AN TOÀN & BẢO MẬT THÔNG TIN

Giảng viên: Ths Phạm Thanh Bình

Bộ môn Kỹ thuật máy tính & mạng

http://dhthuyloi.blogspot.com

Chương 3:

MẬT MÃ KHOÁ CÔNG KHAI VÀ ỨNG DỤNG

- Giới thiệu chung
- Thuật toán mã hoá RSA
- Các hàm Hash và MAC
- Chữ ký số và chứng thực

Không phải mật mã, là trick, dùng phối hợp với mật mã

Bài 3.1 Giới thiệu chung

- Ý tưởng về khoá công khai được Diffie và Hellman đưa ra vào năm 1976.
- Sự phát triển của hệ thống mã hoá khoá công khai đã tạo ra một cuộc cách mạng trong lịch sử ngành mật mã.

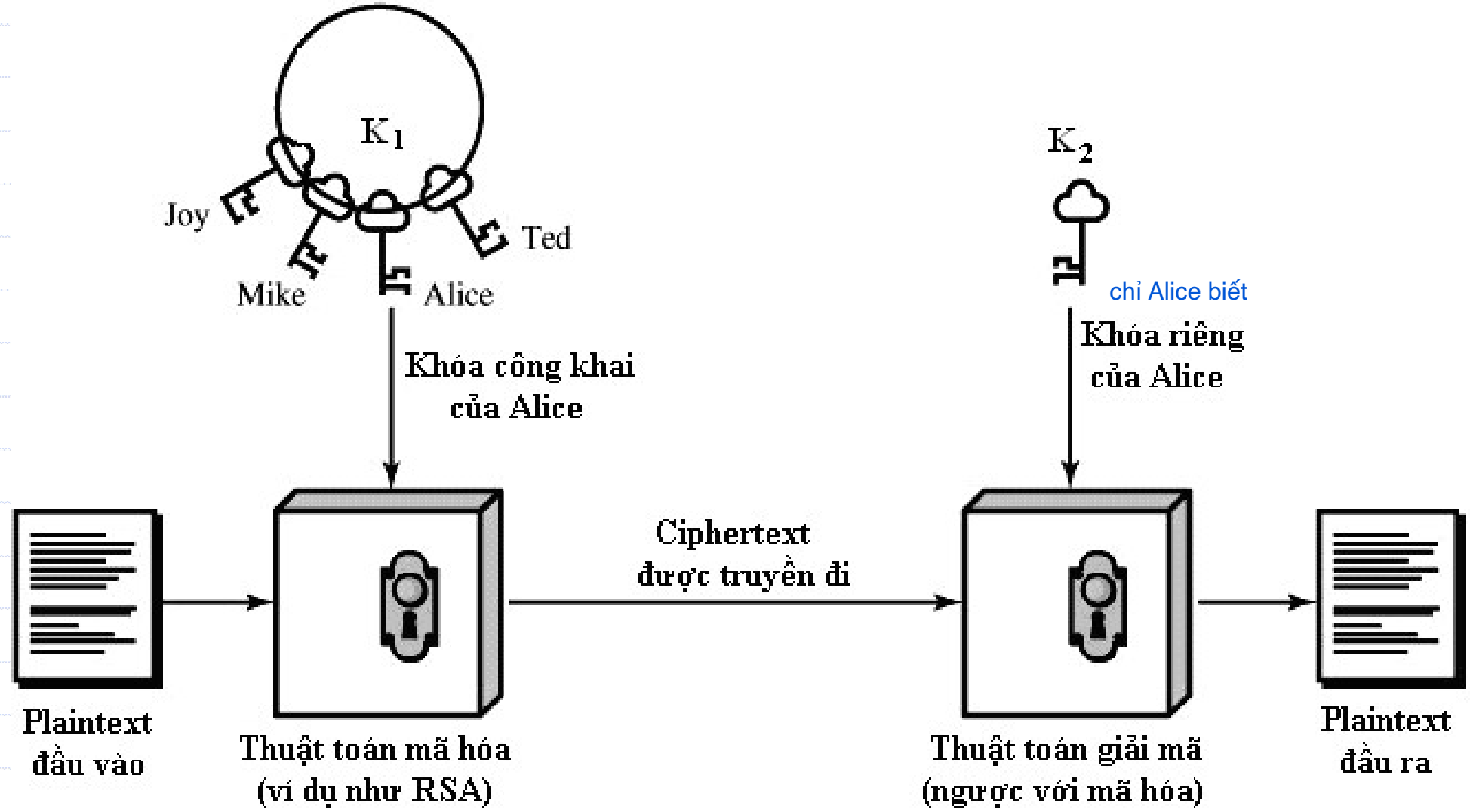
- Các mật mã đối xứng dùng chung một khoá cho quá trình mã hoá và giải mã. Chúng đều dựa trên nền tảng của phép thay thế và hoán vị. Nhưng các thuật toán mã hoá công khai dựa trên các hàm toán học là chủ yếu.
- Hệ mật mã khoá công khai là bất đối xứng, cho phép sử dụng hai khoá riêng biệt cho các quá trình mã hoá và giải mã.
- Việc dùng hai khoá riêng biệt đã tạo ra những khả năng ứng dụng mới trong các lĩnh vực bảo mật, phân phối khoá, và xác thực.

Ứng dụng trong bảo mật

- Giả sử mỗi người dùng sử dụng hai khoá (K_1, K_2), trong đó K_1 dùng để mã hoá, K_2 dùng để giải mã.
- Người đó có thể công bố công khai khoá K_1 (trong "danh bạ") để người gửi tin mã hoá thông điệp, và giữ bí mật K_2 (dùng riêng cho mình) để giải mã khi nhận được thông điệp.

nếu muốn bảo mật thông điệp phải mã hoá = khoá công khai của người nhận
=> ng duy nhất giải mã: Alice giải mã = khoá riêng
người gửi phải mã hoá mã riêng = mã riêng

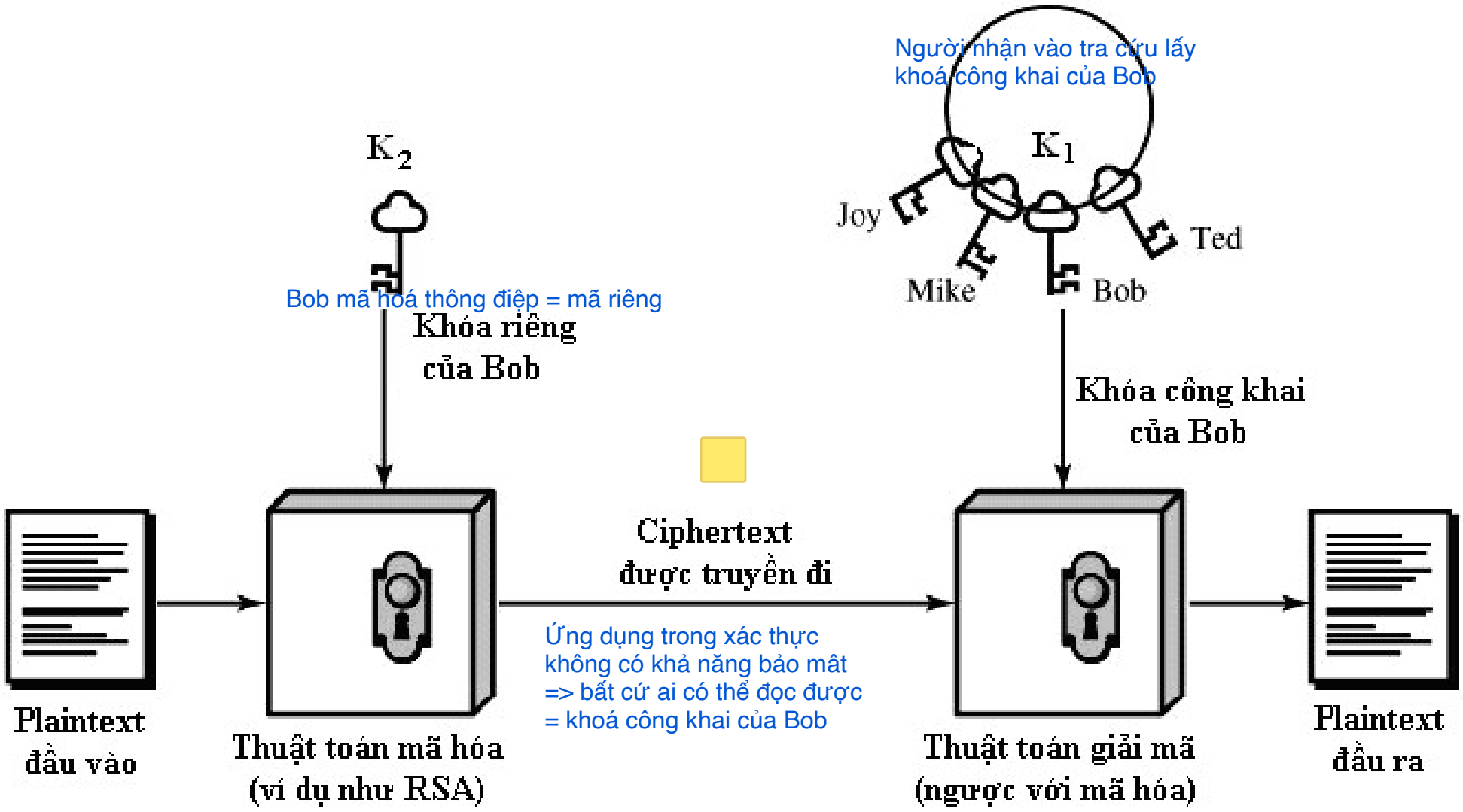
mật mã đối xứng: truyền trên đường truyền từ A -> B nên có thể bị lộ



(a) Sơ đồ mã hóa

Ứng dụng trong xác thực

- Nếu người gửi muốn khẳng định thông điệp là của mình, không phải do kẻ khác làm giả, anh ta có thể mã hoá thông điệp bằng khoá bí mật K_2 của mình trước khi gửi đi.
- Người nhận sẽ dùng khoá công khai K_1 của người gửi để giải mã. Nếu giải mã thành công thì chứng tỏ thông điệp đó đúng là của người gửi



(b) Sơ đồ chứng thực

Yêu cầu:

- Không thể suy ra khoá bí mật dù biết thuật toán và khoá công khai.
- Có thể đạt được điều đó nhờ các hàm toán học đặc biệt gọi là hàm một chiều.

có thể đạt được điều đó nhờ
các hàm toán học đặc biệt gọi
là hàm cửa lật 1 chiều

Hàm một chiều (One-way function)

- Hàm $f(x)$ được gọi là hàm một chiều nếu tính $y = f(x)$ là dễ nhưng việc tính hàm ngược $x = f^{-1}(y)$ là không thể thực hiện.
- Nói cách khác, thời gian tiêu tốn để tính hàm ngược là vô cùng lớn, và được coi là không giải được!

Ví dụ:

không thể ứng dụng hàm 1 chiều vào mật mã

- Hàm $f(x) = x^2 \bmod n$ với $n = p.q$ là tích của hai số nguyên tố lớn, là hàm một chiều.
- Số nguyên tố lớn: dài tới hàng trăm chữ số thập phân

Hàm cửa lật một chiều (Trapdoor one-way function)

- Hàm $f(x)$ được gọi là hàm cửa lật một chiều nếu tính $y = f(x)$ là dễ, tính $x = f^{-1}(y)$ là không thể, nhưng có cửa lật z để tính $x = f^{-1}_z(y)$ là dễ .

Ví dụ:

- Hàm $f(x) = x^a \bmod n$ với $n = p.q$ là tích của hai số nguyên tố lớn, a là số nguyên, là hàm cửa lật một chiều vì:
- Nếu như chỉ biết n và a thì tính $x = f^{-1}(y)$ là rất khó
- Nhưng nếu biết cửa lật, chẳng hạn, biết hai thừa số p, q của n thì sẽ tính được $f^{-1}(y)$ khá dễ dàng

Sự an toàn

- Kích thước khóa cần đủ lớn để làm thất bại các tấn công brute-force, nhưng cần đủ nhỏ để thi hành mã hóa và giải mã
- Trên thực tế, các kích thước khóa giúp ngăn chặn hiệu quả tấn công brute-force lại làm tốc độ mã hóa và giải mã trở nên quá chậm!

Bài 3.2 Thuật toán mã hoá RSA

- Ra đời năm 1977 bởi Ron Rivest, Adi Shamir, và Len Adleman tại MIT
- RSA là một thuật toán mã hoá khối, mỗi khối là một dãy bít nhị phân ứng với một số nguyên trong khoảng từ *0* đến $n - 1$.
- Kích thước điển hình của n là *1024* bit, hay *309* chữ số thập phân. Tức là $n < 2^{1024}$.

- Công thức mã hoá:

$$C = P^a \bmod n \qquad (1)$$

- Công thức giải mã:

$$P = C^b \bmod n \qquad (2)$$

Trong đó:

- $n = p.q$ là tích của hai số nguyên tố lớn
- P, C thuộc Z_n
- a và b là các số nguyên thoả mãn điều kiện:

$$P^{ab} \bmod n = P$$

Chứng minh:

- Thay (1) vào (2) ta có:

$$P = C^b \bmod n = (P^a)^b \bmod n = P^{ab} \bmod n$$

- Vậy để có thể giải mã được thì:

$$P^{ab} \bmod n = P$$

- Có thể đạt được điều đó nếu:

$$ab \bmod \Phi(n) = 1 \quad (*)$$

Với $\Phi(n) = \Phi(pq) = (p-1)(q-1)$

- Điều đó chỉ đúng nếu a (và b) có quan hệ nguyên tố với $\Phi(n)$:

$$ƯSCLN(\Phi(n), a) = 1$$

- Công thức $(*)$ tương đương với:

$$b = a^{-1} \bmod \Phi(n)$$

Các bước tạo khoá:

- Chọn 2 số nguyên tố lớn p, q
- Tính $n = pq$
- Tính $\Phi(n) = (p-1)(q-1)$
- Chọn a sao cho $ƯSCLN(\Phi(n),a) = 1; a < \Phi(n)$
- Tính $b = a^{-1} \bmod \Phi(n)$

- Để mã hoá cần phải biết a và n. Khoá công khai chính là $K1 = (a, n)$
- Để giải mã cần biết b và n. Khoá bí mật là $K2 = (b, n)$

Ví dụ:

- Chọn hai số nguyên tố, $p = 17$ và $q = 11$.
- Tính $n = pq = 17 \times 11 = 187$.
- Tính $\Phi(n) = (p - 1)(q - 1) = 16 \times 10 = 160$.
- Chọn a sao cho a quan hệ nguyên tố với $\Phi(n) = 160$ và nhỏ hơn $\Phi(n)$:

  Ta chọn được $a = 7$.
- Xác định b sao cho $a.b = 1 \pmod{160}$ và b nhỏ hơn 160.

- Giá trị của b tìm được là $b = 23$, vì:

$$23 \times 7 = 161 \bmod 160 = 1$$

(có thể tính b theo thuật toán Ơclit mở rộng)

- Khoá công khai $K1 = (a, n) = (7, 187)$
- Khoá riêng $K2 = (b, n) = (23, 187)$

Giả sử bản rõ $P = 88$, khi đó quá trình mã hoá và giải mã sẽ như sau:

- Mã hoá: $C = P^a \bmod n = 88^7 \ mod \ 187 = 11$
- Giải mã: $P = C^b \bmod n = 11^{23} \ mod \ 187 = 88$

đang không biết tính bài này nè!!!!

Bài tập:

- Chọn một cặp số nguyên tố p, q
- Thực hiện các bước tạo khoá, mã hoá và giải mã theo thuật toán RSA

Sự an toàn

- Sự an toàn của thuật toán RSA dựa trên độ phức tạp của phép phân tích số nguyên n thành các thừa số nguyên tố lớn.
- Nếu biết khoá công khai (a,n) thì cũng không thể tính được khoá bí mật b, vì không thể phân tích n thành $p.q$ khi p, q đã chọn đủ lớn, và do đó không thể tính được $\Phi(n)$.
- Với n dài 1024 bit (309 chữ số thập phân), cả p và q cần lớn từ 10^{75} tới 10^{100}.

Nhận xét:

- Do phải tính toán với các số rất lớn nên tốc độ thực hiện của thuật toán RSA rất chậm, việc ứng dụng RSA để mã hoá các thông điệp có kích thước lớn là khó khăn.
- Trên thực tế, có thể áp dụng RSA để bảo mật các thông điệp ngắn, để chuyển giao khoá cho các mật mã đối xứng, và tạo chữ kí số.

Hết Phần 3_1