AN TOÀN THÔNG TIN

Giảng viên: Th.s Phạm Minh Thái

Email: pmthai@uneti.edu.vn

Tổ Mạng Máy Tính và Công Nghệ Đa Phương Tiện

Khoa Công nghệ Thông tin

CHƯƠNG 3: MÃ HÓA ĐỐI XỨNG HIỆN ĐẠI

3.1. Nguyên lý của các hệ mã hóa khối.

3.2. Chuẩn mã hóa dữ liệu DES.

3.3. Hệ mã hóa 3DES.

3.4. Chuẩn mã hóa tiên tiến AES.

3.5. Các hệ mã hóa khối khác.

3.6. Các phương thức mã hóa liên hợp.

3.7. Triển khai chức năng mã hóa.

3.8. Quản lý và phân phối khóa

Mã hóa đối xứng hiện đại

- Đối tượng: của mã hóa cổ điển là các bản tin ngôn ngữ.
- Đơn vị mã hóa: là các chữ cái, áp dụng phương thức thay thế/phương thức hoán vị.
- Mã hóa hiện đại quan tâm đến: chống phá mã trong các trường hợp biết trước bản rõ, hay bản rõ được lựa chọn.
- Mã hóa đối xứng hiện đại gồm:
  - Mã dòng: mã hóa từng bit/byte của thông điệp.
  - Mã khối: gộp một số bit, mã hóa chúng như một đơn vị.

3.1 Nguyên lý của các hệ mã hóa khối

- Giống như thay thế các ký tự rất lớn (>= 64 bit)
  - Bảng mã hóa gồm 2^n đầu vào (n là độ dài khối)
  - Mỗi khối đầu vào ứng với một khối mã hóa duy nhất
  - Độ dài khóa là n x 2^n bit (quá lớn) => tạo các khối nhỏ hơn.
- Sử dụng ý tưởng dùng mã tích (kết hợp giữa mã thay thế, mã hoán vị và nhiều vòng lặp như vậy).
- Hầu hết các hệ mã hóa khối đối xứng dựa trên cấu trúc hệ mã hóa Feistel (sử dụng liên tiếp toán tử chuyển vị và toán tử thay thế => độ an toàn cao hơn).

Mã hóa Feistel

- Đề xuất bởi Horst Feistel dựa trên khái niệm hệ mã hóa tích hợp thuận nghịch của Shannon.
- Phân mỗi khối dài 2w bit thành hai nửa L_0 và R_0
- Xử lý qua n vòng
- Chia khóa K thành n khóa con K_1, K_2,..., K_n
- Tại mỗi vòng i
  - Thực hiện thay thế ở nửa bên trái L_{i-1} bằng cách XOR nó với $F(K_i, R_{i-1})$
  - F thường gọi là hàm chuyển đổi hay hàm vòng
  - Hoán vị hai nửa L_i và R_i

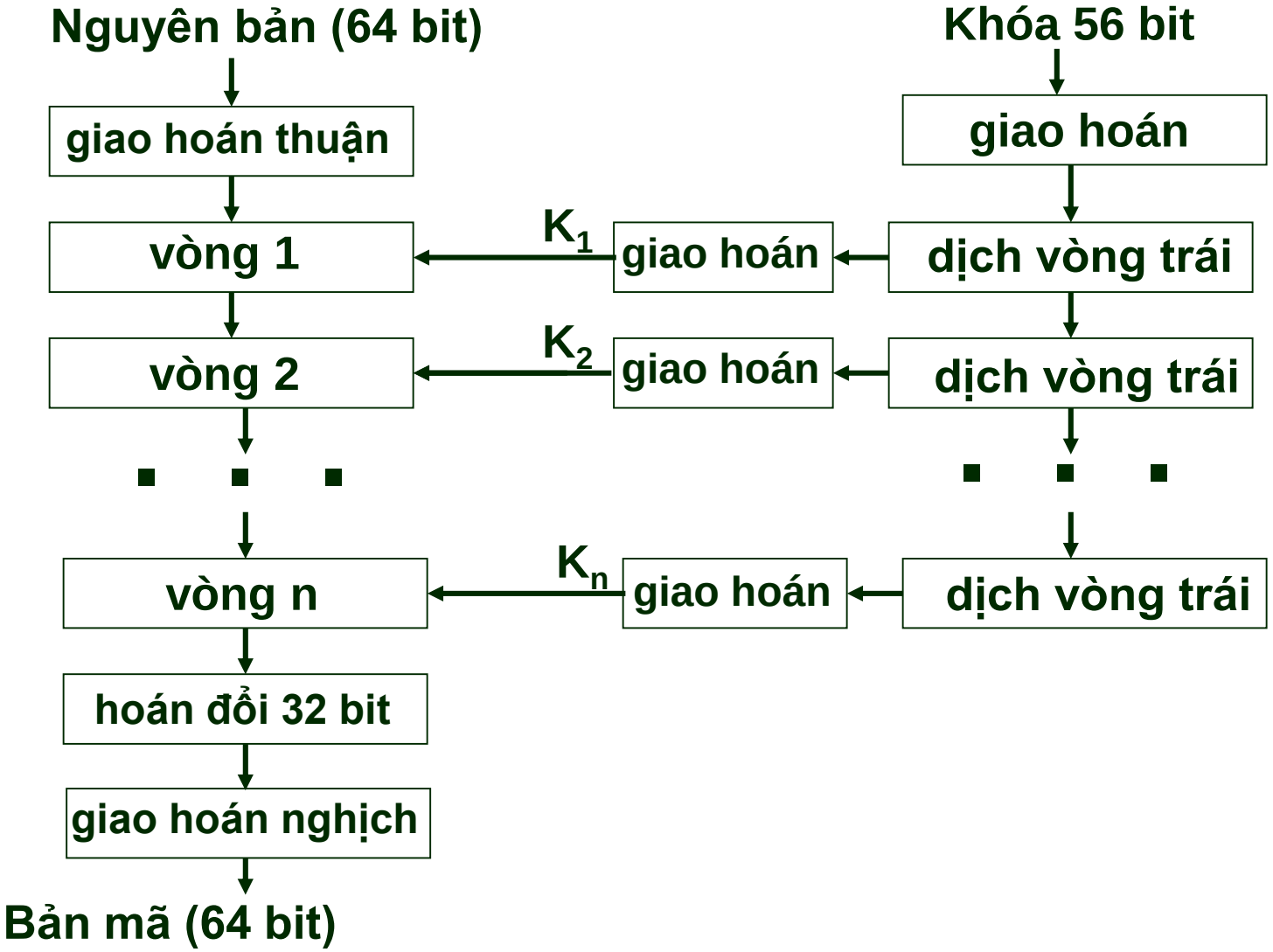
Giải mã Feistel

- Giống giải thuật mã hóa, chỉ khác:
  - Bản mã là dữ liệu đầu vào
  - Các khóa con được dùng theo thứ tự ngược lại
- Tại mỗi vòng kết quả: đầu ra là dữ liệu đầu vào của quá trình mã hóa.
- Đối với quá trình mã hóa:
  - $L_i = R_{i-1}$
  - $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$
- Đối với quá trình giải mã
  - $R_{i-1} = L_i$
  - $L_{i-1} = R_i \oplus F(L_i, K_i)$

3.2 Chuẩn mã hóa dữ liệu DES

- DES (Data Encryption Standard) được công nhận chuẩn năm 1977.
- Tên giải thuật là DEA (Data Encryption Algorithm)
- Là một biến thể của hệ mã hóa Feistel, bổ xung thêm các hoán vị đầu và cuối.
- Kích thước khối: 64 bit
- Kích thước khóa: 56 bit
- Số vòng: 16

Giải thuật mã hóa DES



Phá mã DES

- Khóa 56 bit => có $2^{56} = 7,2 \times 10^{16}$ giá trị.
- Phương pháp vét cạn: không thực tế.
- Tốc độ tính toán cao, có thể phá được khóa.
- Vấn đề còn phải nhận biết được nguyên bản.
- Thực tế: DES vẫn được sử dụng (không có vấn đề).
- Nếu cần an toàn hơn => 3DES hay chuẩn mới AES.

3.3 Hệ mã hóa 3DES

- Sử dụng 3 khóa và chạy 3 lần giải thuật DES
  - Mã hóa: $C = E_{K_3}[D_{K_2}[E_{K_1}[p]]]$
  - Giải mã: $p = D_{K_1}[E_{K_2}[D_{K_3}[C]]]$
- Độ dài khóa thực tế là 168 bit
  - Không tồn tại $K_4 = 56$ sao cho $C = E_{K_4}(p)$
- Vì sao 3 lần: tránh tấn công "gặp nhau ở giữa"
  - $C = E_{K_2}(E_{K_1}(p)) \Rightarrow X = E_{K_1}(p) = D_{K_2}(C)$
  - Nếu biết một cặp (p, C)
    - Mã hóa p với 2^{56} khóa và giải mã C với 2^{56} khóa
- So sánh tìm ra K_1 và K_2 tương ứng
- Kiểm tra lại với 1 cặp (p, C) mới: OK => K_1 và K_2 là khóa

3.4 Chuẩn mã hóa tiên tiến AES

- AES (Advanced Encryption Standard) được công nhận chuẩn mới năm 2001
- Tên giải thuật là Rijndael (Rijmen + Daemen)
- An toàn hơn và nhanh hơn 3DES
- Kích thước khối : 128 bit
- Kích thước khóa : 128/192/256 bit
- Số vòng : 10/12/14
- Cấu trúc mạng S-P, nhưng không theo hệ Feistel
  - Không chia mỗi khối làm đôi