TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI

KHOA CÔNG NGHỆ THÔNG TIN

BÀI TẬP LỚN

AN TOÀN BẢO MẬT THÔNG TIN

ĐỀ TÀI: ỨNG DỤNG HỆ THỐNG MÃ HÓA LAI VÀO CÔNG TÁC BẢO MẬT TRONG TRUYỀN TẢI ĐỀ THI

GVHD : ThS. Trần Phương Nhung

NHÓM: 2 – **Lớp:** 20222IT6001002

Sinh viên thực hiện: Nguyễn Đình Đạt

Hà Nội – Năm học: 2023 - 2024

TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI

KHOA CÔNG NGHỆ THÔNG TIN

BÀI TẬP LỚN

AN TOÀN BẢO MẬT THÔNG TIN

ĐỀ TÀI: ỨNG DỤNG HỆ THỐNG MÃ HÓA LAI VÀO CÔNG TÁC BẢO MẬT TRONG TRUYỀN TẢI ĐỀ THI

NHÓM 2 – Lớp: 20222IT6001002

Tên thành viên	Mã sinh viên
Nguyễn Đình Đạt	2021607831

Giảng viên hướng dẫn: ThS. Trần Phương Nhung

Hà Nội – Năm học: 2023 - 2024

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. Vấn đề khó khăn đặt ra là làm sao giữ được tính bảo mật của thông tin, thông tin đến đúng được địa chỉ cần đến và không bị sửa đổi. Hậu quả sẽ khó lường nếu như thư được gửi cho một người nhưng lại bị một người khác xem trộm và sửa đổi nội dung bức thư trái với chủ ý của người gửi.

Mã hoá thông tin là một trong các phương pháp có thể đảm bảo được tính bảo mật của thông tin. Khi mã hóa, thông tin được biến đổi (được mã hóa) bằng thuật toán mã hóa thông qua việc sử dụng "khóa". Chỉ có người dùng có cùng "khóa" mới phục hồi lại được thông tin ban đầu (giải mã). Do vậy "khóa" cần được bảo vệ nghiêm ngặt và được truyền từ người gửi đến người nhận trên một kênh an toàn riêng sao cho người thứ ba không thể biết được khóa. Phương pháp này được gọi là mã hóa bằng khóa riêng hoặc mật mã khóa đối xứng. Có một số chuẩn thuật toán khóa đối xứng, ví dụ như DES, AES, v.v…

Cụ thể, trong đề tài được giao của nhóm em lần này với đề tài ***"Ứng dụng hệ thống mã hóa lai vào công tác bảo mật trong truyền tải đề thi"*** sẽ sử dụng hệ mật mã bất đối xứng AES và hệ mật mã đối xứng ECC để thực hiện mã hóa và truyền tải đề thi với mong muốn áp dụng kiến thức đã học, giải quyết bài toán bảo mật đề thi trong thi tuyển sinh.

Trong suốt quá trình học tập, nhóm em rất may mắn được cô giáo ***ThS. Trần Phương Nhung*** hướng dẫn một cách tận tâm và nhiệt tình với những giờ học chất lượng và dễ hiểu. Nội dung đề tài được hoàn thành dựa trên những lý thuyết đã học cùng nhiều tài liệu tham khảo khác tuy nhiên không tránh khỏi thiếu xót, nhóm mong nhận thêm phản ánh và góp ý từ phía giảng viên và các bạn đọc .

Nhóm chúng em xin chân thành cảm ơn!

MỤC LỤC

CHƯƠNG I: TỔNG QUAN

1. Lí do và tính cấp thiết của đề tài

Bảo mật đề thi có vai trò hết sức quan trọng đối với các kỳ thi.Đề thi là một trong những tài liệu mật của quốc gia. Hằng năm, các trường học phải thường xuyên tổ chức các kỳ thi nhằm tuyển chọn học sinh vào trường, kỳ thi đánh giá kết quả học tập của học sinh như: Thi tuyển sinh đầu vào, kiểm tra chất lượng, thi học kỳ, thi tốt nghiệp, thi học sinh giỏi… Trong các kỳ thi đó, có những đợt thi các trường thi chung đề thi của Bộ Giáo dục và Đào tạo, của Sở Giáo dục và Đào tạo (SGD&ĐT). Hiện nay, SGD&ĐT bảo mật đề thi của các kỳ thi bằng cách niêm phong các túi đề thi.

Việc bố trí nhân sự, in sao đề thi sẽ thực hiện theo quy định. Phương án vận chuyển bàn giao đề thi từ địa điểm in sao đến các điểm thi được tính đến, bao gồm cả kế hoạch dự phòng. Ban vận chuyển và bàn giao đề thi nhận các túi đề thi còn nguyên niêm phong từ Ban in sao đề thi bảo quản, vận chuyển, phân phối đề thi đến các điểm thi. Các túi đề thi phải được bảo quản trong hòm sắt được khóa, niêm phong và bảo vệ 24 giờ/ngày. Tại các điểm thi, đề thi và bài thi được để trong các tủ riêng biệt. Tủ đựng đề thi, bài thi đảm bảo chắc chắn, được khóa và niêm phong (nhãn niêm phong có đủ chữ ký của trưởng điểm thi, thanh tra và công an), chìa khóa do trưởng điểm thi giữ. Khi mở niêm phong phải có chứng kiến của những người ký nhãn niêm phong, lập biên bản ghi rõ thời gian mở, lý do mở, tình trạng niêm phong.

Ngoài ra, khu vực bảo quản đề thi sẽ có công an trực, bảo vệ liên tục 24 giờ/ngày và phải bảo đảm an toàn phòng chống cháy, nổ. Phòng bảo quản đề thi bảo đảm an toàn, chắc chắn; có camera an ninh giám sát, ghi hình các hoạt động tại phòng liên tục; công an trực, bảo vệ liên tục 24 giờ/ngày; có một phó trưởng điểm thi là người của trường phổ thông không có thí sinh dự thi tại điểm thi trực tại phòng trong suốt thời gian đề thi, bài thi được lưu tại điểm thi. Từng hội đồng thi có trách nhiệm lập phương án bảo vệ đề thi trong suốt quá trình tổ chức kỳ thi. Với

việc nhận và chuyển đề thi theo phương thức này có thể gặp nhiều trở ngại cũng như việc đảm bảo an toàn, bí mật cho đề thi chứa đựng nhiều yếu tố rủi ro, kinh phí cho việc giao nhận và bảo vệ đề thi rất tốn kém.

Để góp phần khắc phục một phần những hạn chế trên, việc sử dụng các công cụ của mật mã học ứng dụng vào công tác bảo mật đề thi trong truyền tải đề thi qua mạng là một vấn đề mang tính thời sự và cấp thiết.

2. Tổng quan về mã hóa thông tin

Thế kỷ XXI là thế kỷ công nghệ thông tin. Công nghệ thông tin đã và đang tác động trực tiếp đến mọi mặt hoạt động kinh tế xã hội trên thế giới. Thông tin có vai trò hết sức quan trọng, vì vậy cần phải đảm bảo để thông tin không bị sai lệch, không bị thay đổi, hay bị lộ trong quá trình truyền từ nơi gửi đến nơi nhận. Với sự phát triển rất nhanh của công nghệ mạng máy tính, đặc biệt là mạng Internet, khối lượng thông tin ngày càng được truyền nhận nhiều hơn. Vấn đề khó khăn đặt ra là làm sao giữ được tính bảo mật của thông tin, thông tin đến đúng được địa chỉ cần đến và không bị sửa đổi. Hậu quả sẽ khó lường nếu như thư được gửi cho một người nhưng lại bị một người khác xem trộm và sửa đổi nội dung bức thư trái với chủ ý của người gửi. Tệ hại hơn nữa là khi một hợp đồng được ký, gửi thông qua mạng và bị kẻ xấu sửa đổi những điều khoản trong đó. Người gửi thư bị hiểu nhầm vì nội dung bức thư bị thay đổi, còn hợp đồng bị phá vỡ bởi những điều khoản đã không còn như ban đầu. Điều này gây ra những mất mát cả về mặt tài chính và quan hệ, tình cảm, v.v... và còn có thể nêu ra rất nhiều tình huống tương tự. Mã hoá thông tin là một trong các phương pháp có thể đảm bảo được tính bảo mật của thông tin. Mã hoá, trong một mức độ nhất định, có thể giải quyết các vấn trên; một khi thông tin đã được mã hoá, kẻ xấu rất khó hoặc không thể giải mã để có được nội dung thông tin ban đầu.

Khi mã hóa, thông tin được biến đổi (được mã hóa) bằng thuật toán mã hóa thông qua việc sử dụng “khóa”. Chỉ có người dùng có cùng “khóa” mới phục hồi lại được thông tin ban đầu (giải mã). Do vậy “khóa” cần được bảo vệ nghiêm ngặt

và được truyền từ người gửi đến người nhận trên một kênh an toàn riêng sao cho người thứ ba không thể biết được khóa. Phương pháp này được gọi là mã hóa bằng khóa riêng hoặc mật mã khóa đối xứng. Có một số chuẩn thuật toán khóa đối xứng, ví dụ như DES, AES, v.v… Người ta đã chứng minh được khả năng bảo mật cao của các thuật toán đối xứng chuẩn nói trên và chúng đã được kiểm định qua thời gian. Tuy nhiên, vấn đề nảy sinh với các thuật toán đối xứng là việc trao đổi khóa. Các bên tham gia giao tiếp đòi hỏi được chia sẻ một bí mật là "khóa", "khóa" cần được trao đổi giữa họ qua một kênh thông tin an toàn. An toàn của thuật toán khóa đối xứng phụ thuộc vào độ mật của khoá. Khóa thường có độ dài hàng trăm bit, tùy thuộc vào thuật toán được sử dụng. Vì thông tin có thể trung chuyển qua các điểm trung gian nên không thể trao đổi khóa một cách trực tuyến và an toàn. Trong một mạng rộng kết nối hàng trăm hệ thống, việc trao đổi khóa trở thành quá khó khăn và thậm chí không thực tế.

Cho đến cuối những năm 1970, tất cả các quá trình truyền thông tin bảo mật đều sử dụng hệ mật mã đối xứng. Điều này có nghĩa rằng một ai đó có đủ thông tin (khóa) để mã hóa thông tin thì cũng có thông tin đủ để giải mã. Năm 1976 Diffe và Hellman đã nêu định hướng phát triển mới cho các hệ thống mật mã bằng việc phát minh hệ mật mã khóa công khai. Ý tưởng chính là sử dụng hàm một chiều (one-way function) để mã hóa. Các hàm sử dụng để mã hóa thuộc một lớp các hàm một chiều đặc biệt, chúng là một chiều nếu một số thông tin nhất định (khóa để giải mã) được giữ bí mật. Nói một cách hình thức, hàm mã hóa khóa công khai là một hàm ánh xạ các dãy tin (bản rõ) thành các dãy được mật mã hóa; bất cứ ai có khóa công khai đều có thể thực hiện việc mã hóa này. Tuy nhiên việc tính toán hàm nghịch đảo (hàm để giải mã thông tin được mã hóa thành các dãy tin ban đầu - bản rõ) không thể thực hiện được trong một khoảng thời gian hợp lý mà không cần thêm một số thông tin bổ sung, gọi là khóa riêng. Điều này có nghĩa rằng mọi người có thể gửi thông tin đến một người nào đó bằng cách sử dụng cùng một khóa để mã hóa bằng cách đơn giản là lấy khóa này tại một vị trí công khai. Người gửi không cần phải thực hiện bất kỳ thỏa thuận bí mật với người nhận; người nhận

không cần có bất kỳ liên hệ trước nào với người gửi. Vì vậy có thể trao đổi thông tin một cách bảo mật bằng cách sử dụng thuật toán khóa công khai mà không cần trao đổi khóa một cách bí mật.

Trong hệ mật mã khóa công khai mỗi người dùng hoặc thiết bị tham gia vào quá trình gửi nhận thông tin có một cặp khóa, một khóa công khai và một khóa riêng, cùng với các quy tắc sử dụng khóa để thực hiện các hoạt động bảo mật dữ liệu. Chỉ người dùng hoặc thiết bị biết khóa riêng của mình, còn khóa công khai được phân phối đến tất cả người dùnghoặc thiết bị khác tham gia vào hệ thống. Vì việc biết khoá công khai không ảnh hưởng tới sự an toàn của các thuật toán, có thể dễ dàng trao đổi khoá công khai trực tuyến. Thông tin cần bảo mật có thể được trao đổi trực tuyến bằng cách trao đổi thông tin đã mã hóa và khóa công khai. Những người chỉ có quyền truy cập vào các thông tin trao đổi công khai sẽ không thể tính toán để giải mã thông tin, trừ khi họ có quyền truy cập và biết khóa riêng của của các bên giao tiếp.

3. Mật mã đối xứng và phi đối xứng

3.1 Mật mã đối xứng

Ngày nay, với sự phát triển bùng nổ của internet, nhu cầu trao đổi thông tin qua mạng ngày càng được ứng dụng rộng rãi trên tất cả mọi lĩnh vực với lượng thông tin giao dịch ngày càng lớn và đa dạng, dung lượng tệp trao đổi rất lớn. Tuy nhiên, đây cũng chính là môi trường thuận lợi để tội phạm máy tính ngày càng gia tăng, chúng thực hiện các cuộc tấn công vào các hệ thống nhằm khai thác thông tin, lấy cắp tài khoản để trục lợi, lừa đảo người dùng… Tội phạm máy tính rất đa dạng, ngày càng gia tăng về số lượng, độ tinh vi, mức độ nghiêm trọng và tổn thất.

Với sự xuất hiện của máy tính, các tài liệu văn bản và các thông tin quan trọng đều được số hóa và xử lý trên máy tính, đồng thời được truyền đi trên một môi trường mà mặc định là không an toàn. Do đó, yêu cầu về việc có một cơ chế, giải pháp để bảo vệ sự an toàn và bí mật của các thông tin nhạy cảm, quan trọng ngày càng trở nên cấp thiết. Việc bảo vệ dữ liệu là vấn đề mà tất cả những ai sử dụng

máy tính đều phải quan tâm. Mã hóa được xem là mức bảo vệ tối ưu nhất đối với dữ liệu, giúp thông tin không bị lộ và nâng cao độ an toàn trong các giao dịch truyền tải thông tin. Sự ra đời của ngành mật mã học đã giải quyết phần nào mong muốn đó.

Cho đến nay, đã có nhiều phương pháp mã hóa và các thuật toán tương ứng với mỗi phương pháp được ứng dụng để mã hóa thông tin, tiêu biểu là mật mã đối xứng (symmetric cryptography) và phi đối xứng (asymmetric cryptography).

Mật mã đối xứng sử dụng cùng một khóa cho cả hai quá trình mã hóa và giải mã. Ưu điểm của phương pháp này là tốc độ xử lý nhanh. Tuy nhiên, khả năng bảo mật chưa thực sự được an toàn khi cần trao đổi thông tin ở mức xử lý với nhiều bên nhận và gửi dữ liệu. Thuật toán mật mã đối xứng được biết đến rộng rãi là AES. Đây là một chuẩn mật mã cao cấp với khóa bí mật cho phép xử lý các khối dữ liệu đầu vào sử dụng các khóa có độ dài 128, 192, 256 bit.

3.2 Mật mã phi đối xứng

Mật mã phi đối xứng, hay còn được gọi là mật mã khóa công khai (public key cryptography) có nguyên tắc hoạt động là mỗi bên tham gia truyền tin sẽ có hai khóa. Một khóa được dùng để mã hóa và có thể được công bố công khai để bất kỳ ai cũng có thể sử dụng khóa này để gửi tin cho chủ thể (được gọi là khóa công khai – public key) và một khóa được dùng trong quá trình giải mã và được giữ bí mật (gọi là khóa bí mật – private key). Khóa giải mã không thể tính toán được từ khóa mã hóa.

Ưu điểm của mật mã phi đối xứng là việc quản lý khóa sẽ linh hoạt và hiệu quả hơn. Người sử dụng chỉ cần bảo vệ khóa bí mật của mình. Tuy nhiên, nhược điểm của mật mã khóa công khai nằm ở tốc độ thực hiện, nó chậm hơn rất nhiều so với mã hóa đối xứng.

CHƯƠNG II: NHIỆM VỤ VÀ CÔNG VIỆC CHÍNH

1. Lựa chọn ngôn ngữ

Ngôn ngữ Python

2. Nội dung công việc

2.1 Tìm hiểu về hệ mã hóa AES

- Đặc điểm, lịch sử phát triển
- Cách AES mã hóa và giải mã thông tin
- Ứng dụng của AES trong mã hóa thông tin

2.2 Tìm hiểu về hệ mã hóa đường cong ECC

- Đặc điểm của đường cong Elliptic
- Cách tạo khóa Kpub và Kpr bởi ECC
- Ứng dụng của ECC

2.3 Tìm hiểu mô hình trao đổi dữ liệu qua internet

- Cách thức bên gửi tạo khóa, mã hóa khóa SK và gửi dữ liệu.
- Cách thức bên nhận tạo khóa công khai, khóa bí mật, giải mã khóa SK và giải mã dữ liệu nhận.

2.4 Phân tích bài toán ***"Ứng dụng hệ thống mã hóa lai vào công tác bảo mật trong truyền tải đề thi"***

- Viết chương trình đề mô với ngôn ngữ Python

CHƯƠNG III: NỘI DUNG THUẬT TOÁN

1. Thuật toán mã hóa khóa đối xứng AES

1.1 Giới thiệu chung

Tổng quan

- AES (viết tắt của từ tiếng anh: Advanced Encryption Standard, hay Tiêu chuẩn mã hóa nâng cao) là một thuật toán mã hóa khối được chính phủ Hoa Kỳ áp dụng làm tiêu chuẩn mã hóa.
- Thuật toán được xây dựng dựa trên Rijndael Cipher phát triển bởi 2 nhà mật mã học người Bỉ: Joan Daemen và Vincent Rijmen.
- AES làm việc với các khối dữ liệu 128bit và độ dài khóa 128bit, 192bit hoặc 256bit. Các khóa mở rộng sử dụng trong chu trình được tạo ra bởi thủ tục sinh khóa Rijndael.
- Hầu hết các phép toán trong thuật toán AES đều thực hiện trong một trường hữu hạn của các byte. Mỗi khối dữ liệu đầu vào 128bit được chia thành 16byte, có thể xếp thành 4 cột, mỗi cột 4 phần tử hay một ma trận 4x4 của các byte, nó gọi là ma trận trạng thái.
- Tùy thuộc vào độ dài của khóa khi sử dụng 128bit, 192bit hay 256bit mà thuật toán được thực hiện với số lần lặp khác nhau.

Các bước xử lý chính

- Quá trình mở rộng khóa sử dụng thủ tục sinh khóa Rijndael.
- Quá trình mã hóa.

1.2 Xây dựng thuật toán

Xây dựng bảng S-box thuận

a. Bảng S-box thuận:

- Bảng S-box thuận được sinh ra bằng việc xác định nghịch đảo cho một giá trị nhất định trên GF(28) = GF(2)[x] / (x8+x4+x3+x+1) (trường hữu hạn Rijindael). Giá trị 0 không có nghịch đảo thì được ánh xạ với 0. Những nghịch đảo được chuyển đổi thông qua phép biến đổi affine.

- Công thức tính các giá trị bảng S-box và bảng S- box tương ứng:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

b. Bảng S-box nghịch đảo

- S-box nghịch đảo chỉ đơn giản là S-box chạy ngược. Nó được tính bằng phép biến đổi affine nghịch đảo các giá trị đầu vào. Phép biến đổi affine nghịch đảo được biểu diễn như sau:

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

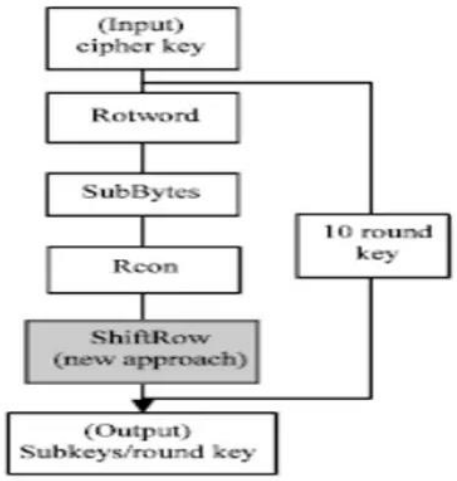
	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1x	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2x	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3x	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4x	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5x	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6x	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7x	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8x	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9x	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
ax	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
bx	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
cx	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
dx	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
ex	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
fx	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Giải thuật sinh khóa phụ

Quá trình sinh khóa gồm 4 bước:

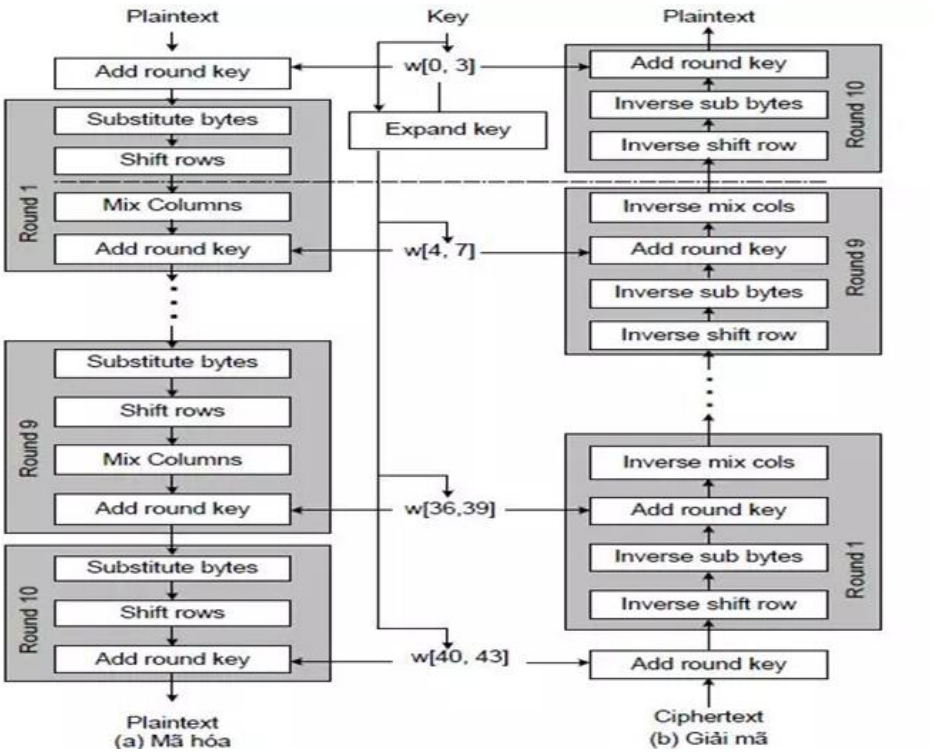
- Rotword: quay trái 8 bít
- SubBytes
- Rcon: tính giá trị Rcon(i) Trong đó : Rcon(i) = x(i-1) mod (x8 + x4 + x3 + x + 1).
- ShiftRow

Hình minh họa quy trình sinh khóa:



Quá trình mã hóa

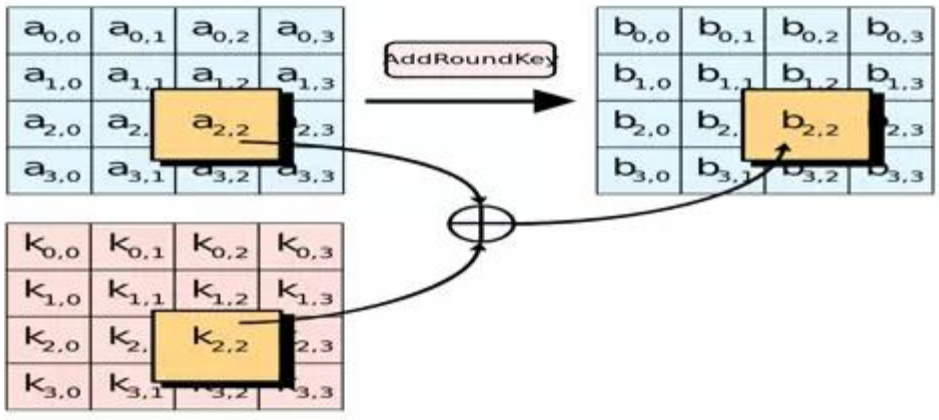
a. Sơ đồ tổng quát



b. Hàm AddRoundKey

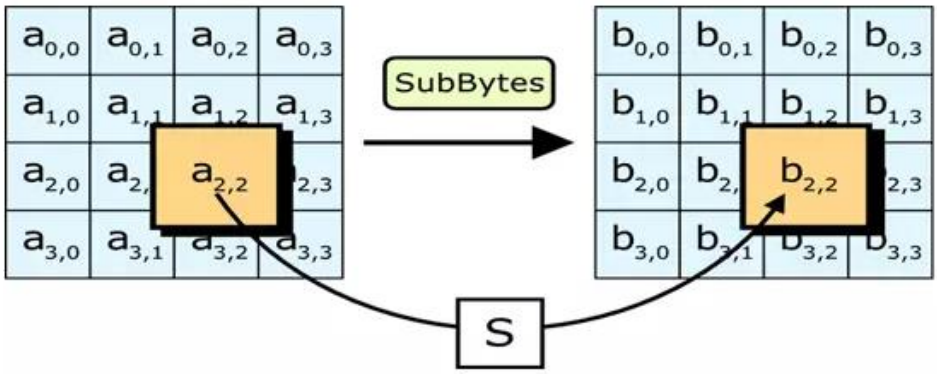
- Được áp dụng từ vòng lặp thứ 1 tới vòng lặp Nr
- Trong biến đổi Addroundkey(), một khóa vòng được cộng với state bằng một phép XOR theo từng bit đơn giản.
- Mỗi khóa vòng gồm có 4 từ (128 bit) được lấy từ lịch trình khóa. 4 từ đó được cộng vào mỗi cột của state, sao cho:

  [S'0,c, S'1,c, S'2,c, S'3,c] = [S0,c, S1,c, S2,c, S3,c] □ [W(4*i + c)] với 0 <= c < 4.



c. Hàm SubBytes

- Biến đổi SubBytes() thay thế mỗi byte riêng rẽ của state Sr,c bằng một giá trị mới S’ r,c sử dụng bảng thay thế (S - box) được xây dựng ở trên.



d. Hàm ShiftRow

- Trong biến đổi ShiftRows(), các byte trong ba hàng cuối cùng của trạng thái được dịch vòng đi các số byte khác nhau (độ lệch). Cụ thể :

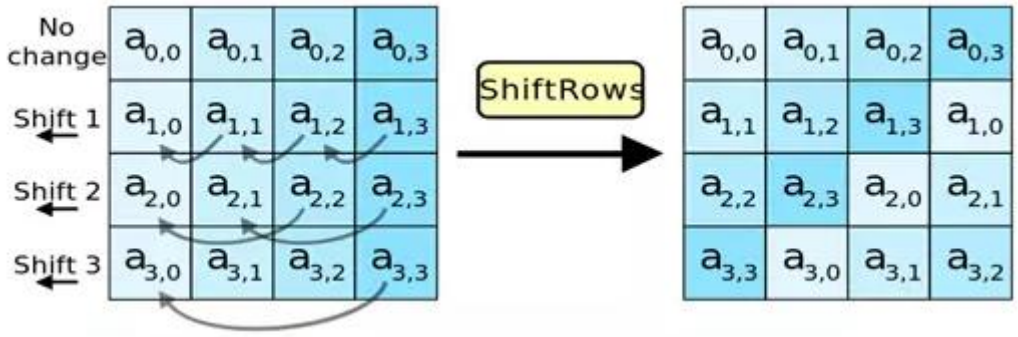
  S’r,c = Sr,(c + shift (r, Nb)) mod Nb (Nb = 4)

- Trong đó giá trị dịch shift (r, Nb) phụ thuộc vào số hàng r như sau:

  Shift(1,4) = 1, shift(2,4) = 2, shift(3,4) = 3.

- Hàng đầu tiên không bị dịch, ba hàng còn lại bị dịch tương ứng:
  - Hàng thứ 1 giữ nguyên.
  - Hàng thứ 2 dịch vòng trái 1 lần.

- Hàng thứ 3 dịch vòng trái 2 lần.
- Hàng thứ 4 dịch vòng trái 3 lần.



e. Hàm MixColumns

- Biến đổi MixColumns() tính toán trên từng cột của state. Các cột được coi như là đa thức trong trường GF(28) và nhân với một đa thức a(x) với:

  a(x) = (03)x^3 +(01)x^2 +(01)x + (02)

- Biến đổi này có thể được trình bày như phép nhân một ma trận, mà mỗi byte được hiểu như là một phần tử trong trường GF(28):

  s’(x) = a(x) □ s(x)

- Biến đổi này có thể được trình bày như phép nhân một ma trận, mà mỗi byte được hiểu như là một phần tử trong trường GF(28): s’(x) = a(x) □ s(x):
- Mô tả bằng ma trận như sau:

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix}$$

- Thuật toán mã hóa:

```
Cipher ( byte in [16], word w[44], byte out[16] )
begin
        byte state [ 4, 4 ]
        state = in
        AddRoundKey ( state, w [ 0, 3 ] )
        for round = 1 step 1 to 9
                SubBytes (state)
                ShiftRows (state)
                MixColumns (state)
                AddRoundKey ( state, w [ 4*round, 4*(round + 1) – 1 ] )
        end for
        SubBytes (state)
        ShiftRows (state)
        AddRoundKey ( state, w [ 40, 43 ] )
        out = state
end
```

Trong đó : in[] : Mảng dự liệu đầu vào Input.

out[] : Mảng dữ liệu đầu ra Output.

W[] : Mảng các w[i] có độ dài 4 bytes.

Quá trình giải mã

- Thuật toán giải mã khá giống với thuật toán mã hóa về mặt cấu trúc nhưng 4 hàm sử dụng là 4 hàm ngược của quá trình mã hóa.

Mã Hóa	Giải Mã
AddRoundKey()	InvAddRoundKey()
SubBytes()	InvSubBytes()
ShiftRows()	InvShiftRows()
MixColumns()	InvMixColumns()

- Thuật toán giải mã:

```
InvCipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin

byte state[4,Nb]
state = in
AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
for round = Nr-1 downto 1
    InvShiftRows(state)
    InvSubBytes(state)
    AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
    InvMixColumns(state)
end for

InvShiftRows(state)
InvSubBytes(state)
AddRoundKey(state, w[0, Nb-1])
out = state
end
```

Trong đó : In[] : Mảng dự liệu đầu vào Input.

Out[] : Mảng dữ liệu đầu ra Output.

Nr : Số vòng lặp.(Nr = 10).

Nb : Số cột(Nb = 4).

W[] : Mảng các w[i] có độ dài 4 bytes.

1.3 Các dạng tấn công vào AES và phương pháp phòng chống.

Side-channel attack.

- Side Channels (Kênh kề) được định nghĩa là các kênh đầu ra không mong muốn từ một hệ thống.

- Tấn công kênh bên hay còn gọi là Tấn công kênh kề là loại tấn công dễ thực hiện trong các loại tấn công mạnh chống lại quá trình triển khai mã hóa, và mục tiêu của loại tấn công này là phân tích các nguyên tố, các giao thức, modul, và các thiết bị trong mỗi hệ thống.

- Phân loại :

+ Tấn công thời gian.

+ Tấn công dựa vào lỗi.

+ Tấn công phân tích năng lượng.

+ Tấn công phân tích điện từ.

Known attacks

- Vào năm 2002, Nicolas Courtois và Josef Pieprzyk phát hiện một tấn công trên lý thuyết gọi là tấn công XSL và chỉ ra điểm yếu tiềm tàng của AES.

- Tuy nhiên, một vài chuyên gia về mật mã học khác cũng chỉ ra một số vấn đề trong cơ sở toán học của tấn công này và cho rằng các tác giả đã có sai lầm trong tính toán. Việc tấn công dạng này có thực sự trở thành hiện thực hay không vẫn còn để ngỏ và cho tới nay thì tấn công XSL vẫn chỉ là suy đoán.

1.4 Các phương pháp phòng chống

- Phương pháp 1: Mã hóa cực mạnh

Sử dụng các biện pháp để tăng tính bảo mật của các thuật toán mã hóa.

- Phương pháp 2: Bảo vệ dữ liệu theo phương pháp vật lý

Nếu một kẻ tấn công không thể tiếp cận vật lý với dữ liệu, dĩ nhiên khả năng đánh cắp khóa mã hóa sẽ khó khăn hơn. Vì vậy, trước những cuộc tấn công qua âm thanh tiềm tàng, bạn có thể sử dụng các giải pháp bảo vệ vật lý như đặt laptop vào các hộp cách ly âm thanh, không để ai lại gần máy tính khi đang giải mã dữ liệu hoặc sử dụng các nguồn âm thanh băng rộng tần số đủ cao để gây nhiễu.

- Phương pháp 3: Kết hợp cả 2 cách trên.

2. Thuật toán mã hóa khóa bất đối xứng ECC.

2.1 Định Nghĩa:

Hệ mã hóa đường cong Elliptic (ECC - Elliptic Curve Cryptography) là một giải thuật mã hóa dữ liệu được sử dụng trong các ứng dụng bảo mật. Nó được xây dựng trên các đường cong hình elip và được sử dụng rộng rãi trong các ứng dụng bảo mật như mã hóa tin nhắn, tạo chữ ký số và xác thực người dùng.

ECC có khả năng mã hóa và giải mã dữ liệu một cách hiệu quả với độ dài khóa ngắn hơn so với các giải thuật khác, nhưng vẫn đảm bảo độ bảo mật cao. Vì vậy, nó thường được sử dụng trong các ứng dụng yêu cầu bảo mật cao nhưng cần sử dụng không quá nhiều không gian bộ nhớ hoặc tài nguyên hệ thống.

ECC là một trong những giải thuật mã hóa dữ liệu mạnh mẽ và được ưa chuộng trong các ứng dụng bảo mật. Nó được xây dựng trên các đường cong hình elip và sử dụng các khóa để mã hóa và giải mã dữ liệu.

Một điểm ưu việt của ECC là nó có khả năng mã hóa và giải mã dữ liệu một cách hiệu quả với độ dài khóa ngắn hơn so với các giải thuật khác, nhưng vẫn đảm bảo độ bảo mật cao. Vì vậy, ECC thường được sử dụng trong các ứng dụng yêu cầu bảo mật cao nhưng cần sử dụng không quá nhiều không gian bộ nhớ hoặc tài nguyên hệ thống.

ECC cũng được sử dụng rộng rãi trong các ứng dụng mạng, như mã hóa tin nhắn, tạo chữ ký số và xác thực người dùng. Nó còn được sử dụng trong các ứng dụng khác nhau như giao dịch điện tử, bảo vệ dữ liệu truyền tải qua mạng và bảo vệ thông tin cá nhân.

Đây là một ví dụ minh họa về cách sử dụng ECC để mã hóa và giải mã một tin nhắn:

- Người gửi tin nhắn sẽ sử dụng một khóa công khai để mã hóa tin nhắn. Khóa công khai này là một khóa được công bố công khai và có thể được sử dụng bởi bất kỳ ai để mã hóa tin nhắn gửi đến người gửi.

- Sau khi mã hóa, tin nhắn được gửi đi và nhận bởi người nhận.
- Người nhận sẽ sử dụng một khóa bí mật để giải mã tin nhắn. Khóa bí mật này là một khóa được bảo mật và chỉ có người nhận mới có thể sử dụng để giải mã tin nhắn.
- Sau khi giải mã, người nhận có thể đọc được nội dung của tin nhắn và trả lời lại người gửi bằng cách sử dụng cùng quy trình mã hóa và giải mã.

2.2 Ưu và Nhược Điểm:

Mã hóa ECC (Elliptic Curve Cryptography) là một phương pháp mã hóa được sử dụng để bảo mật thông tin trong mạng lưới. Nó được xem là một trong những phương pháp mã hóa tốt nhất hiện nay vì có rất nhiều ưu điểm như sau:

- Độ bảo mật cao: Mã hóa ECC có khả năng bảo vệ dữ liệu của bạn với độ bảo mật cao hơn so với các phương pháp mã hóa khác.
- Độ nhẹ: Mã hóa ECC có khả năng mã hóa và giải mã thông tin mà không cần nhiều tài nguyên hệ thống. Do đó, nó thường được sử dụng trong các thiết bị có cấu hình thấp hoặc các mạng lưới không có đủ tài nguyên để sử dụng các phương pháp mã hóa khác.
- Độ linh hoạt: Mã hóa ECC có thể được sử dụng với nhiều loại khóa khác nhau và có thể điều chỉnh độ mạnh của khóa dựa trên nhu cầu bảo mật của người sử dụng.

Tuy nhiên, mã hóa ECC cũng có một số nhược điểm như sau:

- Khó học: Mã hóa ECC là một phương pháp mã hóa khá phức tạp và có nhiều khái niệm toán học khó hiểu đối với những người không có kiến thức toán học sâu sắc.
- Tốc độ chậm: So với các phương pháp mã hóa khác, mã hóa ECC có tốc độ chậm hơn trong việc mã hóa và giải mã thông tin.

- Phụ thuộc vào khóa: Mã hóa ECC phụ thuộc rất nhiều vào khóa mà bạn sử dụng. Nếu khóa bị đánh cắp hoặc mất, thông tin mã hóa sẽ không thể giải mã được.
- Độ phức tạp cao: Mã hóa ECC có độ phức tạp cao trong việc thiết lập và quản lý hệ thống bảo mật. Nó cũng có những rào cản trong việc sử dụng trong các hệ thống lớn và phức tạp.

3. AES và ECC – Một phương pháp kết hợp tiên tiến

- ECC là một kỹ thuật mã hóa nổi tiếng sử dụng mã hóa khóa bất đối xứng sau đây và bảo vệ dữ liệu khỏi truy cập trái phép. Nó sử dụng các cặp khóa công khai và khóa riêng để đảm bảo tính bảo mật của ECC. Trường hai chiều được ECC sử dụng làm trường nhị phân và trường nguyên tố. Việc hack không dễ dàng nếu chúng ta đang sử dụng kỹ thuật mã hóa này vì em nó sử dụng các hoạt động nâng cao và tạo mối quan hệ giữa các trường nhị phân và trường chính và mối quan hệ này trong ECC không thể được đọc bởi những người không được ủy quyền. Kích thước khóa nhỏ là yếu tố chính của ECC. Số điểm tối đa có thể giúp tìm trường thích hợp để triển khai mã hóa trên dữ liệu cho các biện pháp bảo mật. Hoạt động đầu tiên của trường chọn số đầu tiên và sau đó tạo số lớn dựa trên dữ liệu nằm trong khoảng từ 0 đến Z. Cụ thể, để tạo khóa, ECC được sử dụng và giảm độ phức tạp của các thao tác. Do kích thước khóa thấp, khả năng tăng cường của ECC nhiều hơn so với các kỹ thuật mã hóa khác.

- AES là một trong những loại văn bản mật mã sử dụng mật mã khối. Điều này chỉ sử dụng một khóa cho quá trình mã hóa và giải mã để bảo mật dữ liệu. Nó có nhiều hoạt động hiệu suất đang giới hạn trên bộ nhớ đám mây như phân tích thống kê, tìm kiếm trên bộ nhớ đám mây và các hoạt động khác tương tự. Đây là thuật toán chiến lược được sử dụng rộng rãi trên điện toán đám mây để cải thiện các quy tắc bảo mật đối với lưu trữ đám mây.

- ECC và AES tạo ra kỹ thuật mã hóa tiên tiến và hiệu quả nhất trên bộ lưu trữ đám mây. Có thể nói rằng AES đơn chậm hơn một chút so với phương thức kết hợp (ECC-AES) do kích thước khóa lớn hơn, trong khi phương thức kết hợp cho phép giảm kích thước khóa cũng như cơ chế bảo mật nhanh hơn để bảo mật dữ liệu. Vì kích thước khóa nhỏ là thuộc tính chính của ECC, nên khi AES sử dụng ECC để mã hóa, kích thước khóa sẽ giảm và hiệu suất được tăng lên. ECC sử dụng các tiêu chuẩn khóa mã hóa và giải mã để giảm kích thước khóa và tạo hệ thống khóa bảo mật. ECC là kỹ thuật thích hợp nhất để sử dụng cùng với AES để bảo mật dữ liệu khỏi việc sử dụng trái phép. Khi kích thước khóa được đặt, thì

bản mã sẽ tạo mã hóa và giải mã dữ liệu. Khóa được tạo bởi ECC được sử dụng bởi AES. Hiệu ứng kết hợp của cả ECC và AES phù hợp với kỹ thuật đề xuất tại lưu trữ đám mây để có được hệ thống bảo mật. Điều này giúp giảm kích thước lưu trữ với dữ liệu an toàn. Dưới đây, trong Hình 5 , là sơ đồ khối của thuật toán được đề xuất.

3.1 Thuật toán AES – ECC:

- Tạo khóa công khai bằng ECC:

Bước I. Chọn một số n bất kì làm số nguyên tố.

Bước II. Chọn bất kỳ số nào để tạo khóa chung là n (a)

Trong đó n (a) < n

Bước III. Tính điểm trên đường cong là G

Trường hợp G > n

Bước IV. Tính toán khóa công khai là:

$P = n(a) * G$

Bước V. Trả lại khóa công khai P sau khi tính toán.

- Mã hóa và giải mã bằng AES:

Bước I. Lấy tệp đầu vào

Bước II. Bây giờ, hãy thêm khóa do ECC tạo, đây là khóa chung.

Bước III. Mã hóa AES được thực hiện trên tệp đầu vào bằng cách sử dụng khóa chung do ECC tạo.

Bước IV. Tệp được mã hóa được tải lên máy chủ sau khi mã hóa bằng AES.

Bước V. Sau khi tệp được tải lên, tệp sẽ được tải xuống tại máy chủ, sau đó tệp được dịch bằng cách sử dụng khóa chung do ECC cung cấp để tệp gốc được giải mã.

Bước VI. Hiệu suất của hệ thống phụ thuộc vào tác động kết hợp của ECC và AES

3.2 Ưu và Nhược điểm

ECC được sử dụng để đảm bảo tính bảo mật của dữ liệu. Việc duy trì dữ liệu với kích thước khóa giảm có thể giúp tối ưu hóa không gian lưu trữ cũng như đạt được kết quả mong muốn. Nó sử dụng cùng 3072 bit như RSA. Điều có lợi nhất về ECC là giảm kích thước khóa và mã hóa dữ liệu thông qua khóa chung, theo cách tối ưu hóa. ECC có lợi hơn so với RSA vì sử dụng các kỹ thuật thuật toán mới nhất áp dụng cho mã hóa và giải mã dữ liệu cũng như độ chính xác của dữ liệu được giải mã.

AES có nhiều hoạt động hiệu suất đang giới hạn trên bộ lưu trữ đám mây như phân tích thống kê, tìm kiếm trên bộ nhớ đám mây và các hoạt động khác tương tự. Đây là thuật toán chiến lược được sử dụng rộng rãi trên điện toán đám mây để cải thiện các quy tắc bảo mật đối với lưu trữ đám mây. Khóa chung được mọi người biết trong khi quá trình mã hóa và giải mã cũng có thể được thực hiện bằng khóa chung.

Nhiều ưu điểm và kích thước chính của ECC và AES so với RSA được đưa ra trong bảng dưới.

ECC	RSA	So sánh kích thước phím
160 bit	1024 bit	1:6 bit
256 bit	3024 bit	1:12 bit
384 bit	7068 bit	1:20 bit
512 bit	16360 bit	1:20 bit

So sánh với các thuật toán mã hóa khác:

Factors	Proposed Hybrid	DES	3DES	Blowfish	RSA	Diffie-Hellman
No. of key	1	1	1	1	2	Key Exchange
Key Length in bits	64–256	56	112–168	32–448	1024	Key Exchange
Rounds	10	16	48	16	1	56
Limitation	Brute force	Brute force	Computational power	Key frequently changing	Key generation week	Cannot encrypt data

#	Kích thước tệp (KB)	Thời gian mã hóa (ms)						Thời gian giải mã (ms)					
		ECC	AES	Hybrid	RSA	Tỉ lệ		ECC	AES	Hybrid	RSA	Tỉ lệ	
						ECC /Hibrid	RSA /Hibrid					ECC /Hibrid	RSA /Hibrid
	Độ dài khoá AES – 128 (ECC – 256, RSA – 512)												
1	2 209	105	90	92	9 877	**107**	**1.15**	116	109	109	69 503	**639**	**1.07**
2	5 378	141	123	125	27 205	**218**	**1.13**	266	207	207	107 681	**520**	**1.28**
3	9 617	274	234	235	35 503	**151**	**1.17**	333	294	294	198 594	**674**	**1.13**
	Độ dài khoá EAS – 256 (ECC – 512, RSA – 1024)												
4	2 209	227	122	123	39 879	**324**	**1.85**	241	136	136	276 957	**2036**	**1.77**
5	5 378	299	158	160	112 381	**702**	**1.87**	542	236	236	437 562	**1854**	**2.30**
6	9 617	563	278	280	149 325	**533**	**2.01**	678	337	337	798 534	**2370**	**2.01**

Bảng 1. *So sánh thời gian thực thi giữa thuật toán ECC, RSA, mật mã lai(ECC+AES)*

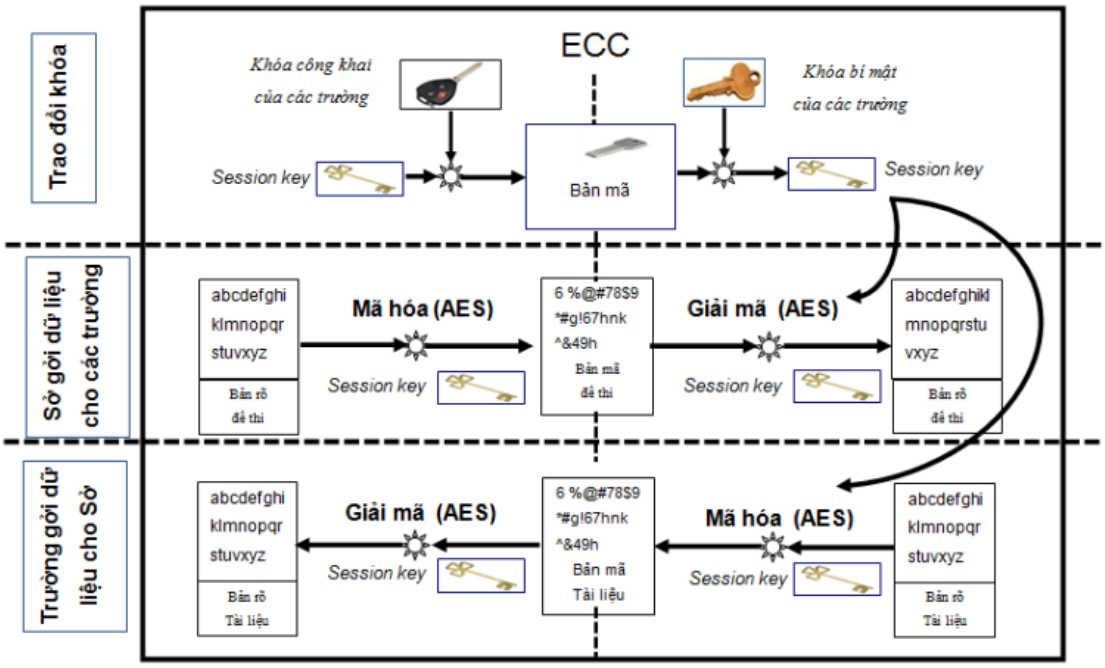
CHƯƠNG IV: THIẾT KẾ, CÀI ĐẶT CHƯƠNG TRÌNH ĐỀ MÔ THUẬT TOÁN

Trên thực tế, mật mã đối xứng và mật mã phi đối xứng, mặc dù có nhiều ưu điểm so với các phương pháp mã hóa trước đó, nhưng với nhược điểm của mình nên vẫn chưa thể được sử dụng một cách rộng rãi trong tất cả mọi lĩnh vực ứng dụng. Để khắc phục các nhược điểm trên, giải pháp là kết hợp hai phương pháp mã hóa này, cụ thể là kết hợp chuẩn mật mã AES và hệ mật mã đường cong elliptic với nhau và được gọi là hệ thống mã hóa lai (Hybrid Cryptosystems). Với sự kết hợp này, hệ thống đã tận dụng được các điểm mạnh của hai hệ thống ở trên đó là tốc độ của mật mã đối xứng và tính an toàn của mật mã phi đối xứng.

*** Giải pháp**

Hiện tại, các trường trung học phổ thông (TTHPT) và SGD&ĐT đều đã được trang bị các máy tính có cấu hình đủ mạnh để chạy các phần mềm có yêu cầu cấu hình cao và đều đã được kết nối internet. Do đó, việc tin học hóa hệ thống quản lý đề thi trong các trường phổ thông dưới sự quản lý của SGD&ĐT có thể được triển khai theo mô hình sau:

Tại máy chủ của SGD&ĐT (bên A) và các TTHPT (bên B), chúng ta cài đặt phần mềm, ví dụ có tên “Phần mềm truyền tải đề thi”. Mỗi khi tiến hành đợt thi, việc truyền tải đề thi sẽ được thực hiện thông qua phần mềm theo nguyên tắc dùng mật mã phi đối xứng ECC để truyền khoá mật mã đối xứng AES, dữ liệu là nội dung đề thi sẽ được mã hoá theo phương pháp đối xứng AES và truyền tải qua kênh thông thường (Hình 1).



Hình 1. *Mô hình trao đổi dữ liệu qua internet*

Khoá bí mật do SGD&ĐT lưu giữ.

Khóa công khai sẽ được gửi cho các TTHPT hoặc được công bố công khai trênwebsite.

* Thực hiện việc trao đổi khóa mật mã đối xứng:

- Bên B sinh khoá mã hoá AES cho phiên làm việc, gọi là SK. SK là một chuỗi ký tự ngẫu nhiên.

- Bên B dùng khoá công khai ECC mã hoá SK và gửi dữ liệu SK đã mã hoá cho bên A.

- Bên A dùng khoá bí mật ECC để giải mã và thu được SK. Cả bên A và bên B đều lưu giữ SK để dùng cho mã hoá dữ liệu đề thi cũng như các dữ liệu trao đổi khác bằng AES.

* Bên A gửi dữ liệu (đề thi) cho các trường:

- Bên A sử dụng SK đã nhận được để mã hóa đề thi

- Đề thi đã được mã hóa sẽ được chuyển cho bên B qua kênh thông thường

- Bên B sử dụng SK giải mã và thu được nội dung đề thi.

* Trường phổ thông gửi dữ liệu cho SGD&ĐT

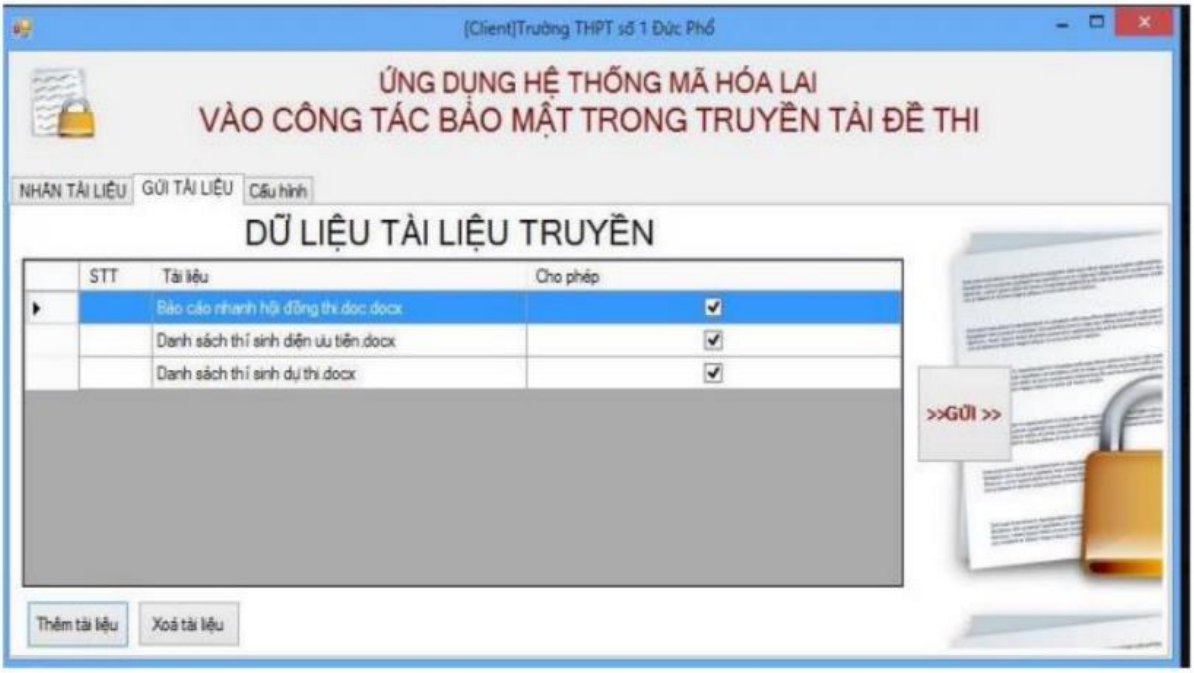
Cũng tương tự trường hợp bên A gửi dữ liệu cho bên B, các bên tham gia tiến hành theo các bước sau:

- Bên B dùng SK để mã hóa dữ liệu
- Dữ liệu đã được mã hóa sẽ được chuyển cho bên A thông qua kênh thông thường
- Bên A dùng SK để giải mã và thu được dữ liệu mà bên B cần chuyển.

CHƯƠNG V: GIAO DIỆN CHƯƠNG TRÌNH ĐỀ MÔ

1. Sở GD truyền đề thi đến các trường

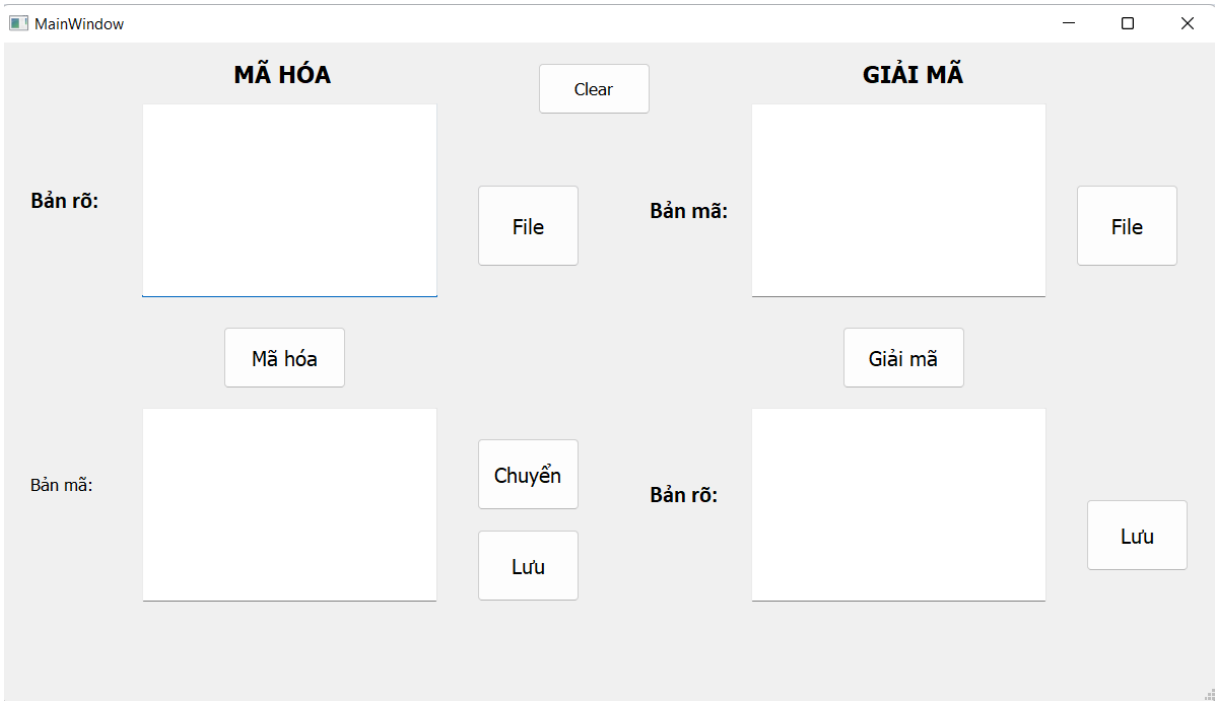
Hình 2. *SGD&ĐT truyền đề thi đến các trường*



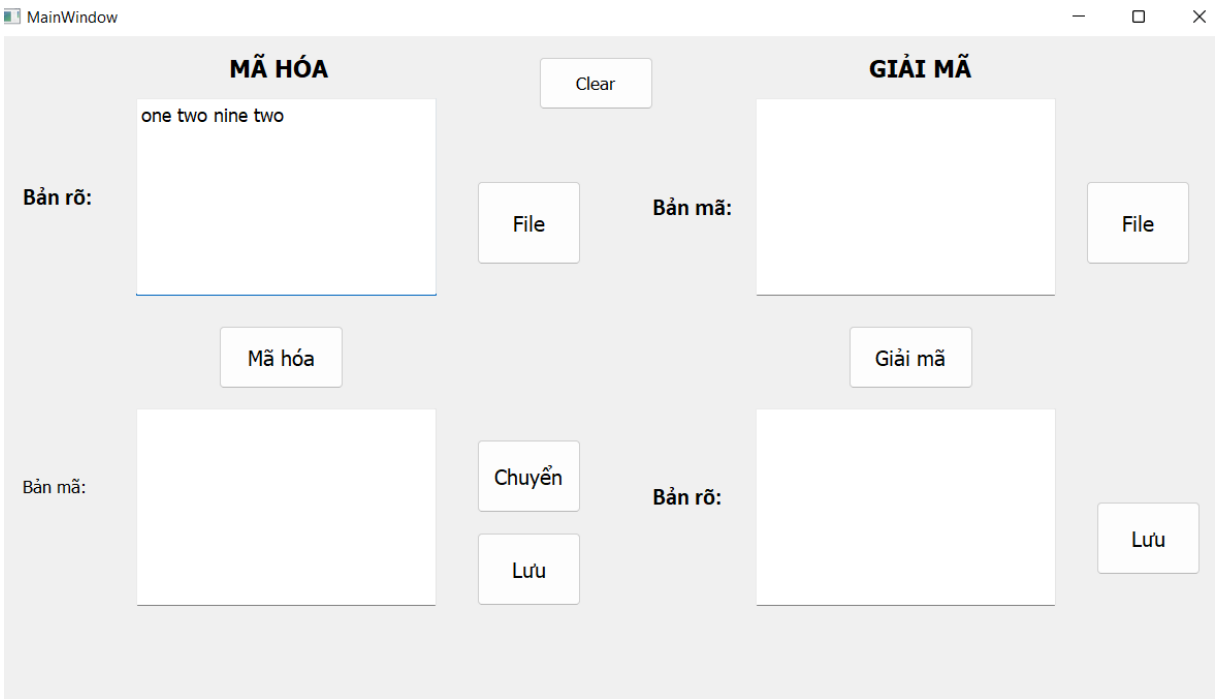
Hình 3. *Các trường truyền dữ liệu cho sở GD&ĐT*

2. Chương trình demo (Ngôn ngữ Python)

- Giao diện lúc bắt đầu vào chương trình:

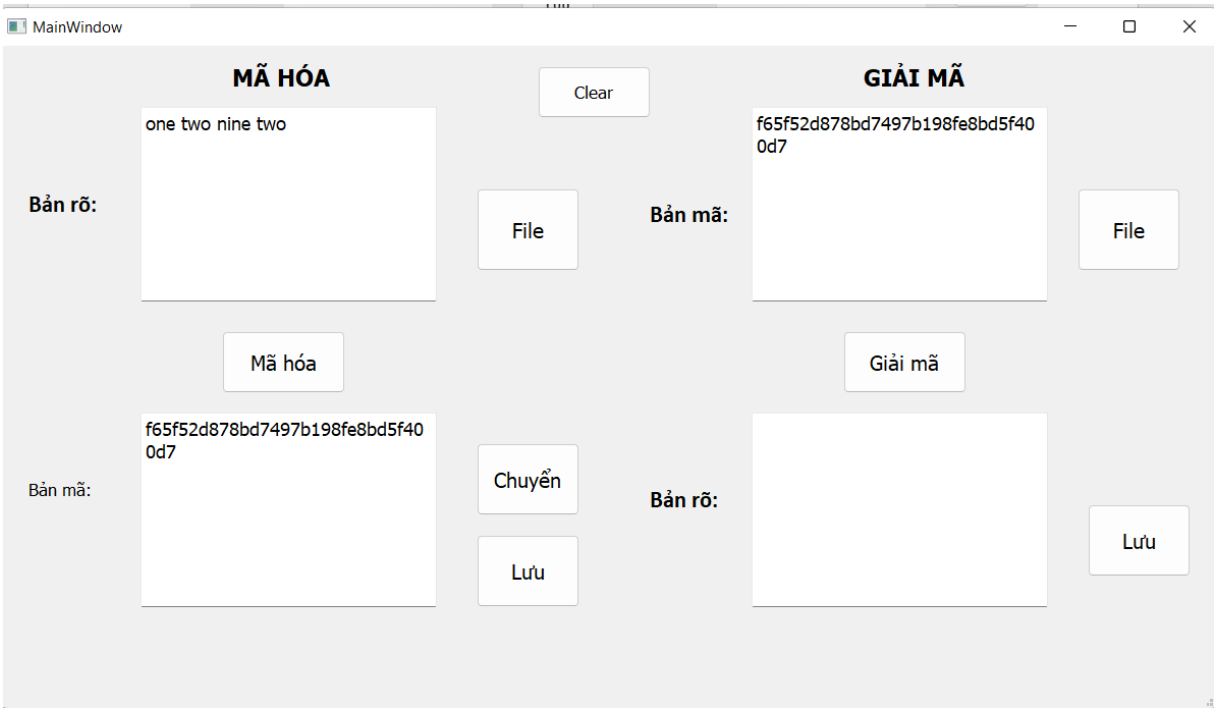


- Nhập thông tin cần mã hóa vào ô bản rõ bằng cách nhập trực tiếp hoặc nhấn nút File để nhập.

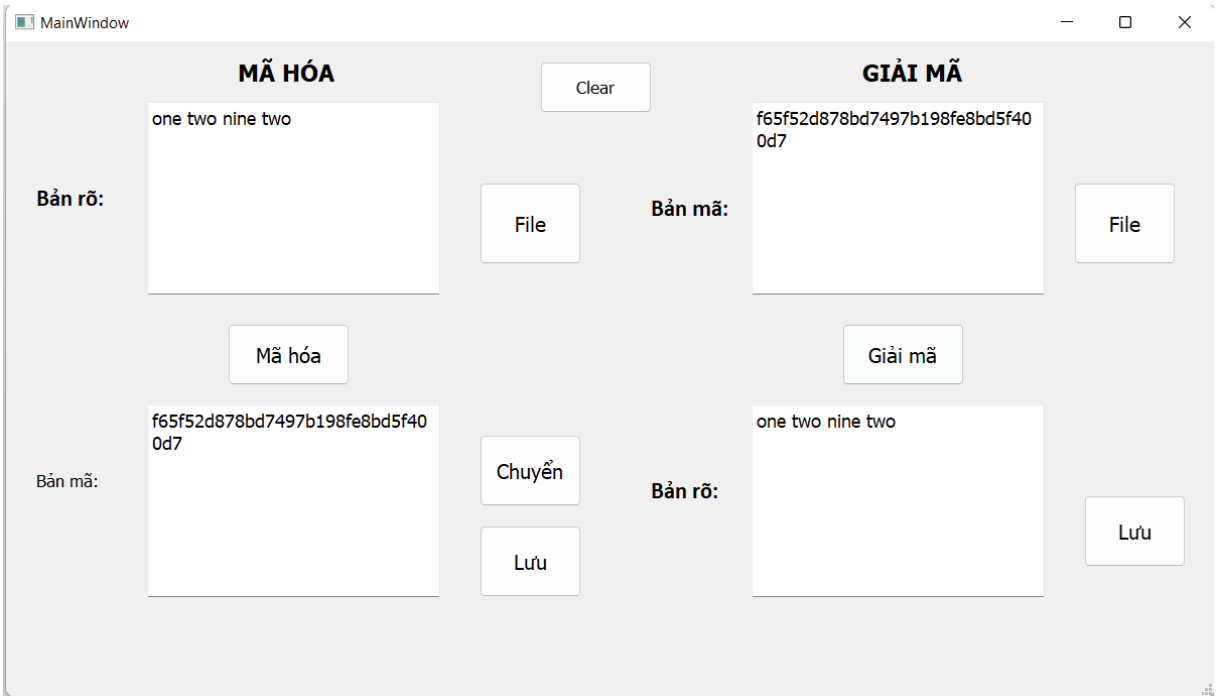


- Sau khi nhập xong bản rõ ta nhấn nút ‘Mã hóa’ để mã hóa bản rõ và thu được bản mã ở ô ‘Bản mã’

- Ta nhấn nút ‘Chuyển’ để chuyển bản mã xang ô ‘Bản mã’ để tiến hành giải mã.



- Ta có thể nhấn nút ‘Lưu’ để lưu bản mã thành File
- Ta tiếp tục giải mã bản rõ vừa mà hóa bằng cách nhấn nút ‘Giải mã’ để tiến hành Giải mã.



- Ta thu được bản rõ như ban đầu.

CHƯƠNG VI: KIẾN THỨC LĨNH HỘI VÀ BÀI HỌC KINH NGHIỆM

1. Nội dung đã thực hiện

1.1 Các kiến thức đã lĩnh hội

- Hiểu được mã hóa AES
- Quá trình mã hóa AES
- Quá trình giải mã AES
- Hiểu được mã hóa ECC
- Thực hiện việc mã hóa và giải mã
- Cài đặt được chương trình demo
- Hiểu được quá trình truyền tải dữ liệu, khóa trong thi tuyển sinh

1.2 Các kĩ năng đã tiếp thu

- Đánh giá được vai trò của bảo mật, các cơ chế, chính sách bảo mật, các kiểu tấn công và các phương pháp phòng thủ.
- 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 AES như (sinh khóa, mã hóa, giải mã) vào việc mã hóa và giải mã để giải quyết bài toán có tính ứng dụng vào thực tiễn.
- Bên cạnh đó còn có các kĩ năng như: kĩ năng viết báo cáo, kỹ năng quản lý thời gian, kỹ năng sử dụng các công cụ,…
- Học thêm về ngôn ngữ lập trình mới.

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.
- Đặt tinh thần trách nhiệm trong công việc lên ưu tiên hàng đầu

2. Những thuận lợi và khó khăn

2.1 Thuận lợi:

- Có thể đọc hiểu được tài liệu tiếng Anh nên có thể tiếp cận được với 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 đề tài.

2.2 Khó khăn:

- Công đoạn cài đặt giao diện phần mềm chưa được bắt mắt do chưa có nhiều kinh nghiệm trong kỹ thuật xử lý giao diện.
- Ở phần xử lý file Docx còn gặp nhiều khó khăn, do khá mới mẻ

CHƯƠNG VII: KẾT LUẬN

Qua quá trình thực hiện đề tài và giải quyết bài toán ***"Ứng dụng hệ thống mã hóa lai vào công tác bảo mật trong truyền tải đề thi"***, nhóm chúng em đã trang bị thêm cho mình nhiều kiến thức về mã hóa thông tin thực sự cần thiết, hiểu thêm được tầm quan trọng của việc mã hóa thông tin và dữ liệu.

Mã hóa thông tin kết hợp các hệ mã hóa khóa đối xứng cũng như khóa bất đối xứng mang đến một giải pháp mã hóa thông tin tuyệt vời, đặc biệt là sự kết hợp của hệ mã AES và ECC. ECC hiện đang được sử dụng trong một loạt các ứng dụng: chính phủ Mỹ sử dụng để bảo vệ thông tin liên lạc nội bộ, các dự án Tor sử dụng để giúp đảm bảo ẩn danh, đây cũng là cơ chế được sử dụng để chứng minh quyền sở hữu trong Bitcoins, cung cấp chữ ký số trong dịch vụ iMessage của Apple, để mã hóa thông tin DNS với DNSCurve, và là phương pháp tốt để xác thực cho các trình duyệt web an toàn qua SSL/TLS. Thế hệ đầu tiên của thuật toán mã hóa khóa công khai như RSA và Diffie-Hellman vẫn được duy trì trong hầu hết các lĩnh vực, nhưng ECC đang nhanh chóng trở thành giải pháp thay thế cho RSA. Trong kỷ nguyên công nghệ thông tin và truyền thông hiện nay, nhu cầu đảm bảo an toàn thông tin là không thể thiếu. Với việc khóa mã hóa có độ dài ngày tăng dần theo thời gian, ECC đang là ứng viên phù hợp để thay thế RSA trong việc tạo ra các khóa mã ngắn hơn mà vẫn đảm bảo an toàn, từ đó có thể triển khai trên nhiều nền tảng thiết bị từ các mạch điện tử đơn giản đến máy tính lớn, dễ dàng tạo ra hệ thống mạng đáng tin cậy phục vụ tốt hơn cho xã hội.

Do kích thước khóa thấp, khả năng tăng cường của ECC tốt hơn nhiều so với các kỹ thuật mã hóa khác. AES kết hợp với ECC có thể làm tốt hơn rất nhiều với việc tối ưu hóa và bảo mật dữ liệu. Tuy nhiên, vẫn cần nhiều bảo mật trong tương lai để mở rộng khái niệm điện toán đám mây thông qua các kỹ thuật mật mã. Trong tương lai, nghiên cứu này có thể được cải thiện bằng cách tăng tính bảo mật của phương pháp kết hợp. Nhiều lớp bảo mật có thể được thêm vào để nâng cao năng suất và hiệu quả của hệ thống. AES kết hợp với ECC có thể làm tốt hơn rất nhiều với việc tối ưu hóa và bảo mật dữ liệu.

Đề tài mà nhóm em thực hiện là một đề tài có tính ứng dụng cao, không chỉ có thể áp dụng cho truyền tải đề thi trên mạng cho các cuộc thi quan trọng cần tính bảo mật cao như kỳ thi THPTQG hay các cuộc thi chọn học sinh giỏi của Quốc gia, tỉnh, huyện mà còn có thể áp dụng để truyền tải dữ liệu lớn trên không gian mạng như áp dụng cho các ngân hàng, các công ty hay doanh nghiệp… Điều này đòi hỏi đề tài cần được thảo luận nhiều hơn trên các diễn đàn mã hóa thông tin quốc gia hay quốc tế.

Trong quá trình thực hiện đề tài, do kiến thức còn nhiều hạn chế và thiếu sót, nhóm chúng em mong nhận được sự góp ý của cô để đề tài cũng như ứng dụng của các thành viên trong nhóm được đầy đủ và hoàn thiện hơn về kiến thức cũng như các chức năng của ứng dụng đề mô.

Nhóm chúng em xin chân thành cảm ơn!

TÀI LIỆU THAM KHẢO

1. Tiếng Việt

[1]. Giáo trình An toàn và bảo mật thông tin - Thư viện điện tử trường Đại học Công nghiệp Hà Nội, http://thuvienso.haui.edu.vn/tailieuvn/doc/giao-trinh-an-toan-bao-mat-thong-tin-2381912.html

2. Internet

[2]. Tìm hiểu thuật toán mã hóa khóa đối xứng AES

https://viblo.asia/p/tim-hieu-thuat-toan-ma-hoa-khoa-doi-xung-aes-gAm5yxOqldb

[3]. Tiêu chuẩn Elliptic Curve Cryptography (ECC)

https://aita.gov.vn/tieu-chuan-elliptic-curve-cryptography-ecc.-1

[4]. Hybrid AES-ECC Model for the Security of Data over Cloud Storage

https://www.mdpi.com/2079-9292/10/21/2673/htm