Chapter 14

Entity Authentication

Chapter 14

Objectives

- To distinguish between message authentication and entity authentication
- To define witnesses used for identification
- To discuss some methods of entity authentication using a password
- To introduce some challenge-response protocols for entity authentication
- To introduce some zero-knowledge protocols for entity authentication
- To define biometrics and distinguish between physiological and behavioral techniques

14-1 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.

Topics discussed in this section:

14.1.1 Data-Origin Versus Entity Authentication

There are two differences between message authentication (data-origin authentication), discussed in Chapter 13, and entity authentication, discussed in this chapter.

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.*

14.1.2 Verification Categories

Something known

Something possessed

Something inherent

14.1.3 Entity Authentication and Key Management

This chapter discusses entity authentication. The next chapter discusses key managment.

14-2 PASSWORDS

The simplest and oldest method of entity authentication is the password-based authentication, where the password is something that the claimant knows.

Topics discussed in this section:

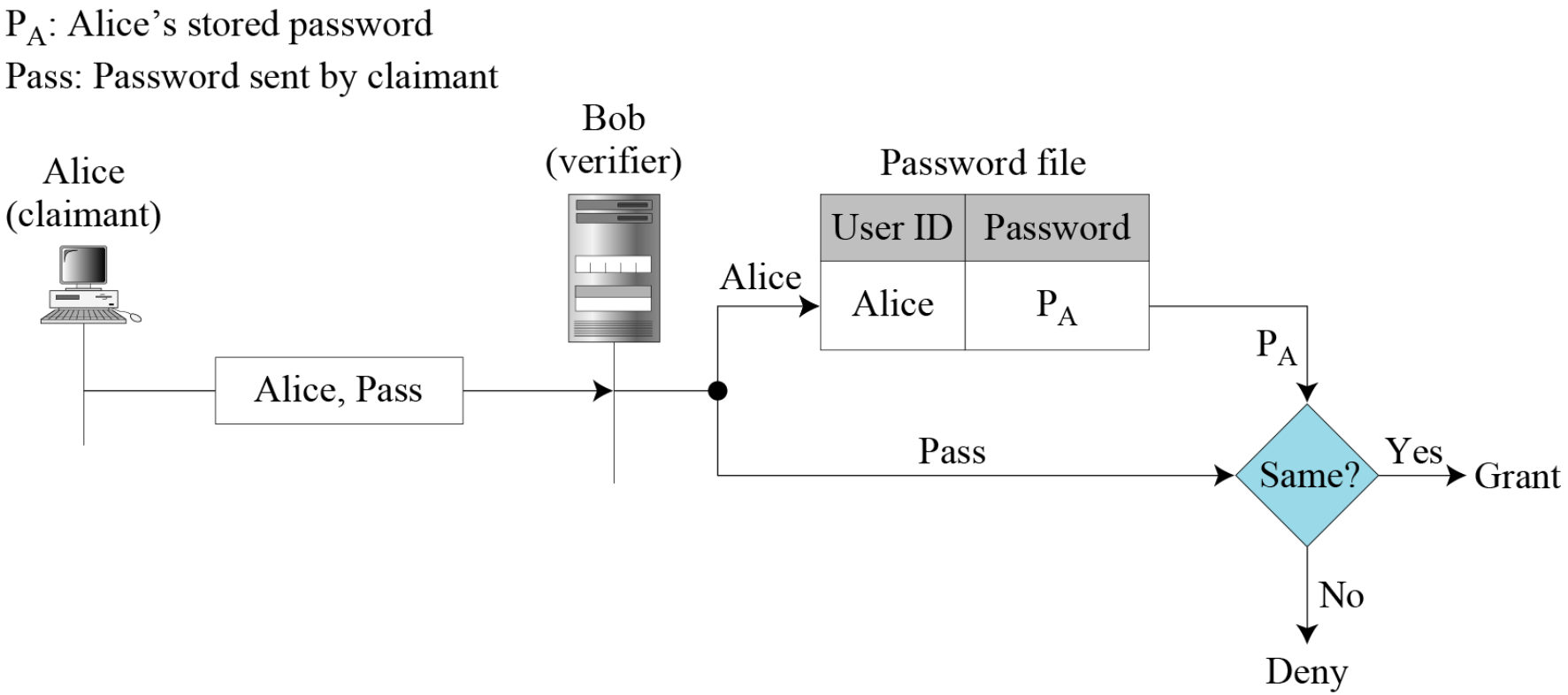
14.2.1 Fixed Password

14.2.2 One-Time Password

14.2.1 Fixed Password

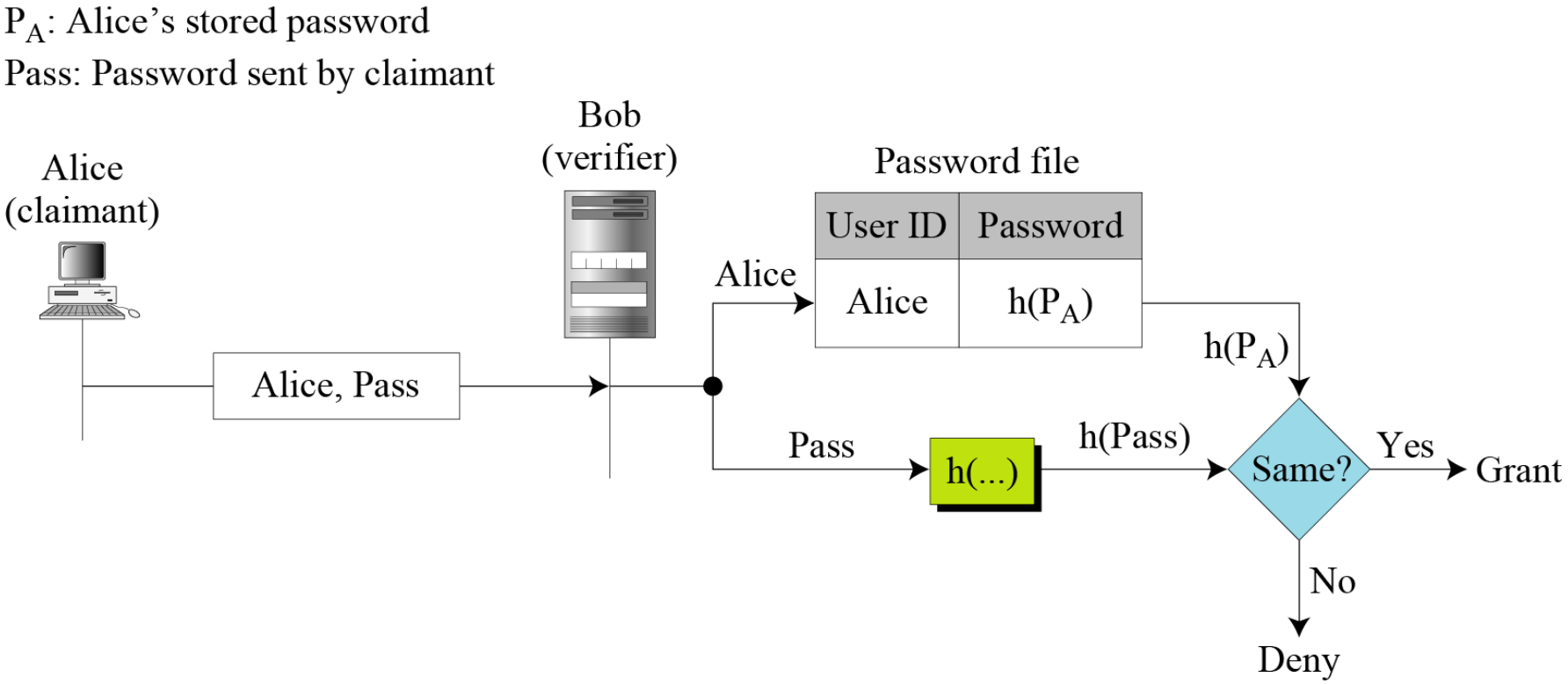
First Approach

Figure 14.1 *User ID and password file*



Second Approach

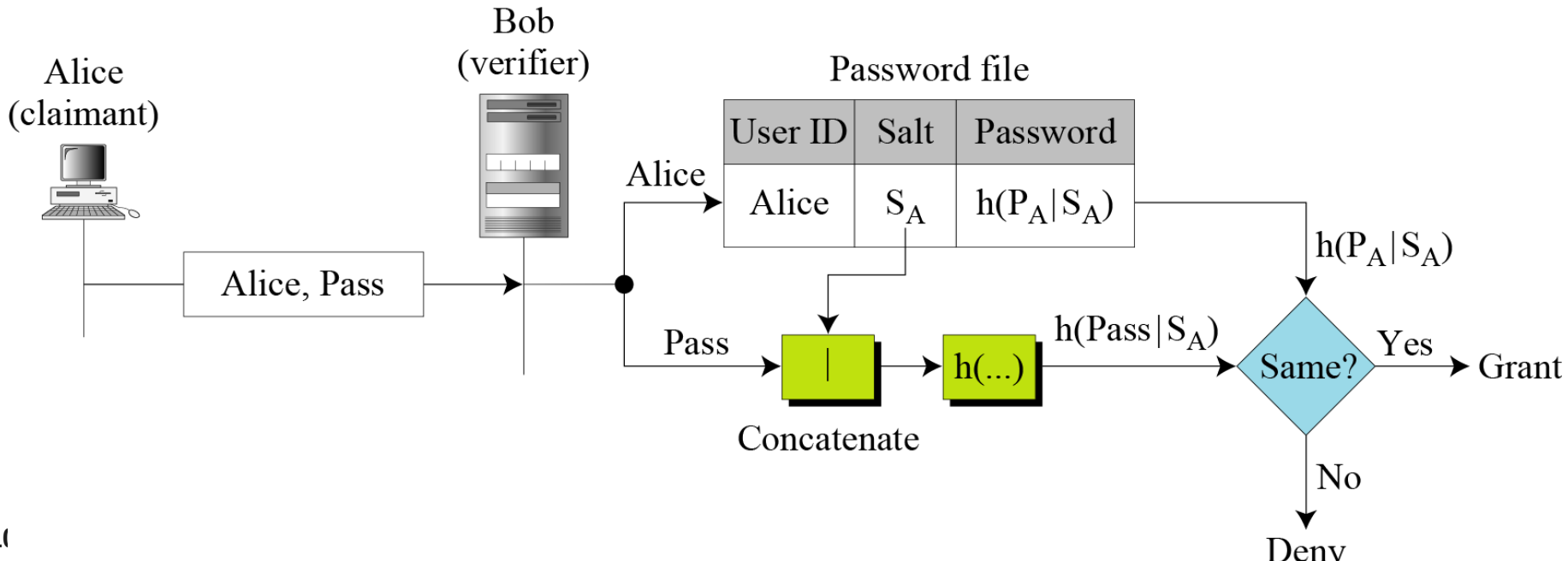
Figure 14.2 *Hashing the password*



Third Approach

Figure 14.3 *Salting the password*

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



14.2.1 Continued

Fourth Approach

In the 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 (personal identification number).

14.2.2 One-Time Password

First Approach

In the first approach, the user and the system agree upon a list of passwords.

Second Approach

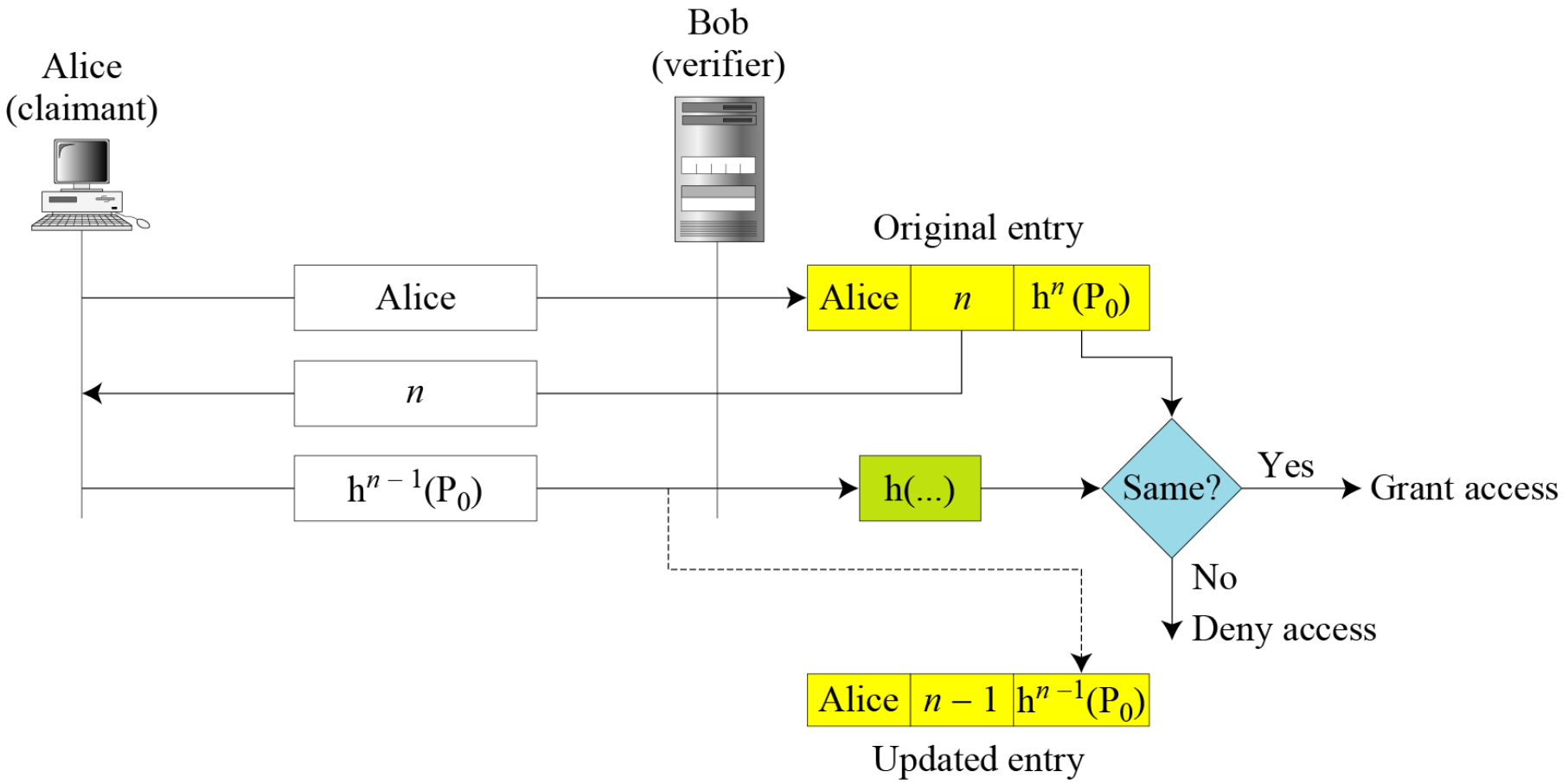
In the second approach, the user and the system agree to sequentially update the password.

Third Approach

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

$$h^n(x) = h(h^{n-1}(x)) \quad h^{n-1}(x) = h(h^{n-2}(x)) \quad \ldots \quad h^2(x) = h(h(x)) \quad h^1(x) = h(x)$$

Figure 14.4 *Lamport one-time password*



14-3 CHALLENGE-RESPONSE

In password authentication, the claimant proves her identity by demonstrating that she knows a secret, the password. In challenge-response authentication, the claimant proves that she knows a secret without sending it.

Topics discussed in this section:

14-3 Continue

Note

In challenge-response authentication, the claimant proves that she knows a secret without sending it to the verifier.

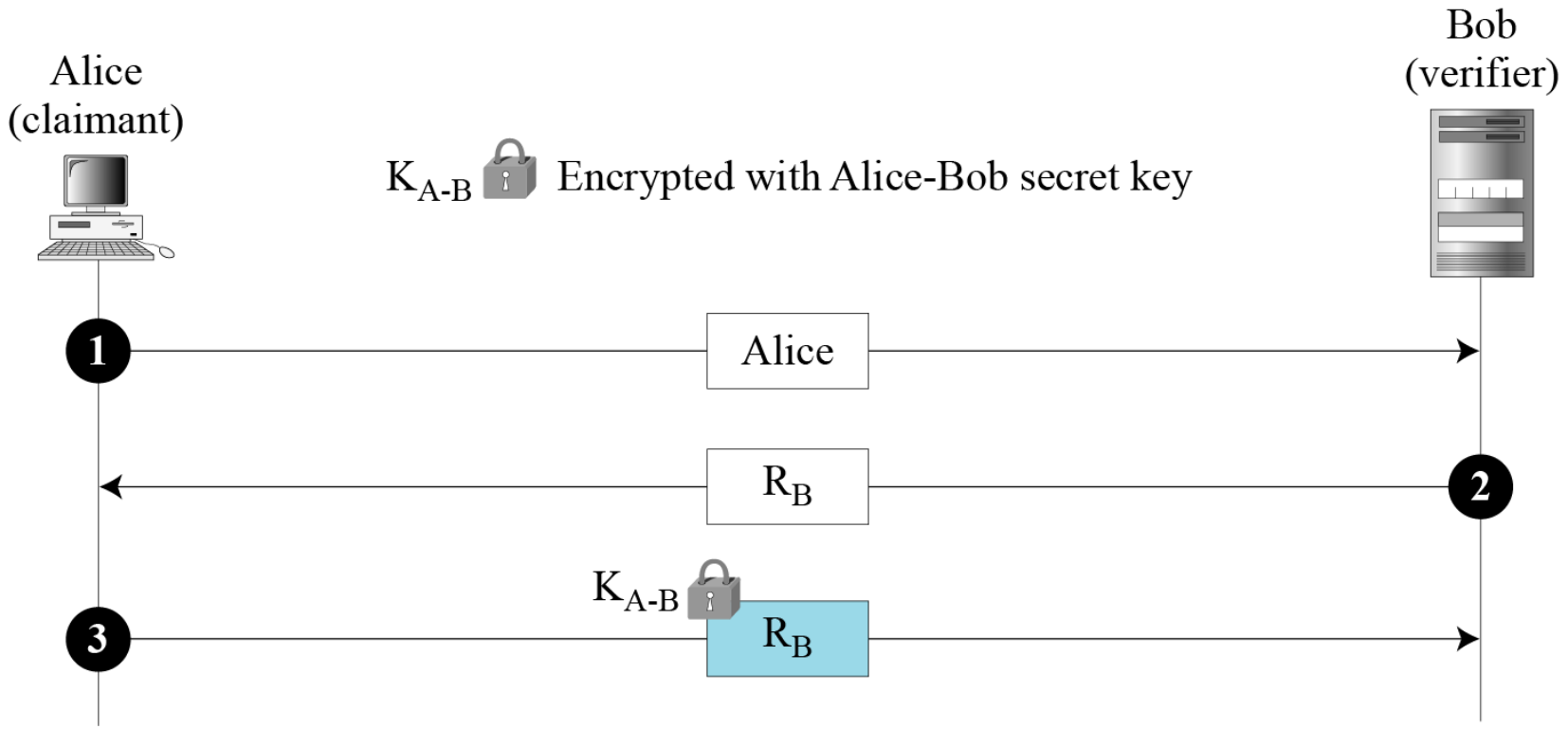
Note

The challenge is a time-varying value sent by the verifier; the response is the result of a function applied on the challenge.

14.3.1 Using a Symmetric-Key Cipher

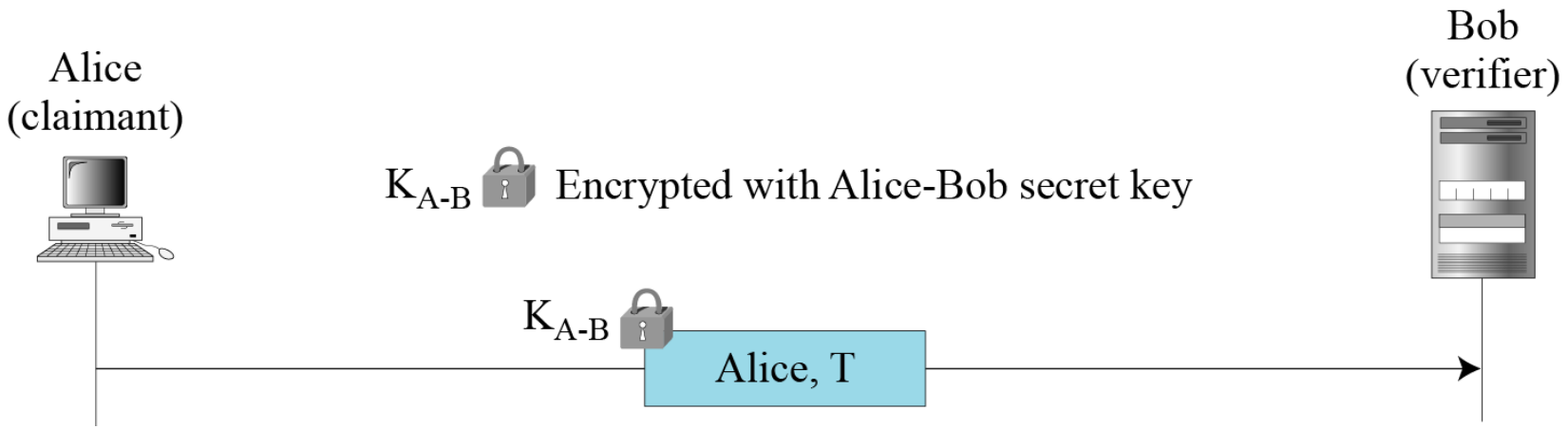
First Approach

Figure 14.5 *Nonce challenge*



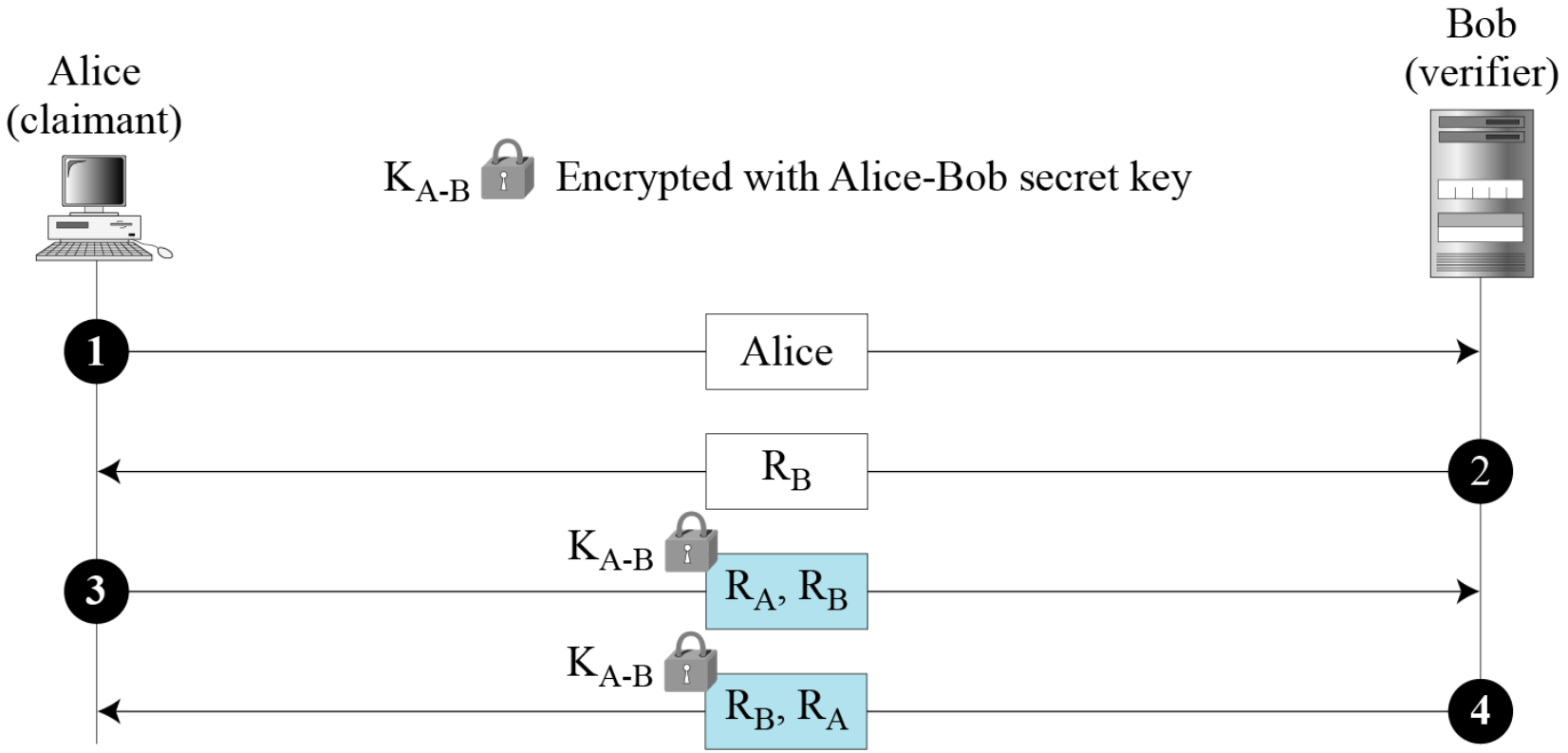
Second Approach

Figure 14.6 *Timestamp challenge*



Third Approach.

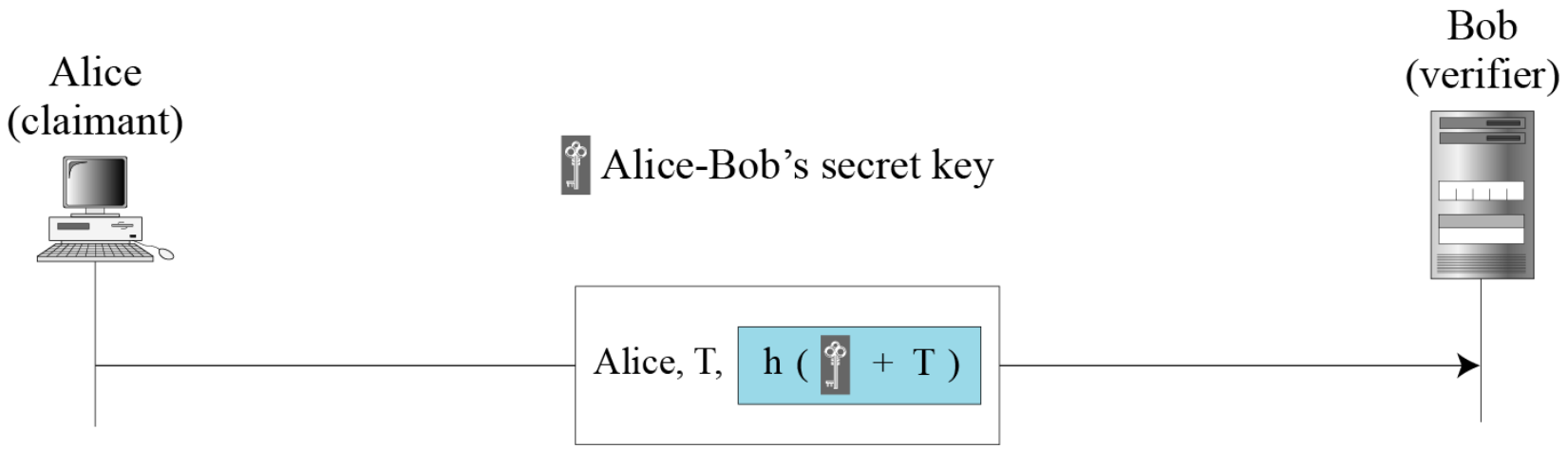
Figure 14.7 ***Bidirectional authentication***



14.3.2 Using Keyed-Hash Functions

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

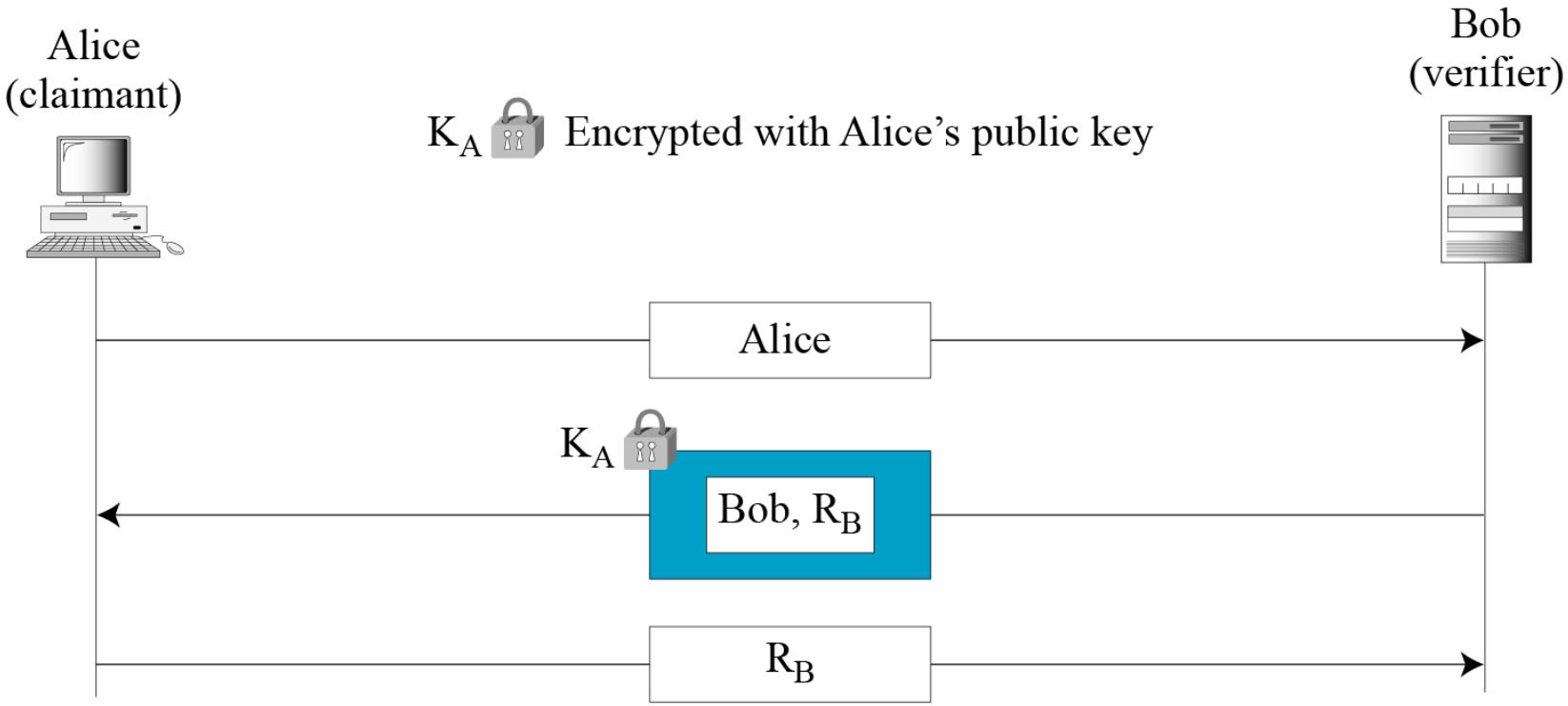
Figure 14.8 *Keyed-hash function*



14.3.3 Using an Asymmetric-Key Cipher

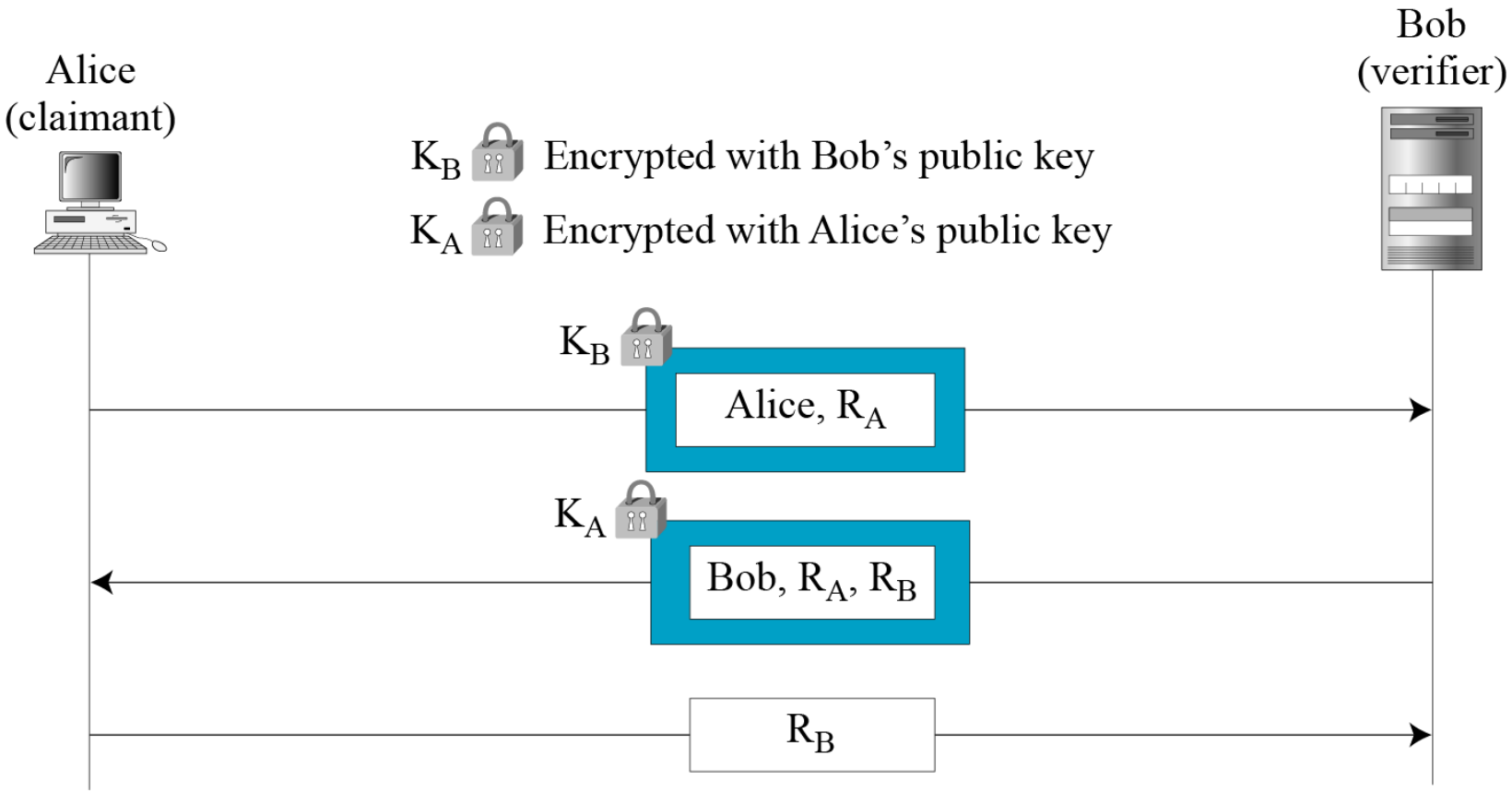
First Approach

Figure 14.9 *Unidirectional, asymmetric-key authentication*



Second Approach

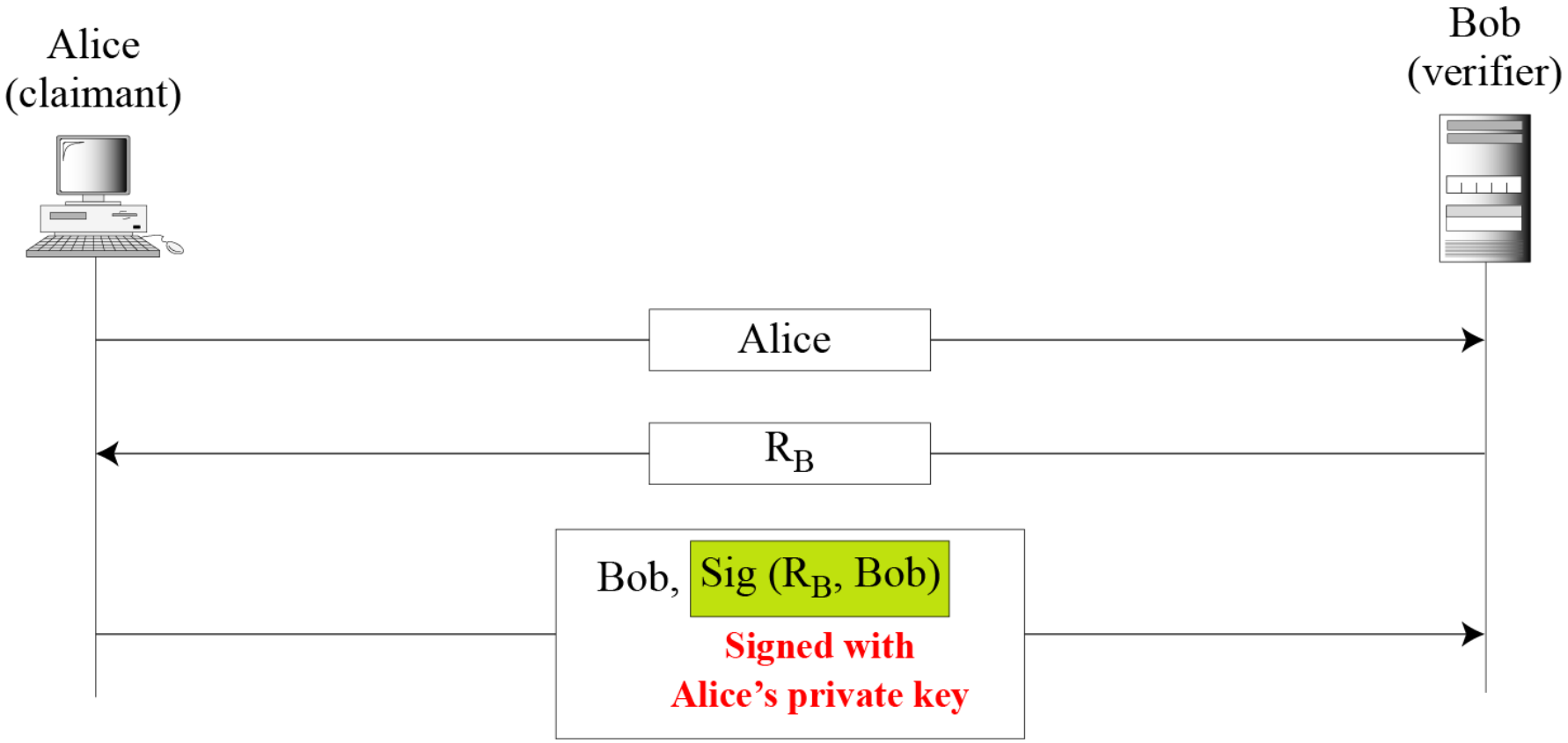
Figure 14.10 *Bidirectional, asymmetric-key*



14.3.4 Using Digital Signature

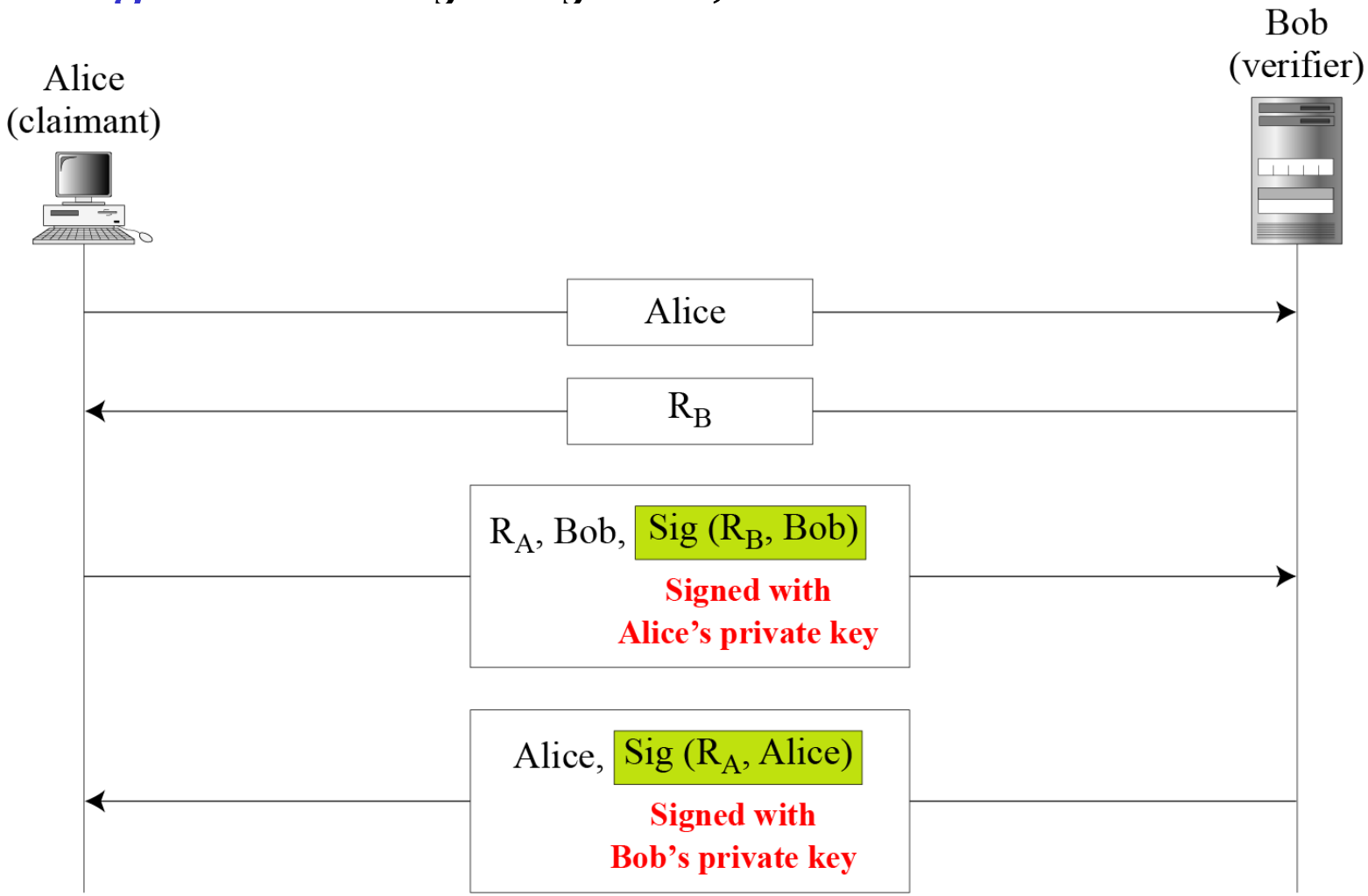
First Approach

Figure 14.11 *Digital signature, unidirectional*



Second Approach

Figure 14.12 *Digital signature, bidirectional authentication*



14-4 ZERO-KNOWLEDGE

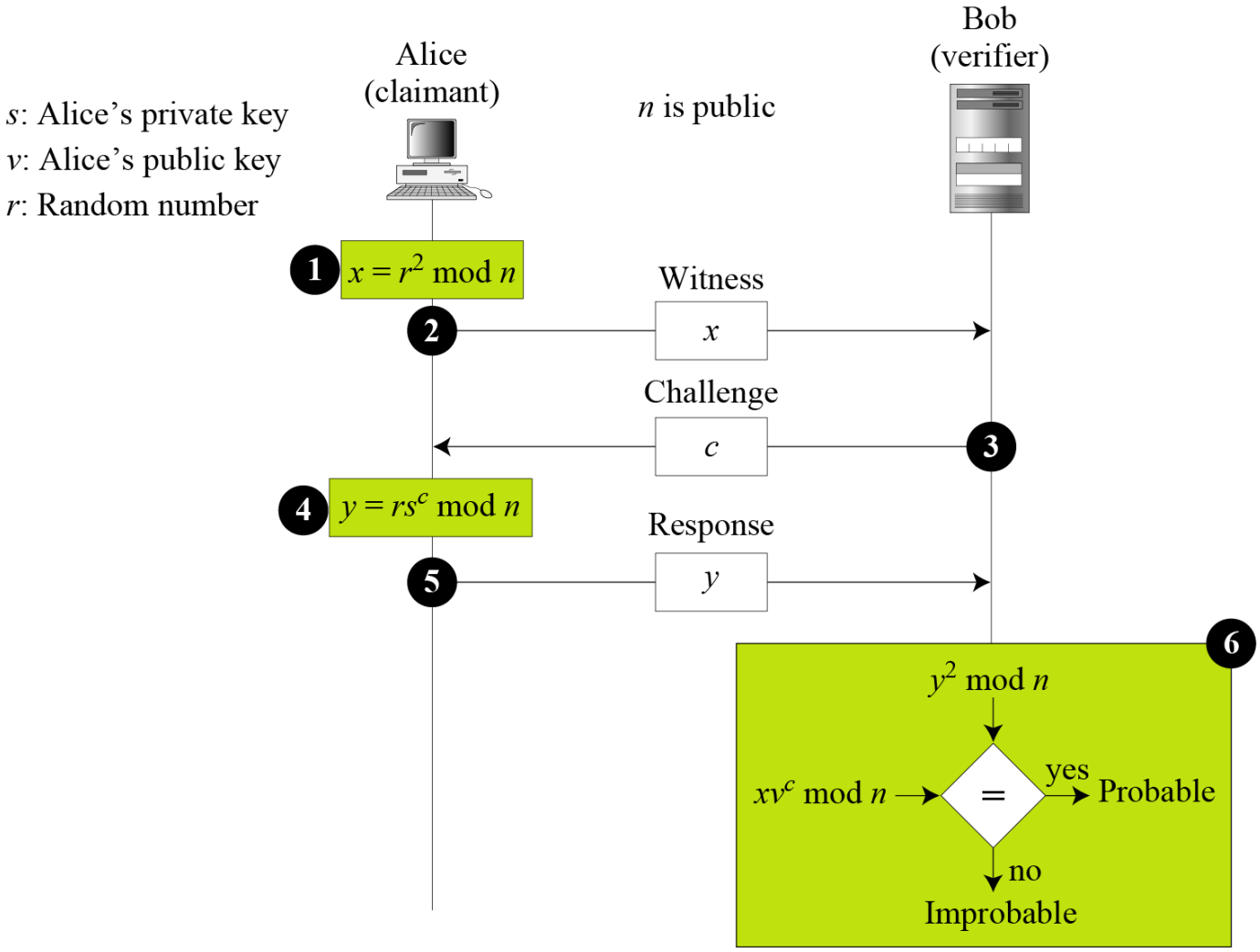
In zero-knowledge authentication, the claimant does not reveal anything that might endanger the confidentiality of the secret. The claimant proves to the verifier that she knows a secret, without revealing it. The interactions are so designed that they cannot lead to revealing or guessing the secret.

Topics discussed in this section:

14.4.1 Fiat-Shamir Protocol
14.4.2 Feige-Fiat-Shamir Protocol
14.4.3 Guillou-Quisquater Protocol

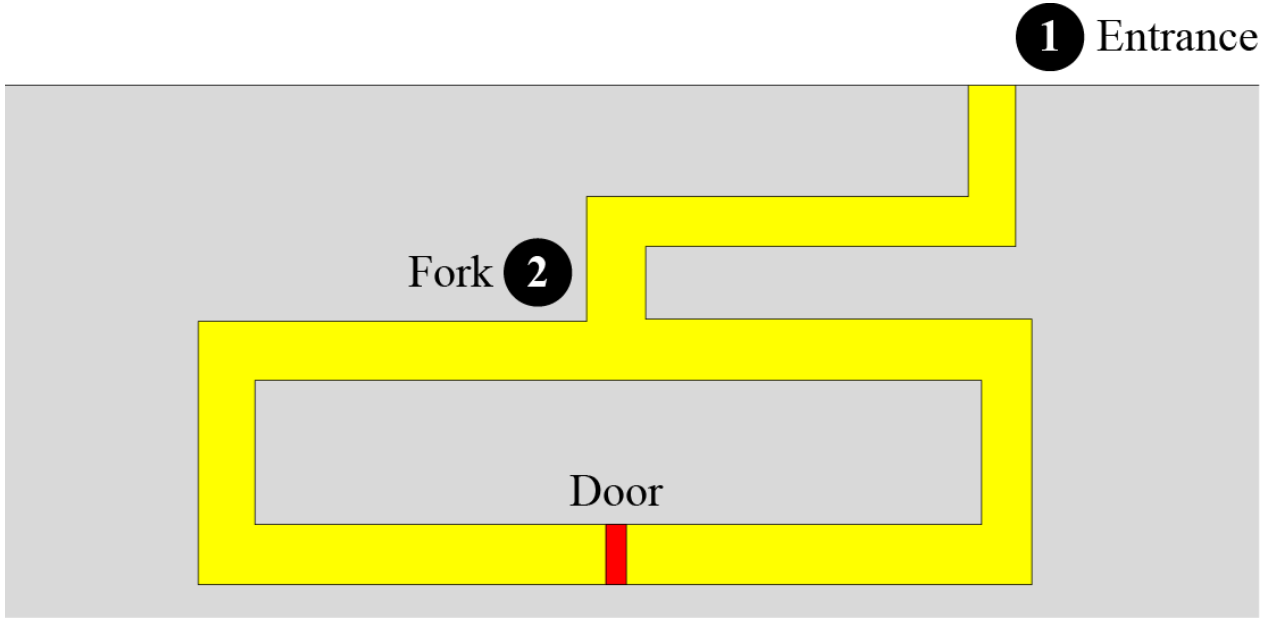
14.4.1 Fiat-Shamir Protocol

Figure 14.13 *Fiat-Shamir protocol*



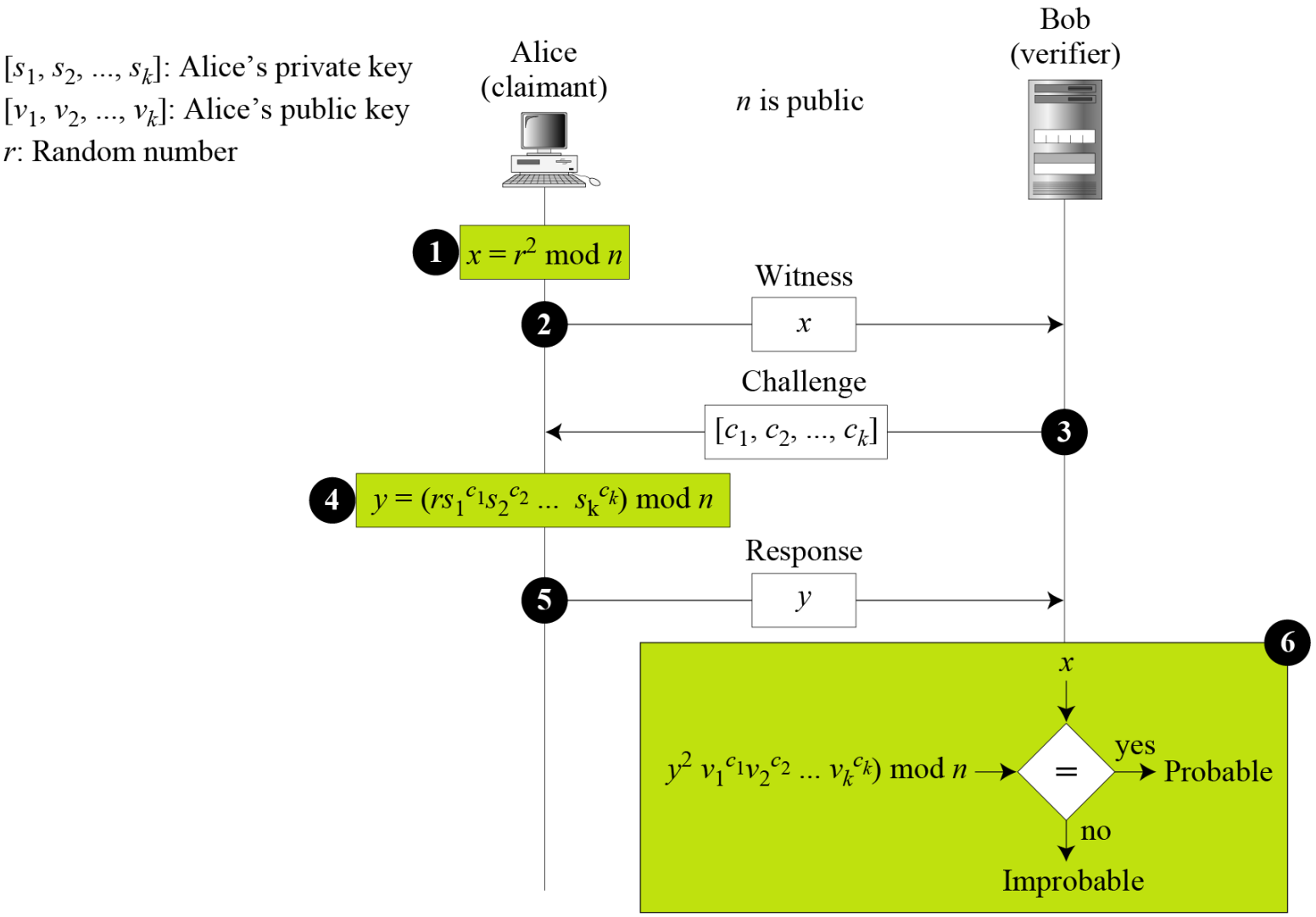
Cave Example

Figure 14.14 *Cave example*



14.4.2 Feige-Fiat-Shamir Protocol

Figure 14.15 *Feige-Fiat-Shamir protocol*



14.4.3 Guillou-Quisquater Protocol

Figure 14.16 *Guillou-Quisquater protocol*

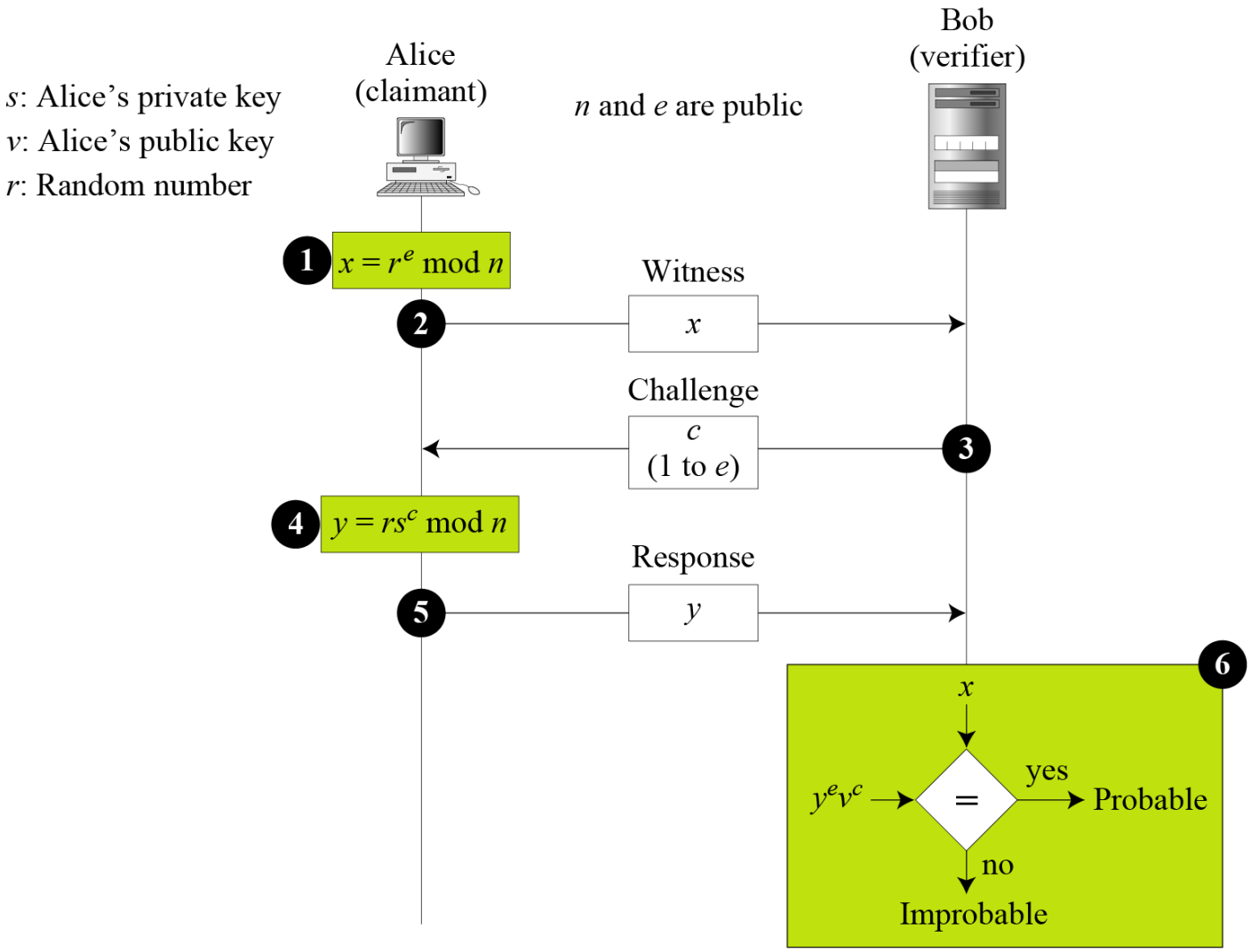
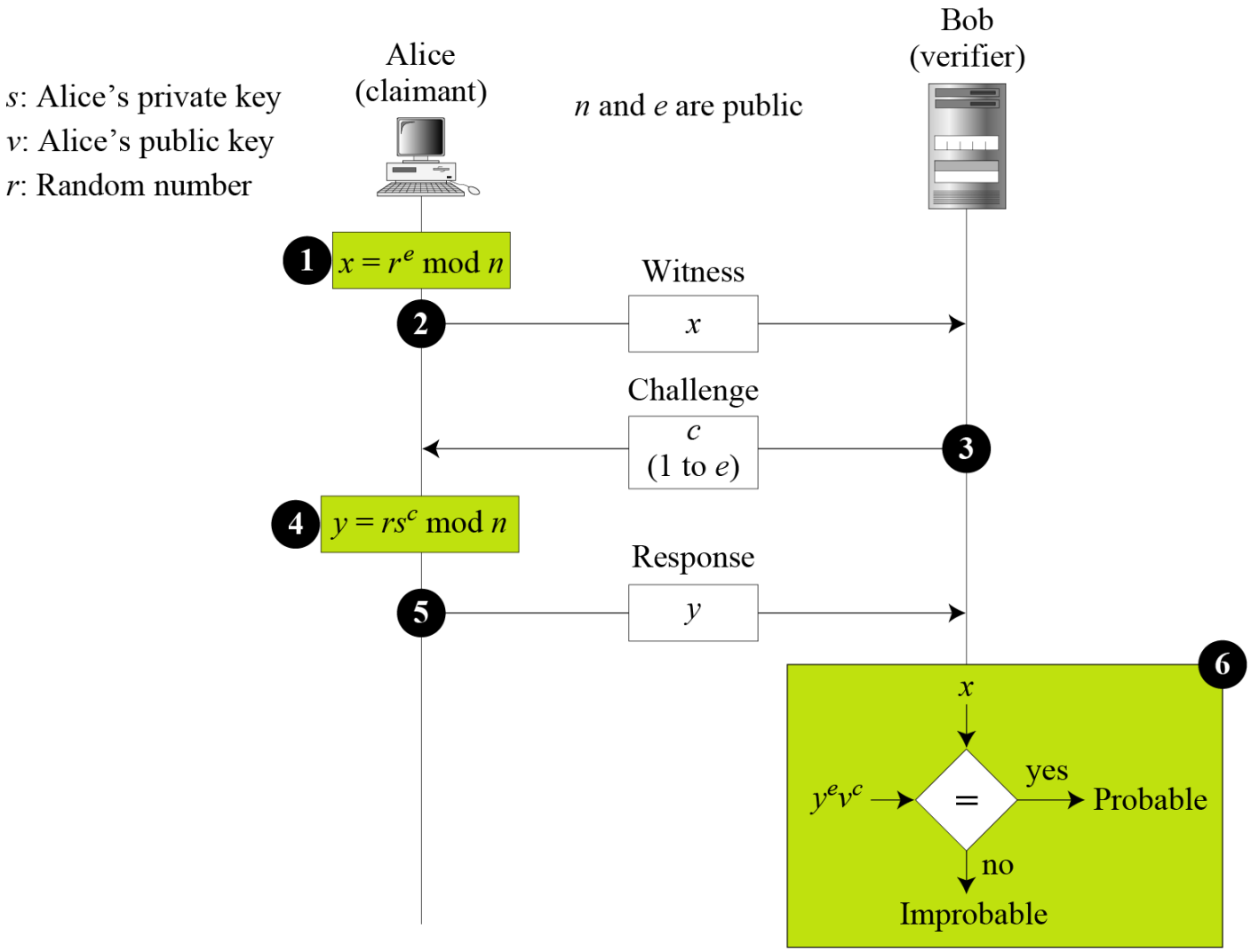


Figure 14.16 *Guillou-Quisquater protocol*



14-5 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.

Topics discussed in this section:

14.5.1 Components

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

14.5.2 Enrollment

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.

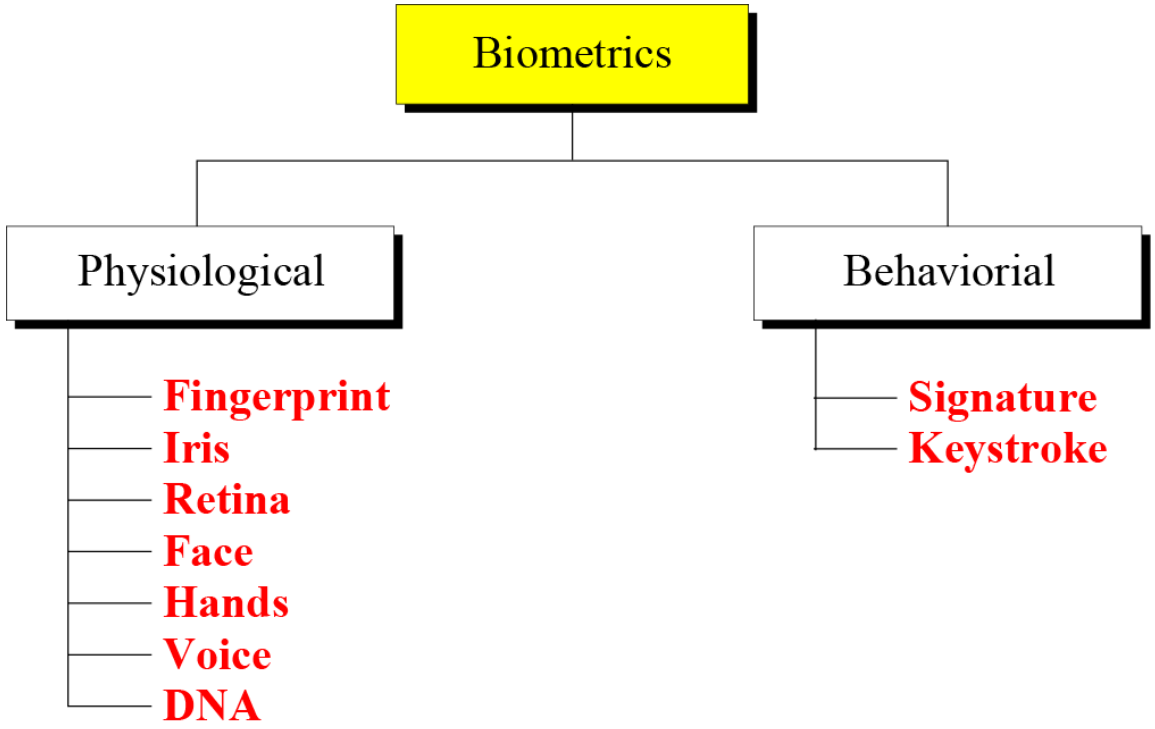
14.5.3 Authentication

Verification

Identification

14.5.4 Techniques

Figure 14.17 *Techniques*



14.5.4 Continued

Physiological Techniques

- Fingerprint
- Hands
- Iris
- Voice
- Retina
- DNA
- Face

14.5.4 Continued

Behavioral Techniques

- ***Signature***
- ***Keystroke***

14.5.5 Accuracy

False Rejection Rate (FRR)

False Acceptance Rate (FAR)

14.5.6 Applications

Several applications of biometrics are already in use. In commercial environments, these include access to facilities, access to information systems, transaction at point-ofsales, 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.