HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN
****

GIAO THỨC AN TOÀN MẠNG

Bài 2.1. Một số nguyên thủy xác thực

1. Khái niệm, phân loại xác thực và giao thức xác thực
2. Truyền trực tiếp bí mật
3. Thách đố bằng nonce
4. Thách đố bằng timestamp

Mục tiêu bài học

❑Kiến thức

- Khái niệm, phân loại xác thực
- Khái niệm, phân loại giao thức xác thực
- Một số nguyên thủy xác thực thuộc các loại khác nhau

❑Kỹ năng

- Phân tích hoạt động của giao thức xác thực

Tài liệu tham khảo

1. Giáo trình "Giao thức an toàn mạng máy tính"// Chương 2 "**Các giao thức xác thực**"
2. Giáo trình "Mật mã ứng dụng"// Chương 5 "**Giao thức mật mã**"

1. Khái niệm, phân loại xác thực và giao thức xác thực
2. Truyền trực tiếp bí mật
3. Thách đố bằng nonce
4. Thách đố bằng timestamp

Một số khái niệm trong xác thực

- **Xác thực** là hành vi xác nhận sự thật một thuộc tính của một đối tượng hoặc một chủ thể.
  - Xác thực thông điệp
  - Xác thực thực thể

Một số khái niệm trong xác thực

- **Xác thực thông điệp** là một cơ chế cho phép khẳng định rằng thông điệp không bị thay đổi trong quá trình truyền và bên nhận có thể kiểm tra được nguồn gốc của thông điệp

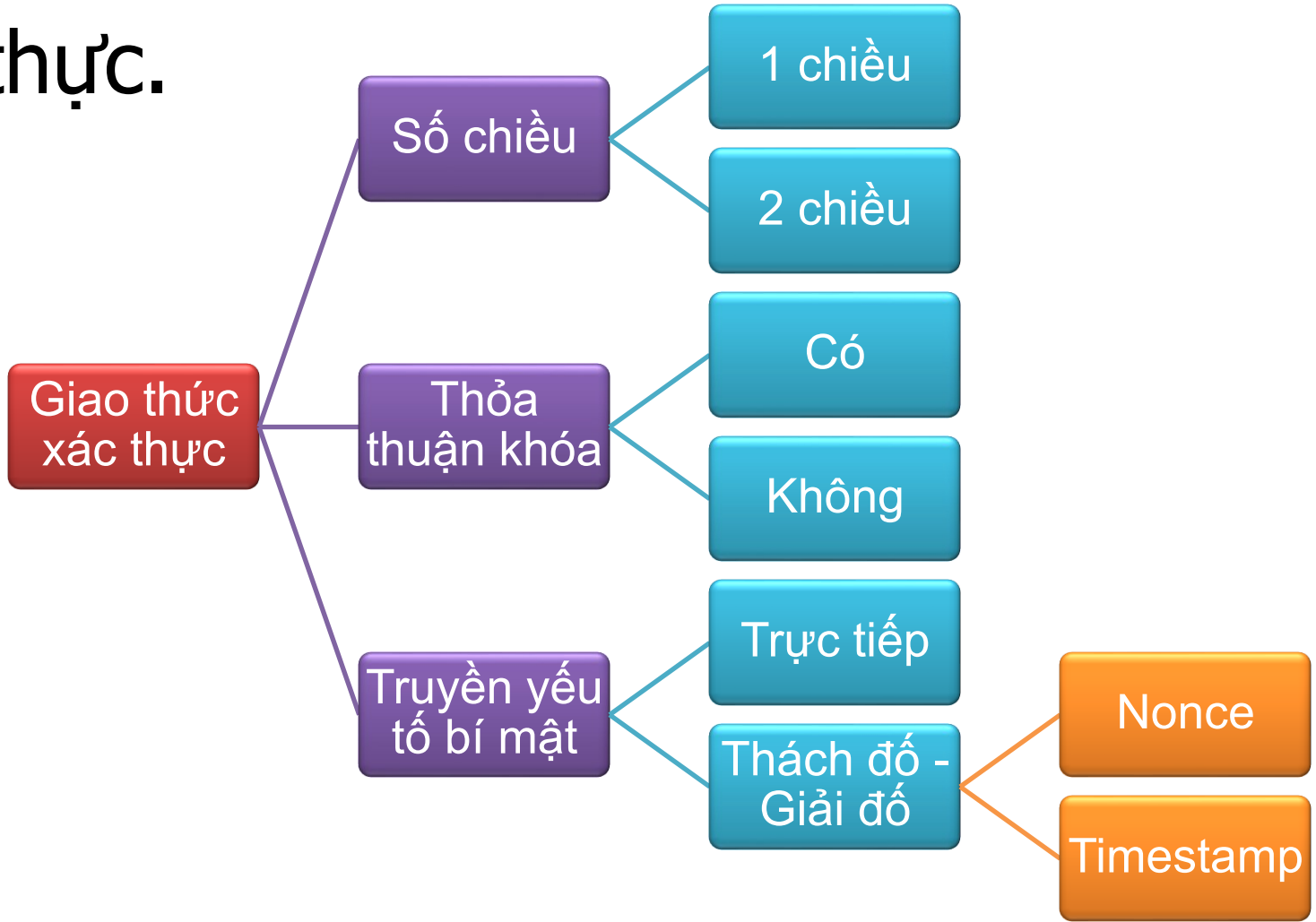
Một số khái niệm trong xác thực

- **Xác thực thực thể** là một thủ tục mà qua đó, một thực thể thiết lập một tính chất được yêu cầu cho một thực thể khác

- **Thực thể**: người dùng, tiến trình, client, server
- **Tính chất được yêu cầu**: có mật khẩu đúng, có nắm giữ khóa bí mật...

Giao thức xác thực

- **Giao thức xác thực (thực thể)** là một giao thức mật mã với mục đích thực hiện xác thực.



Ký hiệu quy ước

- **Alice (A), Bob (B)**... là tên của thực thể;
- **Alice → Bob: m**: Alice gửi *m* đến Bob;
- **{m}K**: mã hóa *m* bởi khóa K;
- **P_A**: mật khẩu của A
- **KP_A**: khóa công khai của A;

Ký hiệu quy ước

- **K_{AB}**: khóa bí mật chia sẻ giữa A và B;
- **T_A**: tem thời gian tạo bởi thực thể A;
- **N_A**: số ngẫu nhiên tạo bởi thực thể A;
- **$sig_A(m)$**: chữ ký số tạo bởi thực thể A trên thông báo *m*;

1. Khái niệm, phân loại xác thực và giao thức xác thực
2. Truyền trực tiếp bí mật
3. Thách đố bằng nonce
4. Thách đố bằng timestamp

Truyền trực tiếp yếu tố bí mật

- **Điều kiện**

  Alice và Bob chia sẻ mật khẩu P_A

- **Yêu cầu**

  Bob xác thực được Alice

- **Thực hiện**

1. Alice $\rightarrow$ Bob: "Alice", P_A
2. Bob kiểm tra tính hợp lệ và chấp nhận hoặc từ chối truy cập

Truyền trực tiếp yếu tố bí mật

- Mật khẩu có thể bị chặn thu
- Nhưng thực tế vẫn được sử dụng rộng rãi (phần lớn các website)
- Để đảm bảo an toàn, quá trình xác thực được thực hiện qua một kênh mã hóa

Truyền trực tiếp yếu tố bí mật

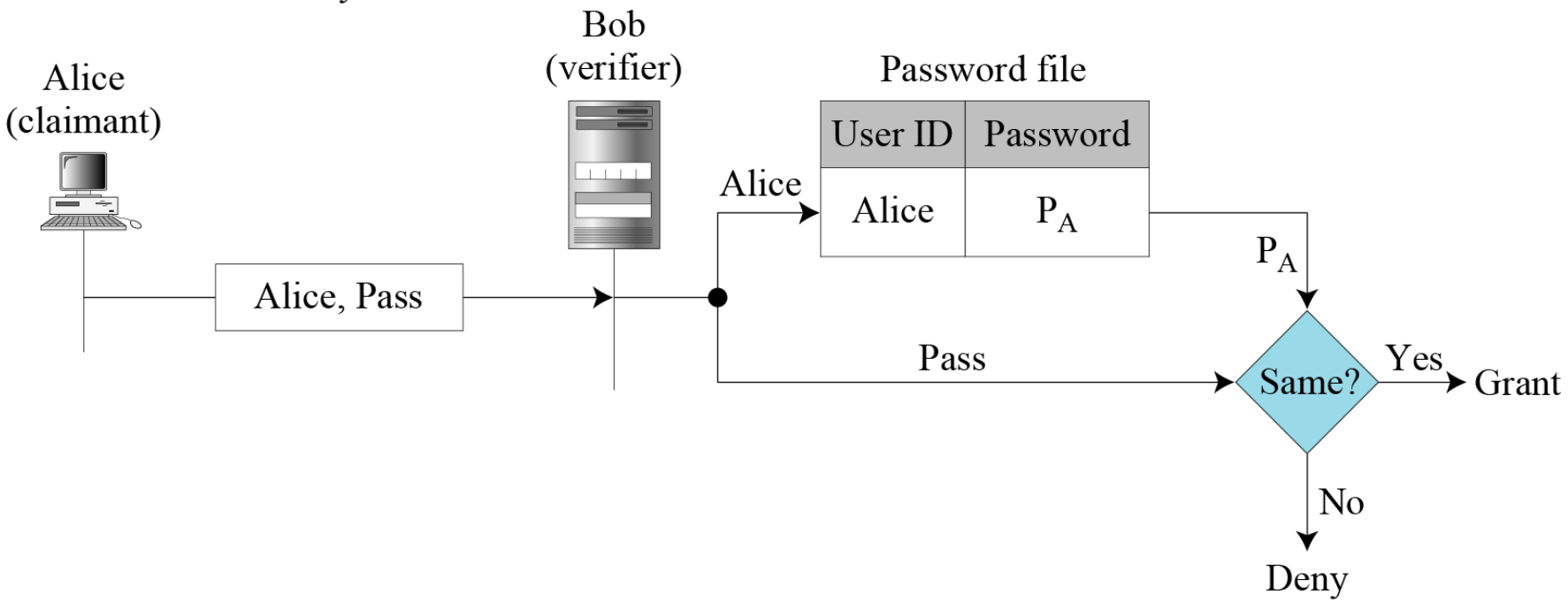
- **Phương án lưu trữ mật khẩu của Alice ở phía Bob:**
  - Lữu trữ dạng rõ
  - Lưu trữ dạng băm
  - Lưu trữ dạng băm có phụ gia (salt)

Xác thực bằng mật khẩu

1.Lưu mật khẩu dạng rõ

P_A: Alice's stored password

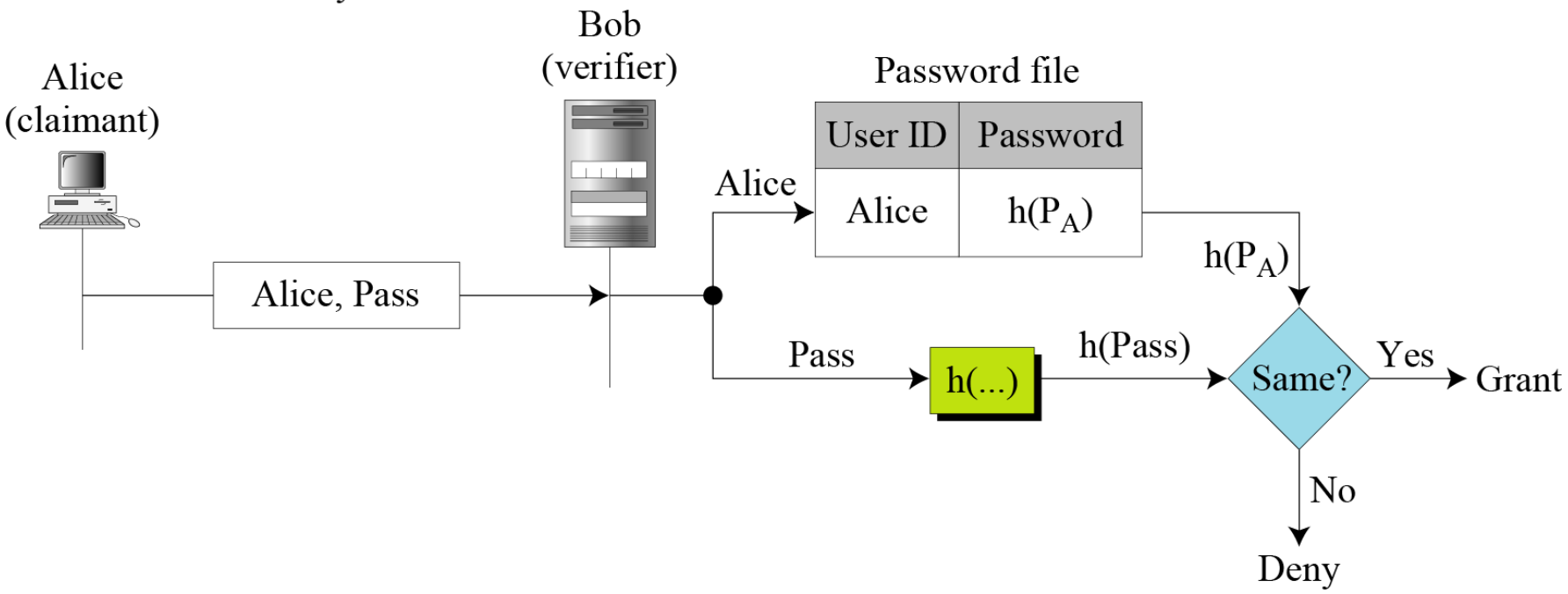
Pass: Password sent by claimant



2. Lưu mật khẩu dạng băm

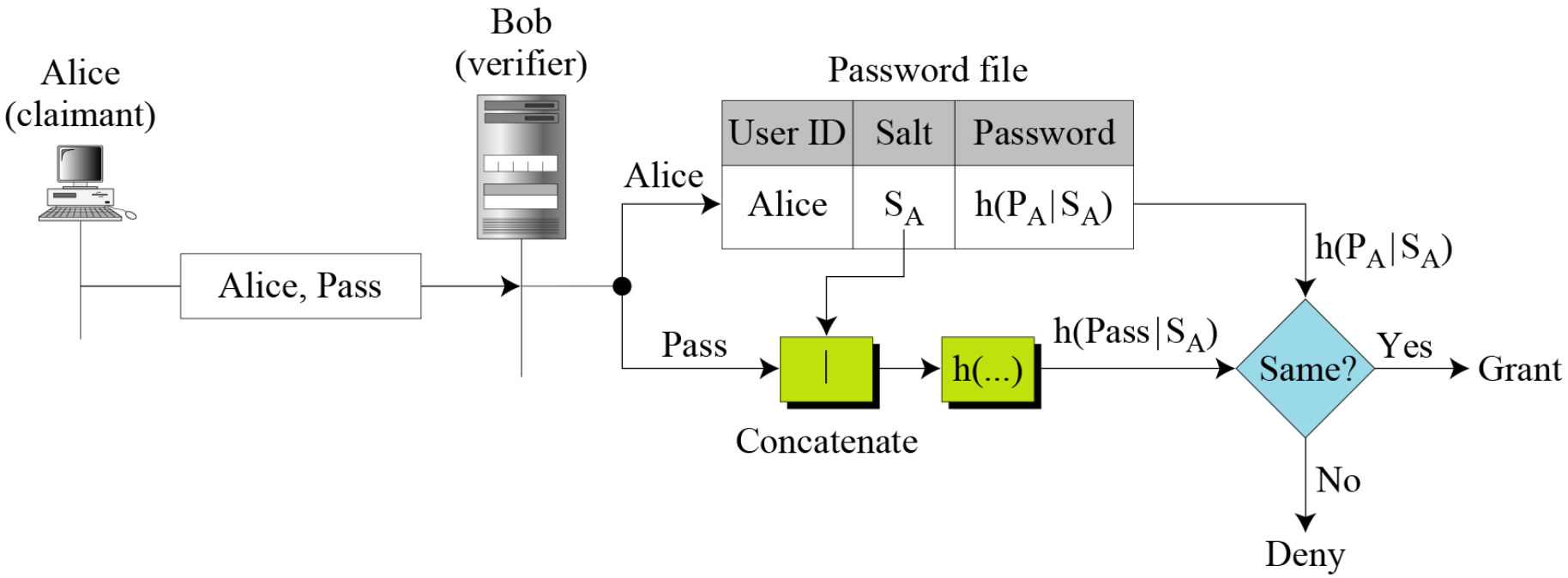
P_A: Alice's stored password

Pass: Password sent by claimant



3. Lưu mật khẩu dạng băm có salt

P_A: Alice's password
S_A: Alice's salt
Pass: Password sent by claimant



1. Khái niệm, phân loại xác thực và giao thức xác thực
2. Truyền trực tiếp bí mật
3. Thách đố bằng nonce
4. Thách đố bằng timestamp

Nonce

- **Nonce** là một đại lượng được sinh ngẫu nhiên, sao cho không bao giờ lặp lại
  - Để không lặp lại, nonce thường có kích thước lớn (~128 bít)
  - Việc nonce không lặp lại giúp đảm bảo tính tươi của thông điệp (thông điệp chỉ được sử dụng 1 lần) trong xác thực
  - Nonce luôn được sinh bởi bên xác thực (authentication server).

Mật mã đối xứng + nonce (1/2)

- **Điều kiện**

  Alice và Bob chia sẻ khóa bí mật K_{AB}

- **Yêu cầu**

  Bob xác thực được Alice

Mật mã đối xứng + nonce (2/2)

❑ Thực hiện

1. Alice → Bob: "Alice" — **Initialization**
2. Bob → Alice: N_B; — **Challenge**
3. Alice → Bob: $\{N_B\}K_{AB}$ — **Response**
4. Bob: — **Decision**
   - Giải mã bằng K_{AB};
   - Chấp nhận nếu thấy N_B;

Hàm băm + nonce (1/2)

- **Điều kiện**

  Alice và Bob chia sẻ khóa bí mật K_{AB}

- **Yêu cầu**

  Bob xác thực được Alice

Hàm băm + nonce (2/2)

❑ Thực hiện

1. Alice $\rightarrow$ Bob: "Alice"
2. Bob $\rightarrow$ Alice: N_B;
3. Alice $\rightarrow$ Bob: $H(K_{AB} \,||\, N_B)$;
4. Bob:
   - Tính lại $H(K_{AB} \,||\, N_B)$
   - Chấp nhận nếu giá trị trùng nhau;

Chữ ký số + nonce (1/2)

- **Điều kiện**

  Alice có cặp khóa bí mật, công khai

- **Yêu cầu**

  Bob xác thực được Alice

Chữ ký số + nonce (2/2)

❑ Thực hiện

1. Alice $\rightarrow$ Bob: "Alice"
2. Bob $\rightarrow$ Alice: N_B
3. Alice $\rightarrow$ Bob: $sig_A(N_B)$
4. Bob:
   - Sử dụng KP_A để kiểm tra chữ ký;
   - Chấp nhận nếu chữ ký hợp lệ;

Mã hóa khóa công khai + nonce (1/2)

- **Điều kiện**

  Alice có cặp khóa bí mật, công khai

- **Yêu cầu**

  Bob xác thực được Alice

Mã hóa khóa công khai + nonce (1/2)

❑ Thực hiện

1. Alice $\rightarrow$ Bob: "Alice"
2. Bob $\rightarrow$ Alice: $\{N_B\}KP_A$
3. Alice $\rightarrow$ Bob: N_B
4. Bob
   - So sánh với N_B ban đầu;
   - Chấp nhận nếu giống nhau.

1. Khái niệm, phân loại xác thực và giao thức xác thực
2. Truyền trực tiếp bí mật
3. Thách đố bằng nonce
4. Thách đố bằng timestamp

Timestamp

- **Timestamp** đại lượng chỉ thời gian trên đồng hồ của mỗi bên tham gia xác thực.
  - Luôn có sự sai lệch giữa đồng hồ của các bên nên phải xác định một sai số chấp nhận được δ: $T_B-\delta \leq T_A \leq T_B+\delta$
  - Mỗi timestamp sẽ hợp lệ trong một khoảng thời gian nhất định → để chống tấn công phát lại (replay attack) bên xác thực cần có cơ chế đảm bảo mỗi timestamp chỉ được sử dụng một lần (ví dụ: ghi nhớ timestamp gần nhất được sử dụng bởi mỗi thực thể)

Mật mã đối xứng + timestamp (1/2)

- **Điều kiện**
  - Alice và Bob thống nhất cơ chế nhãn thời gian
  - Alice và Bob chia sẻ khóa bí mật K_{AB}
- **Yêu cầu**

  Bob xác thực được Alice

Mật mã đối xứng + timestamp (2/2)

❑ Thực hiện

1. Alice $\rightarrow$ Bob: "Alice", $\{T_A\}K_{AB}$
2. Bob
   - Giải mã bằng K_{AB} để thu được T_A
   - Chấp nhận nếu T_A hợp lệ

Hàm băm + timestamp (1/2)

- **Điều kiện**
  - Alice và Bob thống nhất cơ chế nhãn thời gian
  - Alice và Bob chia sẻ khóa bí mật K_{AB}
- **Yêu cầu**

  Bob xác thực được Alice

Hàm băm + timestamp (2/2)

❑ Thực hiện

1. Alice $\rightarrow$ Bob: "Alice", T_A, $H(K_{AB} || T_A)$;
2. Bob:
   - Kiểm tra tính hợp lệ của T_A
   - Tính lại $H(K_{AB} || T_A)$
   - Chấp nhận nếu trùng với giá trị gửi đến;

Chữ ký số + timestamp (1/2)

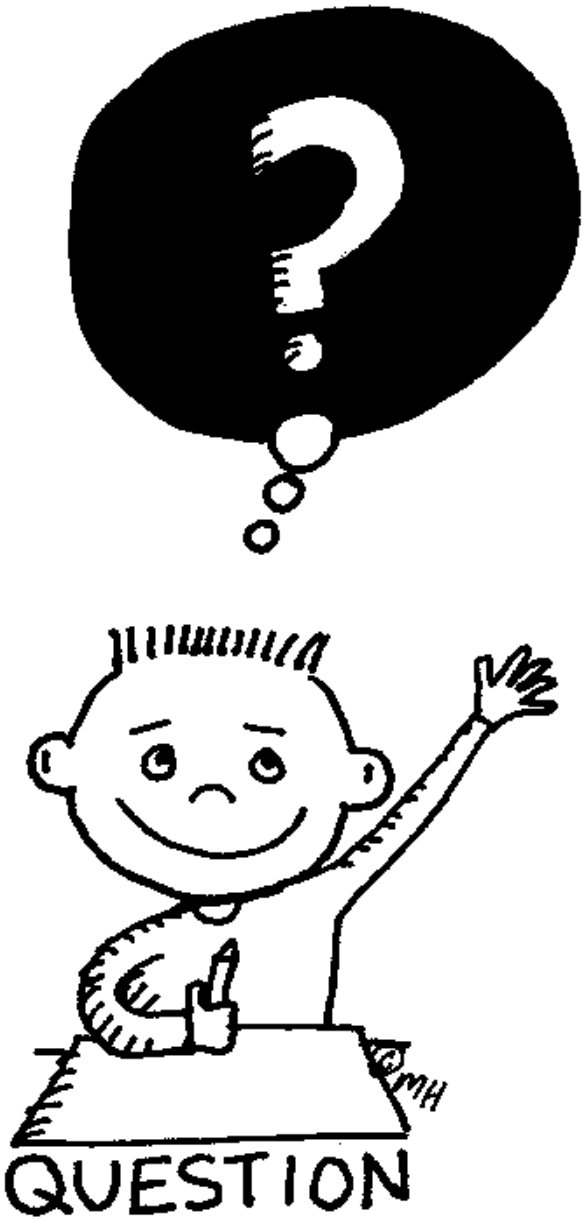
- **Điều kiện**
  - Alice và Bob thống nhất cơ chế nhãn thời gian
  - Alice có cặp khóa bí mật, công khai
- **Yêu cầu**

  Bob xác thực được Alice

Chữ ký số + timestamp (2/2)

❑ Thực hiện

1. Alice $\rightarrow$ Bob: "Alice", T_A, $sig_A(T_A)$
2. Bob:
   - Kiểm tra tính hợp lệ của T_A
   - Sử dụng KP_A để kiểm tra chữ ký;
   - Chấp nhận nếu chữ ký hợp lệ;


QUESTION

TỰ TÌM HIỂU
Các giao thức xác thực khác trong tài liệu [2]