CHƯƠNG 7

HỆ MẬT KHỐI - BLOCK CIPHERS

Nội dung

- Khái niệm cơ bản về hệ mật mã khối

Nội dung

- Khái niệm cơ bản về hệ mật mã khối
- Phương pháp thực hiện mã hóa khối

Nội dung

- Khái niệm cơ bản về hệ mật mã khối
- Phương pháp thực hiện mã hóa khối
- Tích các hệ mật mã

Nội dung

- Khái niệm cơ bản về hệ mật mã khối
- Phương pháp thực hiện mã hóa khối
- Tích các hệ mật mã
- Hệ mật mã Feistel

Nội dung

- Khái niệm cơ bản về hệ mật mã khối
- Phương pháp thực hiện mã hóa khối
- Tích các hệ mật mã
- Hệ mật mã Feistel
- Data Encryption Standard (DES)

Định nghĩa

Mật mã khối n-bit *là hàm* $E : V_n \times \mathcal{K} \to V_n$, *sao cho mỗi khóa* $K \in \mathcal{K}$ *có một hàm khả nghịch (hay hàm mã hóa khóa* K*) từ* V_n *đến* V_n, *ký hiệu* $E_K(P)$. *Hàm ngược của nó, ký hiệu* $D_K(C)$, *được gọi là hàm giải mã. Với* P, C *lần lượt ký hiệu là tin gốc và tin được mã hóa.*

Định nghĩa

Mật mã khối n-bit *là hàm* $E : V_n \times \mathcal{K} \to V_n$*, sao cho mỗi khóa* $K \in \mathcal{K}$ *có một hàm khả nghịch (hay hàm mã hóa khóa* K*) từ* V_n *đến* V_n*, ký hiệu* $E_K(P)$*. Hàm ngược của nó, ký hiệu* $D_K(C)$*, được gọi là hàm giải mã. Với* P*,* C *lần lượt ký hiệu là tin gốc và tin được mã hóa.*

Kích thước khối n là tương đối lớn, thông thường n$\geq$64

Phương pháp thực hiện mã hóa khối

- Electronic codebook (ECB)

Phương pháp thực hiện mã hóa khối

- Electronic codebook (ECB)
- Cipher-block chaining (CBC)

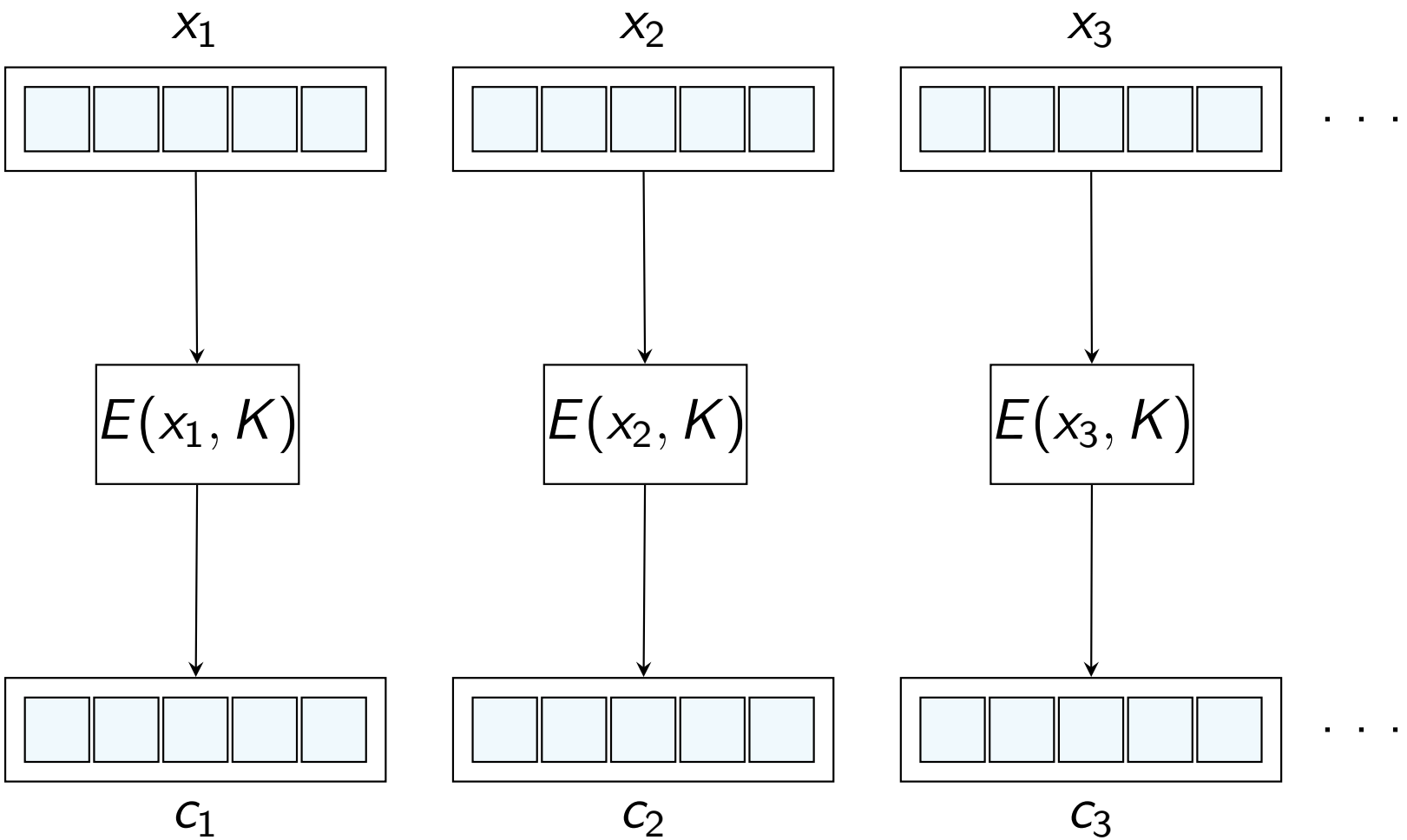
Phương pháp thực hiện mã hóa khối

- Electronic codebook (ECB)
- Cipher-block chaining (CBC)
- Cipher feedback

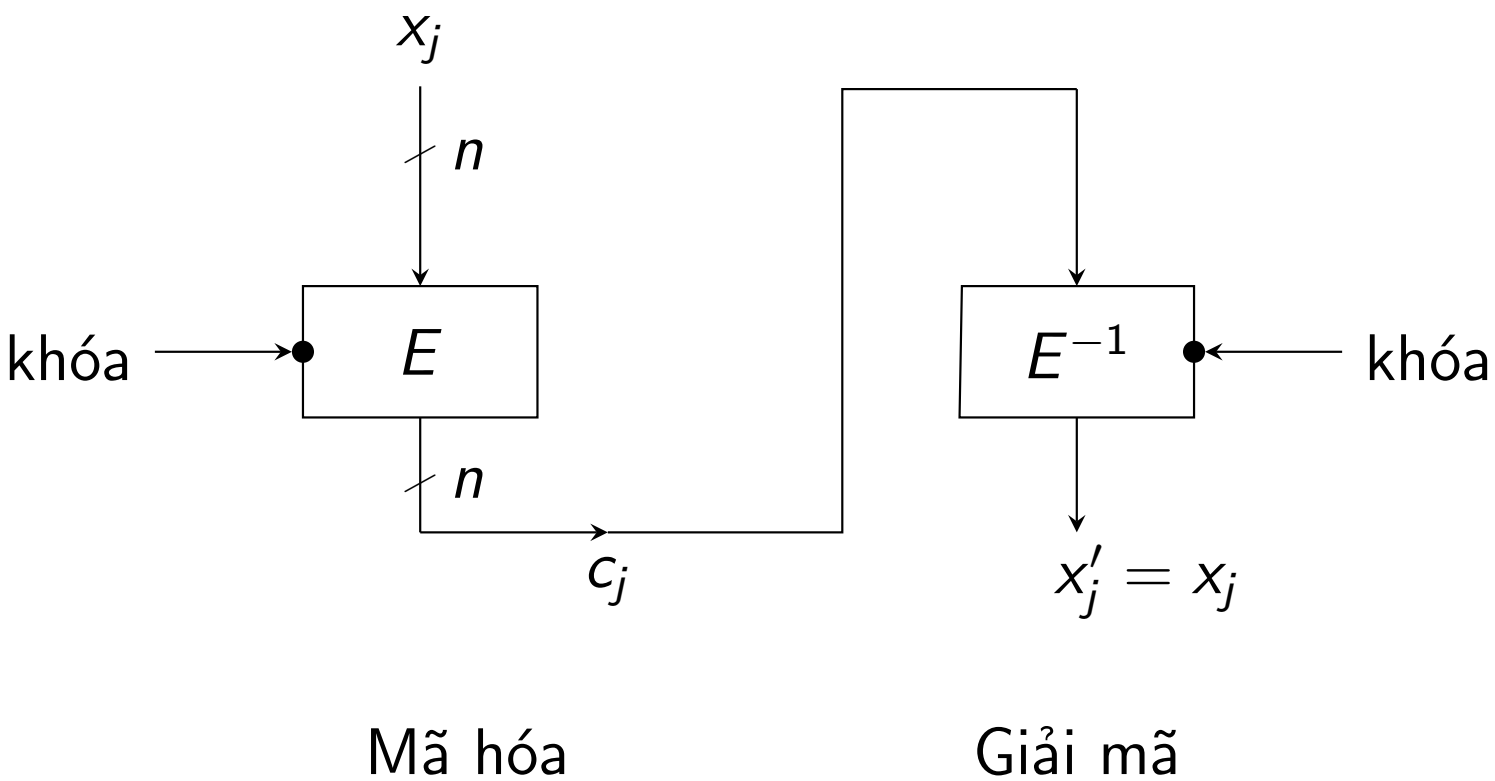
Phương pháp thực hiện mã hóa khối

- Electronic codebook (ECB)
- Cipher-block chaining (CBC)
- Cipher feedback
- Output feedback

Electronic codebook (ECB)



Electronic codebook (ECB)



Điểm chú ý về ECB

- Các khối được mã hóa độc lập nên việc chèn mã độc ở khối nào đó thì không ảnh hưởng đến giải mã ở khối khác

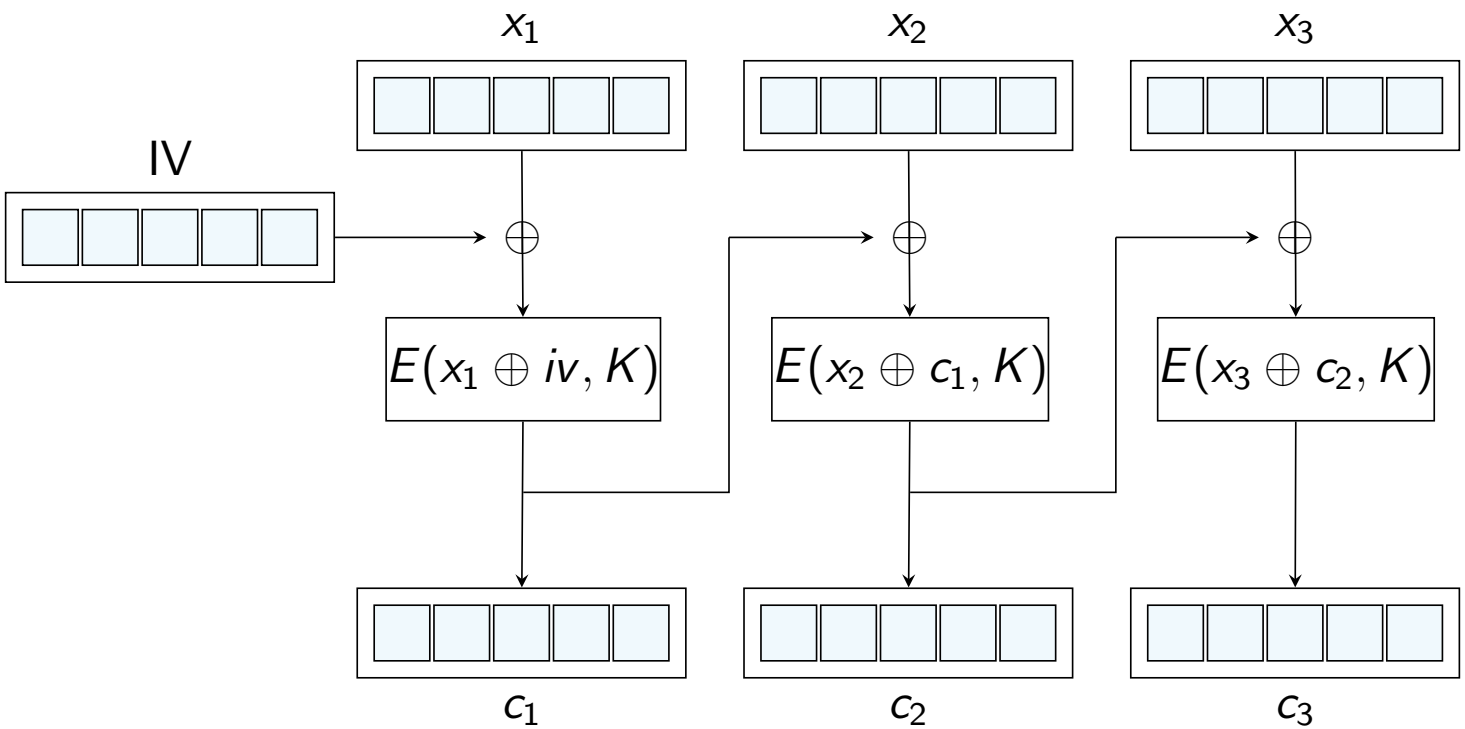
Điểm chú ý về ECB

- Các khối được mã hóa độc lập nên việc chèn mã độc ở khối nào đó thì không ảnh hưởng đến giải mã ở khối khác
- Có thể tính song song

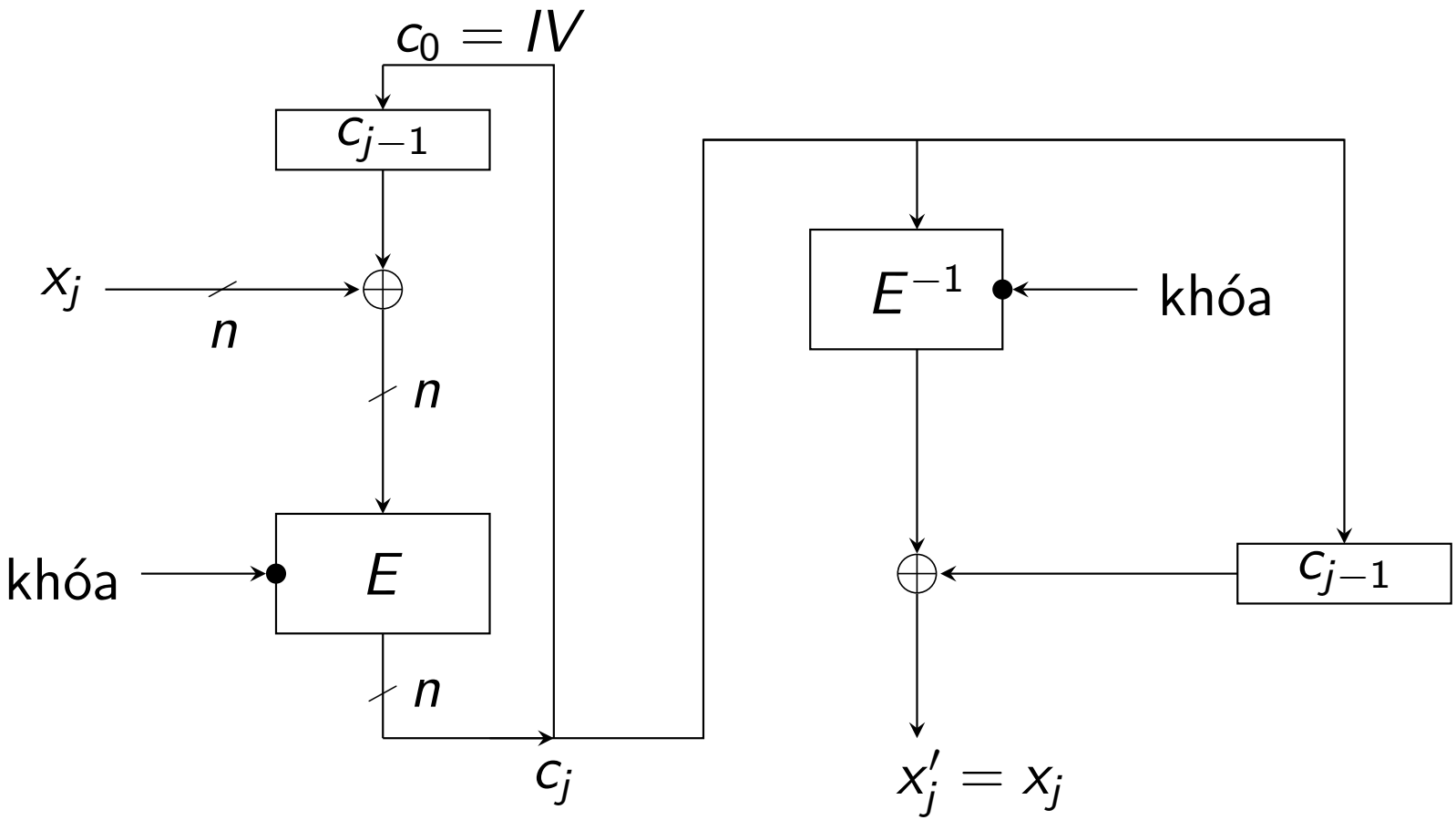
Điểm chú ý về ECB

- Các khối được mã hóa độc lập nên việc chèn mã độc ở khối nào đó thì không ảnh hưởng đến giải mã ở khối khác
- Có thể tính song song
- Mã hóa, giải mã các khối mẫu giống nhau sẽ cho kết quả giống nhau. Kẻ địch dễ thám mã dựa vào đặc tính này vì vậy ECB không được xem xét cho trường hợp dữ liệu kích thước lớn hơn 1 khối với cùng khóa. Khi có nhiều khối thì thường mỗi khối đã được cho thêm các bit ngẫu nhiên để tăng độ an toàn.

Cipher-block chaining (CBC)



Cipher-block chaining (CBC)



Điểm chú ý về CBC

- Mã hóa và giải mã của CBC cần khóa và IV (initialization vector) .

Điểm chú ý về CBC

- Mã hóa và giải mã của CBC cần khóa và IV (initialization vector) .
- Mã hóa giải mã các khối phụ thuộc khối trước đó do đó không thể hoán đổi vị trí các khối.

Điểm chú ý về CBC

- Mã hóa và giải mã của CBC cần khóa và IV (initialization vector) .
- Mã hóa giải mã các khối phụ thuộc khối trước đó do đó không thể hoán đổi vị trí các khối.
- Kẻ địch có thể làm thay đổi các bit trong x_{j+1} khi giải mã nếu sửa bit trong c_j.

Điểm chú ý về CBC

- Mã hóa và giải mã của CBC cần khóa và IV (initialization vector) .
- Mã hóa giải mã các khối phụ thuộc khối trước đó do đó không thể hoán đổi vị trí các khối.
- Kẻ địch có thể làm thay đổi các bit trong x_{j+1} khi giải mã nếu sửa bit trong c_j.
- IV không cần giữ bí mật, tuy nhiên cần giữ tính toàn vẹn của nó.

Định nghĩa

- *Giả sử E_{K_1}, E_{K_2} là hai hệ mật mã khối khóa K_1, K_2 tương ứng. Ta gọi tích của E_{K_1} với E_{K_2} là hệ mật mã E xác định bởi $E(x) = E_{K_2}(E_{K_1}(x))$. Tương tự ta có tích của nhiều hệ mật mã..*

Định nghĩa

- *Giả sử E_{K_1}, E_{K_2} là hai hệ mật mã khối khóa K_1, K_2 tương ứng. Ta gọi tích của E_{K_1} với E_{K_2} là hệ mật mã E xác định bởi $E(x) = E_{K_2}(E_{K_1}(x))$. Tương tự ta có tích của nhiều hệ mật mã..*

- *Trong trường hợp tích của nhiều hệ mật mã khối mà các khóa không độc lập nhau thì gọi là hệ mật mã bội.*

Định nghĩa

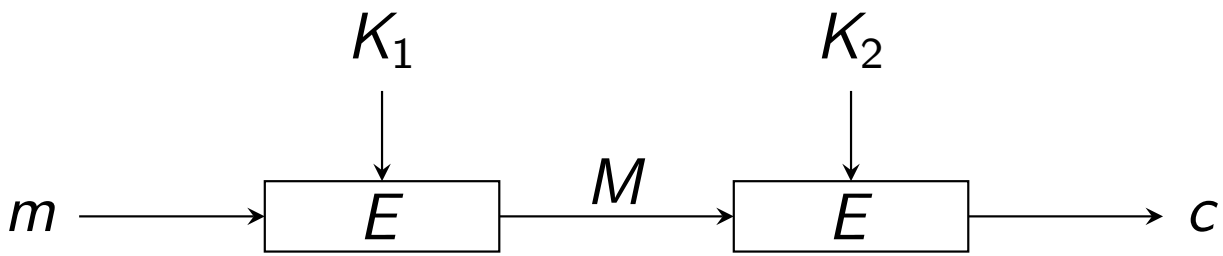
- *Giả sử E_{K_1}, E_{K_2} là hai hệ mật mã khối khóa K_1, K_2 tương ứng. Ta gọi tích của E_{K_1} với E_{K_2} là hệ mật mã E xác định bởi $E(x) = E_{K_2}(E_{K_1}(x))$. Tương tự ta có tích của nhiều hệ mật mã..*

- *Trong trường hợp tích của nhiều hệ mật mã khối mà các khóa không độc lập nhau thì gọi là hệ mật mã bội.*

- *Sử dụng tích các hệ mã để làm tăng độ phức tạp hoặc tăng chi phí bộ nhớ cho việc giải mã.*

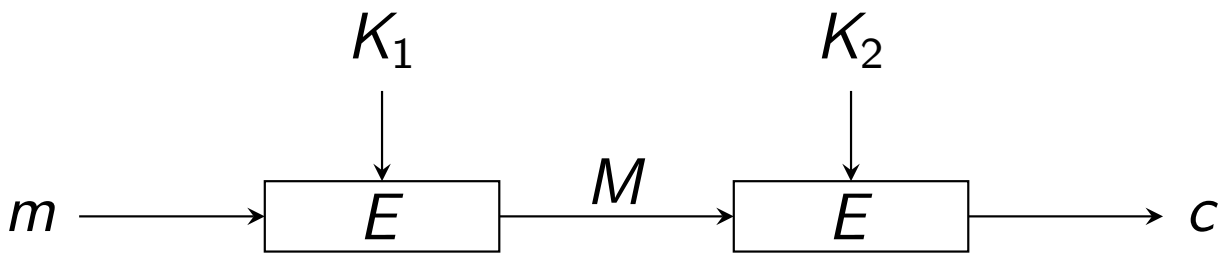
Định nghĩa

- *Tích 2 hệ mã:*

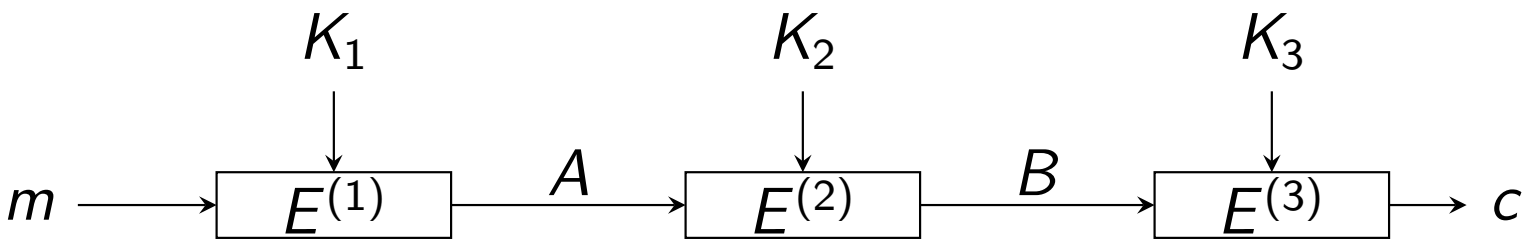


Định nghĩa

- *Tích 2 hệ mã:*



- *Tích 3 hệ mã:*



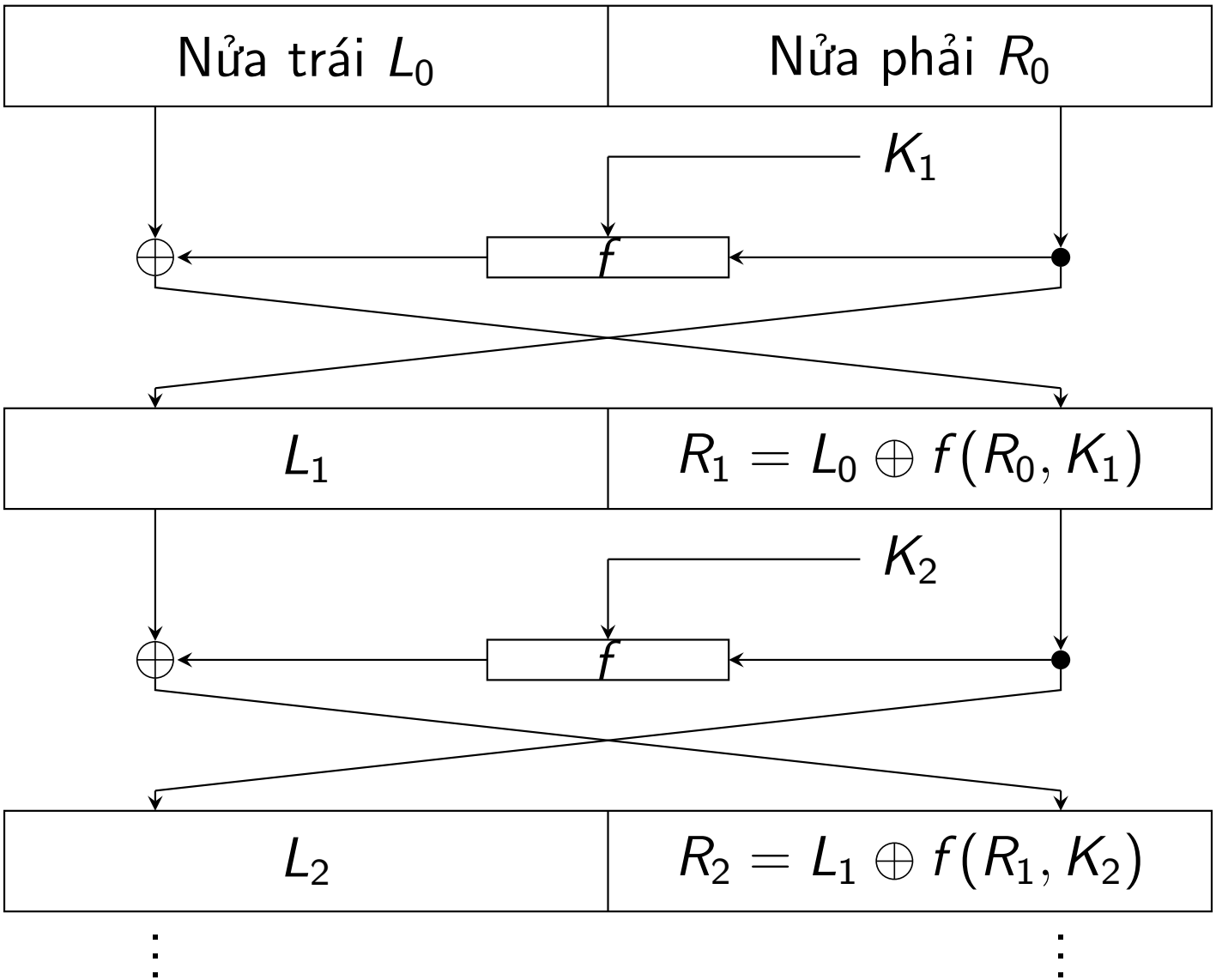
Định nghĩa

Hệ mật mã khối lặp *là hệ mật mã khối liên quan đến việc lặp tuần tự của một hàm gọi là hàm lặp. Các tham số bao gồm số các vòng lặp r, kích thước khối bit n, và độ dài k bit của khóa đầu vào K cho việc sinh ra các khóa con K_i ở r vòng lặp. Ở đó mỗi giá trị của K_i thì hàm lặp là một tương ứng 1-1 trên các giá trị đầu vào.*

Định nghĩa

Hệ mật mã Feistel *là một ánh xạ từ khối* $2t$ *bit* (L_0, R_0), *gồm* t *bit nửa khối trái* L_0 *và* t *bit nửa khối phải* R_0, *thành khối mã* (R_r, L_r) *thông qua quá trình xử lý gồm* r *vòng* $(r \geq 1)$. *Với mỗi* $1 \leq i \leq r$, *vòng thứ* i *xánh xạ* $(L_{i-1}, R_{i-1}) \xrightarrow{K_i} (L_i, R_i)$ *xác định bởi:*
$L_i = R_{i-1}, R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$, *với khóa con* K_i *được sinh ra từ khóa* K.

Hệ mật mã Feistel



Data Encryption Standard (DES)

- DES là hệ mật mã khối Feistel

Data Encryption Standard (DES)

- DES là hệ mật mã khối Feistel
- Kích thước khối $n = 64$ bit

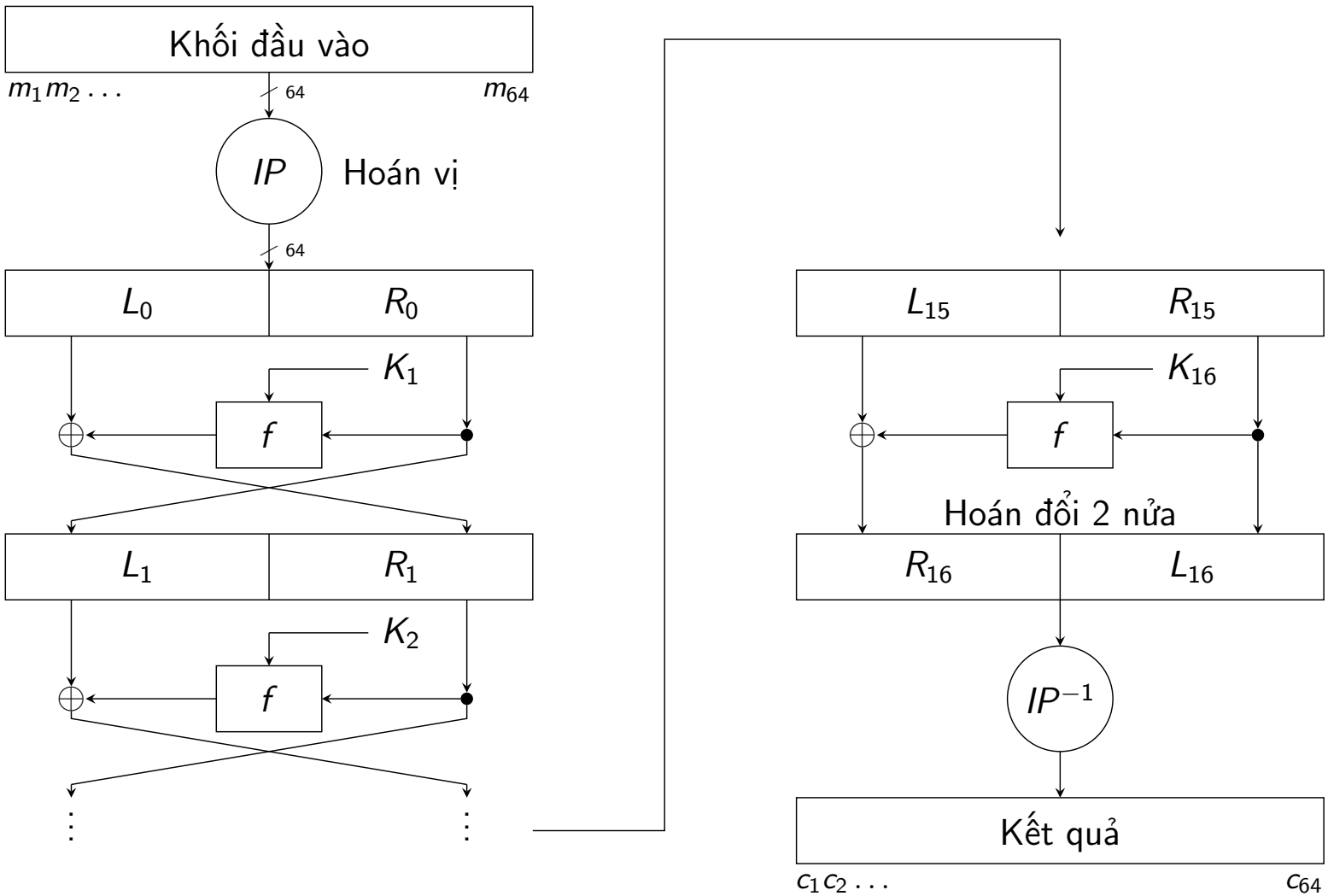
Data Encryption Standard (DES)

- DES là hệ mật mã khối Feistel
- Kích thước khối $n = 64$ bit
- Khóa bí mật có độ dài 56 bit nhưng khóa nhập vào có kích thước $k = 64$ bit trong đó bỏ đi 8 bit ở các vị trí 8,16,...,64.

Data Encryption Standard (DES)

- DES là hệ mật mã khối Feistel
- Kích thước khối $n = 64$ bit
- Khóa bí mật có độ dài 56 bit nhưng khóa nhập vào có kích thước $k = 64$ bit trong đó bỏ đi 8 bit ở các vị trí 8,16,...,64.
- Hàm lặp trong DES: $f(R_{i-1}, K_i) = P(S(E(R_{i-1}) \oplus K_i))$
  - E là các hàm mở rộng từ 32 lên 48 bit (lặp một số bit)
  - S là các hà S-box
  - P là hàm hoán vị các bit

Sơ đồ của DES



Tham khảo về DES: https://en.wikipedia.org/wiki/DES_supplementary_material

Tài liệu tham khảo

Handbook of Applied Crytography, chapter 7

http://cacr.uwaterloo.ca/hac/