BỘ CÔNG THƯƠNG
TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP THÀNH PHỐ HỒ CHÍ MINH
KHOA CÔNG NGHỆ THÔNG TIN

MÔN: NHẬP MÔN AN TOÀN THÔNG TIN

ĐỀ CƯƠNG NGHIÊN CỨU

Đề tài:

NGHIÊN CỨU, VIẾT CHƯƠNG TRÌNH DEMO MÃ AES VÀ MÃ HOÁN VỊ

LỚP HỌC PHẦN: DHCNTT16B
NHÓM: 12
GVHD: Võ Ngọc Tấn Phước

Thành phố Hồ Chí Minh, tháng 11 năm 2022

BỘ CÔNG THƯƠNG
TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP THÀNH PHỐ HỒ CHÍ MINH
KHOA CÔNG NGHỆ THÔNG TIN

MÔN : NHẬP MÔN AN TOÀN THÔNG TIN

ĐỀ CƯƠNG NGHIÊN CỨU

Đề tài:

NGHIÊN CỨU, VIẾT CHƯƠNG TRÌNH DEMO MÃ AES VÀ MÃ HOÁN VỊ

Lớp học phần: DHCNTT16B
Nhóm: 12

STT	HỌ VÀ TÊN	MSSV	CHỮ KÝ
1	Lường Văn Đạt	20045481	
2	Nguyễn Trọng Hậu	20096011	
3	Phan Chí Cường	20096071	
4	Vũ Mạnh Đạt	20100391	
5	Lý Nam Kha	20106011	

Thành phố Hồ Chí Minh, tháng 11 năm 2022

MỤC LỤC

PHẦN MỞ ĐẦU

1. Lí do chọn đề tài

Mã hóa là gì? Mã hóa thực chất là một **phương pháp biến đổi thông tin** dưới dạng bình thường trở nên không thể hiểu được nếu không có phương tiện giải mã. Hay nói một cách đơn giản và dễ hiểu hơn thì mã hóa chính là cách xáo trộn dữ liệu một cách lộn xộn mà chỉ 2 bên trao đổi thông tin mới có thể hiểu. Về mặt kỹ thuật, mã hóa là quá trình chuyển đổi cấu trúc văn bản thuần túy mà con người có thể dễ dàng đọc được nhưng không thể hiểu được nội dung là gì. Cấu trúc này nếu hiểu theo thuật ngữ kỹ thuật gọi là bản mã. Lúc này toàn bộ thông tin văn bản ban đầu sẽ chuyển sang một dạng ngôn ngữ khác không giống với văn bản ban đầu.

Mã hoá dữ liệu là một công việc cơ bản và cần thiết đối với các doanh nghiệp đang hoạt động hiện nay. Bởi nó mang lại những lợi ích nhất định cho doanh nghiệp.

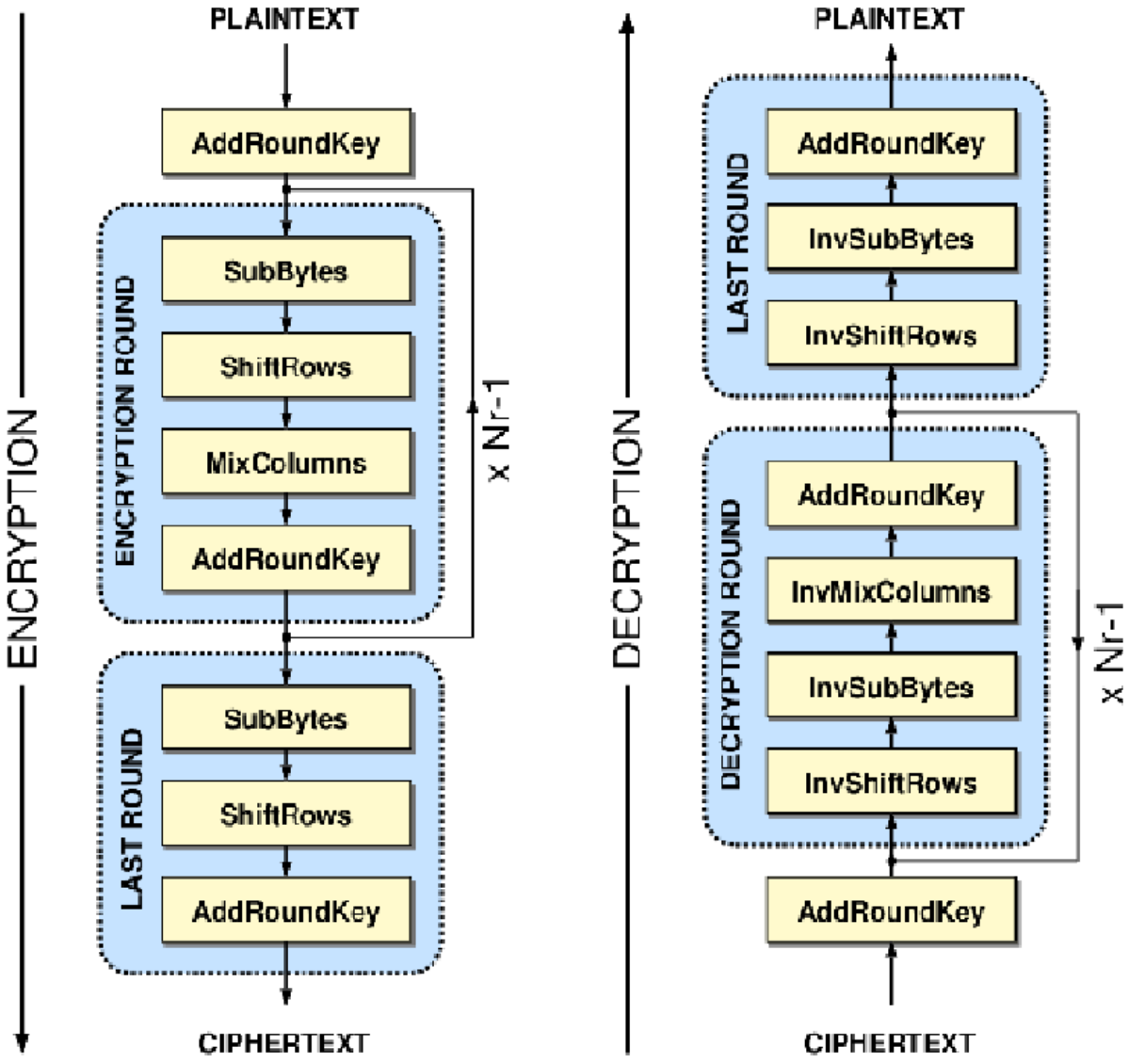
- Trong thời đại công nghệ số hiện nay, mã hoá được xem là giải pháp hiệu quả giúp mọi thông tin của doanh nghiệp khi truyền tải trên internet luôn được đảm bảo an toàn và toàn vẹn nhất.
- Thực hiện mã hoá giúp doanh nghiệp có thể dễ dàng ngăn chặn được các truy cập bất hợp pháp vào hệ thống thông tin đã được thực hiện việc bảo vệ. Bởi chỉ những người có mật khẩu hoặc có quyền truy cập vào khoá giải mã thì mới có thể đọc và hiểu được các dữ liệu, thông tin đã được mã hoá.
- Các thuật toán mã hoá sẽ cung cấp cho doanh nghiệp các yếu tố bảo mật then chốt như tính xác thực cho phép xác minh nguồn dữ liệu, tính toàn vẹn giúp đảm bảo các thông tin không bị thay đổi khi được gửi đi và không thu hồi để đảm bảo việc gửi dữ liệu không bị huỷ.
- Thực hiện mã hoá tương tự như việc gia tăng thêm mức độ bảo mật cho thông tin. Chính vì vậy, cho dù dữ liệu của bạn bị đánh cắp thì việc giải mã cũng rất khó khăn và tốn nhiều thời gian, công sức.

Từ việc hiểu được ảnh hưởng và tầm quan trọng của việc mã hóa thông tin đồng thời đảm bảo kiến thức môn học Nhập môn an toàn thông tin nên nhóm chúng tôi đã thực hiện đề tài "Nghiên cứu, viết chương trình demo mã AES và mã hoán vị".

2. Mã hóa AES

2.1. Khái niệm và nguyên lí hoạt động

AES là một thuật toán "mã hóa khối" (block cipher) ban đầu được tạo ra bởi hai nhà mật mã học người Bỉ là Joan Daemen và Vincent Rijmen. Kể từ khi được công bố là một tiêu chuẩn, AES trở thành một trong những thuật toán mã hóa phổ biến nhất sử dụng khóa mã đối xứng để mã hóa và giải mã (một số được giữ bí mật dùng cho quy trình mở rộng khóa nhằm tạo ra một tập các khóa vòng). Ở Việt Nam, thuật toán AES đã được công bố thành tiêu chuẩn quốc gia TCVN 7816:2007 năm 2007 về Thuật toán mã hóa dữ liệu AES



AES là một thuật toán mã hóa khối đối xứng với độ dài khóa là 128 bít (một chữ số nhị phân có giá trị 0 hoặc 1), 192 bít và 256 bít tương ứng dọi là AES-128, AES-192 và AES-256. AES-128 sử dụng 10 vòng (round), AES-192 sử dụng 12 vòng và AES-256 sử dụng 14 vòng.

Vòng lặp chính của AES thực hiện các hàm sau: SubBytes(), ShiftRows(), MixColumns() và AddRoundKey(). Ba hàm đầu của một vòng AES được thiết kế để ngăn chặn phân tích mã bằng phương thức "mập mờ" (confusion) và phương thức "khuếch tán" (diffusion), còn hàm thứ tư mới thực sự được thiết kế để mã hóa dữ liệu. Trong đó "khuếch tán" có nghĩa là các kiểu mẫu trong bản rõ (Dữ liệu đầu vào của phép mã hóa hoặc dữ liệu đầu ra của phép giải mã) được phân tán trong các bản mã (Dữ liệu đầu ra của phép mã hóa hoặc dữ liệu đầu vào của phép giải mã), "mập mờ" nghĩa là mối quan hệ giữa bản rõ và bản mã bị che khuất. Một cách đơn giản hơn để xem thứ tự hàm AES là: Trộn từng byte (SubBytes), trộn từng hàng (ShiftRows), trộn từng cột (MixColumns) và mã hóa (AddRoundKey).

Đối với phép mã hóa và phép giải mã, thuật toán AES sử dụng một hàm vòng gồm bốn phép biến đổi byte như sau: phép thay thế byte (một nhóm gồm 8 bít) sử dụng một bảng thay thế (Hộp-S), phép dịch chuyển hàng của mảng trạng thái theo các offset (số lượng byte) khác nhau, phép trộn dữ liệu trong mỗi cột của mảng trạng thái, phép cộng khóa vòng và trạng thái. Các phép biến đổi này (cũng như các phép nghịch đảo tương ứng của chúng) được mô tả trong phần dưới đây.

Phép mã hóa

Tại thời điểm bắt đầu phép mã hóa, đầu vào được sao chép vào mảng trạng thái sử dụng các quy ước. Sau phép cộng khóa vòng khởi đầu, mảng trạng thái được biến đổi bằng cách thực hiện một hàm vòng liên tiếp với số vòng lặp là 10, 12 hoặc 14 (tương ứng với độ dài khóa), vòng cuối cùng khác biệt không đáng kể với Nr-1 vòng đầu tiên. Trạng thái cuối cùng được chuyển thành đầu ra. Hàm vòng được tham số hóa bằng cách sử dụng một lược đồ khóa – mảng một chiều chứa các từ 4 byte nhận từ phép mở rộng khóa.

Phép biến đổi cụ thể gồm SubBytes(), ShiftRows(), MixColumns() và AddRoundKey() dùng để xử lý trạng thái.

SubBytes()

Phép biến đổi dùng trong phép mã hóa áp dụng lên trạng thái (kết quả mã hóa trung gian, được mô tả dưới dạng một mảng chữ nhật của các byte) sử dụng một bảng thay thế byte phi tuyến (Hộp S – bảng thay thế phi tuyến, được sử dụng trong một số phép thay thế byte và trong quy trình mở rộng khóa, nhằm thực hiện một phép thay thế 1-1 đối với giá trị mỗi byte) trên mỗi byte trạng thái một cách độc lập.

ShiftRows()

Phép biến đổi dùng trong phép mã hóa áp dụng lên trạng thái bằng cách chuyển dịch vòng ba hàng cuối của trạng thái theo số lượng byte các offset khác nhau.

MixColumns()

Phép biến đổi trong phép mã hóa thực hiện bằng cách lấy tất cả các cột trạng thái trộn với dữ liệu của chúng (một cách độc lập nhau) để tạo ra các cột mới.

AddRoundKey()

Phép biến đổi trong phép mã hóa và phép giải mã. Trong đó, một khóa vòng (các giá trị sinh ra từ khóa mã bằng quy trình mở rộng khóa) được cộng thêm vào trạng thái bằng phép toán XOR (phép toán hoặc và loại trừ). Độ dài của khóa vòng bằng độ dài của trạng thái.

Mở rộng khóa

Thuật toán AES nhận vào một khóa mã K và thực hiện phép mở rộng khóa để tạo ra một lược đồ khóa. Phép mở rộng khóa tạo ra tổng số Nb(Nr+1) từ. Thuật toán yêu cầu một tập khởi tạo gồm Nb từ và mỗi trong số Nr vòng đòi hỏi Nb từ làm dữ liệu khóa đầu vào. Lược đồ khóa kết quả là một mảng tuyến tính các từ 4 byte.

Phép giải mã

Các phép biến đổi trong phép mã hóa có thể được đảo ngược và sau đó thực hiện theo chiều ngược lại nhằm tạo ra phép giải mã trực tiếp của thuật toán AES. Các phép biến đổi sử dụng trong phép giải mã gồm: InvShiftRows(), InvSubBytes(), InvMixColumns() và AddRoundKey().

InvSubBytes()

Phép biến đổi InvSubBytes() là nghịch đảo của phép thay thế theo byte SubBytes(), trong đó sử dụng một hộp-S nghịch đảo áp dụng cho mỗi byte của trạng thái.

InvShiftRows()

Phép biến đổi InvShiftRows() là phép biến đổi ngược của ShiftRows(). Các byte trong ba từ cuối của trạng thái được dịch vòng theo số byte khác nhau. Ở hàng đầu

tiên (r=0) không thực hiện phép chuyển dịch, ba hàng dưới cùng được dịch vòng Nb-shift(r,Nb) byte.

InvMixColumns()

Phép biến đổi InvMixColumns() là phép biến đổi ngược của MixColumns(). Nó thao tác theo từng cột của trạng thái, xem mỗi cột như một đa thức bốn hạng tử.

Biến đổi nghịch AddRoundKey()

Phép biến đổi AddRoundKey() là phép biến đổi thuận nghịch vì nó chỉ áp dụng một phép toán XOR nên nó được thực hiện như nhau ở cả phép mã hóa và phép giải mã.

Ngoài các phép giải mã trên, thuật toán AES còn cho phép thực hiện một phép giải mã tương đương có cùng thứ tự các phép biến đổi như trong phép mã hóa (các biến đổi được thay bằng các phép biến đổi ngược). Có thể thực hiện được điều này là nhờ một thay đổi trong lược đồ khóa. Hai tính chất tạo nên một phép giải mã tương đương là: Tính giao hoán giữa hai phép biến đổi SubBytes() và ShiftRows() (tính chất này cũng đúng với phép nghịch đảo InvSubBytes() và InvShiftRows()), Các phép toán trộn cột MixColumns() và InvMixColumns() là tuyến tính đối với đầu vào cột. Các tính chất này cho phép đảo ngược thứ tự của các phép biến đổi InvSubBytes() và InvShiftRows(). Thứ tự của các phép biến đổi AddRoundKey() và InvMixColumns() cũng có thể đảo ngược với điều kiện đảm bảo rằng các cột của lược đồ khóa giải mã được chỉnh sửa bằng cách sử dụng phép biến đổi InvMixColumns().

Vấn đề thực hiện khóa

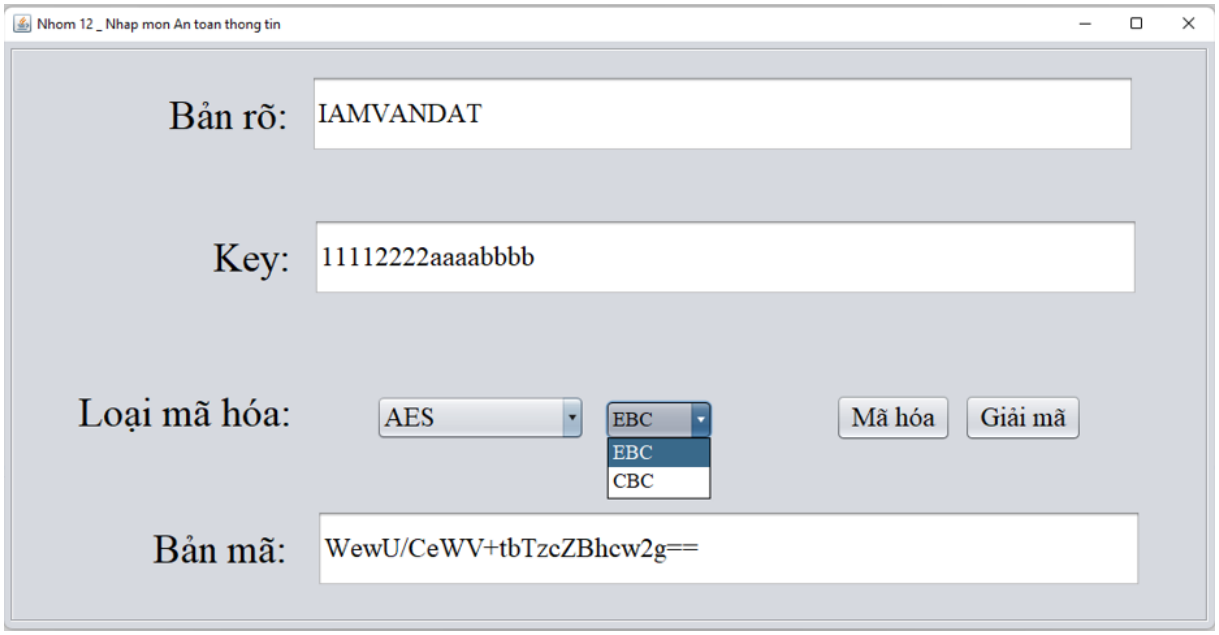
Yêu cầu về độ dài khóa

Việc thực hiện khóa của thuật toán AES sẽ hỗ trợ ít nhất một trong ba độ dài khóa là 128 bít, 192 bít và 256 bít. Việc thực hiện khóa có thể tùy chọn hỗ trợ hai hoặc ba độ dài khóa, nhằm tăng thêm tính tương tác cho các thực hiện thuật toán.

Tham số hóa độ dài khóa, kích thước khối và số vòng

AES quy định cụ thể các giá trị được phép dùng cho chiều dài khóa, kích thước khối và số vòng. Tuy nhiên, các giá trị này có thể thay đổi trong tương lai. Do đó, những nhà triển khai thuật toán AES có thể lựa chọn thiết kế linh hoạt với mong muốn của họ.

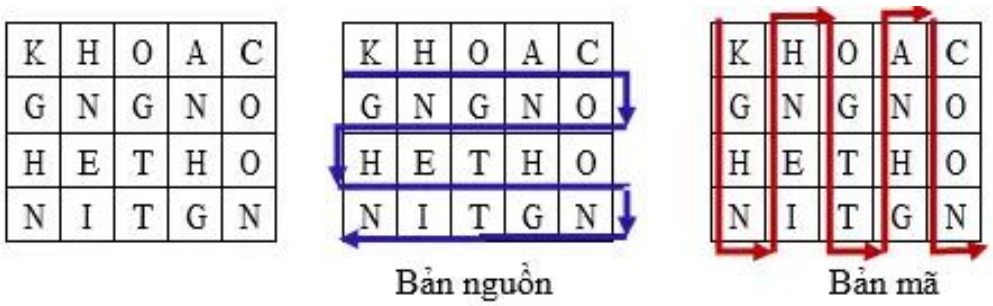
2.2. Demo chương trình



3. Mã hóa Hoán Vị

3.1. Khái niệm và nguyên lí hoạt động

Mã hóa hoán vị về bản chất thì kỹ thuật hoán vị chỗ chính là trường hợp đặc biệt của kỹ thuật thay thế. Trong kỹ thuật này, tập hợp các ký tự của bản nguồn sẽ không thay đổi so với bản mã mà chỉ thay đổi vị trí của các ký tự Thám mã bắt đầu từ việc dự đoán số phần tử đó (chính là số cột của bảng). Để làm điều đó, ta tìm kiếm tất cả các khả năng đổi chỗ trong chu kỳ dự kiến để tìm ra mẫu chung (sử dụng danh sách các cặp, bộ ba,…có nghĩa). Nếu các ký tự có thể được sắp xếp lại trong một nhóm thì ta thử xem xét việc sắp xếp tương tự trong các nhóm khác. Khi đã tìm được các cụm từ có nghĩa, chúng ta sẽ đồng thời tìm được thứ tự đảo của khoá và sẽ suy ra khoá.



		L	E	M	O	N
		2	1	3	5	4
L	2	H	K	O	C	A
E	1	N	O	G	G	N
M	3	E	H	T	O	H
O	5	G	N	T	N	I
N	4	P	S	K	Z	T

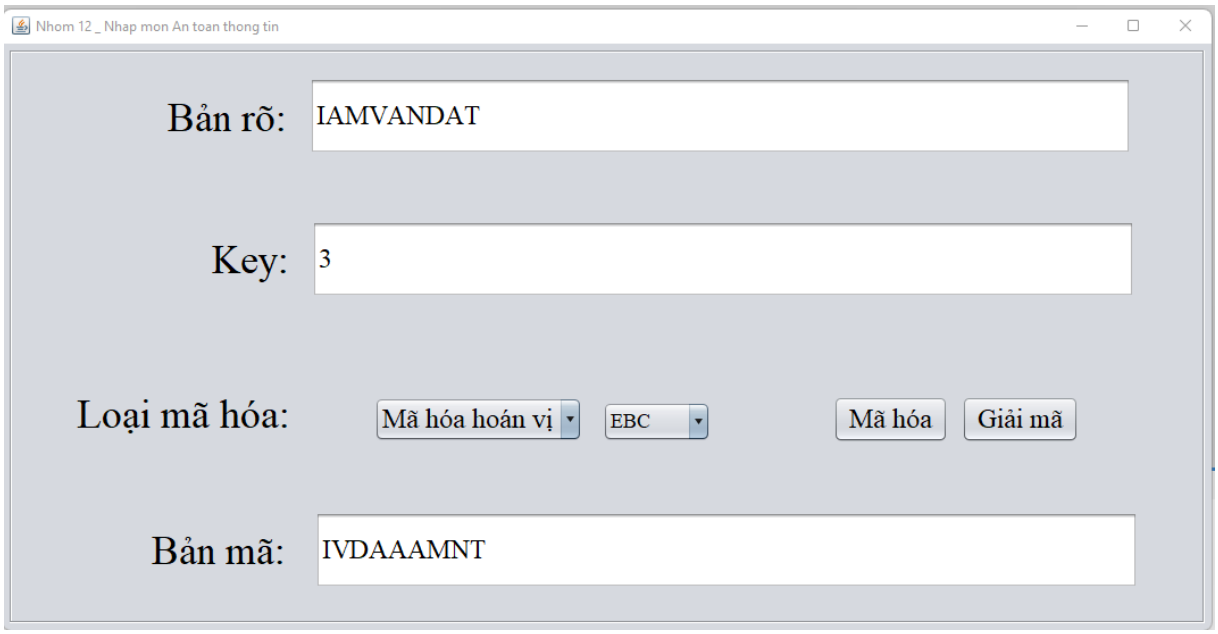
H	K	O	C	A
N	O	G	G	N
E	H	T	O	H
G	N	T	N	I
P	S	K	Z	T

Có một số kỹ thuật đổi chỗ đơn giản như sau:

- **Đảo ngược từ** (Mirror cipher): Các ký tự trong bản mã được viết theo thứ tự ngược lại so với bản nguồn: TOI AN COM à MOC NA IOT
- **Hình học** (Geometric Figure): Viết bản nguồn theo một mẫu và đọc theo mẫu khác.
- **Đổi chỗ theo hàng** (Row Transposition ciphers): Viết bản nguồn theo hàng, hoán vị các cột theo khóa và sau đó đọc lại theo hàng để có được bản mã.
- **Đổi chỗ lộn xộn (**Nihilist cipher**)**: Đổi chỗ cả dòng và cột. Viết thông điệp theo hàng, theo khóa. Để có bản mã, ta đọc từ trái sang phải theo từng hàng, thứ tự hàng được xác định bằng khóa viết theo cột.
- **Đổi chỗ đường chéo (**Diagonal cipher**)**: Viết thông điệp giống như trên và thông điệp theo đường zig-zag để có bản mã.

Khoá của thuật toán đổi chỗ theo hàng chính là số phần tử của khoá và hoán vị của các phần tử đó

3.2. Demo chương trình



DANH MỤC TÀI LIỆU THAM KHẢO

❖ **Website**

1. Xem trên ViettelIDC: https://bom.so/gf6wUq

2. Xem trên website.com: https://bom.so/igkTrR

PHỤ LỤC

TRƯỜNG ĐH CÔNG NGHIỆP TP.HCM CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập – Tự do – Hạnh phúc

BẢNG ĐÁNH GIÁ KẾT QUẢ LÀM VIỆC NHÓM

LỚP HỌC PHẦN: DHCNTT16B

NHÓM: 12

1. Phân công công việc:

Nhóm có tổ chức 1 buổi họp online:

- Thời gian bắt đầu: 19h00 ngày 11/11/2022.
- Thời gian kết thúc: 20h30 ngày 11/11/2022.
- Chủ trì: Lường Văn Đạt.
- Thành phần tham dự gồm: Tất cả thành viên trong nhóm.

Qua cuộc họp, nhóm đã thảo luận và cùng nhau trao đổi về chủ đề thực hiện bài đồ án môn học Nhập môn an toàn thông tin. Được sự thống nhất của tất cả các thành viên trong nhóm, nhóm trưởng đã phân công công việc cho các thành viên như sau:

STT	Họ và tên	MSSV	Vai trò trong nhóm	Công việc được phân công
1	Lường Văn Đạt	20045481		- Lập trình ứng dụng mã hóa AES, Hoán vị - Làm báo cáo word
2	Nguyễn Trọng Hậu	20096011		-
3	Phan Chí Cường	20096071		-
4	Vũ Mạnh Đạt	20100391		-
5	Lý Nam Kha	20106011		-

2. Kết quả đánh giá.

STT	Họ và tên	Mức độ tham gia kịp thời mọi yêu cầu	Mức độ đóng góp	Chất Lượng đóng góp	Nhận xét, góp ý của nhóm	Điểm tổng cộng
1	Lường Văn Đạt					
2	Nguyễn Trọng Hậu					
3	Phan Chí Cường					
4	Vũ Mạnh Đạt					
5	Lý Nam Kha					

Các thành viên đồng ý với kết quả đánh giá trên.

STT	Họ và tên	MSSV	Vai trò trong nhóm	Chữ ký
1	Lường Văn Đạt	20045481		
2	Nguyễn Trọng Hậu	20096011		
3	Phan Chí Cường	20096071		
4	Vũ Mạnh Đạt	20100391		
5	Lý Nam Kha	20106011		