Nhom8 Bao Cao BTL Atbmtt 20223 IT6001001

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

BỘ CÔNG THƯƠNG

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

•••□□□□□•••

BÀI TẬP LỚN
Môn: An toàn và bảo mật thông tin

ĐỀ TÀI 8:
ỨNG DỤNG HỆ THỐNG MÃ HOA LAI VÀO CÔNG TÁC BẢO MẬT TRONG TRUYỀN TẢI ĐỀ THI

GVHD: ThS. Trần Phương Nhung

Nhóm : 8

Thành viên nhóm:

1. Nguyễn Viết Khánh - 2020604925
2. Trần Đăng Khoa - 2020603025
3. Bùi Trung Kiên - 2021602075
4. Mai Thị Khánh Linh - 2021608512

Hà Nội – 2023

MỤC LỤC

MỤC LỤC HÌNH ẢNH

LỜI CẢM ƠN

Lời đầu tiên, nhóm chúng em xin gửi lời cảm ơn sâu sắc đến cô ***Ths. Trần Phương Nhung****. Trong quá trình tìm hiểu và học tập bộ môn An toàn và bảo mật thông tin, chúng em đã được cô cung cấp và truyền đạt tất cả kiến thức chuyên môn cần thiết và quý giá nhất. Ngoài ra, chúng em còn được rèn luyện một tinh thần học tập và làm việc độc lập , sáng tạo. Đây là tính cách hết sức cần thiết để có thể thành công khi bắt tay vào nghề nghiệp trong tương lai. Nhóm đã nhận được sự hướng dẫn và những chia sẻ rất tận tình, tâm huyết của cô. Từ những hướng dẫn tận tình của cô cùng với kiến thức mà nhóm đã học tập, tìm hiểu, chúng em đã hoàn thành báo cáo đề tài "****Ứng dụng mã hóa lai vào công tác bảo mật trong truyền tải đề thi****". Đây là cơ hội để nhóm em có thể áp dụng, tìm hiểu thêm và tổng kết lại những kiến thức mà mình đã học. Đồng thời, rút ra được những kinh nghiệm thực tế và quý giá trong suốt quá trình thực hiện đề tài.*

Với tất cả sự cố gắng, nỗ lực của mình, nhóm em đã hoàn thành tốt nhất bài báo cáo này.Trong quá trình thực hiện đề tài, do kiến thức còn nhiều hạn chế và thiếu sót, nhóm chúng em chắc chắn không tránh khỏi những thiếu sót khi thực hiện . Nhóm chúng em mong nhận được sự góp ý của cô để đề tài cũng như ứng dụng demo 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. Sự phê bình, góp ý của cô sẽ là những bài học kinh nghiệm rất quý báu cho công việc thực tế của chúng em sau này .

Kính chúc cô thật nhiều sức khoẻ, hạnh phúc và thành công trong cuộc sống.

Nhóm chúng em xin chân thành cảm ơn!

LỜI NÓI 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 vẫn 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 AES (Advanced Encryption Standard) từng được chính phủ Mỹ và nhiều quốc gia trên thế giới sử dụng. Đến giờ, AES vẫn được dùng cho các tài liệu tuyệt mật, được cho là FIPS (Federal Information Processing Standard - tiêu chuẩn xử lý thông tin liên bang). Sau đó nó được dùng trong khối tư nhân, là chuẩn mã hóa phổ biến nhất với mã hóa khóa đối xứng.

Bên cạnh đó mật mã đường cong Elip (Elliptic curve cryptography - ECC) là kĩ thuật mã khóa công khai dựa trên lý thuyết về đường cong elip, giúp tạo mật mã nhanh hơn, nhỏ hơn và mạnh hơn. 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 hệ thống mã hóa lai vào công tác bảo mật trong truyền tải đề thi"*** với mong muốn áp dụng kiến thức đã học, giải quyết bài toán bảo mật .

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.

Chương 1. Tổng quan

1.1. Tổng quan về an toàn và bảo mật thông tin

1.1.1.Sự cần thiết của việc đảm bảo an toàn thông tin

Ngày nay sự xuất hiện của internet toàn cầu đã giúp cho việc trao đổi thông tin trở nên nhanh gọn, dễ dàng. Các phương thức chia sẻ dữ liệu qua mạng làm cho việc trao đổi, mua bán, chuyển tiền, … diễn ra mỗi ngày trên nền tảng số.

Tuy nhiên vấn đề mới lại phát sinh. Những thông tin đang nằm ở kho dữ liệu hay đang được truyền đi có thể bị trộm cắp, bị làm sai lệch, giả mạo. Điều này làm ảnh hưởng đến độ an toàn của thông tin nhạy cảm, tin mật, … có thể tác động lớn đến nhiều cá nhân, tổ chức, hay ác động đến an ninh quốc gia.

1.1.2.Khái niệm an toàn thông tin

Định nghĩa của an toàn thông tin được nêu ra từ nhiều nguồn khác nhau, chúng ta có thể hiểu theo nhiều cách sau: *An toàn thông tin nghĩa là thông tin được bảo vệ, các hệ thống và dịch vụ có khả năng chống lại những sự can thiệp, lỗi và những tai họa không mong đợi, các thay đổi tác động đến độ an toàn của hệ thống là nhỏ nhất. Hệ thống không an toàn là hệ thống tồn tại những điểm: thông tin bị rò rỉ ra ngoài, thông tin bị thay đổi, ...*

Giá trị thực sự của thông tin chỉ đạt được khi thông tin được cung cấp chính xác và kịp thời, hệ thống phải hoạt động chuẩn xác thì mới có thể đưa ra những thông tin có giá trị cao. *Mục tiêu của an toàn bảo mật trong công nghệ thông tin là đưa ra một số tiêu chuẩn an toàn và áp dụng các tiêu chuẩn an toàn này vào chỗ thích hợp để giảm bớt và loại trừ những nguy hiểm có thể xảy ra.* Ngày nay với kỹ thuật truyền nhận và xử lý thông tin ngày càng phát triển và phức tạp nên hệ thống chỉ có thể đạt tới một mức độ an toàn nào đó và không có một hệ thống an toàn tuyệt đối.

1.1.3.Các yêu cầu an toàn bảo mật thông tin

Khi nhu cầu trao đổi thông tin dữ liệu ngày càng lớn và đa dạng, các tiến bộ về điện tử - viễn thông và công nghệ thông tin không ngừng được phát triển ứng dụng để nâng cao chất lượng và lưu lượng truyền tin thì các quan niệm ý tưởng và biện pháp bảo vệ thông tin dữ liệu cũng được đổi mới. Bảo vệ an toàn thông tin dữ liệu là một chủ đề rộng, có liên quan đến nhiều lĩnh vực và trong thực tế có thể có rất nhiều phương pháp được thực hiện để bảo vệ an toàn thông tin dữ liệu. Các phương pháp bảo vệ an toàn thông tin dữ liệu có thể được quy tụ vào ba nhóm sau:

- Bảo vệ an toàn thông tin bằng các biện pháp hành chính.

- Bảo vệ an toàn thông tin bằng các biện pháp kỹ thuật (phần cứng).

- Bảo vệ an toàn thông tin bằng các biện pháp thuật toán (phần mềm).

Ba nhóm trên có thể được ứng dụng riêng rẽ hoặc phối kết hợp. Môi trường khó bảo vệ an toàn thông tin nhất và cũng là môi trường đối phương dễ xâm nhập nhất đó là môi trường mạng và truyền tin. Biện pháp hiệu quả nhất và kinh tế nhất hiện nay trên mạng truyền tin và mạng máy tính là biện pháp thuật toán.

Biện pháp hiệu quả nhất và kinh tế nhất hiện nay trên mạng truyền tin và mạng máy tính là biện pháp thuật toán.

Ngày nay, với sự phát triển rất nhanh của khoa học công nghệ, các biện pháp tấn công ngày càng tinh xảo hơn, độ an toàn của thông tin có thể bị đe dọa từ nhiều nơi, theo nhiều cách khác nhau, chúng ta cần phải đưa ra các chính sách đề phòng thích hợp. Các yêu cầu cần thiết của việc bảo vệ thông tin và tài nguyên:

- *Đảm bảo bí mật (Bảo mật):* thông tin không bị lộ đối với người không được phép.
- *Đảm bảo tính tin cậy (Confidentiality):* Thông tin và tài nguyên không thể bị truy cập trái phép bởi những người không có quyền hạn.
- *Đảm bảo tính toàn vẹn (Integrity):* Thông tin và tài nguyên không thể bị sửa đổi, bị thay thế bởi những người không có quyền hạn.
- *Đảm bảo tính sẵn sàng (Availability):* Thông tin và tài nguyên luôn sẵn sàng để đáp ứng sử dụng cho người có quyền hạn.
- *Đảm bảo tính không thể chối bỏ (Non-repudiation):* Thông tin và tài nguyên được xác nhận về mặt pháp luật của người cung cấp.

Các nội dung an toàn thông tin

- *Nội dung chính:*
  - An toàn máy tính: là sự bảo vệ các thông tin cố định bên trong máy tính, là khoa học về bảo đảm an toàn thông tin trong máy tính
  - An toàn truyền tin: là sự bảo vệ thông tin trên đường truyền tin(thông tin được truyền từ hệ thống này sang hệ thống khác), là khoa học bảo đảm an toàn thông tin trên đường truyền tin.
- *Nội dung chuyên ngành:*
  - An toàn dữ liệu (data security)
  - An toàn cơ sở dữ liệu (database security)
  - An toàn hệ điều hành (operation system security)
  - An toàn mạng máy tính (network security)

Các chiến lược bảo đảm an toàn thông tin

*Giới hạn quyền hạn tối thiểu (Last Privilege):*theo nguyên tắc này bất kỳ một đối tượng nào cùng chỉ có những quyền hạn nhất định đối với tài nguyên mạng.

Bảo vệ theo chiều sâu (Defence In Depth): Không nên dựa vào một chế độ an toàn nào dù cho chúng rất mạnh, mà nên tạo nhiều cơ chế an toàn để tương hỗ lẫn nhau.

Nút thắt (Choke Point): Tạo ra một "cửa khẩu" hẹp, và chỉ cho phép thông tin đi vào hệ thống của mình bằng con đường duy nhất chính là "cửa khẩu" này.

*Điểm nối yếu nhất (Weakest Link):*Chiến lược này dựa trên nguyên tắc: " Một dây xích chỉ chắc tại mắt duy nhất, một bức tường chỉ cứng tại điểm yếu nhất".

Tính toàn cục: Các hệ thống an toàn đòi hỏi phải có tính toàn cục của các hệ thống cục bộ.

Tính đa dạng bảo vệ: Cần phải sử dụng nhiều biện pháp bảo vệ khác nhau cho hệ thống khác nhau, nếu không có kẻ tấn công vào được một hệ thống thì chúng cũng dễ dàng tấn công vào các hệ thống khác.

1.1.4.Các phương pháp bảo vệ thông tin

Quyền truy nhập: Là lớp bảo vệ trong cùng nhằm kiểm soát các tài nguyên của mạng và quyền hạn trên tài nguyên đó.

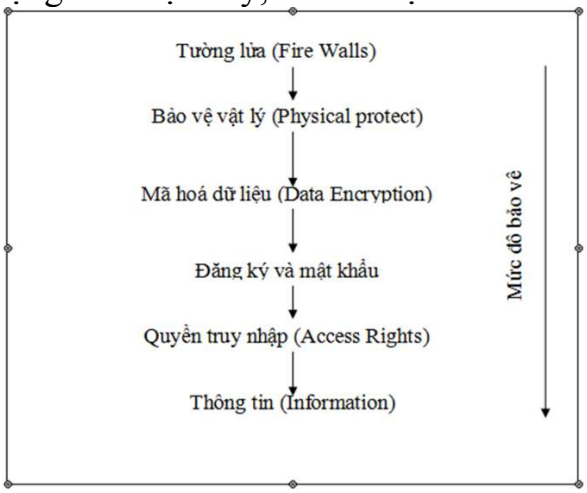
Đăng ký tên /mật khẩu: Thực ra đây cũng là kiểm soát quyền truy nhập, nhưng không phải truy nhập ở mức thông tin mà ở mức hệ thống.

Mã hoá dữ liệu: Dữ liệu bị biến đổi từ dạng nhận thức được sang dạng không nhận thức được theo một thuật toán nào đó và sẽ được biến đổi ngược lại ở trạm nhận (giải mã).

Bảo vệ vật lý: Ngăn cản các truy nhập vật lý vào hệ thống.

Tường lửa: Ngăn chặn thâm nhập trái phép và lọc bỏ các gói tin không muốn gửi hoặc nhận vì các lý do nào đó để bảo vệ một máy tính hoặc cả mạng nội bộ (intranet).

Quản trị mạng: Công tác quản trị mạng máy tính phải được thực hiện một cách khoa học. Toàn bộ hệ thống hoạt động bình thường trong giờ làm việc. Backup dữ liệu quan trọng theo định kỳ, có kế hoạch bảo trì định kỳ, bảo mật dữ liệu, phân quyền, …



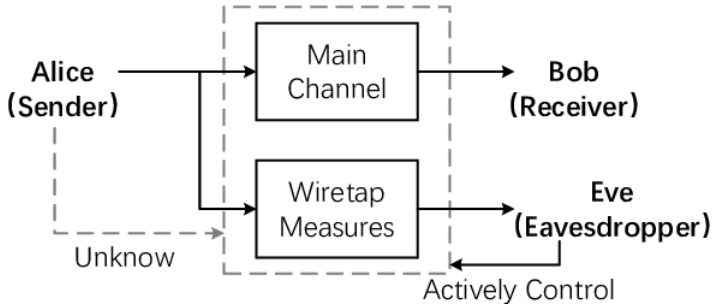
Hình 1 Các mức độ bảo vệ thông tin

1.2. An toàn thông tin bằng mật mã

1.2.1.Mật mã và thông tin

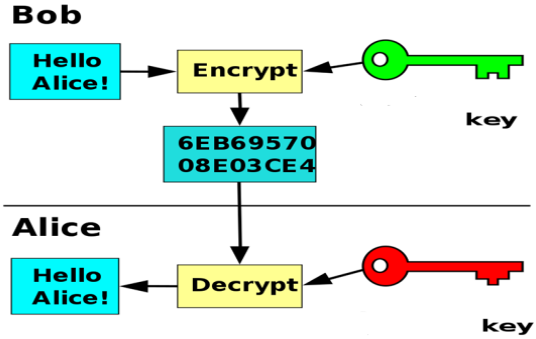
Mật mã là một ngành khoa học chuyên nghiên cứu các phương pháp truyền tin bí mật. Mật mã bao gồm : Lập mã và phá mã.

- *Lập mã* bao gồm hai quá trình: mã hóa và giải mã. Các sản phẩm của lĩnh vực này là các hệ mã mật , các hàm băm, các hệ chữ ký điện tử, các cơ chế phân phối, quản lý khóa và các giao thức mật mã.
- *Phá mã:* Nghiên cứu các phương pháp phá mã hoặc tạo mã giả. Sản phẩm của lĩnh vực này là các phương pháp phá mã , các phương pháp giả mạo chữ ký, các phương pháp tấn công các hàm băm và các giao thức mật mã.



Hình 2 Thông tin gửi đi bị nghe lén

Để bảo vệ thông tin trên đường truyền người ta thường biến đổi nó từ dạng nhận thức được sang dạng không nhận thức được trước khi truyền đi trên mạng, quá trình này được gọi là mã hoá thông tin (encryption), ở trạm nhận phải thực hiện quá trình ngược lại, tức là biến đổi thông tin từ dạng không nhận thức được (dữ liệu đã được mã hoá) về dạng nhận thức được (dạng gốc), quá trình này được gọi là giải mã (decryption). Đây là một lớp bảo vệ thông tin rất quan trọng và được sử dụng rộng rãi trong môi trường mạng.



Hình 3 Bảo vệ thông tin bằng mật mã

Để bảo vệ thông tin bằng mật mã người ta thường tiếp cận theo hai hướng:

- *Theo đường truyền (Link_Oriented_Security):* thông tin được mã hoá để bảo vệ trên đường truyền giữa hai nút mà không quan tâm đến nguồn và đích của thông tin đó. Thông tin chỉ được bảo vệ trên đường truyền, tức là ở mỗi nút đều có quá trình giải mã sau đó mã hoá để truyền đi tiếp, do đó các nút cần phải được bảo vệ tốt.
- *Từ nút đến nút (End_to_End):* thông tin trên mạng được bảo vệ trên toàn đường truyền từ nguồn đến đích. Thông tin sẽ được mã hoá ngay sau khi mới tạo ra và chỉ được giải mã khi về đến đích. Cách này mắc phải nhược điểm là chỉ có dữ liệu của

người dùng thì mới có thể mã hóa được còn dữ liệu điều khiển thì giữ nguyên để có thể xử lý tại các nút.

1.2.2.Hệ mật mã

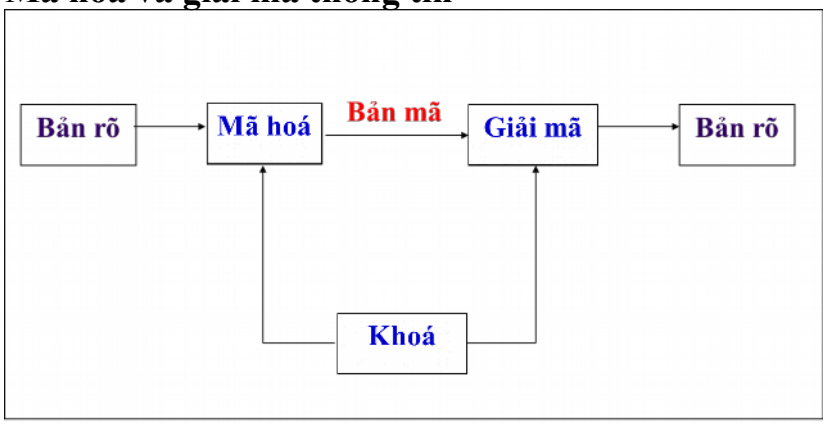
Vai trò của hệ mật mã

Các hệ mật mã phải thực hiện được các vai trò sau:

- Hệ mật mã phải che dấu được nội dung của văn bản rõ (PlainText) để đảm bảo sao cho chỉ người chủ hợp pháp của thông tin mới có quyền truy cập thông tin (Secrety), hay nói cách khác là chống truy nhập không đúng quyền hạn.
- Tạo các yếu tố xác thực thông tin, đảm bảo thông tin lưu hành trong hệ thống đến người nhận hợp pháp là xác thực (Authenticity).
- Tổ chức các sơ đồ chữ ký điện tử, đảm bảo không có hiện tượng giả mạo, mạo danh để gửi thông tin trên mạng.

Ưu điểm lớn nhất của bất kỳ hệ mật mã nào đó là có thể đánh giá được độ phức tạp tính toán mà "kẻ địch" phải giải quyết bài toán để có thể lấy được thông tin của dữ liệu đã được mã hoá. Tuy nhiên mỗi hệ mật mã có một số ưu và nhược điểm khác nhau, nhưng nhờ đánh giá được độ phức tạp tính toán mà ta có thể áp dụng các thuật toán mã hoá khác nhau cho từng ứng dụng cụ thể tuỳ theo yêu cầu về độ an toàn.

Mã hóa và giải mã thông tin



Quá trình mã hóa và giải mã thông tin

Hình 4 Quá trình mã hóa và giải mã thông tin

- Mã hóa: Quá trình chuyển đổi dữ liệu gốc thành dữ liệu được mã hóa sao cho người khác không thể đọc hiểu được.
- Giải mã: Là quá trình ngược lại của mã hóa, biến đổi dữ liệu đã được mã hóa thành dạng gốc ban đầu.
- Bản mã: Tệp dữ liệu đã được mã hóa.

Một hệ thống mã hóa bao gồm các thành phần sau:

- PlainText : Bản tin sẽ được mã hóa hay bản tin gốc.
- CipherText : Bản tin đã được mã hóa hay bản tin mã.
- Thuật toán mã hóa và giải mã :
  - Encryption : quá trình chuyển bản tin gốc sang dạng mật mã.
  - Decryption : quá trình giải bản tin dạng mật mã trở về bản tin gốc.
  - Cách chọn khóa : giá trị toán học dùng để thực hiện mã hóa.

Nhiều phương pháp mã hóa đã được đưa ra dựa trên những giải thuật toán phức tạp, để tạo khó khăn cho những ai đó muốn phá mật mã mà không cần được ai trao chìa khóa. Nói tạo khó khăn là vì trên lý thuyết ta không thể nói việc tìm chìa khóa là vô phương. Nhưng nếu trở ngại đủ lớn để làm nản lòng kẻ gian thì đã là một mức độ an toàn tốt. Quá trình mã hóa và giải mã có thể được minh họa theo sơ đồ sau:

Các thành phần của một hệ mật mã

Một hệ mã mật là bộ 5 (P, C, K, E, D) thoả mãn các điều kiện sau:

- P là tập hữu hạn các bản rõ (PlainText), nó được gọi là không gian bản rõ chứa bản tin gốc ban đầu.
- C là tập hợp hữu hạn bản mã (Crypto), nó còn được gọi là không gian các bản mã. Một phần tử của C có thể nhận được bằng cách áp dụng phép mã hóa E_k lên một phần tử P, với $k \in K$.
- K là tập hữu hạn các khóa hay còn gọi là không gian khoá. Đối với mỗi phần tử k của K được gọi là một khoá (Key). Số lượng của không gian khoá phải đủ lớn để "kẻ địch" không có đủ thời gian thử mọi khoá có thể (phương pháp vét cạn).
- Đối với mỗi $k \in K$ có một quy tắc mã e_k: $P \rightarrow C$ và một quy tắc giải mã tương ứng $d_k \in D$. Mỗi e_k: $P \rightarrow C$ và d_k: $C \rightarrow P$ là những hàm mà:

$d_k(e_k(x))=x$ với mọi bản rõ $x \in P$.

- Hàm giải mã d_k chính là ánh xạ ngược của hàm mã hóa e_k

Phân loại hệ mật mã

Có nhiều cách để phân loại hệ mật mã. Dựa vào cách truyền khóa có thể phân các hệ mật mã thành hai loại:

- Hệ mật đối xứng (hay còn gọi là mật mã khóa bí mật)
- Hệ mật mã bất đối xứng (hay còn gọi là mật mã khóa công khai)

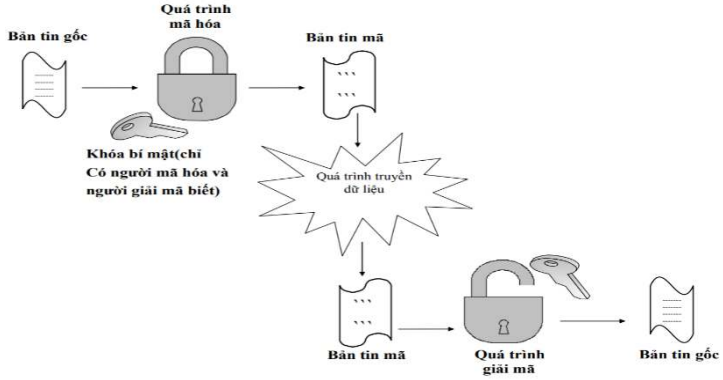
Ngoài ra nếu dựa vào thời gian đưa ra hệ mật mã ta còn có thể phân làm hai loại: Mật mã cổ điển (là hệ mật mã ra đời trước năm 1970) và mật mã hiện đại (ra đời sau năm 1970). Còn nếu dựa vào cách thức tiến hành mã thì hệ mật mã còn được chia làm hai loại là mã dòng (tiến hành mã từng khối dữ liệu, mỗi khối lại dựa vào các khóa khác nhau, các khóa này được sinh ra từ hàm sinh khóa, được gọi là dòng khóa) và mã khối (tiến hành mã từng khối dữ liệu với khóa như nhau).

Mã hóa bằng khóa bí mật

Các hệ thống mã hóa với khóa bí mật còn được gọi là mã hóa bằng khóa riêng, mã hóa đối xứng sử dụng duy nhất một khóa cho cả quá trình mã hóa lẫn quá trình giải mã.

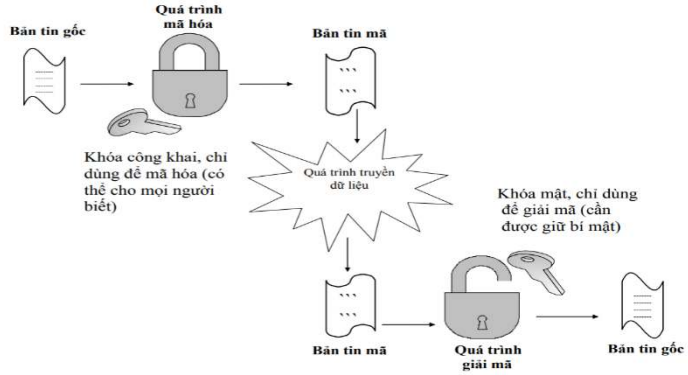
- Stream Algorithms/Stream Ciphers: các thuật toán hoạt động trên văn bản bình thường theo từng bit một.
- Block Algorithms/Block Ciphers : các thuật toán hoạt động trên văn bản theo các khối (32 bit, 64 bit, 128 bit, ...).
- Một số thuật toán đang được sử dụng rộng rãi hiện nay : DES, TripleDES, RC5, RC6, Rijndael ...

Quá trình mã hóa và giải mã bằng cách sử dụng khóa bí mật được minh họa như hình dưới đây:



Hình 5 Sơ đồ mã hóa và giải mã bằng khóa riêng

Mã hóa bằng khóa công khai



Hình 6 Sơ đồ mã hóa và giải mã bằng khóa công khai

Mã hóa bằng khóa công khai còn gọi là mã hóa bất đối xứng hay mã hóa bằng khóa chung. Sự khác biệt cơ bản giữa một hệ thống mã hóa bằng khóa bí mật với hệ thống mã hóa bằng khóa công khai là hệ thống mã hóa khóa công khai dùng hai khóa khác nhau để mã hóa và giải mã. Do đó, một bộ mã công khai sẽ bao gồm hai khóa: một khóa dành cho người mã hóa thường được công khai, và khóa còn lại dùng cho người giải mã thường được giữ bí mật. Như vậy, hệ thống mã hóa với khóa công khai cần có một quá trình sinh ra hai khóa để mã hóa và giải mã thông điệp. Các khóa này được xem như là một đôi:

- Public-key (khóa công khai): được phép công khai mà không phải chịu rủi ro về an toàn. Khóa này được dùng để mã hóa thông điệp.
- Private-key (khóa bí mật): không được để lộ. Mỗi thông điệp được mã hóa bằng public-key chỉ có thể giải mã bằng một khóa mật thích hợp.
- Một số thuật toán mã hóa công khai phổ biến : RSA, Diffie-Hellman KeyExchange Algorithm (dùng cho việc phân phối và trao đổi khóa).

Như vậy, với sự bùng nổ của mạng toàn cầu mọi hệ thống thông tin đều phải đương đầu với bài toán an toàn và bảo mật. Như đã trình bày, có nhiều chiến lược cũng như phương pháp bảo đảm bảo an toàn thông tin. Trong đó, an toàn thông tin bằng mật mã có vai trò pháp quan trọng và được ứng dụng rộng khắp không chỉ trong ngành công nghệ thông tin mà còn dùng để bảo mật những thông tin và tài liệu quan trọng ngoài đời. (Ví dụ như bảo mật đề thi trong tuyển sinh được đề cập đến trong chương sau)

1.3. Đề tài nghiên cứu

Đề tài: *Ứng dụng mã hóa lai vào công tác bảo mật trong truyền tải đề thi*

1.3.1.đối tượng nghiên cứu

Nghiên cứu về chương trình mã hóa và giải mã AES trong mật mã học, hệ mã hóa ECC.

An toàn thông tin là bảo vệ các đặc tính riêng tư (confidentialy), toàn vẹn (intergrity) và khả dụng (availabity) của thông tin.

- C: (Confidentialy) bảo vệ tính riêng tư của dữ liệu thông qua các cơ chế chứng thực và mã hóa, ngăn ngừa những người không hợp lệ sẽ không được đọc những thông tin. Giống như các bì thư khi phát lương thưởng được dán chữ Confidentialy, chúng ta có thể hình dung trong môi trường công nghệ thông tin là một người chưa đăng nhập vào Domain sẽ không được truy cập những dữ liệu chỉ chia sẻ cho các Domain User.

- I: (Intergrity) bảo vệ tính toàn vẹn của dữ liệu thông qua các thuật toán RSA, SHA, MD5 ... ngăn ngừa attacker thay đổi các thông tin nhạy cảm trong quá trình truyền.

- A: (Available) bảo đảm dữ liệu luôn ở trong trạng thái sẵn sằng đáp ứng nhu cầu của người dùng.

- Non-Repudiation: Tính không thể chối bỏ, nghĩa là dữ liệu người nào gửi đi thì họ phải có trách nhiệm với các thông tin của mình thông qua các xác nhận nguồn gốc như chữ kí điện tử.

Các bài báo đầu tiên của Diffie và Hellman đã đưa ra một cách tiếp cận mới đối với mật mã, và thực tế đã thách thức các nhà mật mã học để đưa ra một thuật toán mật mã đáp ứng các yêu cầu đối với các hệ thống khóa công khai. Một số thuật toán đã được đề xuất cho mật mã khóa công khai. Một số trong số này ban đầu đầy hứa hẹn sau đó nó lại có thể bị bẻ gãy.

1.3.2.Phạm vi nghiên cứu

Các kì thi lớn cần đảm bảo mức an toàn thông tin cao như các cuộc thi THPTQG hay cuộc thi cấp tỉnh và miền.

Có thể ứng dụng sang một số linh vực khác như truyền tải tin tình báo, thư mật và các tài liệu quan trong,...

1.3.3.Mục tiêu nghiên cứu

- Xác định và làm rõ các vấn đề liên quan đến đề tài.
- Phân tích chương trình mã hoá và giải mã AES.
- Phân tích hệ mã hóa ECC.
- Ứng dụng cài đặt chương trình mã hóa đề thi với các ngôn ngữ lập trình khác nhau.
- Xác định các ứng dụng thực tế sử dụng chương trình.

1.3.4.Kiến thực cần có

Hệ mật mã đối xứng còn gọi là mật mã khoá đơn hoặc là mật mã khoá riêng. Trong các hệ mật mã này, khoá mật mã mã hoá bảo mật giống với khoá giải mã hoặc trên thực tế là cùng đẳng cấp. Lúc này khoá mật mã cần phải có một đường truyền an toàn để truyền đưa khoá mật mã từ phía người truyền cho phía người nhận. Đặc điểm của mật mã đối xứng là bất luận khi gia công bảo mật hay là khi giải mã đều sử dụng cùng một khoá mật mã. Do đó tính an toàn của mật mã này là sự an toàn của khoá mật mã. nếu như khoá mật mã bị tiết lộ, thì hệ thống mật mã này sẽ bị phá vỡ.

Hệ mật mã bất đối xứng còn gọi là mật mã khoá công khai hoặc mật mã khoá đôi. Trong các hệ mật mã này quá trình mã hoá và giải mã có chìa khoá khác nhau, lúc này không cần có đường truyền an toàn để truyền đưa khoá mật mã mà chỉ cần bộ phát sinh khoá mã tại chỗ để tạo ra khoá giải mã đồng thời lấy đó để khống chế các thao tác giải mã.

Thuật toán **mật mã khóa công khai** được dựa trên các chức năng toán học thay vì thay thế và hoán vị. Quan trọng hơn, mật mã khóa công khai là không đối xứng bao gồm việc sử dụng hai khóa riêng biệt, trái ngược với mã hóa đối xứng, chỉ sử dụng một

khóa. Trước khi tiến hành, ta nên đề cập đến một số khái niệm sai lầm phổ biến liên quan đến mã hóa khóa công khai. Một quan niệm sai lầm như vậy là: Mật mã khóa công khai an toàn hơn từ việc phân tích mật mã hơn mã hóa đối xứng. Trong thực thế, bảo mật của bất kì chương trình mã hóa nào phụ thuộc vào độ dài của khóa và công việc tính toán liên quan đến phã vỡ một mật mã. Không có gì về nguyên tắc của mã hóa đối xứng hoặc mã hóa khóa công khai mà làm cho những cấp trên khác chống lại phân tích mật mã.

1.3.5.Phương pháp nghiên cứu

- Tìm kiếm tài liệu trên internet.
- Quản lý và lưu trữ tài liệu nghiên cứu trên cloud.
- Sử dụng các IDE Dev-C++, Eclipse, Netbeans, Visual Studio, VSCode để xây dựng chương trình.
- Sử dụng các ngôn ngữ lập trình C++, Java, C#, Python, Javascript.

Chương 2. Kết quả nghiên cứu

Như đã trình bày ở chương trước: mọi thông tin cần bảo vệ nên được mã hóa. Với sự phát triển của công nghệ, nhiều hệ mật mã khác nhau được ra đời từ các hệ mật mã truyền thống đến các hệ mật mã hiện đại. Từ những năm 70 của thế kỷ trước, các nhà khoa học đã nghiên cứa và tạo ra nhiều phương thức mật mã với tốc độ mã hóa rất

nhanh chỉ cần giữ bí mật khóa mã (mã hóa đối xứng) và mã hóa được mọi dữ liệu tùy ý. Đó là một bước tiến vĩ đại của kỹ thuật mật mã .Trong đó mã AES (Advanced Encryption Standard) và ECC là 2 chuẩn mã hóa rất phổ biến.

2.1.Giới thiệu

- Khi hoàn thiện xong chương trình thì sẽ thực hiện được các yêu cầu về chương trình mà đề tài đề ra như mã hóa AES, mã hóa đường cong Eliptic.
- Đề tài : Ứng dụng hệ thống mã hóa lai vào công tác bảo mật trong truyền tải đề thi.

2.1.1.Nội dung

1. Tìm hiểu mật mã AES.
2. Hệ mã hóa đường cong Elliptic(ECC)
3. Ứng dụng xây dựng chương trình demo.
4. Demo chương trình

2.1.2.Các yêu cầu cần giải quyết

1. Đọc tài liệu và hiểu được vấn đề đặt ra,nắm được các kiến thức về mã hóa AES và ECC một cách thành thạo(cả tiếng việt và tiếng anh).
2. Hiểu được vấn đề của bài toán.
3. Đọc hiểu được một số tài liệu chuyên môn bằng tiếng Anh
4. Nắm vững một ngôn ngữ lập trình cơ bản(Java,C#,C++,Matlab)và giải được bài toán có tính ứng dụng vào thực tiễn.

2.2.Nội dung thuật toán

2.2.1.Thuật toán AES

2.2.1.1Thuật toán

AES là thuật toán mã hóa khối, nó 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.

Thuật toán AES khá phức tạp, được mô tả khái quát gồm 3 bước như sau:

- 1 Vòng khởi tạo chỉ gồm phép AddRoundKey

- Nr -1 Vòng lặp gồm 4 phép biến đổi lần lượt: SubBytes, ShiftRows, MixColumns, AddRoundKey.
- 1 Vòng cuối gồm các phép biến đổi giống vòng lặp và không có phép MixColumns.

Khái quát:

1. Mở rộng khóa - Các khóa phụ dùng trong các vòng lặp được sinh ra từ khóa chính AES sử dụng thủ tục sinh khóa Rijndael.

2. InitialRound - AddRoundKey— Mỗi byte trong state được kết hợp với khóa phụ sử dụng XOR

3. Rounds - SubBytes—bước thay thế phi tuyến tính, trong đó mỗi byte trong state được thay thế bằng một byte khác sử dụng bảng tham chiếu - ShiftRows—bước đổi chỗ, trong đó mỗi dòng trong state được dịch một số bước theo chu kỳ - MixColumns—trộn các cột trong state, kết hợp 4 bytes trong mỗi cột - AddRoundKey

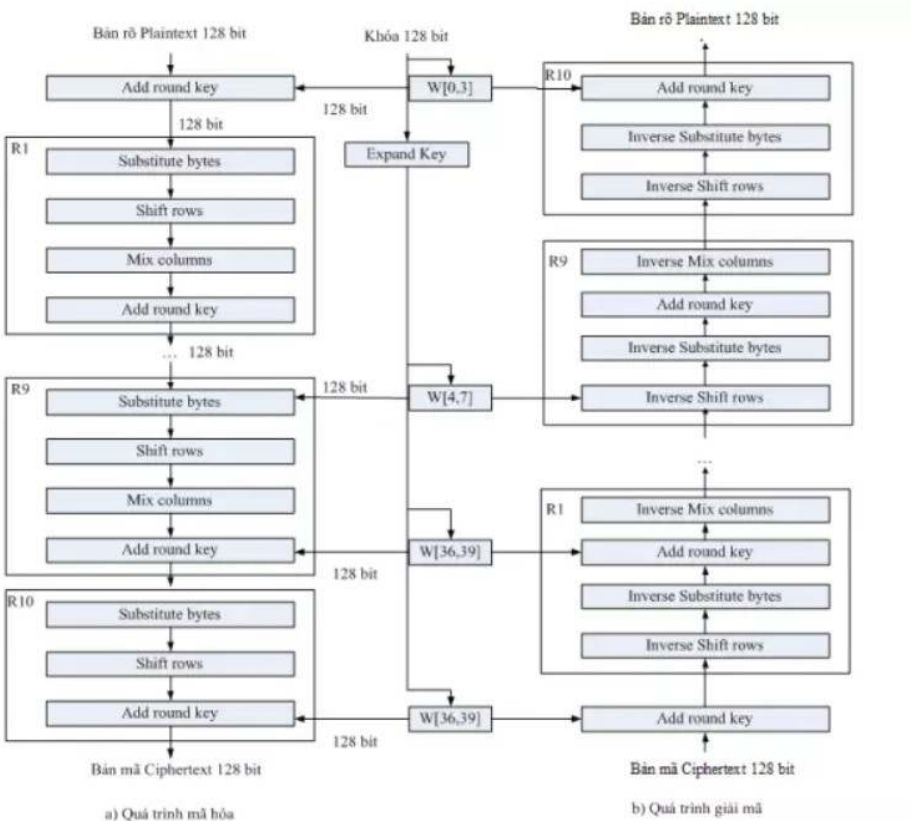
4. Final Round (không MixColumns) - SubBytes - ShiftRows - AddRoundKey.

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. Riêng đối với cấu trúc giải mã trong AES gồm 2 chế độ giải mã:

- Ở cấu trúc giải mã ngược, gồm vòng khởi tạo, Nr-1 vòng lặp và vòng kết thúc. Trong đó vòng khởi tạo chỉ có phép biến đổi AddRounKey, vòng lặp gồm lần lượt 4 phép biến đổi chính: InvShiftRows, InvSubBytes, AddRounKey, InvMixColumns; vòng kết thúc khác với vòng lặp chính ở chỗ không có phép InvMixColumns.

- Ngược lại với cấu trúc giải mã ngược là cấu trúc giải mã xuôi, việc ngược lại thể hiện ở điểm: trong cấu trúc giải mã xuôi việc sắp xếp các phép biến đổi ngược giống hệt với cấu trúc mã hóa, cụ thể bao gồm: vòng khởi tạo, Nr-1 vòng lặp và vòng kết thúc.

Trong đó vòng khởi là phép AddRounKey; ở vòng lặp thứ tự các phép biến đổi ngược lần lượt là: InvSubBytes, InvShiftRows, InvMixColumns, AddRounKey; vòng kết thúc giống vòng lặp nhưng được lược bỏ phép InvMixColumns. Một điểm khác biệt nữa trong hai cấu trúc giải mã ngược và giải mã xuôi đó là: Trong giải mã ngược khóa vòng giải mã chính là khóa vòng mã hóa với thứ tự đảo ngược. Còn trong giải mã xuôi thì khóa giải mã ngoài việc đảo ngược thứ tự khóa vòng mã hóa còn phải thực hiện phép InvMixColumns đối với các khóa vòng của vòng lặp giải mã.



Hình 7 Sơ đồ mã hóa AES 128 bits

2.2.1.2.Xây dựng thuật toán

❖ Xây dựng bảng S-Box

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

Hình 8 bảng giá trị S-Box

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:

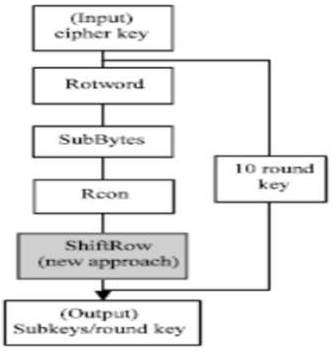
$$\begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix}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

	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

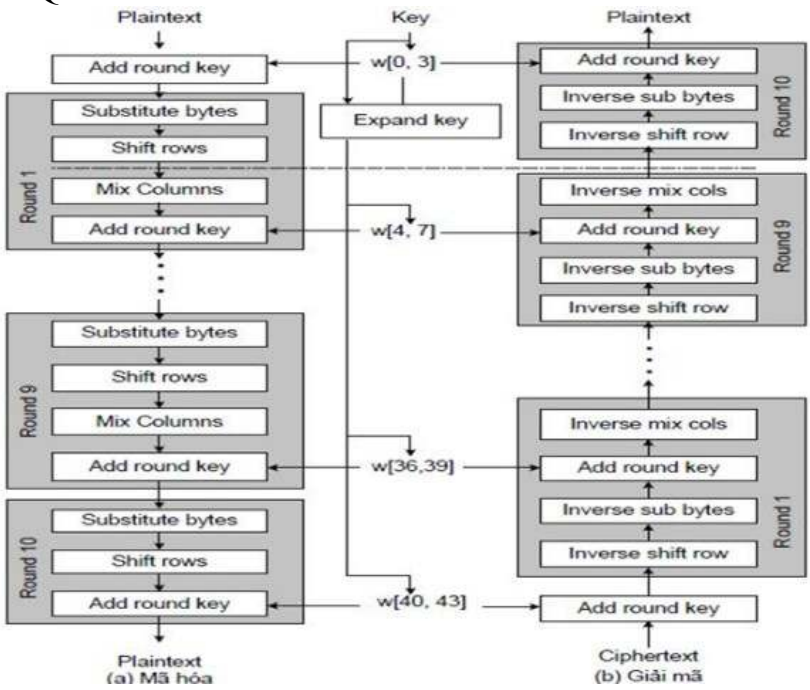
Hình 9 Bảng giá trị S-box nghịch đảo

❖ Giải thuật sinh khóa phụ

- 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



❖ Quá trình mã hóa.



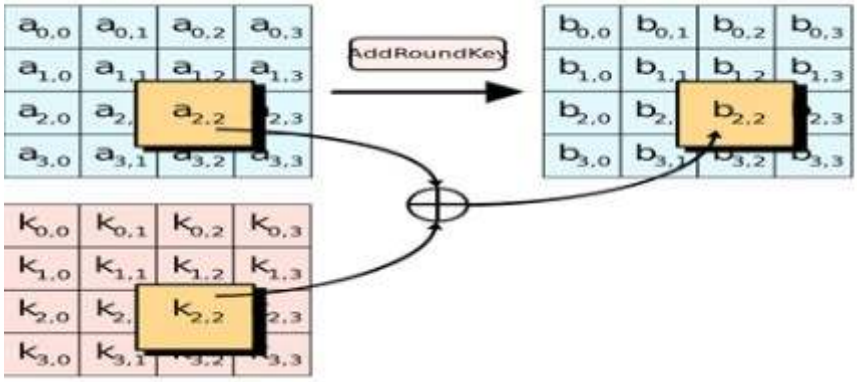
Hình 10 Quá trình mã hóa

a. 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:

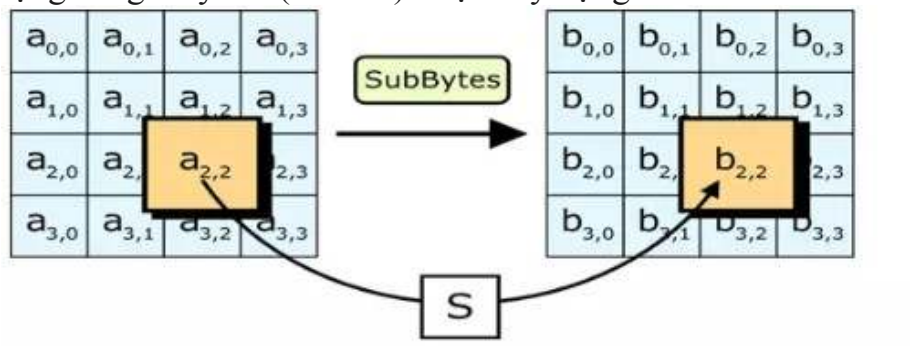
[S'0,c, S'1,c, S'2,c, S'3,c] = [S0,c, S1,c, S2,c, S3,c] ⊕ [W(4*i + c)]

Với 0 <= c < 4.



b. 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.



c. 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)

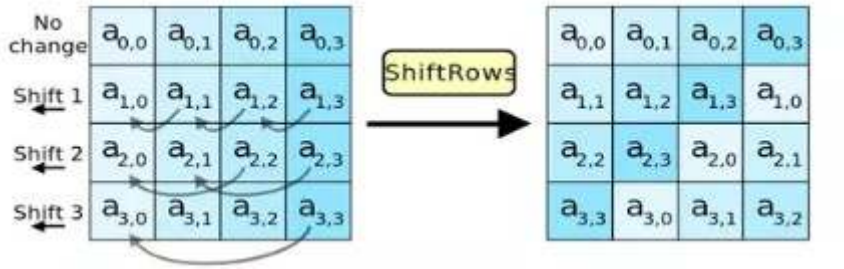
- Trong đó giá trị dịch shift (r, Nb) phụ thuộc vào số hàng r như sau:

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.



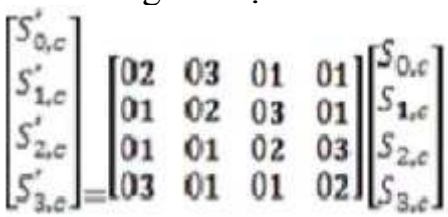
d. Hàm MixColumns.

- 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) ⊗

Mô tả bằng ma trận như sau :



❖ 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()

2.2.1.3 : Ưu , nhược điểm của hệ mã hóa AES :

*** Ưu điểm** :

Thiết kế và độ dài của thuật toán AES (128, 192, 256 bits) là đủ an toàn để bảo vệ các thông tin được xếp loại tối mật (secret) . Các phiên bản thực hiện AES nhằm mục đích bảo vệ hệ thống an ninh hay thng tin quốc gia phải được NSA kiểm định .

Vào tháng 6 năm 2003 , chính phủ Hoa Kì tuyên bố AES có thể sử dụng cho thông tin mật .

Vào thời điểm năm 2006 , dạng tấn công duy nhất thành công lên AES là tấn công kênh bên (side channel attack) . Tấn công kênh bên là tấn công trực tiếp vào thuật toán mã hóa , tấn công lên các hệ thống bảo vệ thuật toán có sơ hở làm lộ dữ liệu .

AES có mô hình toán học đơn giản , cấu trúc rõ ràng đơn giản .

*** Nhược điểm** :

Về an ninh của AES , các nhà khoa học đánh giá là chưa cao . Họ cho rằng ranh giới giữa số chu kì của thuật toán và số chu kì bị phá vỡ quá nhỏ . Nếu các kĩ thuật tấn công dược cải thiện thì AES có thể bị phá vỡ .

Một vấn đề nữa là cấu trúc toán học của AES . AES có mô hình toán học khá đơn giản . Tuy điều này chưa dẫn tới mối nguy hiểm nào nhưng một số nhà ngiên cứu sợ rằng sẽ có người lợi dụng cấu trúc này trong tương lai .

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

a, 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.

b, 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.

c, 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*.

2.2.2. Hệ mã hóa đường cong Elliptic (ECC)

Hệ mật dựa trên đường cong Elliptic (ECDSA/ECC) là một giải thuật khoá công khai. Hiện nay, hệ mật RSA là giải thuật khoá công khai được sử dụng nhiều nhất, nhưng hệ mật dựa trên đường cong Elliptic (ECC) có thể thay thế cho RSA bởi mức an toàn và tốc độ xử lý cao hơn.

Ưu điểm của ECC là hệ mật mã này sử dụng khoá có độ dài nhỏ hơn so với RSA. Từ đó làm tăng tốc độ xử lý một cách đáng kể, do số phép toán dùng để mã hoá và giải mã ít hơn và yêu cầu các thiết bị có khả năng tính toán thấp hơn,

nên giúp tăng tốc độ và làm giảm năng lượng cần sử dụng trong quá trình mã hoá và giải mã. Với cùng một độ dài khoá thì ECC có nhiều ưu điểm hơn so với các giải thuật khác, nên trong một vài năm tới có thể ECC sẽ là giải thuật trao đổi khoá công khai được sử dụng phổ biến nhất.

2.2.2.1.Khái niệm

Mật mã đường cong Elip (Elliptic curve cryptography – ECC) là kĩ thuật mã khóa công khai dựa trên lý thuyết về đường cong elip, giúp tạo mật mã nhanh hơn, nhỏ hơn và mạnh hơn. ECC tạo ra các mật mã thông qua thuộc tính của phương trình đường cong elip thay cho phương pháp sử dụng những số nguyên tố lớn truyền thống. Công nghệ này có thể được sử dụng cùng với hầu hết những phương thức mã hóa công khai như RSA và Diffie-Hellman.

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.

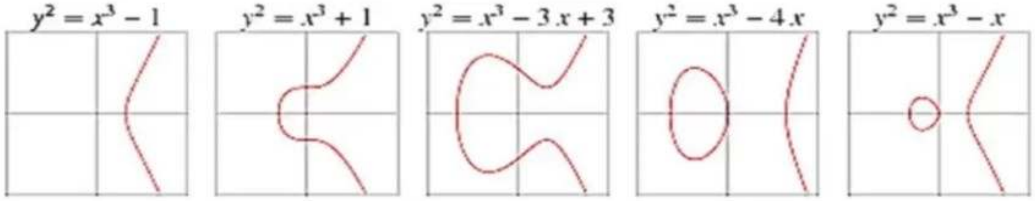
2.2.2.2.Mật mã đường cong ECC

Vì kích thước khóa nhỏ hơn trong ECC có thể cung cấp bảo mật và hiệu suất cao hơn so với các các thuật toán chính, nó được sử dụng rộng rãi trong các thiết bị nhúng nhỏ, cảm biến,và các thiết bị IoT khác, v.v.

Về mặt toán học, một đường cong elliptic thỏa mãn điều kiện toán học sau

phương trình: $y^2 = x^3 + ax + b$, trong đó $4a^3 + 27b^2 \neq 0$

Với các giá trị khác nhau của " a " và " b ", đường cong có các hình dạng khác nhau như được hiển thị trong sơ đồ sau:



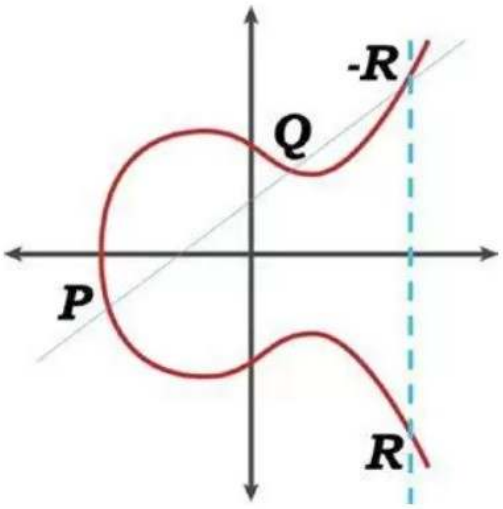
Hình 11 Các dạng đồ thi đường cong

Có một số đặc điểm quan trọng của đường cong elip là được sử dụng trong mật mã, chẳng hạn như:

• Chúng đối xứng theo chiều ngang. tức là, những gì dưới đây trục X là hình ảnh phản chiếu của những gì nằm trên trục X. Vì vậy, bất kỳ điểm nào trên đường cong khi được phản ánh qua Trục X vẫn nằm trên đường cong.

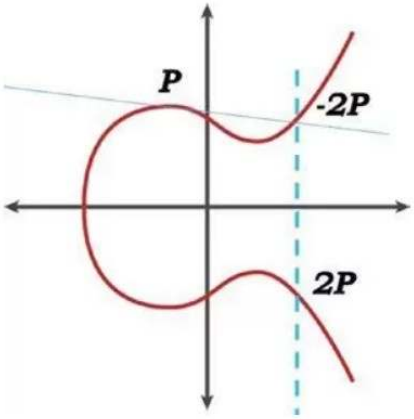
• Bất kỳ đường thẳng nào có thể cắt đường cong tối đa ba nơi.

• Nếu bạn coi hai điểm P và Q trên đường cong elliptic và vẽ một đường thẳng qua chúng, đường thẳng đó có thể chính xác băng qua đường cong ở một nơi nữa. Hãy để chúng tôi gọi nó là (- R). Nếu bạn vẽ một đường thẳng đứng qua (- R), nó sẽ đi qua đường cong tại, chẳng hạn, R , là sự phản chiếu của điểm (- R).Bây giờ, tài sản thứ ba có nghĩa là P + Q = R . Đây là được gọi là "cộng điểm", có nghĩa là cộng hai điểm trên một đường cong elip sẽ dẫn bạn đến một điểm khác trên đường cong. Tham khảo sơ đồ sau để biết hình ảnh biểu diễn của ba thuộc tính này.



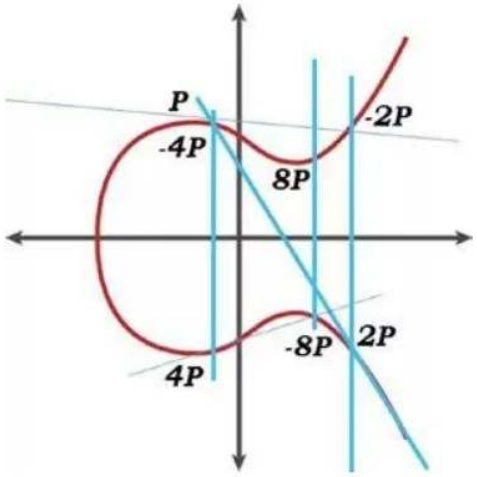
Vì vậy, bạn có thể áp dụng cộng điểm cho hai điểm bất kỳ trên đường cong. Bây giờ, trong tiêu điểm trước, chúng tôi đã cộng điểm P và Q (P + Q) và tìm thấy – R và sau đó cuối cùng đến R . Khi chúng tôi đến R , chúng tôi sau đó có thể vẽ một đường thẳng từ P đến R và thấy rằng đường thẳng lại cắt biểu đồ tại điểm thứ ba. Sau đó chúng ta có thể lấy điểm đó và di chuyển dọc theo một đường thẳng đứng cho đến khi nó lại cắt đồ thị. Đây trở thành điểm ngoài các điểm P và R . Quá trình này với một P và điểm kết quả có thể tiếp tục miễn là chúng ta muốn, và chúng tôi sẽ tiếp tục nhận được những điểm mới trên đường cong.

• Bây giờ, thay vì hai điểm P và Q , điều gì sẽ xảy ra nếu chúng ta áp dụng phép toán đến cùng một điểm P , tức là P và P (được gọi là"Nhân đôi điểm"). Rõ ràng, vô số dòng có thể thông qua P, vì vậy chúng tôi sẽ chỉ xem xét đường tiếp tuyến. Đường tiếp tuyến sẽ cắt đường cong trong một điểm nữa và một đường thẳng đứng từ đó sẽ cắt ngang đường cong một lần nữa để đến giá trị cuối cùng. Nó có thể được hiển thị như sau:



Rõ ràng là chúng ta có thể áp dụng nhân đôi điểm " n " số lần đến điểm ban đầu và mọi lúc nó sẽ dẫn chúng ta đến một điểm khác trên đường cong. Các lần đầu tiên chúng tôi áp dụng nhân đôi điểm cho điểm P , nó đã đưa chúng tôi đến điểm kết quả 2P

như bạn có thể thấy trongbiểu đồ. Bây giờ, nếu lặp lại tương tự, số ” n ” lần, chúng ta sẽ đạt đến một điểm trên đường cong như được hiển thị trong sơ đồ sau:



Trong tình huống đã đề cập ở trên, khi đầu và điểm cuối cùng được đưa ra, không có cách nào ai có thể nói rằng nhân đôi điểm đã được áp dụng ” n ” số lần để đạt được điểm kết quả cuối cùng ngoại trừ việc cố gắng cho tất cả có thể ” n ” từng cái một.

Đây là lôgarit rời rạc vấn đề đối với ECC, trong đó nó tuyên bố rằng đã cho một điểm G và Q , trong đó Q là bội số của G , hãy tìm “ d ” sao cho Q = d G . Điều này tạo thành hàm một chiều không có các phím tắt. Ở đây, Q là khóa công khai và d là khóa riêng tư Chìa khóa. Bạn có thể trích xuất khóa cá nhân d từ khóa công khai Q không? Đây là bài toán logarit rời rạc đường cong elliptic, khó giải quyết về mặt tính toán. Hơn nữa, đường cong phải được xác định trên một lĩnh vực và không đưa chúng ta đến vô cùng! Điều này có nghĩa là “tối đa” giá trị trên trục X phải được giới hạn ở một số giá trị, vì vậy chỉ cuộn lại các giá trị khi chúng tôi đạt đến mức tối đa.

Cái này giá trị được biểu diễn dưới dạng P (không phải P được sử dụng trong biểu đồ tại đây) trong hệ thống mật mã ECC và được gọi là “modulo” giá trị và nó cũng xác định kích thước khóa, do đó đồng ruộng. Trong nhiều triển khai của ECC, một số nguyên tố cho ” P ” được chọn.

Kích thước chữ “ P ” tăng lên dẫn đến nhiều giá trị hữu dụng hơn trên đường cong, do đó an toàn hơn.

• Chúng tôi quan sát thấy rằng việc cộng điểm và nhân đôi điểmtạo cơ sở cho việc tìm kiếm các giá trị được sử dụng cho mã hóa và giải mã.

Vì vậy, để xác định ECC, các tham số miền sau đây cần được định nghĩa:

• Phương trình đường cong: $y^2 = x^3 + ax + b$, trong đó $4\,a^3 + 27\,b^2 \neq 0$

• P : Số nguyên tố, xác định trường hữu hạn rằng đường cong sẽ được xác định trên (giá trị mô-đun)

• a và b : Hệ số xác định đường cong elliptic

• G : Điểm gốc hoặc điểm tạo trên đường cong. Cái này là điểm mà tất cả các hoạt động điểm bắt đầu và nó xác định nhóm con tuần hoàn.

• n : Số hoạt động điểm trên đường cong cho đến khi đường kết quả là thẳng đứng. Vì vậy, nó là thứ tự của G , tức là, số dương nhỏ nhất sao cho $nG = \infty$. Nó là thường là số nguyên tố.

• h : Nó được gọi là "cofactor", tương đương với thứ tự của đường cong chia cho n . Nó là một giá trị số nguyên và thường là gần bằng 1.

*Thuật toán chữ ký số đường cong Elliptic

ECDSA là một loại DSA sử dụng ECC để tạo khóa. Như một cái tên cho thấy, mục đích của nó là chữ ký số chứ không phải mã hóa. ECDSA có thể là một giải pháp thay thế tốt hơn cho RSA về kích thước khóa nhỏ hơn, bảo mật tốt hơn, và hiệu suất cao hơn. Nó là một trong những mật mã quan trọng nhất các thành phần được sử dụng trong Bitcoin!

Chúng tôi đã xem xét cách chữ ký điện tử được sử dụng để thiết lập lòng tin giữa người gửi và người nhận. Vì tính xác thực của người gửi và tính toàn vẹn của thông điệp có thể được xác minh thông qua chữ ký điện tử, haicác bên không xác định có thể giao dịch với nhau. Lưu ý rằng người gửi và người nhận phải đồng ý về các thông số miền trước khi tham gia vào các thông tin liên lạc.

Có ba bước rộng rãi để thực hiện ECDSA: thế hệ chìa khóa, tạo chữ ký và xác minh chữ ký

Thế hệ chìa khóa

Vì các tham số miền (P , a , b , G , n , h) được thiết lập trước nên đường cong và điểm cơ sở được biết bởi cả hai bên. Ngoài ra, P nguyên tố tạo nên nó là một trường hữu hạn cũng được biết đến (P thường là 160 bit và có thể lớn hơn ổn). Vì vậy, người gửi, giả sử, Alice thực hiện những việc sau để tạo các khóa:

• Chọn một số nguyên ngẫu nhiên d trong khoảng [1 , n – 1]

• Tính Q = d G

• Khai báo Q là khóa công khai và giữ d là khóa riêng tư Chìa khóa.

Tạo chữ kí

Khi các khóa được tạo, Alice, người gửi, sẽ sử dụng khóa riêng tư " D " để ký vào tin nhắn (m). Vì vậy, cô ấy sẽ thực hiện các bước sau trong thứ tự được chỉ định để tạo chữ ký:

• Chọn một số ngẫu nhiên k trong khoảng [1 , n – 1]

• Tính kG và tìm tọa độ mới (x 1 , y 1) và tìm r = x 1 mod n

Nếu r = 0 thì bắt đầu lại từ đầu

• Tính e = SHA-1 (m)

• Tính s = k −1 (e + d. R) mod n Nếu s = 0, thì hãy bắt đầu lại từ bước đầu tiên

• Chữ ký của Alice cho thông điệp (m) bây giờ sẽ là (r , s)

Xác minh chữ ký

Giả sử Bob là người nhận ở đây và có quyền truy cập vào miền tham số và khóa công khai Q của người gửi Alice. Như một bảo mật đo lường, trước tiên Bob nên xác minh rằng dữ liệu mà anh ta có, đó là miền các tham số, chữ ký và khóa công khai Q của Alice đều hợp lệ. Để xác minh Chữ ký của Alice trên tin nhắn (m), Bob sẽ thực hiện những điều sau hoạt động theo thứ tự được chỉ định:

• Xác minh rằng r và s là các số nguyên trong khoảng [1 , n – 1]

• Tính e = SHA-1 (m)

• Tính w = s −1 mod n

• Tính u 1 = ew mod n và u 2 = rw mod n

• Tính X = u 1 G + u 2 G, trong đó X đại diện cho tọa độ, giả sử (x 2 , y 2)

• Tính v = x 1 mod n

• Chấp nhận chữ ký nếu r = v , nếu không thì từ chối nó

2.2.2.3. Ưu , Nhược Điểm của hệ mã hóa EEC:

*Ưu 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.

*Nhược điểm :

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.

2.2.2.4. Mật mã đường cong Elliptic được sử dụng để làm gì?

ECC là một trong những kỹ thuật triển khai được sử dụng phổ biến nhất cho chữ ký số trong tiền điện tử. Cả Bitcoin và Ethereum đều áp dụng Thuật toán Chữ ký Kỹ thuật số Đường cong Elliptic (ECDSA) đặc biệt trong việc ký kết các giao dịch.

Tuy nhiên, ECC không chỉ được sử dụng trong tiền điện tử. Đây là một tiêu chuẩn mã hóa sẽ được hầu hết các ứng dụng web sử dụng trong tương lai do độ dài khóa ngắn hơn và hiệu quả của nó.

2.2.3.AES – ECC và ứng dụng trong truyền tải đề thi

Với cách truyền tải đề thi cổ điển , bộ giáo dục phải trực tiếp đến các địa điểm thi, trực tiếp giao đề thi, sau đó các trường học in và phát các đề thi. Và ngược lại các trường muốn gửi các bài thi thì cần phải trực tiếp đến bộ giáo dục. Nhưng trong truyền tải đề thi trực tuyến các

bước truyền tải đề thi, nộp bài thi, chấm điểm có thể thực hiện trên máy tính ... vừa đảm bảo tính bảo mật không bị rò rỉ đề thi vừa minh bạch lại an toàn.

Truyền tải đề thi gồm 3 phần chính: mã hóa đề thi, truyền tải và giải mã đề thi.

Trong truyền tải đề thi phải áp dụng thêm các kỹ thuật mã hóa, ký số,... để bảo đảm an toàn thông tin.

Ở phần 2.2.1.3 và 2.2.2.3 , ta thấy AES và ECC đều có rất nhiều ưu điểm so với các phương pháp mã hóa khác , 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, chúng em đề xuất 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.

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 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.

2.2.3.2 .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 .

2.2.3.2 . Kết quả phân tích giữa hệ mã hóa lai AES-ECC , AES và ECC :

(Trích từ tập chí khoa học và công nghệ , Đại học Đà Nẵng – Số 12(73).2013.Quyển 2)

Kết quả, tác giả đã xây dựng được chương trình cho phép chuyển tải đề thi nói riêng và dữ liệu nói chung qua mạng internet với khả năng mã hoá dữ liệu đảm bảo theo nguyên tắc bảo mật của mật mã phi đối xứng nhưng với hiệu quả của mật mã đối xứng. Chức năng khả năng SGD&ĐT tiếp nhận kết nối từ nhiều điểm thi – TTHPT khác nhau và lựa chọn tệp để truyền tải đến các TTHPT. Tương tự, chức năng gửi tệp từ TTHPT đến SGD&ĐT cũng được xây dựng. Vì mục đích nghiên cứu và chứng minh sự đúng đắn trong việc lựa chọn kết hợp ECC và AES, các tác giả còn xây dựng công cụ đánh giá hiệu quả khi so sánh ba hệ mật mã ECC, RSA và mật mã lai (kết hợp ECC và AES) khi truyền tải dữ liệu ở hai thông số thời gian thực hiện mã hoá và thời gian giải mã. Kích thước của khoá cho cả ba hệ mật mã có thể được thiết đặt ở giao diện cấu hình trên quan điểm đảm bảo tương đương về độ an toàn dữ liệu. Kết quả đo thời gian mã hoá và thời gian giải mã các tệp có kích thước khác nhau với các độ dài khoá khácnhau tương ứng với độ dài khoá của EAS là 128bit và 256bit , độ dài khoá cho các hệ mật mã để đảm bảo độ bảo mật tương đương. Chẳng hạn, với độ dài khoá cho EAS 128bit thì cho ECC sẽ là 256bit và RSA là 512bit. Với độ dài khoá cho EAS là 256bit thì cho ECC là 512bit và RSA là 1024bit.

Cho trường hợp mật mã lai, độ dài khoá của ECC và EAS được chọn tương ứng. Các tác giả cũng tiến hành đo độ dài tệp đã mã hoá và thấy rằng, kích thước tệp đã mã hoá cho EAS và ECCla bằng nhau. Với trường hợp RSA, kích thước lớn hơn không đáng kể

#	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 so sánh thời gian thực thi giữa thuật toán ECC , RSA và mật mã lai (AES kết hợp ECC)

2.2.4.Giải pháp và xây dựng chương trình

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, chúng em đề xuất 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.

Xây dựng chương trình :

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. Khoá bí mật do SGD&ĐT lưu giữ. Khóa công khai sẽ được gửi cho các TTHPT.

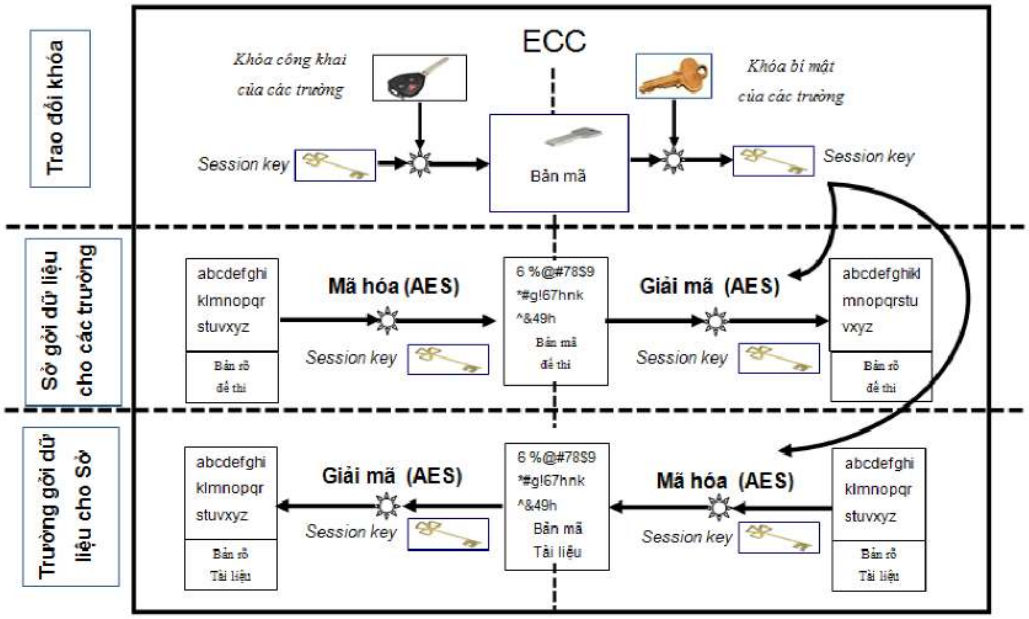
❖ Thực hiện việc trao đổi khóa mật mã đối xứng

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

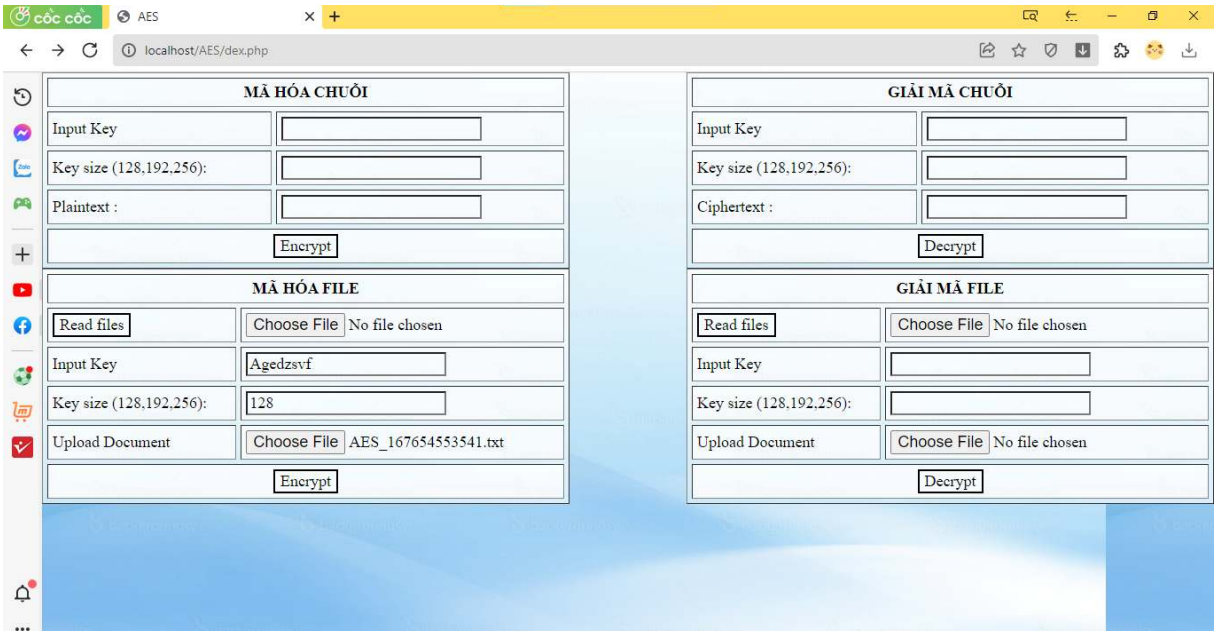
- Bên A sử dụng SK đã nhận được để mã hóa đề thi;
- Đề thi đã được mã hóa sẽ được chuyển cho bên B qua kênh thông thường;
- Bên B sử dụng SK giải mã và thu được nội dung đề thi.



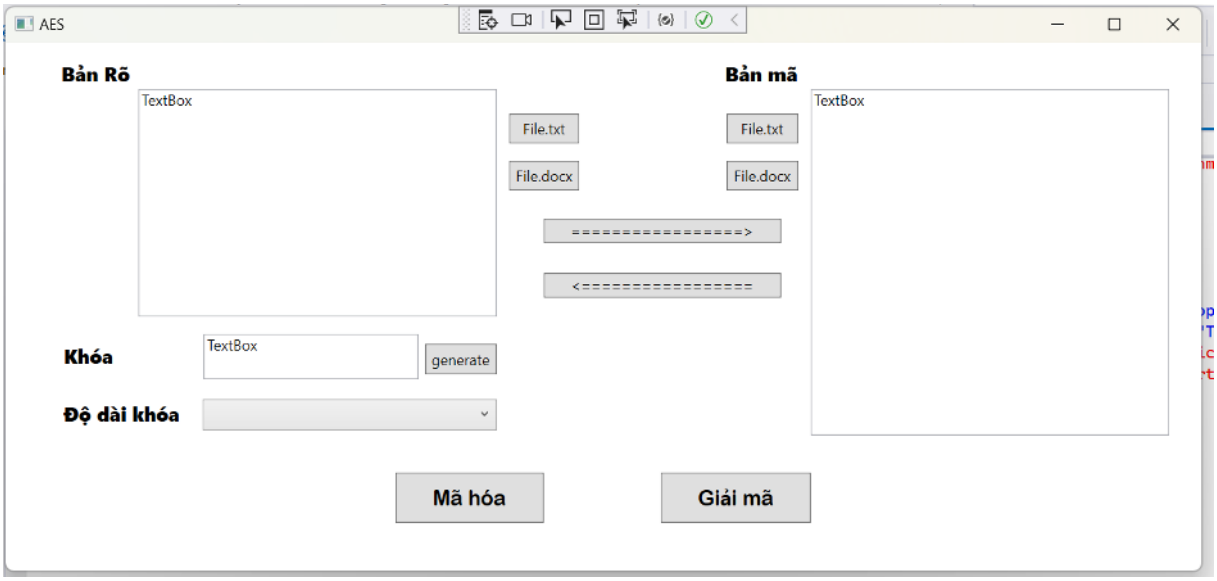
Hình 12 Sơ đồ truyền tải đề thi qua mạng internet

2.3.Thiết kế, cài đặt chương trình đề mô thuật toán

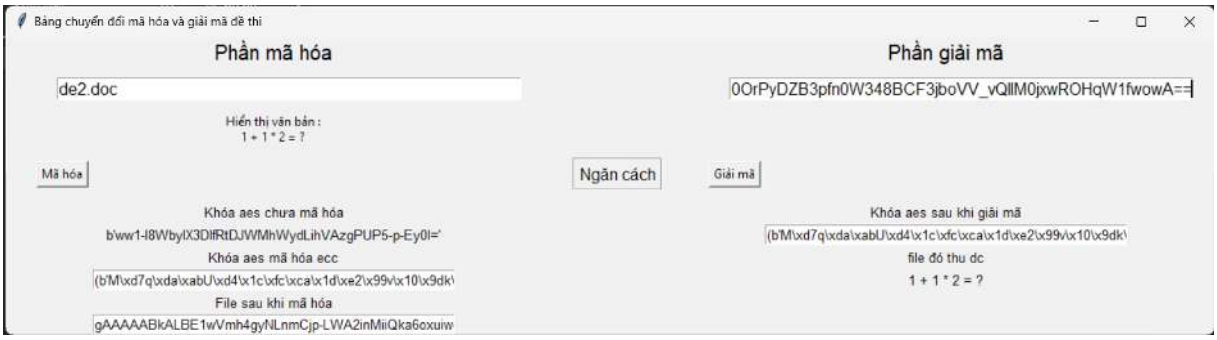
2.3.1.Giao diện chương trình đề mô



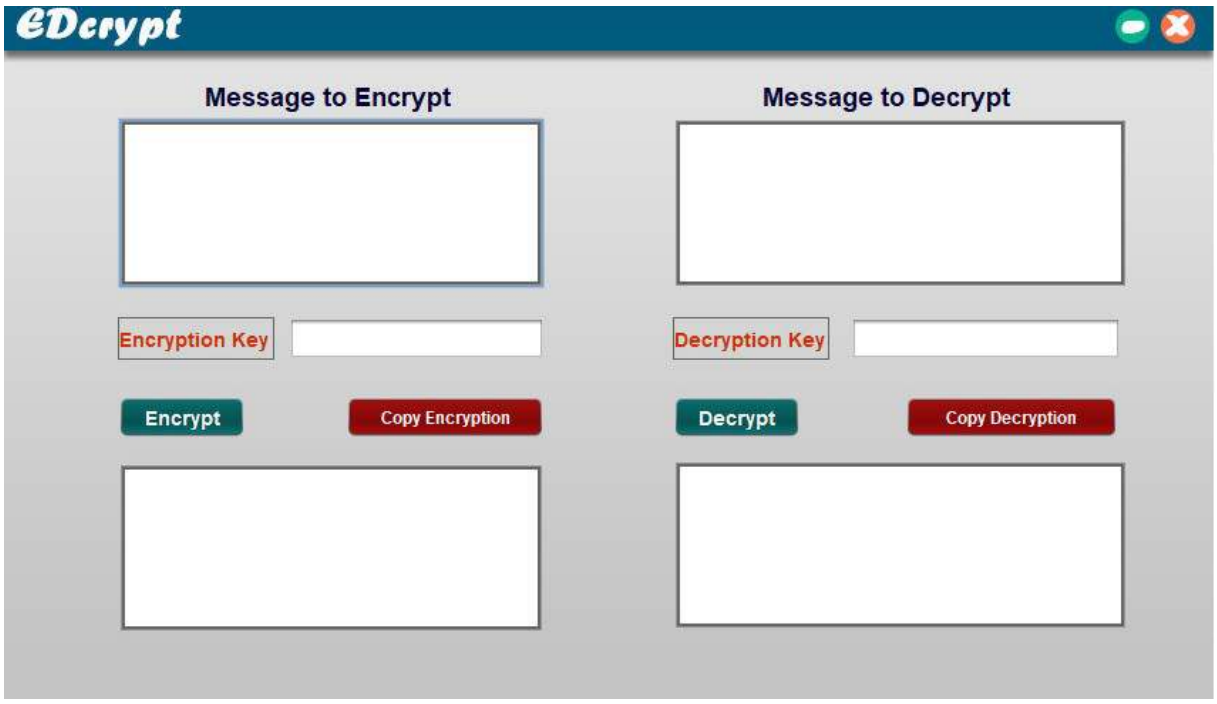
Hình 13 : Demo chương trình bằng ngôn ngữ PHP của Mai Thi Khánh Linh



Hình 14 Demo chương trình bằng ngôn ngữ C# của Trần Đăng Khoa



Hình 15 Demo chương trình bằng ngôn ngữ Python của Bùi Trung Kiên



Hình 16 Demo chương trình bằng ngôn ngữ Java của Nguyễn Viết Khánh

2.3.2.Cài đặt và triển khai

2.3.2.1.Giới thiệu công cụ

Công Cụ:

- Visual Studio Code và chạy chương trình trên Google Chorme (Thực hiện ngôn ngữ Javascrip)
- Visual Studio 2022 Netbeans IDE 8.2 (Thực hiện ngôn ngữ java)
- Visual studio 2022, C# Windows form (.NET Framework 4.7.2)

Visual Studio là trình soạn thảo code gọn nhẹ nhưng mạnh mẽ chạy trên máy tính, có sẵn cho Windows, macOS và Linux. VSCode đi kèm với sự hỗ trợ tích hợp cho JavaScript, TypeScript, Node.js và có một hệ sinh thái mở rộng phong phú cho các ngôn ngữ khác (như C++, C#, Java, Python, PHP, Go).

- sublime text và các thư viện base64, Crypto, tinyec, tkinter hỗ trỡ.

Ngôn Ngữ:

- ***PHP***

Hình 17 Ngôn ngữ lập trình PHP

- PHP là một ngôn ngữ lập trình kịch bản phía máy chủ mã nguồn mở. Nó được sử dụng để phát triển các ứng dụng web tĩnh hoặc động.
- PHP tượng trưng cho Hypertext Preprocessor. Còn trước đây, PHP là viết tắt của Personal Home Pages
- IDE (Môi trường phát triển tích hợp) cho phép các lập trình viên hợp nhất các khía cạnh khác nhau của việc viết một lập trình máy tính.
- IDE (Môi trường phát triển tích hợp) cho phép các lập trình viên hợp nhất các khía cạnh khác nhau của việc viết một lập trình máy tính.

- ***C#***

Hình 18 Ngôn ngữ lập trình C#

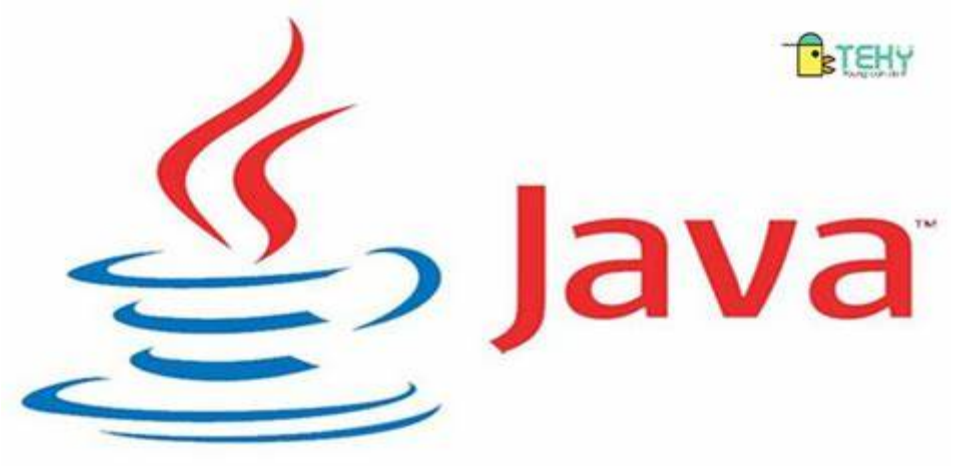
C# (hay C sharp) là một ngôn ngữ lập trình đơn giản, được phát triển bởi đội ngũ kỹ sư của Microsoft vào năm 2000, trong đó người dẫn đầu là Anders Hejlsberg và Scott Wiltamuth. Là ngôn ngữ lập trình hiện đại, hướng đối tượng và nó được xây dựng trên nền tảng của hai ngôn ngữ mạnh nhất là C++ và Java. C# được thiết kế cho Common Language Infrastructure (CLI), mà gồm Executable Code và Runtime Environment, cho phép chúng ta sử dụng các ngôn ngữ high-level đa dạng trên các nền tảng và cấu trúc máy tính khác nhau.

.NET framework có thể được sử dụng để tạo cả những ứng dụng dựa trên biểu mẫu (Form-based) và dựa trên Web (Web-based). Các web service cũng có thể được phát triển bằng cách sử dụng .NET framework.

- Java

Java được phát thành và phát triển từ năm 1995. Java được ứng dụng trên nhiều thiết bị như máy tính, điện thoại và phần cứng khác. Java là ngôn ngữ lập trình hướng đối tượng nên có đặc điểm chung với các ngôn ngữ khác như:

- Tính trừu tượng: xác định và nhóm các thuộc tính, các hành động liên quan đến một thực thể đặc thù.
- Tính đa hình: Cho phép tác động khác nhau trên nhiều loại đối tượng khác nhau
- Tính kế thừa: Cho phép các đối tượng chia sẽ, mở rộng các đặc tính sẵn có
- Tính đóng gói: Che giấu việc thực thi những chi tiết của đối tượng đối với người sử dụng đối tượng ấy.



Hình 19 Ngôn ngữ lập trình Java

Java được ứng dụng nhiều trong đời sống thường ngày như:

Viết ứng dụng web: Java được sử dụng để xây dựng hệ thống web cần sự bảo mật cao, số lượng người dùng lớn

- Viết ứng dụng mobile: Java được sử dụng để viết nên các ứng dụng, app hay game trên điện thoại
- Viết ứng dụng desktop: Java sử dụng viết các ứng dụng trên máy tính. Chỉ cần viết một lần và sau đó có thể đưa chương trình lên windows để chạy mà không cần phải viết lại.

-Python:

Python là ngôn ngữ lập trình hướng đối tượng đơn giản, dễ học, mạnh mẽ, cấp cao. Python có cấu trúc cú pháp ít hơn các ngôn ngữ khác.

Hình 20 Ngôn ngữ Python

Các tính năng của Python bao gồm:

- Dễ học: Python có ít từ khóa, cấu trúc đơn giản và cú pháp được định nghĩa rõ ràng. Điều này cho phép người mới học tiếp cận ngôn ngữ một cách nhanh chóng.
- Dễ đọc: Mã Python được định nghĩa rõ ràng hơn và có thể nhìn thấy bằng mắt.
- Dễ bảo trì: Mã nguồn của Python khá dễ bảo trì.
- Một thư viện tiêu chuẩn rộng: Phần lớn thư viện của Python rất dễ đính kèm và đa nền tảng tương thích trên UNIX, Windows và Macintosh.
- Chế độ tương tác: Python có hỗ trợ cho chế độ tương tác cho phép kiểm tra tương tác và debug.

- Portable: Python có thể chạy trên nhiều nền tảng phần cứng khác nhau và có cùng giao diện trên tất cả các nền tảng.
- Có thể mở rộng: Bạn có thể thêm các module cấp thấp vào trình thông dịch Python. Các module này cho phép các lập trình viên thêm hoặc tùy chỉnh các công cụ của mình để hiệu quả hơn.
- Cơ sở dữ liệu: Python cung cấp phương thức giao tiếp cho tất cả các cơ sở dữ liệu.
- Lập trình GUI: Python hỗ trợ các ứng dụng GUI có thể được tạo và chuyển sang nhiều cuộc gọi hệ thống, thư viện và hệ thống cửa sổ, như Windows MFC, Macintosh và hệ thống X Window của Unix.
- Khả năng mở rộng: Python cung cấp cấu trúc và hỗ trợ tốt hơn cho các chương trình lớn hơn so với kịch bản lệnh shell.

2.3.2.2. Hướng dẫn cài đặt và chạy chương trình demo đã cài đặt

- **Chương trình viết bằng ngôn ngữ PHP**

+ Có 4 sự lựa chọn :

1 . Mã hóa chuỗi :
- Điền khóa Input key
- Điền kích thước khóa : có thể là 128 , 192 hoặc 256
- Điền chuỗi cần mã hóa Plaintext
- Bấm encrypt để mã hóa

2 . Giải mã chuỗi :
- Điền khóa Input key
- Điền kích thước khóa : có thể là 128 , 192 hoặc 256
- Điền chuỗi cần giải mã hóa Ciphertext
- Bấm Decrypt để giải mã

3. Mã hóa file (chỉ chấp nhận file có đuôi .txt) :
- Chọn file cần mã hóa rồi bấm read files để đọc file
- Điền khóa Input key
- Điền kích thước khóa : có thể là 128 , 192 hoặc 256
- Chọn file cần mã hóa Upload document
- Bấm encrypt để mã hóa

File sau khi mã hóa sẽ ở tệp dekrip

4.Giải mã file (chỉ chấp nhận file có đuôi .txt) :
- Chọn file cần mã hóa rồi bấm read files để đọc file
- Điền khóa Input key
- Điền kích thước khóa : có thể là 128 , 192 hoặc 256
- Chọn file cần mã hóa Upload document
- Bấm Decrypt để giải mã

File sau khi giải mã sẽ ở tệp ekrip

- C**hương trình viết bằng ngôn ngữ C#**

+ Có 4 sự lựa chọn :

1 . Mã hóa chuỗi :

- Điền khóa Input key
- Lựa chọn thước khóa : có thể là 128 , 192 hoặc 256
- Điền chuỗi cần mã hóa
- Bấm Mã hóa để mã hóa

2 . Giải mã chuỗi :

- Điền khóa Input key
- Điền kích thước khóa : có thể là 128 , 192 hoặc 256
- Điền chuỗi cần giải mã hóa
- Bấm Giải mã để giải mã

3. Mã hóa file (chỉ chấp nhận file có đuôi .txt,docx) :

- Chọn file cần mã
- Điền khóa Input key
- Điền kích thước khóa : có thể là 128 , 192 hoặc 256
- Chọn file cần mã hóa
- Bấm Mã hóa để mã hóa

File sau khi mã hóa sẽ ở tệp outPut.txt

4.Giải mã file (chỉ chấp nhận file có đuôi .txt,docx) :

- Chọn file cần mã hóa
- Điền khóa Input key
- Điền kích thước khóa : có thể là 128 , 192 hoặc 256
- Chọn file cần mã hóa
- Bấm Giải mã để giải mã

File sau khi giải mã sẽ ở file outPut.txt

- **Chương trình viết bằng ngôn ngữ Java**

+ Chọn chức năng mã hóa hoặc giải mã:

+ Mã hóa:

Nhập bản mã Message to Encrypt từ bàn phím

Nhập khóa: nhập khóa từ bàn phím khóa Encryption Key với độ dài 16 ký tự

Nhấn vào nút “Encrypt” để mã hóa bản mã đã chọn.

Nhấn nút “Copy Encryption” để copy bản rõ

+ Giải mã:

Nhập bản rõ Message to Decrypt từ bàn phím

Nhập khóa: nhập khóa từ bàn phím khóa Decryption Key với độ dài 16 ký tự

Nhấn vào nút “Decrypt” để giải mã bản rõ đã chọn.

Nhấn nút “Copy Decryption” để copy bản mã

- **Chương trình viết bằng ngôn ngữ Python**.

+Chọn file : Viết tên File cần mã hóa vào hộp “Phần mã hóa”, chương trình có thể thực hiện được với File có đuôi là .txt hoặc là .doc

(Lưu ý nếu file có tên không tồn tại thì chương trình sẽ không được thực hiện).

+ Tiếp theo click vào ô “Mã hóa”, sau đó thì khóa AES chưa mã hóa sẽ được sinh ra ngẫu nhiên.

+ Khóa ECC sẽ xuất hiện tương ứng để mã hóa khóa AES.

+ Sau đó chương trình sẽ sinh ra khóa AES đã bị mã hóa bởi khóa ECC tương ứng ở ô “File sau khi đã mã hóa”. Chúng ta copy khóa này rùi add vô ô “Phần giải mã” và Click vào ô “Giải mã”.

+ Khóa AES sau khi được giải mã chính là khóa AES đã được mã hóa bởi khóa ECC. Từ đó chúng ta sẽ thu được File ban đầu.

2.3.3.Thực hiện bài toán

2.3.3.1.Phân công công việc

Tên sinh viên	Tên công việc
Mai Thị Khánh Linh	Tìm hiểu về ATBMTT, hệ mã hóa AES và cài đặt thực hiện chương trình theo ngôn ngữ PHP
Trần Đăng Khoa	Tìm hiểu về ATBMTT, hệ mã hóa AES và cài đặt thực hiện chương trình theo ngôn ngữ C#
Nguyễn Viết Khánh	Tìm hiểu về hệ mã hóa ECC và cài đặt thực hiện chương trình theo ngôn ngữ Java
Bùi Trung Kiên	Tìm hiểu về hệ mã hóa AES, ECC và cài đặt thực hiện chương trình theo ngôn ngữ Python

Mai Thị Khánh Linh - Phương pháp mã hóa AES, ECC để đảm bảo tính an toàn, toàn vẹn dữ liệu bằng ngôn ngữ PHP

- Tìm hiểu về An Toàn Bảo Mật Thông Tin.
- Tìm hiểm về hệ mã hóa AES
- Tìm hiểu ngôn ngữ PHP
- Viết chương trình đề mô với ngôn ngữ PHP

Trần Đăng Khoa - Phương pháp mã hóa AES, ECC để đảm bảo tính an toàn, toàn vẹn dữ liệu bằng ngôn ngữ C#

- Tìm hiểu về thuật toán AES
- Tìm hiểu ngôn ngữ C#
- Viết chương trình đề mô với ngôn ngữ C#

Nguyễn Viết Khánh - Phương pháp mã hóa AES, ECC để đảm bảo tính an toàn, toàn vẹn dữ liệu bằng ngôn ngữ Java

- Tìm hiểu hệ mã hóa ECC
- Tìm hiểu ngôn ngữ Java
- Viết chương trình đề mô với ngôn ngữ Java

Bùi Trung Kiên - Phương pháp mã hóa AES, ECC để đảm bảo tính an toàn, toàn vẹn dữ liệu bằng ngôn ngữ Python

- Tìm hiểu hệ mã hóa AES, ECC
- Tìm hiểu ngôn ngữ Python
- Viết chương trình đề mô với ngôn ngữ PyThon

Chương 3. Kiến thức lĩnh hội và bài học kinh nghiệm

3.1. Nội dung đã thực hiện

***Những hiểu biết :**

Qua quá trình tìm hiểu và giải quyết đề tài "***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 rất nhiều kiến thức về :

- Thuật Toán AES :

+ Hiểu được thuật toán AES và những ứng dụng của thuật toán AES.
+ Các bức xử lý của thuật toán AES.
+ Quy trình mã hóa và giải mã.

<u>Tìm hiểu thêm về mã hóa AES :</u>

AES được xây dựng & phát triển bởi 2 nhà mật mã học người Bỉ: Joan Daemen và Vincent Rijmen. Đây là một thuật toán được viết riêng cho chính phủ Mỹ nhằm thay thế cho chuẩn mã hóa cũ là DES (Data Encryption Standard) của IBM ra đời vào những năm 1970.

- Hệ mã hóa ECC:

+ Hiểu được kiến thức căn bản về hệ mã hóa.
+ Hiển và thực hiện được các bức xử lý.

? Những điều bạn chưa biết về hệ mật mã ECC :

Mật mã đường cong elliptic (ECC) được giới thiệu lần đầu vào năm 1991 bởi các công trình nghiên cứu độc lập của Neals Koblitz và Victor Miller.

Độ an toàn của ECC dựa vào bài toán logarit rời rạc trên nhóm các điểm của đường cong elliptic (ECDLP). Đối với bài toán logarit rời rạc trên trường hữu hạn hoặc bài toán phân tích số, tồn tại các thuật toán dưới dạng dạng hàm mũ để giải các bài toán này (tính chỉ số hoặc sàng trường số). Tuy nhiên, đối với bài toán ECDLP cho đến nay vẫn chưa tìm được thuật toán dưới hàm mũ để giải.

Nhà toán học nổi tiếng J. Silverman cũng như nhiều nhà thám mã khác đã nghiên cứu các thuật toán tương tự, như thuật toán tính chỉ số để áp dụng cho ECDLP nhưng đều không thành công. Hiện nay, thuật toán tốt nhất để giải bài toán ECDLP là Pollard với độ phức tạp cỡ . Điều này đã tạo ra những ưu việt của hệ mật ECC so với các hệ mật khóa công khai khác.

Neals Koblitz và Victor Miller

- ECC và AES:

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.

- Các kĩ năng về ngôn ngữ lập trình :

+ Ngôn ngữ C#
+ Ngôn ngữ Java
+ Ngôn ngữ PHP
+Nhôn ngữ python

***Những khó khăn:**

Trong quá trình thức hiện giải quyết đề tài , nhóm em đã gặp rất nhiều khó khăn :
- Thứ nhất : Do không hiểu rõ về năng lực của các thành viên trong nhóm nên đã gặp nhiều vấn đề trong việc lựa chọn ngôn ngữ vì hầu hết mọi người mới học 1 vài ngôn ngữ

- Thứ hai : Việc lập trình gặp nhiều khó khăn vì ban đầu không hiểu rõ về thuật toán
- Thứ ba : Việc tìm hiểu ngôn ngữ ECC cũng như hệ mã hóa lai AES kết hợp ECC vì có rất ít các tài liệu nói về chúng .
- Thứ tư: Có một số bạn trong nhóm chưa thực hành code giao diện nên mất kha khá thời gian để thích ứng.
- Thứ năm: Ban đầu mọi người khá là rụt rè không giao tiếp thảo luận với nhau nhưng sau những lần họp mặt đã tốt lên rất nhiều.

***Hoạt động của nhóm :**.

Nhóm chúng em đã rất đoàn kết để hoàn thành BTL :

- Tuy gặp rất nhiều khó khăn trong việc lựa chọn ngôn ngữ nhưng các bạn thành viên trong nhóm đã dành ra rất nhiều thời gian để thỏa thuận với nhau để có được kết quả tốt nhất.
- Các thành viên đã cố gắng hoàn thành công việc nhanh và đầy đủ nhất có thể .

***Bài học rút ra :**

Qua quá trình tìm hiểu và giải quyết đề tài "***Ứng dụng hệ thống mã hóa lai vào công tác bảo mật trong truyền tải đề thi***", nhóm chúng em đã rút ra được rất nhiều bài học quý giá :

- Chúng em đã có thêm được rất nhiều kiến thức trong việc lập trình
- Có cái nhìn toàn diện hơn về môn An toàn và bảo mật thông tin
- Hiểu rõ hơn về thuật toán cũng như quá trình thực hiện mã hóa và giải mã trên máy tính .

3.2.Hướng phát triển

3.2.1 .Tính khả thi của đề tài nghiên cứu :

- 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 khả thi và 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.

3.2.2 . Những thuận lợi , khó khăn trong quá trình nghiên cứu :

*** Những thuận lợi :**

Trong cuộc cách mạng công nghệ 4.0 hiện nay , với sự phát triển như vũ bão của ngành công nghệ thông tin vào trong mọi mặt của cuộc sống đã tạo ra một môi trường rất thuận lợi cho việc áp dụng các phương pháp mã hóa bảo mật thông tin .

***Những khó khăn , hạn chế :**

- Phương pháp mã hóa lai AES kết hợp ECC chưa được áp dụng rộng rãi và được nhiều người biết tới

- Nghiên cứu và xây dựng mật mã đường cong elliptic là vấn đề mới và khó về lý thuyết, là một lĩnh vực đầy thách thức. Bên cạnh các kiến thức toán học để xây dựng một hệ mật an toàn theo lý thuyết, cần phải có đầy đủ những kiến thức về lập mã/thám mã để đảm bảo hệ mật đó an toàn dưới các mô hình tấn công của người mã thám.

3.3.3. Hướng phát triển và mở rộng của đề tài :

- Đề án không chỉ có tính ứng dụng trong công tác truyền tải đề thi mà còn có thể áp dụng trong

+ Trong lĩnh vực giáo dục truyền tải điểm thi , bài giảng , …

+ Trong việc phát triển các app hay trang web : việc bảo vệ quyền riêng tư của mọi người như bảo vệ tin nhắn , bảo vệ thông tin cá nhân ,…

Tài liệu tham khảo :

[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://en.wikipedia.org/wiki/Advanced_Encryption_Standard

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

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

https://doc.edu.vn/tai-lieu/de-tai-tim-hieu-dua-ra-uu-va-nhuoc-diem-cac-phien-ban-cua-cac-thuat-toan-des-triple-des-aes-7643/

https://tinhte.vn/thread/tim-hieu-chuan-ma-hoa-aes-duoc-my-ap-dung-trong-viec-ma-hoa-du-lieu.2871055/

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

https://vi.wikipedia.org/wiki/M%C3%A3_h%C3%B3a

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

https://vnkrypto.com/elliptic-curve-cryptography-ecc-la-gi-tim-hieu-mat-ma-duong-cong-elliptic

https://websitehcm.com/mat-ma-duong-cong-ecliptic/

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

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