1 Tổng quan về mật mã khóa công khai

1.1 Lịch sử

Ý tưởng về hệ thống mã hóa khóa công khai được Martin Hellman, Ralph Merkle và Whitfield Diffie tại Đại học Stanford giới thiệu vào năm 1976.

Sách:

Diffie, W.; Hellman, M.E. (November 1976). "New directions in cryptography". IEEE Transactions on Information Theory

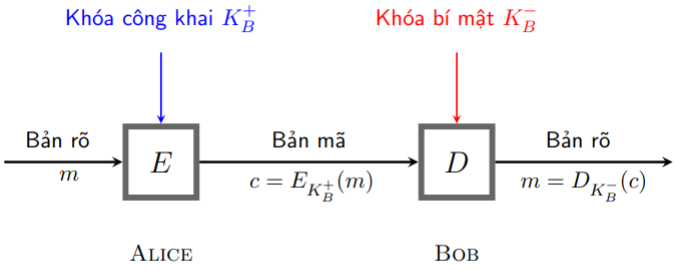
1.2 Khái niệm:

Mật mã khóa công khai (public-key) là hệ mã không đối xứng, nghĩa là sử dụng hai khóa liên đới cho việc mã hoá và giải mã thay vì một khóa duy nhất như trong các hệ mã cổ điển (hay còn gọi là hệ mã đối xứng). Việc này đáp ứng được các yêu cầu trong các ứng dụng về bảo mật riêng tư, phân phối khóa, và xác thực điện tử.

Lưu ý:

Một hệ mật khóa công khai không bao giờ cung cấp độ mật vô điều kiện - thực tế, đó là hàm cửa sập một chiều (a trapdoor one-way function).

1.3 Mô hình hệ mật khóa công khai tổng quát



Hình 6.1 Mô hình hệ mật khóa công khai tổng quát

Hình 1: Mô hình hệ mật khóa công khai tổng quát

Ý tưởng:

- Mỗi người dùng: sử dụng một cặp khóa (khóa công khai, khóa bí mật)
  - Khóa công cộng (public key): được công bố rộng rãi và được sử dụng trong mã hóa thông tin

  - Khóa riêng (private key): chỉ do một người nắm giữ và được sử dụng để giải mã thông tin đã được mã hóa bằng khóa công cộng tương ứng

- Mã hóa: A muốn gửi thông điệp cho B - mã hóa bằng khóa công khai của B

$$y = E(e_B, x)$$

- Giải mã: B giải mã bằng khóa bí mật của mình

$$x = D(d_B, y)$$

- Hàm mã hóa và giải mã có thể đổi chỗ

Trong đó:

- Các phương pháp mã hóa này khai thác những ánh xạ f mà
  - Biết x, tính y=f(x) dễ dàng
  - Biết y, việc thực hiện ánh xạ ngược f –1 tính x là rất khó

  Hàm f có tính chất trên thường gọi là hàm một chiều
- Ví dụ: Cho các số nguyên tố p1, p2, ..., pn
  - Tính N= p1* p2* ... * pn- dễ
  - Ngược lại, biết N, tìm p1, p2, ..., pn là khó

Hàm cửa sập (trap door):

- Để xây dựng hệ mã khóa công khai - thường dùng hàm một chiều đặc biệt có tham số/cửa sập
  - Hàm mã hóa - là hàm cửa sập
  - Khóa (bí mật) - chính là thông tin tham số - bẫy trap door

1.4 Những hệ mật khóa công khai quan trọng nhất

- RSA: dựa trên độ khó của phép phân tích các số nguyên lớn.
- Merkle-Hellman Knapsack: và các hệ liên quan dựa trên độ khó của bài toán subset sum (được biết là NP-complete). Tuy nhiên, có nhiều hệ mật dựa trên bài toán sắp ba lô đã được chứng minh là không bảo mật.
- McEliece: dựa trên bài toán giải mã của một mã tuyến tính (cũng được cho là NP-complete).
- ElGamal: dựa trên bài toán Logarit rời rạc trên trường hữu hạn.
- Chor-Rivest: là một hệ sắp ba lô nhưng được xem là bảo mật.
- Elliptic Curve: là sự cải tiến của các hệ mật khác, chẳng hạn tương tự ElGamal nhưng dựa trên các đường cong elíp thay vì trường hữu hạn. Ưu điểm của các hệ mật dạng này là có thể duy trì được độ bảo mật với khóa nhỏ hơn thông thường.

2 Hệ mật RSA

2.1 Lịch sử

Hệ mật RSA, được phát triển bởi Ron Rivest, Adi Shamir và Leonard Adleman (1977), có thể được sử dụng trong bảo mật dữ liệu và công nghệ chữ ký điện tử.

2.2 Ý tưởng

Bảo mật của RSA dựa trên giả thuyết không có các thuật toán đủ nhanh để khai triển luỹ thừa một số. Qui trình áp dụng RSA gồm hai bước:

1. Lựa chọn (sinh) cặp khóa công khai và khóa bí mật
2. Thực hiện thuật toán mã hoá và thuật toán giải mã

2.3 Mô tả hệ mật

- Các phép tính được thực hiện trên Z_n với $n = p \cdot q$.
- $S = \langle P, C, K, E, D \rangle$
  - $n = pq$ với p và q là hai số nguyên tố lẻ phân biệt. $\phi(n) = (p-1)(q-1)$
  - $P = C = Z_n$
  - $K = \{(n, p, q, a, b) : n = pq, p, q \text{ là số nguyên tố, } ab \equiv 1 \mod \phi(n)\}$

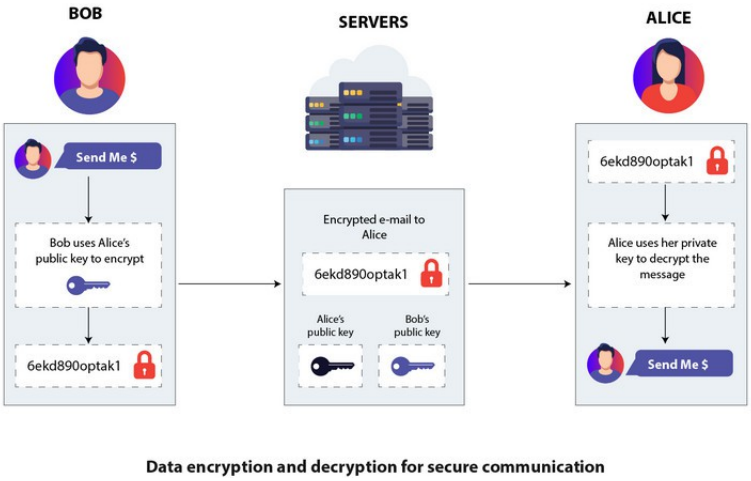
Với mỗi $k = (n, p, q, a, b) \in K$, định nghĩa:

$$e_k(x) = x^b \mod n$$
$$d_k(y) = y^a \mod n$$

với $x, y \in Z_n$.

2.4 Sinh cặp khóa công khai - bí mật

1. Chọn hai số nguyên tố đủ lớn, p và q
2. Tính toán $n = pq$ và $\phi(n) = (p-1)(q-1)$
3. Chọn một số, e $(1 < e < \phi(n))$ sao cho $\gcd(e, \phi(n)) = 1$. Giá trị e sẽ được sử dụng trong mã hoá
4. Tìm một số d sao cho $ed-1$ chia hết cho $\phi(n)$, hay nói cách khác $d = e^{-1} \mod \phi(n)$. Giá trị d sẽ được sử dụng để giải mã
5. Công khai khóa K_B^+ = (n, e) và giữ bí mật khóa K_B^- = (n, d)



Hình 2: Thuật toán mã hoá (Alice) và thuật toán giải mã (Bob)

Mã hoá (Alice):

Giả sử Alice muốn gửi cho Bob một mẫu bit, hoặc một số m sao cho $m < n$. Để mã hoá, Alice thực hiện tính luỹ thừa, m^e, sau đó tính toán số dư khi đem chia m^e cho n. Vì vậy, giá trị được mã hoá (c) của bản tin m là: $c = m^e \mod n$

Giải mã (Bob):

Để giải mã đoạn tin mã hoá nhận được (c), Bob tính toán: $m = c^d \mod n$. Việc này đòi hỏi phải sử dụng khóa bí mật (n, d).

Ví dụ:

Giả sử B chọn $p = 101$ và $q = 113$, khi đó $n = 11413$ và $\phi(n) = 11200$.

Giả sử B chọn $b = 3533$, khi đó bằng thuật toán Euclidean mở rộng ta tính được

$$a = b^{-1} \equiv 6597 \pmod{11200}.$$

B công khai bộ $(n = 11413, b = 3533)$.

Bây giờ giả sử A muốn gửi từ hiện 9726 cho B, A sẽ tính

$$9726^{3533} \equiv 5761 \pmod{11413},$$

là từ mã.

Khi B nhận được 5761, B sẽ tính

$$5761^{6597} \equiv 9726 \pmod{11413},$$

và thu được từ hiện A muốn gửi.

2.5 Áp dụng hệ mật RSA

1. Sinh hai số nguyên tố có giá trị lớn: p và q

2. Tính $n = pq$ và $\phi(n) = (p-1)(q-1)$
3. Chọn ngẫu nhiên một số nguyên e $(1 < e < \phi(n))$ thỏa $\gcd(e, \phi(n)) = 1$
4. Tính giá trị $d = e^{-1} \mod \phi(n)$ (bằng thuật toán Euclide mở rộng)
5. Công bố giá trị (n, e) (khóa công khai)
6. Giữ bí mật giá trị (p, q, d) (khóa bí mật)

References:

Diffie, W.; Hellman, M.E. (November 1976). "New directions in cryptography". IEEE Transactions on Information Theory

https://ieeexplore.ieee.org/document/1055638

Slide mật mã thầy Hân

Slide mật mã thầy Nam