Mã hóa khóa công khai và chứng thực thông tin

Một số nhược điểm của mã hóa đối xứng

1) **Vấn đề quản lý khóa**: vấn đề trao đổi khóa giữa người gửi và người nhận rất phức tạp trong môi trường nhiều người sử dụng. Với n NSD thì phải tạo n(n-1)/2 khóa. Mỗi người dùng phải lưu (n-1) khóa bí mật để làm việc với n-1 người khác

2) **Tính bí mật của khóa**: không có cơ sở quy trách nhiệm nếu khóa bị tiết lộ.

- Năm 1976 Whitfield Diffie và Martin Hellman đã tìm ra một phương pháp mã hóa khác mà có thể giải quyết được hai vấn đề trên, đó là mã hóa khóa công khai (public key cryptography) hay còn gọi là mã hóa bất đối xứng (asymetric cryptography).

- Đây có thể xem là một bước đột phá quan trọng nhất trong lĩnh vực mã hóa

Để khắc phục điểm yếu của mã hóa đối xứng người ta tập trung vào nghiên cứu theo hướng: có phương pháp nào để việc *mã hóa và giải mã dùng hai khóa khác nhau*? Có nghĩa là $C = E(P, K_1)$ và $P = D(C, K_2)$. Nếu thực hiện được như vậy thì chúng ta sẽ có 2 phương án

Phương án 1: người nhận (Bob) giữ bí mật khóa K_2, còn khóa K_1 thì công khai cho tất cả mọi người biết. Alice muốn gởi dữ liệu cho Bob thì dùng khóa K_1 để mã hóa. Bob dùng K_2 để giải mã. Ở đây Trudy cũng biết khóa K_1, tuy nhiên không thể dùng chính K_1 để giải mã mà phải dùng K_2. Do đó chỉ có duy nhất Bob mới có thể giải mã được. Điều này bảo đảm *tính bảo mật* của quá trình truyền dữ liệu. Ưu điểm của phương án này là không cần phải truyền khóa K_1 trên kênh an toàn.

~~$P = D(C, K_1)$~~ $P = D(C, K_2)$

Phương án 2: người gửi (Alice) giữ bí mật khóa K_1, còn khóa K_2 thì công khai cho tất cả mọi người biết. Alice muốn gởi dữ liệu cho Bob thì dùng khóa K_1 để mã hóa. Bob dùng K_2 để giải mã. Ở đây Trudy cũng biết khóa K_2 nên Trudy cũng có thể giải mã được. Do đó phương án này *không đảm bảo tính bảo mật*. Tuy nhiên lại có tính chất quan trọng là *đảm bảo tính chứng thực và tính không từ chối*. Vì chỉ có duy nhất Alice biết được khóa K_1, nên nếu Bob dùng K_2 để giải mã ra bản tin, thì điều đó có nghĩa là Alice là người gửi bản mã. Nếu Trudy cũng có khóa K_1 để gửi bản mã thì Alice sẽ bị quy trách nhiệm làm lộ khóa K_1. Trong phương án này cũng không cần phải truyền K_2 trên kênh an toàn.

Chức thực thông tin

- **Chứng thực thông tin** là thủ tục cho phép các bên giao tiếp xác minh các dữ liệu nhận được là chính xác.
- Hai khía cạnh quan trọng: nội dung không bị thay đổi, xác minh danh tính người gửi, chống thoái thác (giải quyết tranh chấp).

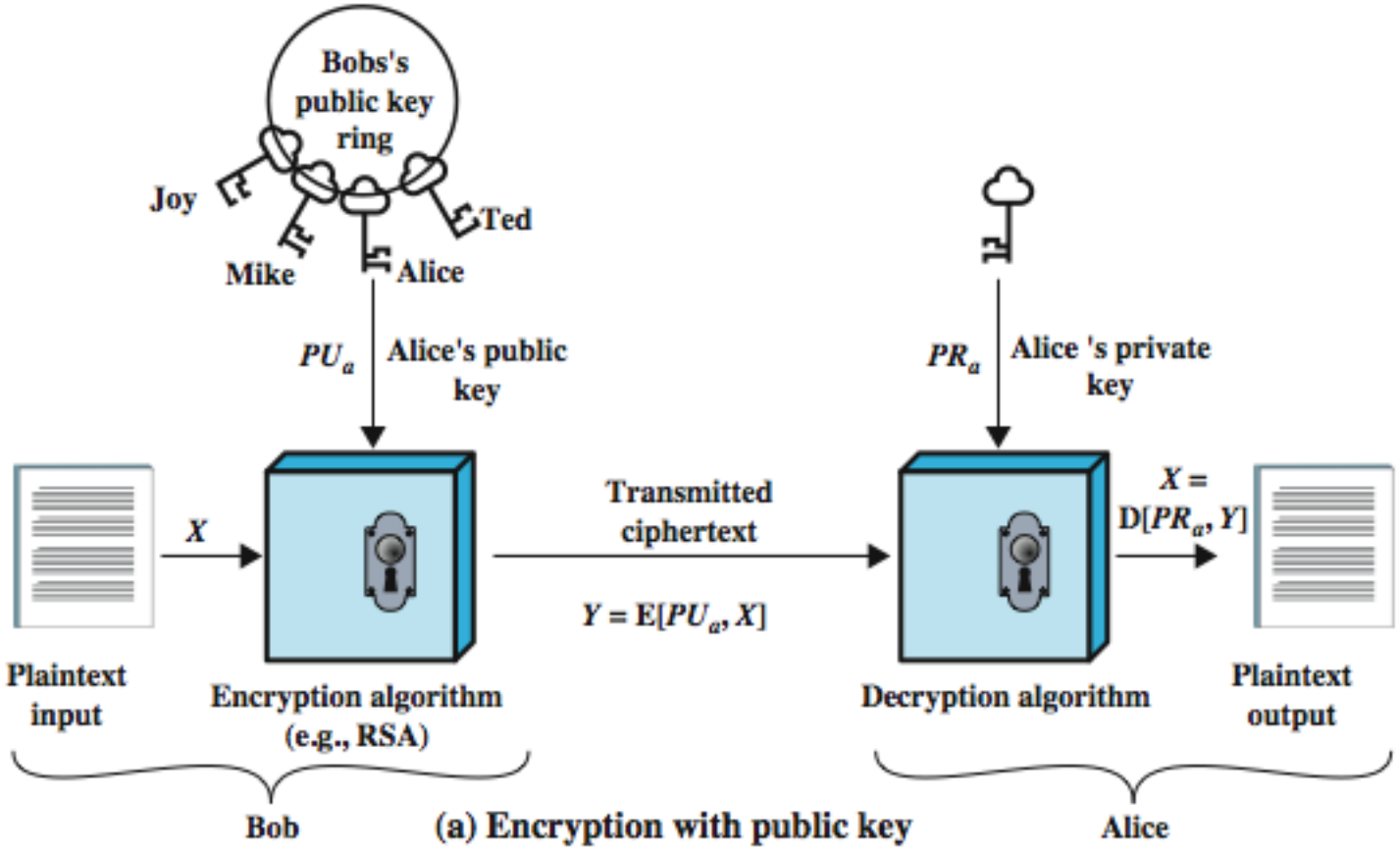
Chức thực thông tin

- Ba chức năng được sử dụng:

- Hàm băm
- Mã hóa thông điệp
- Mã xác thực thông điệp (MAC)

Nguyên lý mã hóa khóa công khai

- Sử dụng 2 khóa: public và private key



RSA

- Đặt tên theo 3 nhà phát minh: Rivest, Shamir & Adleman of MIT in 1977
- Sử dụng 2 khóa có quan hệ toán học với nhau: khóa công khai và khóa bí mật
- **Khóa công khai** được **công bố rộng rãi** cho mọi người và dùng **để mã hóa**
- **Khóa bí mật** được dùng **để giải mã**

Bảo mật, chứng thực và không từ chối với mã hóa khóa công khai

- Alice gửi dữ liệu cho Bob
- Khóa riêng – công khai của Alice là K_{RA}, K_{UA} và của Bob là K_{RB}, K_{UB}
- Alice gửi dữ liệu cho Bob: mã hoá dữ liệu bằng khóa công khai **K_{UB}** của Bob, Bob dùng khóa riêng **K_{RB}** để giải mã.

$C=E(M, K_{UB})$ và $M=D(C, K_{RB})$

Để đảm bảo tính chứng thực (Alice Không từ chối trách nhiệm đã gửi dữ liệu)

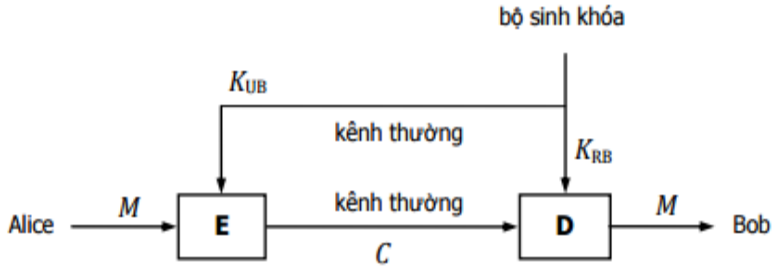
- Alice mã hóa dữ liệu bằng khóa riêng K_{RA} và Bob dùng khóa công khai K_{UA} của Alice để giải mã

$C=E(M, K_{RA})$, $M=D(C, K_{UA})$

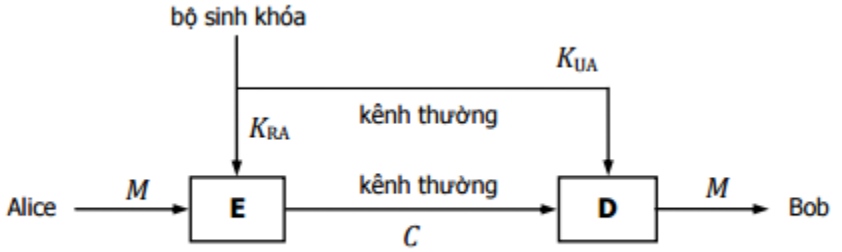
Tính bảo mật: ???

Trudy có thể giải mã C, biết M

Bởi biết khóa công khai



Hình 4-1. Mô hình bảo mật với mã hóa khóa công khai

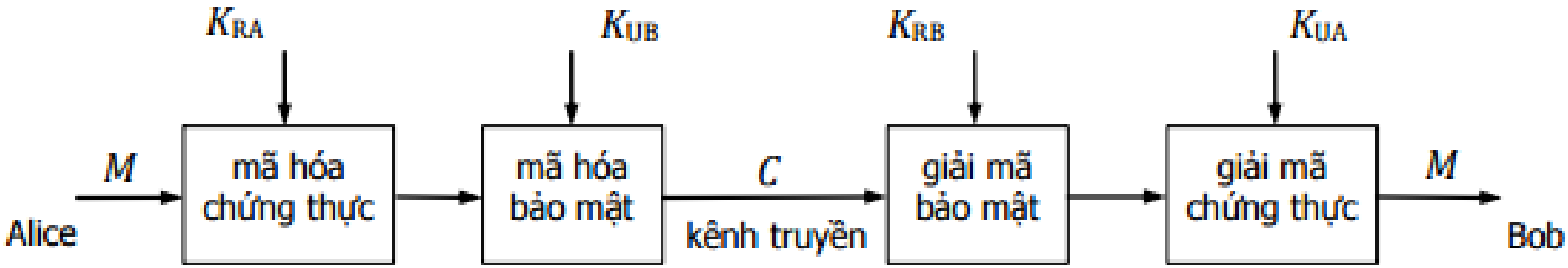


Hình 4-2. Mô hình không thoái thác với mã hóa khóa công khai

Mô hình kết hợp tính bảo mật, chứng thực và không chối bỏ

$$C = E(E(M, K_{RA}), K_{UB})$$

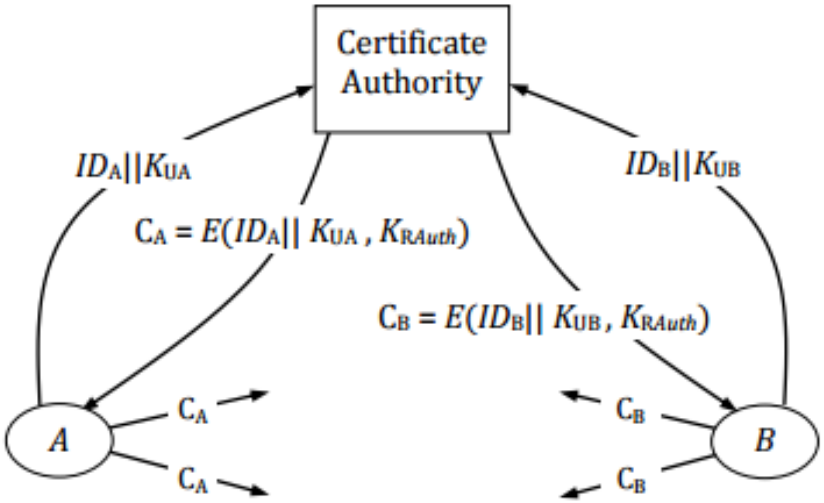
$$M = D(D(C, K_{RB}), K_{UA})$$



Trao đổi khóa

- **Trao đổi khóa công khai** tự phát: có thể mạo danh
- Tổ chức làm nhiệm vụ trung tâm chứng thực: Certificate Authority (CA)

1. Alice gửi định danh ID_A và khóa công khai của mình đến trung tâm chứng thực (TT)
2. TT kiểm tra tính hợp lệ của Alice
3. TT cấp C_A để xác nhận K_{UA} là tương ứng với ID_A. Chứng chỉ được ký chứng thực bằng khóa riêng của TT
4. Alice công khai chứng chỉ C_A
5. Bod muốn trao đổi với Alice thì giải mã C_A bằng khóa công khai của TT để được K_{UA} của Alice



Trao đổi khóa

- Dùng khóa công khai để trao đổi khóa bí mật
- ✓ Thời gian mã hóa và giải mã mã hóa khóa công khai chậm hơn khóa bí mật.
- ✓ Trong thực tế, đối với vấn đề đảm bảo tính bí mật, người ta vẫn sử dụng phương pháp mã hóa đối xứng.
- ✓ Mã hóa khóa công khai được sử dụng để thiết lập khóa bí mật cho mỗi phiên trao đổi dữ liệu (gọi là khóa phiên – session key), các phiên trao đổi khác nhau sẽ dùng các khóa bí mật khác nhau

Phương pháp trao đổi khóa Diffie-Hellman

- Dùng để thiết lập một khóa bí mật giữa người gửi và người nhận (không cần dùng đến khóa công khai)

Trước tiên Alice và Bob sẽ thống nhất sử dụng chung một số nguyên tố p và một số g nhỏ hơn p và là *primitive root* của p (nghĩa là phép toán $g^x \bmod p$ khả nghịch). Hai số p và g không cần giữ bí mật. Sau đó Alice chọn một số a và giữ bí mật số a này. Bob cũng chọn một số b và giữ bí mật số b. Tiếp theo Alice tính và gửi $g^a \bmod p$ cho Bob, Bob tính và gửi $g^b \bmod p$ cho Bob. Trên cơ sở đó Alice tính:

$$(g^b)^a \bmod p = g^{ab} \bmod p$$

Bob tính:

$$(g^a)^b \bmod p = g^{ab} \bmod p$$

Do đó Alice và Bob có chung giá trị $g^{ab} \bmod p$. Giá trị này có thể dùng làm khóa cho phép mã hóa đối xứng.

Như vậy, kẻ phá mã Trudy có thể có được g, p, g^a và g^b . Muốn tính được $g^{ab} \bmod p$, Trudy không thể dùng cách:

$$g^a g^b \bmod p = g^{a+b} \bmod p \neq g^{ab} \bmod p$$

Muốn tính được $g^{ab} \bmod p$, Trudy phải tính được a hoặc được b. Tuy nhiên việc tính a hay b theo công thức:

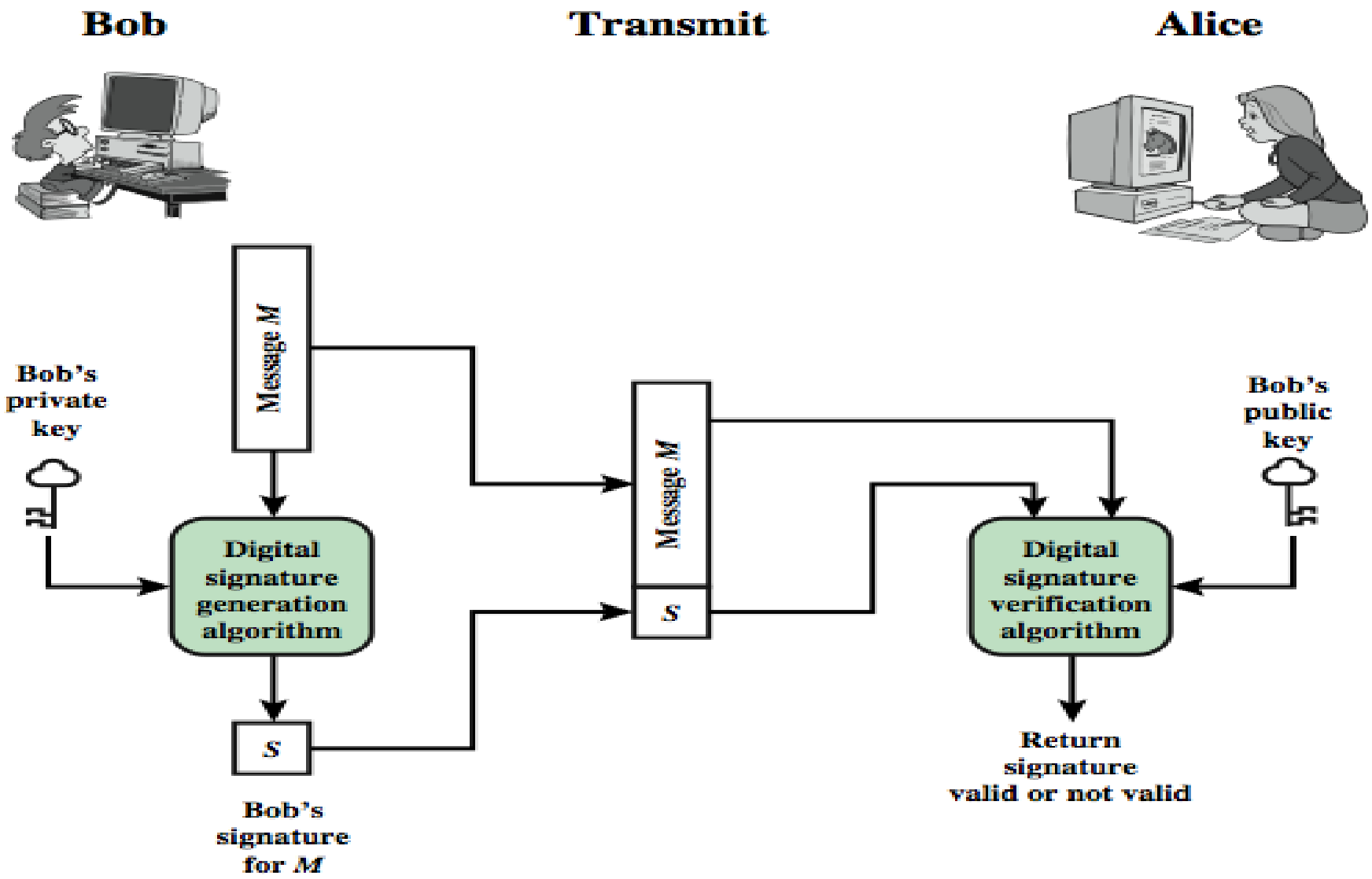
$$a = dlog_{g,p} g^a \quad \text{hay} \quad b = dlog_{g,p} g^b$$

là không khả thi do tính phức tạp của phép logarith rời rạc. Vậy Trudy không thể nào tính được $g^{ab} \bmod p$. Hay nói cách khác, khóa dùng chung được trao đổi bí mật giữa Alice và Bob.

Chữ ký số

- Là thông điệp đã được **"ký"** bằng **khóa bí mật** của người dùng nhằm **xác định người chủ** của thông điệp đó.
- **Mục đích:**
  - Xác thực: ai là chủ thông điệp
  - Tính toàn vẹn: kiểm tra xem thông điệp có bị thay đổi
  - Tính chống thoái thác: ngăn chặn người dùng từ chối đã tạo ra và gửi thông điệp.

Mô hình chữ ký số



Mô hình chữ ký số