



ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

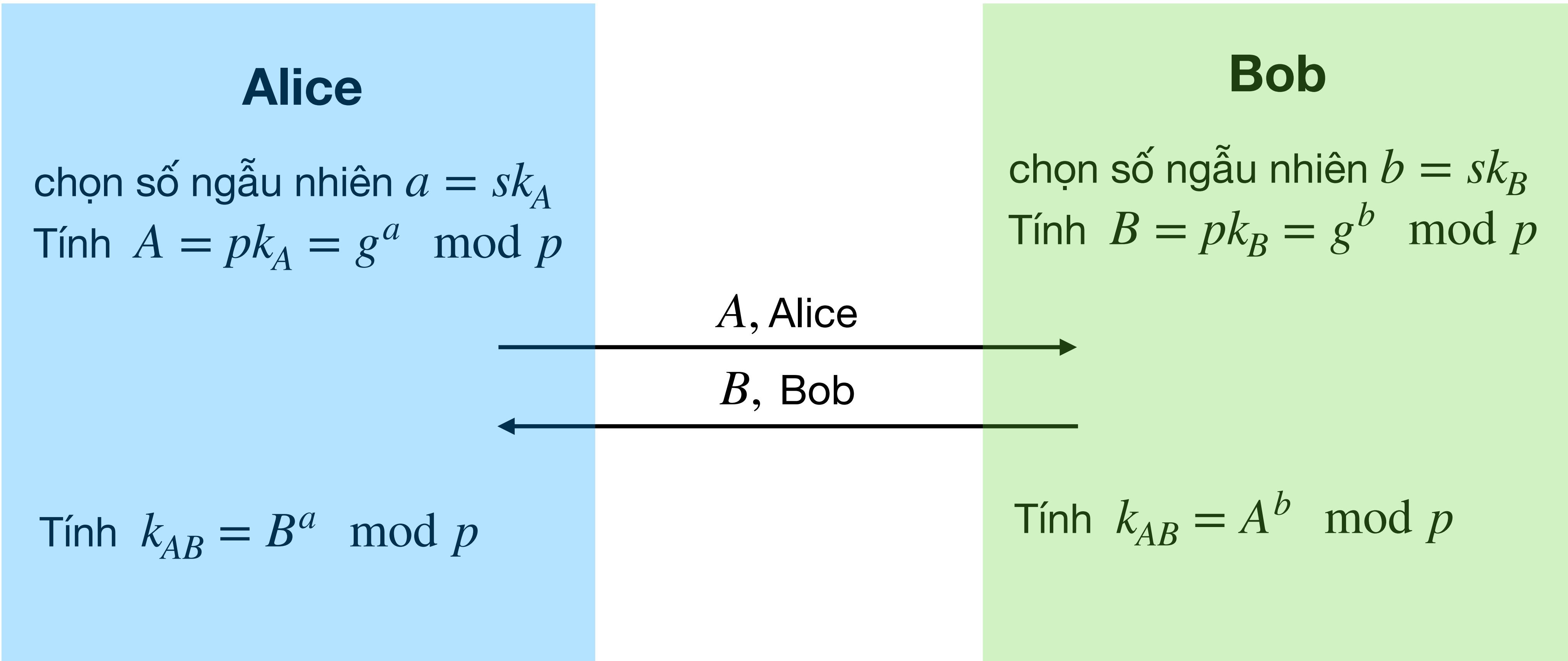
Nhập môn An toàn thông tin

Chứng chỉ số và
cơ sở hạ tầng khoá công khai

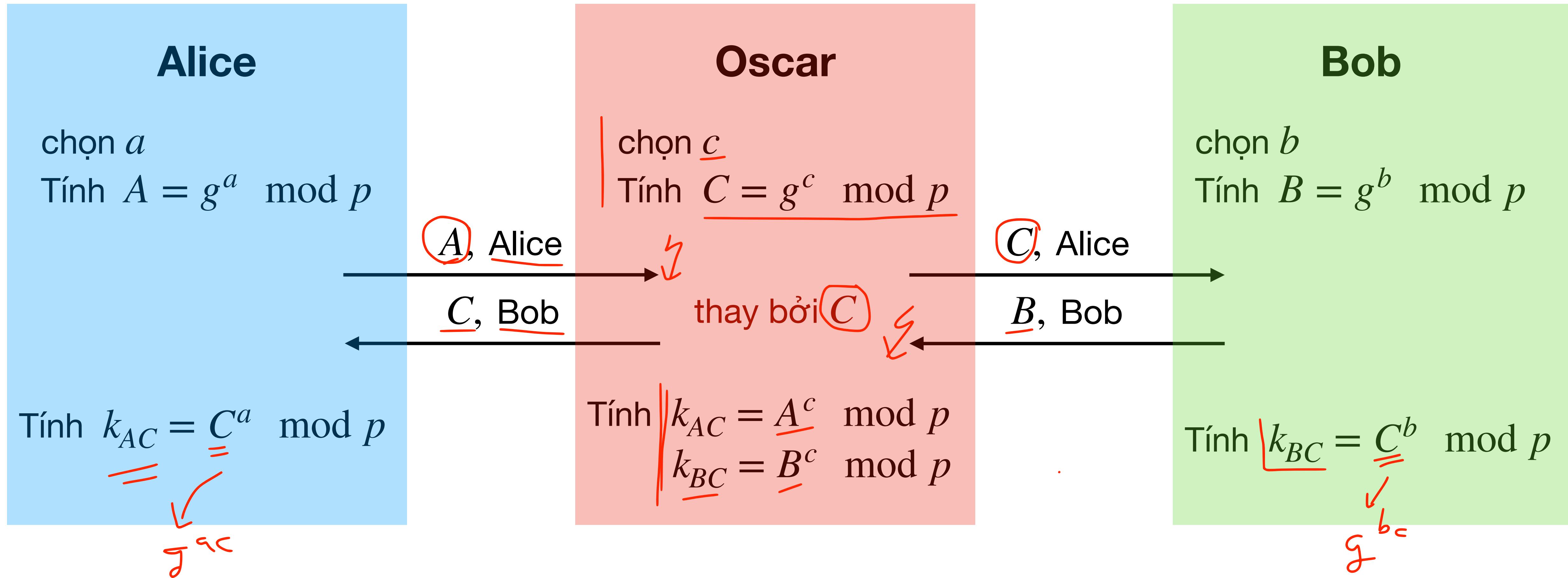
Nội dung

- **Chứng chỉ số**
- Cơ sở hạ tầng khoá công khai

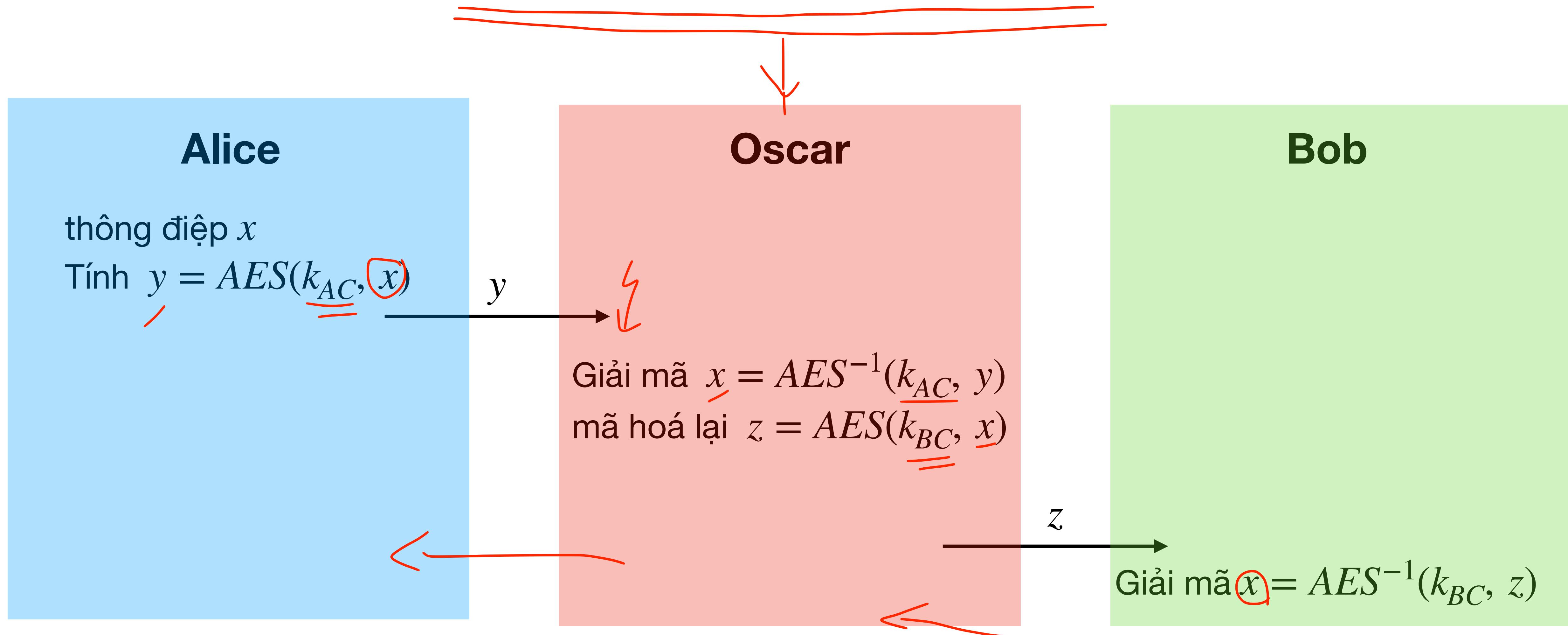
Giao thức trao đổi khoá Diffie-Hellman



Man-in-the-Middle Attack



Sau khi Man-in-the-Middle Attack



Vấn đề

- Khoá của người dùng Alice:

$$k_A = (\underline{pk}_A, \underline{ID}_A)$$

với ID_A là thông tin định danh, ví dụ địa chỉ IP hoặc tên kèm ngày sinh; và
khoá công khai pk_A là một xâu nhị phân (độ dài 2048 bit).

- Khi Oscar thực hiện tấn công, anh ta phải thay đổi khoá thành:

$$k = (\cancel{\underline{pk}_O}, \underline{ID}_A) \leftarrow$$

- **Giải pháp:** Phải xác thực cặp $(\underline{pk}_x, \underline{ID}_x)$ là “hợp lệ”.

Giải pháp

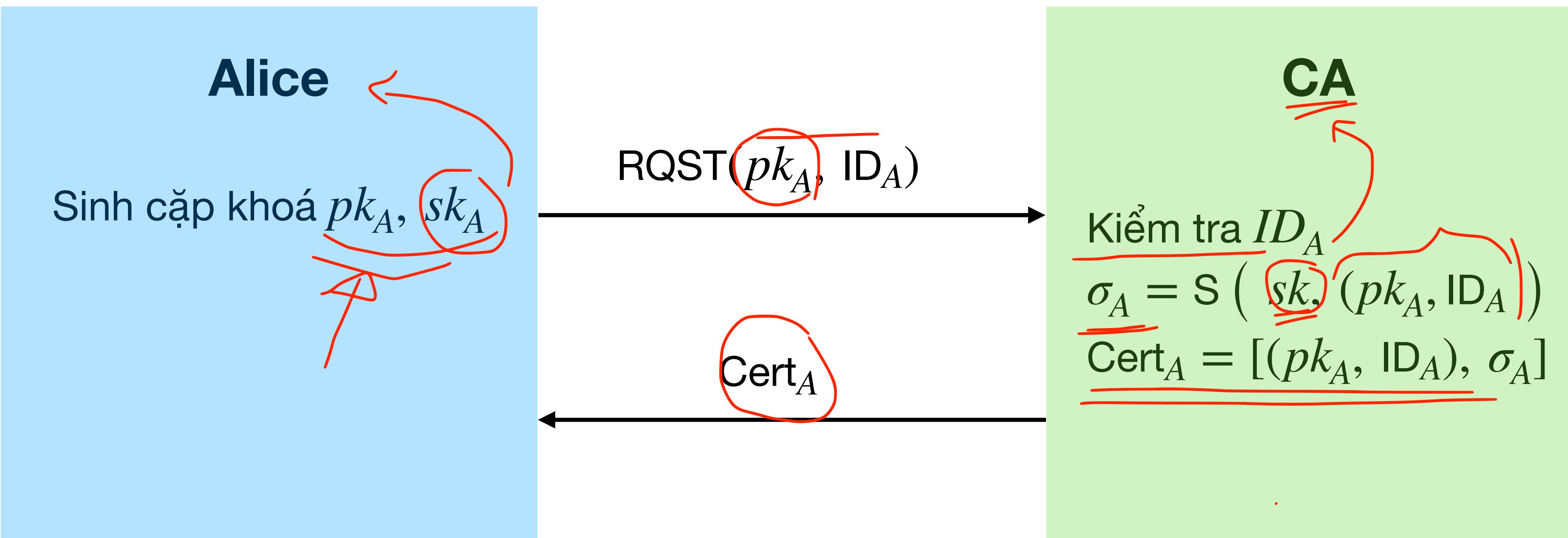
- Chứng chỉ số cho người dùng Alice:

$$\text{Cert}_A = [(pk_A, ID_A), \underline{\sigma}]$$

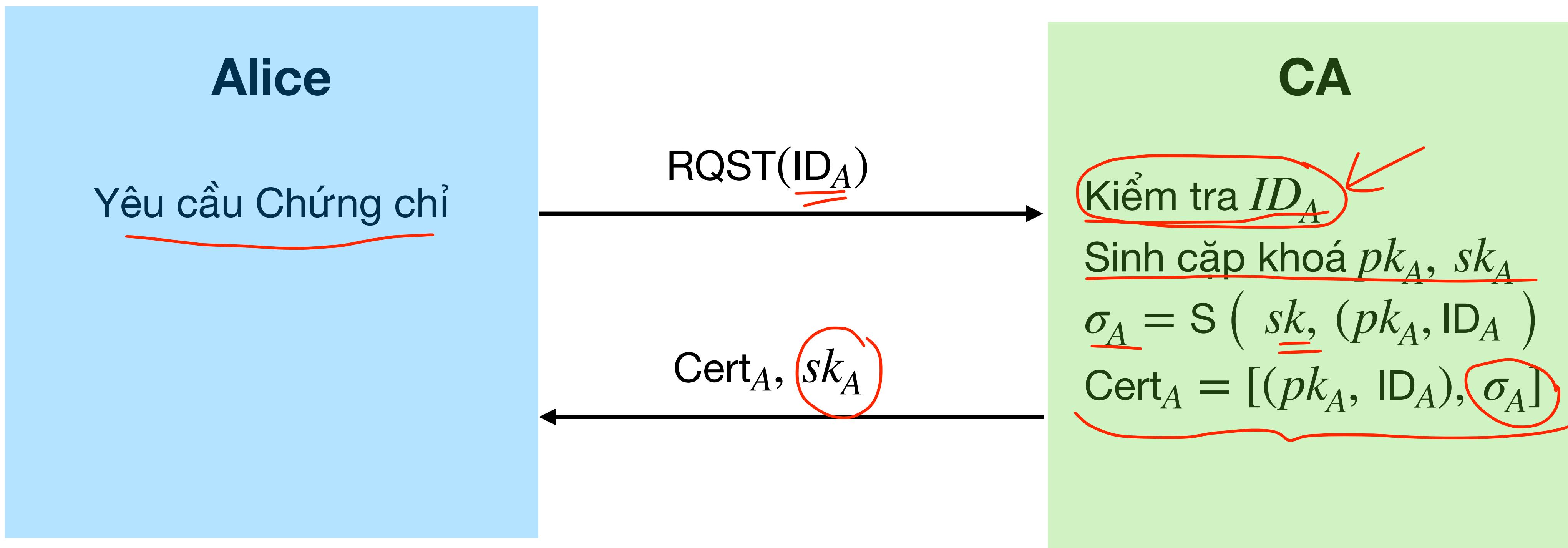
với $\underline{\sigma} = S(\underline{sk}, (pk_A, ID_A))$ là chữ ký số tạo bởi người có thẩm quyền cấp Chứng chỉ số (CA, Certificate Authority)

- **Chứng chỉ số gắn định danh của người dùng với khoá công khai của anh ta**

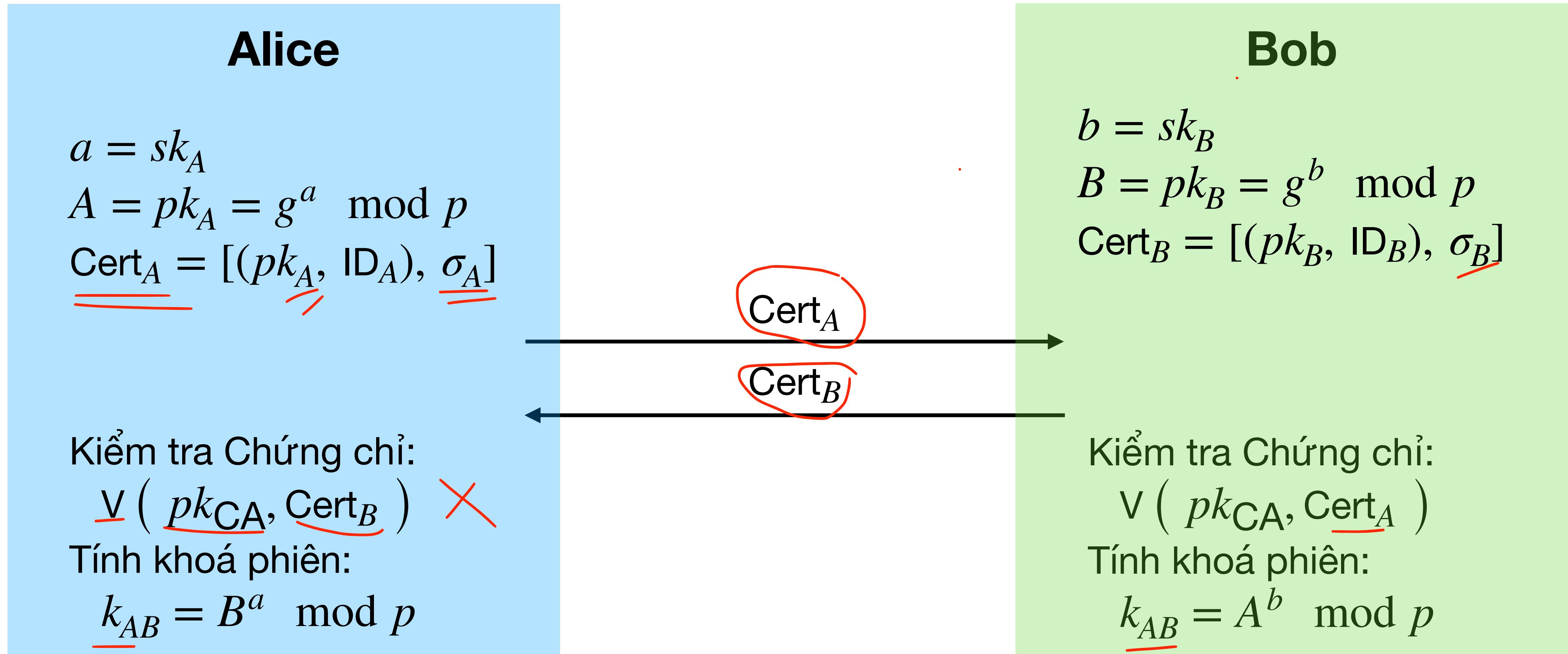
Sinh Chứng chỉ số với khoá người dùng cấp



Sinh Chứng chỉ và khoá



Trao đổi khoá Diffie-Hellman với Chứng chỉ số



Nội dung

- Chứng chỉ số
 - Cơ sở hạ tầng khoá công khai
-

Hạ tầng khoá công khai

- Hệ thống gồm các bên có thẩm quyền xác thực khoá công khai (CA)
- cùng với cơ chế liên quan gọi là **cơ sở hạ tầng khoá công khai**

Chứng chỉ số X509

- **Certificate Algorithm:** Thuật toán ký. ví dụ: RSA với SHA-1 hoặc (EC)DSA với SHA-2
- **Issuer:** Có nhiều công ty và tổ chức cấp Chứng chỉ số. Trường này xác định ai đã cấp Chứng chỉ này.
- **Period of Validity:** Chứng chỉ số thường chỉ có giá trị trong một khoảng thời gian nhất định.

Serial Number
Certificate Algorithm: - Algorithm - Parameters
Issuer
Period of Validity: - Not Before Date - Not After Date

Chứng chỉ số X509 (tiếp)

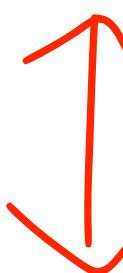
- **Subject:** Thông tin về ID_A hoặc ID_B như trong ví dụ trước. Thường xác định thông tin như tên người trong tổ chức.
- **Subject's Public Key:** Khoá công khai được xác thực bởi Chứng chỉ. Gồm dãy bit tương ứng với khoá công khai và thuật toán (ví dụ: Diffie-Hellman) và tham số thuật toán.
- **Signature:** Chữ ký trên mọi trường của Chứng chỉ.

Subject
Subject's Public Key: <ul style="list-style-type: none">- Algorithm- Parameters- Public Key
Signature

Ví dụ: Chứng chỉ số X.509

▼ Details

Subject Name	
Common Name	mail.google.com
Issuer Name	
Country or Region	US
Organization	Google Trust Services LLC
Common Name	GTS CA 1C3
Serial Number	68 FE 3F 57 2A 7A 32 EA 0A 00 00 00 00 CE 57 C5
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	None
Not Valid Before	Monday, 3 May 2021 at 18:24:58 Indochina Time
Not Valid After	Monday, 26 July 2021 at 18:24:57 Indochina Time



Ví dụ: Chứng chỉ số X.509

Public Key Info

Algorithm Elliptic Curve Public Key (1.2.840.10045.2.1)

Parameters Elliptic Curve secp256r1 (1.2.840.10045.3.1.7)

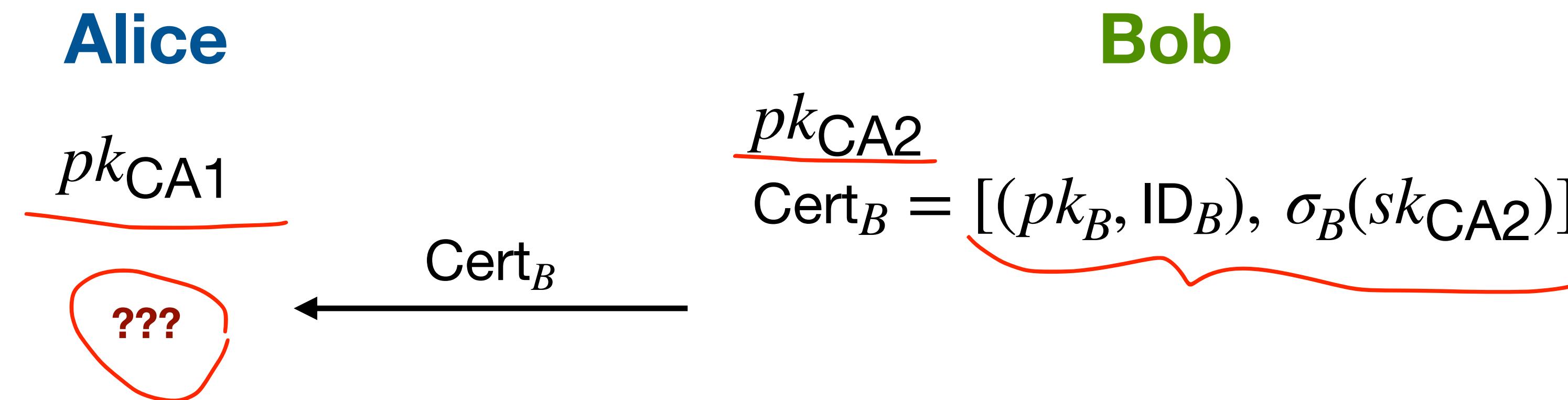
Public Key 65 bytes : 04 E8 C8 1F 1E 31 04 F4 ...

Key Size 256 bits

Key Usage Encrypt, Verify, Derive

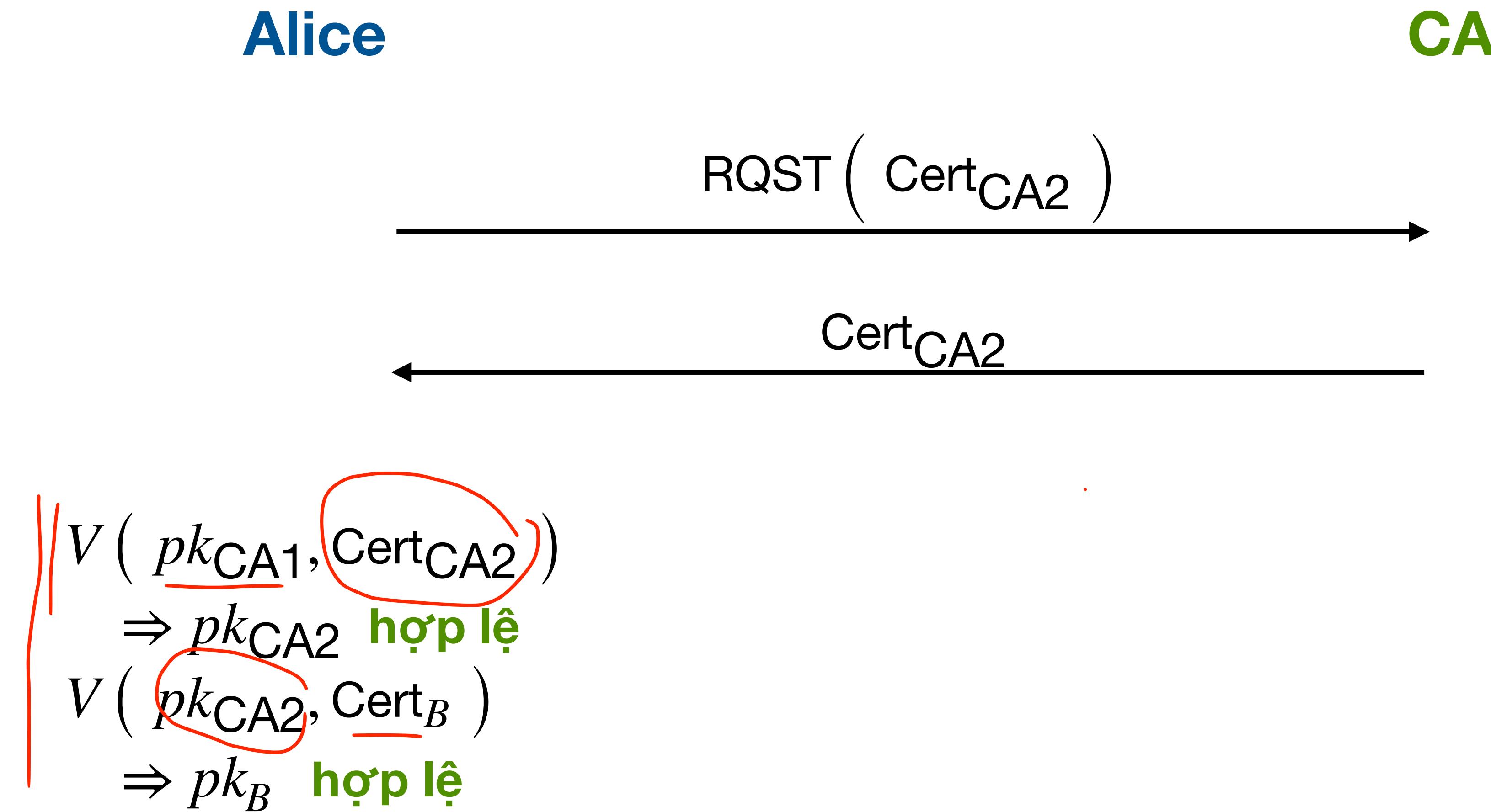
Signature 256 bytes : 96 AF C4 29 E8 4E 26 A4 ...

Dãy CA



- Chứng chỉ số của Alice được cấp bởi CA1
- CA1 cấp chứng chỉ số uỷ quyền cho CA2 được phép xác thực khoá công khai.
- Chứng chỉ số của Bob được cấp bởi CA2

Kiểm tra khoá công khai của CA





25
YEARS ANNIVERSARY
SOICT

VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY

