

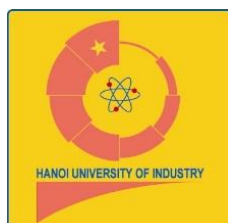


Nhom9 Bao Cao BTL Atbmtt 20221 IT6001001

tiếng anh cơ khí cơ bản 3 (Trường Đại học Công nghiệp Hà Nội)

TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI
KHOA CÔNG NGHỆ THÔNG TIN

=====***=====



BÁO CÁO BÀI TẬP LỚN
MÔN HỌC: AN TOÀN VÀ BẢO MẬT THÔNG TIN
ĐỀ TÀI: Ứng dụng thuật toán DES
và lược đồ chia sẻ bí mật vào thi
tuyển sinh

GVHD: **ThS. Trần Phương Nhung**

Nhóm: 9

Thành viên:	1. Vũ Minh Tân	- 2019606159
	2. Phạm Hồng Thái	- 2019601279
	3. Hoàng Văn Thắng	- 2019600645
	4. Trần Mạnh Thắng	- 2019603424
	5. Vương Toàn Thắng	- 2019605136

LỜI MỞ 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 vấn 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 DIES 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.

MỤC LỤC

Chương 1. Tổng Quan Về Đề Tài	4
1.1 Giới thiệu về đề tài	5
1.2 Sơ lược về thuật toán DES	5
1.2.1 Mô tả về thuật toán Des	6
1.3 Các vấn đề xung quanh DES	8
1.3.1 DES trong thực tế	8
1.3.2 Một vài kết luận về mã DES	8
1.4 Tổng quan về chia sẻ bí mật	10
1.4.1 Khái niệm về chia sẻ bí mật	10
1.4.2 Mục đích chia sẻ bí mật	10
1.4.3 Sơ đồ chia sẻ bí mật	10
1.4.4 Khái niệm “ sơ đồ chia sẻ bí mật”	11
1.4.5 Định nghĩa sơ đồ chia sẻ bí mật hoàn thiện	11
1.5 Quy trình thực hiện	12
1.5.1 Các bước thực hiện	12
Chương 2. Kết Quả Nghiên Cứu	14
2.1 Giới thiệu	14
2.2 Thuật toán của chương trình	14
2.2.1 Giao diện chương trình demo	14
2.2.2 Luồng hoạt động của chương trình	14
2.3 Thiết kế và cài đặt chương trình demo	15
2.3.1 Chương trình demo bằng ngôn ngữ Javascript	15
2.3.2 Chương trình demo bằng ngôn ngữ PHP	19
2.3.3 Chương trình demo bằng ngôn ngữ C#	23
2.3.4 Chương trình demo bằng ngôn ngữ Python	24
2.3.5 Chương trình demo bằng ngôn ngữ java	35
2.4 Phân công công việc	40
Chương 3. Kiến Thức Lĩnh Hội Và Bài Học Kinh Nghiệm	41
3.1 Nội dung đã thực hiện	41

3.1.1 Các kiến thức đã lĩnh hội	41
3.1.2 Các kỹ năng đã tiếp thu	41
3.1.3 Bài học kinh nghiệm	41
3.2 Hướng phát triển	43
3.2.1 Tính khả thi của đề tài	43
3.2.2 Những thuận lợi và khó khăn nhóm gặp phải	43

Chương 1. Tổng Quan Về Đề Tài

1.1 Giới thiệu về đề tài

Trong những năm gần đây, việc để lộ đề thi trước các kì thi tuyển sinh không còn quá xa lạ nữa. Đề thi bị lộ ảnh hưởng tới rất nhiều tới việc xét tuyển học sinh, sinh viên vào các trường. Để khắc phục điều đó, ta có thể áp dụng thuật toán “DES và sơ đồ chia sẻ bí mật vào thi tuyển sinh.

thuật toán DES và sơ đồ chia sẻ bí mật được ứng dụng rất nhiều chẳng hạn trong đấu thầu từ xa, trong mã thẻ ATM, trong thi tuyển sinh...

Ở đây ta nghiên cứu một ứng dụng là trong thi tuyển sinh, vậy có một bài toán được đưa ra là: Trong một kì 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 thi trên mạng máy tính sao cho đảm bảo về tính bảo mật. Cùng với đó, cần phải có nhiều người có các mảnh khóa ghép vào với nhau mới tạo nên một khóa chính. Điều này tạo nên sự an toàn về việc bảo mật thông tin vì lúc mở đề ra sẽ có nhiều người chứng kiến. Nếu đề thi bị lộ ra thì chỉ có nhóm người đó đưa ra. Lúc đó vấn đề tìm đối tượng kỉ luật sẽ dễ dàng hơn.

1.2 Sơ lược về thuật toán 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 kỹ thuật

mật mã. Trong đó mã DES (Data Encryption Standard) là một điển hình của bước tiến này.

1.2.1 Mô tả về thuật toán Des

DES mã hóa một chuỗi bit x :

Khóa k độ dài 64 bit trong đó có 56 bit dùng để mã hóa và 8 bit để kiểm tra.

Bản mã y nhận được cũng là một chuỗi bit có độ dài như bản rõ x . Thuật toán

1. Với bản rõ cho trước x , một chuỗi bit x_0 sẽ được tạo ra bằng cách hoán vị các bit của x theo phép hoán vị cố định ban đầu IP. Ta viết : $x_0 = IP(X) = L_0R_0$, trong đó L_0 gồm 32 bit đầu và R_0 là 32 bit cuối.
2. Sau đó tính toán 16 lần lặp theo một hàm xác định. Ta sẽ tính được L_iR_i , $1 \leq i \leq 16$ theo quy tắc sau:

$$L_i = R_{i-1}$$

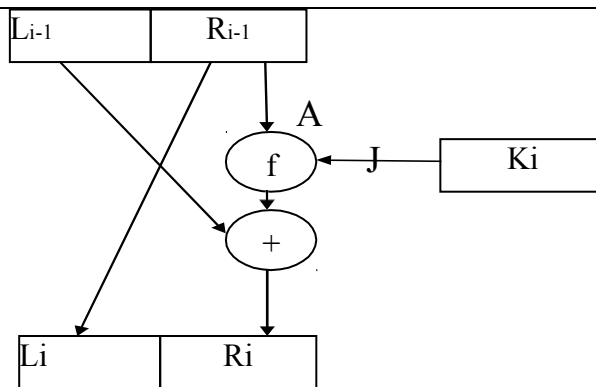
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

Trong đó: \oplus ký hiệu cộng theo modulo 2 của 2 chuỗi bit.

f là một hàm mà của R_{i-1} , K_i mô tả sau.

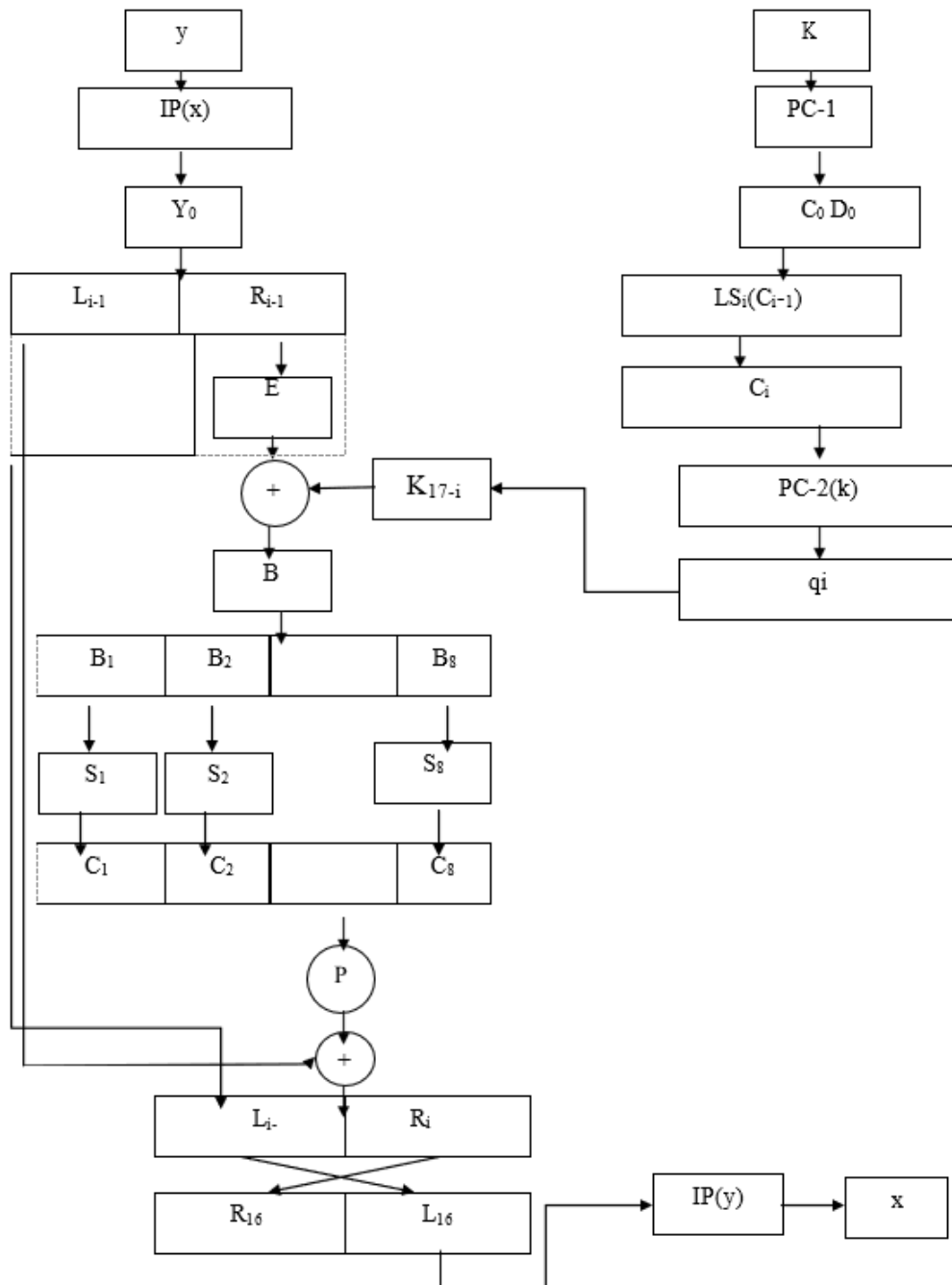
K_i là các chuỗi bit độ dài 48 bit được tính như hàm của khóa k . (Trên thực tế mỗi K_i là một phép chọn hoán vị bit trong k).

3. Áp dụng phép hoán vị ngược IP^{-1} cho chuỗi bit $R_{16}L_{16}$ ta thu được bản mã y . Tức là $y = IP^{-1}(R_{16} L_{16})$.



Giải mã DES

Tương tự như mã hóa, để giải mã một chuỗi ký tự đã bị mã hóa ta cũng làm tương tự theo các bước trên, tuy nhiên hệ thống khóa lúc này đã được tạo theo chiều ngược lại.



1.3 Các vấn đề xung quanh DES

1.3.1 DES trong thực tế

Ngay cả khi việc mô tả DES khá dài dòng thì DES được thực hiện rất hiệu quả trong cả phần cứng lẫn phần mềm. 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 k_1, k_2, \dots, k_{16} tất cả được thực hiện trong thời gian ngắn bởi bảng tìm kiếm trong phần mềm hoặc cách nối dây cứng chúng vào một mạch. Những thi hành phần cứng hiện thời có thể đạt tốc độ mã hóa cực nhanh, công ty thiết bị số thông báo tại CRYPTO'92 rằng họ vừa mới chế tạo được một chip với 50k Transistors có thể mã hóa với tốc độ 1GB/s sử dụng một đồng hồ tốc độ là 250MHz. Giá của chip này khoảng 300USD. Năm 1991 có 45 phần cứng và chương trình cài sẵn thi hành DES đã được ủy ban tiêu chuẩn quốc gia Mỹ phê chuẩn.

Một ứng dụng rất quan trọng của DES là ứng dụng vào việc giao dịch ngân hàng sử dụng các tiêu chuẩn được hiệp hội các ngân hàng Mỹ phát triển. DES được sử dụng để mã hóa các con số, nhận dạng các nhân (PIN) và trao đổi tài khoản được máy thu ngân tự động thực hiện (ATM). DES cũng được clearing House Interbank System (CHIPS) sử dụng để trao đổi có liên quan đến trên $1,5 \cdot 10^{12}$ USD/ tuần.

DES cũng được sử dụng rộng rãi trong các tổ chức chính phủ như: Bộ năng lượng, Bộ tư pháp và hệ thống phản chứng liên bang.

1.3.2 **Một vài kết luận về mã DES**

Có rất nhiều phương pháp mã hóa để đảm bảo an toàn dữ liệu. Để đánh giá tính ưu việt một giải thuật mã hóa, người ta thường dựa vào các yếu tố: Tính bảo mật, độ phức tạp, tốc độ thực hiện giải thuật và vấn đề phân khóa trong môi trường nhiều người sử dụng.

Hiện nay phương pháp mã hóa DES được sử dụng rộng rãi nhất. Các chip chuyên dụng được DES thiết kế nhằm tăng tốc độ xử lý của DES. Rất nhiều nhà toán học ,tin học đã bỏ nhiều công nghiên cứu trong nhiều năm nhằm tìm cách phá vỡ DES (tức là tìm ra cách giải mã trong khoảng thời gian ngắn hơn thời gian cần để thử lần lượt tất cả các khóa). Ngoại trừ việc tìm ra 4 khóa yếu và 12 khóa tương đối yếu cho tới nay chưa có một thông báo nào về việc tìm ra cách phá vỡ phương pháp mã hóa này. Để phá vỡ DES bằng phương pháp “ vét cạn” thử tất cả các khóa trong không gian khóa cần có một khoản tiền lớn và đòi hỏi một khoảng thời gian dài.

Nhược điểm của DES: nó là thuật toán mã hóa đối xứng. Khi phương pháp này mới được tìm ra ý tưởng thực hiện 50000 tỷ phép mã hóa cần thiết để vượt mặt DES bằng cách thử lần lượt các khóa có thể là điều không thể làm được nhưng ngày nay với sự phát triển mạnh của phần cứng liệu độ dài 56 bit đã đủ chưa? Và các phép thay thế đã đủ phức tạp chưa? Để đạt được độ an toàn thông tin như mong muốn, đó là vấn đề người ta vẫn đang bàn luận.

Tuy vậy, DES đã được phân tích kỹ lưỡng và công nhận là vững chắc. Các hạn chế của nó đã được hiểu rõ và có thể xem xét trong quá trình thiết kế và để tăng độ an toàn hơn, ngày

nay các hệ thống mã hóa sử dụng DES mở rộng (3DES), được ứng dụng rộng rãi. Với DES mở rộng khóa có thể là 128 bit,...độ lớn khối có thể là 128 bit. Do vậy độ an toàn mở rộng của DES cao hơn rất nhiều.

1.4 Tổng quan về chia sẻ bí mật

1.4.1 Khái niệm về chia sẻ bí mật

Thông tin cần giữ bí mật được chia thành nhiều mảnh và giao cho nhiều người, mỗi người giữ một mảnh. Thông tin này có thể được xem lại, khi mọi người giữ các mảnh đồng ý. Các mảnh khớp lại để được tin gốc.

Thông tin cần giữ bí mật được chia thành nhiều mảnh và chia cho mỗi thành viên tham gia nắm giữ. Để lấy được thông tin gốc thì phải ghép tất cả mảnh ghép lại với nhau.

1.4.2 Mục đích chia sẻ bí mật

Đảm bảo trao đổi thông tin dữ liệu an toàn, thông tin bảo mật được an toàn

Phòng ngừa hiện tượng đánh cắp dữ liệu

Tránh hậu quả dính tới pháp luật

1.4.3 Sơ đồ chia sẻ bí mật

Bài toán thực tế: Trước các kỳ thi tuyển sinh, tất cả các bộ đề sẽ được niêm phong và khóa lại. Để đảm bảo tính bảo mật, người ta cần thiết kế một hệ thống sao cho phải có 3 người mới mở được khóa, 1 hoặc 2 người sẽ không thể mở được khóa. Vấn đề này có thể được giải quyết bằng lược đồ chia sẻ bí mật.

1.4.4 **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. Cấu trúc truy nhập và sơ đồ chia sẻ bí mật

1.4.5 **Định nghĩa sơ đồ chia sẻ bí mật hoàn thiện**

Một sơ đồ chia sẻ bí mật hoàn thiện thể hiện cấu trúc truy nhập Γ là phương pháp chia sẻ khóa K cho một tập w thành viên (được kí hiệu là P) thỏa mãn 2 tính chất sau:

1. Nếu một tập con hợp thức các thành viên BP góp chung các mảnh của họ thì họ có thể xác định được giá trị của K .
2. Nếu một tập con không hợp thức các thành viên BP góp chung các mảnh của họ thì họ không thể xác định được khóa k .

Ví dụ:

Trong sơ đồ Shamir $A(t, m)$ thể hiện cấu trúc truy nhập sau: $\Gamma = \{BP : /B/\}$

Vậy sơ đồ Shamir là sơ đồ chia sẻ bí mật hoàn thiện.

Chú ý: “Tập trên” của một “tập hợp thức” sẽ là “tập hợp thức”

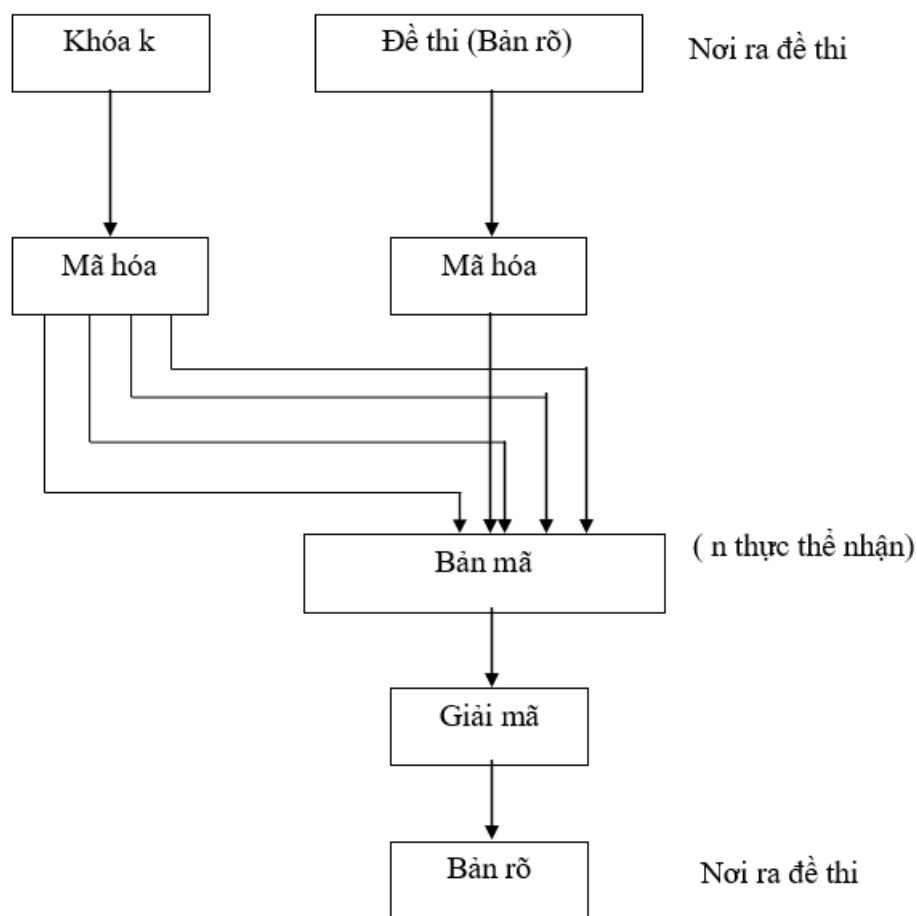
Giả sử $B \vdash$ và BCP, giả sử tập con C muốn K

Vì B là một tập con hợp thức nên nó có thể xác định được K.

Tập con C có thể xác định được khóa K bằng cách bỏ qua các mảnh (tin) của các thành viên trong B, C.

Tức là: Nếu $B \vdash$ và BCP thì $C \vdash$

1.5 Quy trình thực hiện



1.5.1 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 $(v_j, f(v_j))$
 - 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 ký tự sang Hexa sau đó dùng thuật toán DES để mã hóa.

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

Gửi bản tin: Dựa vào lược đồ chia sẻ bí mật chìa khóa k thành 2 mảnh rời nhau $k_1, k_2 : k_1 + k_2 = k$. Sau đó gửi k_1 cho n thực thể (các địa chỉ thi). Quy định đến đúng giờ G vụ Đào tạo gửi nốt k_2 cho n thực thể đó trên cơ sở k_1, k_2 . 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).

Chương 2. Kết Quả Nghiên Cứu

2.1 Giới thiệu

- Tên đề tài nghiên cứu: Ứng dụng DES và lược đồ chia sẻ khóa bí mật vào thi tuyển sinh
- Các bước thực hiện triển khai đề tài bao gồm:
 - Nghiên cứu nội dung kiến thức.
 - Tìm hiểu thuật toán.
 - Thiết kế và cài đặt chương trình bằng các ngôn ngữ khác.
- Hình thức sản phẩm: Sản phẩm ứng dụng.
- Kết quả đạt được: Nghiên cứu, cài đặt demo thuật toán.

2.2 Thuật toán của chương trình

2.2.1 Giao diện chương trình demo

The screenshot displays two side-by-side panels for a DES encryption/decryption demo. The left panel is titled 'Server' and the right panel is titled 'Client'. Both panels have a similar layout: an 'Input:' text area with a 'Choose File' button and 'No file chosen' text; a 'Key:' text input with a 'Generate Key' button; an 'Output:' text area with a 'Save File' button; and a central action button ('Encrypt' for Server, 'Decrypt' for Client). The Server panel also includes a 'Share' button at the bottom right.

2.2.2 Luồng hoạt động của chương trình

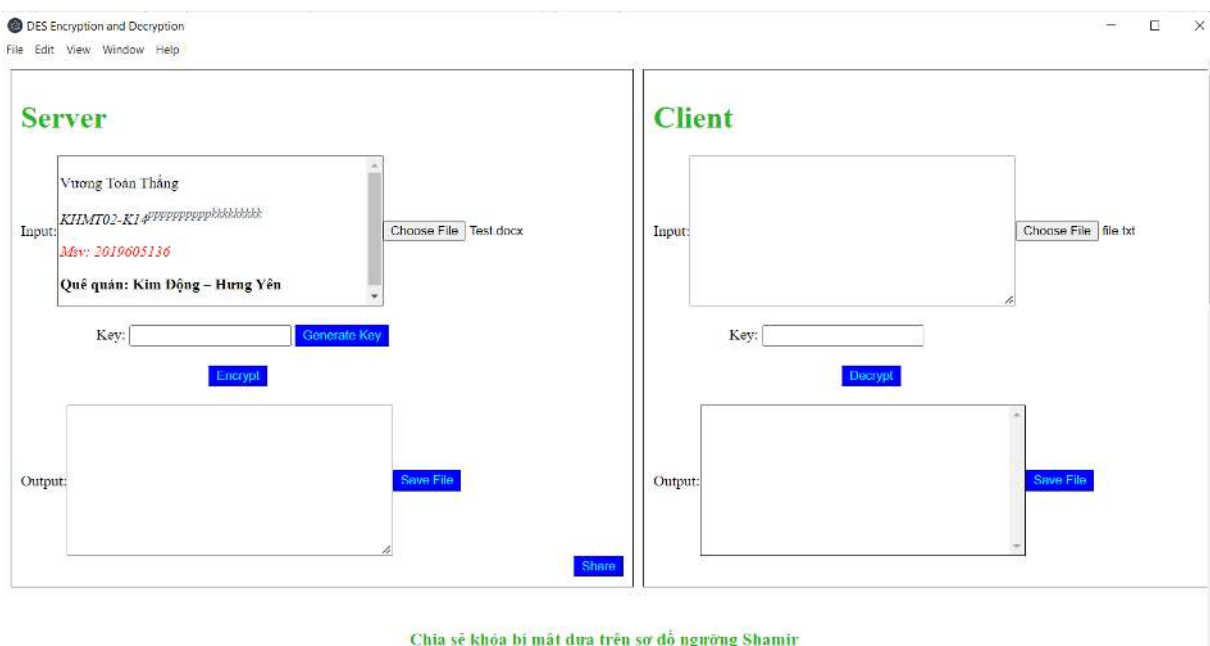
- Nhập, mở file txt hoặc docx vào ô input phía Server
- Nhấn generate key hoặc nhập khóa trực tiếp vào ô key
- Nhấn vào nút Encrypt để mã hóa dữ liệu
- Nhấn vào nút share để chia sẻ bản mã từ Server qua input ở phía Client
- Nhập key vào ô key ở phía Client

- Nhấn vào nút Decrypt để giải mã
- Ấn lưu để lưu tài liệu về

2.3 Thiết kế và cài đặt chương trình demo

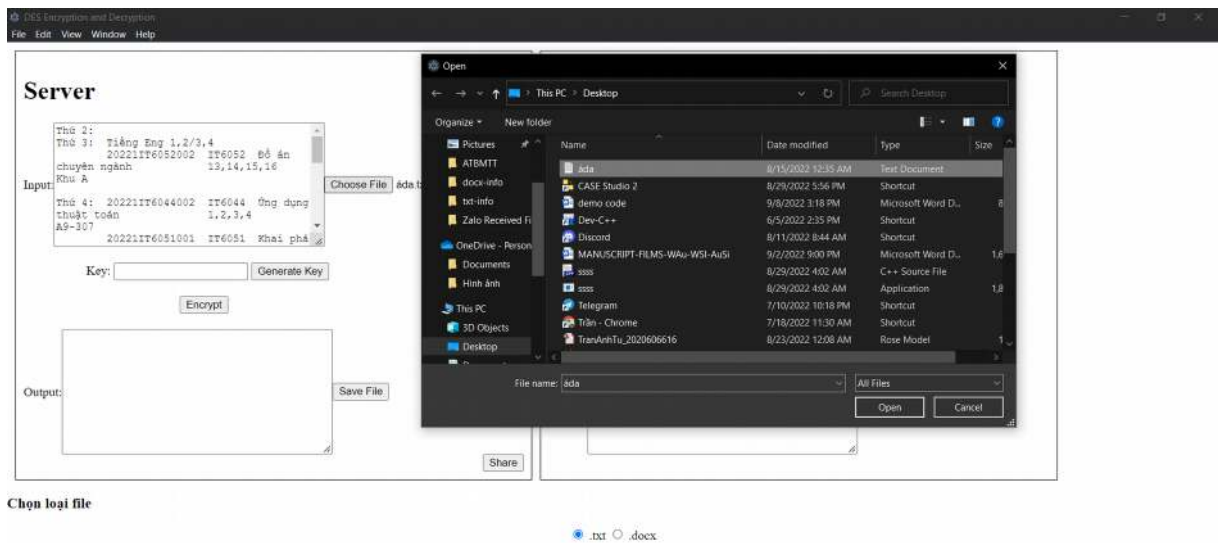
2.3.1 Chương trình demo bằng ngôn ngữ Javascript(Vương Toàn Thắng)

- Giao diện chính

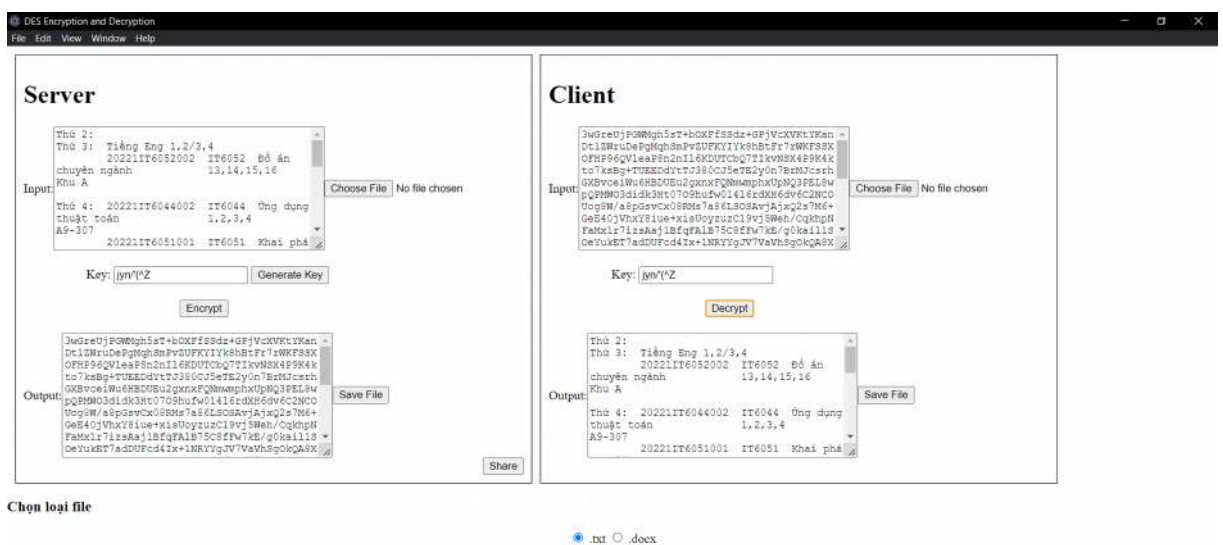


- Nhập thông tin mã hóa vào input → ấn generate key để tạo khóa ngẫu nhiên → ấn encrypt để mã hóa và bản mã sẽ nhận được ở ô output.
- Nhấn nút share để chia sẻ bản mã từ Output Server qua Input bên Client → nhập khóa trùng với khóa giải mã → ấn Decrypt để giải mã

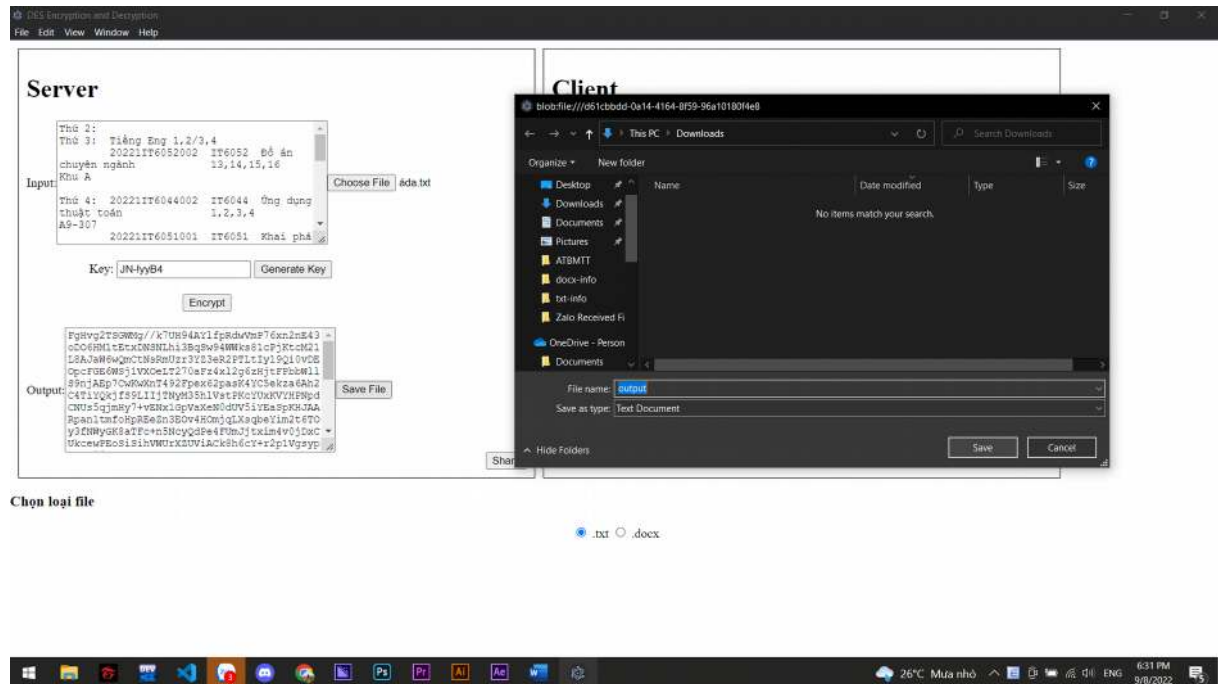
- Chọn Choose file ☐ chọn file txt, dữ liệu file txt sẽ được đưa ra input phía server.



- Các bước tiếp theo sẽ giống như thao tác nhập tay



- Có thể save lại bản mã bằng cách click nút save file ở server và bản rõ bằng cách click vào nút save file ở client



2.3.2 Chương trình demo bằng ngôn ngữ PHP(Trần Mạnh Thắng)

_Giao diện bắt đầu của chương trình:

Trần Mạnh Thắng

MSV: 2019603424 Lớp:20221IT6001001 Khóa:K14

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

Chia sẻ khóa

Khôi phục khóa

Mã hóa DES

- Giao diện chia sẻ khóa:

Click “Chia sẻ khóa”trên giao diện chính,sau đó nhập vào khóa cần chia sẻ,số thành viên giữ khóa,số thành viên tối thiểu để mở khóa và giá trị p sau đó click “Chia sẻ”sẽ ra được như sau:

Chương trình chia sẻ khóa bí mật dựa vào sơ đồ tín ngưỡng Shamir

Khóa cần chia sẻ

10

Số thành viên giữ khóa

5

Số thành viên tối thiểu để mở khóa

3

Giá trị p

17

Chia sẻ

#	x_i	p_i
1	1	1
2	2	9
3	3	0
4	4	8
5	5	16

-
- Khóa được chia sẻ thành công là 10
 - Giao diện khôi phục khóa:

Click “Chia sẻ khóa” trên giao diện chính, sau đó nhập vào số thành viên tối thiểu để mở khóa, nhập xi và pi của từng người và giá trị p (phải là số nguyên tố) như ở chia sẻ khóa sau đó click “Khôi phục khóa” ta sẽ thu được khóa cần tìm như lúc đầu:

Chương trình chia sẻ khóa bí mật dựa vào sơ đồ tín ngưỡng Shamir

Số thành viên tối thiểu để mở khóa

Nhập xi của từng người cách nhau bằng dấu cách

Nhập Pi của từng người cách nhau bằng dấu cách

Giá trị p

Khóa: 10

- Khôi phục khóa thành công và ta tìm được khóa ban đầu là 10

- Giao diện mã hóa DES: Click “Mã hóa DES”trên giao diện chính,sau đó

Chúng ta có thể mã hóa và giải mã các file văn bản ,file text và file word

Nhập văn bản chúng ta sẽ gõ trực tiếp vào ô nhập thông tin:

Mã hóa DES

Nhập thông tin

tran manh thang

File .txt

Chọn tệp Không có tệp nào được chọn

File .doc

Chọn tệp Không có tệp nào được chọn

Nhập khóa

Mã hóa

Hoặc ta có thể xử lý file txt và doc bằng cách click vào “chọn tệp” file .txt hoặc file .doc ,sau đó chọn file tương ứng rồi click vào “open”

Name	Date modified	Type	Size
9_TranManhThang_2019603424	1/4/2023 10:58 PM	File folder	
9_TranManhThang_2019603424	1/5/2023 9:05 PM	WinRAR archive	11,556
Des_Doc	1/4/2023 10:55 PM	Microsoft Word D...	12
Des_Text	1/4/2023 9:21 PM	Text Document	1
Nhom9	1/5/2023 8:08 PM	Microsoft Word D...	5,497
Nhom9_BaoCao	12/28/2022 6:51 PM	Microsoft Word D...	5,445

< >

ne: Des_Doc

Tất cả Tệp tin

Open Cancel

_ Nhập tiếp khóa vào ô “Nhập khóa” sau đó click vào “Mã hóa” để được bản mã như hình bên dưới

Mã hóa DES

Nhập thông tin
tran manh thang

File .txt
Chọn tệp Không có tệp nào được chọn

File .doc
Chọn tệp Không có tệp nào được chọn

Nhập khóa
12345678

Mã hóa

Bản mã
83abeb38c4b55e476e26f4cf623bb7ba

Nhập khóa

Giải mã

_ Giải mã ngược lại bản mã vừa thu được bằng cách nhập khóa vào ô “nhập khóa” sau đó click “giải mã” để thu được bản mã ban đầu:

Mã hóa DES

Nhập thông tin

File .txt
Chọn tệp Không có tệp nào được chọn

File .doc
Chọn tệp Không có tệp nào được chọn

Nhập khóa

Mã hóa

Bản rõ
tran manh thang

2.3.3 Chương trình demo bằng ngôn ngữ C#(Phạm Hồng Thái)

- Giao diện chính của chương trình
- Nhập các thông số cần thiết để chia khóa
- Khóa được chia thành công
- Khôi phục khóa bằng phương pháp công thức nội suy Lagrange
- Nhập số nguyên tố và các giá trị khôi phục khóa

Demo Mã hóa DES

Mã hoá và giải mã 1 file

File : Files..

Đổi tên file

Khoá

Tiến trình

Mã hoá file Giải mã file

Mã hoá và Giải mã văn bản(Text)

Text :

Khoá

Kết quả mã hoá và giải mã

1011111010000101011011001010001111011001110110011011011111
0010000001001001011011000001111110100010110110110001110100101
011011100010001110001011111001100010100001010110000010010011
1011001111101011011110001111011100010100101100001111001010000
11001000

Mã hoá văn bản Giải mã văn bản

Chia Sẻ Khóa

Khoá

Số p

V1 a1

V2

Chia khóa

Ghép khóa

Số p

(v1, f(v1))

(v2, f(v2))

Khôi phục khóa

Khoá

HEX

2.3.4 Chương trình demo bằng ngôn ngữ Python(Hoàng Văn Thắng)

- Giao diện chính của Chương trình

The screenshot shows a Windows application window titled "Ứng dụng thuật toán DES và lược đồ chia sẻ bí mật vào thi tuyển sinh". The window has three tabs: "Mã Hóa DES", "Chia sẻ khóa", and "Khôi phục khóa". The "Mã Hóa DES" tab is active. The interface is divided into four main sections: "Khóa bí mật:" with a text input field and a "Tạo ngẫu nhiên" button; "Nhập bản rõ" and "Nhập bản mã" with large text input areas; "Kết quả mã hóa" and "Kết quả giải hóa" with large text output areas; and a bottom row with three buttons: "Mã hóa", "Giải mã", and "Nhập file".

- Nhập vào plain text □ nhập vào key hoặc nhấn Tạo ngẫu nhiên để tạo khóa □ Nhấn Mã hóa để mã hóa

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

Mã Hóa DES Chia sẻ khóa Khôi phục khóa

Khóa bí mật: 12973282 Tạo ngẫu nhiên

Nhập bản rõ **Nhập bản mã**

hoang van thang 0011101100011001110011100011

Kết quả mã hóa **Kết quả giải hóa**

0011101100011001110011100011

Mã hóa Giải mã Nhập file

- Nhấn nút Giải mã để giải mã bản mã vừa mã hóa.

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

Mã Hóa DES

Chia sẻ khóa

Khôi phục khóa

Khóa bí mật:

12973282

Tạo ngẫu nhiên

Nhập bản rõ

hoang van thang

Nhập bản mã

0011101100011001110011100011

Kết quả mã hóa

0011101100011001110011100011

Kết quả giải hóa

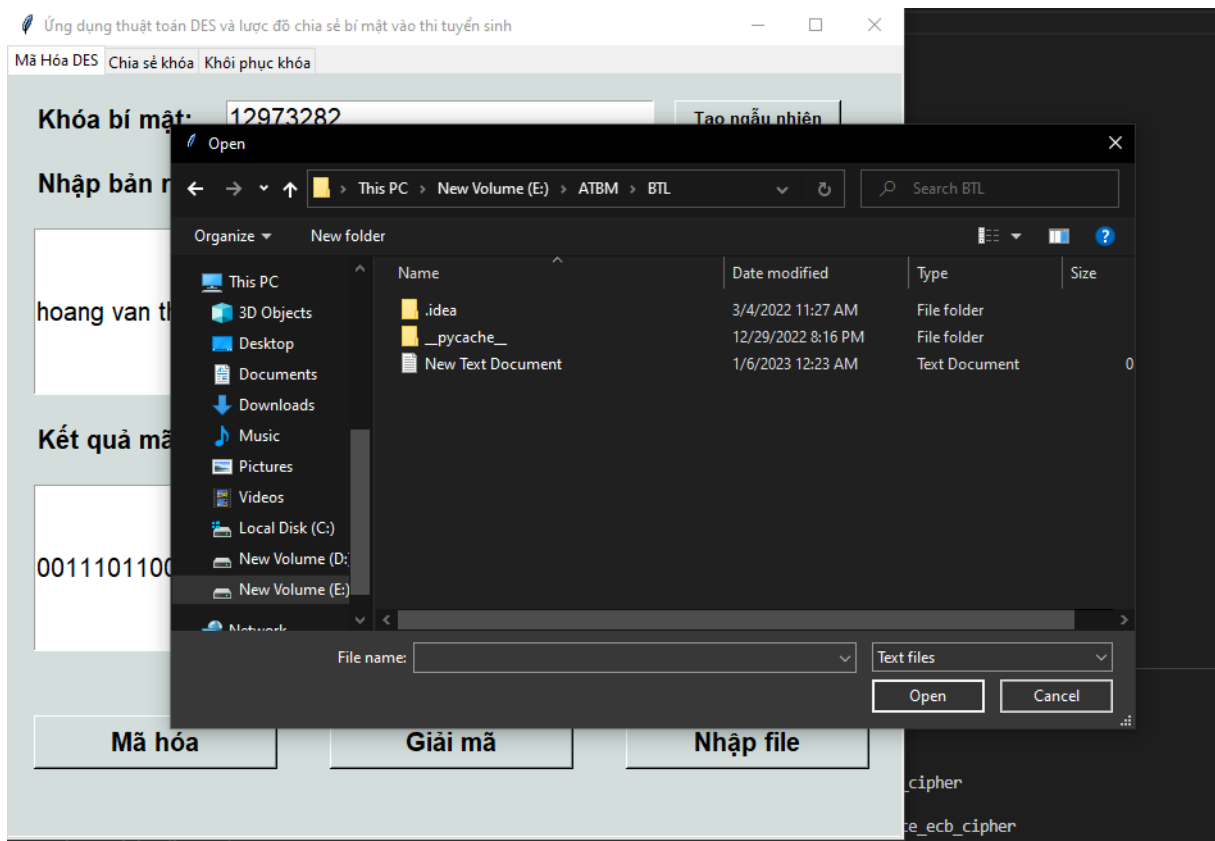
hoang van thang

Mã hóa

Giải mã

Nhập file

- Chọn file docx hoặc file txt



- Định dạng chữ sẽ được đẩy vào plaintext □ nhập key hoặc ấn vào Tạo ngẫu nhiên để nhận key mã hóa □ ấn vào nút Mã hóa để mã hóa

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

Mã Hóa DES Chia sẻ khóa Khôi phục khóa

Khóa bí mật: 12973282 Tạo ngẫu nhiên

Nhập bản rõ **Nhập bản mã**

"hello cac ban"minh la Hoang Van T 0111010101001110101010001000

Kết quả mã hóa **Kết quả giải hóa**

0111010101001110101010001000

Mã hóa **Giải mã** **Nhập file**

- Nhấn nút Giải mã để giải mã bản mã vừa mã hóa.

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

Mã Hóa DES Chia sẻ khóa Khôi phục khóa

Khóa bí mật: 12973282 Tạo ngẫu nhiên

Nhập bản rõ Nhập bản mã

"hello cac ban"minh la Hoang Van T 0111010101001110101010001000

Kết quả mã hóa Kết quả giải hóa

0111010101001110101010001000 "hello cac ban"minh la Hoang Van T

Mã hóa Giải mã Nhập file

- Giao diện chia sẻ khóa

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

Mã Hóa DES Chia sẻ khóa Khôi phục khóa

Khóa cần chia sẻ

Giá trị P

Số thành viên giữ khóa: 5

Nhập giá trị của mỗi thành viên

Thành viên 1: Thành viên 3: Thành viên 5:

Thành viên 2: Thành viên 4:

Nhập 2 số bất kì thuộc vành Z_p

Số thứ nhất: Số thứ hai:

Chia sẻ khóa

Các mảnh khóa được chia cho các thành viên là

Thành viên thứ 1: Thành viên thứ 3: Thành viên thứ 5:

Thành viên thứ 2: Thành viên thứ 4:

- Nhập các giá trị cần thiết cho chia sẻ khóa

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

Mã Hóa DES Chia sẻ khóa Khôi phục khóa

Khóa cần chia sẻ

Giá trị P

Số thành viên giữ khóa: 5

Nhập giá trị của mỗi thành viên

Thành viên 1: Thành viên 3: Thành viên 5:

Thành viên 2: Thành viên 4:

Nhập 2 số bất kì thuộc vành Z_p

Số thứ nhất: Số thứ hai:

Chia sẻ khóa

Các mảnh khóa được chia cho các thành viên là

Thành viên thứ nhất: 18 Thành viên thứ ba: 46 Thành viên thứ năm: 98

Thành viên thứ hai: 29 Thành viên thứ tư: 69

- Các mảnh khóa được chia sẻ cho các thành viên

Các mảnh khóa được chia cho các thành viên là

Thành viên thứ nhất: 18 Thành viên thứ ba: 46 Thành viên thứ năm: 98

Thành viên thứ hai: 29 Thành viên thứ tư: 69

- Giao diện khôi phục khóa

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

Mã Hóa DES Chia sẻ khóa Khôi phục khóa

Chọn ít nhất 3 thành viên để khôi phục khóa

<input type="checkbox"/> Thành viên 1:	Giá trị: 1	Giá trị mảnh khóa: 18
<input type="checkbox"/> Thành viên 2:	Giá trị: 2	Giá trị mảnh khóa: 29
<input type="checkbox"/> Thành viên 3:	Giá trị: 3	Giá trị mảnh khóa: 46
<input type="checkbox"/> Thành viên 4:	Giá trị: 4	Giá trị mảnh khóa: 69
<input type="checkbox"/> Thành viên 5:	Giá trị: 5	Giá trị mảnh khóa: 98

Khôi phục khóa

Thoát chương trình

- Khi chọn không đủ 3 thành viên trở lên

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

Mã Hóa 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: 1	Giá trị mảnh khóa: 18
<input type="checkbox"/> Thành viên 2:	Giá trị: 2	Giá trị mảnh khóa: 29
<input checked="" type="checkbox"/> Thành viên 3:	Giá trị: 3	Giá trị mảnh khóa: 46
<input type="checkbox"/> Thành viên 4:	Giá trị: 4	Giá trị mảnh khóa: 69
<input type="checkbox"/> Thành viên 5:	Giá trị: 5	Giá trị mảnh khóa: 98

Phải chọn ít nhất là 3 thành viên để khôi phục khóa

Khôi phục khóa

Thoát chương trình

- Giao diện sau khi khôi phục

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

Mã Hóa DESChia sẻ khóaKhôi phục khóa

Chọn ít nhất 3 thành viên để khôi phục khóa

<input checked="" type="checkbox"/> Thành viên 1:	Giá trị: 1	Giá trị mảnh khóa: 18
<input checked="" type="checkbox"/> Thành viên 2:	Giá trị: 2	Giá trị mảnh khóa: 29
<input checked="" type="checkbox"/> Thành viên 3:	Giá trị: 3	Giá trị mảnh khóa: 46
<input type="checkbox"/> Thành viên 4:	Giá trị: 4	Giá trị mảnh khóa: 69
<input type="checkbox"/> Thành viên 5:	Giá trị: 5	Giá trị mảnh khóa: 98

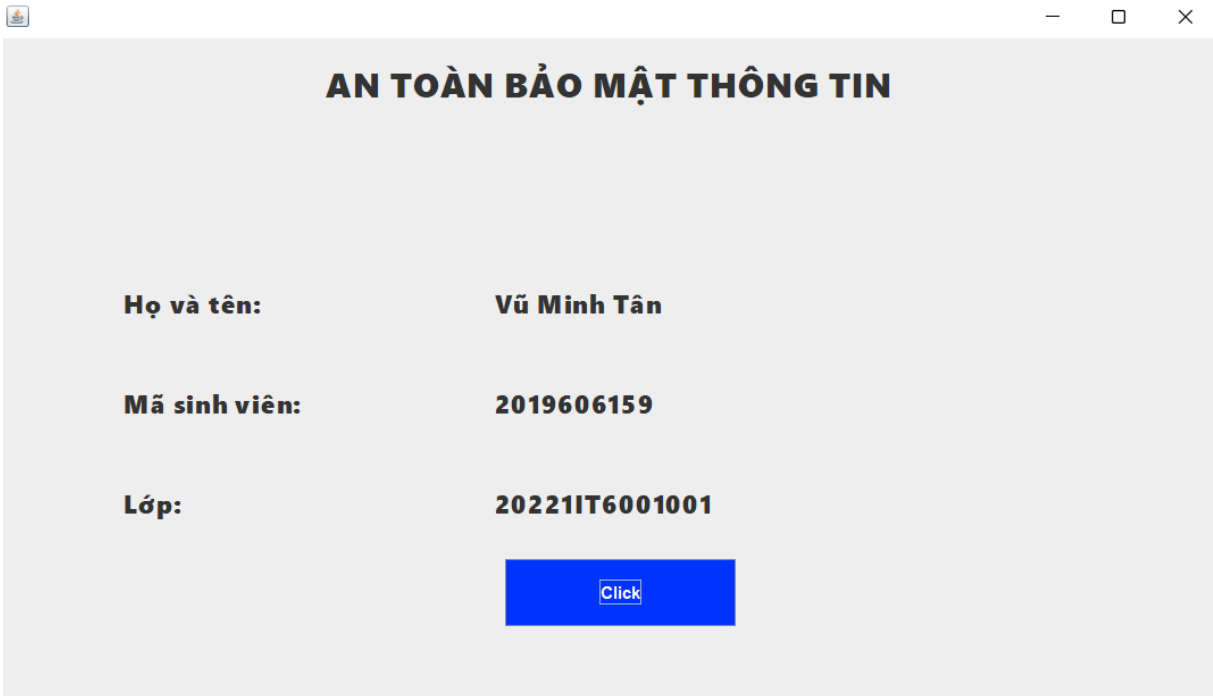
Khóa được khôi phục là: 13

Khôi phục khóa

Thoát chương trình

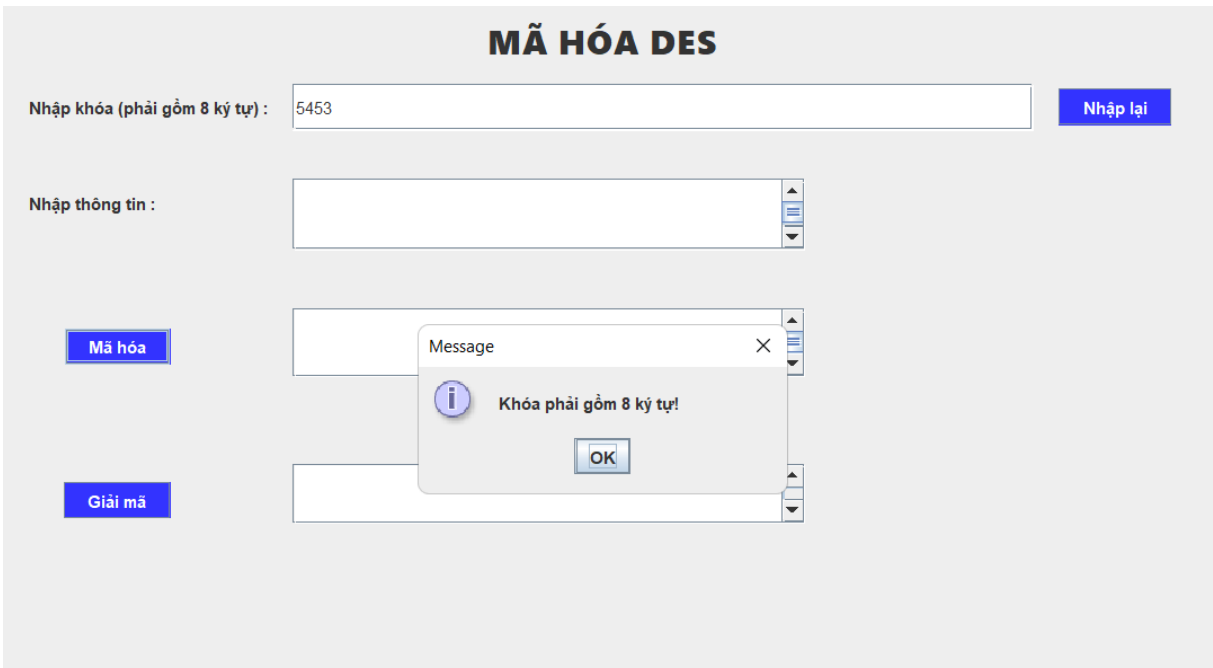
2.3.5 Chương trình demo bằng ngôn ngữ java(Vũ Minh Tân)

- Giao diện lúc bắt đầu vào chương trình



The screenshot shows a Java application window titled "AN TOÀN BẢO MẬT THÔNG TIN". It contains three labels and text fields: "Họ và tên:" with the value "Vũ Minh Tân", "Mã sinh viên:" with the value "2019606159", and "Lớp:" with the value "20221IT6001001". Below these fields is a blue button labeled "Click".

- Mã hóa DES
- Nhập khóa và thông tin cần mã hóa vào ô text, nếu nhập khóa không đủ 8 ký tự chương trình sẽ thông báo 'Khóa phải gồm 8 ký tự'



The screenshot shows a Java application window titled "MÃ HÓA DES". It has a text field for "Nhập khóa (phải gồm 8 ký tự):" containing "5453" and a blue "Nhập lại" button. Below this is a text area for "Nhập thông tin :". On the left, there are two blue buttons: "Mã hóa" and "Giải mã". A modal dialog box titled "Message" is open, displaying an information icon and the text "Khóa phải gồm 8 ký tự!" with an "OK" button.

- Sau khi nhập đầy đủ thông tin, nhấn nút “mã hóa” để mã hóa, chuỗi kí tự mã hóa sẽ được hiển thị bên cạnh nút “mã hóa”

MÃ HÓA DES

Nhập khóa (phải gồm 8 ký tự) : Nhập lại

Nhập thông tin :

Mã hóa

Giải mã

- Nhấn nút giải mã để giải mã lại thông tin đã nhập

MÃ HÓA DES

Nhập khóa (phải gồm 8 ký tự) : Nhập lại

Nhập thông tin :

Mã hóa

Giải mã

- Chia sẻ khóa

- Nhập dữ liệu số khóa cần chia sẻ, số thành viên dữ khóa, số thành viên tối thiểu để mở khóa và giá trị P. Khi nhập P nhỏ hơn khóa cần chia sẻ, chương trình sẽ thông báo “Khóa cần chia sẻ phải bé hơn p”, hoặc khi nhập p không phải là số nguyên tố, chương trình sẽ thông báo “p phải là số nguyên tố”.

Chương trình chia sẻ khóa bí mật dựa vào sơ đồ ngưỡng shamir

CHIA SẺ KHÓA

Khóa cần chia sẻ:

Số thành viên giữ khóa:

Số nguyên tố p:

Số thành viên tối thiểu để khôi phục khóa:


Chia sẻ khóa

Nhập lại

Giá trị của thành viên:

Thành Viên	Giá Trị

Message

 Khóa cần chia sẻ phải bé hơn p!

OK

Thành Viên	Giá Trị

Mảnh khóa thành viên giữ:

Thành Viên	Giá Trị

Chương trình chia sẻ khóa bí mật dựa vào sơ đồ ngưỡng shamir

CHIA SẺ KHÓA

Khóa cần chia sẻ:

Số thành viên giữ khóa:

Số nguyên tố p:

Số thành viên tối thiểu để khôi phục khóa:


Chia sẻ khóa

Nhập lại

Giá trị của thành viên:

Thành Viên	Giá Trị

Message

 p phải là số nguyên tố!

OK

Thành Viên	Giá Trị

Mảnh khóa thành viên giữ:

Thành Viên	Giá Trị

- Khi nhập số thành viên tối thiểu để khôi phục khóa vượt quá số lượng thành viên giữ khóa chương trình sẽ thông báo “Số thành viên để khôi phục khóa không lớn hơn số thành viên giữ khóa!”

Chương trình chia sẻ khóa bí mật dựa vào sơ đồ ngưỡng shamir

CHIA SẺ KHÓA

Khóa cần chia sẻ: Số thành viên giữ khóa:

Số nguyên tố p: Số thành viên tối thiểu để khôi phục khóa:

Giá trị của thành viên:

Thành Viên	Giá Trị

Mảnh khóa thành viên giữ:

Thành Viên	Giá Trị

Message ×

Số thành viên để khôi phục khóa không lớn hơn số thành viên giữ khóa!

- Sau khi nhập đúng và đầy đủ các thông tin, nhấn nút “chia sẻ khóa” chương trình sẽ thông báo “chia sẻ khóa thành công”

và dữ liệu sẽ được hiển thị ra các bảng

Chương trình chia sẻ khóa bí mật dựa vào sơ đồ ngưỡng shamir

CHIA SẺ KHÓA

Khóa cần chia sẻ: Số thành viên giữ khóa:

Số nguyên tố p: Số thành viên tối thiểu để khôi phục khóa:

Giá trị của thành viên:

Thành Viên	Giá Trị
1	954
2	964
3	676
4	376
5	359

Ai	Giá Trị
1	1
2	1

Mảnh khóa thành viên giữ:

Thành Viên	Giá Trị
1	911083
2	930273
3	457665
4	141765
5	129253

- Khôi phục khóa
- Sau khi đã có dữ liệu, chọn thành viên để khôi phục khóa. Nhấn nút “Khôi phục khóa” nếu chưa chọn thành viên để khôi phục, chương trình sẽ thông báo “Số thành viên tối thiểu dùng để khôi phục khóa là số thành viên tối thiểu đã nhập”

Chương trình chia sẻ khóa bí mật dựa vào sơ đồ ngưỡng shamir

KHÔI PHỤC KHÓA

Số nguyên tố p:

Mảnh khóa thành viên giữ:

Thành Viên	Giá Trị	Mảnh khóa
1	954	911083
2	964	930273
3	676	457665
4	376	141765
5	359	129253

Chọn thành viên để khôi phục khóa:

Message

Số thành viên tối thiểu dùng để khôi phục khóa là 3

Các thành viên đã chọn để khôi phục khóa:

Thành Viên	Giá Trị	Mảnh khóa
------------	---------	-----------

Khóa

- Sau khi chọn số thành viên tối thiểu để khôi phục khóa, chương trình sẽ thông báo “Khôi phục khóa thành công” và hiển thị khóa ra màn hình

Chương trình chia sẻ khóa bí mật dựa vào sơ đồ ngưỡng shamir

KHÔI PHỤC KHÓA

Số nguyên tố p:

Mảnh khóa thành viên giữ:

Thành Viên	Giá Trị	Mảnh khóa
1	954	911083
2	964	930273
3	676	457665
4	376	141765
5	359	129253

Chọn thành viên để khôi phục khóa: Chọn

Message

Khôi phục khóa thành công

OK

Các thành viên đã chọn để khôi phục khóa:

Thành Viên	Giá Trị	Mảnh khóa
1	964	930273
2	676	457665
3	376	141765

Khôi phục khóa

13

2.4 Phân công công việc

Tên sinh viên	Nhiệm vụ
Vũ Minh Tân	<ul style="list-style-type: none"> - Nghiên cứu, tìm hiểu về hệ mã hóa DES - Trình bày nội dung thuật toán DES - Tìm hiểu quá trình chia sẻ khóa bí mật - Cài đặt chương trình với ngôn ngữ Java
Phạm Hồng Thái	<ul style="list-style-type: none"> - Nghiên cứu, tìm hiểu về hệ mã hóa DES - Mô tả tổng quát đề tài nghiên cứu - Tìm hiểu quá trình chia sẻ khóa bí mật - Cài đặt chương trình với ngôn ngữ C#
Hoàng Văn Thắng	<ul style="list-style-type: none"> - Nghiên cứu, tìm hiểu về hệ mã hóa DES - Tìm hiểu các ví dụ về thuật toán DES - Tìm hiểu quá trình chia sẻ khóa bí mật - Cài đặt chương trình với ngôn ngữ Python

Trần Mạnh Thắng	<ul style="list-style-type: none"> - Nghiên cứu, tìm hiểu về hệ mã hóa DES - Tìm hiểu quá trình chia sẻ khóa bí mật - Tổng hợp và hoàn thiện báo cáo word - Cài đặt chương trình với ngôn ngữ PHP
Vương Toàn Thắng	<ul style="list-style-type: none"> - Nghiên cứu, tìm hiểu về hệ mã hóa DES - Tìm hiểu quá trình chia sẻ khóa bí mật - Cài đặt chương trình với ngôn ngữ JavaScript

Chương 3. Kiến Thức Lĩnh Hội Và Bài Học Kinh Nghiệm

3.1 Nội dung đã thực hiện

3.1.1 Các kiến thức đã lĩnh hội

- Hiểu được mã hóa DES
- Quá trình mã hóa DES
- Quá trình giải mã DES
- Hiểu được lược đồ chìa khóa shimir
- Thực hiện được việc chìa khóa
- Thực hiện được chương trình demo bằng nhiều ngôn ngữ khác nhau
- Hiểu được quá trình truyền tải dữ liệu, khóa trong thi tuyển sinh

3.1.2 Các kỹ năng đã tiếp thu

- Đánh giá được vai trò của bảo mật thông tin, các cơ chế, chính sách bảo mật, các kiểu tấn công và phương pháp phòng chống.
- Phân tích được các kỹ thuật sử dụng để mã hóa và xác thực thông tin.
- Hiểu và áp dụng các thuật toán liên quan đến hệ mã hóa DES như (thuật toán sinh khóa, thuật toán mã hóa, thuật toán giải mã) vào việc mã hóa và giải mã để giải quyết bài toán có tính ứng dụng vào thực tiễn.
- Tổ chức được hoạt động nhóm.
- Bên cạnh đó còn có kỹ năng quản lý thời gian hiệu quả, kỹ năng viết báo cáo, thành thạo các công cụ trong bộ office...
- Biết thêm về nhiều ngôn ngữ lập trình khác nhau

3.1.3 Bài học kinh nghiệm

- Nắm rõ kỹ năng xác định vấn đề, kỹ năng phân tích vấn đề và sàng lọc ý kiến.
- Nhóm trưởng cần xác định vai trò của từng thành viên, kiểm soát công việc tối ưu nhất và đưa ra những quyết định đúng đắn.
- Biết lắng nghe, tôn trọng ý kiến của từng thành viên.
- Đặt tinh thần trách nhiệm trong công việc thành ưu tiên hàng đầu.
- Có thêm kỹ năng sử dụng tra tài liệu bằng tiếng anh

3.2 Hướng phát triển

3.2.1 *Tính khả thi của đề tài*

- Chủ đề nghiên cứu của nhóm chúng em khá phù hợp với thời gian được cho phép để hoàn thiện bài tập lớn, bên cạnh đó các thuật toán và mã hóa đều đã có sẵn được thử nghiệm bởi các nhà nghiên cứu bảo mật nên trong thời gian nghiên cứu, nhóm nhận thấy cần phải thực sự hiểu rõ về hệ mật mã DES
- Các thư viện có sẵn trên mạng hỗ trợ tối đa và có kỹ thuật lập trình ở mức khá nên chúng em có thể hoàn thành được đề tài này


3.2.2 *Những thuận lợi và khó khăn nhóm gặp phải*

Thuận lợi

- Có thể đọc hiểu được tài liệu tiếng anh nên có thể dễ dàng tiếp cận các nguồn tài liệu chính thống.
- Các thuật toán đã có sẵn, chỉ cần áp dụng một chút kỹ thuật xử lý về Form, File là đã có thể hoàn thành bài toán của đề tài.
- Các thành viên trong nhóm hòa đồng, cởi mở, tương tác với các thành viên khác trong nhóm khá sôi nổi nên các công việc liên quan đến cả nhóm thường diễn ra khá suôn sẻ.

Khó khăn

- Công đoạn thiết giao diện phần mềm mã hóa chưa được bắt mắt do chưa có nhiều kinh nghiệm trong kỹ thuật xử lý giao diện.
- Các thành viên đều chưa sử dụng được đa dạng loại ngôn ngữ nên việc chia ngôn ngữ và sử dụng ngôn ngữ mới gặp rất nhiều vấn đề

-
- 
- Ở phần xử lý về File Docx sử dụng để lấy bản rõ khá mới mẻ với các thành viên trong nhóm nên giai đoạn hoàn thiện chức năng tốn khá nhiều thời gian.