**BỘ CÔNG THƯƠNG**

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

**---------------------------------------**

****

**BÀI TẬP LỚN**

**MÔN: AN TOÀN VÀ BẢO MẬT THÔNG TIN**

**XÂY DỰNG CHƯƠNG TRÌNH MÃ HÓA VÀ GIẢI MÃ AES (SỬ DỤNG NGÔN NGỮ C++, C#)**

GVHD: TS. Phạm Văn Hiệp

Lớp: 20241IT6001002

Nhóm: 5

Thành viên nhóm: Trần Anh Đức – 2021607565

Trần Thái Quyền – 2022607309

Phạm Văn Thành – 2021608254

Trương Thị Thủy - 2021603283

Hà Nội - Năm 2024

# LỜI CẢM ƠN

Em xin chân thành cảm ơn các thầy, cô khoa Công nghệ thông tin – Trường Đại học Công Nghiệp Hà Nội đã tận tình dạy dỗ, truyền đạt cho chúng em những kiến thức bổ ích và quý báu trong suốt những năm học đã qua.

Chúng em xin tỏ lòng biết ơn sâu sắc đến thầy Phạm Văn Hiệp, người đã trực tiếp hướng dẫn, giúp đỡ và truyền đạt cho chúng em những kinh nghiệm để đề tài này được thực hiện và hoàn thành.

Chúng em xin cảm ơn gia đình và bạn bè đã động viên giúp đỡ em trong suốt thời gian em làm bài báo cáo bài tập lớn.

Vì thời gian có hạn, trình độ hiểu biết của chúng em còn nhiều hạn chế. Cho nên trong bài báo cáo không tránh được những thiếu sót, em rất mong nhận được sự đống góp ý kiến của cô cũng như bạn bè để bài báo cáo của chúng em được hoàn thiện hơn.

**Em xin chân thành cảm ơn!**

Hà Nội, ngày … tháng … năm 2022

Nhóm sinh viên

# LỜI MỞ ĐẦU

Sự phát triển vượt bậc của công nghệ mạng dẫn đến vấn đề an toàn thông tin trong là rất quan trọng. Có nhiều phương pháp để trao đổi thông tin mật, trong đó phương pháp mã hóa thông tin được coi là xuất hiện sớm nhất, tuy nhiên phương pháp này làm cho người ta dễ phát hiện. Trong đề tài này sẽ sử dụng phương pháp mã hóa AES (advanced encryption standard) để mã hóa thông tin mật. Nội dung báo cáo gồm 3 chương chính sau:

**Chương 1: Tổng quan**

Giới thiệu tổng quan về mã hóa thông tin, phương pháp mã hóa AES.

**Chương 2: Kết quả nghiên cứu**

Thuật toán, sơ đồ thuật toán, ví dụ minh họa của mã hóa AES, đưa ra công cụ hướng dẫn cài đặt và chạy chương trình

**Chương 3: Phần kiến thức lĩnh hội và bài học kinh nghiệm.**

Tổng kết các phần trong bài tập lớn đã làm được, rút ra bài học kinh nghiệm

## CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN THÔNG TIN

## Tìm hiểu về 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 xân 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. An toàn thông tin bao gồm các nội dung sau: - Tính bí mật: tính kín đáo riêng tư của thông tin - Tính xác thực của thông tin, bao gồm xác thực đối tác( bài toán nhận danh), xác thực thông tin trao đổi. - Tính trách nhiệm: đảm bảo người gửi thông tin không thể thoái thác trách nhiệm về thông tin mà mình đã gửi. Để đảm bảo an toàn thông tin dữ liệu trên đường truyền tin và trên mạng máy tính có hiệu quả thì điều trước tiên là phải lường trước hoặc dự đoán trước các khả năng không an toàn, khả năng xâm phạm, các sự cố rủi ro có thể xảy ra đối với thông tin dữ liệu được lưu trữ và trao đổi trên đường truyền tin cũng như 1 http://www.ebook.edu.vn trên mạng. Xác định càng chính xác các nguy cơ nói trên thì càng quyết định được tốt các giải pháp để giảm thiểu các thiệt hại. Có hai loại hành vi xâm phạm thông tin dữ liệu đó là: vi phạm chủ động và vi phạm thụ động. Vi phạm thụ động chỉ nhằm mục đích cuối cùng là nắm bắt được thông tin (đánh cắp thông tin). Việc làm đó có khi không biết được nội dung cụ thể nhưng có thể dò ra được người gửi, người nhận nhờ thông tin điều khiển giao thức chứa trong phần đầu các gói tin. Kẻ xâm nhập có thể kiểm tra được số lượng, độ dài và tần số trao đổi. Vì vậy vi pham thụ động không làm sai lệch hoặc hủy hoại nội dung thông tin dữ liệu được trao đổi. Vi phạm thụ động thường khó phát hiện nhưng có thể có những biện pháp ngăn chặn hiệu quả. Vi phạm chủ động là dạng vi phạm có thể làm thay đổi nội dung, xóa bỏ, làm trễ, xắp xếp lại thứ tự hoặc làm lặp lại gói tin tại thời điểm đó hoặc sau đó một thời gian. Vi phạm chủ động có thể thêm vào một số thông tin ngoại lai để làm sai lệch nội dung thông tin trao đổi. Vi phạm chủ động dễ phát hiện nhưng để ngăn chặn hiệu quả thì khó khăn hơn nhiều. Một thực tế là không có một biện pháp bảo vệ an toàn thông tin dữ liệu nào là an toàn tuyệt đối. Một hệ thống dù được bảo vệ chắc chắn đến đâu cũng không thể đảm bảo là an toàn tuyệt đối.

## **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 dộ yêu cầu về đọ an toàn.

**Các thành phần của một hệ mật mã :**

Định nghĩa :

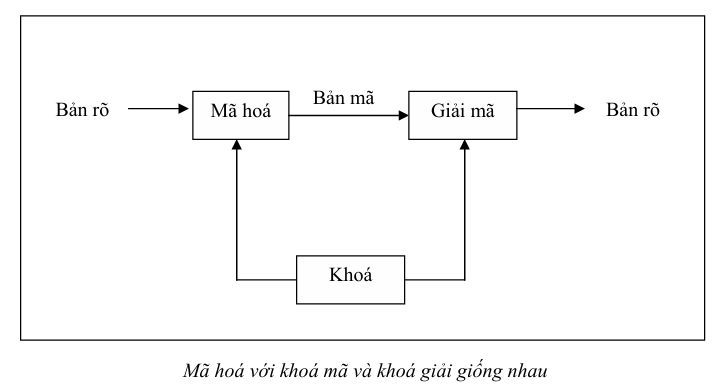
Một hệ mật là một bộ 5 (P,C,K,E,D) thoả mãn các điều kiện sau:

- P là một tập hợp hữu hạn các bản rõ (PlainText), nó được gọi là không gian bản rõ.

- C là tập các hữu hạn các bản mã (Crypto), nó còn được gọi là không gian các bản mã. Mỗi phần tử của C có thể nhận được bằng cách áp dụng phép mã hoá Ek lên một phần tử của P, với k ∈ K.

- K là tập hữu hạn các khoá 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 7 http://www.ebook.edu.vn phải đủ lớn để “kẻ địch: không có đủ thời gian để thử mọi khoá có thể (phương pháp vét cạn).

- Đối với mỗi k ∈ K có một quy tắc mã eK: P → C và một quy tắc giải mã tương ứng dK ∈ D. Mỗi eK: P → C và dK: C → P là những hàm mà: dK (eK(x))=x với mọi bản rõ x ∈ P.



## 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): là những hệ mật dung chung một khoá cả trong quá trình mã hoá dữ liệu và giải mã dữ liệu. Do đó khoá phải được giữ bí mật tuyệt đối.

- Hệ mật mã bất đối xứng (hay còn gọi là mật mã khóa công khai) : Hay còn gọi là hệ mật mã công khai, các hệ mật này dùng một khoá để mã hoá sau đó dùng một khoá khác để giải mã, nghĩa là khoá để mã hoá và giải mã là khác nhau. Các khoá này tạo nên từng cặp chuyển đổi ngược nhau và không có khoá nào có thể suy được từ khoá kia. Khoá dùng để mã hoá có thể công khai nhưng khoá dùng để giải mã phải giữ bí mật. 8 <http://www.ebook.edu.vn>

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)

## Tiêu chuẩn đánh giá hệ mật mã

Để đánh giá một hệ mật mã người ta thường đánh giá thông qua các tính chất sau:

### Độ an toàn:

Một hệ mật được đưa vào sử dụng điều đầu tiên phải có độ an toàn cao. Ưu điểm của mật mã là có thể đánh giá được độ an toàn thông qua độ an toàn tính toán mà không cần phải cài đặt. Một hệ mật được coi là an toàn nếu để phá hệ mật mã này phải dùng n phép toán. Mà để giải quyết n phép toán cần thời gian vô cùng lớn, không thể chấp nhận được.

Một hệ mật mã được gọi là tốt thì nó cần phải đảm bảo các tiêu chuẩn sau: - Chúng phải có phương pháp bảo vệ mà chỉ dựa trên sự bí mật của các khoá, công khai thuật toán. - Khi cho khoá công khai eK và bản rõ P thì chúng ta dễ dàng tính được eK(P) = C. Ngược lại khi cho dK và bản mã C thì dễ dàng tính được dK(M)=P. Khi không biết dK thì không có khả năng để tìm được M từ C, nghĩa là khi cho hàm f: X → Y thì việc tính y=f(x) với mọi x∈ X là dễ còn việc tìm x khi biết y lại là vấn đề khó và nó được gọi là hàm một chiều.

- Bản mã C không được có các đặc điểm gây chú ý, nghi ngờ.

### Tốc độ mã và giải mã:

Khi đánh giá hệ mật mã chúng ta phải chú ý đến tốc độ mã và giải mã. Hệ mật tốt thì thời gian mã và giải mã nhanh.

### Phân phối khóa:

Một hệ mật mã phụ thuộc vào khóa, khóa này được truyền công khai hay truyền khóa bí mật. Phân phối khóa bí mật thì chi phí sẽ cao hơn so với các hệ mật có khóa công khai. Vì vậy đây cũng là một tiêu chí khi lựa chọn hệ mật mã.

## CHƯƠNG 2: TỔNG QUAN VỀ AN TOÀN THÔNG TIN

## Chuẩn mã nâng cao (AES – Advanced Encryption Standard)

### Giới thiệu

Vào năm 1999, cục tiêu chuẩn quốc gia Hoa Kỳ (NIST) đã ban hành một phiên bản mới của tiêu chuẩn DES chỉ ra rằng DES chỉ nên được sử dụng cho các hệ thống kế cũ và DES ba lần được sử dụng. DES ba lần có hai ưu điểm đảm bảo cho việc sử dụng rộng rãi trong vài năm tới. Đầu tiên, với độ dài khóa 168-bit, nó khắc phục được lỗ hổng đối với cuộc tấn công vét cạn của DES. Thứ hai, thuật toán mã hóa cơ bản trong DES ba lần cũng giống như trong DES. Thuật toán này đã được giám sát kỹ lưỡng hơn bất kỳ thuật toán mã hóa nào khác trong một khoảng thời gian dài và không có cuộc tấn công phá mã hiệu quả nào dựa trên thuật toán thay vì vét cạn được tìm thấy. Do đó, DES ba lần có khả năng chống phá mã rất tốt. Nếu bảo mật là yếu tố duy nhất được xem xét, thì DES ba lần sẽ là lựa chọn thích hợp cho thuật toán mã hóa tiêu chuẩn trong nhiều thập kỷ tới.

Hạn chế chính của DES ba lần là thuật toán tương đối chậm trong phần mềm. DES ban đầu được thiết kế để triển khai bằng phần cứng giữa những năm 1970 và không tạo ra mã phần mềm hiệu quả. DES ba lần, có số vòng gấp ba lần DES, do đó thực hiện chậm hơn DES ban đầu. Một nhược điểm phụ là cả DES và DES ba lần đều sử dụng kích thước khối 64-bit. Vì lý do cả hiệu quả và bảo mật, kích thước khối lớn hơn là cần thiết.

Vì những nhược điểm này, DES ba lần không phải là ứng cử viên thích hợp để sử dụng lâu dài. Để thay thế, vào năm 1997 NIST đã đưa ra lời kêu gọi đề xuất Tiêu chuẩn mã hóa nâng cao (AES) mới, tiêu chuẩn này phải có sức mạnh bảo mật bằng hoặc tốt hơn DES ba lần và cải thiện đáng kể hiệu quả. Ngoài các yêu cầu chung này, NIST quy định rằng AES phải là mật mã khối đối xứng với độ dài khối 128 bit và hỗ trợ độ dài khóa có thể là 128, 192 và 256 bit.

Trong vòng đánh giá đầu tiên, 15 thuật toán được đề xuất đã được chấp nhận. Vòng thứ hai thu hẹp còn 5 thuật toán. NIST đã hoàn thành quá trình đánh giá của mình và xuất bản tiêu chuẩn cuối cùng vào tháng 11 năm 2001. NIST đã chọn Rijndael làm thuật toán AES được đề xuất. Hai nhà nghiên cứu đã phát triển và gửi Rijndael cho AES đều là những nhà mật mã học đến từ Bỉ: Tiến sĩ Joan Daemen và Tiến sĩ Vincent Rijmen.

Cuối cùng, AES được thiết kế để thay thế DES ba lần, nhưng quá trình này sẽ mất một số năm. NIST dự đoán rằng DES ba lần vẫn sẽ là một thuật toán được sử dụng trong tương lai gần

Bảng 4.11: Liệt kê tham số của AES tùy thuộc vào kích thước của khóa. Trong phần này ta lựa chọn khóa 128 bits là kích thước thông dụng thường được triển khai trong thực tế.

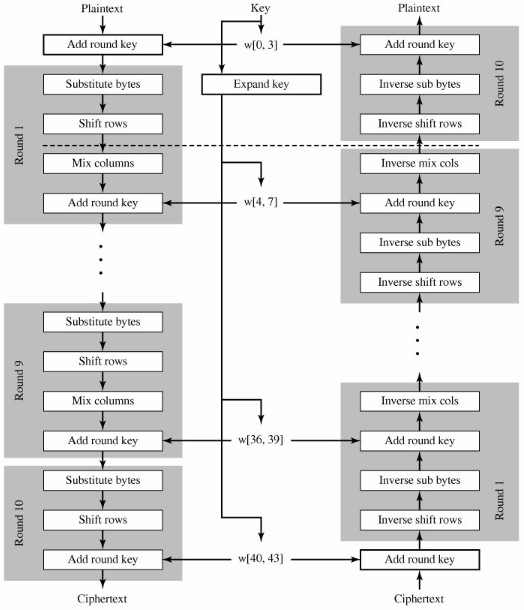
|  |  |  |  |
| --- | --- | --- | --- |
| Kích thước khóa (words/bytes/bits) | 4/16/128 | 6/24/192 | 8/32/256 |
| Kích thước khối của bản rõ (words/bytes/bits) | 4/16/128 | 4/16/128 | 4/16/128 |
| Số vòng | 10 | 12 | 14 |
| Kích thước khóa tại mỗi vòng (words/bytes/bits) | 4/16/128 | 4/16/128 | 4/16/128 |
| Kích thước khóa mở rộng (words/bytes) | 44/176 | 52/208 | 60/240 |

Bảng 4.11. Tham số của AES

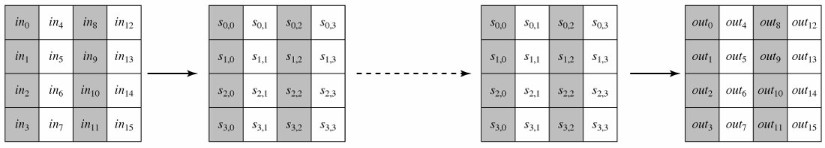
### Mã hóa và giải mã

Cấu trúc tổng thể của mã hóa AES được mô tả trên hình 4.10. Đầu vào cho thuật toán mã hóa và giải mã là một khối 128 bít, khối bít này được mô tả là một ma trận vuông, mỗi ô là 1 byte. Khối này được sao chép vào một mảng trạng thái, được sửa đổi ở mỗi giai đoạn mã hóa hoặc giải mã. Sau giai đoạn cuối cùng, mảng trạng thái này được sao chép vào một ma trận đầu ra. Các hoạt động này được mô tả trong hình 4.11.

Tương tự, khóa 128 bit được mô tả như một ma trận vuông, mỗi phần tử là một byte. Khóa này sau đó được mở rộng thành một mảng các từ (word), mỗi từ là bốn byte và tổng chiều dài khóa là 44 từ cho khóa 128 bit như hình 4.12. Lưu ý rằng thứ tự của các byte trong ma trận là theo cột. Vì vậy, bốn byte đầu tiên của bản rõ 128 bit đầu vào chiếm cột đầu tiên của ma trận, bốn byte thứ hai chiếm cột thứ hai, v.v. Tương tự, bốn byte đầu tiên của khóa mở rộng, tạo thành một từ, chiếm cột đầu tiên của ma trận w.



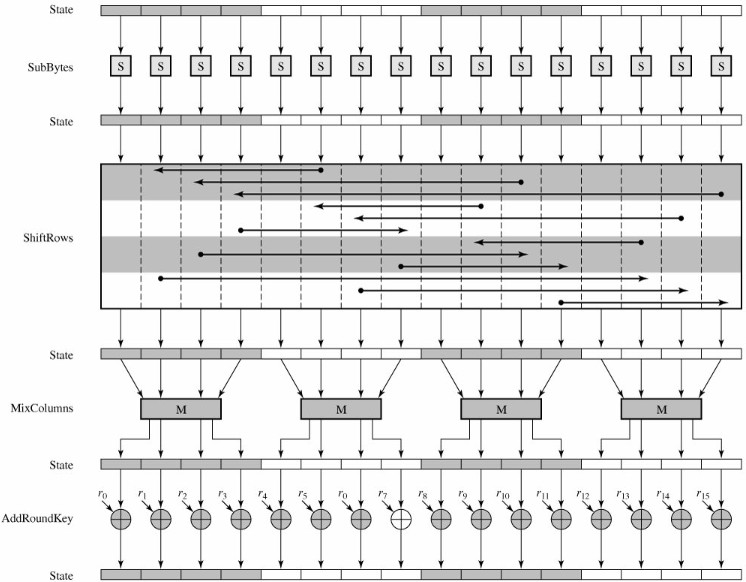
Hình 4.10. Cấu trúc mã hóa và giải mã AES



Hình 4.11. Đầu vào, mảng trạng thái và đầu ra



Hình 4.12. Khóa và mở rộng khóa

Cấu trúc của thuật toán AES tương đối đơn giản. Cả thuật toán mã hóa và giải mã đều bắt đầu giai đoạn AddRoundKey, tiếp theo là 9 vòng, mỗi vòng đầy đủ 4 giai đoạn: Thay thế các bytes (Substitute bytes) sử dụng hộp S để thực hiện việc thay thế từng byte của khối; dịch các dòng (ShiftRows) đơn giản là thực hiện hoán vị; trộn cột (MixColumns) là phép thay thế sử dụng các phép toán số học trên Z256; AddRoundKey đơn giản chỉ là phép XOR của khối hiện tại với một phần của khóa được mở rộng. Vòng cuối cùng chỉ có 3 giai đoạn. Hình 4.13 minh họa một vòng mã hóa đầy đủ.

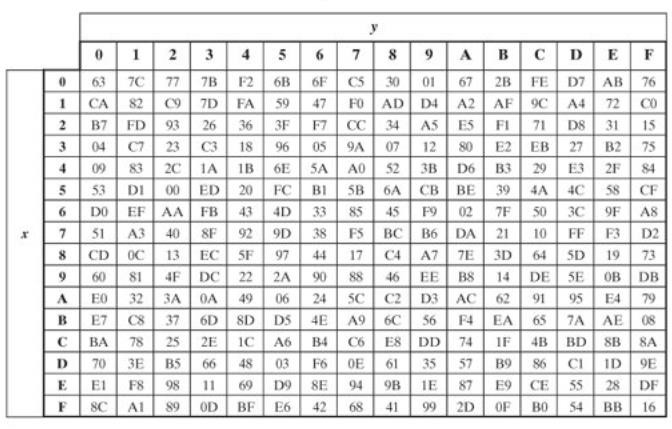
Hình 4.13. Minh họa một vòng mã AES

Tiếp theo ta đi xét chi tiết các giai đoạn trong một vòng mã hóa.

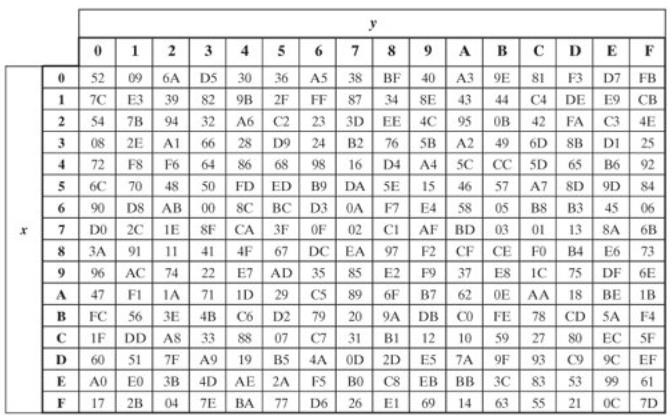
#### Thay thế byte

#### Thay thế byte đơn giản chỉ là tra cứu trong bảng 16 x 16, mỗi ô là 1 byte và được gọi là hộp S như bảng 4.12 và hộp S đảo bảng 4.13. Minh họa việc tra cứu hộp S như hình 4.14.

Hình 4.14. Phép thay thế byte sử dụng hộp S

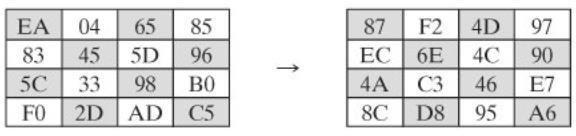


Bảng 4.12. Hộp S



Bảng 4.13. Hộp S đảo (inverse S box)

Ví dụ minh họa phép thay thế byte như hình 4.15



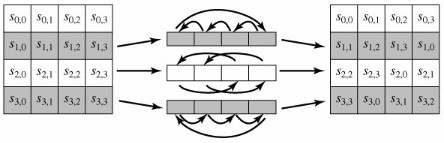
Hình 4.15. Minh họa phép thay thế byte

Để tìm byte thay thế của byte EA, ta tra dòng E và cột A trong hộp S thu được byte 87.

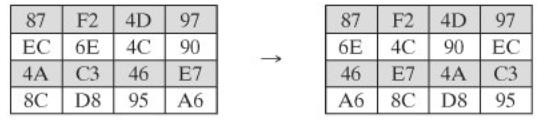
Như vậy, byte EA sẽ được thay thế bằng byte 87. Tương tự, byte 04 ta tra dòng 0 và cột 4 thu được F2.

Ta làm tương tự cho các byte còn lại sẽ thu được ma trận kết quả sau khi thực hiện phép thay thế.

#### Dịch dòng (Shiftrows)

Hình 4.16 minh họa phép dịch dòng. Dòng đầu tiên của ma trận trạng thái được giữ nguyên, dòng thứ hai quay trái 1 byte, dòng thứ 3 quay trái 2 byte và dòng cuối cùng quay trái 3 byte. Hình 4.17 ví dụ minh họa phép dịch dòng.

Hình 4.16. Minh họa phép dịch dòng

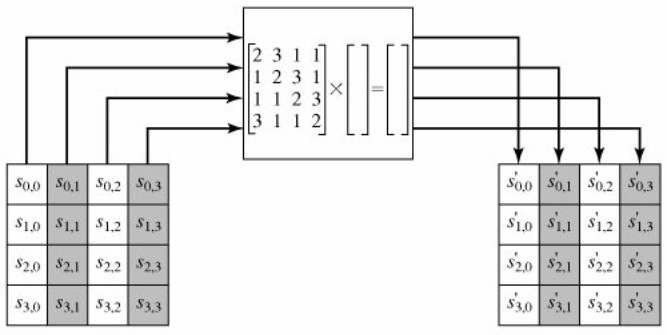


Hình 4.17. Ví dụ minh họa phép dịch dòng

Đối với thuật toán giải mã ta sử dụng phép dịch dòng ngược. Tức là, dòng đầu tiên của ma trận trạng thái giữ nguyên, dòng thứ 2 quay phải 1 byte, dòng thứ 3 quay phải 2 bytes và dòng cuối cùng quay phải 3 bytes.

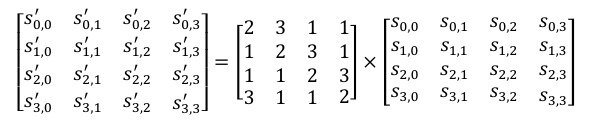
#### Trộn cột

Phép trộn cột được thực hiện như minh họa trên hình 4.18.



Hình 4.18. Minh họa phép trộn cột

Như vậy, kết quả của phép trộn cột sẽ được xác định theo công thức sau:



Áp dụng phép nhân hai ma trận ta thu được:

𝑠′ = (2 ∙ 𝑠0,𝑗) + (3 ∙ 𝑠1,𝑗) + 𝑠2,𝑗 + 𝑠3,𝑗

0,𝑗

𝑠′ = 𝑠0,𝑗 + (2 ∙ 𝑠1,𝑗) + (3 ∙ 𝑠2,𝑗) + 𝑠3,𝑗

1,𝑗

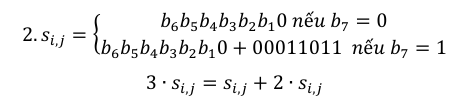
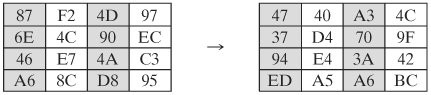
𝑠′ = 𝑠0,𝑗 + 𝑠1,𝑗 + (2 ∙ 𝑠2,𝑗) + (3 ∙ 𝑠3,𝑗)

2,𝑗

𝑠′ = (3 ∙ 𝑠0,𝑗) + 𝑠1,𝑗 + 𝑠2,𝑗 + (3 ∙ 𝑠3,𝑗)

3,𝑗

Trong đó, phép nhân (.) được thực hiện theo luật sau: Giả sử si,j được biểu diễn dưới dạng 8 bít b7b6b5b4b3b2b1b0 khi nhân với 2 sẽ được thực hiện theo công thức sau:

Phép cộng (+) trong các công thức trên là phép XOR bit.

Hình 4.9. Minh họa phép trộn cột

Ta diễn giải cách xác định phần tử đầu tiên trong ma trận sau khi thực hiện phép trộn cột.

0,0

𝑠′= 2 ∙ (87) + 3. (6𝐸) + 46 + 𝐴6.

Chuyển các số từ hệ 16 sang hệ 2 thu được 87h = 10000111. Do bít b7 = 1 nên 2.(87)

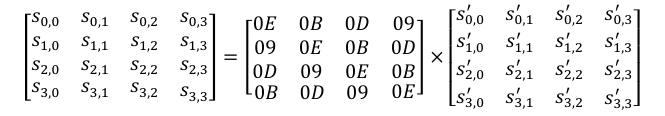
= 00001110 XOR 00011011 = 00010101, 6Eh = 01101110, 46h = 01000110, A6h = 10100110 và 3.(6E) = 6E + 2.(6E). Do bít b7 của 6E là 0 nên 2.(6E) = 11011100. Do đó,

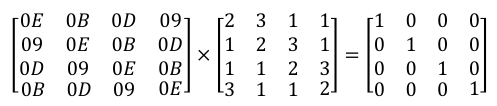
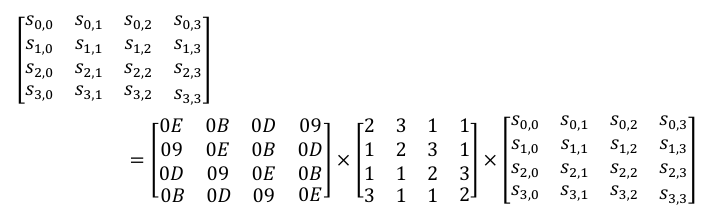
3.(6E) = 01101110 XOR 11011100 = 10110010.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2.(87) | = | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 |
| 3.(6E) | = | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 |
| 46 | = | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 |
| A6 | = | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 |
| XOR |  | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 = 47h |

Tính toán tương tự cho các phần tử còn lại ta thu được trạng thái sau khi thực hiện phép trộn cột.

Phép chuyển đổi đảo trộn cột (inverse mix column transform) trong thuật toán giải mã được thực hiện như sau:



Thay thế công thức của phép trộn cột vào thì ta thu được công thức sau

Như vậy, thì công thức sau phải được thỏa mãn

Ta chứng minh phần tử đầu tiên thỏa mãn yêu cầu. Thật vậy, 2.(0E) + 0B + 0D + 3.(09) = 00011100 + 00001011 + 00001101 + 3.(09). Trong đó, 3.(09) = 09 + 2.(09) =

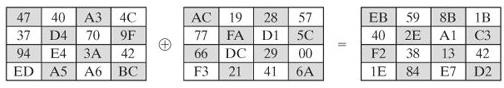
00001001 XOR 00010010 = 00011011. Cuối cùng ta thu được.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2.(0E) | = | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| 0B | = | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 |
| 0D | = | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 |
| 3.(09) | = | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 |
| XOR |  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 = 1 |

Các phần tử còn lại người đọc tự chứng mình như là một bài tập.

#### Cộng với khóa (add round key)

Phép cộng với khóa là thực hiện phép XOR bít của 128 bít của ma trận trạng thái và 128 bít của khóa tương ứng của vòng. Hình 4.10 minh họa ví dụ thực hiện phép cộng khóa, ma trận đầu tiên là trạng thái và ma trận thứ 2 là khóa của vòng.

Hình 4.10. Ví dụ minh họa phép cộng khóa

Mở rộng khóa

Thuật toán mở rộng khóa có đầu vào là 4 từ (16 bytes) khóa và tạo ra một mảng đầu ra 44 từ (176 bytes). Mã giả của thuật toán được mô tả như sau:

KeyExpansion (byte key[16], word w[44])

{

word temp for(i=0;i<4;i++)

w[i] = (key[4\*i], key[4\*i+1], key[4\*i+2], key[4\*i+3]) for(i=4,i<44;i++)

{

temp = w[i-1] if(i mod 4 = 0)

temp = SubWord(RotWord(temp)) XOR Rcon[i/4] w[i] = w[i-4] XOR temp

}

}

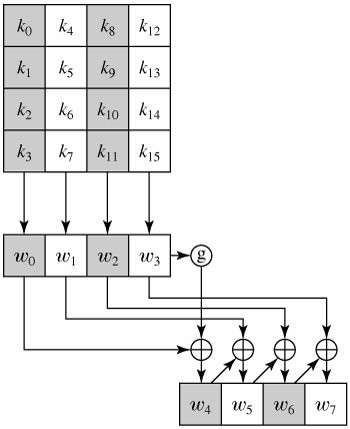
Trong đó, phép toán RotWord là thực hiện phép quay trái 1 byte, tức là đầu vào l từ có 4 byte [b0, b1, b2, b3] thì kết quả sau khi thực hiện phép quay trái 1 byte sẽ là [b1, b2, b3, b0]. Phép toán SubWord là phép thay thế byte sử dụng bảng S. Hằng số cho mỗi vòng khóa Rcon[j] = (RC[j], 0, 0, 0), với RC[1] = 1, RC[j] = 2.RC[j-1] và phép nhân (.) được thực hiện theo luật như trong thuật toán trộn cột. Giá trị của RC[j] được xác định như bảng

4.14 ở hệ thập lục phân (hexadecimal).

Bảng 4.14. Giá trị của RC[j]

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| j | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| RC[j] | 01 | 02 | 04 | 08 | 10 | 20 | 40 | 80 | 1B | 36 |

Hình 4.11 minh họa cách xác định khóa của một vòng.



Hình 4.11. Minh họa cách xác định khóa của vòng 1

Ví dụ minh họa cách xác định khóa cho vòng thứ 9 khi khóa tại vòng 8 là EA D2 73 21 B5 8D BA D2 31 2B F5 60 7F 8D 29 2F tương ứng w[32] = [EA, D2, 73, 21], w[33] = [B5, 8D, BA, D2], w[34] = [31, 2B, F5, 60] và w[35] = [7F, 8D, 29, 2F]. Giá trị của khóa tại vòng 9 được xác định như bảng sau:

Bảng 4.15. Ví dụ xác định khóa tại vòng 8

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Giá trị i ở hệ thập phân | temp | Sau khi thực hiện phép RotWord | Sau khi thực hiện phép SubWord | Rcon(9) | Sau khi XOR với Rcon | w[i-4] | w[i] = temp XOR w[i-4] |
| 36 | 7F8D292F | 8D292F7F | 5DA515D2 | 1B000000 | 46A515D2 | EAD27321 | AC7766F3 |
| 37 | AC7766F3 | AC7766F3 | AC7766F3 | 1B000000 | AC7766F3 | B58DBAD2 | 19FABC21 |
| 38 | 19FABC21 | 19FABC21 | 19FABC21 | 1B000000 | 19FABC21 | 312BF560 | 28B14941 |
| 39 | 28B14941 | 28B14941 | 28B14941 | 1B000000 | 28B14941 | 7F8D292F | 575C606E |

Như vậy, khóa của vòng 9 sẽ là AC 77 66 F3 19 FA BC 21 28 B1 49 41 57 5C 60 6E.