Chương 2: Mã khóa đối xứng và bảo mật thông điệp

BÀI 2: Mã đối xứng và bảo mật thông điệp

Tình huống dẫn nhập

- Cần che giấu nội dung thông tin không cho người không có thẩm quyền xem
- Tạo nên công cụ chuẩn để mọi người dễ dàng sử dụng
- Thay đổi thông điệp nhờ thuật toán chuẩn chung và thông tin bí mật chia sẻ giữa người gửi và người nhận
- Người nhận biến đổi ngược lại thông báo nhận được để có thông điệp gốc

Nội dung

- Các nguyên lý mã đối xứng
- Các thuật toán mã đối xứng
  - Chuẩn mã dữ liệu DES
  - Chuẩn mã nâng cao AES
- Các chế độ thao tác mã khối
- Mã dòng RC4
- Vị trí đặt các thiết bị mã

Mục tiêu

- Hiểu được các thành phần mã đối xứng, các khía cạnh tăng cường sức mạnh của mã
- Các nguyên lý mã khối đối xứng hiện đại: kết hợp nhiều vòng và nhiều kiểu thao tác
- Xử lý khối dữ liệu của DES và AES
- Các chế độ thao tác trên mã khối
- Nguyên lý mã dòng và bộ sinh số giả ngẫu nhiên
- Mã đầu cuối và mã kết nối trên mô hình mạng

2.1 Các khái niệm cơ bản

- Bản rõ là bản tin gốc.
- Bản mã là bản tin gốc đã được mã hoá.
- Mã là thuật toán chuyển bản rõ thành bản mã
- Khoá là thông tin dùng để mã hoá, chỉ có người gửi và người nhận biết.
- Mã hoá chuyển bản rõ thành bản mã
- Giải mã chuyển bản mã thành bản rõ.
- Mật mã nghiên cứu các nguyên lý và phương pháp mã hoá.
- Thám mã nghiên cứu các nguyên lý và phương pháp giải mã mà không biết khoá.
- Lý thuyết mã bao gồm cả mật mã và thám mã.

Các nguyên lý mã đối xứng

- Sơ đồ mã có 5 khái niệm:
  - Bản rõ
  - Thuật toán mã hóa
  - Khóa mật
  - Bản mã
  - Thuật toán giải mã
- An ninh phụ thuộc vào bảo mật khóa, chứ không phải bảo mật thuật toán
- *Câu hỏi:Tại sao lại cho rằng thuật toán mọi người đều biết?*
- *Trả lời: Vì ta phải chuẩn hóa các thuật toán dùng chung trên các giao thức trên mạng, và số thuật toán dùng được cũng không nhiều, nên luôn giả thiết là phổ cập*

Các nguyên lý mã đối xứng

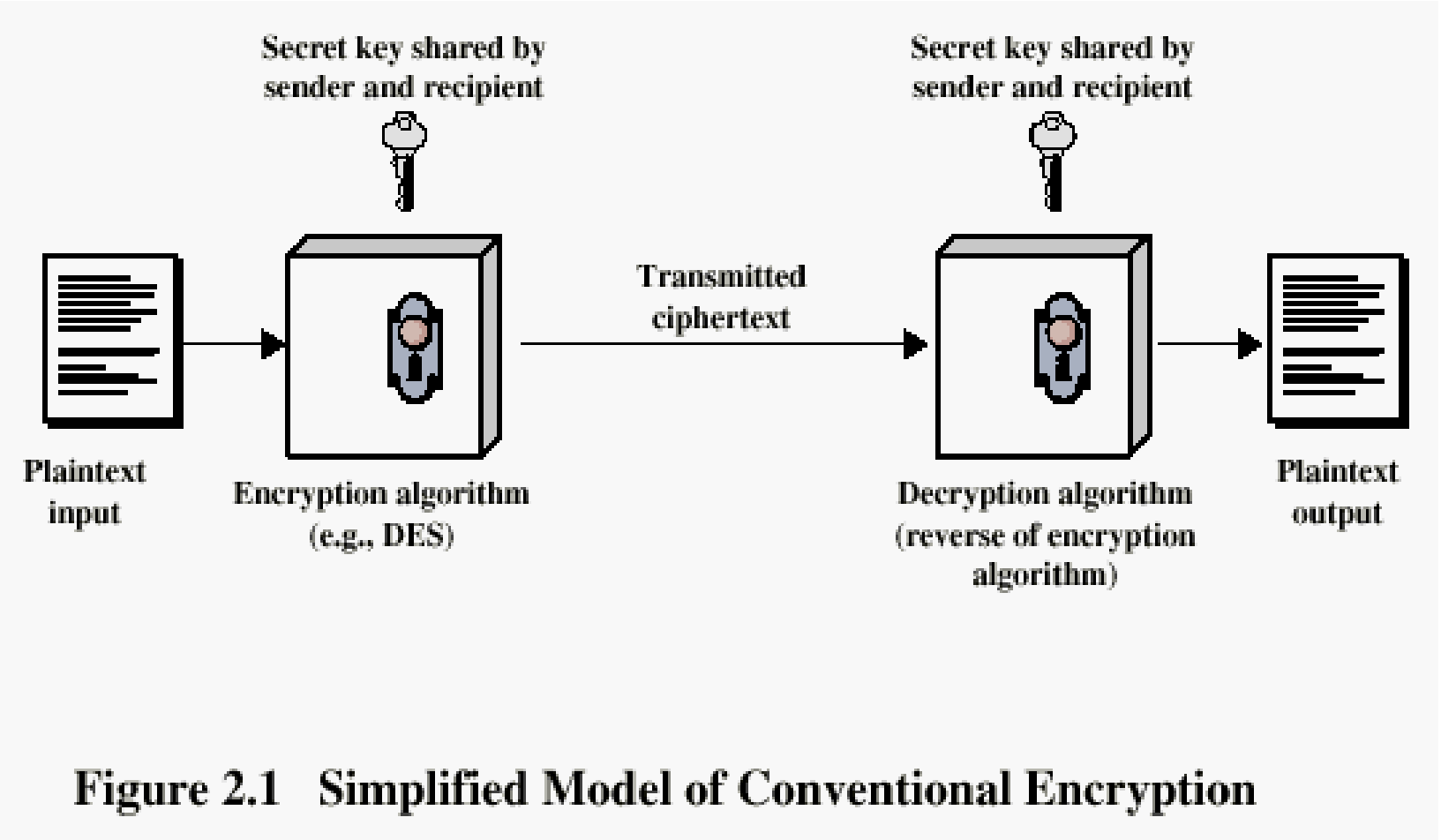


Figure 2.1 Simplified Model of Conventional Encryption

Mã hóa

- Được phân loại theo ba kích thước độc lập sau:
  - Kiểu thao tác để chuyển bản rõ thành bản mã
    - phép thế,
    - thay đổi vị trí hay
    - tích của chúng.
  - Số khóa được sử dụng
    - Đối xứng (khóa duy nhất)
    - Không đối xứng (hai khóa, hoặc mã khóa công khai)
  - Và cách mà ở đó bản rõ được xử lý
    - khối hay
    - dòng bít

Mã thế cổ điển

- Ở đây các chữ của bản rõ được thay bằng các chữ khác hoặc các số hoặc các ký hiệu.
- Hoặc nếu xem bản rõ như một dãy bít, thì phép thế thay các mẫu bít bản rõ bằng các mẫu bít bản mã
- Mã thế được biết sớm nhất, sáng tạo bởi Julius Ceasar
- Đầu tiên được sử dụng trong quân sự
- Thay mỗi chữ bằng chữ thứ ba tiếp theo
- Ví dụ:

```
meet me after the toga party
PHHW  PH  DIWHU  WKH  WRJD  SDUWB
```

Thời gian trung bình để tìm khóa theo phương pháp vét cạn

- Luôn có thể thử từng khoá
- Phần lớn công sức của các tấn công đều tỷ lệ thuận với kích thước khoá.
- Giả thiết là biết hoặc nhận biết được bản rõ.

Kích thước khóa (bits)	Số khóa có thể có	Thời gian với tốc độ giải mã 10^6 ký tự/μs
32	$2^{32} = 4.3 \times 10^9$	2.15 mili giây
56	$2^{56} = 7.2 \times 10^{16}$	10 giờ
128	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{18} năm
168	$2^{168} = 3.7 \times 10^{50}$	5.9×10^{30} năm

Cấu trúc mã Feistel

- Mọi thuật toán mã khối đối xứng, kể cả DES đều có cấu trúc được mô tả đầu tiên bởi Horst Feistel của IBM vào năm 1973
- Sau này trở thành chuẩn chung cho các mã khối đối xứng hiện đại.
- Các mã cụ thể theo sơ đồ mạng Fesitel phụ thuộc vào việc lựa chọn các tham số và các đặc trưng thiết kế sau (xem trang sau):

Cấu trúc mã Feistel

- **Kích thước khối**: kích thước khối càng lớn an toàn càng cao
- **Kích thước khóa**: kích thước khóa càng lớn an toàn càng cao
- **Số vòng**: nhiều vòng lặp sẽ tăng cường anh ninh
- **Thuật toán sinh khóa con:** độ phức tạp càng lớn sẽ dẫn đến độ khó thám mã càng cao.
- **Mã hoá / giải mã nhanh**: tốc độ thực hiện thuật toán mã hóa trở nên rất quan trọng

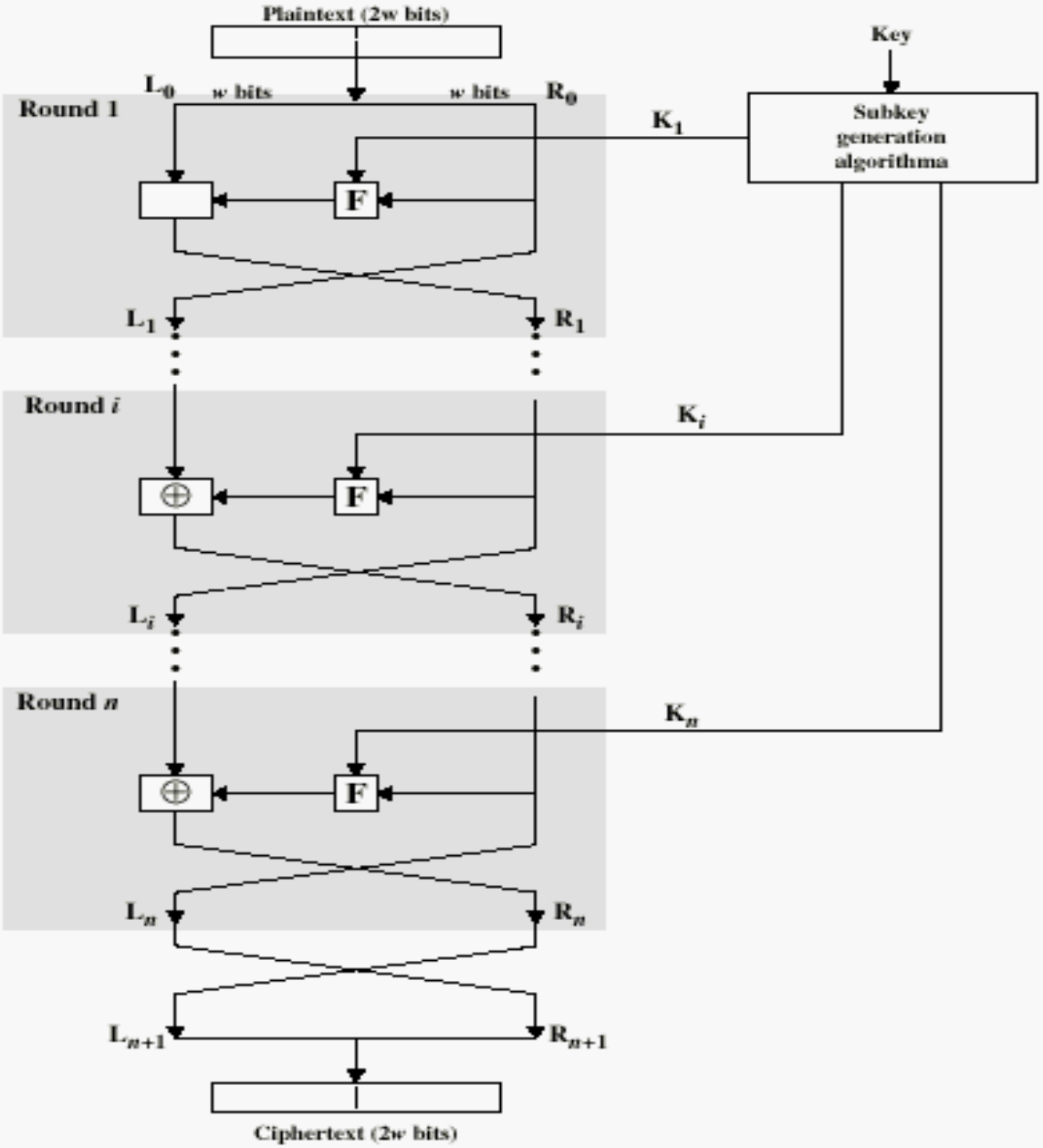


Figure 2.2 Classical Feistel Network

2.3 Chuẩn mã dữ liệu
Data Encryption Standard (DES)

- Mã khối sử dụng rộng rãi nhất trên thế giới
- Được đưa ra năm 1977 bởi NBS – văn phòng chuẩn Quốc gia (bây giờ là NIST - Viện chuẩn và công nghệ Quốc gia)
- Mã khối dữ liệu 64 bít và dùng khoá dài 56 bít
- Được sử dụng rộng rãi
- Được tranh luận kỹ về mặt an toàn

Đặc trưng của DES

- Kế thừa mã Lucifer, được lãnh đạo bởi Fiestel
- Năm 1973 NBS yêu cầu đề xuất chuẩn mã Quốc gia
- IBM đề nghị bản sửa đổi Lucifer, sau này gọi là Chuẩn mã dữ liệu – DES
- Sử dụng khối dữ liệu 64 bít và khoá 56 bít
- Có hoán vị đầu, cuối và xử lý qua 16 vòng
- Sinh 16 khóa con cho mỗi vòng
- Sau đó tiếp tục phát triển như mã thương mại

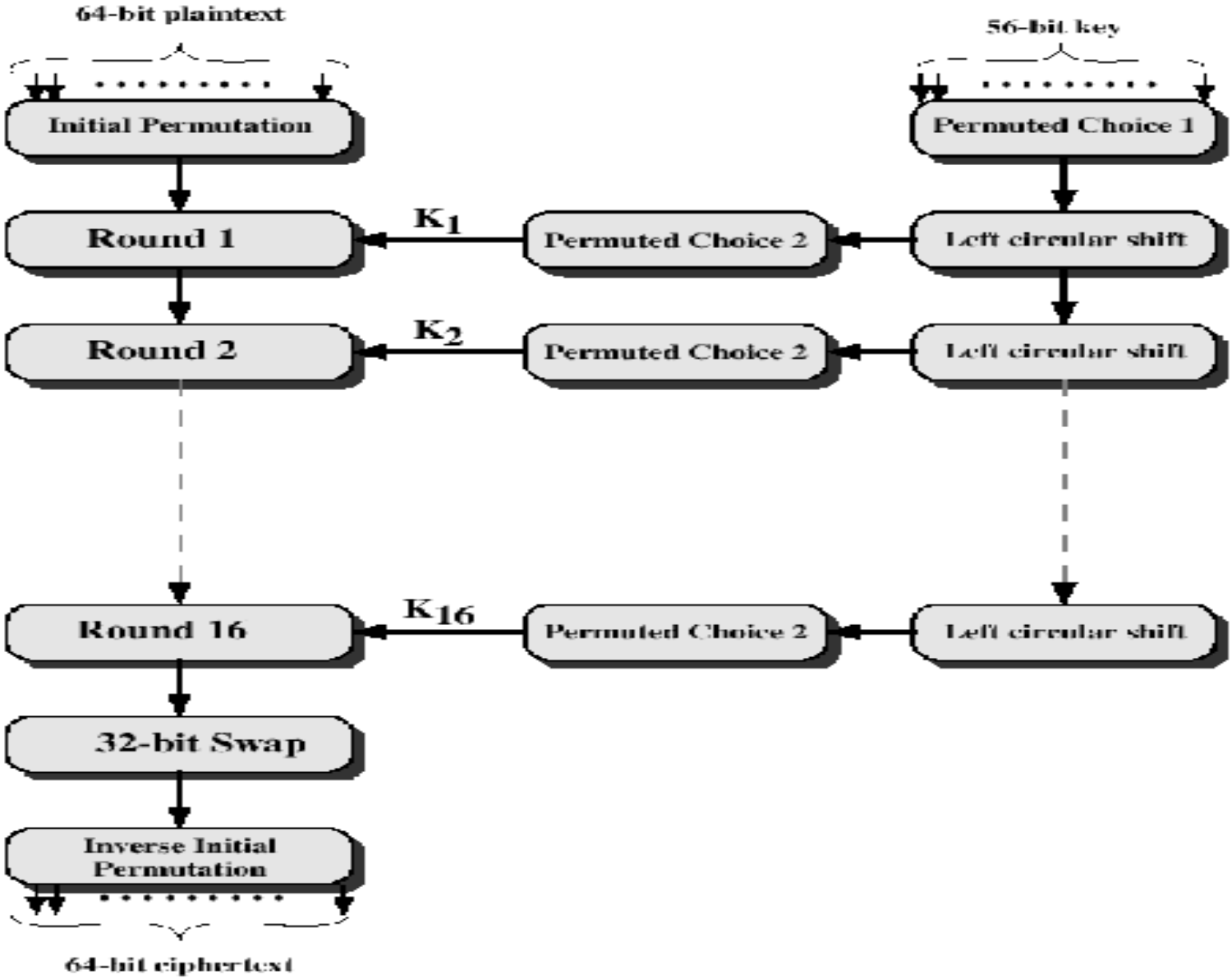


Figure 2.3 General Depiction of DES Encryption Algorithm

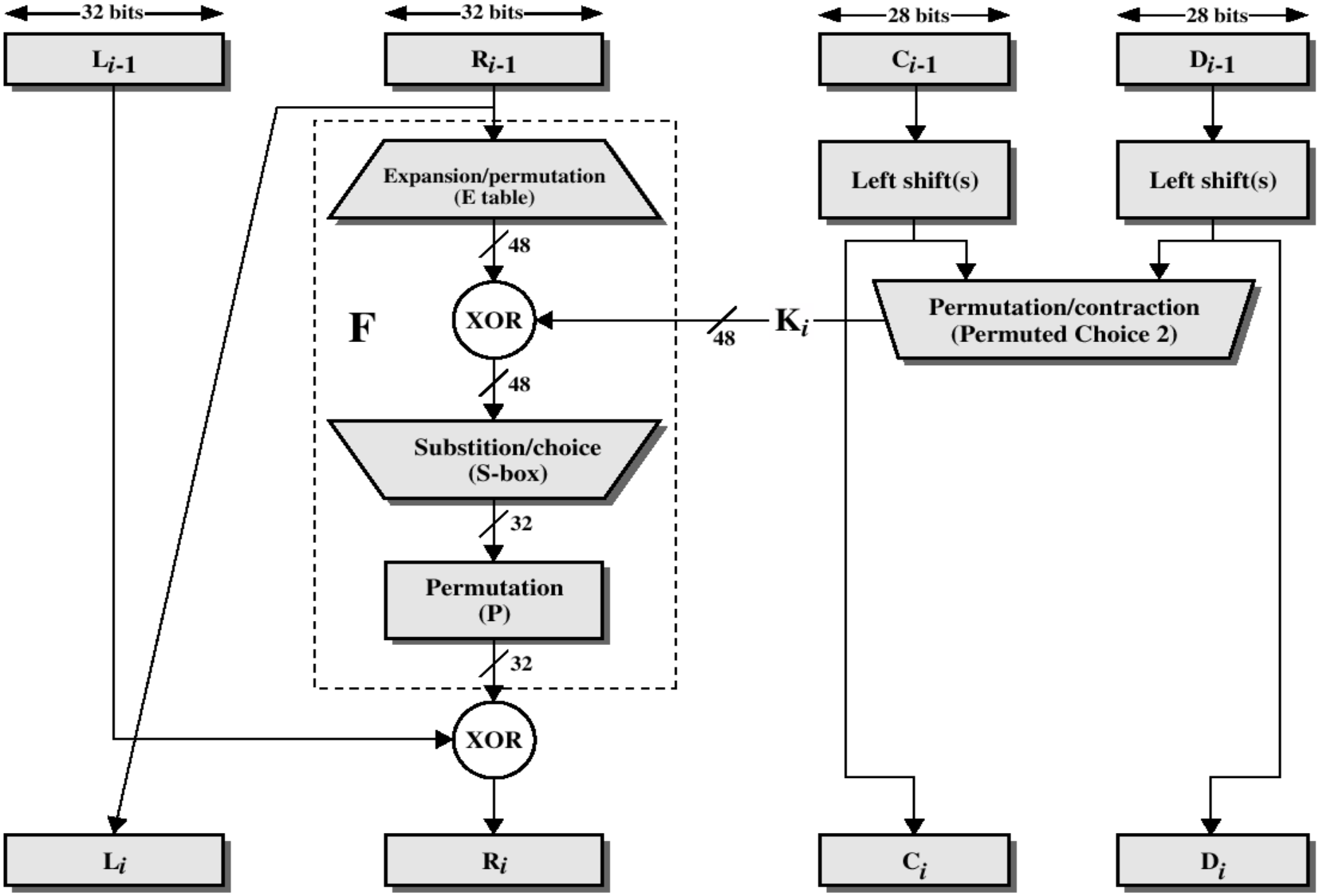
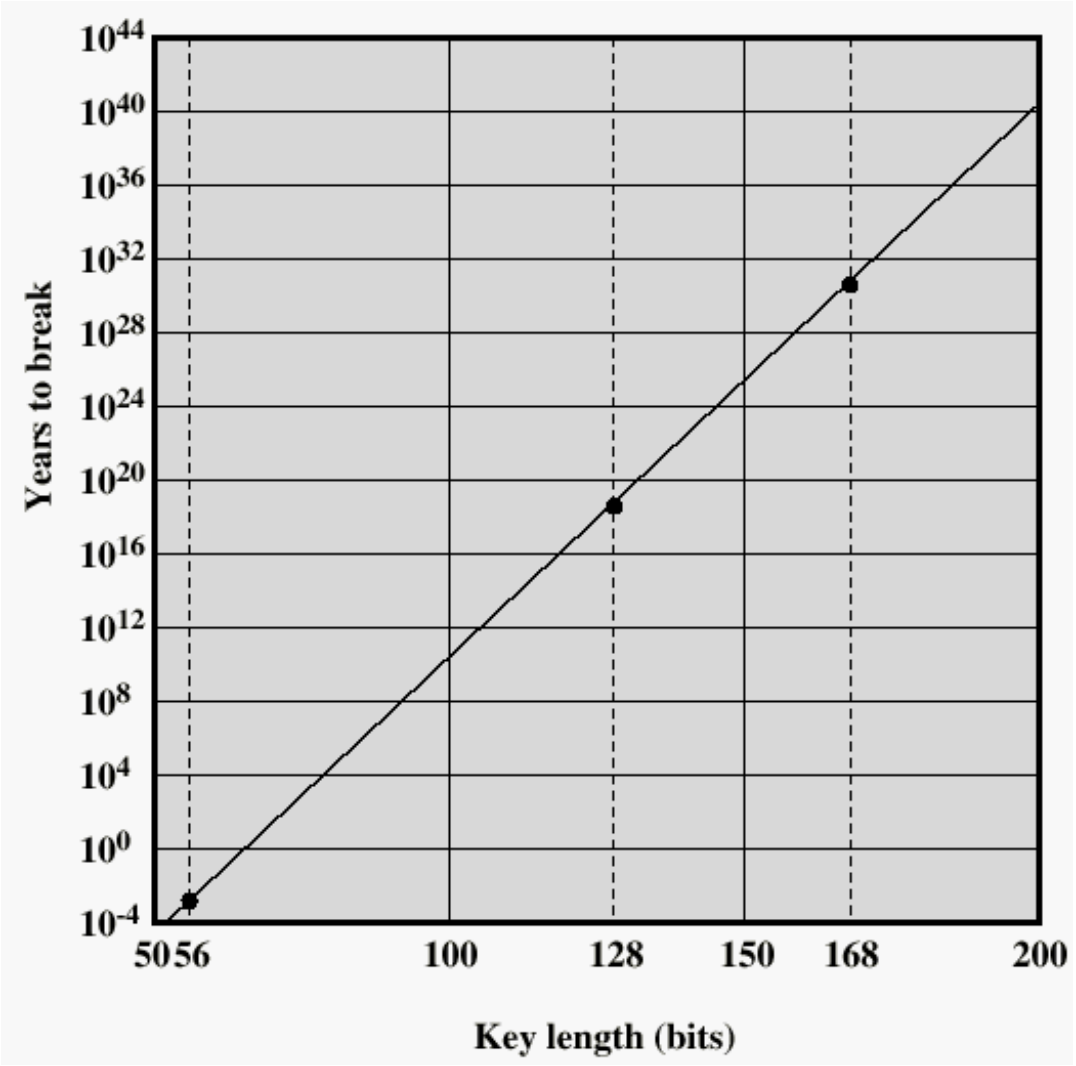


Figure 2.4 Single Round of DES Algorithm

Cấu tạo một vòng của DES

- Cấu tạo một vòng của DES
  - Sử dụng hai nửa 32 bít trái và 32 bít phải
  - Như đối với mọi mã Fiestel có thể biểu diễn
- $L_i = R_{i-1}$
- $R_i = L_{i-1}$ xor F(R_{i-1}, K_i)
  - F lấy 32 bít nửa phải R và 48 bít khoá con và
    - mở rộng R thành 48 bít nhờ hoán vị E
    - Cộng vào với khoá con
    - Qua 8 S-box để nhận được kết quả 32 bít
    - Đảo lần cuối sử dụng hoán vị 32 bít P

Thời gian bẻ mã phụ thuộc vào độ dài khóa (Tốc độ giải mã 10^6 ký tự/μs)



Triple DES với 2 khoá

- Cần sử dụng 3 mã, vậy có thể dùng 3 khoá khác nhau
- Nhưng có thể sử dụng 2 khoá theo trình tự:

  E-D-E

$$C = E_{K1}(D_{K2}(E_{K1}(P)))$$

  - Về mặt an toàn mã và giải mã tương đương nhau
  - Nếu K1 = K2 thì tương đương làm việc với 1 DES
  - Chuẩn hoá trong ANSI X9.17 & ISO8732
  - Chưa thấy tấn công thực tế.

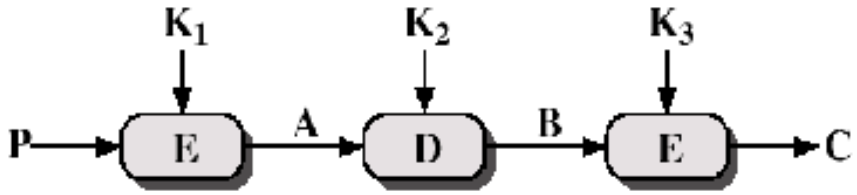
Triple DES với 3 khoá

- Mặc dù chưa có tấn công thực tế nhưng Triple DES với 2 khoá có một số chỉ định
- Cần phải sử dụng DES 3 khoá để tránh điều đó

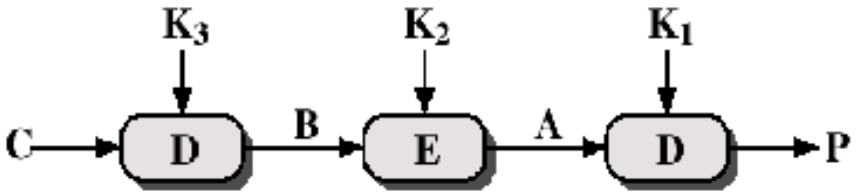
$$C = E_{K3}(D_{K2}(E_{K1}(P)))$$

- Được chấp nhận bởi một số ứng dụng trên Internet: PGP, S/MIME
- *Câu hỏi: Tại sao không phải là 2DES mà là 3DES?*
- *Trả lời: Vì 2DES gặp phải tấn công trung gian. Đoán bản rõ, mò cặp khóa cho đến khi đạt được: mã bản rõ = giải mã bản mã*

Triple DEA–Lặp 3 lần thuật toán DEA



(a) Encryption



(b) Decryption

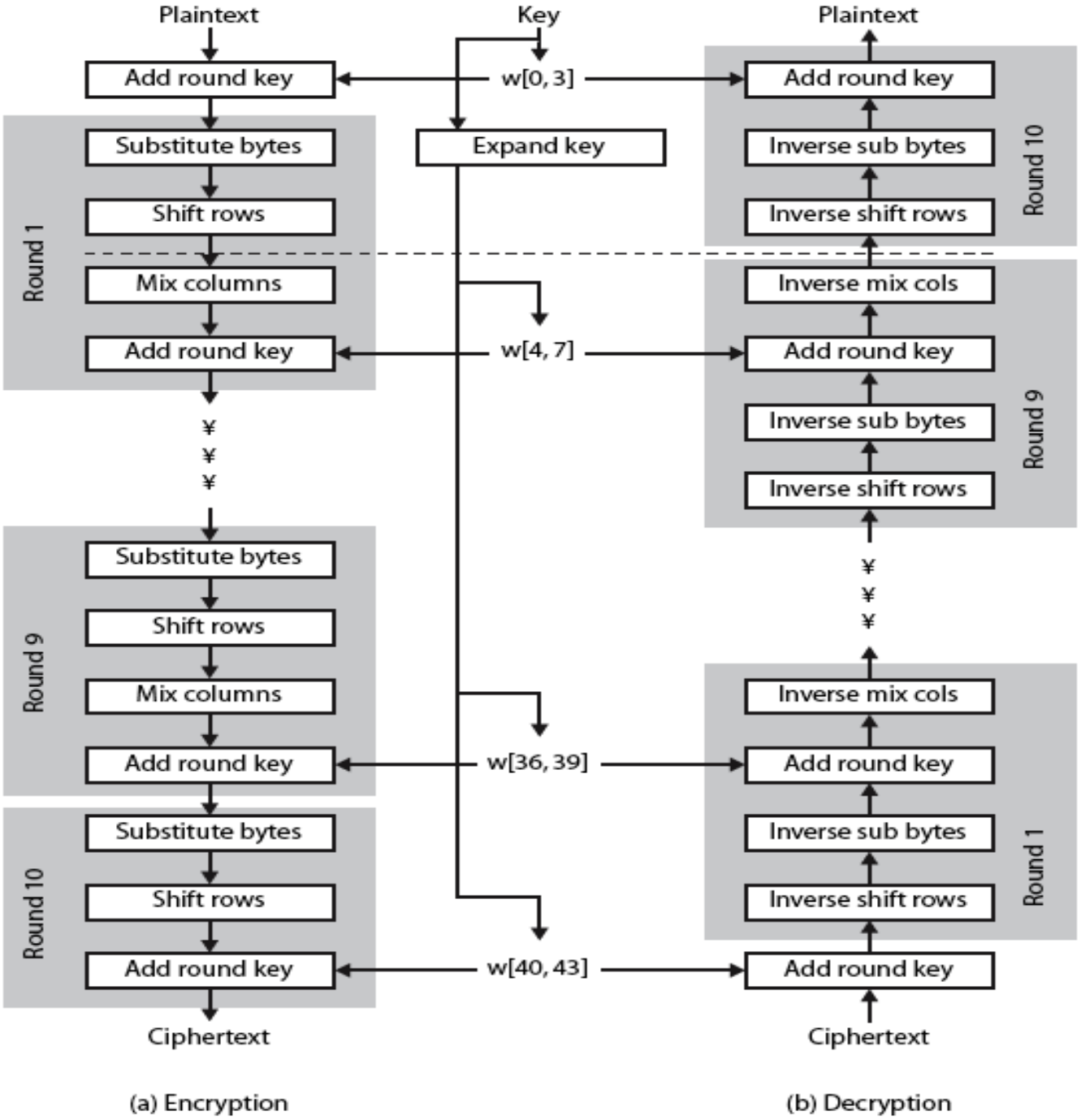
Figure 2.6 Triple DEA

2.4 Chuẩn mã nâng cao AES

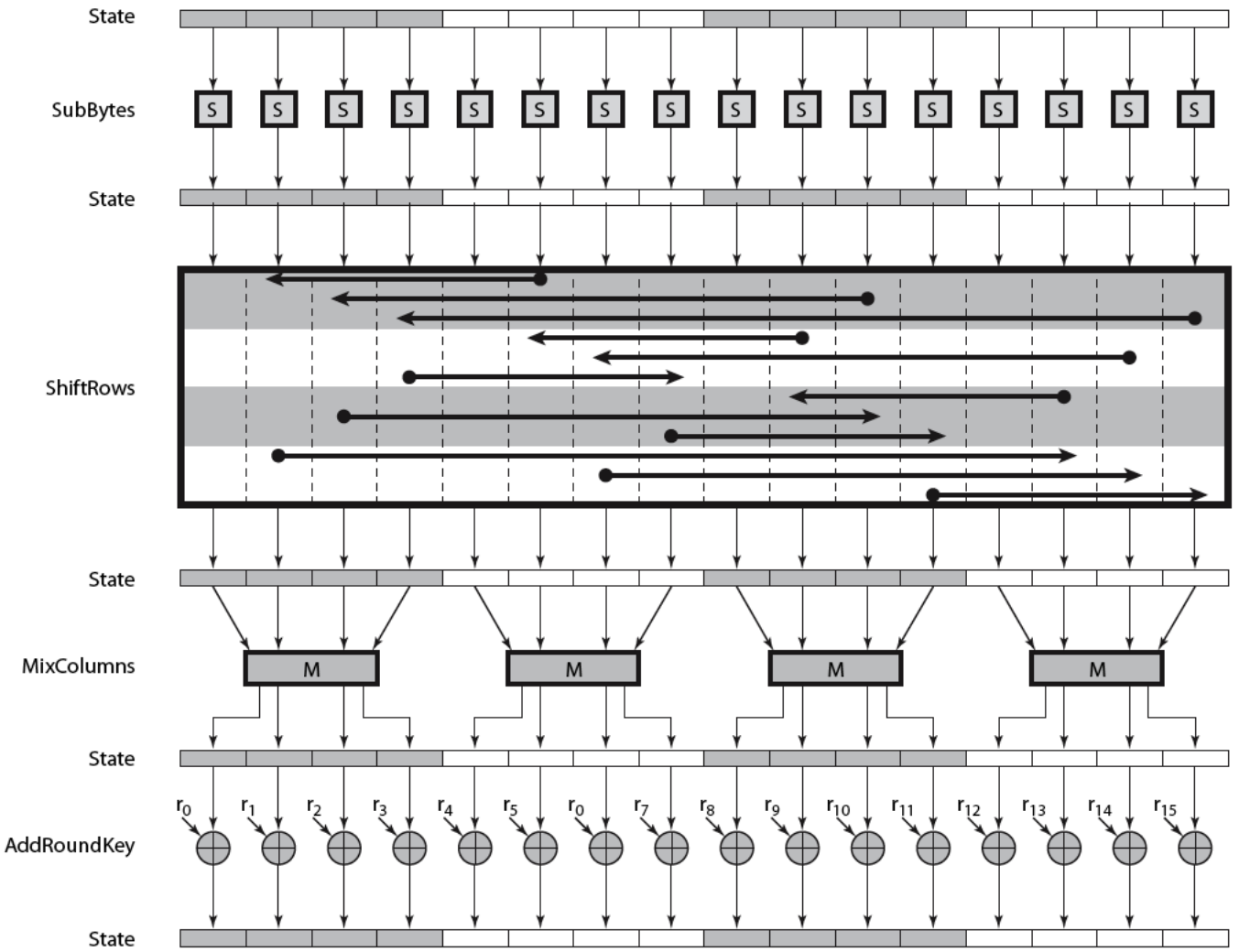
- Dựa trên mã Rijndael, thiết kế bởi Rijmen – Daemen ở Bỉ
- Có 128/192/256 bit khoá và 128 bit dữ liệu
- Lặp hơi khác với Fiestel
  - Chia dữ liệu thành 4 nhóm – 4 byte
  - Thao tác trên cả khối mỗi vòng
- Thiết kế để:
  - chống lại các tấn công đã biết
  - tốc độ và nén mã trên nhiều CPU
  - Đơn giản trong thiết kế

Cấu tạo chuẩn mã nâng cao AES

- Xử lý dữ liệu như 4 nhóm của 4 byte (trạng thái)
- Khoá mở rộng thành mảng các từ
- Có 9/11/13 vòng, trong đó mỗi vòng gồm
  - Phép thế byte (1 S box cho 1 byte)
  - Dịch hàng (hoán vị byte giữa nhóm/cột)
  - Trộn cột (sử dụng nhân ma trận của các cột)
  - Cộng khoá vòng (XOR trạng thái với dữ liệu khoá)
- Dữ liệu khoá được sử dụng để sinh ra các khóa con cho mỗi vòng
- Mọi phép toán được kết hợp trong XOR và bảng tra nên rất nhanh và hiệu quả


Plaintext
Key
Plaintext
Add round key
w[0, 3]
Add round key
Substitute bytes
Expand key
Inverse sub bytes
Round 10
Shift rows
Inverse shift rows
Round 1
Mix columns
Inverse mix cols
Add round key
w[4, 7]
Add round key
Inverse sub bytes
Round 9
Inverse shift rows
¥
¥
¥
Substitute bytes
Shift rows
Inverse mix cols
Round 9
Mix columns
Add round key
w[36, 39]
Add round key
Substitute bytes
Inverse sub bytes
Round 10
Shift rows
Inverse shift rows
Round 1
Add round key
w[40, 43]
Add round key
Ciphertext
Ciphertext
(a) Encryption
(b) Decryption

AES Round


State
SubBytes
S
State
ShiftRows
State
MixColumns
M
State
AddRoundKey
r0 r1 r2 r3 r4 r5 r0 r7 r8 r9 r10 r11 r12 r13 r14 r15
State

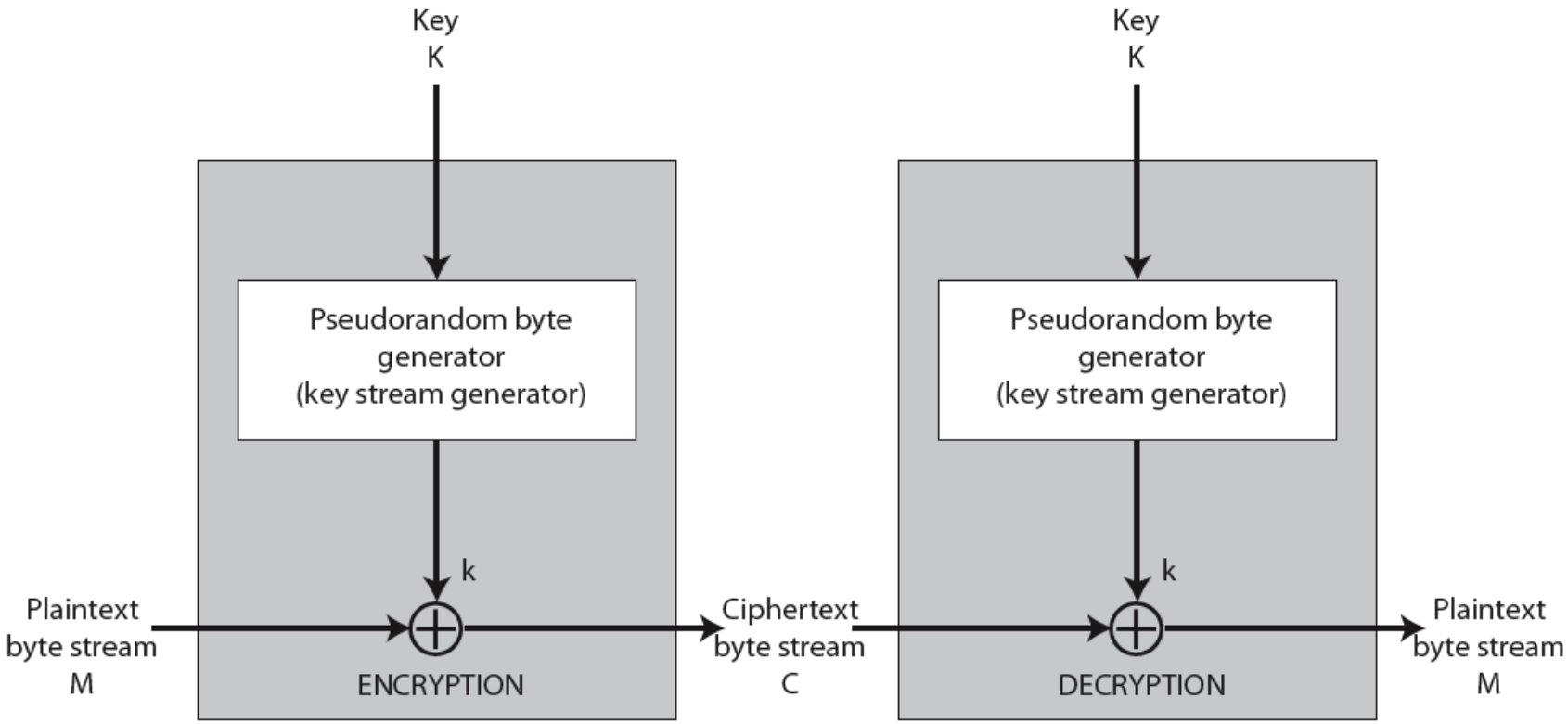
2.5 Mã dòng

- Xử lý mẩu tin lần lượt theo từng bit
- Thông thường có khoá dòng (giả) ngẫu nhiên
- Kết hợp XOR với bản rõ theo từng bit
- Ngẫu nhiên với khoá dòng sẽ xoá bỏ hoàn toàn các phân tích thống kê của mẩu tin, xử lý mẩu tin từng bit một như dòng bit

$$C_i = M_i \text{ XOR } StreamKey_i$$

- Rất đơn giản, nhưng khoá không được sử dụng lại
- *Câu hỏi: `StreamKey` được tạo ra như thế nào?*
- *Trả lời: được sinh ra theo cơ chế tạo ra dãy số giả ngẫu nhiên nhờ mồi đầu vào là khóa mật chia sẻ.*

Cấu trúc mã dòng



Mã dòng RC4

- Mã đăng ký bản quyền của RSADSI
- Thiết kế bởi Ronald Rivest, đơn giản nhưng hiệu quả
- Có nhiều cỡ khoá và mã bit dòng
- Được sử dụng rộng rãi (Web SSL/TLS, không dây WEP – Wired Equivalent Privacy)
- Khoá 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 khoá RC4

- Bắt đầu từ mảng S với biên độ: 0..255
- Sử dụng khoá để xáo trộn đều thực sự
- S tạo trạng thái trong của mã

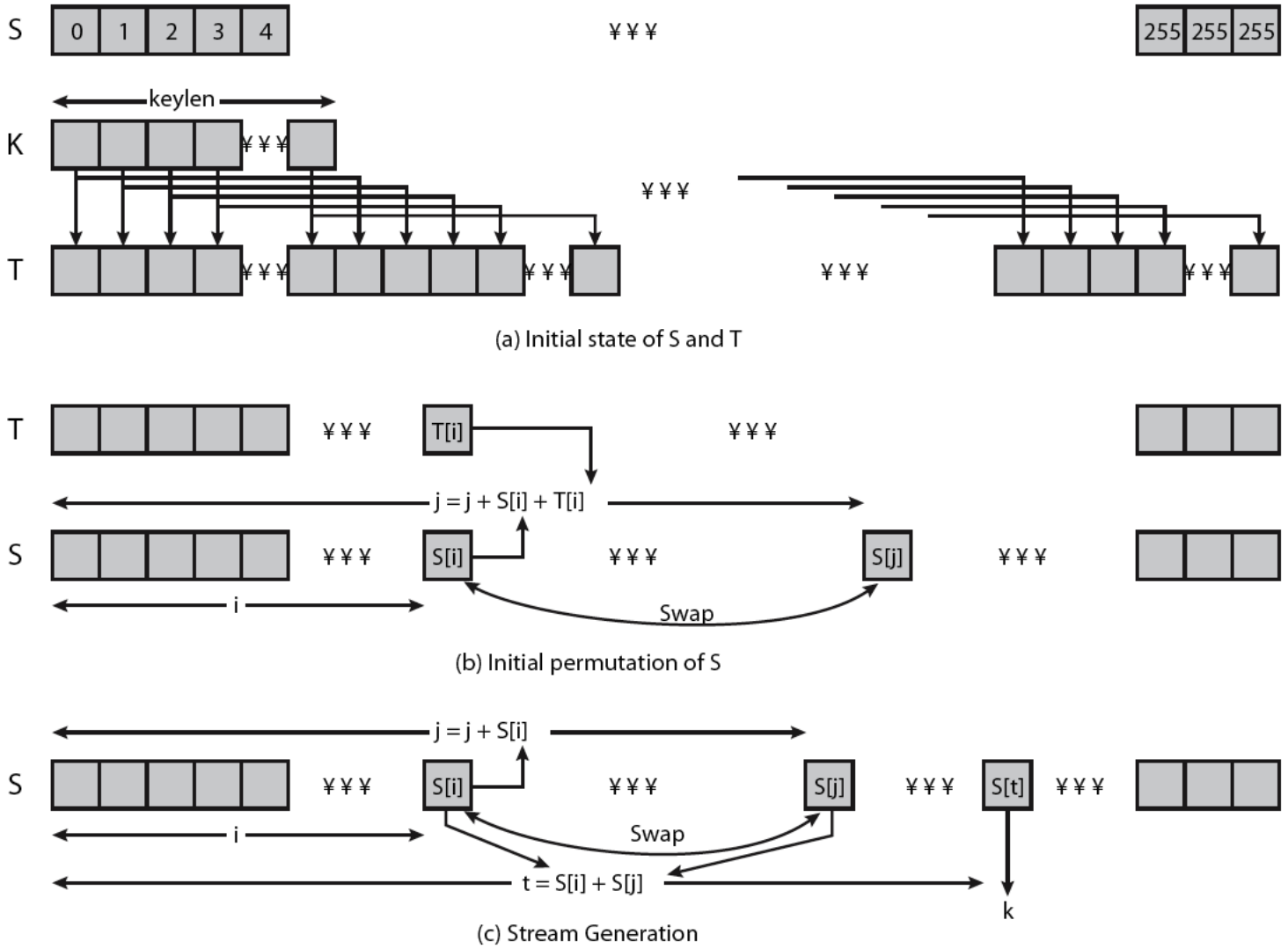
```
for i = 0 to 255 do
   S[i] = i
   T[i] = K[i mod keylen]
j = 0
for i = 0 to 255 do
   j = (j + S[i] + T[i]) (mod 256)
   swap (S[i], S[j])
```

Mã RC4

- Mã tiếp tục trộn các giá trị của mảng
- Tổng của các cặp trộn chọn giá trị khoá dòng từ hoán vị
- XOR S[t] (k) 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]
```

Tổng quan RC4



2.5 Các kiểu thao tác mã khối

- Mã khối mã các block có kích thước cố định
- Chẳng hạn DES mã các block 64 bít với khoá 56 bít
- Cần phải có cách áp dụng vào thực tế vì các thông tin cần mã có kích thước tùy ý.
- Có 4 cách được định nghĩa cho DES theo chuẩn ANSI

ANSI X3.106-1983 Modes of Use

- Bây giờ có 5 cách cho DES và AES
- Có kiểu khối và dòng

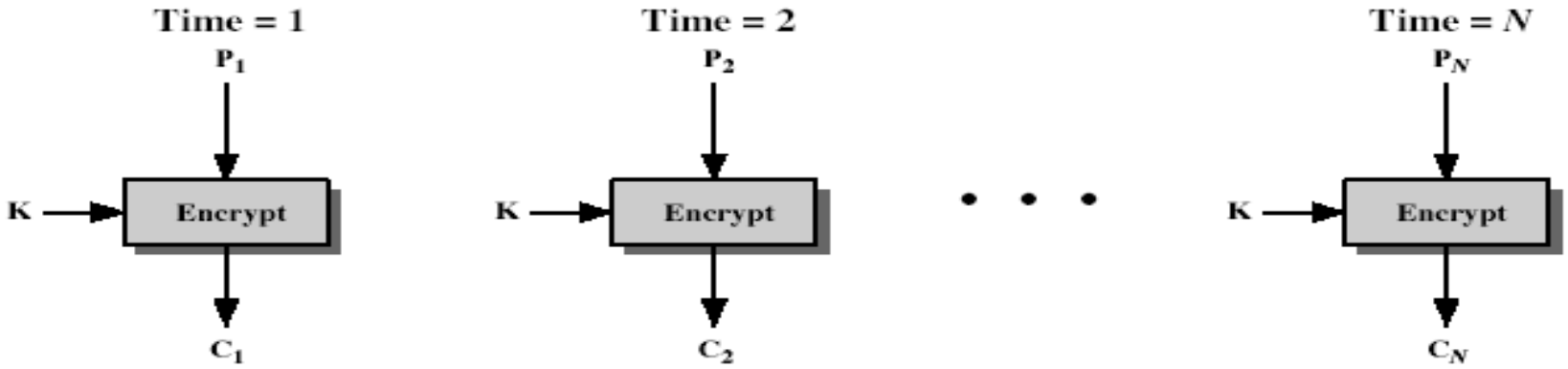
Sách mật mã điện tử (ECB)

- 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

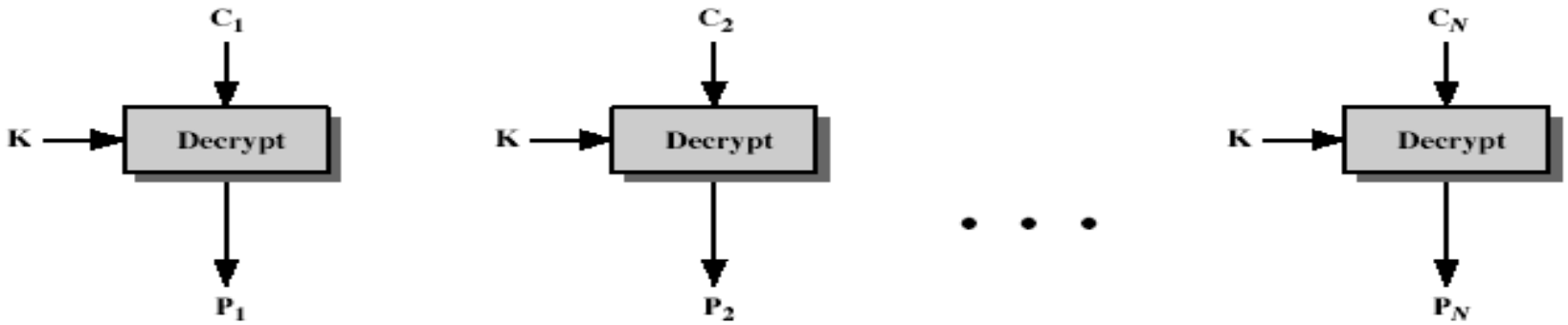
$$C_i = DES_{K1}(P_i)$$

- Khi dùng: truyền an toàn từng khối riêng lẻ
- *Câu hỏi: tại sao gọi là sách điện tử? Lặp trên bản rõ có tạo nên lặp trên bản mã không?*
- *Trả lời: vì giống như khi đã biết khóa, ta mã và giải mã từng khối bằng cách tra sách mã*

Sách mật mã điện tử (ECB)



(a) Encryption



(b) Decryption

Dây chuyền mã khối (CBC)

- Các mẫu tin được chia thành các khối, sẽ khắc phục việc lặp trên dữ liệu tạo ra việc lặp trên mã
- 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

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

$$C_{-1} = IV$$

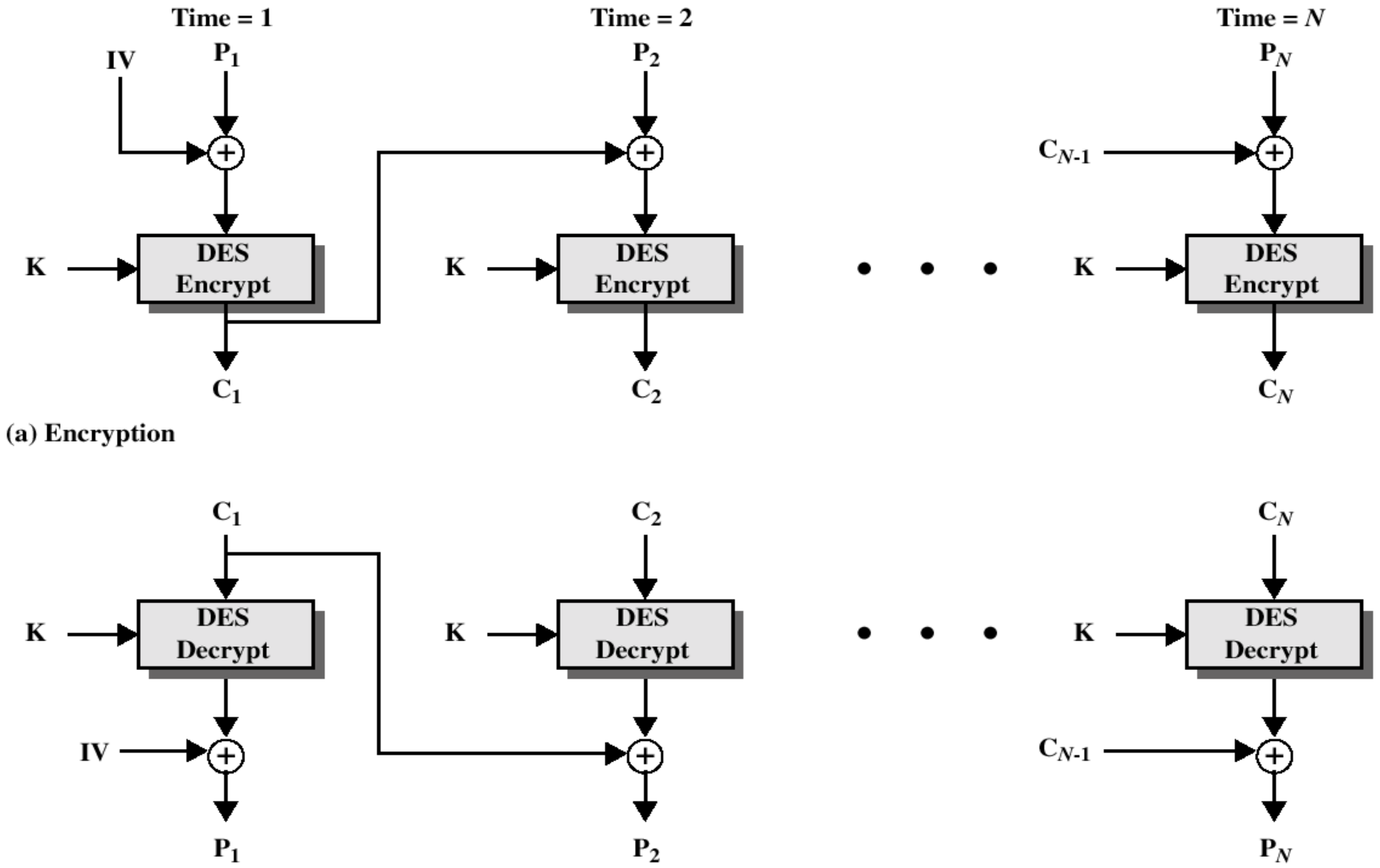


Figure 2.7 Cipher Block Chaining (CBC) Mode

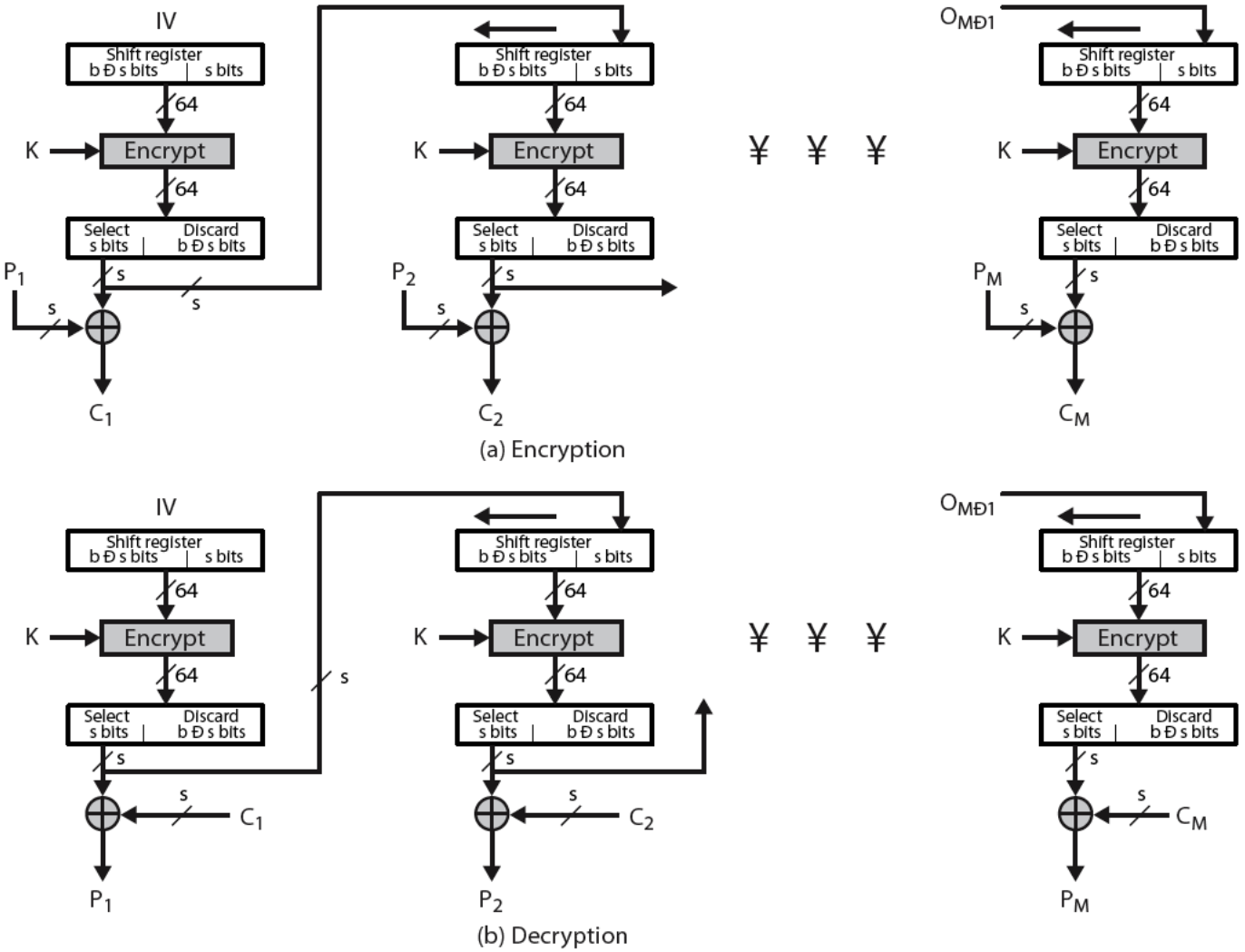
Phản hồi ngược đầu ra (OFB)

- Mẩu tin xem như dòng bit
- Đầu ra của mã được bổ sung cho mẩu tin
- Đầu ra do đó là phản hồi, do đó có tên như vậy
- Phản hồi ngược là độc lập đối với bản tin
- Có thể được tính trước

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

- Được dùng cho mã dòng trên các kênh âm thanh
- *Câu hỏi: tại sao dùng như mã dòng được?*
- *Trả lời: vì ta có thể thỏa thuận chọn trước số s bit tùy ý cho một lần mã, giống như trong mã dòng.*

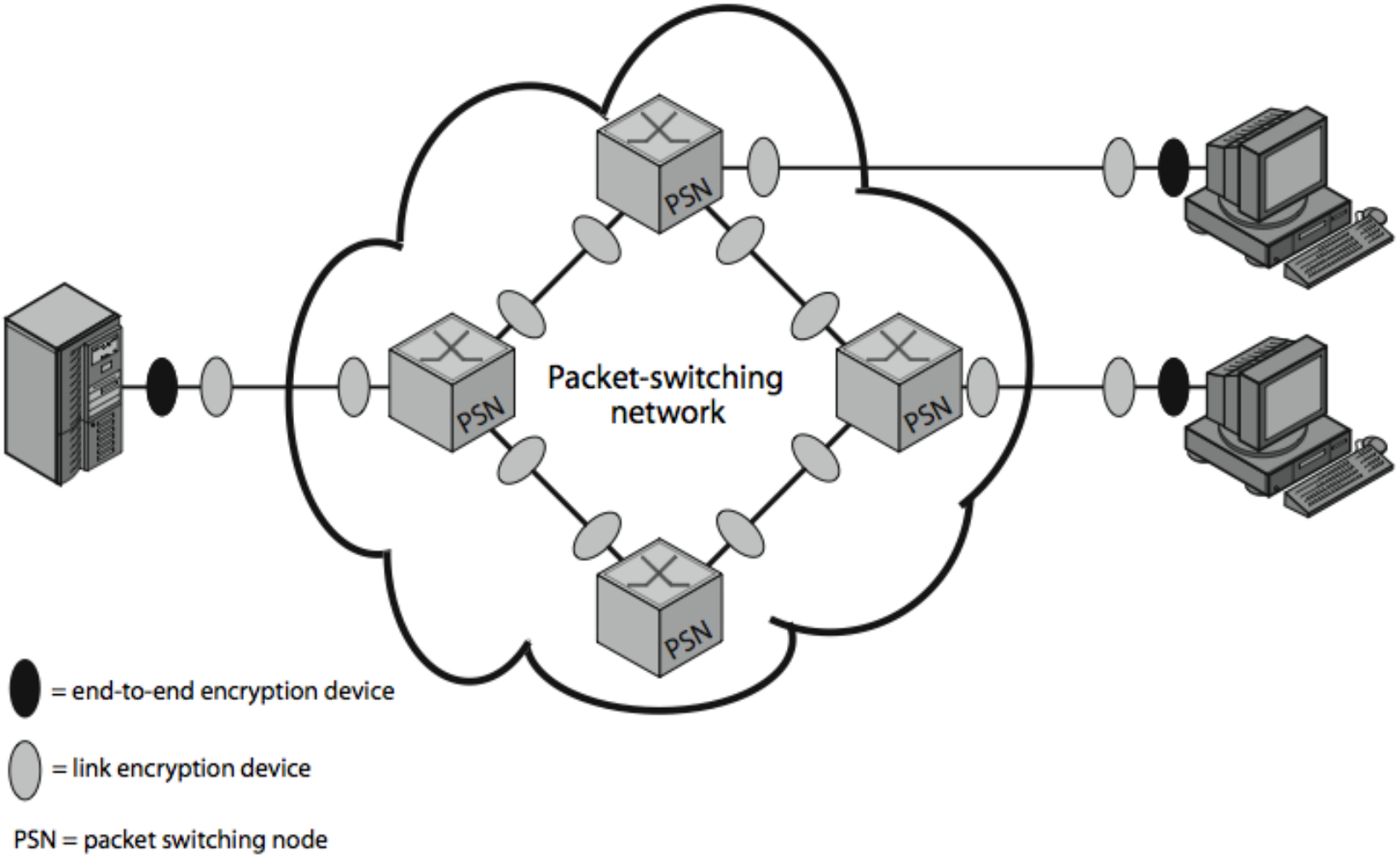
Phản hồi ngược đầu ra (OFB)



2.6 Chỗ đặt mã

- Có hai phương pháp chính xác định chỗ đặt mã trên mô hình mạng
- Mã kết nối (Link Encription)
  - 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 khoá
- Mã đầu cuối (End to end Encription) AES là mã mới thay thế
  - Mã xảy ra giữa điểm gốc và điểm đích
  - Cần thiết bị tại mỗi đầu cuối và khoá chia sẻ

Chỗ đặt mã


PSN
PSN
PSN
PSN
Packet-switching network
= end-to-end encryption device
= link encryption device
PSN = packet switching node

Chỗ đặt mã

- 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
- Lý tưởng là muốn bí mật cả hai
- Mã đầu cuối bảo vệ nội dung thông tin trên cả đường truyền và cung cấp danh tính
- Mã kết nối bảo vệ luồng truyền khỏi việc theo dõi.

Chỗ đặt mã

- Có thể đặt mã ở nhiều tầng khác nhau trong mô hình OSI
- Mã kết nối thực hiện ở tầng 1 hoặc 2
- Mã đầu cuối có thể thực hiện ở tầng 3, 4, 6, 7 (tuỳ sự tương thích của kiến trúc)
- Dịch chuyển đến tầng càng cao, càng ít thông tin được mã hoá, nhưng càng an toàn hơn tuy nhiên phức tạp hơn với nhiều đối tượng và khoá hơn.
- *Câu hỏi: tại sao lại có câu khẳng định trên?*
- *Trả lời*: *Vì tại giao thức ở mỗi tầng, cần bổ sung thông tin tham số cho đầu mỗi gói tin ở dạng tường minh để trao đổi giữa bên gửi và bên nhận cùng tầng*

Tóm tắt

- Khái niệm mã đối xứng
- 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

Câu hỏi trắc nghiệm 1

- Câu 1: Mục nào không phải là thành phần của Khóa đối xứng
  A. Một khóa chia sẻ người gửi và người nhận
  B. Hai thuật toán mã hóa và giải mã
  C. Bản rõ và bản mã
  D. Thuật toán nén văn bản
- Câu 2: Nói chung coi độ khó thám mã không phụ thuộc vào
  A. Độ phức tạp của thuật toán mã hóa
  B. Độ lớn của không gian khóa
  C. Che giấu thuật toán mã hóa
  D. Che giấu khóa mật

Câu hỏi trắc nghiệm 2

- Câu 3: Thao tác xử lý dữ liệu sau nào không dùng trong mã đối xứng:
  A. Dùng phép thế xâu ký tự bản rõ bằng xâu ký tự bản mã
  B. Dùng phép hoán vị đảo chỗ các ký tự bản rõ tạo ra bản mã
  C. Kết hợp cả hai phép toán trên và có thể xử lý nhiều vòng
  D. Che giấu dữ liệu trong môi trường khác
- Câu 4: 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 hỏi trắc nghiệm 3

- **Câu 5. 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 6. 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 hỏi trắc nghiệm 4

- **Câu 7. 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 ngẫu nhiên
- **Câu 8. 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
  - D, Khóa, thuật toán mã hóa, giải mã, bản rõ bản mã đều là các thành phần của mã đối xứng, nén không dùng đến.
- Câu 2
  - C, luôn coi thuật toán mã hoá là mọi người đều biết
- Câu 3
  - D, Che giấu dữ liệu không phải là thao tác mã hóa, mà là giấu sự tồn tại của dữ liệu mật trong môi trường nào đó
- Câu 4
  - C, trong 16 vòng, mỗi vòng dùng một khóa con riêng

Đáp án câu hỏi trắc nghiệm - tiếp

- Câu 5
  - C, mỗi vòng xử lý cả khối 128 bit, tức là cả 4 nhóm - mỗi nhóm 4 byte
- Câu 6
  - A, ECB là chế độ sách mã, tức là mã các khối độc lập
- Câu 7
  - C, Không cần sinh khóa con vì không có vòng lặp
- Câu 8
  - D, Tầng phiên kiểm soát hội thoại giữa các máy tính, nên thông thường không dùng mã ở tầng này.

Glossary - Từ điển thuật ngữ

- Bản rõ là bản tin gốc.
- Bản mã là bản tin gốc đã được mã hoá.
- Mã là thuật toán chuyển bản rõ thành bản mã
- Khoá là thông tin dùng để mã hoá, chỉ có người gửi và người nhận biết.
- Mã hoá chuyển bản rõ thành bản mã
- Giải mã chuyển bản mã thành bản rõ.
- Mật mã nghiên cứu các nguyên lý và phương pháp mã hoá.
- Thám mã nghiên cứu các nguyên lý và phương pháp giải mã mà không biết khoá.
- Lý thuyết mã bao gồm cả mật mã và thám mã

Glossary - Từ điển thuật ngữ - tiếp

- Mã đối xứng là mã ở đó hai người nhận và gửi chia sẻ chung một khóa.
- 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

FAQ – Câu hỏi thường gặp

1. Nêu sự khác biệt giữa mã thế và mã hoán vị
2. Thế nào là mã đối xứng mạnh. Nó cần có các tính chất gì?
3. Mô tả kiến trúc mã đối xứng Fiestel
4. Nêu các đặc trưng của DES. Trong mỗi vòng nó thực hiện các thao tác gì trên dữ liệu?
5. Để tăng cường an ninh cho DES người ta đưa ra các giải pháp gì?
6. Nêu các đặc trưng của AES. Trong mỗi vòng nó thực hiện các thao tác gì trên dữ liệu?

FAQ – Câu hỏi thường gặp (tiếp)

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:

1. Mã thế là thay mỗi ký tự bản rõ bằng 1 xâu bản mã; mã hoán vị đảo thứ tự các ký tự trong bản rõ để tạo nên bản mã.
2. Mã đối xứng mạnh cần có các tính chất sau:

   - Kích thước khối dữ liệu mã và khóa tương đối lớn: cân bằng với tốc độ
   - Thuật toán mã hóa mạnh: lặp nhiều vòng, mỗi vòng kết hợp hoán vị với thế; thuật toán sinh khóa con phức tạp cho mỗi vòng. Bản mã có tính chất khoếch tán và tác dụng đồng loạt để khó thám mã
3. Kiến trúc mã khối Fiestel

   - Lặp nhiều vòng, sinh khóa con riêng cho từng vòng
   - Quá trinh giải mã ngược lại với quá trình mã hóa
   - Cân đối việc tăng kích thước khối, khóa và số vòng để đảm bảo an ninh với tốc độ thực hiện
4. 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

Trả lời câu hỏi – (tiếp)

5. 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.
6. 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.
7. 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.
8. 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
9. 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.
10. Mã đầu cuối đặt ở các máy chủ và mã kết nối đặt ở mạng chuyển gói tin
11. Mã đầu cuối bảo vệ nội dung thông tin trên cả đường truyền và cung cấp danh tính
12. 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,