HUTECH

Đại học Công nghệ Tp.HCM

Bài giảng Bảo mật Thông tin
Bài 3: Mã hóa đối xứng hiện đại

Trình bày:
Ths. Lương Trần Hy Hiến
http://hienlth.info/hutech/baomatthongtin

Nội dung

1. Mã dòng
2. Mã khối
3. DES
4. Một số thuật toán mã khối khác
5. Các mô hình ứng dụng mã khối
6. Bố trí công cụ mã hóa
7. Quản lý trao đổi khóa bí mật

1. Mã dòng (Stream Ciphers)

- Kích thước một đơn vị mã hóa: gồm k bít.
  Bản rõ được chia thành các đơn vị mã hóa:
  $P \rightarrow p_0 p_1 p_2 \ldots p_{n-1}$ (p_i: k bit)
- Một bộ sinh dãy số ngẫu nhiên: dùng một khóa K ban đầu để sinh ra các số ngẫu nhiên có kích thước bằng kích thước đơn vị mã hóa:
  StreamCipher(k) → $S = s_0 s_1 s_2 \ldots s_{n-1}$ (s_i: k bit)
- Mỗi số ngẫu nhiên được XOR với đơn vị mã hóa của bản rõ để có bản mã.
  $C_0 = p_0 \oplus s_0$, $c_1 = p_1 \oplus s_1 \ldots$;
  $C = c_0 c_1 c_2 \ldots c_{n-1}$

1. Mã dòng (Stream Ciphers)

- Quá trình giải mã được thực hiện ngược lại, bản mã C được XOR với dãy số ngẫu nhiên S để cho ra lại bản rõ ban đầu:
- $p_0 = c_0 \oplus s_0$, $p_1 = c_1 \oplus s_1$, …

Các thuật toán

- Tiny RC4
- RC4

Tiny RC4

- Đơn vị mã hóa của TinyRC4 là 3 bít.
- TinyRC4 dùng 2 mảng S và T mỗi mảng gồm 8 số nguyên 3 bít.
- Khóa là một dãy gồm N số nguyên 3 bít.
- Bộ sinh số mỗi lần sinh ra 3 bít để sử dụng trong phép XOR.
- Quá trình sinh số của TinyRC4 gồm hai giai đoạn:

Tiny RC4

a) *Giai đoạn khởi tạo*:

```
/* Khoi tao day so S va T */
for  i = 0 to 7 do
     S[i] = i;
     T[i] = K[i mod N];
next i
/* Hoan vi day S */
j = 0;
for  i = 0 to 7 do
     j = (j + S[i] + T[i]) mod 8;
     Swap(S[i], S[j]);
next i
```

Trong giai đoạn này, trước tiên dãy S gồm các số nguyên 3 bít từ 0 đến 7 được sắp thứ tự tăng dần. Sau đó dựa trên các phần tử của khóa K, các phần tử của S được hoán vị lẫn nhau đến một mức độ ngẫu nhiên nào đó.

Ví dụ: mã hóa bản rõ P = 001000110 (từ “bag“) với khóa K gồm 3 số 2, 1, 3 (N=3).

(xem giáo trình)

Tiny RC4

b) Giai đoạn sinh số

```
i, j = 0;
while (true)
      i = (i + 1) mod 8;
      j = (j + S[i]) mod 8;
      Swap (S[i], S[j]);
      t = (S[i] + S[j]) mod 8;
      k = S[t];
end while;
```

Trong giai đoạn này, các phần tử của S tiếp tục được hoán vị. Tại mỗi bước sinh số, hai phần tử của dãy S được chọn để tính ra số k 3 bít là số được dùng để XOR với đơn vị mã hóa của bản rõ.

RC4

Cơ chế hoạt động của RC4 cũng giống như TinyRC4 với các đặc tính sau:

- Đơn vị mã hóa của RC4 là một byte 8 bít.
- Mảng S và T gồm 256 số nguyên 8 bít
- Khóa K là một dãy gồm N số nguyên 8 bít với N có thể lấy giá trị từ 1 đến 256.
- Bộ sinh số mỗi lần sinh ra một byte để sử dụng trong phép XOR.

(xem giáo trình)

2. Mã khối (Block Cipher)

- So với mã hóa dòng
  - Mã hóa khối xử lý thông báo theo từng khối
  - Mã hóa luồng xử lý thông báo 1 bit hoặc 1 byte mỗi lần
- Giống như thay thế các ký tự rất lớn ($\geq$ 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
    - Tính thuận nghịch
  - Độ dài khóa là n x 2^n bit quá lớn
- Xây dựng từ các khối nhỏ hơn
- Hầu hết các hệ mã hóa khối đối xứng dựa trên cấu trúc hệ mã hóa Feistel