MẬT MÃ ỨNG DỤNG TRONG AN TOÀN THÔNG TIN

(Applied Cryptography In Secure Information System)

ThS. Bùi Hữu Đông
buihuudong19@gmail.com
0903.82.36.46

Học viện Kỹ thuật Mật mã, khoa An toàn thông tin

Ngày 7 tháng 12 năm 2020

Buổi 07

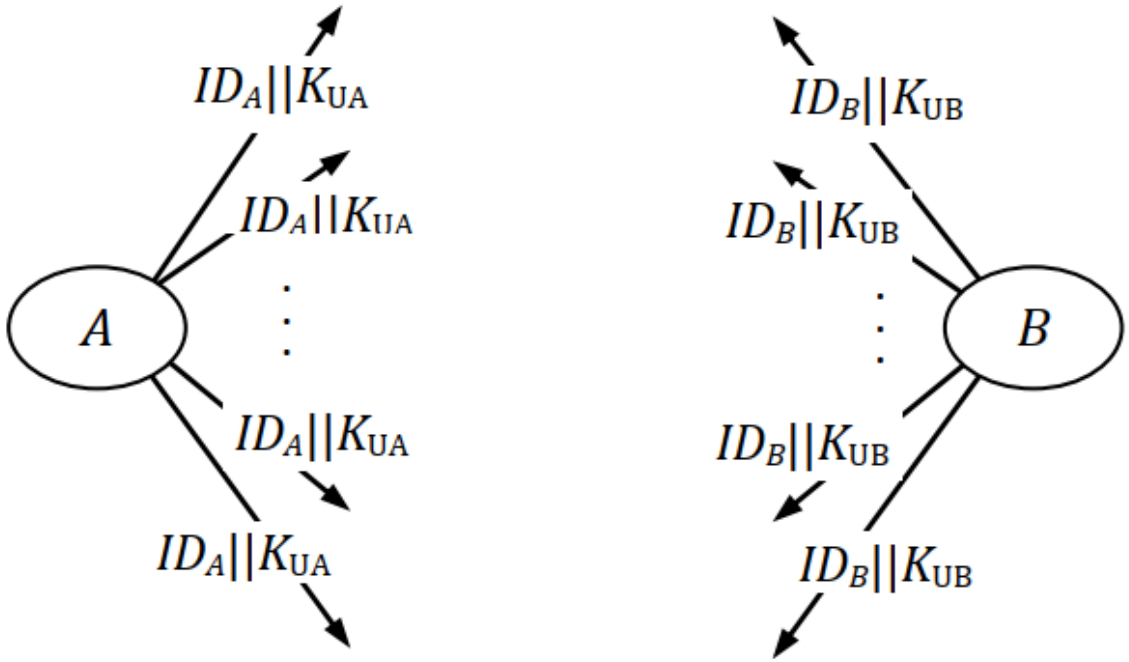
PHƯƠNG PHÁP QUẢN LÝ VÀ PHÂN PHỐI KHÓA

Tổng quan

- Nhược điểm lớn nhất của mã hóa đối xứng là việc chuyển giao, trao đổi khóa giữa các đối tác trong môi trường không tin cậy
- Việc mã hóa bằng hệ mã đối xứng bảo vệ tốt thông tin và tốc độ nhanh
- Nếu dùng mã hóa đối xứng trong an toàn thông tin khi giao dịch với nhiều đối tác => thiết lập những phương thức chuyển giao khóa an toàn.

Trao đổi khóa công khai

- Khi hai người sử dụng muốn truyền dữ liệu với nhau bằng phương pháp mã hóa khóa công khai, trước tiên họ phải trao đổi khóa công khai cho nhau
- Vì là khóa công khai nên không cần giữ bí mật việc trao đổi này và khóa có thể truyền công khai trên các kênh thường
  - Mô hình trao đổi khóa công khai tự phát:



Trao đổi khóa công khai

- *Vấn đề đặt ra theo mô hình trên*:
  - Làm thế nào để chứng thực rằng khóa K_{UB} chính là khóa công khai của người B
  - Kẻ tham mã T có thể mạo danh B bằng cách lấy khóa K_{UT} và nói rằng đó là khóa của người B
- Vì vậy theo mô hình trên, việc chứng thực dựa trên từng cá nhân $=>$ tức là, A muốn gửi message cho B thì phải tin tưởng vào khóa K_{UB} của B và ngược lại
- Để giảm trách nhiệm cho từng cá nhân, một mô hình "chứng chỉ khóa công khai (public-key certificate)" được sử dụng.

Trung tâm chứng thực - Certificate Authority (CA)

- *Mô tả:* Theo mô hình này, có một tổ chức làm nhiệm vụ cấp chứng chỉ được gọi là *trung tâm chứng thực*
- *Các bước cấp chứng chỉ cho người A:*
  - Người A gửi định danh ID_A và khóa công khai K_{UA} của mình đến trung tâm chứng thực (CA)
  - CA chứng nhận kiểm tra tính hợp lệ của người A. Thí dụ: nếu ID_A là 'ACT13 Company' thì người A phải có bằng chứng chứng tỏ mình là công ty ACT13
  - Khi xác nhận đầy đủ thông tin, trung tâm chứng thực cấp một chứng chỉ C_A để xác nhận rằng khóa công khai K_{UA} tương ứng với ID_A

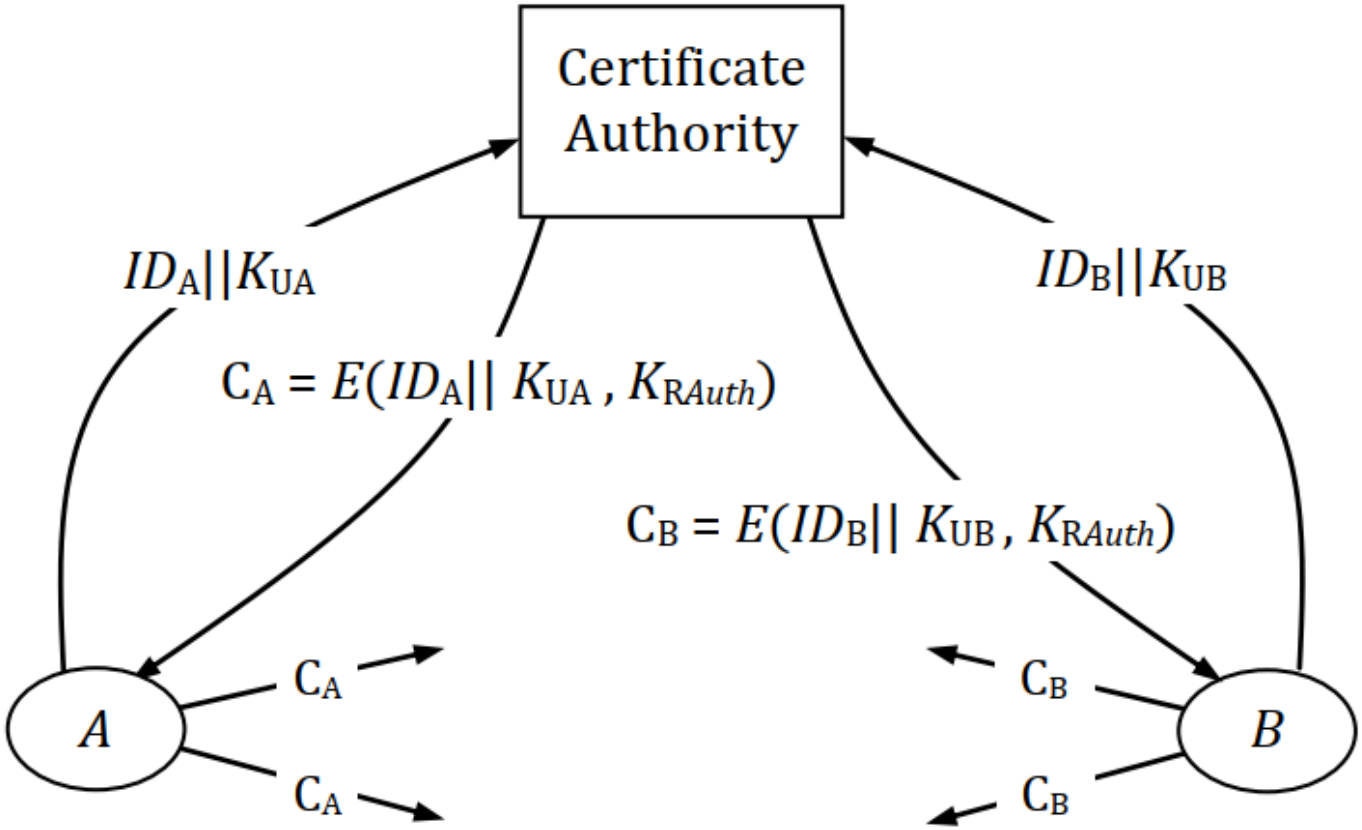
Trung tâm chứng thực - Certificate Authority (CA)

- *Các bước cấp chứng chỉ cho người A <tiếp>:*
  - Chứng chỉ được ký chứng thực bằng khóa riêng của trung tâm => nội dung của chứng chỉ do trung tâm ban hành

$$C_A = E(ID_A||K_{UA}, K_{RAuth})$$

    Với || là phép nối bit
  - Người A công khai chứng chỉ C_A
  - Người B muốn trao đổi với A thì sẽ thực hiện giải mã C_A bằng khóa công khai của trung tâm CA để có được khóa K_{UA} của người gửi A => nếu người B tin tưởng CA thì sẽ tin K_{UA} là tương ứng của ID_A, tức tương ứng với người A

Mô hình trao đổi khóa qua trung tâm CA



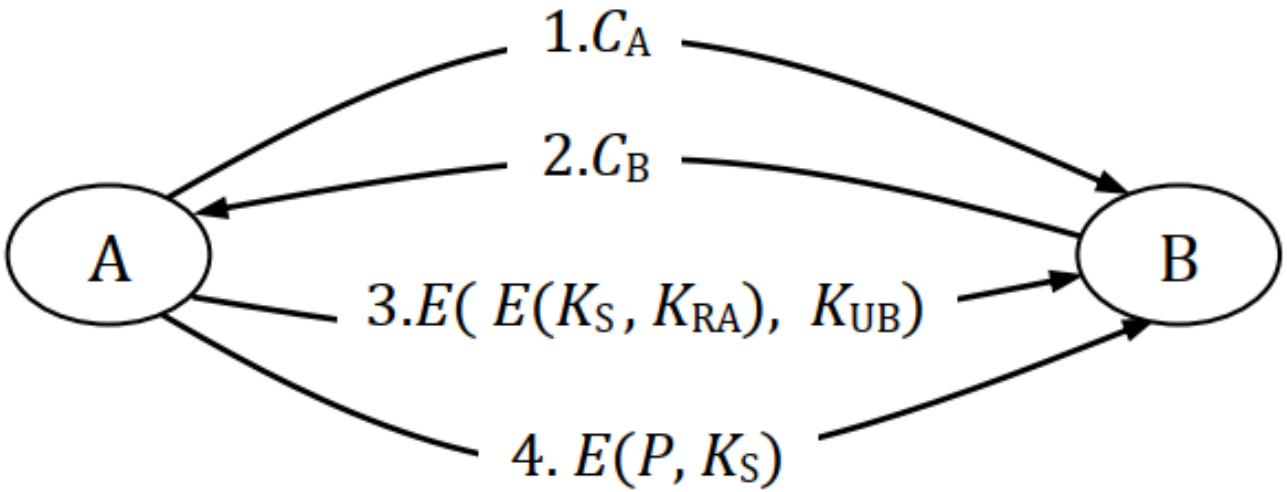
Mô hình trao đổi khóa qua trung tâm CA

- *Nhận xét:* Theo mô hình này, người B muốn gửi thông điệp của người A, C, D,...thì B không cần phải tin tưởng vào khóa công khai của A, C, D... nữa mà chỉ cần tin tưởng vào một đơn vị duy nhất là CA và khóa công khai của CA là đủ.
- Mô hình chứng chỉ khóa công khai đang được áp dụng rộng rãi với chuẩn của chứng chỉ là chuẩn $X.509$
- Hiện nay, trên thế giới có khoảng 80 tổ chức chứng thực chứng chỉ khóa công khai

Trao đổi khóa bí mật

- Do đặc điểm toán học của phương pháp mã hóa công khai, ta thấy thời gian mã hóa và giải mã chậm hơn mã hóa đối xứng
- Trong thực tế, Mã hóa khóa công khai được dùng để thiết lập khóa bí mật cho mỗi phiên trao đổi dữ liệu. Lúc này khóa bí mật được gọi là khóa phiên (session key), các phiên trao đổi dữ liệu khác nhau sẽ dùng các khóa bí mật khác nhau

Mô hình đơn giản thiết lập khóa phiên



- Người A tạo một khóa phiên K_S, mã hóa bằng khóa riêng của người A. Sau đó mã hóa bằng khóa công khai của người B
- Người B giải mã K_S bằng khóa riêng của B và khóa công khai của người A.

Mô hình đơn giản thiết lập khóa phiên

- Nhờ tính bảo mật mà người A biết chỉ có người B mới biết được K_S
- Nhờ tính không từ chối, người B biết rằng ngoài B chỉ có người A mới biết được K_S vì người A khóa riêng để mã hóa $K_S => K_S$ có thể dùng làm khóa bí mật cho mã hóa đối xứng để trao đổi dữ liệu
- Sau phiên trao đổi dữ liệu, K_S được hủy bỏ nên khóa bí mật này sẽ ít có khả năng bị lộ
- Lúc này vai trò của mã hóa khóa công khai không phải là bảo mật dữ liệu nữa (việc này do mã hóa đối xứng đảm trách) mà là bảo đảm tính bí mật của khóa đối xứng, chỉ có A và B biết khóa K_S.

Phương pháp trao đổi khóa Diffie – Hellman

- *Giới thiệu*:
  - Phương pháp trao đổi khóa Diffie-Hellman dùng để thiết lập một khóa bí mật giữa người gởi và người nhận mà không cần dùng đến mã hóa công khai. Nói cách khác, Phương thức Diffie–Hellman cho phép hai đối tác không biết gì với nhau từ trước có thể thỏa thuận với nhau để sử dụng chung một khóa mã bí mật thông qua một môi trường giao dịch không an toàn.
  - Sơ đồ trao đổi khóa này được Whitfield Diffie và Martin Hellman công bố lần đầu tiên vào năm 1976
  - Đến năm 2002, Hellman đề nghị gọi tên thuật toán là trao đổi khóa Diffie-Hellman-Merkle để ghi nhận đóng góp của Ralph Merkle
  - Phương pháp này dùng hàm một chiều làm hàm logarith rời rạc item[○]

    Diffie-Hellman không có ý nghĩa về mặt mã hóa giống như RSA

Phương pháp trao đổi khóa Diffie – Hellman

- *Mô tả hoạt động*:
  - Trước tiên An và Bình sẽ thống nhất sử dụng chung một số nguyên tố p và một số g với $g < p$, g là căn nguyên thủy (primitive root) của p nghĩa là $g^x mod\ p$ khả ngịch
  - Hai số p và g không cần giữ bí mật
  - Sau đó, An chọn một số a, Bình chọn một số b và cả An và Bình đều giữ bí mật 2 số này.
  - Tiếp theo, An tính $g^a mod\ p$ và gửi cho Bình. Bình tính $g^b mod\ p$ và gửi cho An

Phương pháp trao đổi khóa Diffie – Hellman

- *Mô tả hoạt động <tiếp>*:
  - Khi nhận được từ Bình gửi, An tính:

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

  - Khi nhận được từ An, Bình tính:

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

  - Vì An và Bình có chung giá trị $g^{ab} \ mod \ p$, giá trị này có thể dùng làm khóa cho phép mã hóa đối xứng.

Phương pháp trao đổi khóa Diffie – Hellman

- *Mô tả hoạt động <tiếp>*:
  - Kẻ phá mã T có thể có được g, p, g^a và g^b. Muốn tính được $g^{ab}\ mod\ p$ T không thể dùng cách:

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

  - Muốn tính được $g^{ab}\ mod\ p$ thì T phải tìm được a và b. Tuy nhiên, việc tính a và b theo công thức:

$$a = dlog_{g,p} g^a, b = dlog_{g,p} g^b$$

    là không khả thi do tính phức tạp của phép logarith rời rạc
  - Do không tính được $g^{ab}\ mod\ p$, nói cách khác, khóa dùng chung được trao đổi bí mật giữa An và Bình.

Thí dụ - Diffie – Hellman

- Bảng tổng quát:

An				Bình		
Bí mật	Công khai	Tính toán	Gửi	Tính toán	Công khai	Bí mật
a	p, g		p, g →			b
a	p, g, A	$g^a \bmod p = A$	A →		p, g	b
a	p, g, A		← B	$g^b \bmod p = B$	p, g, A, B	b
a, s	p, g, A, B	$B^a \bmod p = s$		$A^b \bmod p = s$	p, g, A, B	b, s

Thí dụ - Diffie – Hellman

- An và Bình thống nhất dùng $p = 23$ và $g = 5$
- An chọn số nguyên bí mật $a = 6$ và gửi cho Bình số $A = g^a \ mod \ p$ (công khai)

$$A = 5^6 \ mod \ 23 = 15.625 \ mod \ 23 = 8$$

- Bình chọn số nguyên bí mật $b = 15$ và gửi cho An số $B = g^b \ mod \ p$

$$B = 5^{15} \ mod \ 23 = 30.517.578.125 \ mod \ 23 = 19$$

- An tính $s = B^a \ mod \ p = 19^6 \ mod \ 23 = 47.045.881 \ mod \ 23 = 2$

Thí dụ - Diffie – Hellman

- Bình tính toán
  $s = A^b \ mod \ p = 8^{15} \ mod \ 23 = 35.184.372.088.832 \ mod \ 23 = 2$
- An và Bình chia sẻ nhau con số bí mật: $s = 2$ Khi đó nếu bất kỳ người nào biết được cả hai số nguyên riêng của cả An và Bình thì cũng đều có thể tính được s như sau:

  $s = 5^{6*15} \ mod \ 23 = 5^{15*6} \ mod \ 23 = 5^{90} \ mod \ 23 = 2$

Dùng khóa công khai để bảo vệ khóa Diffie – Hellman (D-H)

- Dù D-H khá an toàn, tuy nhiên, thuật toán Diffie-Hellman lại thất bại đối với cách tấn công kẻ-đứng-giữa. Tức kẻ phá mã T sẽ đứng giữa An và Bình, để chặn thông điệp giữa An và Bình. Có thể giả mạo thông điệp mà cả An và Bình đều không biết.
- Vì thế, T có thể thiết lập khóa Diffie-Hellman $g^{at}\ mod\ p$ với An và khóa $g^{bt}\ mod\ p$ với Bình.
- Khi An gửi dữ liệu, T giải mã bằng $g^{bt}\ mod\ p$ sau đó mã hóa lại bằng $g^{bt}\ mod\ p$ và gửi cho Bình $=>$ cả An và Bình không hề biết còn kẻ T thì xem trộm được thông điệp.

Dùng khóa công khai để bảo vệ khóa Diffie – Hellman (D-H)

- Mô hình truyền dữ liệu bị T đánh cắp:

Dùng khóa công khai để bảo vệ khóa Diffie – Hellman (D-H)

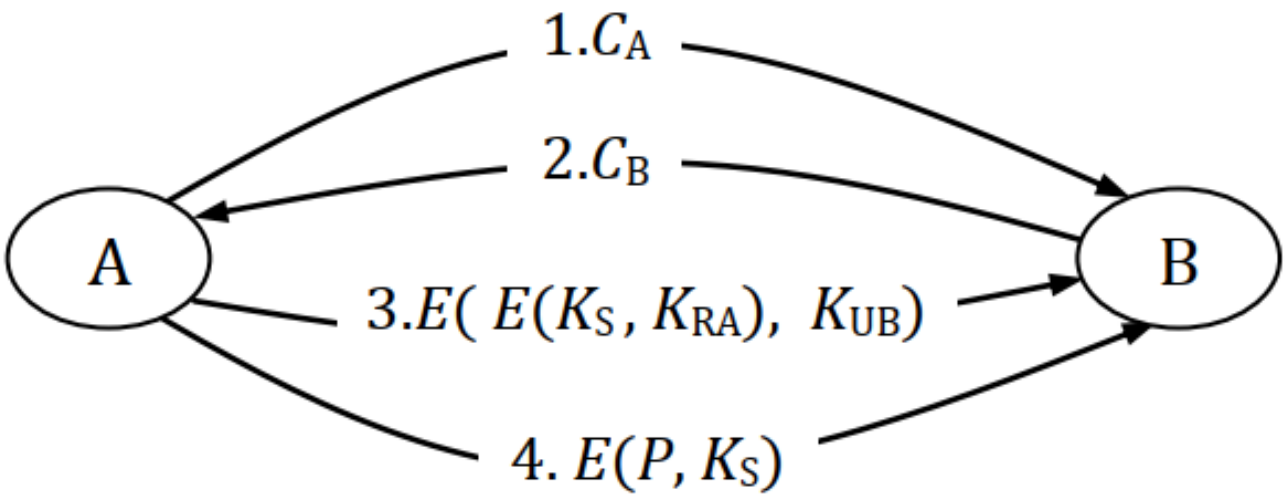
- Để an toàn, quá trình thiết lập khóa Diffie-Hellman vẫn phải được mã hóa bằng một khóa công khai

  Lúc này một câu hỏi được đặt ra là nếu đã được bảo vệ bằng khóa công khai rồi, thì có thể chọn khóa đối xứng bất kỳ, cần gì chọn khóa Diffie-Hellman?

- Tuy nhiên có một số trường hợp, khi mà cách thức tấn công kẻ-đứng-giữa không thể thực hiện được, thì phương thức Diffie-Hellman tỏ ra rất hữu dụng

Dùng khóa công khai để bảo vệ khóa Diffie – Hellman (D-H)

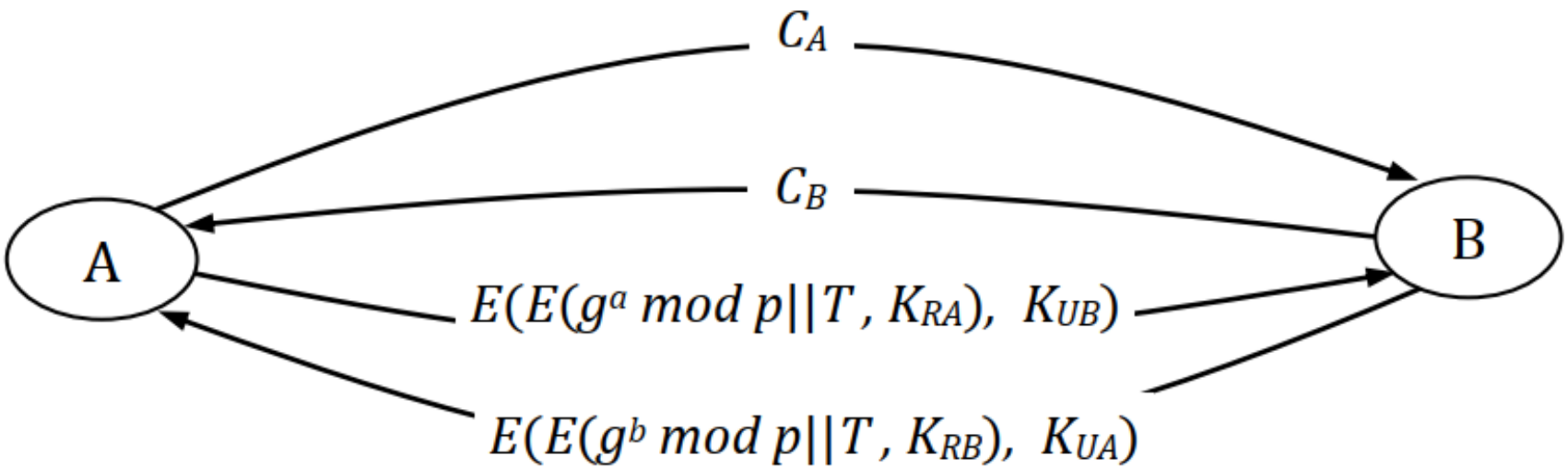
- Theo mô hình thiết lập khóa phiên



Giả sử T ghi nhận lại hết tất cả các thông điệp giữa An và Bình. Sau này nếu T phát hiện ra được khóa riêng K_{RA} và K_{RB} của An và Bình, T có thể khôi phục lại được khóa đối xứng K_S => Có thể phục lại các bản rõ mà được mã hóa bằng khóa K_S

Dùng khóa công khai để bảo vệ khóa Diffie – Hellman (D-H)

- *Mô hình Diffie-Hellman được bảo vệ bằng mã hóa khóa công khai*:



Dùng khóa công khai để bảo vệ khóa Diffie – Hellman (D-H)

- Trong mô hình trên, dù cho sau này T phát hiện ra được khóa riêng K_{RA} và K_{RB} của An và Bình và T tìm ra được $g^a \ mod \ p$ và $g^b \ mod \ p$
- Tuy vậy, T cũng không thể nào khôi phục lại được khóa bí mật $g^{ab} \ mod \ p => $ Không thể khôi phục bản rõ
- Đây chính là ý nghĩa của phương pháp Diffie-Hellman.

Luyện tập

1. Hàm một chiều là gì? Cho ví dụ về hàm một chiều
2. Nêu nguyên tắc của mã hóa khóa công khai? Tại sao trong mã hóa khóa công khai không cần dùng đến kênh an toàn để truyền khóa?
3. Ngoài vấn đề truyền khóa, mã hóa khóa công khai còn ưu điểm hơn mã hóa đối xứng ở điểm nào?
4. Diffie-Hellman có phải là một phương pháp mã hóa khóa công khai và Diffie-Hellman là gì?
5. Nghiên cứu thêm thuật toán Miller-Rabin để kiểm tra một số nguyên n cho trước có phải là nguyên tố hay không?