Chương 4 –Hệ mật mã khóa công khai

Public Key Cryptosystem
(phần 1)

4.1) Giới thiệu tổng quan

- Hệ mật mã khóa công khai là một thành tựu lớn của mật mã hiện đại
  - Thay đổi nguyên tắc truyền thống của mật mã
  - Giải quyết bài toán chia sẻ và quản lý khóa của mật mã khóa đối xứng
  - Tạo ra giải pháp **chữ ký số (chữ ký điện tử)** hiện được áp dụng trong hầu hết các dịch vụ và ứng dụng CNTT

A) Hoàn cảnh ra đời

- Năm 1976, Diffie và Hellman đưa ra ý tưởng vẫn đảm bảo tính bí mật của hệ mật mã
- Năm 1977, Rivest, Shamir và Adleman phát minh hệ mật mã khóa công khai
- Các hệ mật mã khác xuất hiện sau đó: Rabin , El-Gammal, Elliptic Curve

B) Đặc điểm

- Trong hệ mật mã khóa công khai (PKC), mỗi chủ thể
  - Khóa công khai K_E (public key)
  - Khóa riêng K_D (private key)
- Khóa công khai có thể
- Khóa riêng phải được chủ thể sở hữu

Cặp khóa K_D và K_E

- $K_E \neq K_D$ nhưng có

- Mã hóa M bằng K_E
  - $M = D(K_D, E(K_E, M))$ (1)
  - $M = D(K_E, E(K_D, M))$ (2)

- Công thức (1) là cơ sở để

- Công thức (2) là cơ sở để

C) Nguyên tắc thiết kế hệ PKC

- Sử dụng cơ chế với tính chất sau
  - *Với mọi đầu vào X, tính Y = f(X) là dễ*
  - *Biết Y, rất khó để tính ngược X trừ khi biết "cửa lật"*

- *"Cửa lật"* chính là để có thể giải mã bằng hàm ngược f^{-1} $X = f^{-1}(Y)$

- Không biết cửa lật để giải mã, việc phá mã trở nên vô cùng khó

So sánh

Hệ mật mã khóa công khai

- Mỗi bên truyền tin sở hữu 1 cặp khóa khác nhau

- Ứng dụng trong chữ ký số
- Hàm mã hóa là hàm toán học 1 chiều và có cửa bẫy

Hệ mật mã khóa đối xứng

- Cả hai bên cùng sở hữu 1 khóa

- Không thể sử dụng trong chữ ký số
- Hàm mã hóa là hàm biến đổi với hoán vị và thay thế

4.2) Hệ mật mã RSA

- RSA là hệ mật mã khóa công khai phổ biến nhất và được ứng dụng rộng rãi nhất hiện nay

- RSA được áp dụng trong
  - Mã hóa dữ liệu

- Một số giao thức mã hóa chủ chốt trên Internet hiện nay như SSL, TSL sử dụng RSA

A) Cơ sở toán học

- Hàm f của RSA là hàm
  - $Y = f(X) = X^e \ mod \ N$ **(1)**
  - N và e là những số nguyên rất lớn (Big Integer)
- Hàm f là hàm 1 chiều có cửa lật
  - Biết X, e và N, có thể tính Y tương đối đơn giản
  - Tuy nhiên, tính X từ Y, e và N là rất rất khó, gần như phải thử tất cả giá trị X trong miền {0,.., N-1}
- "Cửa lật" của hàm f như sau:

$$X = f^{-1}(Y) = Y^d \ mod \ N \ \textbf{(2)}$$

Tương quan giữa e và d

- Từ (1) và (2), theo tính chất modulo của lũy thừa =>

$$X = X^{ed} \bmod N \ (3)$$

- Từ (3), theo định lý Euler suy ra tương quan của e và d

$$\mathbf{ed = 1 \bmod \Phi(N)} \ \textbf{(4)}$$

với $\Phi(N)$ là số lượng các số $Z < N$ và nguyên tố cùng nhau với N: USCLN(Z,N) = 1

- Khi tồn tại d và e thỏa mãn (4)
- Giả sử chọn trước số e, điều kiện để d tồn tại và tính được d là:
- *Như vậy, trong việc xác định d*

Cách tạo Φ(N) như sau

- Chọn p và q là 2 số nguyên tố ngẫu nhiên cực lớn, ta có N = p * q và $\Phi(N) = (p-1)(q-1)$
- $d = e^{-1} \bmod \Phi(N)$ và e đã biết,
- Như vậy, cửa lật của RSA
- Muốn phá mã RSA, phải
- Do đó, độ an toàn của RSA sẽ phụ thuộc vào
- Khi chọn p và q rất lớn, có thì phá mã RSA trở thành bài toán cực kỳ khó

B) Thuật toán RSA

- Công đoạn sinh khóa công khai và khóa riêng
  - 1) Chọn 2 số nguyên tố *rất lớn* p và q.
  - 2) Chọn 1 số e:
  - 3) Tính d từ e và Z bằng thuật toán GCD mở rộng (3.2.5)
- Khóa riêng thu được là , khóa công khai là
- Để sử dụng RSA mã hóa bản tin M (dữ liệu nhị phân):
  - Chuyển M thành dạng số nguyên
  - Sử dụng khóa công khai để mã hóa qua hàm sau
- Công đoạn giải mã C
  - Sử dụng khóa riêng **d** giải mã

Ví dụ

- Sinh khóa
  - Chọn p = 2, q = 11
  - Tính N = 2 * 11 , (p-1)(q-1) = 1 * 10
  - Chọn e và tính d
- Mã hóa
  - Chọn M = 4, tính C
- Giải mã
  - Cho C = 15, tính M

C) Các vấn đề kĩ thuật trong thuật toán RSA

- Vấn đề chọn p và q
  - Sử dụng thuật toán
  - Sử dụng thuật toán
- Tính nhanh modulo N của lũy thừa bằng cách

  hàm modulo $M^e \mod N$

- **Tính lũy thừa nhanh modulo N**

  $C = M^e \mod N$

  Ví dụ: N = 179, e = 73, M = 7,

  Tính C = $7^{73} \mod 179$

- Ví dụ tính $7^{73} \mod 179$
- Khai triển
- Tính lần lượt các giá trị sau

$7^2 \mod 179 = (7 * 7) \mod 179 = 49$

$7^4 \mod 179 = (49 * 49) \mod 179 = 74$

$7^{16} \mod 179 = (106 * 106) \mod 179 = 138$

$7^{32} \mod 179 = (138 * 138) \mod 179 = 70$

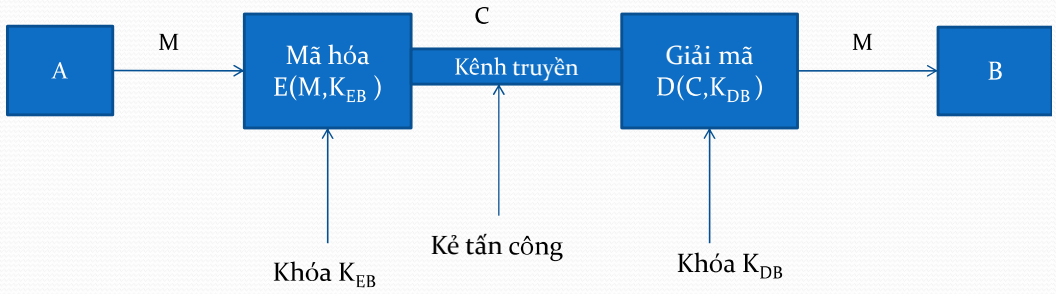
- Kết quả

  $C = 7^{(1+8+64)} \bmod 179 =$

D) Sơ đồ bảo mật truyền tin trong hệ RSA

- Tình huống:
  - A và B cần truyền tin mật
- Khởi tạo
  - A có khóa riêng K_{DA} và khóa công khai K_{EA}
  - B có khóa riêng K_{DB} và khóa công khai K_{EB}
  - A và B

- A sử dụng để mã hóa M tạo thành C



- B sử dụng để giải mã C thu được M

Chú ý

- Tốc độ mã hóa của RSA thấp hơn nhiều so với các hệ mật mã khóa đối xứng như 3-DES và AES
- RSA thường chỉ được sử dụng để bảo mật trong trường hợp
  - Kích thước dữ liệu nhỏ
  - Tốc độ truyền thấp

E) Đánh giá an toàn RSA

- Để tìm ra khóa d, cần
  (đây là bài toán khó với độ phức tạp hàm mũ)

- Với hệ thống siêu máy tính đã có thể phân tích thành công N với kích thước khoảng 900 bit (270 chữ số thập phân) trong 2 năm

- Hệ mật mã RSA hiện nay đều dùng N có 1024 bit trở lên
  - RSA-1024 (N có khoảng 309 chữ số)
  - RSA-2048 ( )
  - RSA-3072 ( )

Tổng kết

- RSA được coi là an toàn với điều kiện

- Các phiên bản RSA
  - RSA-758 đã bị phá mã
  - RSA-1024 hiện tại chưa bị phá mã nhưng không còn được xem là thật sự an toàn
  - RSA-2048
  - RSA-3072