

5. D chọn w phần tử khác nhau và khác 0 trong Z_p và kí hiệu chúng là: $x_i, 1 \leq i \leq w$ ($w \geq p+1$).

Với $1 \leq i \leq w$, D cho giá trị x_i cho p_i . Các giá trị x_i là công khai.

Phân phối mảnh:

6. Giả sử D muốn phân chia khóa $k \in Z_p$. D sẽ chọn một cách bí mật (ngẫu nhiên và độc lập) $t-1$ phần tử $Z_p, a_1 \dots a_{t-1}$
7. Với $1 \leq i \leq w$, D tính $y_i = a(x_i)$, trong đó

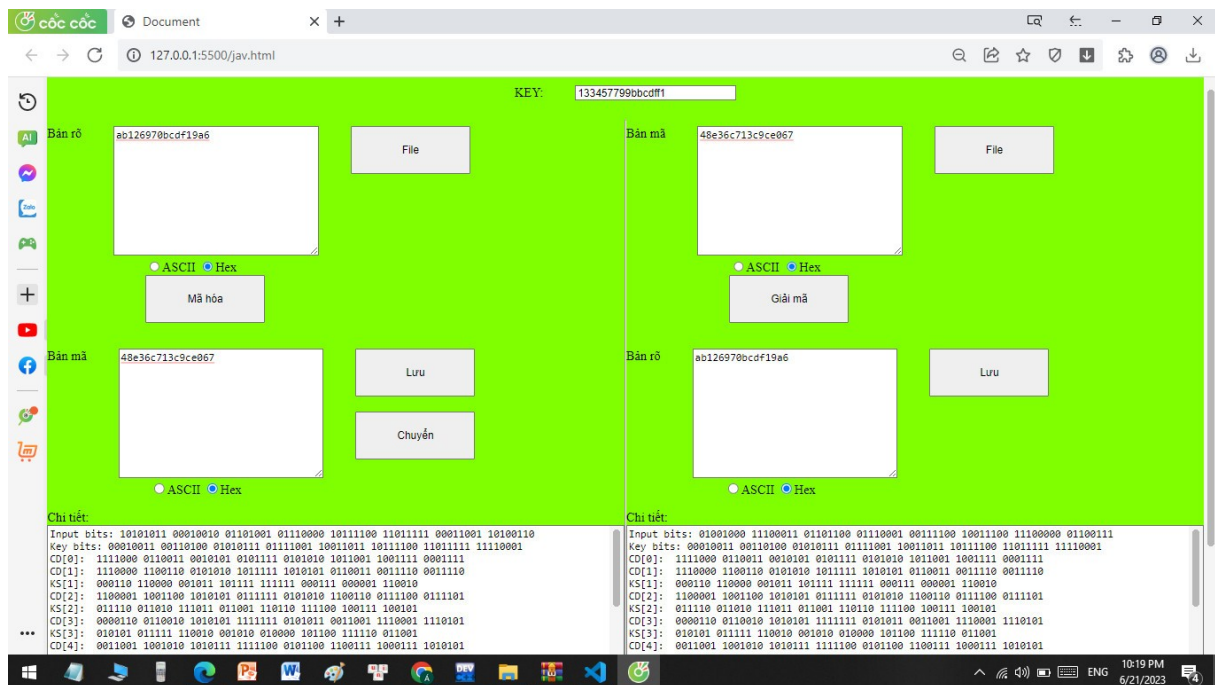
$$a(x) = k + \sum_{i=1}^{t-1} a^i x^i \bmod p$$

8. Với $1 \leq i \leq w$, D sẽ trao mảnh y_i cho p_i

Trong sơ đồ ngưỡng Shamir xây dựng một đa thức ngẫu nhiên $a(x)$ có bậc tối đa là $t-1$. Trong đa thức này hằng số là khóa k . Mỗi thành viên p_i sẽ có một điểm (x_i, y_i) . Ta xét một tập con B gồm t thành viên tạo lại khóa k bằng 2 phương pháp:

- Phép nội suy đa thức
- Công thức nội suy Lagrange

Chương trình demo bằng ngôn ngữ Java scripts (Dư Ngọc Ánh)



2.5.4 : Trần Đức An - Ứng dụng lược đồ chia sẻ bí mật của Lagrange để phân phối khóa

1. Các ứng dụng:

Ta có thể áp dụng thuật toán DES và sơ đồ chia sẻ bí mật vào rất nhiều ứng dụng chẳng hạn trong đấu thầu từ xa, trong mã thẻ ATM, trong thi tuyển sinh, đăng ký bỏ phiếu điện tử... Ở đây ta nghiên cứu một ứng dụng là trong thi tuyển sinh

2. Nội dung thực hiện giải bài toán.

Một số bài toán trong thi tuyển sinh.

2.1. Bài toán bảo mật thông tin đề thi

Hội đồng soạn đề gửi thông tin về nội dung đề thi văn về cho ban giáo dục để tiến hành kiểm duyệt và tiến hành in đề thi.

Vấn đề nảy sinh:

Trên đường truyền, thông tin về đề thi có thể bị kẻ gian thay đổi thông tin, hoặc đánh cắp.

Phương pháp giải quyết:

Sử dụng các kỹ thuật mã hóa DES

2.2. Bài toán thẩm định độ xác thực của đề thi

Trong quá trình gửi thông tin đề thi, để bộ giáo dục có thể cấp quyền gửi thông tin về cho bộ các thành viên trong hội đồng soạn đề thi phải xác thực thông tin của giáo viên soạn đề thi có đáp ứng được yêu cầu của bộ hay không. (có phải là giáo viên được chỉ định soạn đề thi hay không,...)

Vấn đề nảy sinh:

Người trong hội đồng soạn đề có thể cấu kết với thành viên trong bộ giáo dục để tuồn thông tin ra ngoài hoặc thay đổi thông tin đề thi mà không có sự thống nhất của hội đồng soạn đề thi.

Phương pháp giải quyết:

Sử dụng kỹ thuật chia sẻ khóa bí mật để giải mã thông điệp.

2.3. Bài toán ban đăng ký ký vào đề thi (Đã ẩn danh).

Sau khi thẩm định đề thi được gửi, nếu thông điệp hợp lệ thì bộ giáo dục sẽ ký lên thông điệp và gửi lại cho hội đồng soạn đề, xác nhận rằng đề thi phù hợp và xác nhận thông qua.

Vấn đề nảy sinh:

Người trong hội đồng soạn đề thi có thể cấu kết với thành viên trong bộ giáo dục để xin cấp chữ ký cho mình nhiều lần. Như vậy sẽ xảy ra tình trạng bán chữ ký.

Phương pháp giải quyết:

Sử dụng kỹ thuật chia sẻ khóa bí mật để ký.

Chương trình demo bằng ngôn ngữ Java(Trần Đức An)

DES

DES

Bản rõ

Khóa

Bản mã

Bản mã

Khóa

Bản rõ

DES

Bản rõ


Khóa

Bản mã

Bản mã

Khóa

Bản rõ

 DES
 —
□
×

DES

Bản rõ

ABCDEF

Chọn File

Khóa

A049B2BF378631CD

MaHoa

Bản mã

10111110111010000111100000101100101101101101

Sinh Khóa

◀

|||

▶

Lưu

Chuyển

Bản mã

10111110111010000111100000101100101101101101

Chọn File

Khóa

A049B2BF378631CD

GiaiMa

Bản rõ

ABCDEF

Lưu

 DES
 —
□
×

DES

Bản rõ

Chào bạn

Chọn File

Khóa

0123456789ABCDE1

MaHoa

Bản mã

10001111100100110000110111110110000001111110

Sinh Khóa

Lưu

Chuyển

Bản mã

1000111110010011000011011111011000000111111000

Chọn File

Khóa

0123456789ABCDE1

GiaiMa

Bản rõ

Chào bạn

Lưu

Chương 2. Phần kiến thức lĩnh hội và bài học kinh nghiệm

2.1 Nội dung đã thực hiện

3.1.1. Nội dung thực hiện khi nghiên cứu đề tài

- Biết được đặc điểm của hệ mã hóa DES.
- Thuật toán mã hóa, giải mã
- Ưu nhược điểm
- Cách tính hàm f
- Nắm vững được bài toán chia sẻ bí mật
- Sơ đồ chia sẻ bí mật
- Công thức nội suy Lagrange
- Phép nội suy đa thức
- Tìm hiểu bài toán bảo mật đề thi

3.1.2. Các kỹ năng học được.

Sau khi thực hiện xong đề tài, nhóm em học được rất nhiều kỹ năng như: phân tích đề bài, tìm kiếm thông tin, tổ chức phân công công việc, lắng nghe và đặc biệt là kỹ năng làm việc nhóm. Phân tích đề bài giúp cho nhóm em có thể hiểu rõ được nội dung công việc phải làm. Kỹ năng lắng nghe giúp các thành viên trong nhóm hiểu nhau hơn, biết được điểm yếu của nhau để cùng góp ý sửa chữa. Bên cạnh đó kỹ năng tổ chức phân công công việc cũng rất

quan trọng, đảm bảo sự đồng đều giữa các thành viên với nhau để tránh sự phân biệt trong công việc và không bị giám đoạn vì bất kỳ lý do gì.

3.1.3. Các kinh nghiệm đúc rút.

- Tìm hiểu kỹ có chọn lọc các thông tin trên mạng.
- Cần phải nâng cao kỹ năng làm việc nhóm để bài tập lớn hoàn thiện hơn.
- Hiểu được tầm quan trọng của an toàn và bảo mật thông tin.

Sau BTL chúng em có thêm một số kinh nghiệm như:

- Ta có thể áp dụng các giải thuật, cụ thể ở đây là DES và sơ đồ chia sẻ bí mật vào để xử lý rất nhiều ứng dụng chẳng hạn trong đấu thầu từ xa, trong mã thẻ ATM, trong thi tuyển sinh, đăng ký bỏ phiếu...
- Biết sử dụng và áp dụng giải thuật DES vào thực tế, cụ thể ở đề tài này ta đã áp dụng, nghiên cứu một ứng dụng là trong thi tuyển sinh, vậy có một bài toán được đưa ra là: Khi gửi thông tin đề thi, hội đồng soạn đề thi gửi thông tin về hội đồng kiểm duyệt. Trên được truyền, hồ sơ đăng ký của cử tri có thể bị kẻ gian hay đổi thông tin hoặc đánh thông tin đề thi. Ta phải sử dụng các kỹ thuật mã hóa DES để bảo vệ và bảo mật thông tin đề thi.
- Tuy rằng đề tài của chúng em là về kỹ thuật mã hoá DES, song trong quá trình thực hiện bài tập lớn, xen lẫn tới tìm hiểu trên mạng, chúng em có thể thấy rõ những điểm chưa tốt và chưa hoàn thiện của DES so với 1 số hệ mã hoá khác như khoá khá ngắn so với tiêu chuẩn hiện đại ngày nay, hay nó sử dụng hệ thống ECB... so với các hệ thống khác như AES hoặc TripleDES.

2.2 Hướng phát triển.

2.2.1

thi của đề tài

Xác định tính khả

Trong phạm vi bài tập lớn, chúng em đề cập đến bài toán ứng dụng thuật toán DES và lược đồ chia sẻ bí mật vào việc thi tuyển sinh vào đại học ở mức cơ bản nhất.

2.2.2

trong quá trình nghiên cứu.

Những thuận lợi

Nguồn tài liệu phong phú, nhiều ví dụ hay.

Với sự hỗ trợ của open ai và một số công cụ sử dụng trí thông minh nhân tạo cũng giúp cho việc nghiên cứu trở nên dễ dàng hơn.

2.2.3

Những khó khăn

trong quá trình nghiên cứu

Bài toán ứng dụng thuật toán DES và lược đồ chia sẻ bí mật vào thi tuyển sinh là một đề tài có nội dung rộng, mặt khác khả năng am hiểu về hệ thống của nhóm em vẫn còn nhiều hạn chế nên chưa thể triển khai bài toán một cách hiệu quả nhất.

Trong quá trình học trên lớp, tuy được giảng dạy kỹ nhưng so với các thuật toán mã hóa khác như Hill, Affine, ... thì DES thực sự có quá nhiều bước và đồ sộ, khiến chúng em gặp khó khăn trong việc kiểm thử chương trình để tránh sai sót.

2.2.4

Hướng phát triển

Trong thời gian sắp tới, nhóm sẽ tiếp tục xây dựng tích hợp các chức năng ứng dụng để cho ra một ứng dụng thực thi bài toán ứng dụng thuật toán DES và lược đồ chia sẻ bí mật vào thi tuyển sinh với đầy đủ tính năng.

Chương 3. Kết luận

Các ứng dụng trên mạng máy tính ngày càng trở lên phổ biến, thuận lợi và quan trọng thì yêu cầu về an toàn mạng, về an ninh dữ liệu càng trở lên cấp bách và cần thiết.

Thuật toán mã hóa được ứng dụng trong rất nhiều lĩnh vực như: xác thực người dùng, chữ ký số, mã hóa và xác thực dữ liệu...

Kết quả của bài toán của em gồm 2 phần chính:

1. Tìm hiểu lý thuyết về mật mã

Nghiên cứu lý thuyết về mật mã, thuật toán DES và lược đồ chia sẻ bí mật.

0. Phản ứng dụng

Bài toán đề cập đến vấn đề ứng dụng thuật toán DES và lược đồ chia sẻ bí mật vào thi tuyển sinh. Phần ứng dụng chưa được áp dụng trong thực tế do đó không thể tránh khỏi những thiếu sót, rất mong được sự góp ý của giáo viên để ứng dụng được hoàn thiện hơn.

Chúng em xin chân thành cảm ơn !

Tài liệu tham khảo

1. Phan Đình Diệu (2002). Lí thuyết mật mã và an toàn thông tin. NXB Đại học Quốc gia Hà Nội.
2. Lê Thị Sinh (2010) Nghiên cứu một số mô hình đảm bảo an ninh cơ sở dữ liệu và thử nghiệm ứng dụng, luận văn thạc sĩ Công nghệ thông tin, trang 28-25, Trường Đại học công nghệ - Đại học Quốc gia Hà Nội.
3. Dương Anh Đức (2008) Mã hóa và ứng dụng. Nhà xuất bản Đại học Quốc gia TPHCM.
4. Nguyễn Viết Kính (2007) Mã hóa. Bài giảng cho học viên cao học Trường Đại học Quốc gia Hà Nội.

5. Bảo mật thông tin, mô hình và ứng dụng, Nguyễn Xuân Dũng, 2007, Nhà xuất bản thống kê.
6. Douglas (1994) Mật mã lí thuyết và thực hành. Người dịch Nguyễn Bình.

