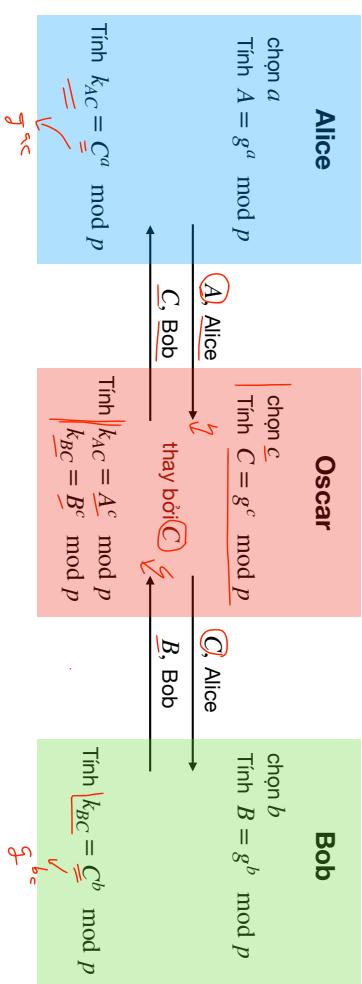


Nội dung

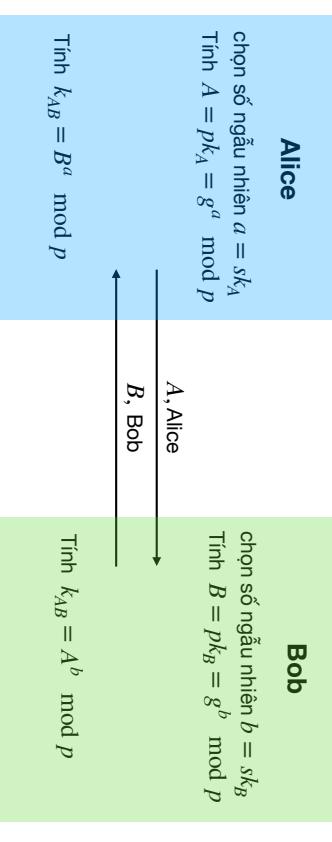
Man-in-the-Middle Attack

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



Giao thức trao đổi khoá Diffie-Hellman

Nhập môn An toàn thông tin
Chứng chỉ số và
cơ sở hạ tầng khoá công khai



Sinh Chứng chỉ số với khoá người dùng cấp

Vấn đề

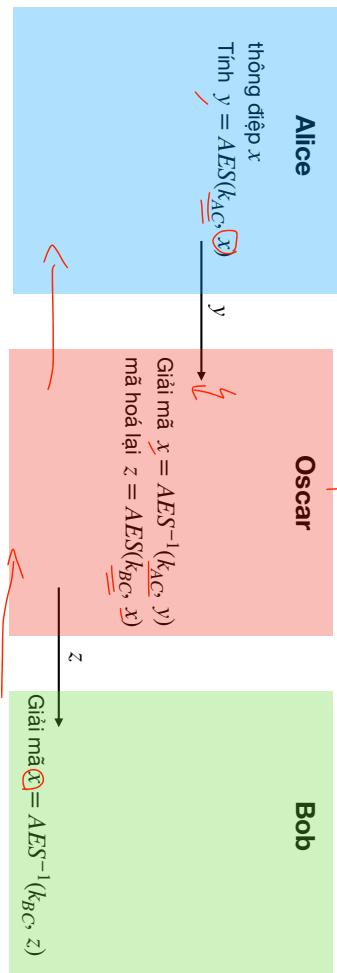
- Khoá của người dùng Alice:

$k_A = (pk_A, ID_A)$
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:

$$k = (pk_O, ID_A)$$

- Giải pháp:** Phải xác thực cặp (pk_X, ID_X) là “hợp lệ”.



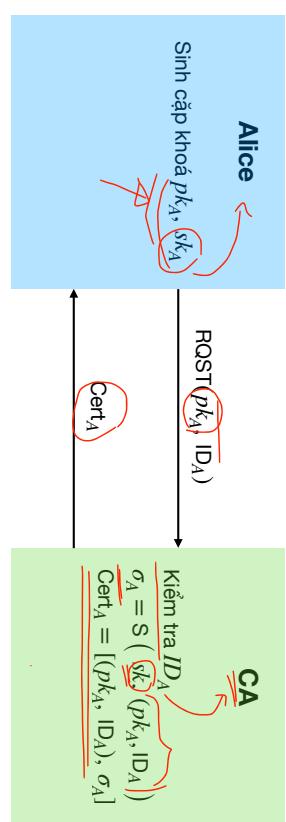
Sau khi Man-in-the-Middle Attack

Giải pháp

- Chứng chỉ số** cho người dùng Alice:

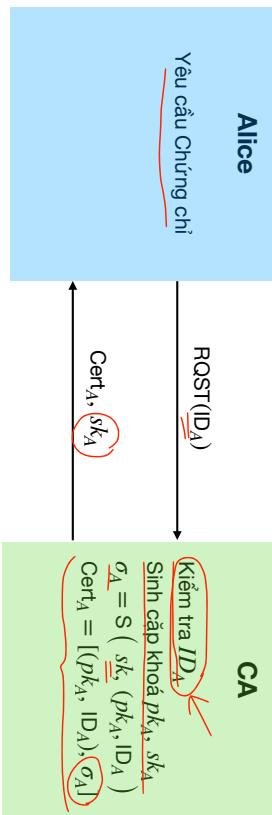
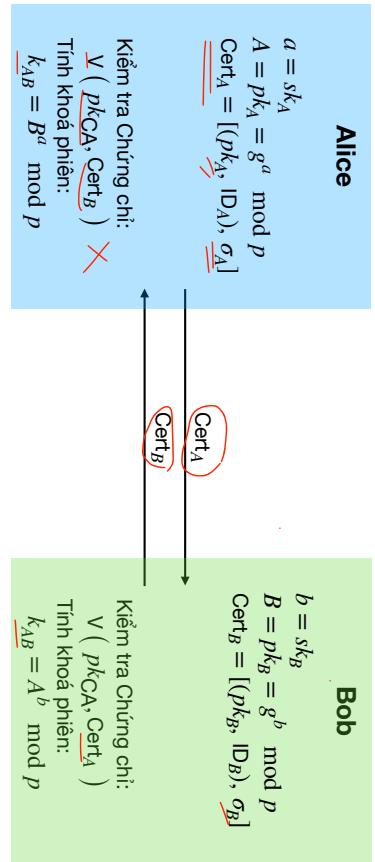
$Cert_A = [(pk_A, ID_A), \sigma]$
với $\sigma = S(sk, (pk_A, ID_A))$ là chữ ký số tạo bởi người có thẩm quyền
cấp Chứng chỉ số (CA, Certificate Authority)

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



Trao đổi khoá Diffie-Hellman với Chứng chỉ số

Hạ tầng khoá công khai



Nội dung

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

Chứng chỉ số X509 (tiếp)

Ví dụ: Chứng chỉ số X.509

Ví dụ: Chứng chỉ số X.509

Subject
Subject's Public Key: - Algorithm - Parameters - Public Key
Signature

- 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:** Khoa công khai được xác thực bởi Chứng chỉ. Gồm dây bit tương ứng với khóa công khai và thuật toán (ví dụ: Diffie-Hellman) và tham số thuật toán.
- Signature:** Chữ ký trên mọi trường của Chứng chỉ.

Public Key Info	
Algorithm	Elliptic Curve Public Key (1.2.840.10045.3.1.7)
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 ...

- 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.

Kiểm tra khoá công khai của CA

Alice

CA2

RQST(Cert_{CA2})

Cert_{CA2}

$V(pk_{CA1}, Cert_{CA2})$
 $\Rightarrow pk_{CA2}$ hợp lệ
 $V(pk_{CA2}, Cert_B)$
 $\Rightarrow pk_B$ hợp lệ

Dãy CA

Alice

Bob

pk_{CA1}
???

$Cert_B$

pk_{CA2}
 $Cert_B = [(pk_B, ID_B), \sigma_B(sk_{CA2})]$

- Chứng chỉ số của Alice được cấp bởi CA1

- CA1 cấp chứng chỉ số uỷ quyền cho CA2

- Chứng chỉ số của Bob được cấp bởi CA2

