# BÀI 4.
# GIAO THỨC MẬT MÃ

Bùi Trọng Tùng,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội



## Nội dung

- Tổng quan về giao thức mật mã
- Các giao thức trao đổi khóa
- Các giao thức chữ ký điện tử

# 1. TỔNG QUAN VỀ GIAO THỨC MẬT MÃ

3

## Giao thức mật mã là gì?

- Chúng ta đã biết về "mật mã" và các ứng dụng của nó:
  - Bảo mật
  - Xác thực
- Nhưng chúng ta cần biết "Sử dụng mật mã như thế nào?"
  - Hệ mật mã an toàn chưa đủ để làm cho quá trình trao đổi thông tin an toàn
  - Cần phải tính đến các yếu tố, cá nhân tham gia không trung thực
- *Giao thức là một chuỗi các bước thực hiện mà các bên phải thực hiện để hoàn thành một tác vụ nào đó.*
  - Bao gồm cả quy cách biểu diễn thông tin trao đổi
- *Giao thức mật mã: giao thức sử dụng các hệ mật mã để đạt được các mục tiêu an toàn bảo mật*

4

## Các thuộc tính của giao thức mật mã

- Các bên tham gia phải hiểu về các bước thực hiện giao thức
- Các bên phải đồng ý tuân thủ chặt chẽ các bước thực hiện
- Giao thức phải rõ ràng, không nhập nhằng
- Giao thức phải đầy đủ, xem xét mọi tình huống có thể
- ***Với giao thức mật mã: Giao thức phải được thiết kế để khi thực hiện không bên nào thu được nhiều lợi ích hơn so với thiết kế ban đầu.***

5

## Yêu cầu Perfect Forward Secrecy

- Một giao thức cần đảm bảo an toàn cho khóa phiên ngắn(short-term key) trong các phiên làm việc trước là an toàn khi khóa phiên dài (long-term key) không còn an toàn

6

## Tấn công khóa đã biết (known-key)

- Sử dụng sự mất an toàn của khóa phiên trong các phiên làm việc trước để tấn công các phiên làm việc tới.

7

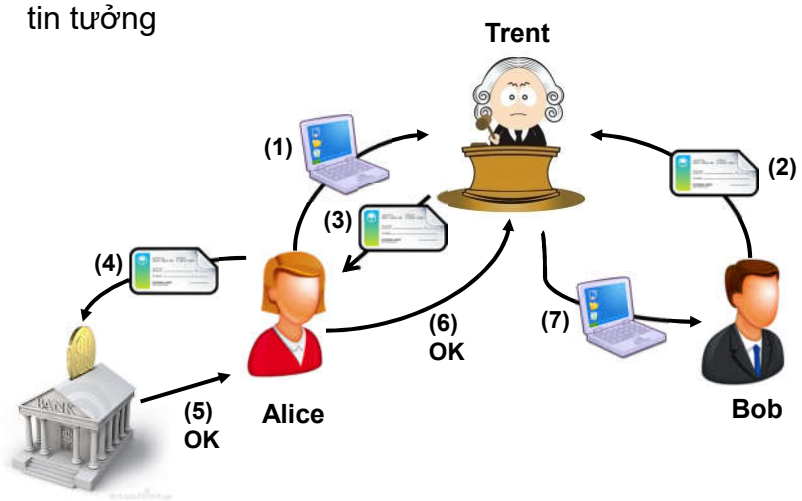
## Giao thức có trọng tài(Trusted arbitrator)

- Trọng tài là bên thứ 3 thỏa mãn:
  - Không có quyền lợi riêng trong giao thức
  - Không thiên vị
- Các bên cần tin tưởng vào trọng tài
  - Mọi thông tin từ trọng tài là đúng và tin cậy
  - Trọng tài luôn hoàn thành đầy đủ nhiệm vụ trong giao thức
- Ví dụ: Alice cần bán một chiếc máy tính cho Bob, người sẽ trả bằng séc
  - Alice muốn nhận tờ séc trước để kiểm tra
  - Bob muốn nhận  máy tính trước khi giao séc

8

# Giao thức có trọng tài – Ví dụ

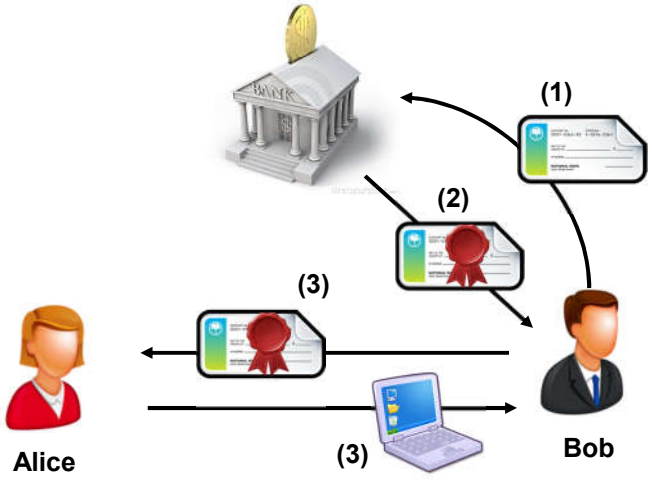
- Alice và Bob tin tưởng vào Trent-Bên thứ 3 mà cả 2 cùng tin tưởng




9

# Giao thức có trọng tài – Ví dụ

- Alice tin tưởng vào ngân hàng mà Bob ủy nhiệm




10

## Giao thức sử dụng trọng tài

- Khi 2 bên đã không tin tưởng nhau, có thể đặt niềm tin vào bên thứ 3 không?
- Tăng chi phí
- Tăng trễ
- Trọng tài trở thành "cổ chai" trong hệ thống
- Trọng tài bị tấn công

11

## Giao thức có người phân xử(*Adjudicated Protocols)*

- Chia giao thức có trọng tài thành 2 giao thức:
  - Giao thức không cần đến trọng tài, có thể thực hiện bất kỳ khi nào 2 bên muốn
  - Giao thức cần người phân xử: chỉ sử dụng khi có tranh chấp
- Hãy xem xét lại giao dịch trong ví dụ trên với giải pháp mới này!

12

## Giao thức tự phân xử(*Self-Enforcing Protocols*)

- Không cần đến bên thứ 3
- Giao thức có cơ chế để một bên có thể phát hiện sự gian lận của bên còn lại
- Không phải tình huống nào cũng có thể tìm ra giao thức như vậy

13

## Các dạng tấn công vào giao thức mật mã

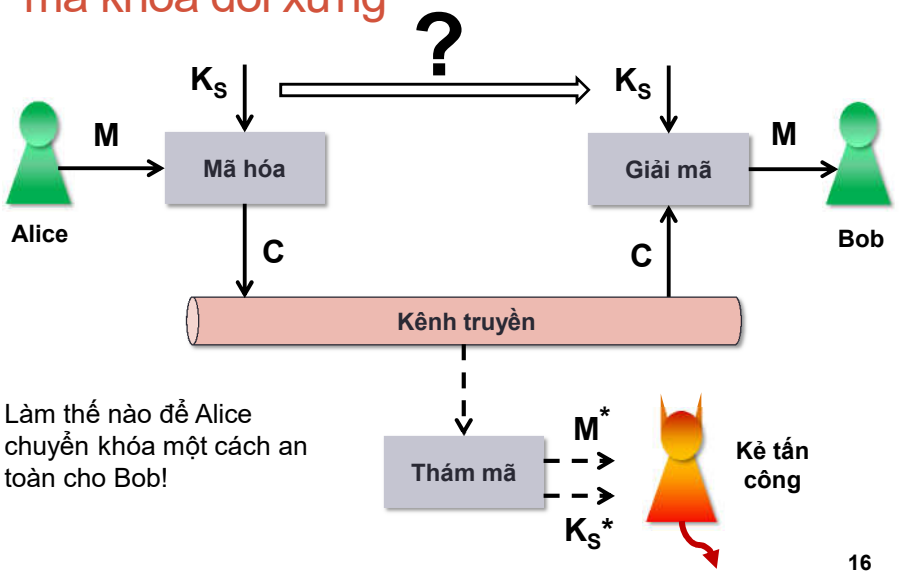
- Có thể lợi dụng các điểm yếu trong:
  - Hệ mật mã
  - Các bước thực hiện
- Tấn công thụ động: nghe trộm
- Tấn công chủ động: can thiệp vào giao thức
  - Chèn thông điệp
  - Thay thế thông điệp
  - Sử dụng lại thông điệp
  - Giả mạo một trong các bên

14

## 2. CÁC GIAO THỨC PHÂN PHỐI KHÓA BÍ MẬT

15

## Hãy xem lại sơ đồ bảo mật sử dụng mật mã khóa đối xứng




Làm thế nào để Alice chuyển khóa một cách an toàn cho Bob!

16

## Giao thức phân phối khóa không tập trung

- Khóa chính: $K_M$ đã được A và B chia sẻ an toàn
  - Làm thế nào vì đây chính là bài toán đang cần giải quyết ☺
  - Khóa chính được sử dụng để trao đổi khóa phiên $K_S$
- Khóa phiên $K_S$: sử dụng để mã hóa dữ liệu trao đổi
- Giao thức 1.1

  (1) A → B: $ID_A$

  (2) B → A: $E(K_M, ID_B||K_S)$
- Giao thức này đã đủ an toàn chưa?
  - Tấn công nghe lén
  - Tấn công thay thế
  - Tấn công giả mạo
  - Tấn công phát lại

17

## Giao thức phân phối khóa không tập trung – Giao thức 1.2

- Sử dụng các yếu tố chống tấn công phát lại (replay attack)

  (1) A → B: $ID_A || N_1$

  (2) B → A: $E(K_M, ID_B || K_S || N_1 || N_2)$

  (3) A → B: A kiểm tra $N_1$ và gửi $E(K_S, N_2)$

  (4) B kiểm tra $N_2$
- Hạn chế của phân phối khóa không tập trung?

18

## Giao thức phân phối khóa tập trung

- Sử dụng bên thứ 3 được tin cậy – KDC (Key Distribution Centre):
  - Sinh khóa bí mật $K_S$
  - Phân phối $K_S$ tới A và B
- A và KDC đã chia sẻ một khóa bí mật $K_A$, B và KDC đã chia sẻ một khóa bí mật $K_B$
  - Làm thế nào?

19

## Giao thức phân phối khóa tập trung- Giao thức 2.1

(1) A → KDC: $ID_A \| ID_B$

(2) KDC → A: $E(K_A, K_S \| ID_A \| ID_B \| E(K_B, ID_A \| K_S))$

(3) A giải mã, thu được $K_S$

(4) A → B: $E(K_B, ID_A \| K_S)$

(5) A ↔ B: $E(K_S, Data)$

- Hãy xem xét tính an toàn của giao thức này?
  - Tấn công nghe lén
  - Tấn công thay thế
  - Tấn công giả mạo
  - Tấn công phát lại

20

## Giao thức phân phối khóa tập trung- Giao thức 2.2 (Needham-Schroeder)

(1) A → KDC: $ID_A$ || $ID_B$ || **$N_1$**

(2) KDC → A: E($K_A$, $K_S$ || $ID_A$ || $ID_B$ || **$N_1$** || E($K_B$, $ID_A$ || $K_S$))

(3) A giải mã, kiểm tra $N_1$ thu được $K_S$

(4) A → B: E($K_B$, $ID_A$ || $K_S$) ← B giải mã, thu được $K_S$

**(5) B → A: E($K_S$, $N_2$)**

**(6) A → B: E($K_S$, f($N_2$)) ← B giải mã kiểm tra f($N_2$)**

(7) A ↔ B: E($K_S$, Data)

$N_1$, $N_2$: giá trị ngẫu nhiên dùng 1 lần (nonce)

f(x): hàm biến đổi dữ liệu bất kỳ

- Hãy xem xét lại tính an toàn của giao thức này!

21

## Giao thức 2.2 (Needham-Schroeder)

22

## Giao thức phân phối khóa tập trung- Giao thức 2.3 (Denning)

(1) A → KDC: $ID_A$ || $ID_B$

(2) KDC → A: E($K_A$, $K_S$ || $ID_A$ || $ID_B$ || **T** || E($K_B$, $ID_A$ || $K_S$ || **T**))

(3) A giải mã, kiểm tra T, thu được $K_S$

(4) A → B: E($K_B$, $ID_A$ || $K_S$ || **T**) ← B giải mã, kiểm tra T

**(5) B → A: E($K_S$, $N_1$)**

**(6) A → B: E($K_S$, f($N_1$)) ← B giải mã, kiểm tra $N_1$**

(7) A ↔ B: E($K_S$, Data)

T: nhãn thời gian (time stamp)

- Kiểm tra tính an toàn của sơ đồ này:
  - Mất đồng bộ đồng hồ của các bên

23

## Giao thức 2.3 (Denning)

24

## Giao thức phân phối khóa tập trung- Giao thức 2.4 (Kehne)

(1) A → B: $ID_A \| N_A$

(2) B → KDC: $ID_B \| N_B \| E(K_B, ID_A \| N_A \| T_B)$

(3) KDC → A: $E(K_A, ID_B \| N_A \| K_S) \| E(K_B, ID_A \| K_S \| T_B) \| N_B$

(4) A →B: $E(K_B, ID_A \| K_S \| T_B) \| E(K_S, N_B)$

- Vì sao việc sử dụng nhãn thời gian $T_B$ của B tốt hơn nhãn thời gian T của KDC trong giao thức 2.3
- Hãy xem thêm các giao thức khác trong Section 3.1, Chapter 3, *"Applied Cryptography: Protocols, Algorithms, and Source Code in C"*, 2nd Edition, Bruce Schneier

25

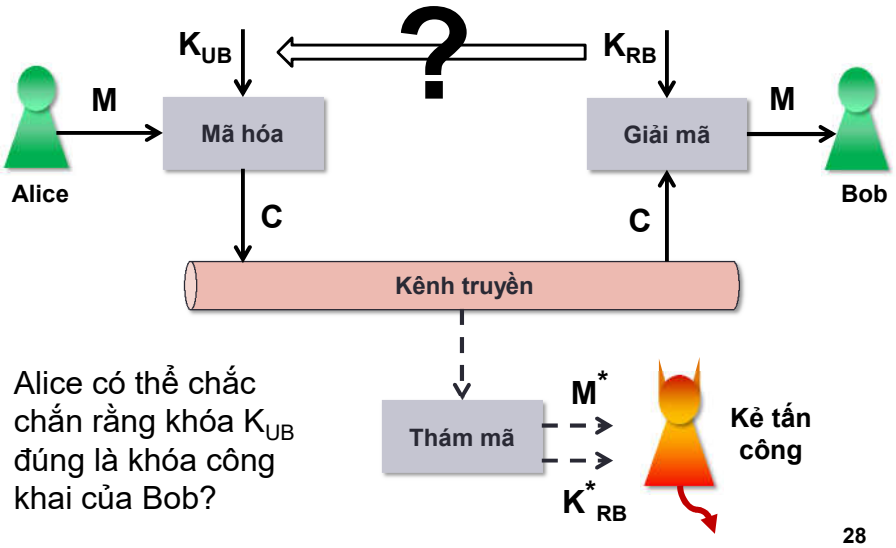
## Giao thức 2.4 (Kehne)

26

## 3. CÁC GIAO THỨC PHÂN PHỐI KHÓA CÔNG KHAI

27

## Hãy xem lại sơ đồ bảo mật sử dụng mật mã khóa công khai




Alice có thể chắc chắn rằng khóa $K_{UB}$ đúng là khóa công khai của Bob?

28

## Giao thức phân phối khóa không tập trung

- Hãy xem xét giao thức sau(Giao thức 3.1):

(1) A → B: $ID_A \| K_{UA} \| N_1$

(2) B → A: $ID_B \| K_{UB} \| N_2 \| E(K_{UA}, f(N_1))$

(3) A kiểm tra $f(N_1)$

A → B: $E(K_{UB}, g(N_2))$

(4) B kiểm tra $g(N_2)$

(5) B → A: $E(K_{UA}, Data_A)$

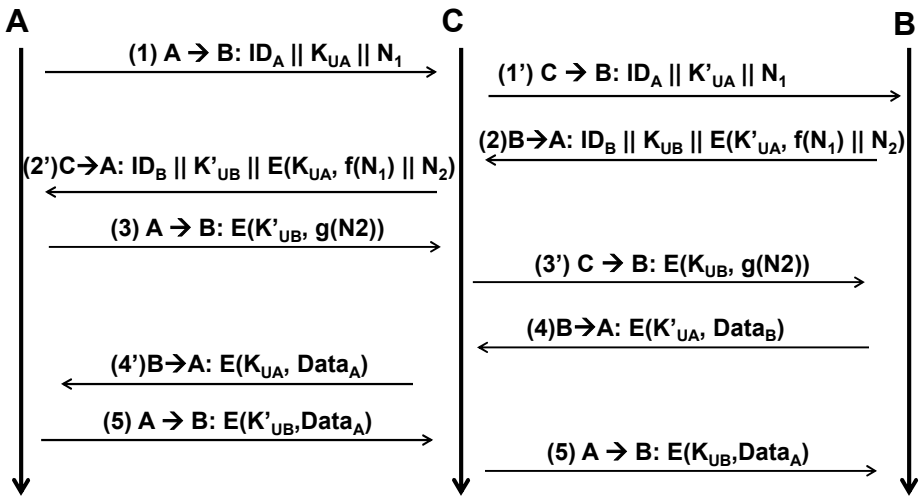
(6) A → B: $E(K_{UB}, Data_B)$

- Nhận xét: Nếu f(x) và g(x) được giữ bí mật hoàn toàn thì C không thể giả mạo A hoặc B?

29

## Giao thức 3.1 – Tấn công man-in-the-middle

- C tự sinh cặp khóa $(K'_{UA}, K'_{RA})$ và $(K'_{UB}, K'_{RB})$




30

## Giao thức 3.2

- Hãy xem xét giao thức sau(Giao thức 3.2):

(1) A → B: $ID_A$ || $K_{UA}$ || $N_1$

(2) B → A: $ID_B$ || $K_{UB}$ || $N_2$ || $E(K_{UA}, f(N_1))$

B chỉ gửi một phần của mẩu tin này cho A

(3) A → B: $E(K_{UB}, g(N_2))$

A chỉ gửi một phần mẩu tin này cho B

(4) B gửi phần còn lại bản tin $E(K_{UA}, f(N_1))$

(4') A giải mã với $K_{RA}$ nhận được $f(N_1)$ và kiểm tra
A gửi phần còn lại của bản tin $E(K_{UB}, g(N_2))$ cho B

(4'') B giải mã với $K_{RB}$ nhận được $g(N_2)$ và kiểm tra.

(5) B → A: $E(K_{UA}, Data_A)$

(6) A → B: $E(K_{UB}, Data_B)$

31

## Giao thức phân phối khóa tập trung- Giao thức 4.1

- Sử dụng bên thứ 3 tin cậy – PKA (Public Key Authority)
  - Có cặp khóa ($K_{UPKA}$, $K_{RPKA}$)
  - Nhận các khóa công khai $K_{UA}$ của A và $K_{UB}$ của B một cách an toàn. Làm thế nào vì đây chính là bài toán đang cần giải quyết ☺
- A và B đều có khóa công khai $K_{UPKA}$ của PKA
- Giao thức 4.1

(1) A → PKA: $ID_A$ || $ID_B$

(2) PKA → A: $E(K_{RPKA}, ID_B || K_{UB})$

(3) A → B: $E(K_{UB}, N_1)$

(4) B → PKA: $ID_B$ || $ID_A$

(5) PKA → B: $E(K_{RPKA}, ID_A || K_{UA})$

(6) B → A: $E(K_{UA}, N_1)$

- Kiểm tra tính an toàn của giao thức này?
- Có thể tấn công vào giao thức này như thế nào?

32

## Giao thức 4.1



## Giao thức phân phối khóa tập trung- Giao thức 4.2

(1) A → PKA: $ID_A \| ID_B \| T_1$

(2) PKA → A: $E(K_{RPKA}, ID_B \| K_{UB} \| T_1)$

(3) A → B: $E(K_{UB}, N_1)$

(4) B → PKA: $ID_B \| ID_A \| T_2$

(5) PKA → B: $E(K_{RPKA}, ID_A \| K_{UA} \| T_2)$

(6) B → A: $E(K_{UA}, N_1)$

$T_1$, $T_2$: nhãn thời gian chống tấn công phát lại

- Giao thức này có hạn chế gì?

## Giao thức 4.2

35

## Giao thức phân phối khóa tập trung- Giao thức 4.3

- Bên thứ 3 được tin cậy – CA(Certificate Authority)
  - Có cặp khóa ($K_{UCA}$, $K_{RCA}$)
  - Phát hành chứng thư số cho khóa công khai của các bên có dạng

  Cert = E($K_{RCA}$, ID || $K_U$ || Time)

  *ID*: định danh của thực thể

  $K_U$: khóa công khai của thực thể đã được đăng ký tại CA

  *Time*: Thời hạn sử dụng khóa công khai. Thông thường có thời điểm bắt đầu có hiệu lực và thời điểm hết hiệu lực.

36

## Giao thức phân phối khóa tập trung- Giao thức 4.3 (tiếp)

(1) A → CA: $ID_A$ || $K_{UA}$ || $Time_A$

(2) CA → A: $Cert_A$= E($K_{RCA}$, $ID_A$ || $K_{UA}$ || $Time_A$)

(3) B → CA: $ID_B$ || $K_{UB}$ || $Time_B$

(4) CA → B: $Cert_B$= E($K_{RCA}$, $ID_B$ || $K_{UB}$ || $Time_B$)

(5) A → B: $Cert_A$

(6) B → A: $Cert_B$

- Làm thế nào để A và B có thể yên tâm sử dụng khóa công khai của nhau?
- Hãy cải tiến lại các giao thức trong các khâu cần đến xác thực thông điệp (sử dụng MAC hoặc hàm băm)
- Đọc thêm về PKI và chứng thư số theo chuẩn X.509

37

## Giao thức 4.3 (tiếp)

38

## Phân phối khóa bí mật của hệ mật mã khóa đối xứng

- Hạn chế chung của các giao thức phân phối khóa bí mật trong hệ mật mã khóa đối xứng
  - Giao thức không tập trung: Số lượng khóa sử dụng lớn
  - Giao thức tập trung: PKA phải đáp ứng yêu cầu với tần suất rất lớn
  - Không có cơ chế xác thực rõ ràng

  → Sử dụng mật mã khóa công khai trong các giao thức phân phối khóa bí mật

  (1) A → B: $E(K_{UB}, E(K_{RA}, K_S))$

  (2) B giải mã với $K_{RB}$, sau đó kiểm tra để chắc chắn thông điệp xuất phát từ A. Khóa $K_S$ thu được là khóa phiên.

  (3) A ↔ B: $E(K_S, Data)$
- Tất nhiên giao thức trên không chống được tấn công phát lại. Việc cải tiến giao thức trên như là một bài tập.

39

## Kết luận

- Hệ thống có nguy cơ mất an toàn ngay cả khi chúng ta sử dụng hệ mật mã tốt nếu không có một giao thức quản lý và phân phối khóa an toàn
- Mật mã phải gắn liền với xác thực
- Thực tế các giao thức phân phối khóa đã trình bày đều xác thực dựa trên các sơ đồ mã hóa của hệ mật mã. Chúng ta biết rằng, giải pháp này chưa thực sự an toàn (hãy xem lại những phân tích trong bài §3. Xác thực thông điệp).
  - Bài tập: Hãy sử dụng MAC, hàm băm, chữ ký điện tử để tăng cường an toàn cho các sơ đồ trên.

40

## Một số lưu ý khác

- Đảm bảo tính bí mật:
  - Khóa bí mật
  - Khóa cá nhân
  - Các giá trị chia sẻ bí mật khác
- Bảm bảo tính toàn vẹn, xác thực:
  - Khóa bí mật
  - Khóa công khai
  - Thông tin sinh khóa
- Kiểm tra tính hợp lệ của các tham số nhóm
- Kiểm tra tính hợp lệ của khóa công khai
- Kiểm tra quyền sở hữu khóa cá nhân

41

## Một số lưu ý khác

- Không kết thúc ngay giao thức khi có 1 lỗi xảy ra
  - Làm chậm thông báo lỗi
- Thông báo lỗi không nêu cụ thể nguyên nhân lỗi

42