CHƯƠNG 4: MÃ KHỐI HIỆN ĐẠI VÀ CHUẨN MÃ DỮ LIỆU

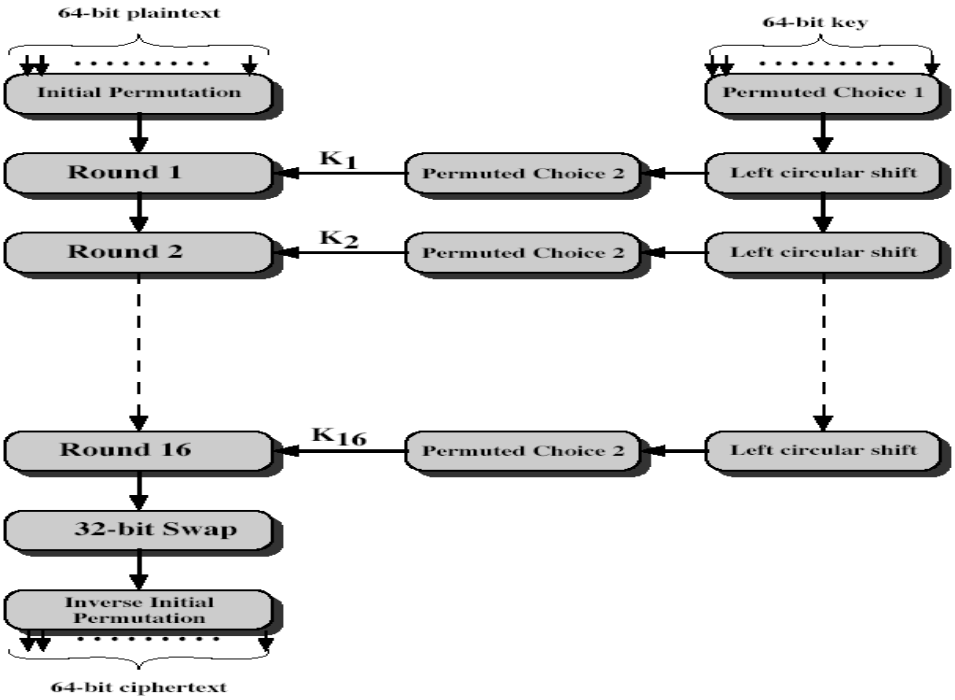
4.1. Chuẩn mã dữ liệu DES

DES (Data Encryption Standards) là mã khối sử dụng rộng rãi nhất trên thế giới trong thời gian vừa qua. Nó được đưa ra năm 1977 bởi NBS – văn phòng chuẩn Quốc gia Hoa Kỳ (bây giờ là NIST - Viện chuẩn và công nghệ Quốc gia). DES là mã khối với mỗi khối dữ liệu 64 bit và dùng khóa dài 56 bit. Nó được sử dụng rộng rãi và đã được tranh luận kỹ về mặt an toàn.

Lịch sử DES

Cuối những năm 1960, IBM phát triển mã Lucifer, được lãnh đạo bởi Fiestel. Ban đầu Lucifer sử dụng khối dữ liệu 64 bit và khóa 128 bit. Sau đó tiếp tục phát triển như mã thương mại. Năm 1973 NBS yêu cầu đề xuất chuẩn mã Quốc gia. IBM đề nghị bản sửa đổi Lucifer, sau này gọi là DES. Đã có các tranh luận về thiết kế của DES. Vì chuẩn của DES được công khai, mọi người đóng góp ý kiến về tốc độ, độ dài khóa và mức độ an toàn, khả năng thám mã. Người ta đề xuất chọn khóa 56 bit thay vì 128 để tăng tốc độ xử lý và đưa ra các tiêu chuẩn thiết kế một chuẩn mã dữ liệu. Các suy luận và phân tích chứng tỏ rằng thiết kế như vậy là phù hợp. Do đó DES được sử dụng rộng rãi, đặc biệt trong lĩnh vực tài chính.

4.1.1. Sơ đồ mã DES



- **Sinh khóa con của DES**
  - Tạo 16 khóa con sử dụng cho 16 vòng của DES. 56 bit khóa đầu vào được sử dụng như bảng 8 x 8, trong đó cột thứ 8 không sử dụng.
  - Hoán vị ban đầu của khóa PC1 và tách 56 bit thành hai nửa 28 bit.
  - 16 giai đoạn bao gồm
    - Ở mỗi vòng nửa trái và nửa phải được dịch trái vòng quanh tương ứng 1 và 2 bit. Hai nửa này được dùng tiếp cho vòng sau.

        - Đồng thời hai nửa cũng cho qua hoán vị PC2 và chọn mỗi nửa 24 bit gộp lại thành 48 bit để sinh khóa con.
    - Ứng dụng thực tế trên cả phần cứng và phần mềm đều hiệu quả
- **Hoán vị ban đầu IP**: đây là bước đầu tiên của tính toán dữ liệu, hoán vị IP đảo thứ tự các bit đầu vào: các bit chẵn sang nửa trái và các bit lẻ sang nửa phải. Hoán vị trên dễ dàng thực hiện trên phần cứng.
  Mỗi số trong hệ 16 biểu diễn bởi 4 bit, 16 số được thể hiện bởi 64 bit. Mỗi bit có một vị trí xác định qua hoán vị ban đầu.

- **Thực hiện 16 vòng:** mỗi vòng sử dụng một khóa con riêng

- **Cấu tạo một vòng của DES**
  Sử dụng hai nửa 32 bit trái và 32 bit phải. Như đối với mọi mã Fiestel, nửa phải của vòng trước được chuyển qua nửa trái của bước sau và lấy đầu ra của hàm vòng trên nửa phải và khóa con cộng cơ số 2 với nửa trái. Có thể biểu diễn bằng công thức như sau:

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

  $$R_i = L_{i-1} \text{ xor } F(R_{i-1}, K_i)$$

  Ở đây F lấy 32 bit nửa phải R, mở rộng thành 48 bit nhờ hoán vị E, rồi cộng vào với khóa con 48 bit. Sau đó chia thành 8 cụm 6 bit và cho qua 8 S-box để nhận được kết quả 32 bit. Đảo lần cuối sử dụng hoán vị 32 bit nhận được 32 bit đầu ra, rồi cộng với nửa trái để chuyển thành nửa phải của bước sau.

4.1.2. Triple DES

Rõ ràng cần phải thay thế DES, vì có những tấn công về mặt lý thuyết có thể bẻ được nó. Một số tấn công nghiên cứu thấu đáo khóa đã được trình diễn. Người ta thấy rằng, cần sử dụng Triple DES (sử dụng DES ba lần liên tiếp) cho các ứng dụng đòi hỏi tăng cường bảo mật.

Mã DES nhiều lần là giải pháp để tăng cường độ mật của mã. Rõ ràng DES cần được thay thế, vì

- Các tấn công về mặt lý thuyết có thể bẻ gãy nó.
- Tấn công khóa toàn diện đã được trình diễn.

AES là mã mới thay thế. Trước nó người ta đã sử dụng lặp DES, tức là sử dụng nhiều lần cùng một thuật toán, nhưng có thể với khóa khác nhau. Triple DES là dạng đã được chọn, ở đây lặp DES ba lần. Tại sao lại là Triple DES, mà không phải là lặp hai lần Double DES: khi lặp hai lần không hoàn toàn là trùng với một lần DES nào đó, nhưng cũng có thể là như vậy.

- Có thể dùng hai lần DES trên một block với hai khóa K1 và K2 :

  $$C = EK2(EK1(P))$$

- Vấn đề là có thể rút gọn về một bước không và
- Double DES gặp tấn công ở mức trung gian, tức là khi sử dụng một mã nào đó hai lần như trên, thì ta có viết

  $$X = E_{K1}[P] = D_{K2}[C]$$

Khi đó kẻ thám mã tấn công bằng cách phán đoán bản rõ P và mã với mọi khóa và lưu lại. Và giải mã bản mã C với các khóa và sánh trùng nhau ở mức trung gian X. Có thể chỉ ra rằng cần $O(2^{56})$ bước dò tìm.

Triple DES với hai khóa

- Để tránh tấn công ở mức trung gian, cần sử dụng ba lần mã, nói chung có thể dùng ba khóa khác nhau.
- Nhưng để đơn giản hơn có thể sử dụng 2 khóa theo trình tự: E–D-E, tức là mã, giải mã, rồi lại mã.

$$C = E_{K1}[D_{K2}[E_{K1}[P]]]$$

Về mặt an toàn mã và giải mã tương đương nhau. Nếu K1 = K2, thì Triple DES làm việc tương đương với một lần DES, nên K1 phải khác K2. Mô hình này chưa thấy tấn công thực tế.

Triple DES với ba khóa

- Mặc dù chưa có tấn công thực tế, nhưng Triple DES với hai khóa có một số chỉ định để tránh rơi vào một số trường hợp đặc biệt.
- Do đó cần phải sử dụng ba lần DES với ba khóa để tránh điều đó

$$C = E_{K3}[D_{K2}[E_{K1}[P]]]$$

- Được chấp nhận dùng trong một số ứng dụng trên Internet: PGP, S/MIME

4.2. Chuẩn mã nâng cao AES

Rõ ràng Triple DES có quá trình mã và giải mã chậm, đồng thời với khối dữ liệu nhỏ. Do đó Viện chuẩn quốc gia Hoa Kỳ US NIST ra lời kêu gọi tìm kiếm chuẩn mã mới vào năm 1997. Sau đó có 15 đề cử được chấp nhận vào tháng 6 năm 1998. Và được rút gọn còn 5 ứng cử viên vào tháng 6 năm 1999. Đến tháng 10 năm 2000, mã Rijndael được chọn làm chuẩn mã nâng cao.

Yêu cầu của AES

Là mã khối đối xứng khóa riêng với kích thước khối dữ liệu 128 bit và độ dài khóa là tùy biến: 128, 192 hoặc 256 bit. Chuẩn mã mới phải mạnh và nhanh hơn Triple DES. Mã mới có cơ sở lý thuyết mạnh để thời gian sống của chuẩn khoảng 20-30 năm (cộng thêm thời gian lưu trữ). Khi đưa ra thành chuẩn yêu cầu cung cấp chi tiết thiết kế và đặc tả đầy đủ, đảm bảo rằng chuẩn mã mới cài đặt hiệu quả trên cả C và Java. Viện chuẩn Hoa kỳ NIST in rút gọn mọi đề xuất, phân tích tìm kiếm chuẩn mã nâng cao.

Tiêu chuẩn triển khai của AES

An toàn tổng thể, dễ cài đặt phần mềm và phần cứng, chống được tấn công về mặt cài đặt, mềm dẻo trong mã/giải mã, khóa và các yếu tố khác

Chuẩn mã nâng cao AES – Rijndael

Cuối cùng Rijndael được chọn là chuẩn mã nâng cao. Nó được thiết kế bởi Rijmen – Daemen ở Bỉ, có các đặc trưng sau: có 128/192/256 bit khóa và 128 bit khối dữ liệu, thao tác trong các vòng lặp hơi khác với Fiestel. Trong mô hình Fiestel, mỗi vòng chỉ xử lý một nửa, còn mỗi vòng AES xử lý toàn bộ dữ liệu:

- Chia dữ liệu thành 4 nhóm – 4 byte
- Thao tác trên cả khối mỗi vòng

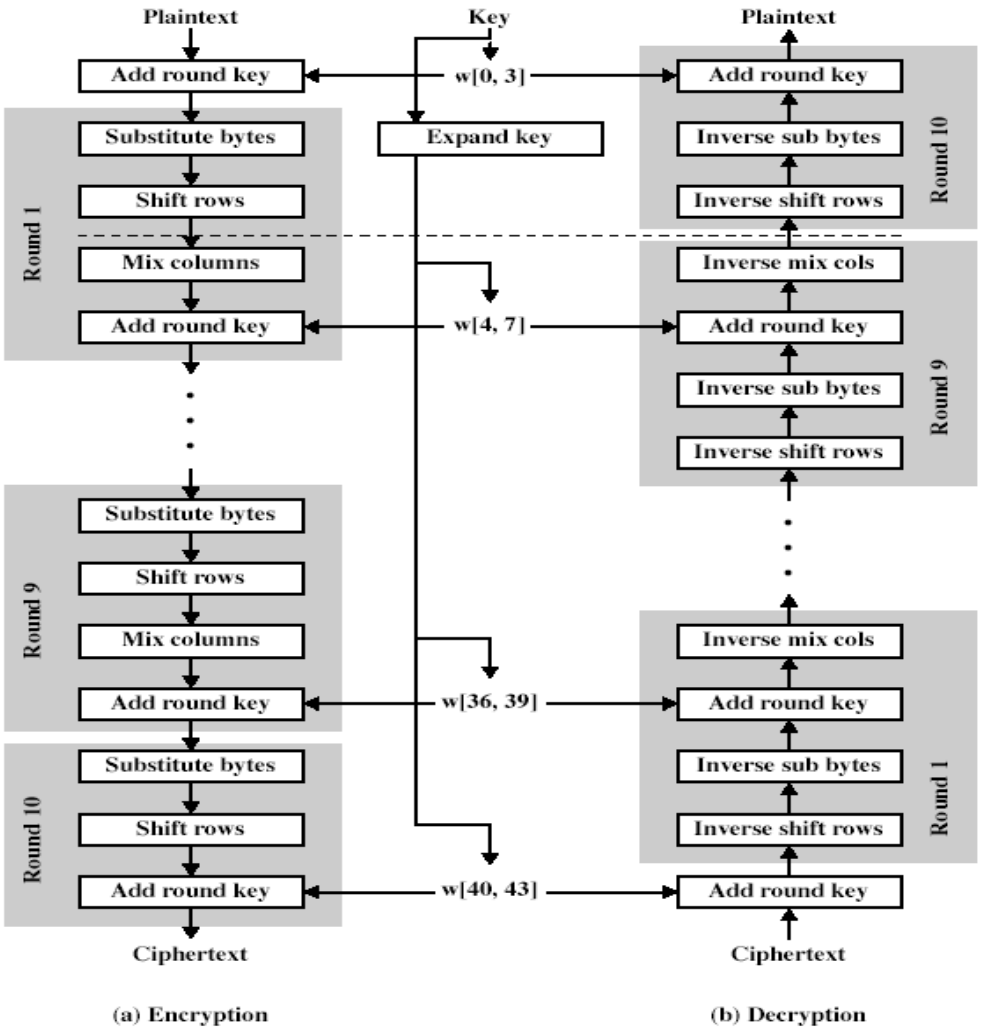
- Thiết kế để chống lại các tấn công đã biết, tốc độ nhanh và nén mã trên nhiều CPU.

Rijndael có thiết kế rõ ràng, xử lý khối dữ liệu 128 bit như 4 nhóm của 4 byte: 128 = 4*4*8 bit. Mỗi nhóm nằm trên một hàng, bố trí thành ma trận 4 hàng, 4 cột với mỗi phần tử là 1 byte coi như trạng thái được xử lý qua các vòng mã hoá và giải mã. Như vậy mỗi khối

Khóa mở rộng thành mảng gồm 44 từ, mỗi từ 32 bit w[i] với i =0, ..., 43. Mỗi vòng dùng 4 từ khóa. Có tùy chọn 9/11/13 vòng, trong đó mỗi vòng bao gồm

- Phép thế byte (dùng S box để xác định phần tử thế cho 1 byte)
- Dịch hàng (hoán vị byte giữa nhóm/cột)
- Trộn cột (sử dụng nhân ma trận của các cột)
- Cộng khóa vòng (XOR trạng thái dữ liệu với khóa vòng).
- Mọi phép toán được thực hiện với XOR và bảng tra, nên rất nhanh và hiệu quả.

Sơ đồ Rijndael



Một v

Phép thế Byte

- Phép thế byte đơn giản.

- Sử dụng một bảng 16 x 16 byte chứa hoán vị của tất cả 256 giá trị khác nhau có độ dài 8 bit.
- Mỗi byte trạng thái được thay bởi byte trên hàng xác định bởi 4 bit trái và cột xác định bởi 4 bit phải.
- Chẳng hạn {95} được thay bởi phần tử ở hàng 9, cột 5, mà giá trị sẽ là {2A}.
- Thiết kế để chống mọi tấn công đã biết

Dịch hàng

- Dịch hàng vòng quanh trên mỗi hàng
  - Hàng 1 không đổi.
  - Hàng 2 dịch vòng quanh 1 byte sang trái.
  - Hàng 3 dịch vòng quanh 2 byte sang trái.
  - Hàng 4 dịch vòng quanh 3 byte sang trái.
- Giải mã thực hiện dịch ngược lại sang phải.
- Vì trạng thái được xử lý bởi cột, bước này thực chất là hoán vị byte giữa các cột.

Trộn các cột

- Mỗi cột được xử lý riêng biệt.
- Mỗi byte được thay bởi một giá trị phụ thuộc vào tất cả 4 byte trong cột

Cộng khóa vòng

- XOR trạng thái với 128 bit khóa của vòng đó
- Mọi bước trước đều không sử dụng đến khóa và có thể nghịch đảo được mà không cần khóa.
- Khóa vòng được sinh như một số giả ngẫu nhiên và dùng như bộ đệm một lần, nên mã và giải mã nhanh và hiệu quả.
- Thiết kế sinh khóa vòng đơn giản nhất có thể, đòi hỏi thêm một số bước tăng độ phức tạp và tính an toàn.

Mở rộng khóa AES

- Dùng khóa 128 bit (16 byte) và mở rộng thành mảng gồm 44/52/60 từ 32 bit.
- Bắt đầu bằng việc copy khóa vào 4 từ đầu tiên.
- Sau đó tạo quay vòng các từ mà phụ thuộc vào giá trị ở các vị trí trước và 4 vị trí sau:
  - 3 trong 4 trường hợp chỉ là XOR chúng cùng nhau.
  - Mỗi cái thứ 4 có S box kết hợp quay và XOR với hằng số trước đó, trước khi XOR cùng nhau.
  - Thiết kế chống các tấn công đã biết.

Thuật toán sinh khóa vòng được mô tả trong chương trình giả mã sau:

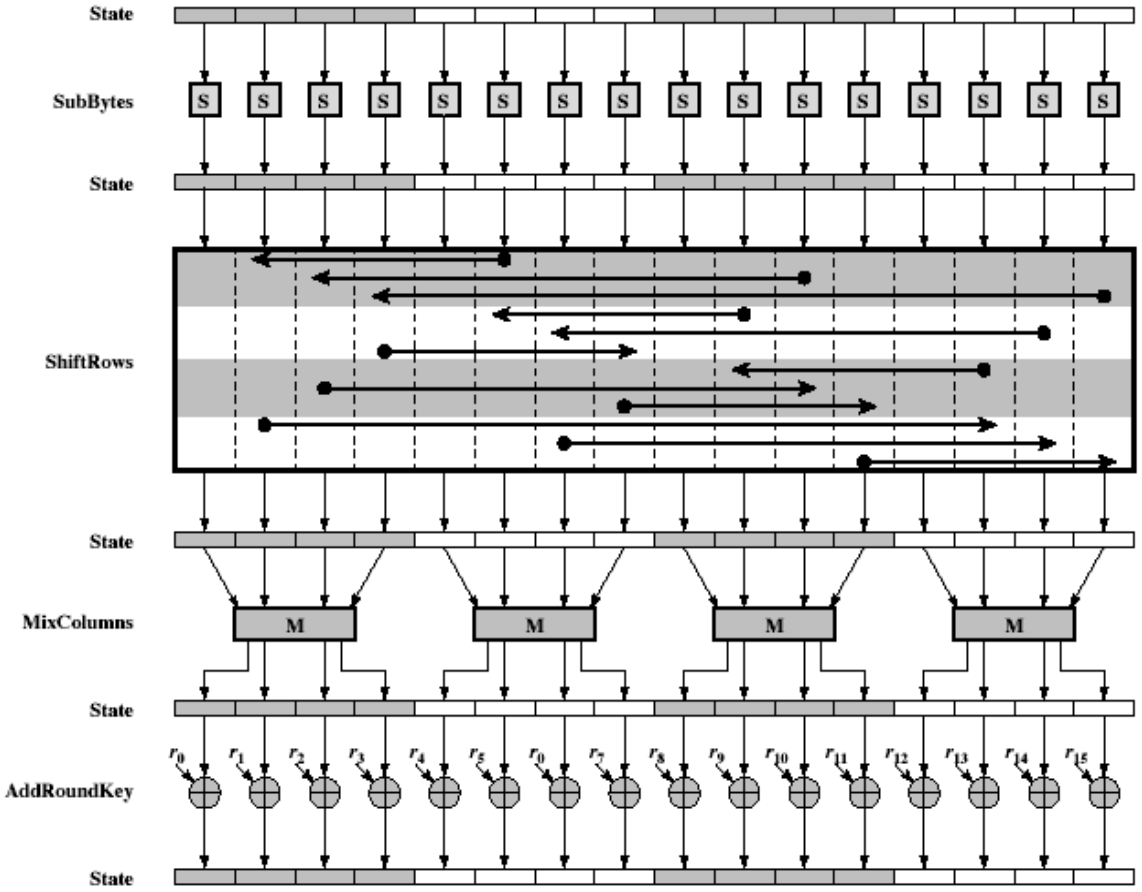
```
KeyExpansion(byte key[16], word w[44])
{
    word temp
```

```
    for (i -0, i < 4; i++) w[i]  = (key[4*i], key[4*i + 1] , kekey[4*i + 2], y[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

- RotWord thực hiện dịch trái vòng quanh 1 byte trong từ đó.
- Subword thực hiện thế byte trên hộp S box
- Kết quả các bước 1 và 2 được XOR với hằng số cho trước của vòng Rcon[i/4].

- **Giải mã AES**
  - Thông thường các thuật toán giải mã sử dụng mở rộng khóa theo thứ tự ngược lại. Nhưng thuật toán giải mã AES không giống thuật toán mã hóa.
  - Trước hết khẳng định rằng 4 bước trong mỗi vòng đều có thể nghịch đảo được. Như vậy ta sẽ có các phép toán ngược của các bước trong một vòng mã.
  - Do đó mỗi vòng ta thực hiện các bước theo thứ tự: dịch hàng ngược, thế byte ngược, cộng khóa vòng và trộn cột ngược.



- **Lý do mở rộng khóa.** Các tiêu chuẩn thiết kế bao gồm

- Giả sử biết một phần khóa, khi đó không đủ để biết nhiều hơn, tức là các khóa con khác hoặc khóa nói chung.
- Phép biến đổi nghịch đảo được, nhanh đối với nhiều kiểu CPU.
- Sử dụng hằng số vòng để làm mất tính đối xứng
- Khuếch tán bit khóa thành khóa con cho các vòng
- Có đủ tính phi đối xứng để chống thám mã
- Đơn giản trong việc giải mã

- **Các khía cạnh cài đặt:**
  - Có thể cài đặt hiệu quả trên CPU 32 bit, sử dụng từ 32 bit.
  - Có thể tính trước 4 bảng với 256 đầu vào.
  - Sau đó mỗi cột trong mỗi vòng có thể tính bằng cách tra 4 bảng và 4 XOR.
  - Cần 16 Kb để lưu các bảng để đẩy nhanh tốc độ tính toán.
  - Những nhà thiết kế tin tưởng rằng việc cài đặt rất hiệu quả này là yếu tố cơ bản trong việc chọn mã AES làm chuẩn nâng cao.

4.3. Mã dòng

RC4 là mã đăng ký bản quyền của RSADSI, được thiết kế bởi Ronald Rivest. RC4 đơn giản, nhưng hiệu quả, có nhiều cỡ khóa và là mã bit dòng. Mã được sử dụng rộng rãi (Web SSL/TLS, thuật toán bảo mật cho mạng không dây WEP). Khóa thực hiện hoán vị ngẫu nhiên cả 8 giá trị bit. Sử dụng hoán vị đó để khuấy thông tin đầu vào được xử lý từng byte.

Sinh khóa RC4

Bắt đầu từ mảng S với biên độ: 0..255. Sau đó sử dụng khóa để xáo trộn đều thực sự.

Mảng S sẽ tạo trạng thái trong của mã.

Tổng quan RC4

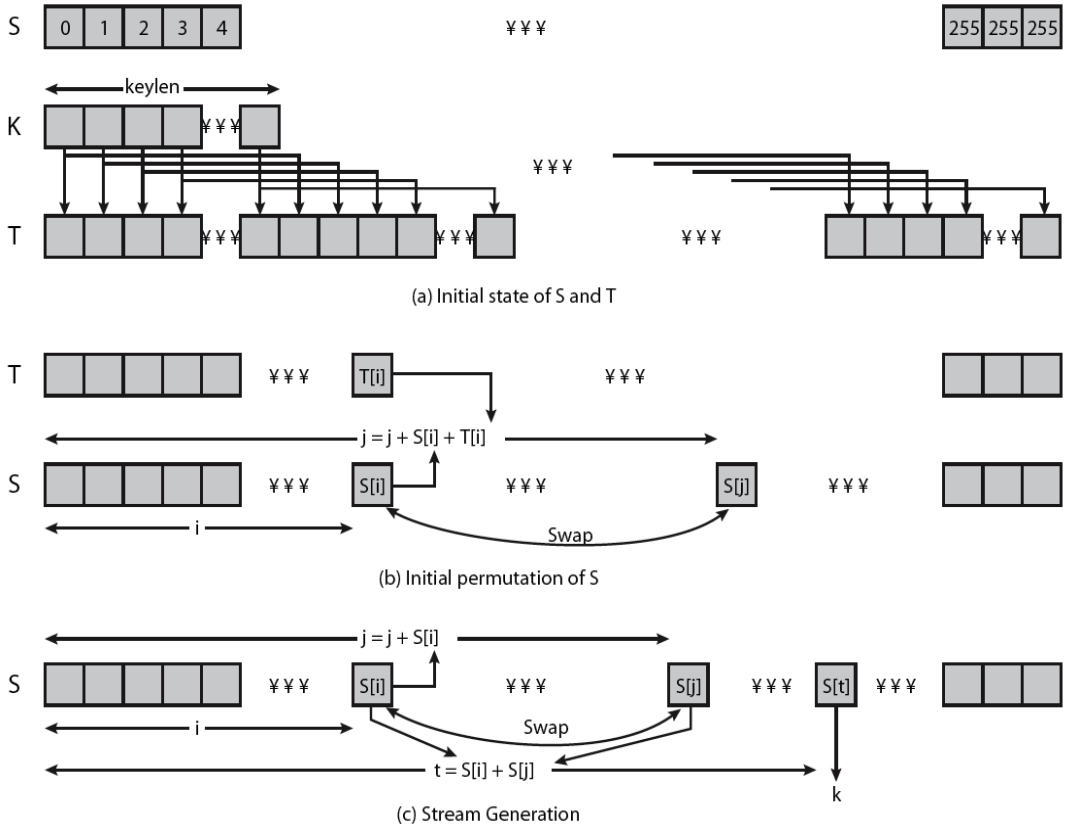
Mã RC4

Mã tiếp tục trộn các giá trị của mảng. Dựa vào tổng của các cặp trộn để chọn giá trị khóa dòng từ hoán vị và XOR S[t] với byte tiếp theo của bản tin để mã/giải mã:

```
i = j = 0
for each message byte Mi
i = (i + 1) (mod 256)
j = (j + S[i]) (mod 256)
swap(S[i], S[j])
t = (S[i] + S[j]) (mod 256)
Ci = Mi XOR S[t]
```

An toàn RC4

Mã dòng RC4 đảm bảo an toàn chống các tấn công đã biết, có một số thám mã, nhưng không thực tế. Mã cho kết quả rất phi tuyến và vì RC4 là mã dòng nên không được sử dụng lại khóa.



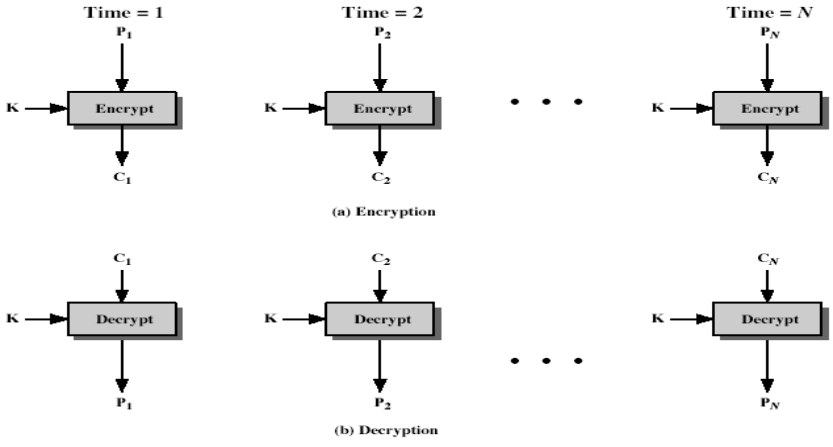
4.4. Bảo mật thông điệp

4.4.1. Các chế độ thao tác khối

Mã khối mã các block có kích thước cố định. Chẳng hạn DES mã các block 64 bit với khóa 56 bit Cần phải có cách áp dụng vào thực tế vì các thông tin cần mã có kích thước tùy ý. Trước kia có 4 kiểu thao tác được định nghĩa cho DES theo chuẩn ANSI: ANSI X3.106-1983 Modes of Use. Bây giờ mở rộng thêm có 5 cách cho DES và chuẩn mã nâng cao (AES – Advanced Encryption Standards). Trong đó có kiểu áp dụng cho khối và có kiểu áp dụng cho mã dòng. Sau đây ta xem xét 3 chế độ cơ bản.

Sách mật mã điện tử (Electronic Code Book - ECB)

- Mẫu tin được chia thành các khối độc lập, sau đó mã từng khối
- Mỗi khối là giá trị cần thay thế như dùng sách mã, do đó có tên như vậy
- Mỗi khối được mã độc lập với các mã khác $C_i = DES_{K1}(P_i)$
- Khi dùng: truyền an toàn từng giá trị riêng lẻ



- Nhược điểm của ECB: lặp trên bản mã sẽ nhận biết được việc lặp trên bản rõ, đặc biệt nếu dóng đúng khối và thường xảy ra với hình ảnh hoặc với bản tin mà thay đổi rất ít sẽ trở thành đối tượng để thám mã.
- Do nhược điểm là các khối được mã độc lập; nên được sử dụng chủ yếu khi gửi dữ liệu có kích thước nhỏ.

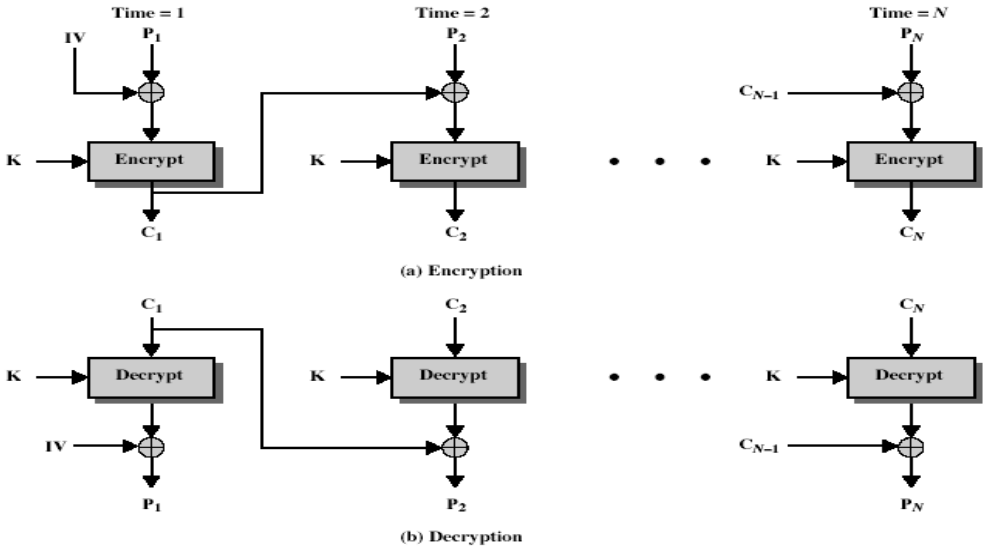
Dây chuyền mã khối (Cipher Block Chaining - CBC)

- Các mẫu tin được chia thành các khối, nhưng chúng được liên kết với nhau trong quá trình mã hoá.
- Các block được sắp thành dãy, vì vậy có tên như vậy
- Sử dụng véctơ ban đầu IV để bắt đầu quá trình

$$C_i = DES_{K1}(P_i \text{ XOR } C_{i-1})$$

$$C_{-1} = IV$$

- Dùng khi: mã dữ liệu lớn và cho mục đích xác thực



Ưu điểm của CBC

- Mỗi khối mã phụ thuộc vào tất cả các khối bản rõ, nên các khối bản mã giống nhau nói chung sẽ có các bản mã khác nhau.
- Sự thay đổi của bản tin ở đâu đó sẽ kéo theo sự thay đổi của mọi khối mã, nên có thể dùng khối cuối làm đặc trưng của cả thông điệp

Nhược điểm của CBC

- Cần giá trị véc tơ ban đầu IV được biết trước bởi người gửi và người nhận. Tuy nhiên nếu IV được gửi công khai, kẻ tấn công có thể thay đổi bit đầu tiên và thay đổi cả IV để bù trừ. Vậy IV cần phải có giá trị cố định trước hoặc mã hoá trong chế độ ECB và gửi trước phần còn lại của mẩu tin.
- Chế độ mã CBC thực hiện chậm, vì khối sau phải chờ các khối trước thực hiện xong.
- Lỗi ở các khối trước lan truyền sang các khối kế tiếp.

Bộ đệm

Ở cuối bản tin, để kiểm soát các block ngắn còn lại. Có thể bổ sung các giá trị không phải dữ liệu như NULL hoặc dùng bộ đệm cuối với số byte đếm kích thước của nó.

Ví dụ

[b1 b2 b3 0 0 0 0 5] <- 3 data bytes, vậy có 5 bytes dành cho đệm và đếm.

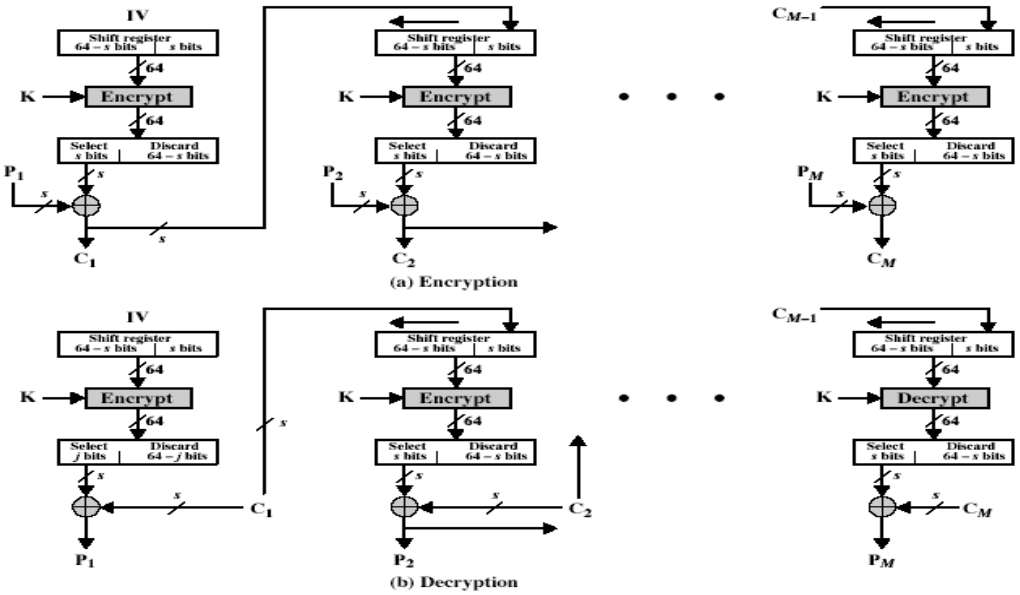
Mã phản hồi ngược (Cipher Feed Back - CFB)

- Bản tin coi như dòng các bit, bổ sung vào đầu ra của mã khối
- Kết quả phản hồi trở lại cho giai đoạn tiếp theo, vì vậy có tên như vậy.
- Nói chung cho phép số bit phản hồi là 1, 8, 64, hoặc tuỳ ý: ký hiệu tương ứng là CFB1, CFB8, CFB64,…
- Thường hiệu quả sử dụng cả 64 bit

$$C_i = P_i \text{ XOR } DES_{K1}(C_{i-1})$$

$$C_{-1} = IV$$

- Được dùng cho mã dữ liệu dòng và mục đích xác thực



Ưu điểm của mã phản hồi ngược

- Được dùng khi dữ liệu đến theo byte/bit, chế độ dòng thường gặp nhất
- Lặp trên bản rõ không tạo lặp trên bản mã.

Nhược điểm của mã phản hồi ngược

- Hạn chế là cần ngăn chuồng khi mã khối sau mỗi n bit để chỉ cho phép lỗi lan ra một vài block sau đó
- Mã/giải mã chậm, do các khối sau phải chờ các khối trước thực hiện xong.

4.4.2. Các vị trí đặt mã

Yêu cầu: mã đối xứng truyền thống được dùng để giữ bí mật bản tin.

Xét kịch bản tiêu biểu

- Các máy trạm ở một mạng LAN truy cập vào các máy trạm và máy chủ ở một mạng LAN khác.

- Các mạng được kết nối sử dụng chuyển mạch và đường truyền (switches/routers).
- Với các đường truyền vật lý hoặc liên kết vô tuyến/vệ tinh.

Xét việc tấn công và cách đặt mã trong kịch bản trên

- Điều tra từ một máy trạm khác.
- Sử dụng kết nối đến mạng hoặc máy chủ để tìm kiếm thông tin.
- Sử dụng kết nối ngoài để xâm nhập và điều tra.
- Theo dõi và/hoặc làm thay đổi việc truyền ở kết nối bên ngoài.

Có hai phương pháp chính xác định chỗ đặt mã:

Mã kết nối (Link Encryption)

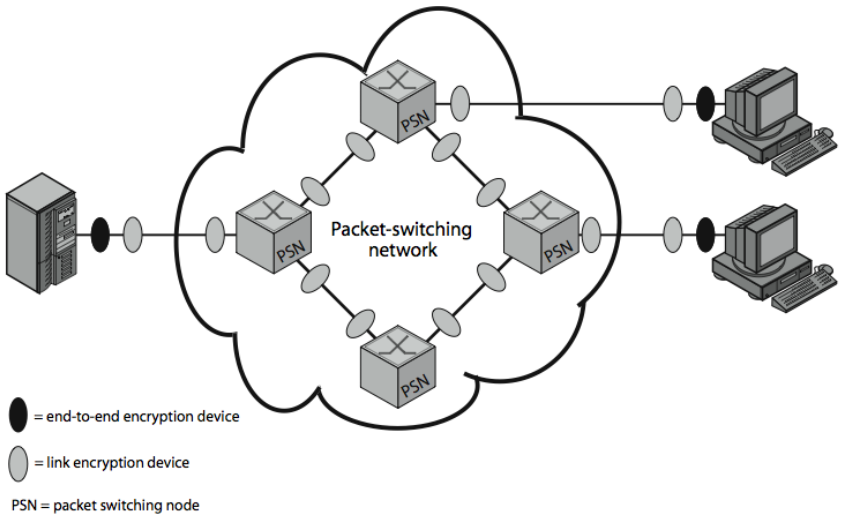
- Mã xảy ra độc lập trên mỗi kết nối.
- Suy ra cần phải giải mã truyền tin giữa các kết nối
- Đòi hỏi nhiều thiết bị và các cặp khóa

Mã đầu cuối (End to end Encryption):

- Mã xảy ra giữa điểm gốc và điểm đích
- Cần thiết bị tại mỗi đầu cuối và khóa chia sẻ

Thám mã thông tin truyền

Khi dùng mã đầu cuối cần phải để thông tin đầu của nó rõ ràng, vì như vậy mạng mới định hướng đúng đắn thông tin. Vì vậy tuy nội dung tin được bảo vệ, nhưng khuôn dòng tin truyền thì không. Tốt nhất là muốn bí mật cả hai. Mã đầu cuối bảo vệ thông tin nội dung trên cả đường truyền và cung cấp danh tính. Còn mã kết nối bảo vệ luồng truyền khỏi việc theo dõi.



Vị trí mã

Có thể đặt mã ở nhiều tầng khác nhau trong mô hình Hệ thống truyền thông mở OSI.

- Mã kết nối thực hiện ở tầng 1 hoặc 2.

- Mã đầu cuối có thể thực hiện ở tầng 3, 4, 6, 7
- Dịch chuyển đến tầng càng cao, càng ít thông tin được mã hóa, nhưng càng đảm bảo tính riêng tư hơn do người sử dụng giữ bí mật được khóa, tuy nhiên phức tạp hơn với nhiều đối tượng và khóa.

Thám mã thông tin truyền. Thám mã là theo dõi dòng thông tin truyền giữa hai đối tác:

- Được dùng cả trong quân sự và thương mại
- Có thể được dùng để tạo kênh giám sát
- Mã kết nối che lấp chi tiết đầu tin, nhưng xét trên toàn mạng và ở các đầu cuối nó vẫn nhìn thấy được.
- Bộ đệm truyền có thể che được dòng tin, nhưng với phải truyền liên tục với tần suất truyền hầu như không đổi theo thời gian.

TÓM LƯỢC CUỐI BÀI

- Cấu trúc mã khối Fiestel
- Chuẩn mã dữ liệu DES và các chế độ mã
- Triple DES và chuẩn mã nâng cao
- Mã dòng
- Chỗ đặt mã: mã link và mã đầu cuối
- Phân phối khóa: khóa chủ và khóa phiên

CÂU HỎI TRẮC NGHIỆM CUỐI BÀI

Câu 1: Trong mã hóa DES điều khẳng định nào là không đúng

A. Mã khối với mỗi khối 64 bit, khóa có độ dài 56 bit
B. Hoán vị đầu, nghịch đảo cuối và lặp 16 vòng
C. Khóa dùng chung cho 16 vòng
D. Mỗi vòng: hoán vị 2 nửa, xử lý một nửa dùng phép thế qua hộp và cộng khóa con

Câu 2. Trong thuật toán mã AES điều khẳng định nào là không đúng:

A. Có 128/192/256 bit khoá và 128 bit dữ liệu
B. Có 9/11/13 vòng, mỗi vòng: thế byte, dịch hàng, trộn cột, cộng khóa
C. Mỗi vòng: chia 2 nửa, đảo chỗ và xử lý một nửa
D. Xử lý dữ liệu như 4 nhóm của 4 byte

Câu 3. Các chế độ làm việc của DES. Khẳng định nào sau đây là sai

A. ECB: khối mã trước quay vòng tác động vào khối mã sau
B. CBC: khối mã trước cộng nhị phân với khối bản tin sau rồi mã
C. CFB: bản tin như dòng bit cộng nhị phân đầu ra của mã, rồi phản hồi
D. OFB: đầu ra mã phản hồi và cộng nhị phân với dòng bit của bản tin

Câu 4. Thành phần của mã dòng không bao gồm:

A. Khóa chia sẻ người gửi và người nhận
B. Bộ sinh số giả ngẫu nhiên dưới tác động của khóa
C. Bộ sinh các khóa con từ khóa chính
D. Bộ cộng loại trừ bit giữa dữ liệu với dãy giả nhẫu nhiên

Câu 5. Mã đối xứng không đặt ở vị trí đặt nào:

A. Mã đầu cuối ở máy tính đầu - cuối bảo vệ thông tin nội dung trên cả đường truyền và cung cấp danh tính, tầng 3, 4, 6, 7
B. Mã kết nối đặt ở máy tính đầu cuối và mạng chuyển gói tin bảo vệ luồng truyền khỏi việc theo dõi, tầng 1, 2
C. Kết hợp cả hai dạng trên
D. Mã đầu cuối ở tầng 5 - tầng phiên

ĐÁP ÁN CÂU HỎI TRẮC NGHIỆM

Câu 1: C, trong 16 vòng, mỗi vòng dùng một khóa con riêng
Câu 2: C, mỗi vòng xử lý cả khối 128 bit, tức là cả 4 nhóm - mỗi nhóm 4 byte
Câu 3: A, ECB là chế độ sách mã, tức là mã các khối độc lập
Câu 4: C, Không cần sinh khóa con vì không có vòng lặp
Câu 5: D, Tầng phiên kiểm soát hội thoại giữa các máy tính, nên thông thường không dùng mã ở tầng này.

THUẬT NGỮ TRONG BÀI

- DES - chuẩn mã dữ liệu là mã khối 64 bit, khóa 56 bit
- 3DES là cải tiến của DES, dùng lặp 3 lần DES với 2 hoặc 3 khóa
- AES - chuẩn mã nâng cao là mã khối 128 bit, khóa 128 bit thay thế DES.
- EBC: sách mã điện tử - mã riêng biệt từng khối mã với cùng một khóa
- CBC: dây chuyền mã khối - khối mã trước cộng nhị phân với khối bản tin sau rồi mã
- CFB: mã phản hồi ngược - bản tin như dòng bit cộng nhị phân đầu ra của mã, rồi phản hồi
- OFB: phản hồi đầu ra - đầu ra mã phản hồi và cộng nhị phân với dòng bit của bản tin

CÂU HỎI THƯỜNG GẶP

1. Nêu các đặc trưng của DES. Trong mỗi vòng nó thực hiện các thao tác gì trên dữ liệu?
2. Để tăng cường an ninh cho DES người ta đưa ra các giải pháp gì?
3. Nêu các đặc trưng của AES. Trong mỗi vòng nó thực hiện các thao tác gì trên dữ liệu?
7. Phân biệt mã khối và mã dòng
8. Nêu các chế độ thao tác trên mã khối
9. Mô tả thao tác mã dòng RC4
10. Có những vị trí nào đặt mã đối xứng trên mô hình mạng?
11. Chức năng nhiệm vụ của mã đầu cuối? Ưu, nhược điểm
12. Chức năng nhiệm vụ của mã kết nối? Vị trí đặt, ưu, nhược điểm

TRẢ LỜI CÂU HỎI THƯỜNG GẶP

1. Các đặc trưng của DES:
   - Mã khối 64 bit, khóa 56 bit, 16 vòng
   - Mỗi vòng chia 2 nửa, đảo hai nửa, xử lý nửa phải bằng cách hoán vị, mở rộng, cộng khóa vòng, thế nhờ các hộp box và lại hoán vị
   - Khó thám mã, cài đặt phần mềm, phần cứng
2. Ban đầu đưa ra giải pháp 3DES – mã 3 lần 2 khóa hoặc 3 khóa. Sau này xây dựng Chuẩn mã nâng cao để tăng tốc độ xử lý.

3. Chuẩn mã nâng cao AES: dùng sơ đồ Fiestel, khối dữ liệu 128 bit, khóa 128/192/256, vòng 9/11/13. Mỗi vòng thực hiện các thao tác: thế byte, dịch hàng, trộn cột, cộng khóa vòng. An toàn tương đương 3DES, tốc độ nhanh hơn.
4. Mã khối thao tác trên từng khối dữ liệu; Mã dòng thao tác trên từng bit hoặc từng byte. Mã dòng thường dùng trên các tầng mạng thấp.
5. Có 5 chế độ thao tác mã khối như DES và AES: sách mã điện tử ECB, dây mã khối dây chuyền mã khối CBC, mã phản hồi ngược CFB, phản hồi ngược đầu ra OFB và Bộ đếm CTR
6. Dùng mảng S gồm 256 số tự nhiên đầu tiên và mảng T lặp từ khóa K. Sau đó trộn S nhờ T và đảo S dựa vào chính nó.
7. Mã đầu cuối đặt ở các máy chủ và mã kết nối đặt ở mạng chuyển gói tin
8. Mã đầu cuối bảo vệ nội dung thông tin trên cả đường truyền và cung cấp danh tính
9. Mã kết nối bảo vệ luồng truyền khỏi việc theo dõi, có thể đặt ở nhiều tầng mạng, tầng càng cao, càng ít thông tin được mã hoá,

10.CÂU HỎI TỰ LUẬN

Câu 1 Nêu cấu trúc mã khối Fiestel?

Câu 2 Mô tả các đặc trưng của DES và nêu các thao tác trong một vòng của mã DES?

Câu 3 Mã hoá 3DES là gì? Ưu điểm và nhược điểm của 3DES?

Câu 4 Mô tả các đặc trưng của AES và nêu các thao tác trong một vòng của mã AES?

Câu 5 Nêu các chế độ thao tác mã khối, công dụng, ưu và nhược điểm của từng chế độ đó?

Câu 6 Có chế độ nào trong mã khối có thể được dùng cho mã dòng được không? Hãy mô tả cách dùng?

Câu 7 Mô tả thao tác của mã dòng RC4?

Câu 8 Nêu công dụng và nơi đặt mã đầu cuối?

Câu 9 Nêu công dụng và nơi đặt mã kết nối?

Câu 10 Theo bạn, khi hai người sử dụng dùng chung khóa và mã đối xứng trao đổi thông tin với nhau, có thể có biện pháp gì để chống từ chối và tạo chữ ký điện tử để tách vai trò hai người đó không?

BÀI TẬP TRẮC NGHIỆM

1. **Mã DES có khối dữ liệu, khóa (bit) và số vòng tương ứng như sau**
   a) 128, 56 và 16
   b) 64, 64 và 16
   c) 64, 56 và 16
   d) 64, 56 và 12
2. **Trong sơ đồ sinh khóa của DES từ khóa chính 56 bit sinh**
   a) 8 khóa con mỗi khóa 48 bit, mỗi khóa dùng cho 1 vòng
   b) 16 khóa con mỗi khóa 32 bit, mỗi khóa dùng cho 1 vòng
   c) 12 khóa con mỗi khóa 32 bit, mỗi khóa dùng cho 1 vòng
   d) 16 khóa con mỗi khóa 48 bit, mỗi khóa dùng cho 1 vòng
3. **Một vòng của DES không thực hiện thao tác nào**
   a) Hoán vị đầu và cuối ngược nhau
   b) Đổi vị trí hai nửa, nửa trái mới giữ nguyên và xử lý nửa phải

c) Không tách 2 nửa, xử lý cả khối 64 bit
d) Mở rộng nửa phải 32 bit thành 4 bit, cộng với khóa con, thế qua 8 hộp box

4. Trong thuật toán mã DES điều khẳng định nào là đúng

a) Tám hộp S cố định và hoán vị ban đầu phụ thuộc vào khóa
b) Tám hộp S phụ thuộc vào khóa và hoán vị ban đầu là cố định
c) Tám hộp S và hoán vị ban đầu phụ thuộc vào khóa
d) Tám hộp S và hoán vị ban đầu là cố định

5. Các chế độ làm việc của DES. Khẳng định nào sau đây là sai

a) ECB: khối mã trước quay vòng tác động vào khối mã sau
b) CBC: khối mã trước cộng nhị phân với khối bản tin sau rồi mã
c) CFB: bản tin như dòng bit cộng nhị phân đầu ra của mã, rồi phản hồi
d) OFB: đầu ra mã phản hồi và cộng nhị phân với dòng bit của bản tin

6. Với chuẩn mã nâng cao AES. điều khẳng định nào sau đây là đúng

a) 128 bit dữ liệu, 128 bit khóa và 11 vòng
b) 128 bit dữ liệu, 192 bit khóa và 13 vòng
c) 128 bit dữ liệu, 256 bit khóa và 9 vòng
d) 128 bit dữ liệu, 128/192/256 bit khóa và 9/11/13 vòng

7. Một vòng mã AES không thực hiện thao tác nào:

a) Khối dữ liệu 128 bit chia thành 16 byte bố trí thành 4 hàng, 4 cột, thực hiện phép thế byte
b) Tách thành 2 nửa, mỗi nửa 64 bit, đảo vị trí 2 nửa.
c) Chia dữ liệu thành 4 hàng, mỗi hàng dịch qua phải số vị trí tùy theo số thứ tự của hàng.
d) Trộn cột dựa vào phép nhân với một ma trận, rồi cộng với khóa con của vòng.

8. Số giả ngẫu nhiên được ứng dụng nhiều, điều gì sau đây là không đúng:

a) Làm nhãn đặc trưng cho bản tin
b) Tạo khóa phiên dùng chung giữa hai người sử dụng
c) Sinh khóa chung cộng cơ số 2 với dòng dữ liệu trong cơ chế mã và giải mã dòng.
d) Sinh ra số nguyên tố dùng làm khóa

9. Trong chế độ ECB, nếu có lỗi ở bản mã truyền đi, chỉ có khối bản rõ đó bị ảnh hưởng. Tuy nhiên trong chế độ CBC lỗi này sẽ lan truyền. Chẳng hạn lỗi sinh ra ở khối mã thứ nhất, khi đó nó sẽ tác động đến bao nhiêu khối mã?

a) Một khối mã ngay sau đó
b) Không tác động đến khối mã sau đó
c) Tác động đến mọi khối mã sau khối có lỗi
d) Chỉ tác động đến khối mã cuối cùng

10. Nếu lỗi sinh ra trong quá trình truyền một ký tự 8 bit của bản mã trong chế độ OFB, lỗi này lan truyền như thế nào:

a) Một khối mã ngay sau đó
b) Không tác động đến khối mã sau đó
c) Tác động đến mọi khối mã sau khối có lỗi
d) Chỉ tác động đến khối mã cuối cùng

11. Giả sử một người đề xuất cách sau đây để khẳng định các bạn gồm hai người đều sở hữu cùng một khóa mật. Bạn tạo một xâu bit ngẫu nhiên có độ dài bằng khóa, XOR nó với khóa và gửi kết quả trên kênh. Đối tác của bạn XOR block đến với cùng khóa của bạn và gửi lại. Bạn kiểm tra xem xâu bạn nhận có phải là dãy bit ngẫu nhiên gốc không, bạn sẽ kiểm chứng được đối tác của bạn có cùng khóa mật không, chứ bạn không bao giờ truyền khóa đi. Trong sơ đồ đó có khiếm khuyết nào?

a) Nếu biết xâu gửi đến và xâu trả lời, kẻ thám mã sẽ thực hiện phép XOR hai xâu và nhận được khóa

b) Xác thực tốt người nhận có cùng khóa mật với mình và an toàn

c) Không xác thực được người có cùng khóa

d) Chỉ cần thám mã được một trong 2 block truyền đi hoặc truyền lại là có thể biết được khóa mật

12. Mã đối xứng đầu cuối đặt ở máy người gửi và máy người nhận chia sẻ khóa dùng chung, làm nhiệm vụ bảo mật nội dung thông điệp trao đổi, không đặt ở tầng nào sau đây:

a) Tầng vật lý 1 và tầng liên kết dữ liệu 2

b) Tầng mạng 3

c) Tầng giao vận 4

d) Tầng trình diễn 6 và tầng ứng dụng 7

13. Mã kết nối bảo mật thông tin trên đường truyền, không đặt ở tầng nào sau đây:

a) Tầng vật lý 1

b) Tầng liên kết dữ liệu 2

c) Tầng giao vận 4

d) Tầng ứng dụng 7

BÀI TẬP ÔN TẬP

Câu 1: Cho P = (15 – 23) mod 52. Hỏi

A. P = 43; B. P = 42;

C. P = 44; D. P = 46.

Câu 2: Cho Q = 23^{-1} mod 206. Hỏi

A. Q = 8; B. Q = 11;

C. Q = 9; D. Q = 13.

Câu 3: Cho Q = 25^{-1} mod 274. Hỏi

A. Q = 10; B. Q = 12;

C. Q = 11; D. Q = 13.

Câu 4: Cho Q = 3^{10} mod 16. Hỏi

A. Q = 8; B. Q = 11;

C. Q = 7; D. Q = 9.

Câu 5: Cho X mod 25 = 5 và X mod 23 = 15 . Khi đó

A. X mod 25.23= 80;
B. X mod 25.23 = 130;
C. X mod 25.23 = 105;
D. X mod 25.23 = 155.

Câu 6: Tìm ra kết luận đúng về hàm Euler
A. Φ(9) = 7, Φ(17) = 16, Φ(33) = 18;
B. Φ(9) = 6, Φ(17) = 15, Φ(33) = 20;
D. Φ(9) = 7, Φ(17) = 15, Φ(33) = 18;
C. Φ(9) = 6, Φ(17) = 16, Φ(33) = 20;

Câu 7: Tìm ra kết luận đúng về hàm Euler:
A. Φ(10) = 4, Φ(23) = 20, Φ(39) = 22;
B. Φ(10) = 5, Φ(23) = 22, Φ(39) = 23;
C. Φ(10) = 4, Φ(23) = 22, Φ(39) = 24;
D. Φ(10) = 6, Φ(23) = 21, Φ(39) = 25.

Câu 8: Tìm ra kết luận sai:
A. 2^6 mod 12 = 1;
B. 4^{12} mod 21 = 1;
C. 8^{12} mod 21 = 1;
D. 5^4 mod 12 = 1;

Câu 9: Tìm ra kết luận sai:
A. 2^6 mod 7 = 1;
B. 3^4 mod 5 = 1;
C. 2^5 mod 11 = 1;
D. 5^{10} mod 11 = 1.

Câu 10: Tìm ra kết luận sai:
A. 2 là căn nguyên của 3;
B. 2 là căn nguyên của 4;
C. 2 là căn nguyên của 5;
D. 3 là căn nguyên của 5.

Câu 11: Tìm ra kết luận đúng:
A. 2 là căn nguyên của 6;
B. 2 là căn nguyên của 4;
C. 2 là căn nguyên của 5;
D. 3 là căn nguyên của 6;

Câu 12: Tìm kết luận đúng:
A. Log_2 5 mod 9 = 2;
B. Log_2 6 mod 9 = 3;
C. Log_2 7 mod 9 = 4;
D. Log_2 4 mod 9 = 5.