



Cryptography and Network Security

Eighth Edition
by William Stallings



Chapter 15

Cryptographic Key Management and Distribution

Cryptographic Key Management

- The secure use of cryptographic key algorithms depends on the protection of the cryptographic keys
- *Cryptographic key management* is the process of administering or managing cryptographic keys for a cryptographic system
 - It involves the generation, creation, protection, storage, exchange, replacement, and use of keys and enables selective restriction for certain keys
- In addition to access restriction, key management also involves the monitoring and recording of each key's access, use, and context
- A key management system will also include key servers, user procedures, and protocols
- The security of the cryptosystem is dependent upon successful key management

Key Distribution Technique

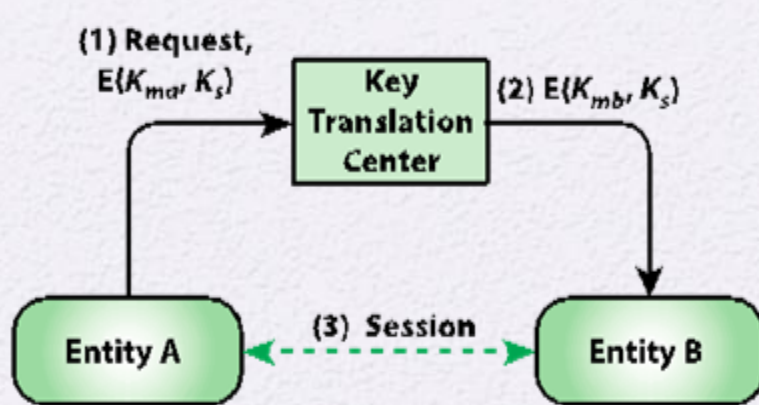
- Term that refers to the means of delivering a key to two parties who wish to exchange data without allowing others to see the key
- For symmetric encryption to work, the two parties to an exchange must share the same key, and that key must be protected from access by others
- Frequent key changes are desirable to limit the amount of data compromised if an attacker learns the key

Symmetric Key Distribution

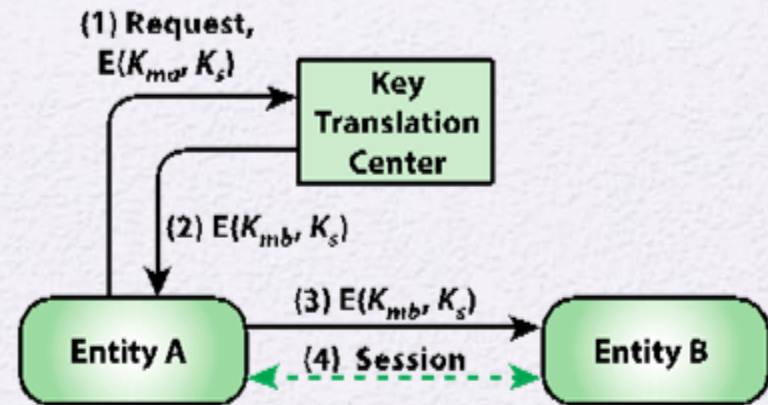
Given parties A and B, key distribution can be achieved in a number of ways:

- A can select a key and physically deliver it to B
- A third party can select the key and physically deliver it to A and B
- If A and B have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key
- If A and B each has an encrypted connection to a third party C, C can deliver a key on the encrypted links to A and B

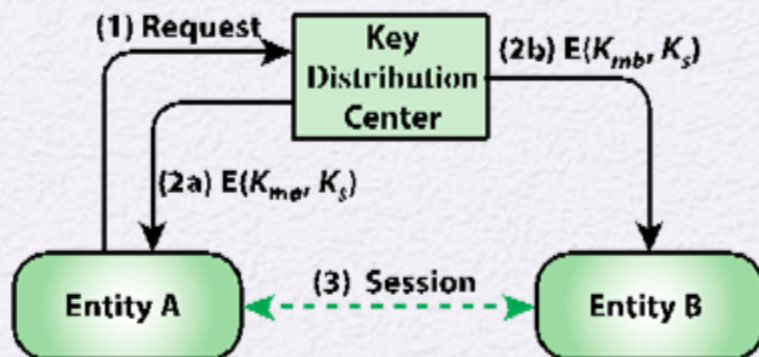




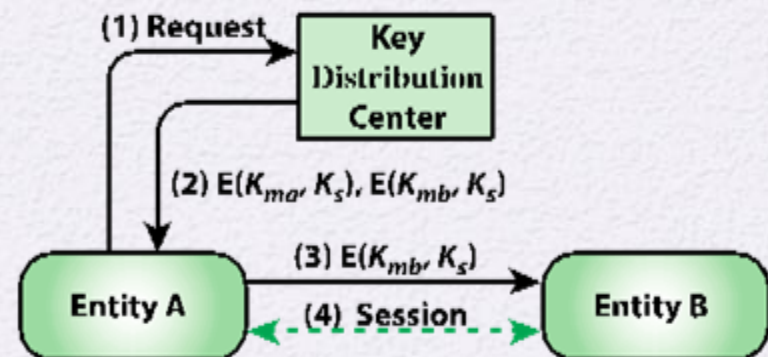
(a) Key Translation



(b) Key Translation with Key Forwarding



(c) Key Distribution



(d) Key Distribution with Key Forwarding

Figure 15.1 Key Distribution Between Two Communicating Entities

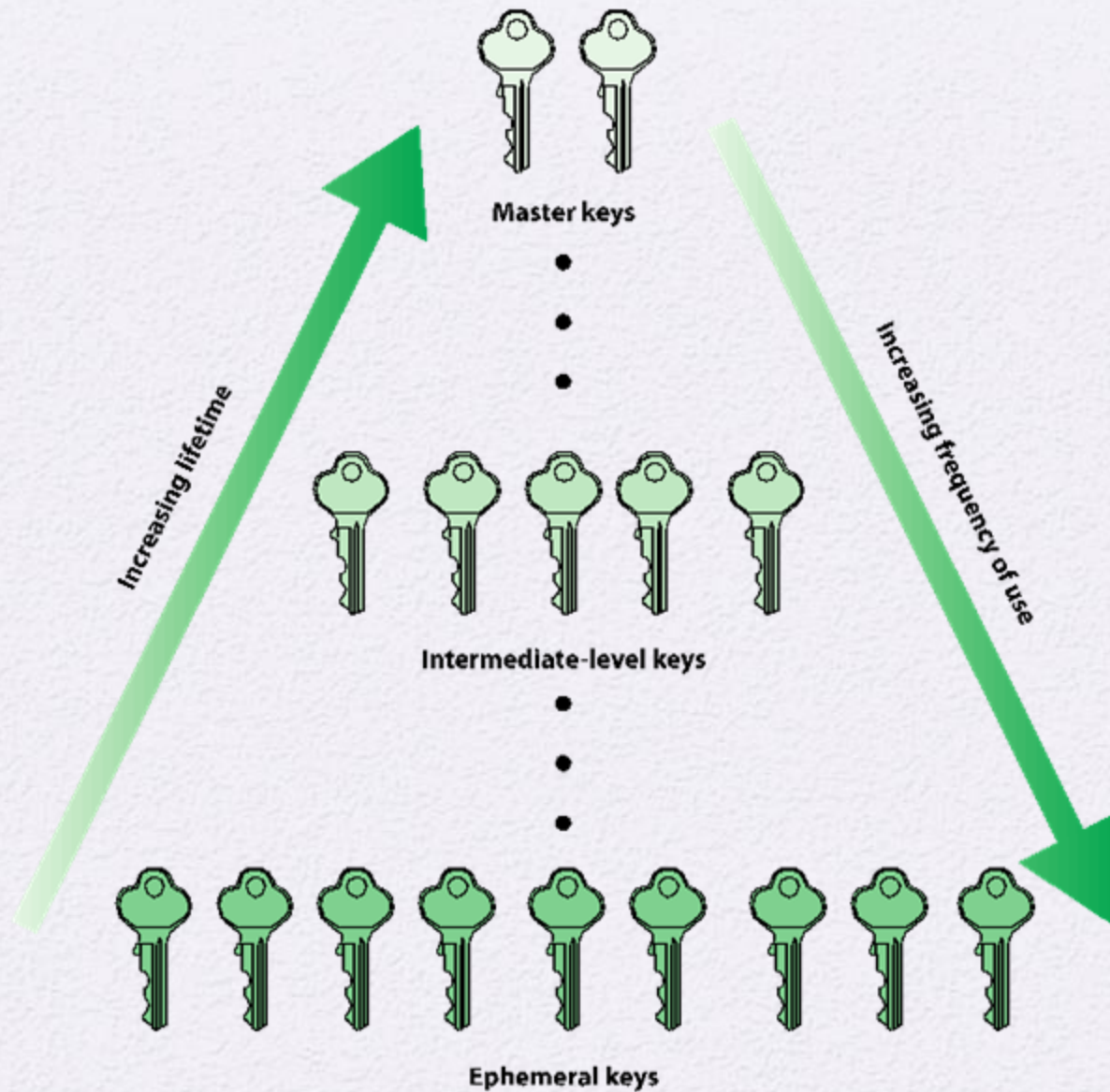


Figure 15.2 Symmetric Key Hierarchy

Symmetric Key Distribution

Asymmetric encryption

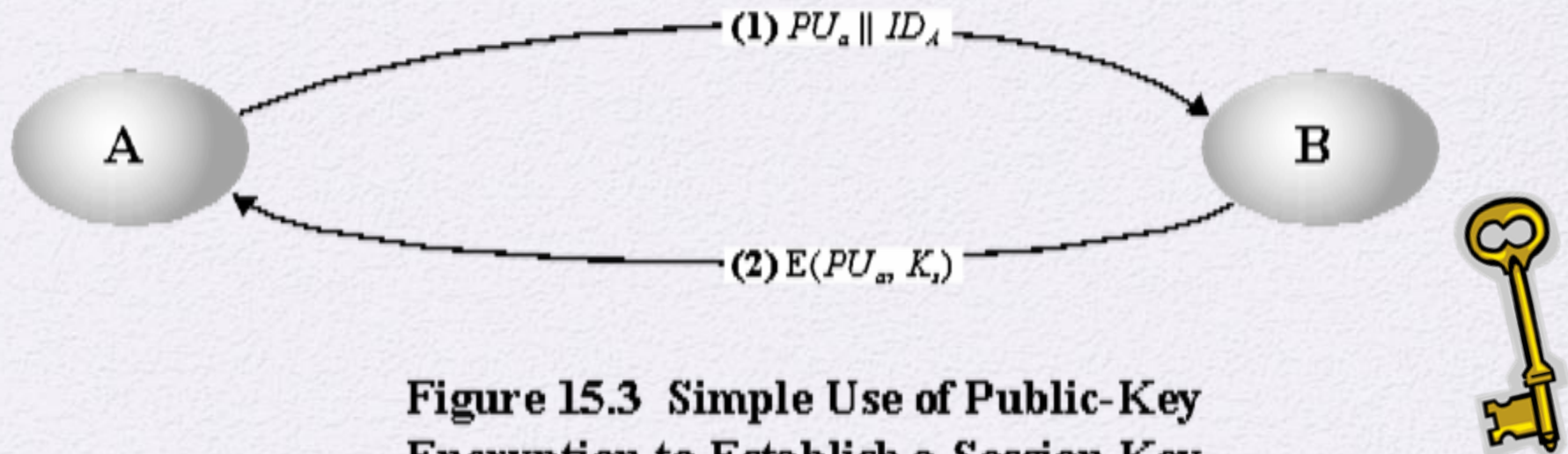


Figure 15.3 Simple Use of Public-Key Encryption to Establish a Session Key

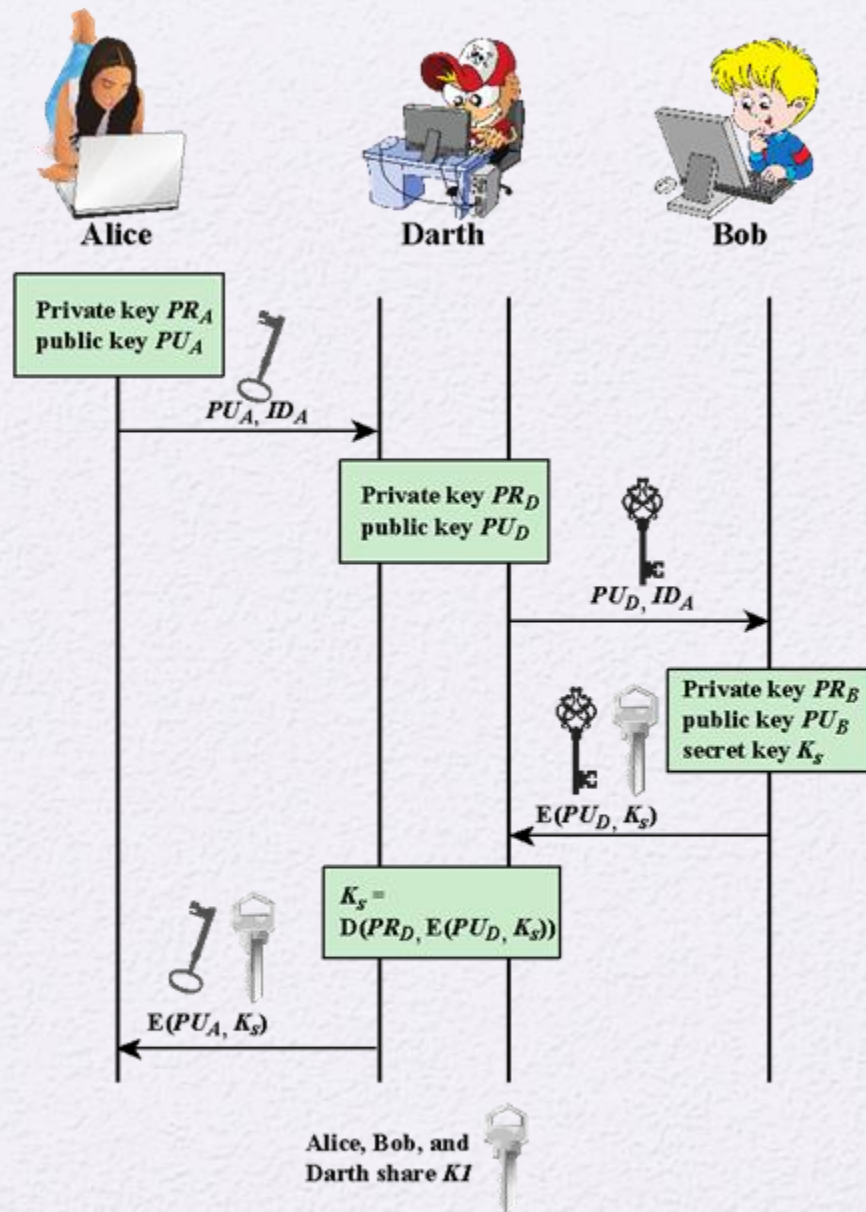


Figure 15.4 Another Man-in-the-Middle Attack

Symmetric Key Distribution

Asymmetric encryption

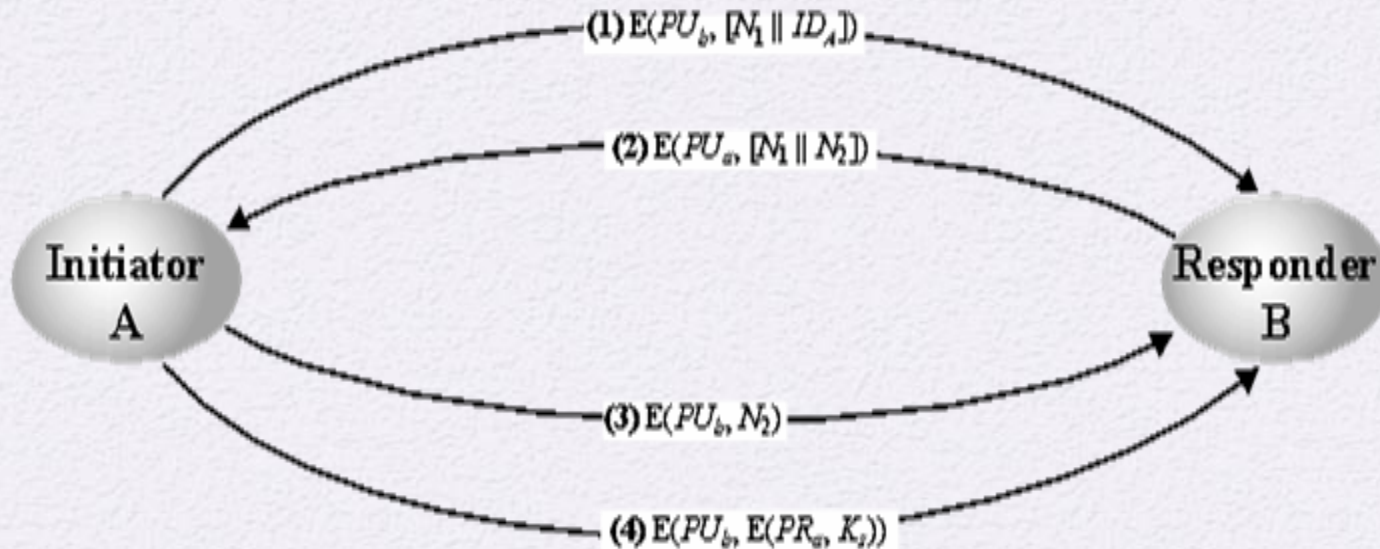


Figure 15.5 Public-Key Distribution of Secret Keys

Ensures confidentiality and authentication

Public Key Distribution

Public announcement of public keys

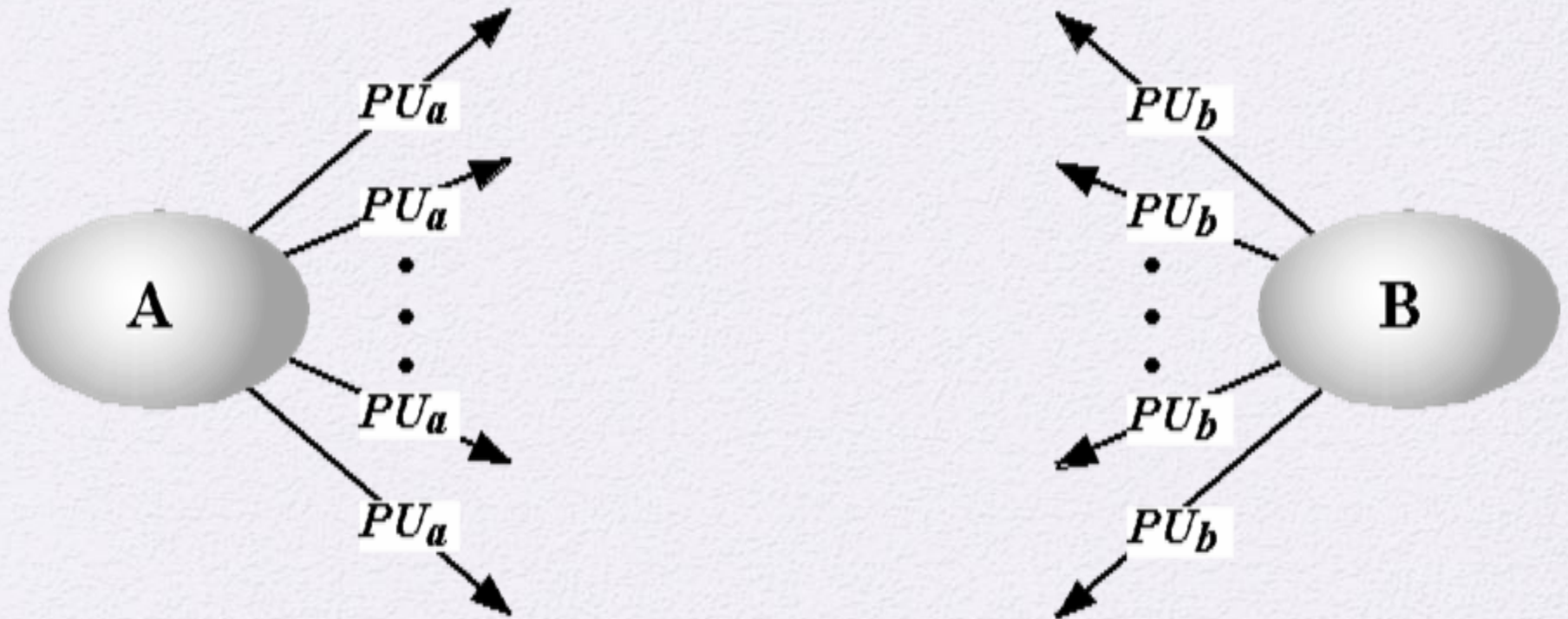


Figure 15.6 Uncontrolled Public Key Distribution

Publicly Available Directory

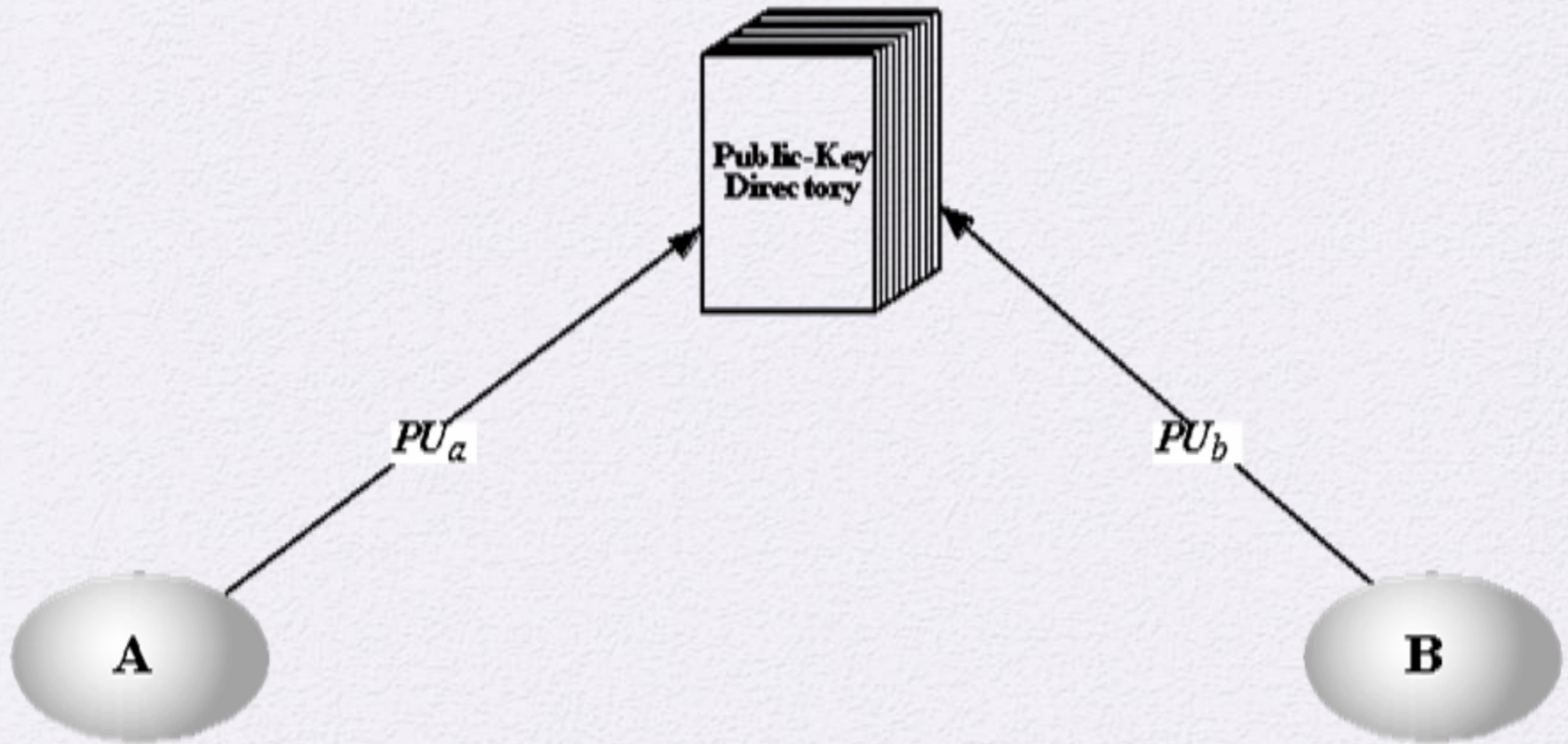


Figure 15.7 Public Key Publication

Public Key Authority

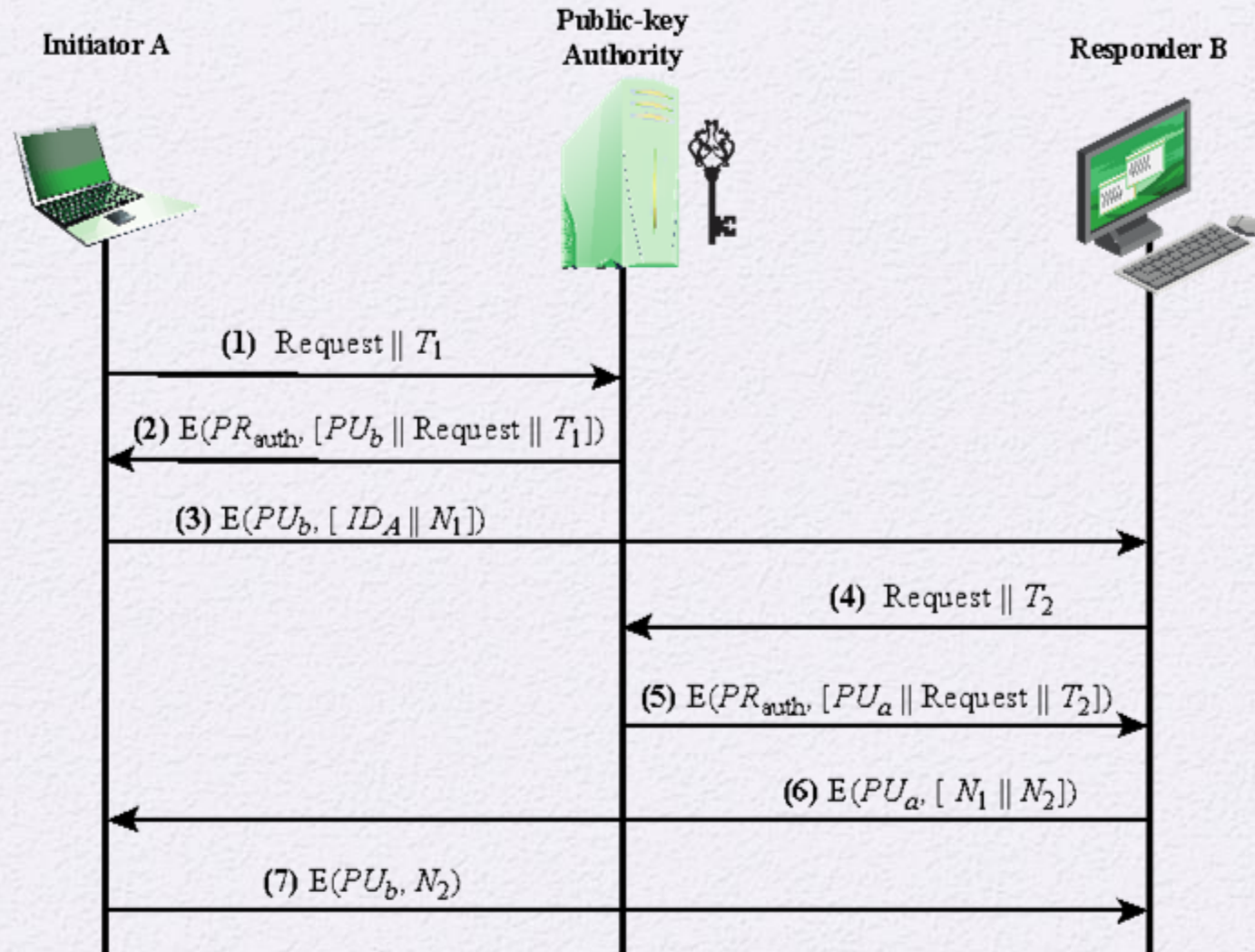
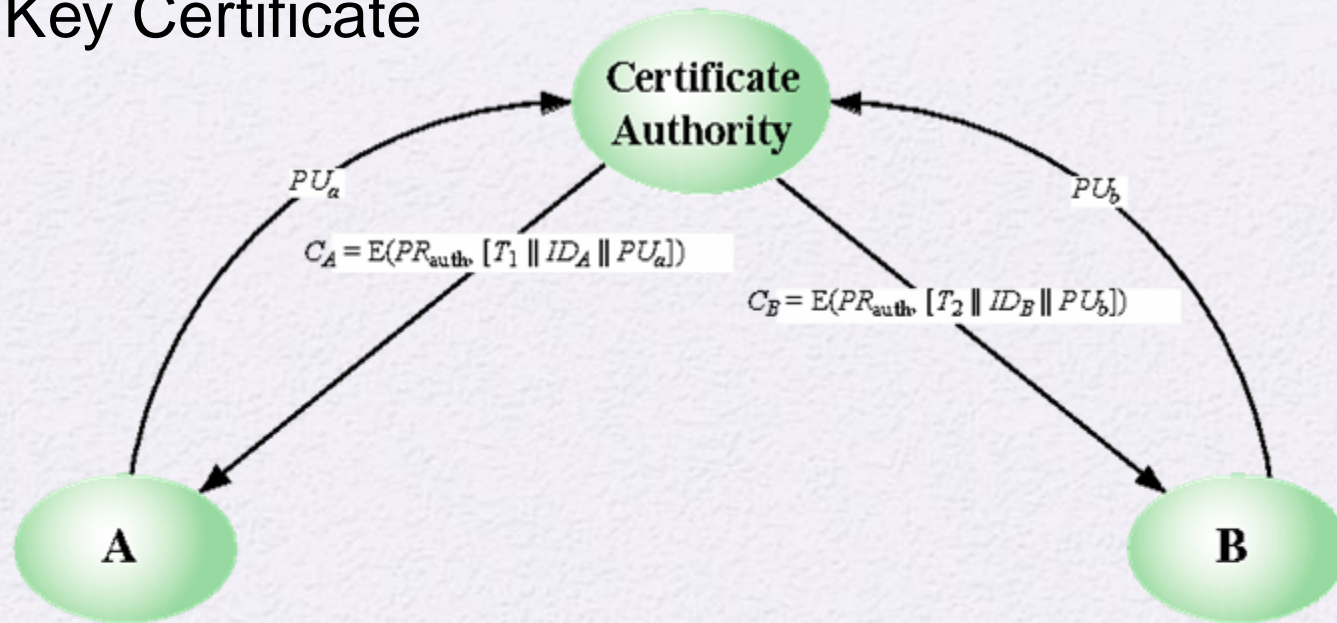
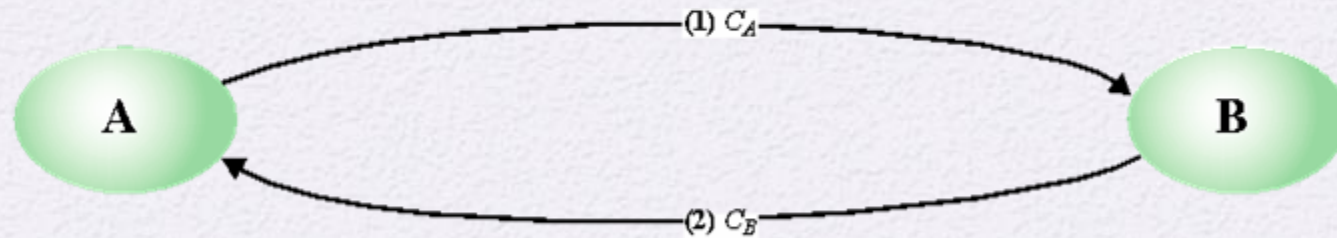


Figure 15.8 Public-Key Distribution Scenario

Public Key Certificate



(a) Obtaining certificates from CA



(b) Exchanging certificates

Figure 15.9 Exchange of Public-Key Certificates

X.509 Certificates

- Part of the X.500 series of recommendations that define a directory service
 - The directory is, in effect, a server or distributed set of servers that maintains a database of information about users
- X.509 defines a framework for the provision of authentication services by the X.500 directory to its users
 - Was initially issued in 1988 with the latest revision in 2016
 - Based on the use of public-key cryptography and digital signatures
 - Does not dictate the use of a specific algorithm but recommends RSA
 - Does not dictate a specific hash algorithm
- Each certificate contains the public key of a user and is signed with the private key of a trusted certification authority
- X.509 defines alternative authentication protocols based on the use of public-key certificates

Certificates

Created by a
trusted
Certification
Authority (CA)
and have the
following
elements:

- Version
- Serial number
- Signature algorithm identifier
- Issuer name
- Period of validity
- Subject name
- Subject's public-key information
- Issuer unique identifier
- Subject unique identifier
- Extensions
- Signature

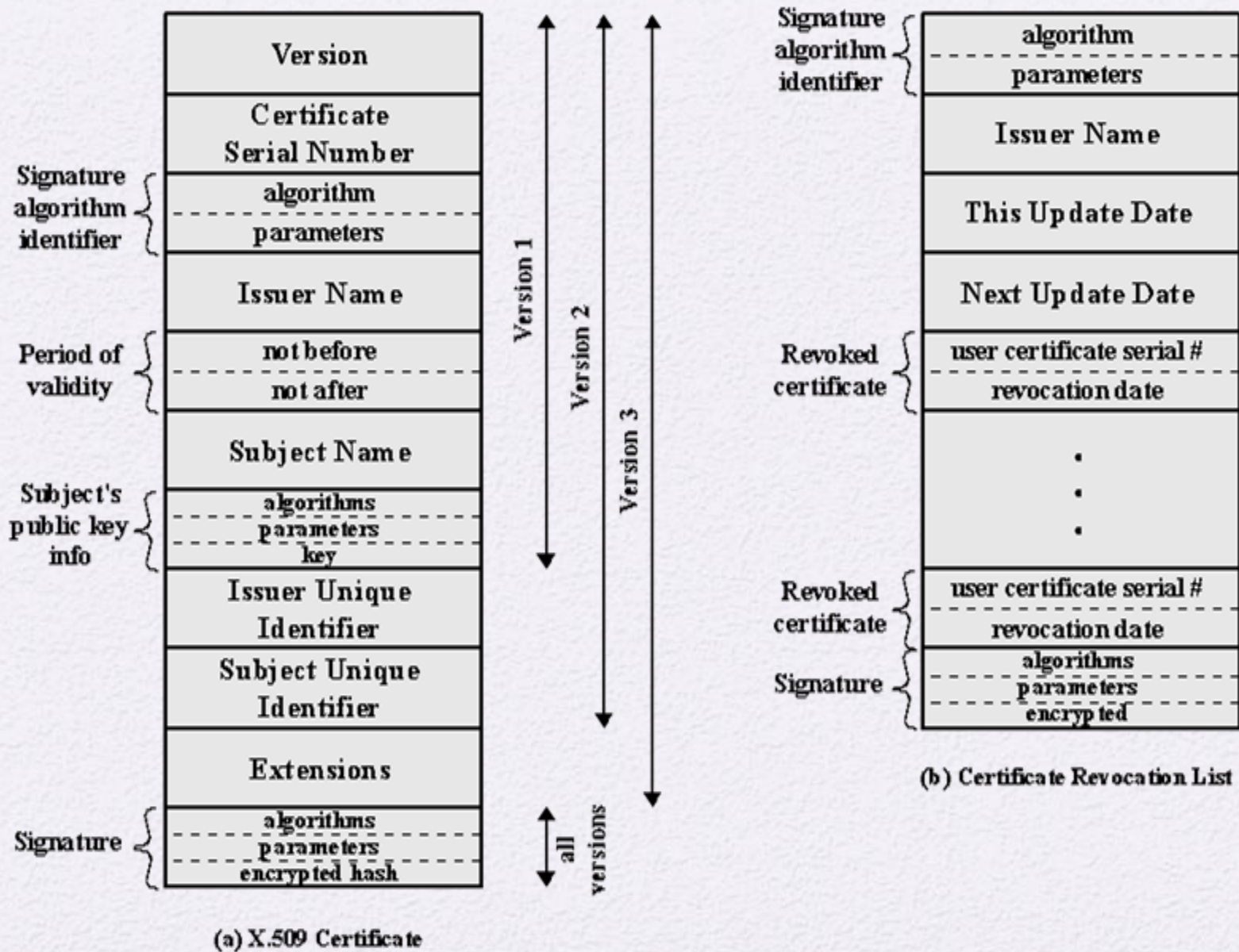


Figure 15.11 X.509 Formats

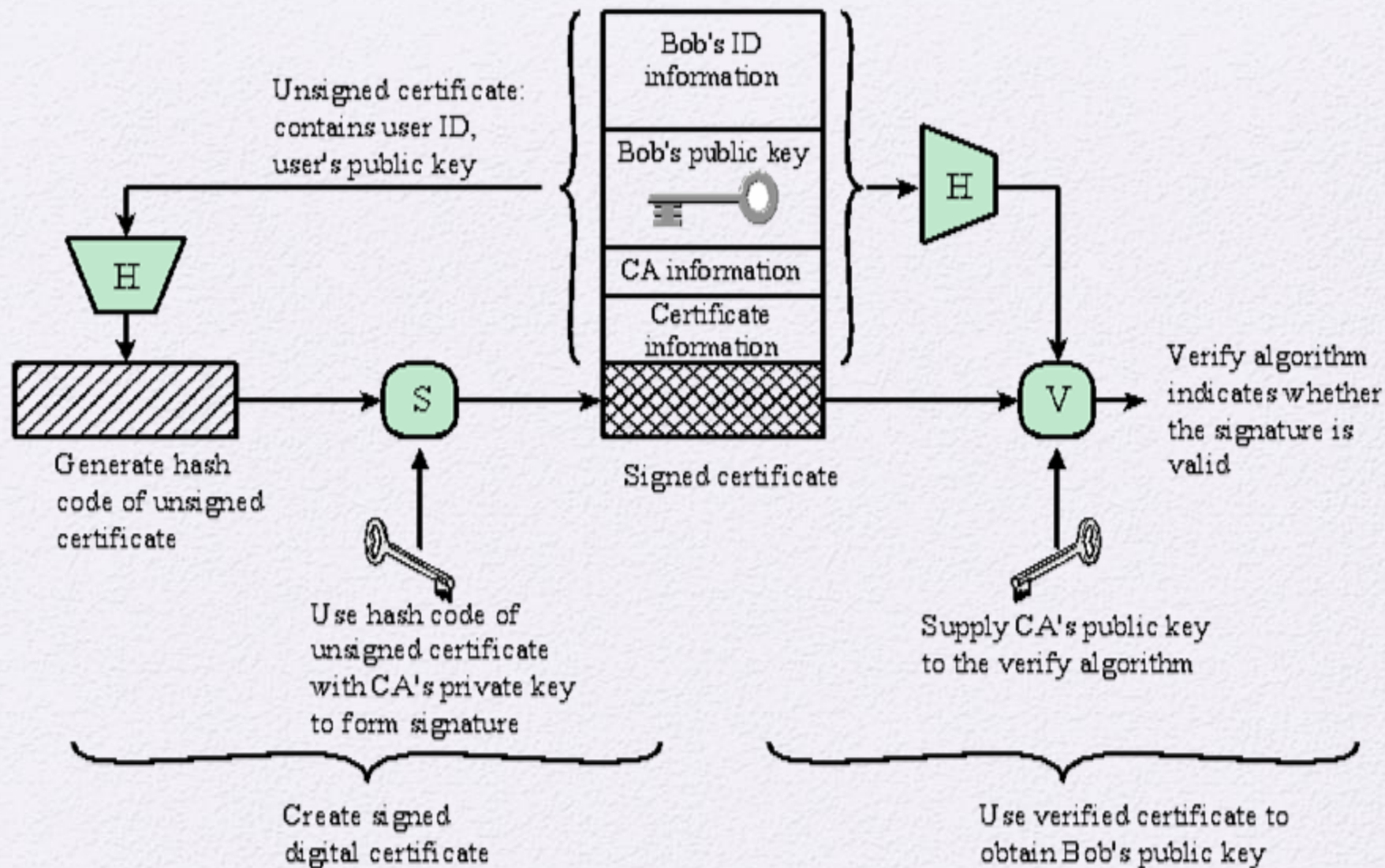


Figure 15.10 Public-Key Certificate Use

Obtaining a Certificate

User certificates generated by a CA have the following characteristics:

- Any user with access to the public key of the CA can verify the user public key that was certified
- No party other than the certification authority can modify the certificate without this being detected

- Because certificates are unforgeable, they can be placed in a directory without the need for the directory to make special efforts to protect them
 - In addition, a user can transmit his or her certificate directly to other users
- Once B is in possession of A's certificate, B has confidence that messages it encrypts with A's public key will be secure from eavesdropping and that messages signed with A's private key are unforgeable

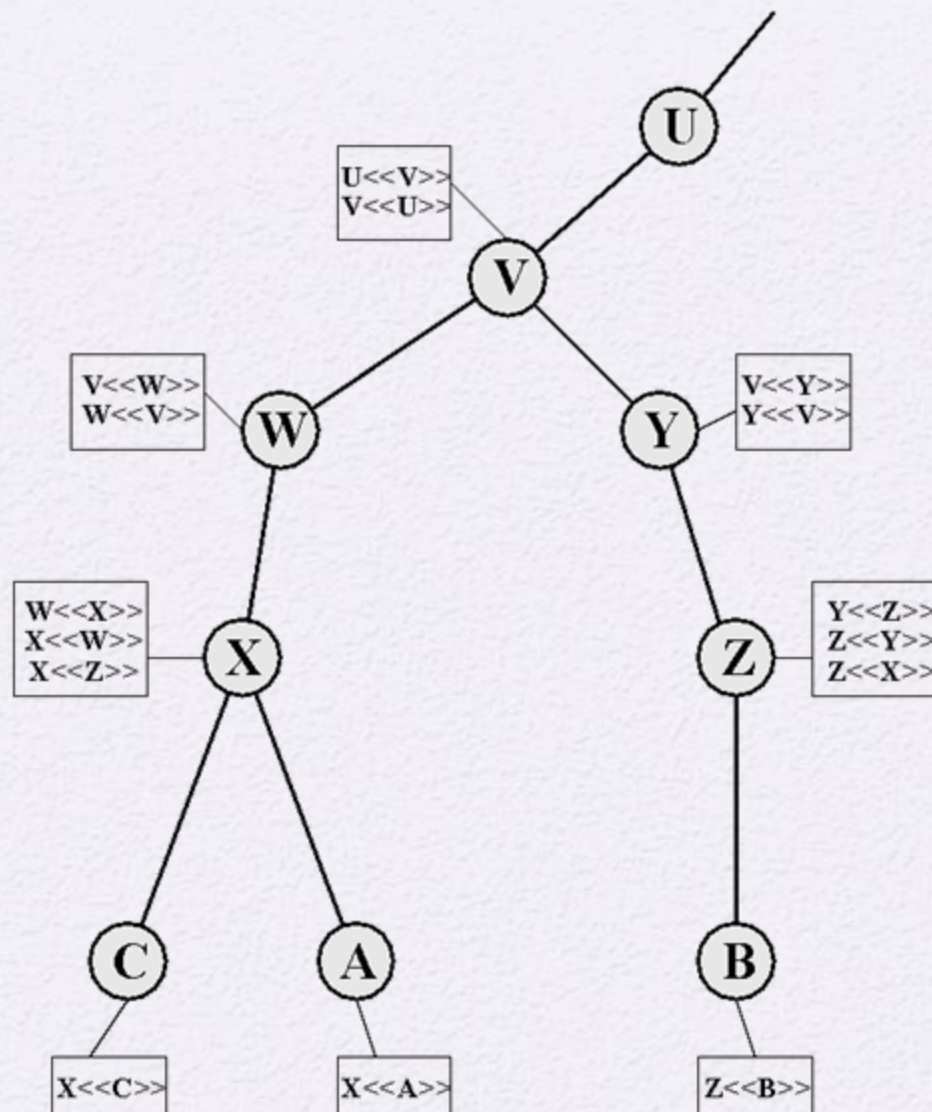


Figure 15.12 X.509 CA Hierarchy: a Hypothetical Example

Certificate Revocation

- Each certificate includes a period of validity
 - Typically a new certificate is issued just before the expiration of the old one
- It may be desirable on occasion to revoke a certificate before it expires, for one of the following reasons:
 - The user's private key is assumed to be compromised
 - The user is no longer certified by this CA
 - The CA's certificate is assumed to be compromised
- Each CA must maintain a list consisting of all revoked but not expired certificates issued by that CA
 - These lists should be posted on the directory



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

The security certificate presented by this website has expired or is not yet valid.

The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

✅ [Click here to close this webpage.](#)

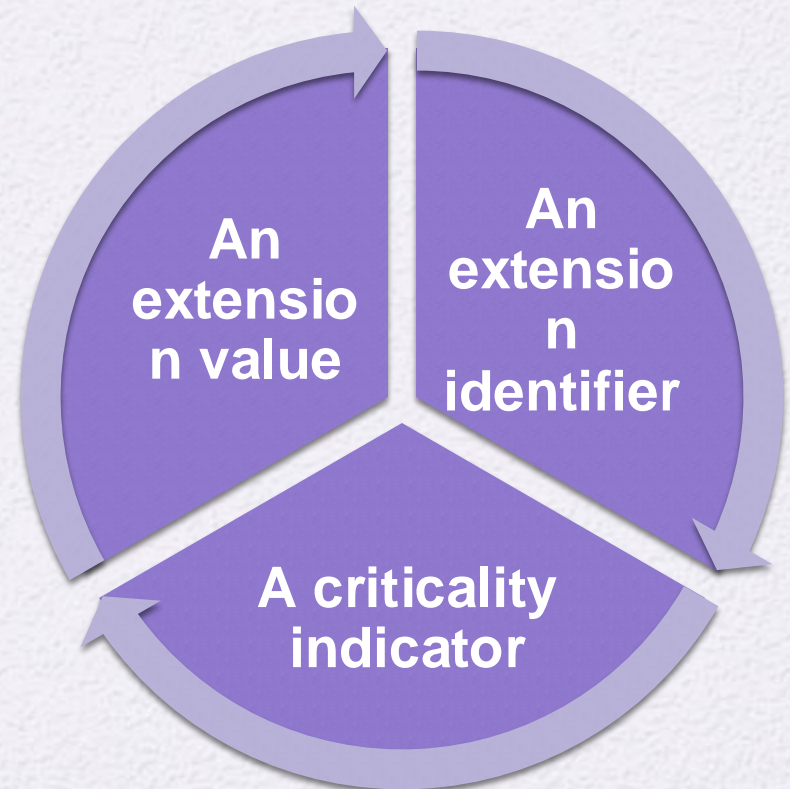
❌ [Continue to this website \(not recommended\).](#)

🔍 [More information](#)

X.509 Version 3

- Version 2 format does not convey all of the information that recent design and implementation experience has shown to be needed
- Rather than continue to add fields to a fixed format, standards developers felt that a more flexible approach was needed
 - Version 3 includes a number of optional extensions
- The certificate extensions fall into three main categories:
 - Key and policy information
 - Subject and issuer attributes
 - Certification path constraints

Each extension consists of:

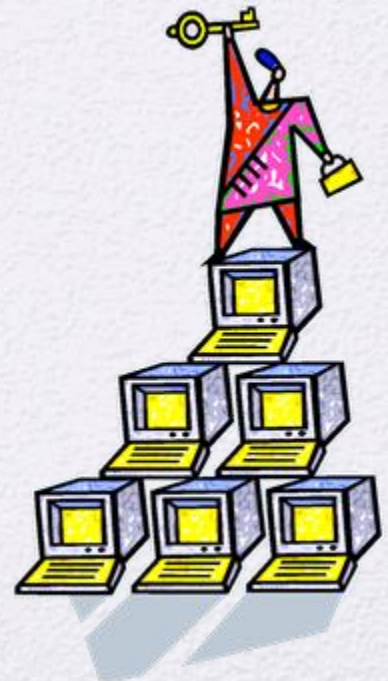


Key and Policy Information

- These extensions convey additional information about the subject and issuer keys plus indicators of certificate policy
- A certificate policy is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements

Included are:

- Authority key identifier
- Subject key identifier
- Key usage
- Private-key usage period
- Certificate policies
- Policy mappings



Certificate Subject and Issuer Attributes

- These extensions support alternative names, in alternative formats, for a certificate subject or certificate issuer
- Can convey additional information about the certificate subject to increase a certificate user's confidence that the certificate subject is a particular person or entity
- The extension fields in this area include:
 - Subject alternative name
 - Issuer alternative name
 - Subject directory attributes



Certification Path Constraints

- These extensions allow constraint specifications to be included in certificates issued for CAs by other CAs
- The constraints may restrict the types of certificates that can be issued by the subject CA or that may occur subsequently in a certification chain
- The extension fields in this area include:
 - Basic constraints
 - Name constraints
 - Policy constraints



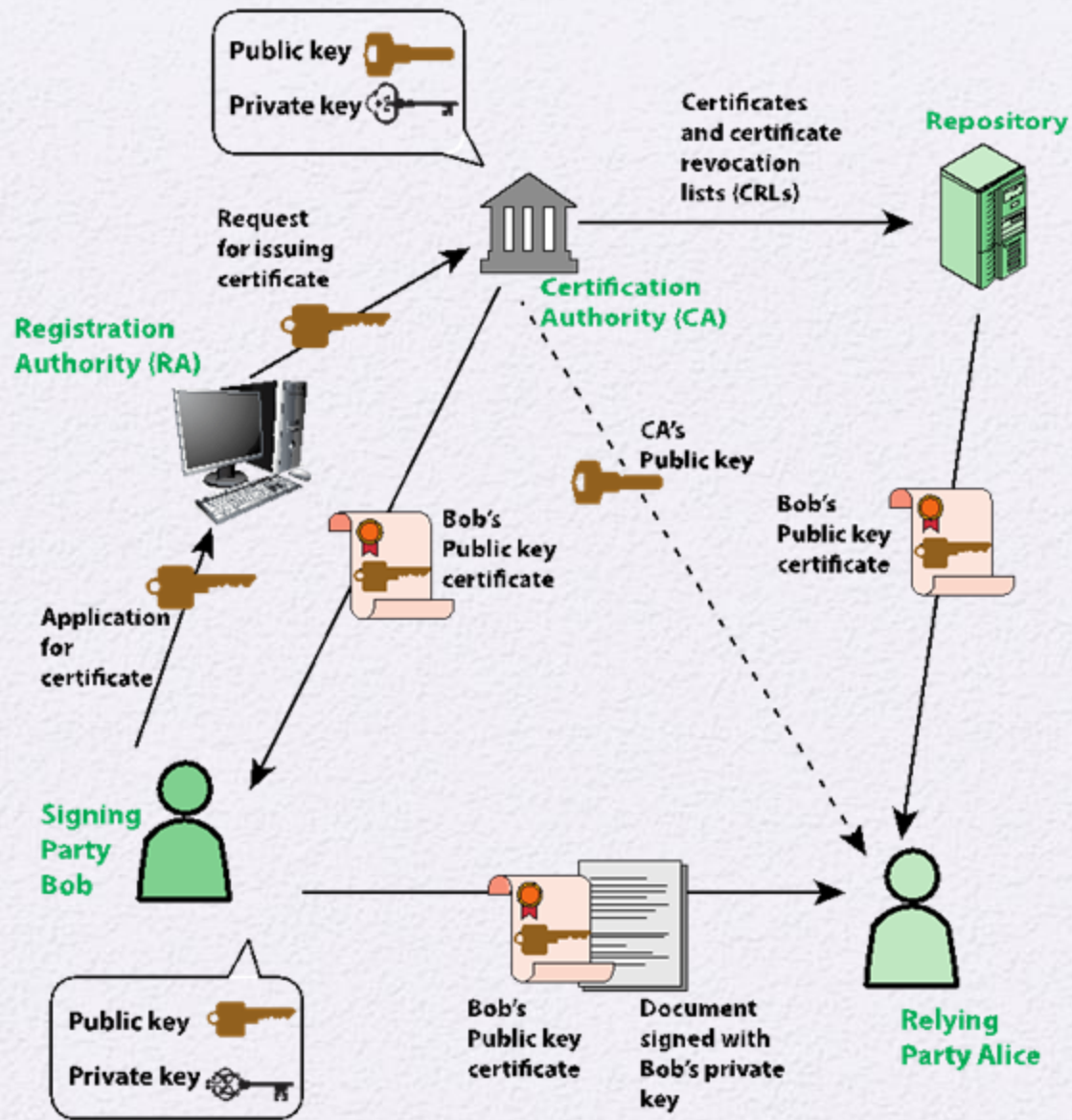



Figure 15.13 PKI Scenario

Summary

- Discuss the concept of a key hierarchy
 - Understand the issues involved in using asymmetric encryption to distribute symmetric keys
 - Present an overview of public-key infrastructure concepts
- 
- Present an overview of approaches to public-key distribution and analyze the risks involved in various approaches
 - List and explain the elements in an X.509 certificate