Entity Authentication

Dr. B C Dhara
Department of Information Technology
Jadavpur University

Objectives

- Distinguish between message authentication and entity authentication
- Discuss some methods of entity authentication using a password
- Introduce some challenge-response protocols for entity authentication
- Introduce some zero-knowledge protocols for entity authentication
- Discuss biometrics and distinguish between physiological and behavioral techniques

Introduction

- *Entity authentication is a technique designed to let one party prove the identity of another party*
- *An entity can be a person, a process, a client, or a server*
- *The entity whose identity needs to be proved is called the claimant*
- *The party that tries to prove the identity of the claimant is called the verifier*

Message authentication Vs. Entity authentication

1) *Message authentication might not happen in real time; entity authentication does*
2) *Message authentication simply authenticates one message; the process needs to be repeated for each new message; Entity authentication authenticates the claimant for the entire duration of a session*

Entity authentication

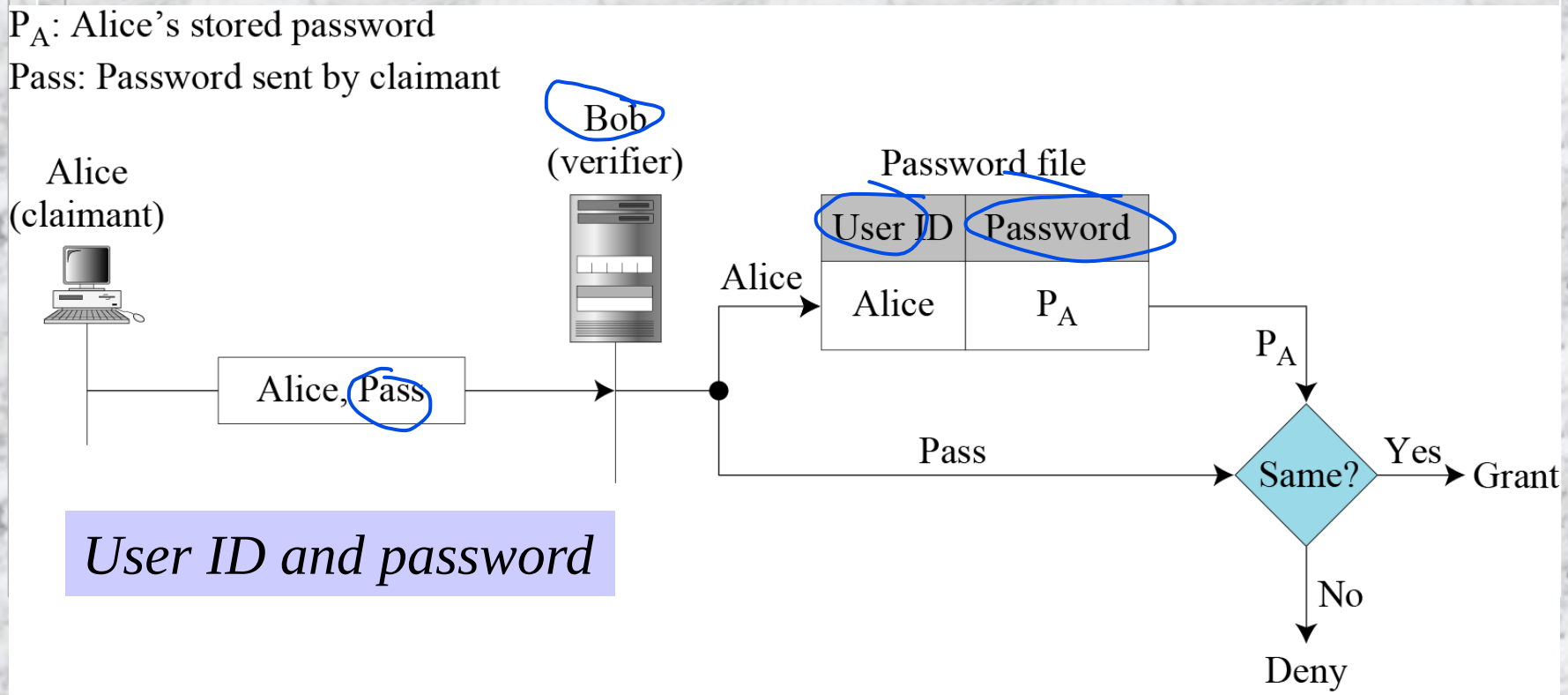
- Entity authentication can be done with one of witnesses:
  - Something known
    - Known by claimant, can be checked by verifier
      - Password, PIN, private key etc.
  - Something possessed
    - A passport, driving license etc
  - Something inherent
    - Biometrics, …

Password base authentication

- *The simplest and oldest method of entity authentication is the password-based authentication, where the password is something that the claimant knows*
  - Fixed Password
  - One-Time Password

Fixed password

- Same password is used again and again for every access
- *First Approach:*

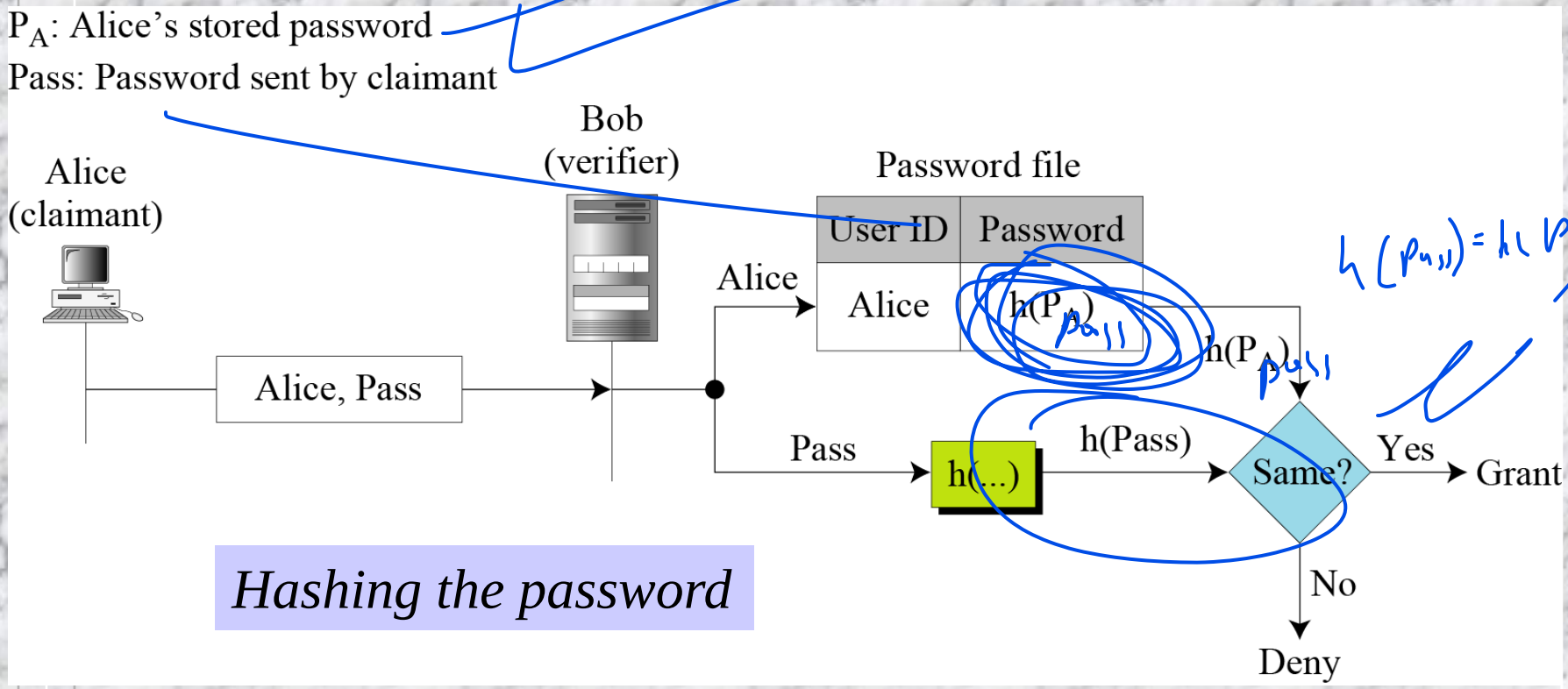


User ID and password

Attacks on first approach

- Eavesdropping
- Stealing a Password
- Accessing Password file
- Guessing a Password

Second approach: hashing the password



Hashing the password

If Password length is limited, then all possible cases can be considered

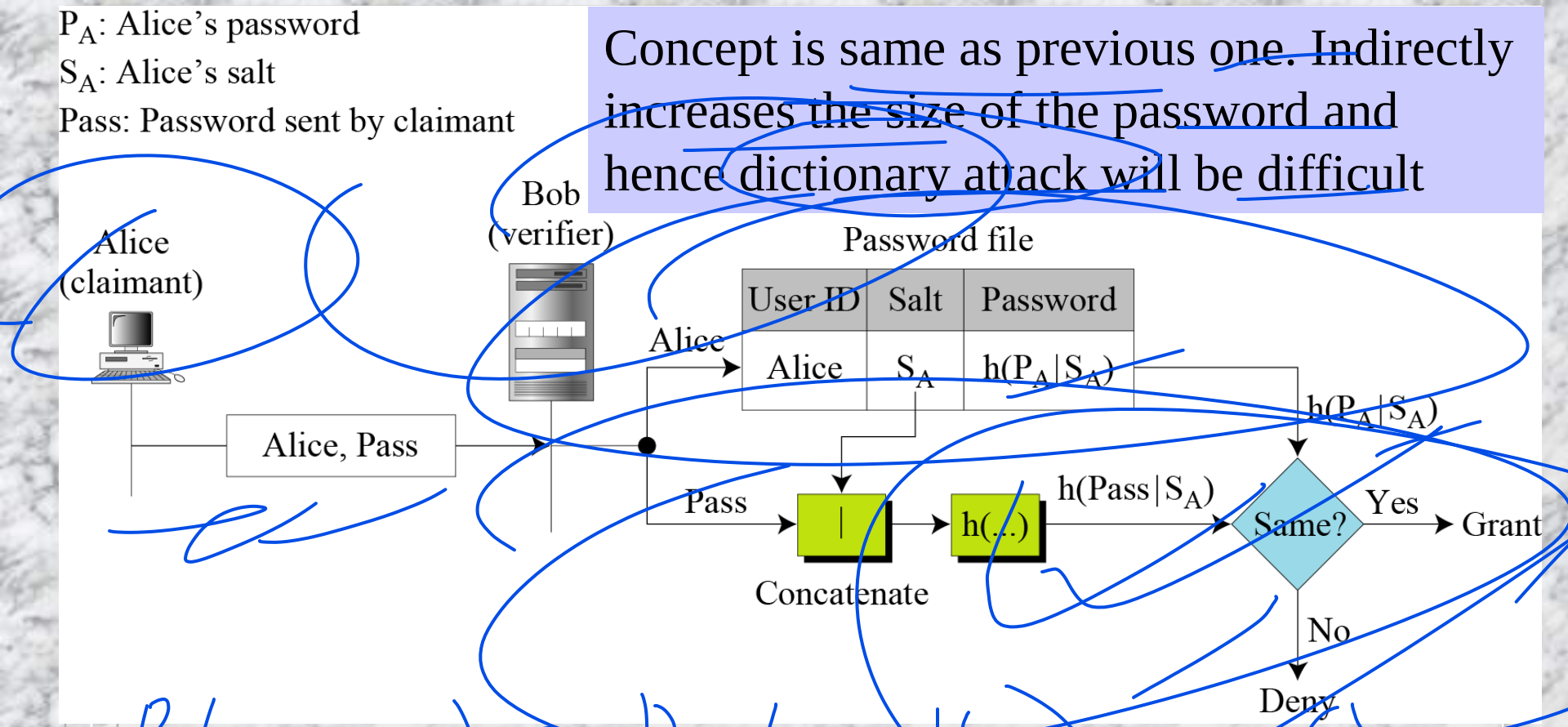
Third Approach: Salting the Password

P_A: Alice's password

S_A: Alice's salt

Pass: Password sent by claimant

Concept is same as previous one. Indirectly increases the size of the password and hence dictionary attack will be difficult



Fourth approach

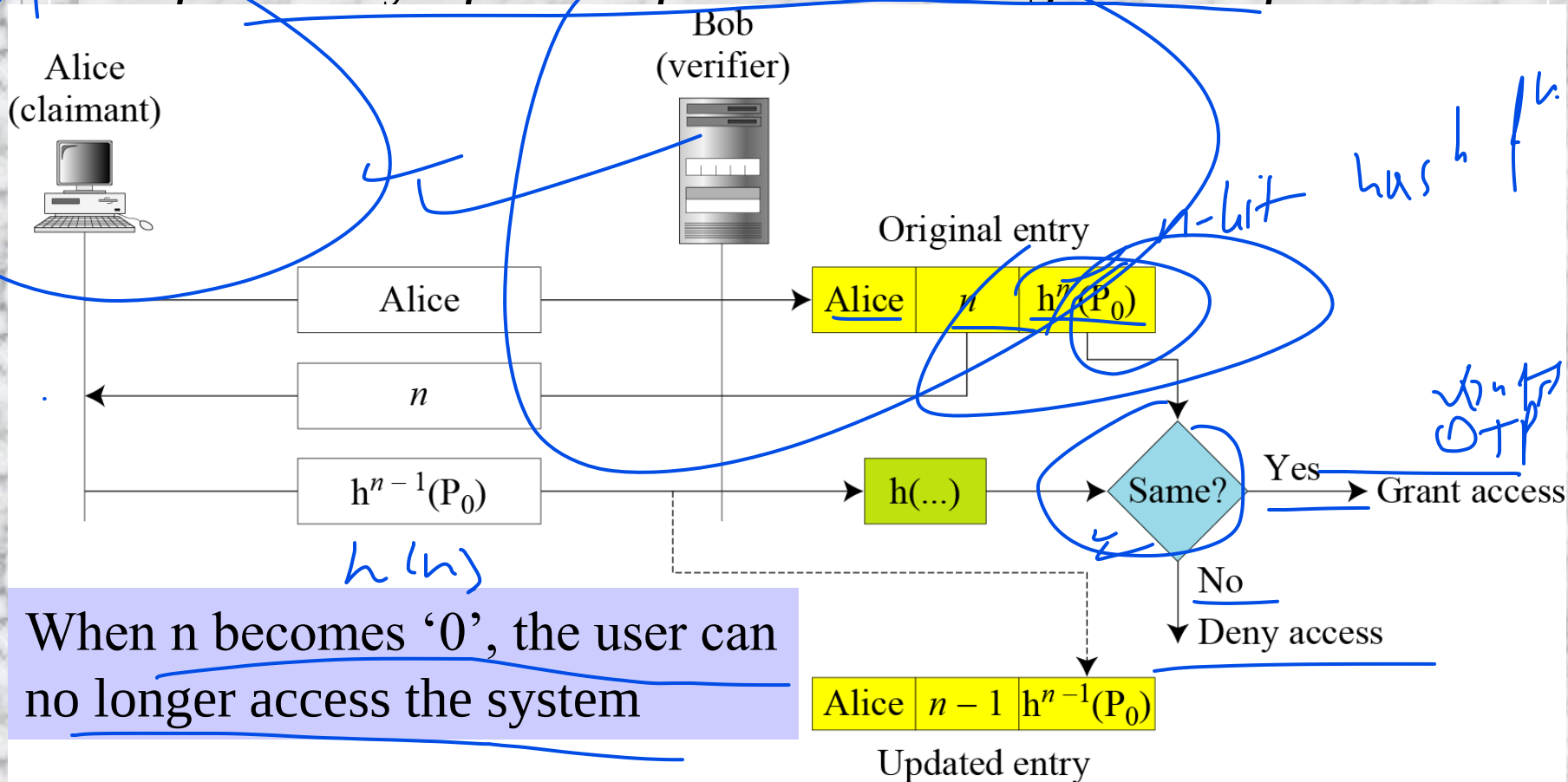
- *Two identification techniques are combined*
  - *A good example of this type of authentication is the use of an ATM card with a PIN*
  - *Card belongs to "something possessed" and PIN "something known"*

One time password (OTP)

- *First Approach*
  - *In this approach, the user and the system agree upon a list of passwords*
    - *System and user has to keep the list of passwords*
    - *If password not used in sequential order, a long search*
    - *eavesdropping and reuse are useless*
- *Second approach*
  - *In the second approach, the user and the system agree to sequentially update the password*
    - *P_{i+1} created at the time i-th login and encrypted by P_i*
    - *If first password can guess, then all subsequent will be available*

OTP

- Third approach
  - *In the third approach, the user and the system create a sequentially updated password using a hash function*



When n becomes ‘0’, the user can no longer access the system

CHALLENGE-RESPONSE PTOCOLS

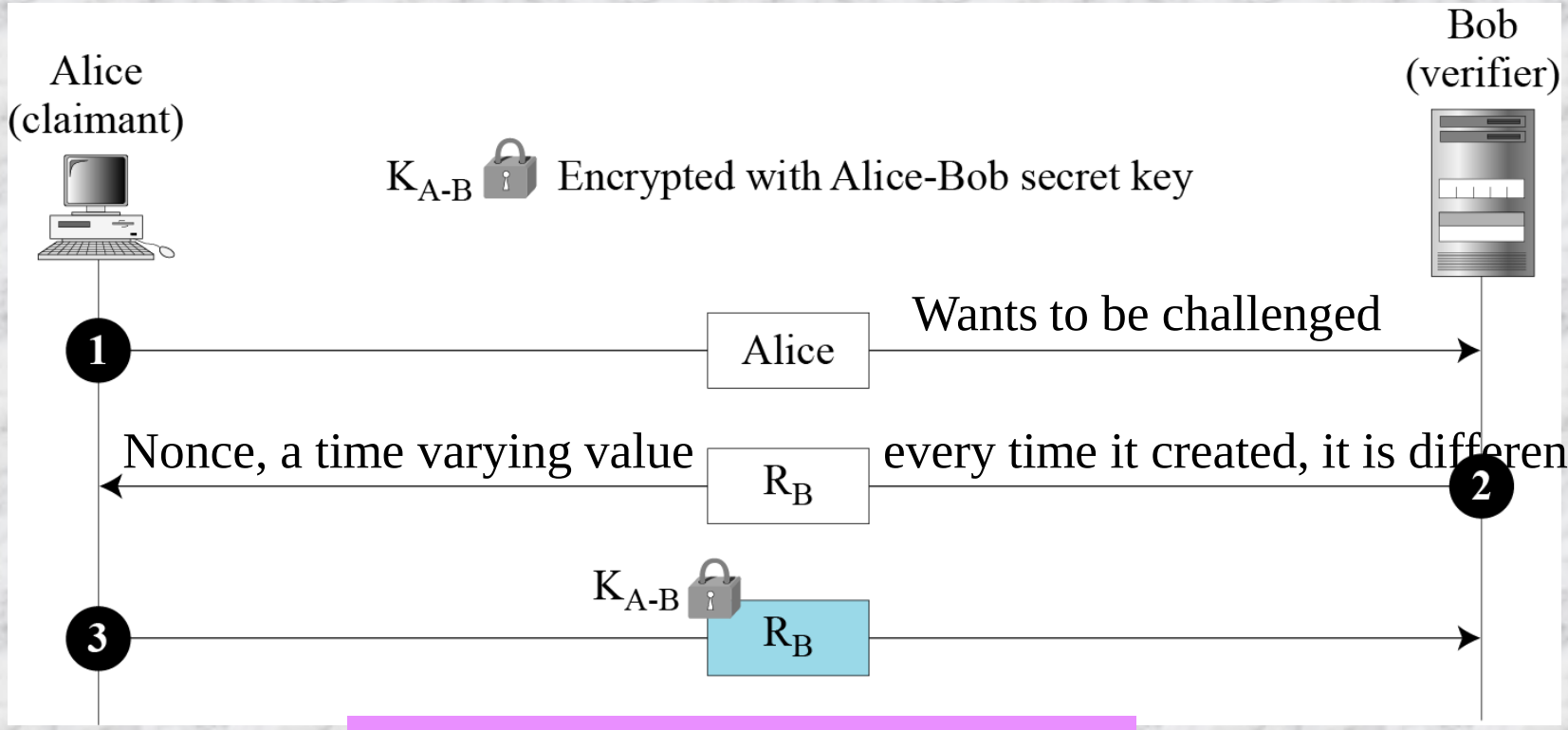
- In password based scheme, the claimant proves the identity by demonstrating that she knows a secret
- In challenge-response authentication,
  - The claimant proves that she knows a secret without sending it
  - The claimant does not need to send the secret to the verifier, either verifer has it or finds it

CHALLENGE-RESPONSE PTOCOLS

- First, claimant takes the initiative for the communication
- Then, verifier send a time-varying value (or, time stamp), which is called challenge, send to claimant
- The claimant applies a function to the challenge and the result, called as response, sends to the verifier

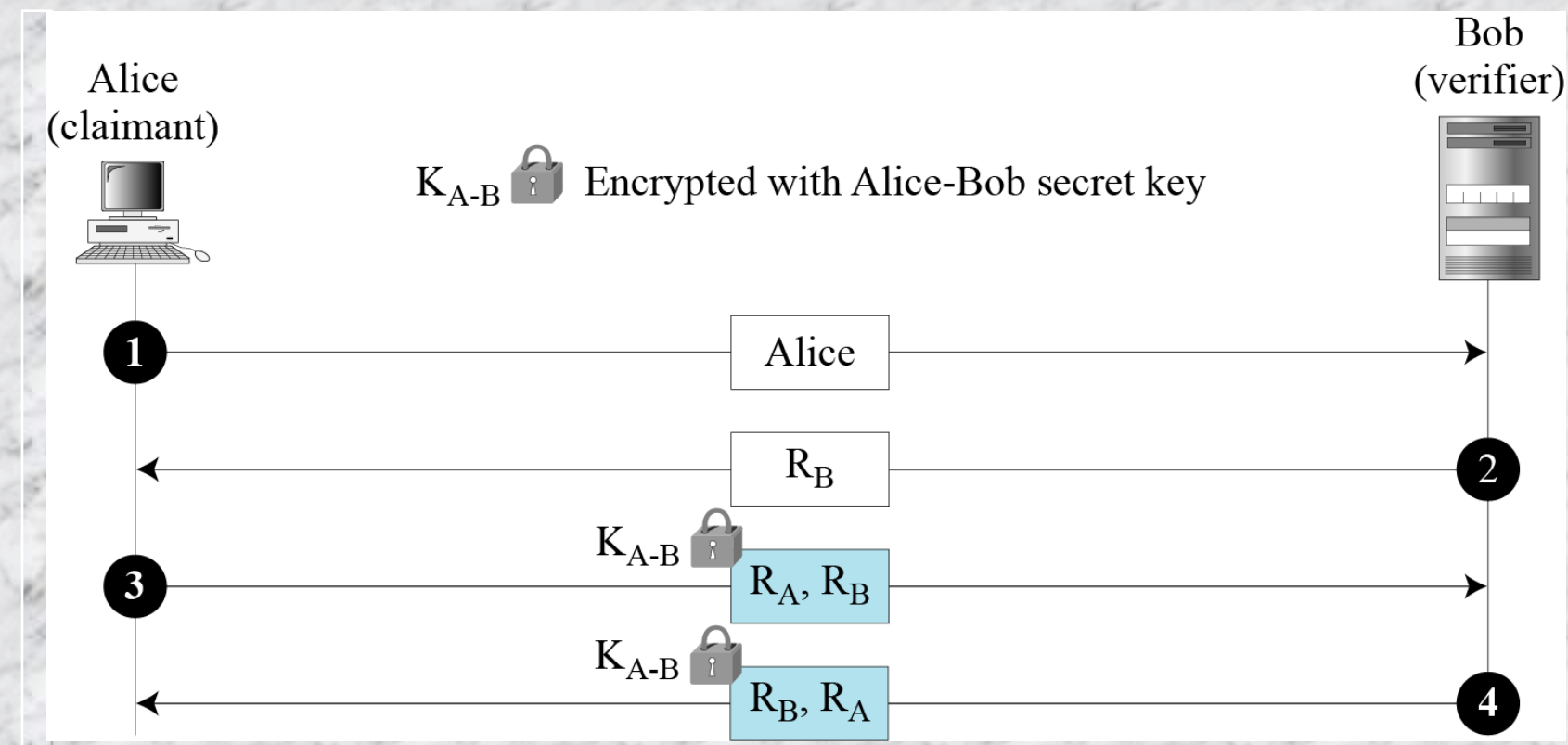
CHALLENGE-RESPONSE PTOCOLS:
Using a Symmetric-Key Cipher

- First approach:



Unidirectional authentication

CHALLENGE-RESPONSE PTOCOLS: Using a Symmetric-Key Cipher (contd…)

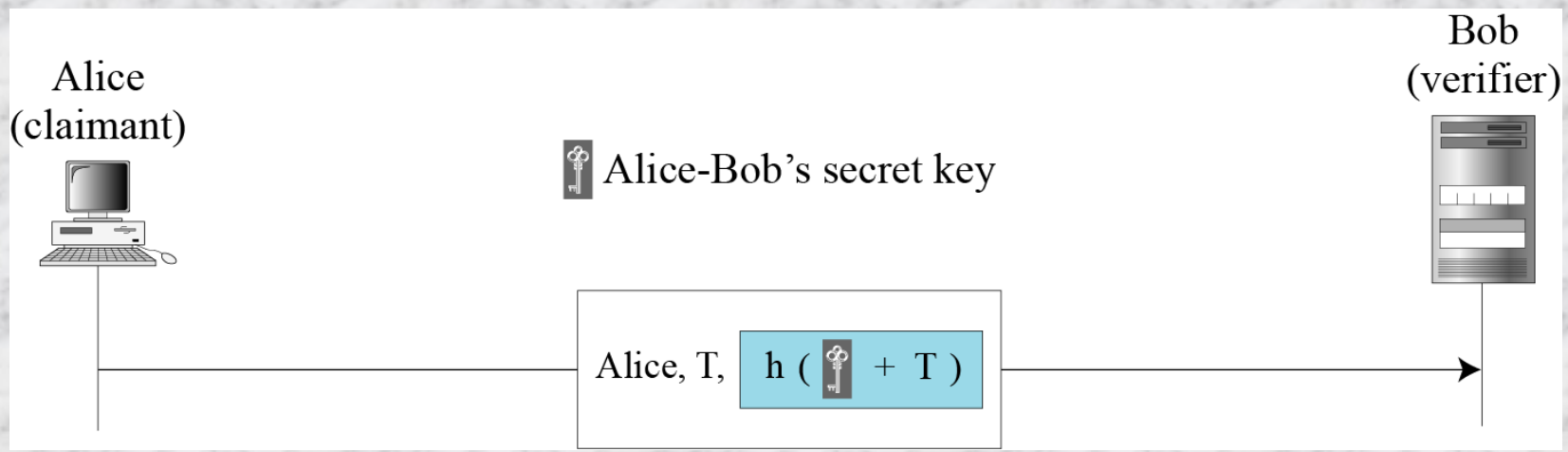


Bidirectional authentication

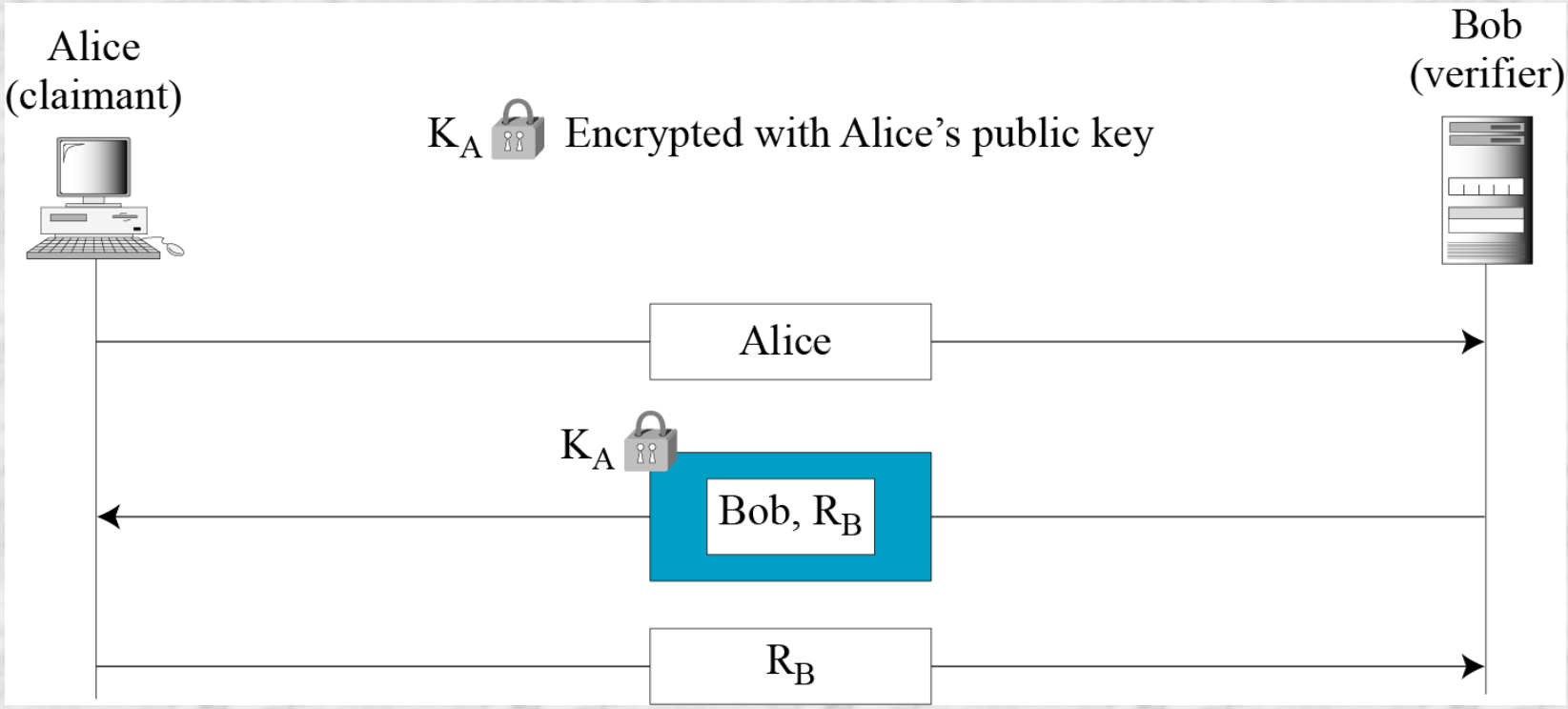
Using Keyed-Hash Functions

Instead of using encryption/decryption for entity authentication, we can also use a keyed-hash function (MAC).

Advantage: this method preserves the integrity of challenge and response messages

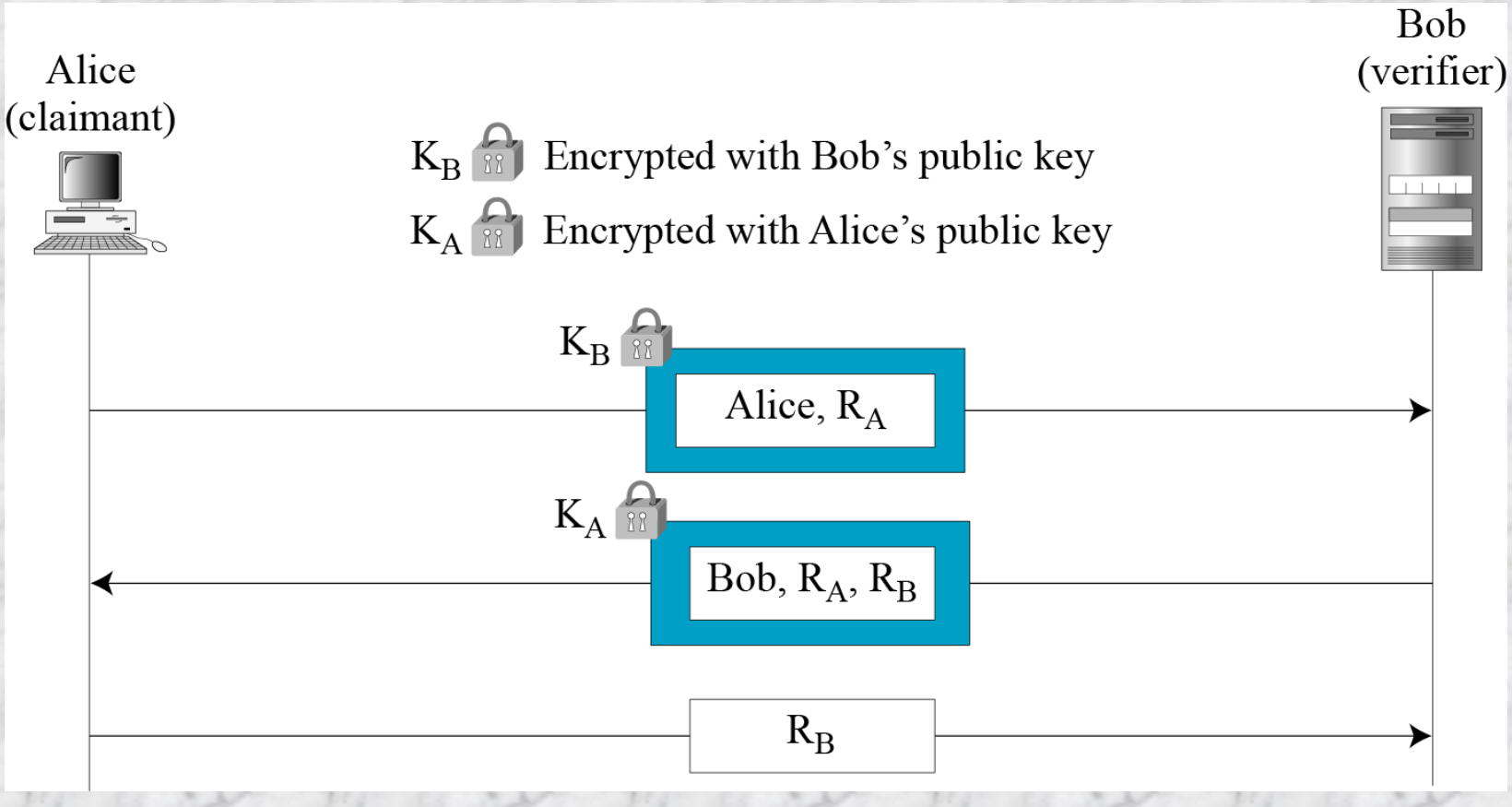


Using an Asymmetric-Key Cipher



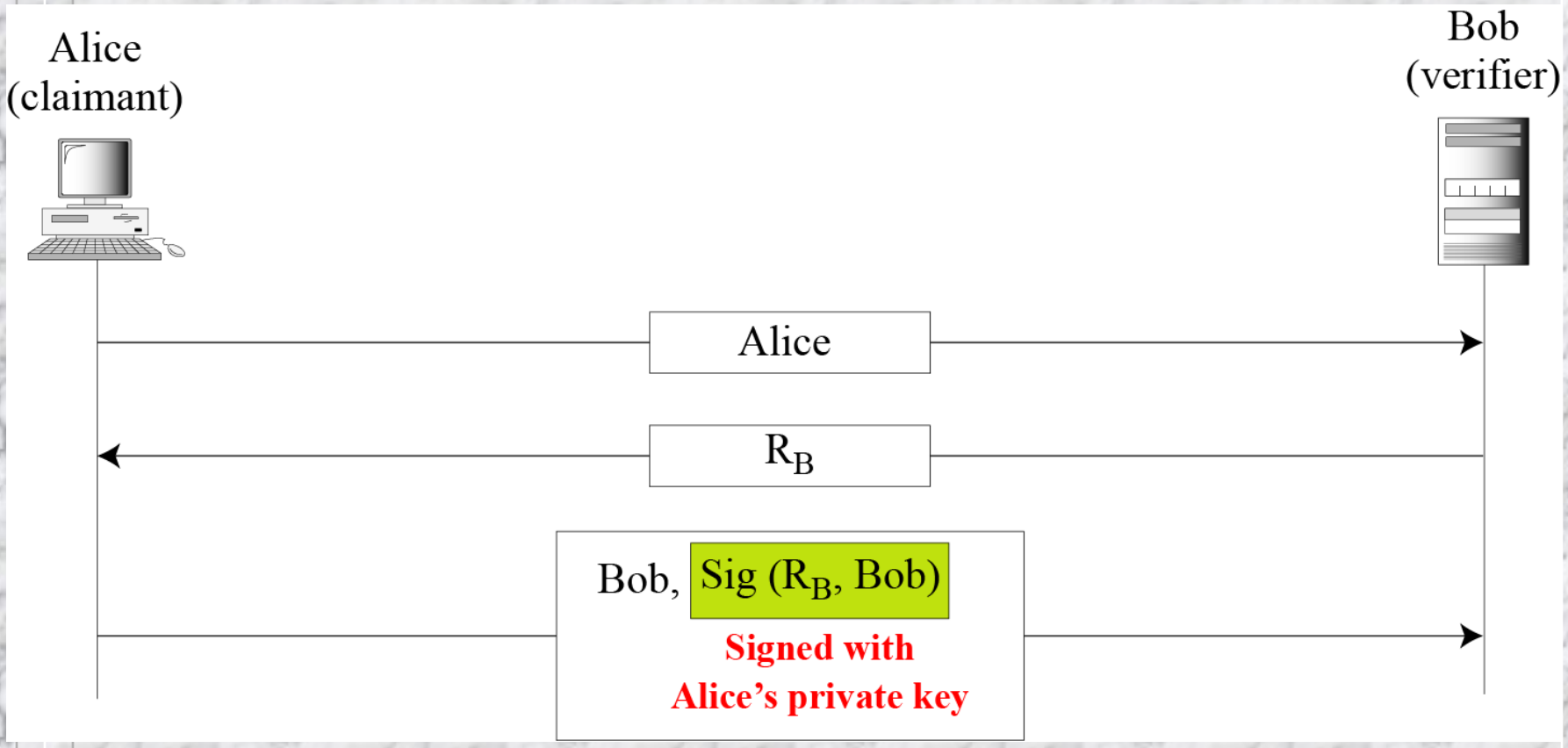
Unidirectional, asymmetric-key authentication

Using an Asymmetric-Key Cipher (contd…)



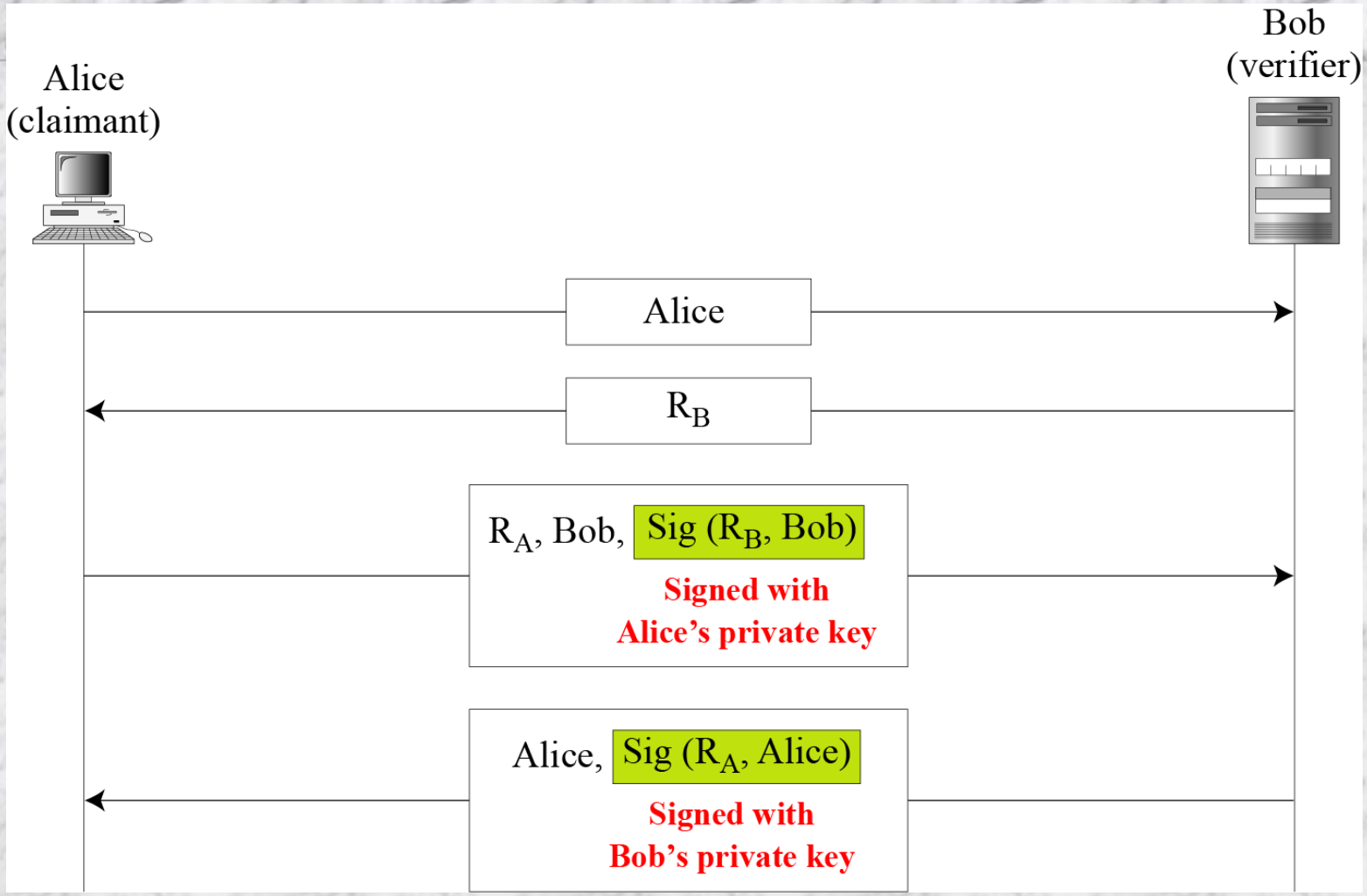
Bidirectional, asymmetric-key

Using Digital Signature



Digital signature, unidirectional

Using Digital Signature (contd…)



Digital signature, bidirectional authentication

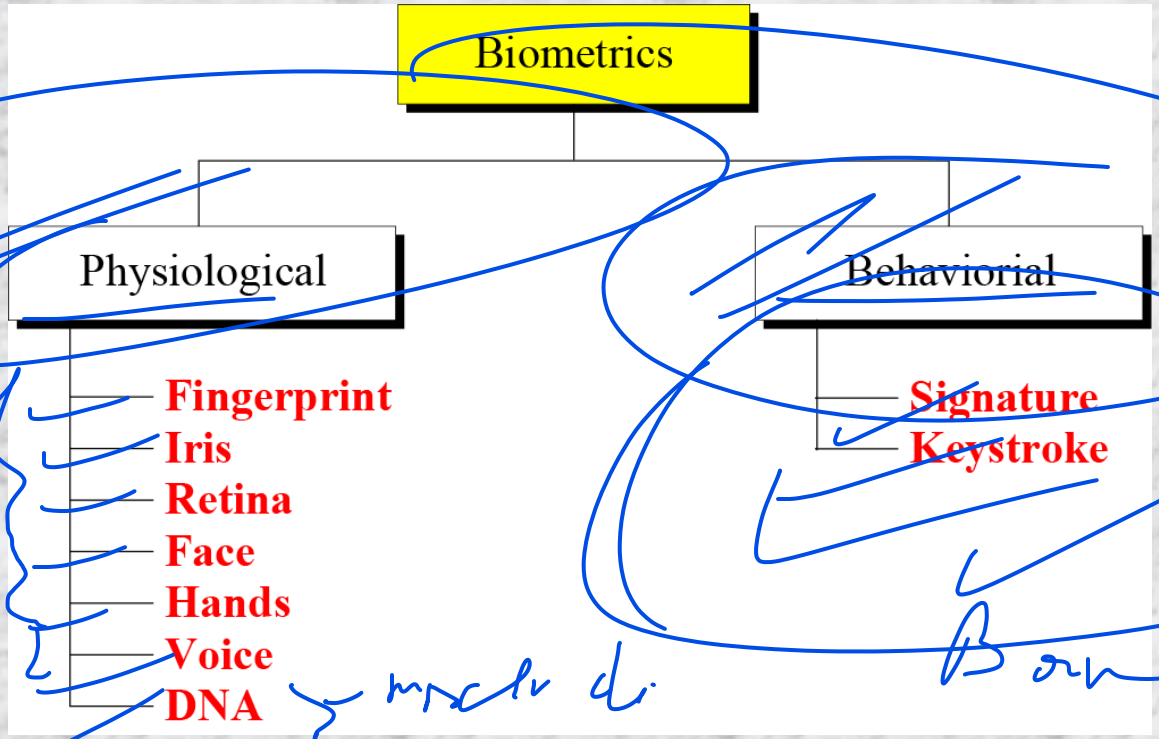
Biometrics

- *Biometrics is the measurement of physiological or behavioral features that identify a person (authentication by something inherent). Biometrics measures features that cannot be guessed, stolen, or shared.*

Several components are needed for biometrics, including capturing devices, processors, and storage devices..

Before using any biometric techniques for authentication, the corresponding feature of each person in the community should be available in the database. This is referred to as enrollment.

Types of Biometrics



Authentication

- Verification: 1-2-1 matching
- Identification: 1-2-m matching

Accuracy

- False Rejection Rate (FRR): System should recognize the person, but fails to recognize
- False Acceptance Rate (FAR): should not recognize, but system recognize the person

Applications of biometric

- Several applications of biometrics are already in use
- In commercial environments, these include access to facilities, access to information systems, transaction at point-of sales, and employee timekeeping
- In the law enforcement system, they include investigations (using fingerprints or DNA) and forensic analysis
- Border control and immigration control also use some biometric techniques