Security Threats and Security Solutions

Most Common Security Threats

- **Malicious code (malware, exploits)**
  - Drive-by downloads
  - Viruses
  - Worms
  - Ransomware
  - Trojan horses
  - Backdoors
  - Bots, botnets
  - Threats at both client and server levels

Virus	Worm	Trojan Horse
Virus is a software or computer program that connect itself to another software or computer program to harm computer system.	Worms replicate itself to cause slow down the computer system.	Trojan Horse rather than replicate capture some important information about a computer system or a computer network.
Virus replicates itself.	Worms are also replicates itself.	But Trojan horse does not replicate itself.
Virus can't be controlled by remote.	Worms can be controlled by remote.	Like worms, Trojan horse can also be controlled by remote.
Spreading rate of viruses are moderate.	While spreading rate of worms are faster than virus and Trojan horse.	And spreading rate of Trojan horse is slow in comparison of both virus and worms.
The main objective of virus to modify the information.	The main objective of worms to eat the system resources.	The main objective of Trojan horse to steal the information.
Viruses are executed via executable files.	Worms are executed via weaknesses in system.	Trojan horse executes through a program and interprets as utility software.

Most Common Security Threats (cont.)

- **Potentially unwanted programs (PUPs)**
  - Browser parasites:
    - report browsing habits
    - change browser settings
    - redirect search engine results
  - Adware:
    - any software with banner advertisements displayed while it is running
  - Spyware:
    - gather information about user without their knowledge

Most Common Security Threats (cont.)

- **Phishing**
  - Social engineering
  - E-mail scams
  - Spear-phishing
  - Identity fraud/theft

Most Common Security Threats (cont.)

- **Hacking**
  - Hackers vs. crackers

Hacker	Cracker
The good people who hack for knowledge purposes.	The evil person who breaks into a system for benefits.
They are skilled and have a advance knowledge of computers OS and programming languages.	They may or may not be skilled, some of crackers just knows a few tricks to steal data.
They work in an organization to help protecting there data and giving them expertise on internet security.	These are the person from which hackers protect organizations .

  - Types of hackers: white, black hats
  - Hacktivism

Most Common Security Threats (cont.)

- **Cyber vandalism:**
  - Disrupting, defacing, destroying Web site
- **Data breach**
  - Losing control over corporate information to outsiders

Most Common Security Threats (cont.)

- Credit card fraud/theft
- Spoofing and pharming
- Spam (junk) Web sites (link farms)
- Identity fraud/theft
- Denial of service (DoS) attack
  - Hackers flood site with useless traffic to overwhelm network
- Distributed denial of service (DDoS) attack

Most Common Security Threats (cont.)

- **Sniffing**
  - Eavesdropping program that monitors information traveling over a network
- **Insider attacks**
- **Poorly designed server and client software**
- **Social network security issues**

Most Common Security Threats (cont.)

- **Mobile platform security issues**
  - Smishing and Vishing:
    - types of phishing attacks that try to lure victims via SMS message and voice calls.
    - Both rely on the same emotional appeals employed in traditional phishing scams and are designed to drive you into urgent action.
  - Madware:
    - combining the words mobile and adware
- **Cloud security issues**

Technology Solutions

Technology Solutions

- **Protecting Internet communications**
  - Encryption
- **Securing channels of communication**
  - SSL, VPNs
- **Protecting networks**
  - Firewalls, Intrusion Detection System(IDS)
- **Protecting servers and clients**

Tools Available to Achieve Site Security

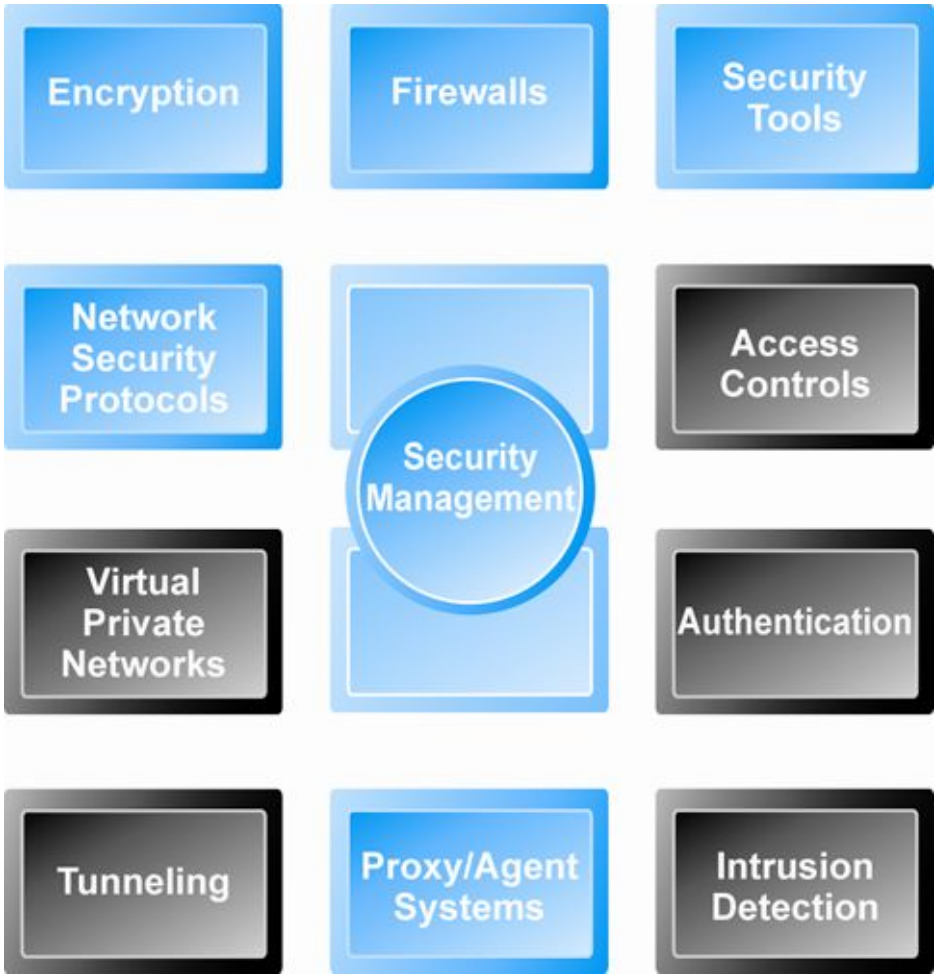


Figure 5.5, Page 276

Encryption

- **Encryption**
  - Transforms data into cipher text readable only by sender and receiver
  - Secures stored information and information transmission
  - Provides 4 of 6 key dimensions of e-commerce security:
    - Message integrity
    - Nonrepudiation
    - Authentication
    - Confidentiality

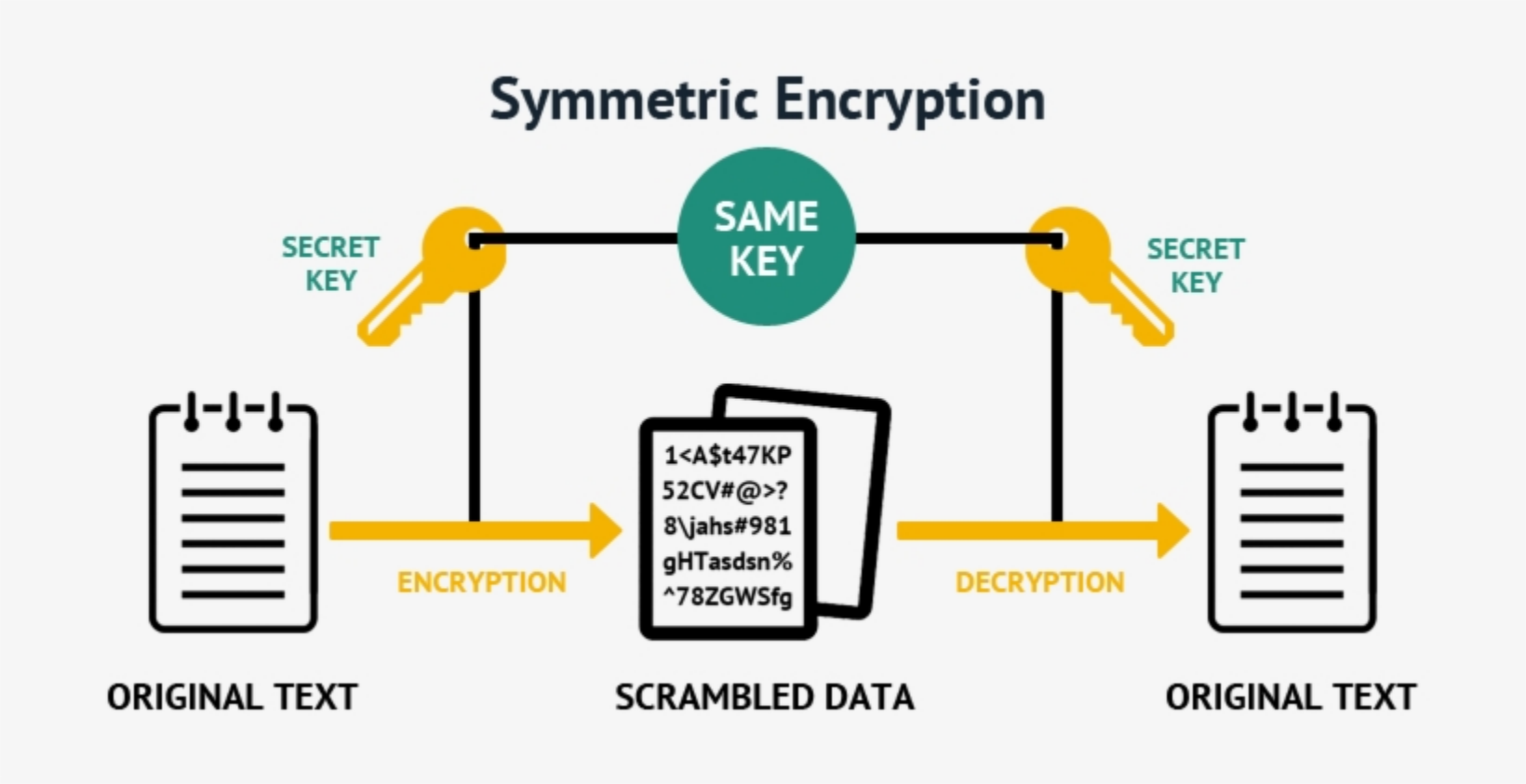
Encryption

- **Two types of encryption:**
  1. **Symmetric Key Encryption**
     - Sender and receiver use same digital key to encrypt and decrypt message
  2. **Asymmetric key encryption / Public Key Encryption**
     - Uses two mathematically related digital keys
       - Public key (widely disseminated)
       - Private key (kept secret by owner)

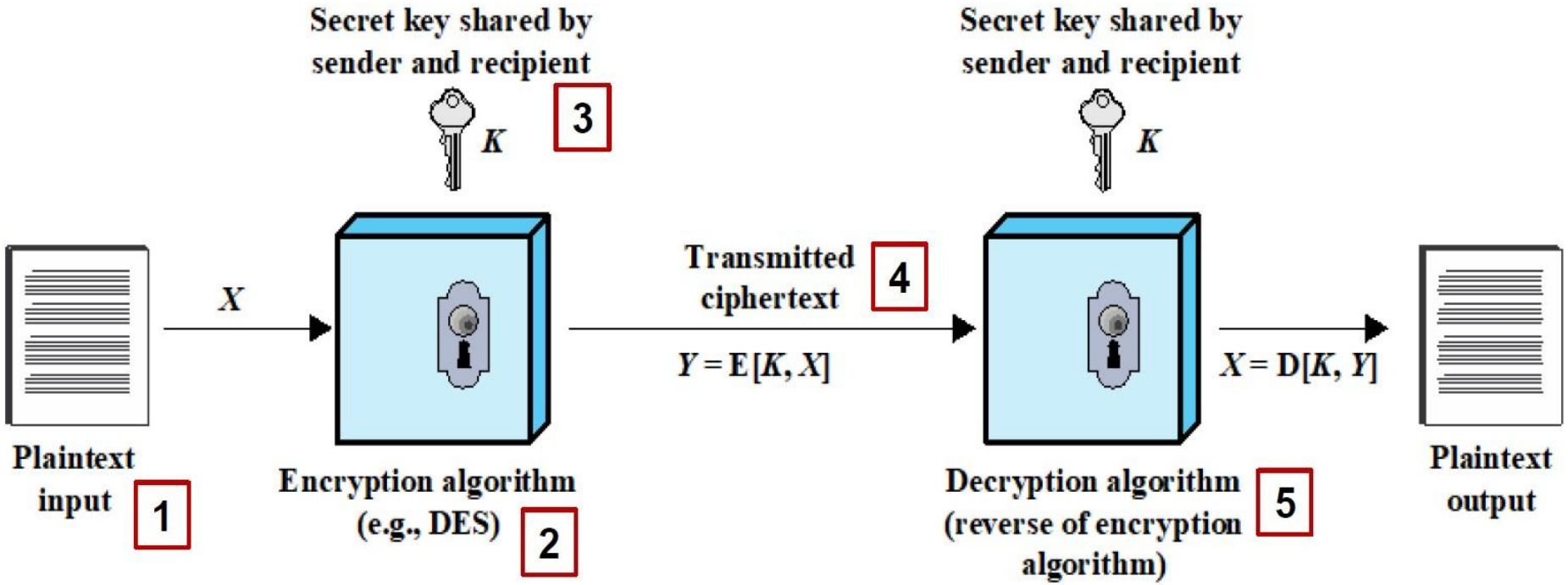
Symmetric Key Encryption

- **Sender and receiver use same digital key to encrypt and decrypt message**
- **Requires different set of keys for each transaction**
- **Strength of encryption**
  - Length of binary key used to encrypt data
- **Data Encryption Standard (DES)**
- **Advanced Encryption Standard (AES)**
  - Most widely used symmetric key encryption
  - Uses 128-, 192-, and 256-bit encryption keys
- **Other standards use keys with up to 2,048 bits**

Symmetric Key Encryption



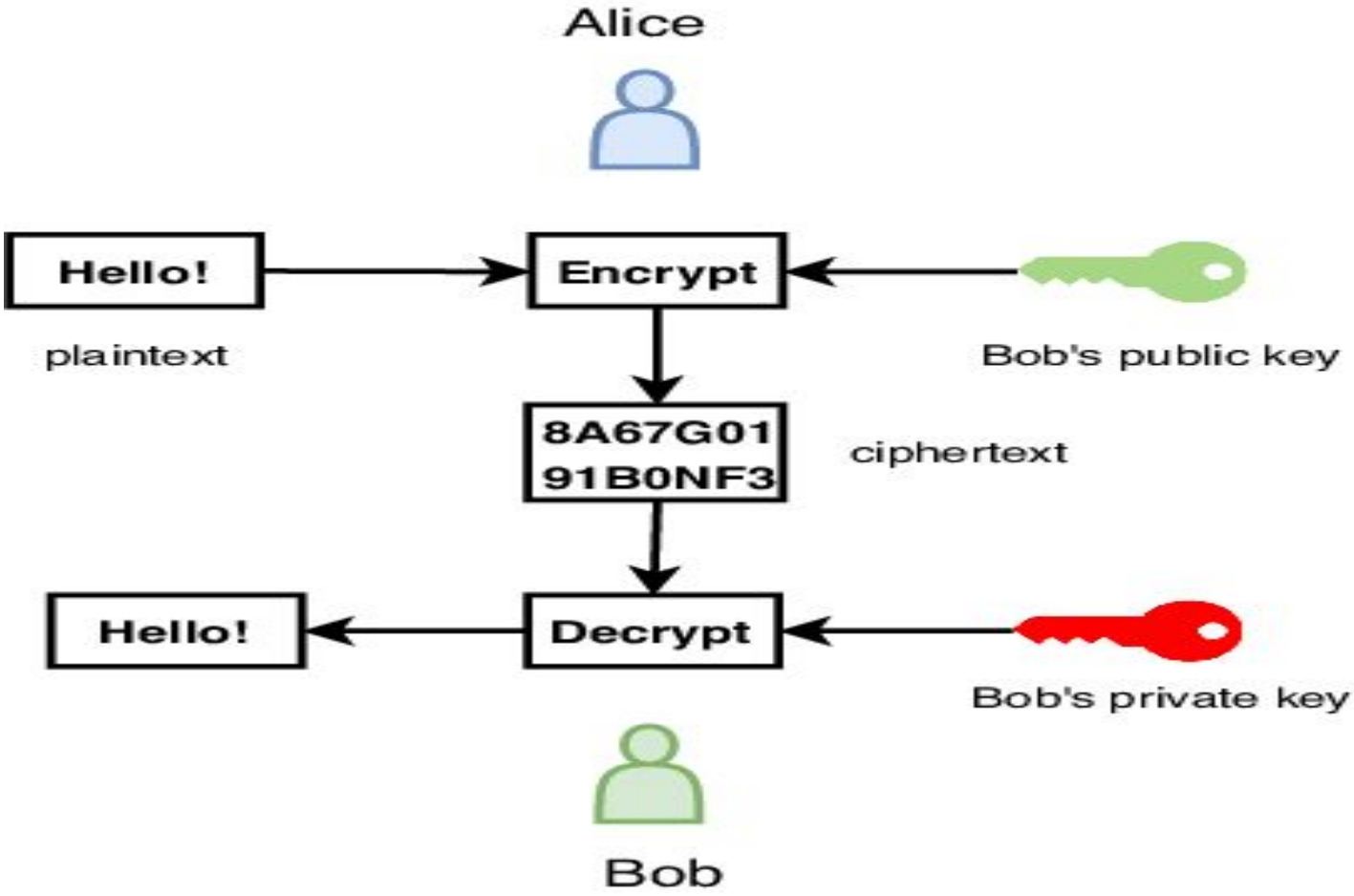
Symmetric Key Encryption



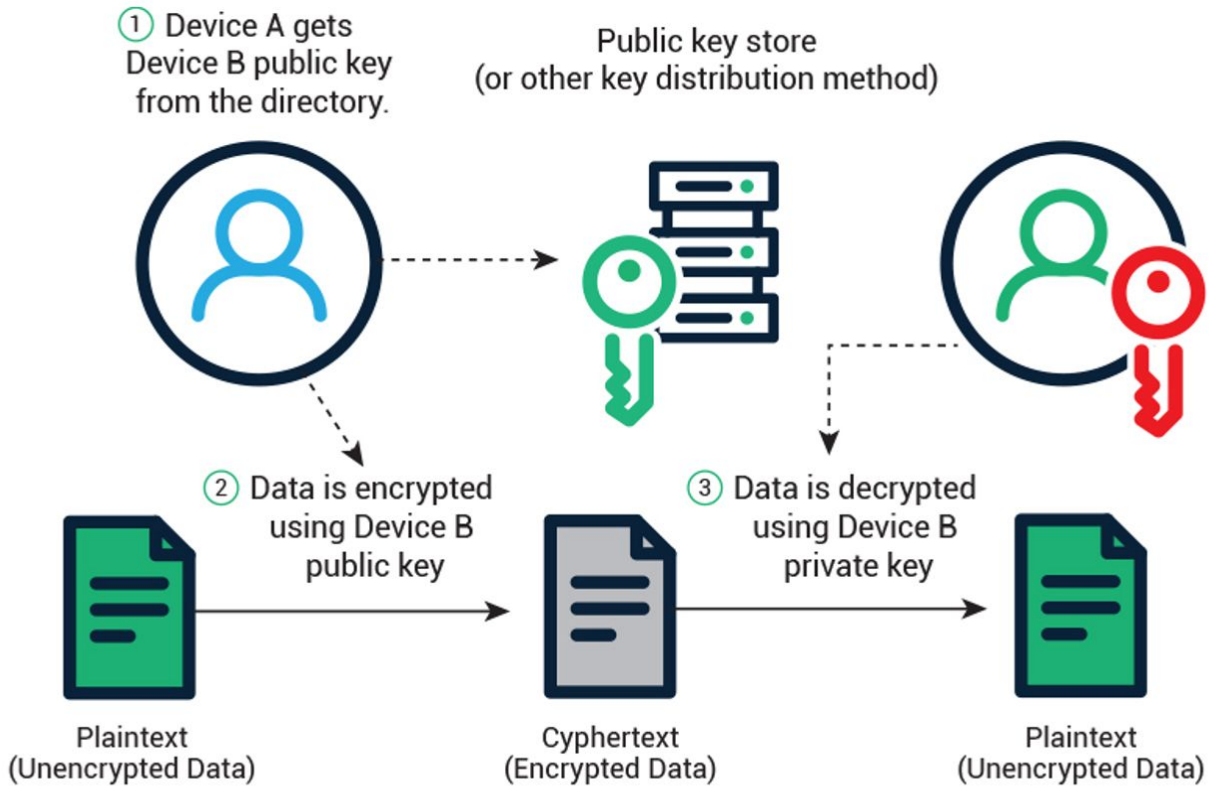
Public Key Encryption

- **Uses two mathematically related digital keys**
  - Public key (widely disseminated)
  - Private key (kept secret by owner)
- **Both keys used to encrypt and decrypt message**
- **Once key used to encrypt message, same key cannot be used to decrypt message**
- **Sender uses recipient's public key to encrypt message; recipient uses private key to decrypt it**

Public Key Encryption



Public Key Encryption



Public Key Cryptography: A Simple Case

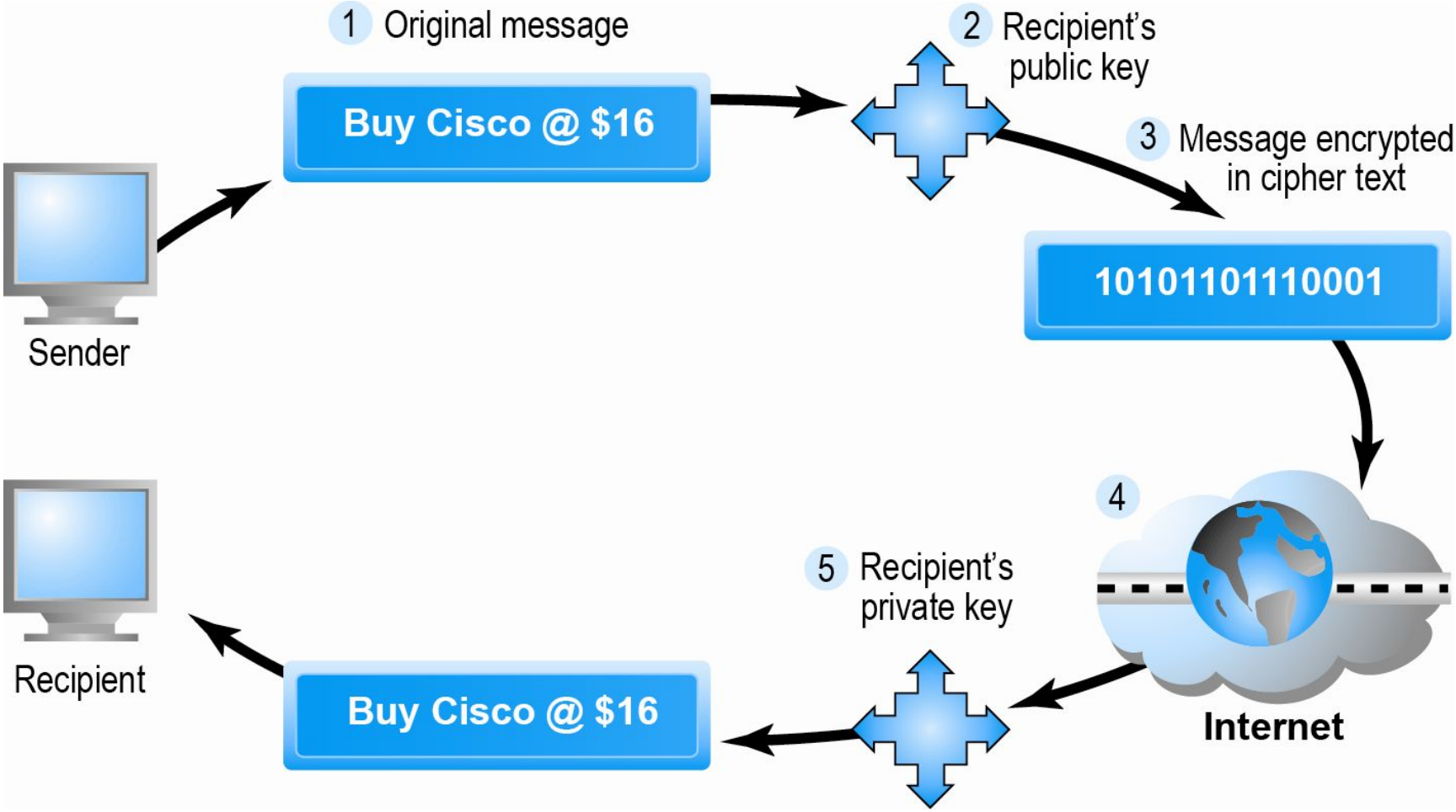


Figure 5.6, Page 279

Hashing

What is Hashing ?

- a mathematical algorithm that converts plaintext to a unique fixed-length unreadable text or a Hash Digest

The purpose of Hashing:

- To verify data integrity
- Authentication
- To store sensitive data

- Source: https://www.section.io/engineering-education/understand-hashing-in-cryptography/#what-is-hashing

Hashing

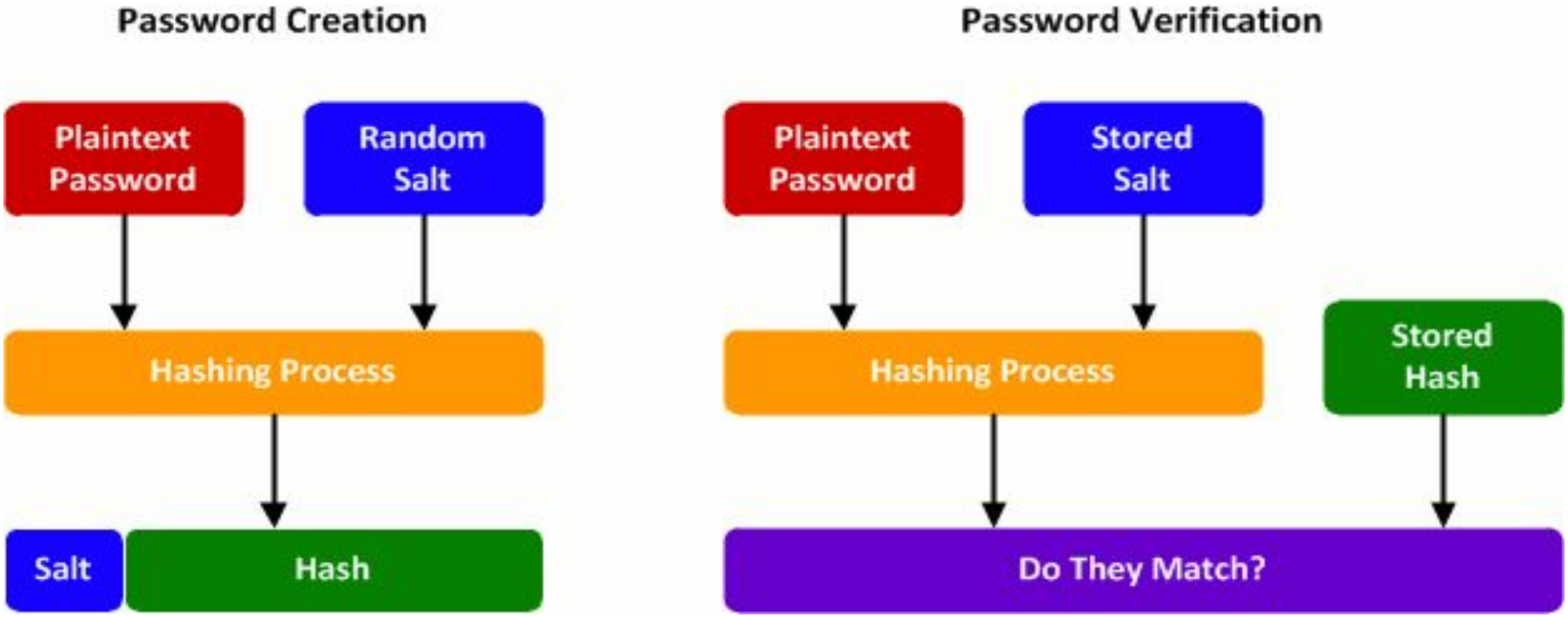
Properties of a hash function :

- Deterministic - The output will be the same for a given outcome.
- Not reversible – We can't reverse a hash function back to the original password.
- Collision resistant – Two inputs do not result in the same output.
- Non-predictable – A hash function randomly generates a unique hash value that is not predictable.
- Compression – The hash function's output is much smaller than the input size.

Hashing

Applications of hashing

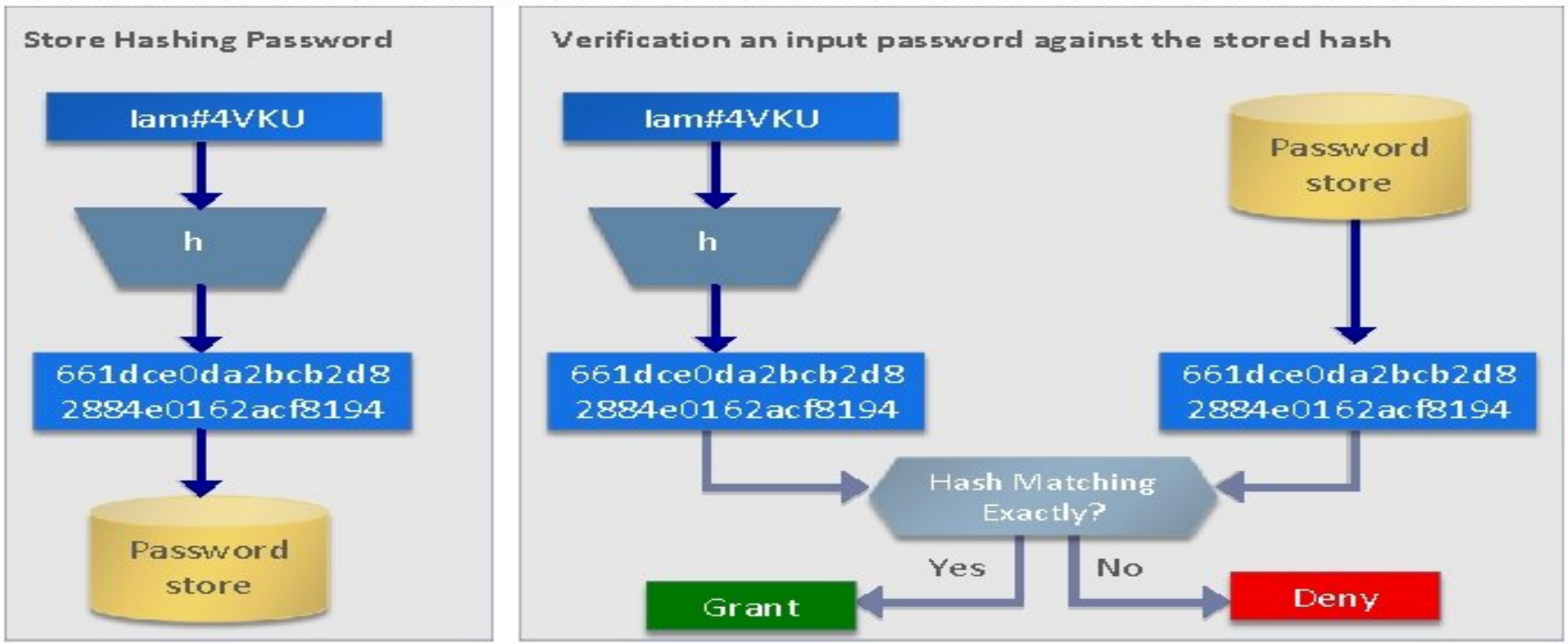
- Password storage and verification



Hashing

Applications of hashing

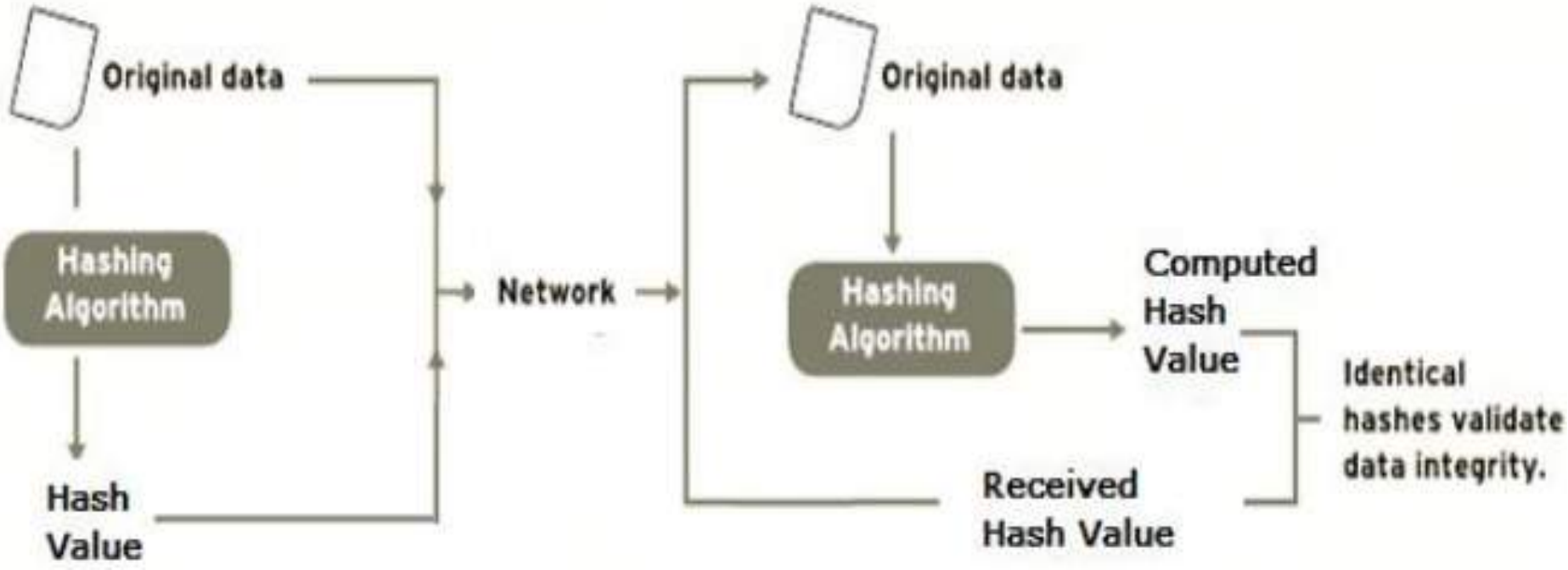
- Password storage and verification



Hashing

Applications of hashing

- Password storage and verification
- Checking of data integrity



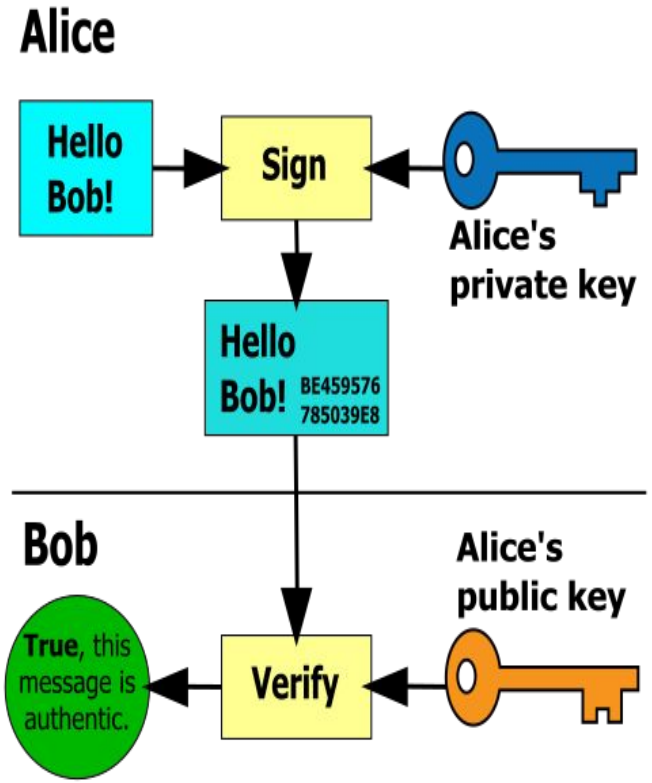
Hashing

Characteristics of a hash function:

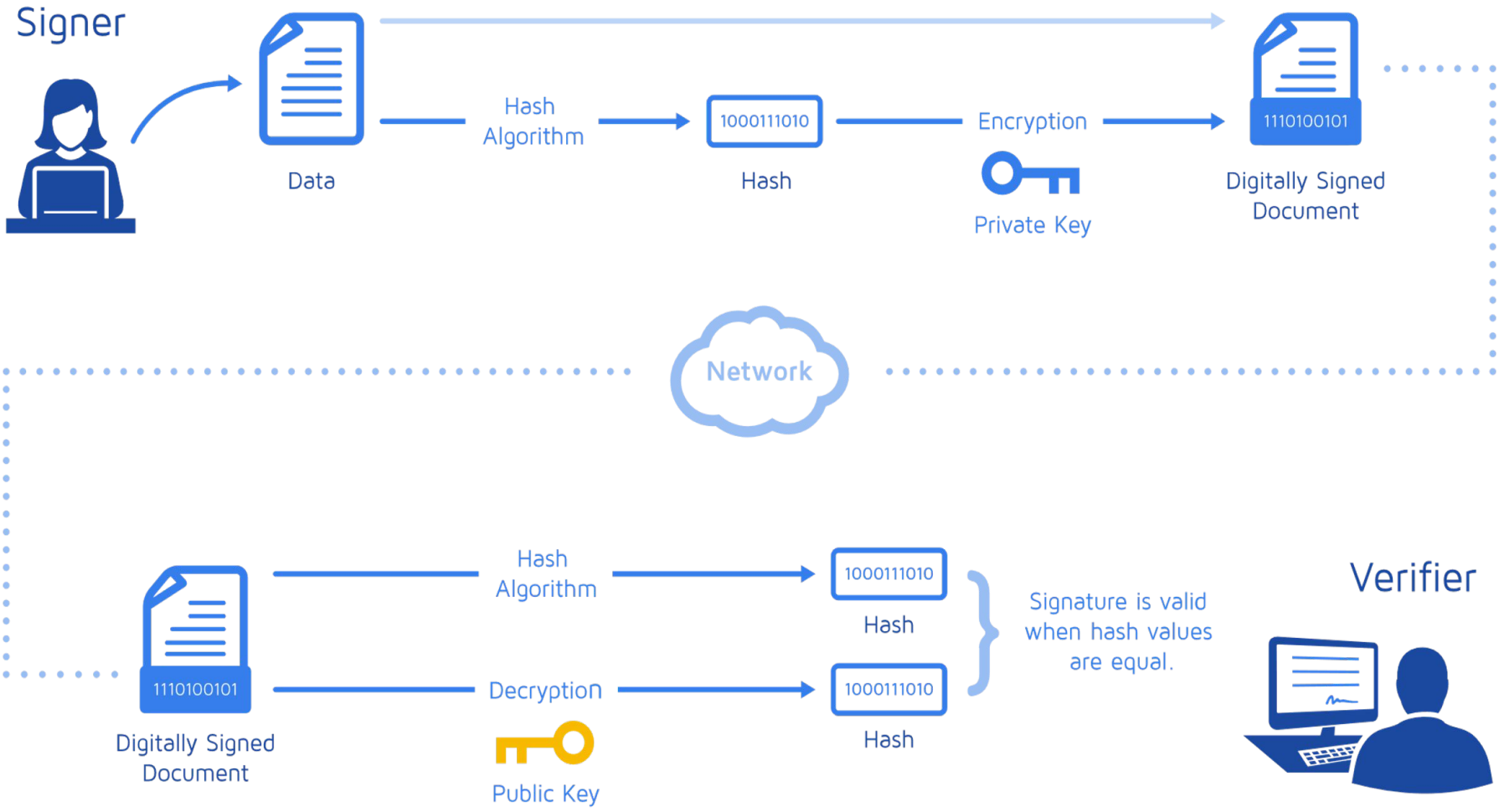
- Secure – A hash function is irreversible. It is a one-way function.
- Unique – Two different datasets cannot produce the same digest.
- Fixed-size – The hash function gives a fixed size digest.

Digital Signature

A **mathematical algorithm used to validate the authenticity and integrity of a message** (e.g., an email, a credit card transaction, or a digital document



Digital Signature



Public Key Encryption using Digital Signatures and Hash Digests

- Hash digest of message sent to recipient along with message to verify integrity
- Hash digest and message encrypted with recipient's public key
- Entire cipher text then encrypted with recipient's private key—creating digital signature—for authenticity, nonrepudiation

Public Key Cryptography with Digital Signatures

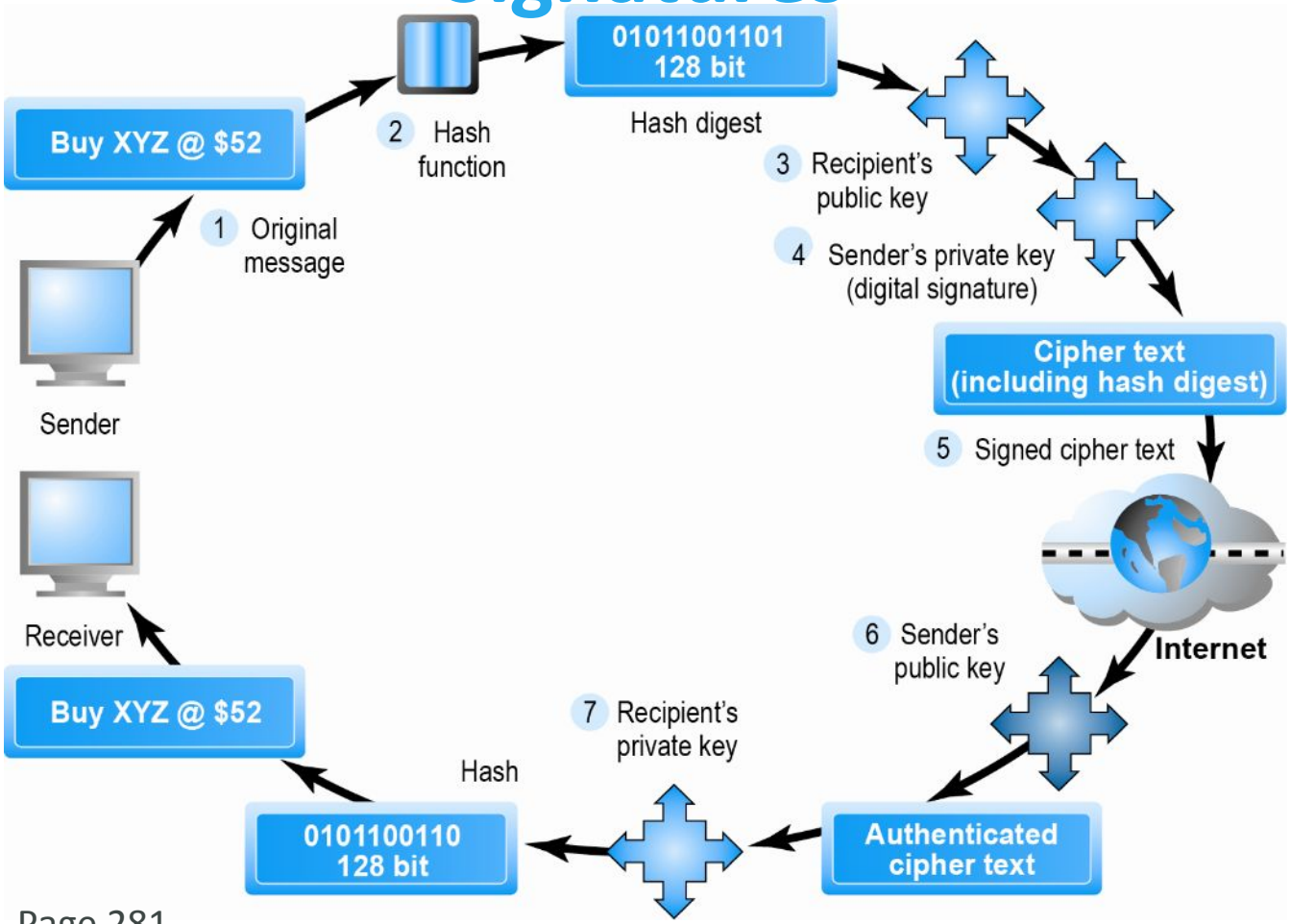
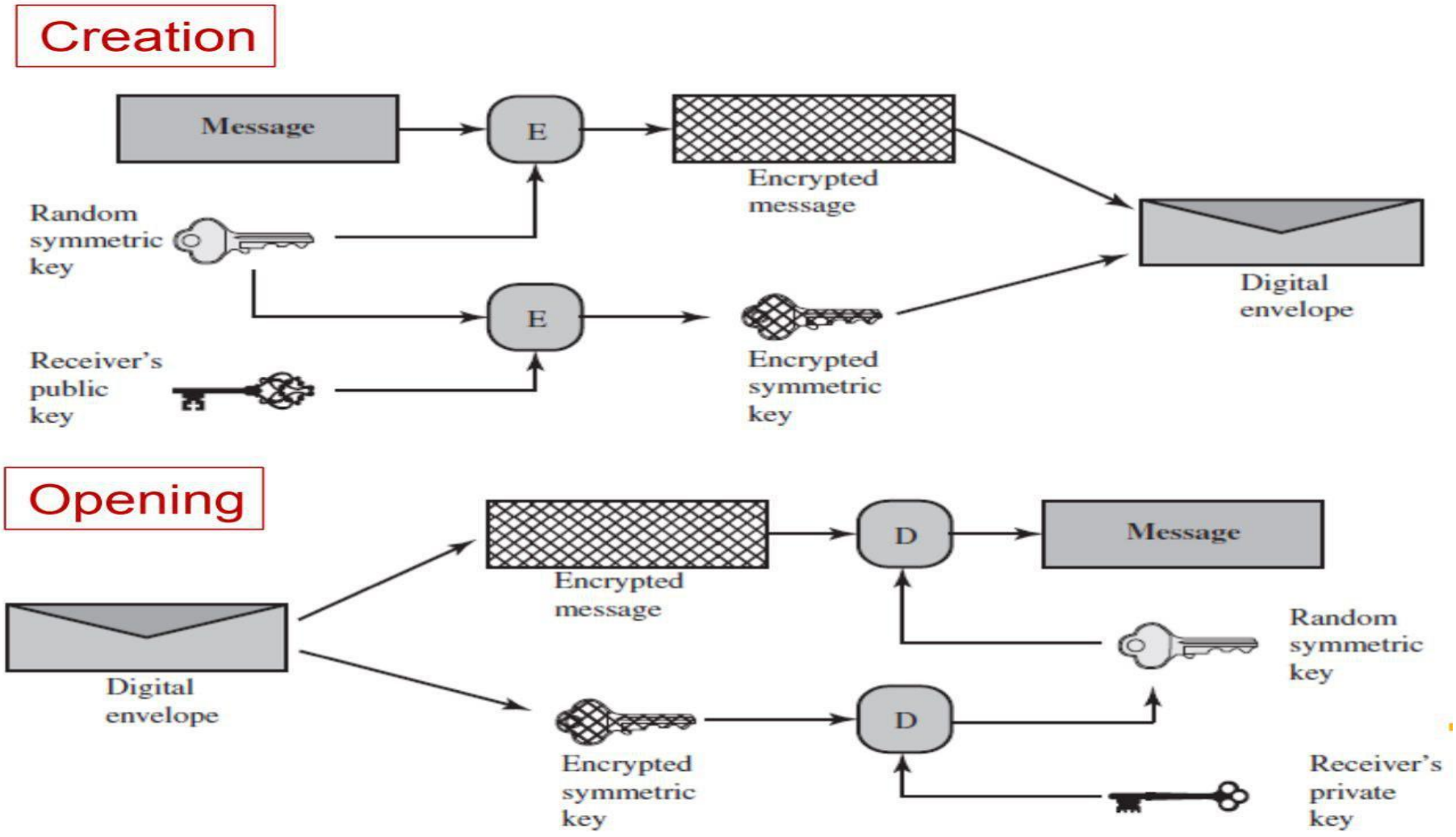


Figure 5.7, Page 281

Digital Envelopes

- **Address weaknesses of:**
  - Public key encryption
    - Computationally slow, decreased transmission speed, increased processing time
  - Symmetric key encryption
    - Insecure transmission lines
- **Uses symmetric key encryption to encrypt document**
- **Uses public key encryption to encrypt and send symmetric key**

Digital Envelope: Creation and Opening



Digital Certificates

- A credentials that facilitate the verification of identities between users in a transaction.
- Much as a passport certifies one's identity as a citizen of a country
- The purpose of a digital certificate is to establish the identity of users within the ecosystem.

- Source: https://cpl.thalesgroup.com/faq/signing-certificates-and-stamping/what-digital-certificate

Digital Certificates

- **Digital certificates are used**
  - to identify the users to whom encrypted data is sent,
  - or to verify the identity of the signer of information
  - protecting the authenticity and integrity of the certificate is imperative in order to maintain the trustworthiness of the system.
- **In order to bind public keys with their associated user (owner of the private key), public key infrastructures (PKIs) use digital certificates.**

Why Digital Certificates

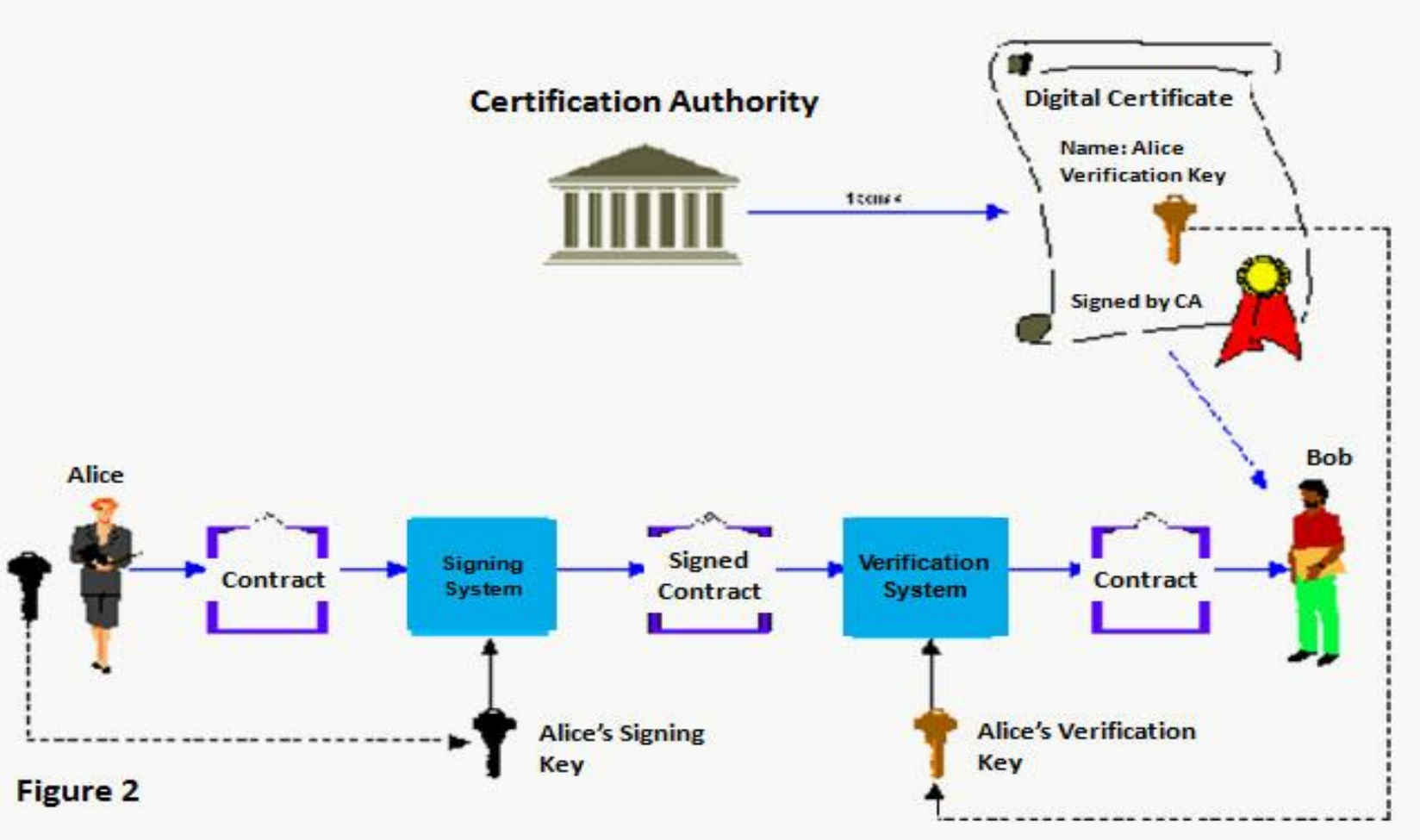


Figure 2

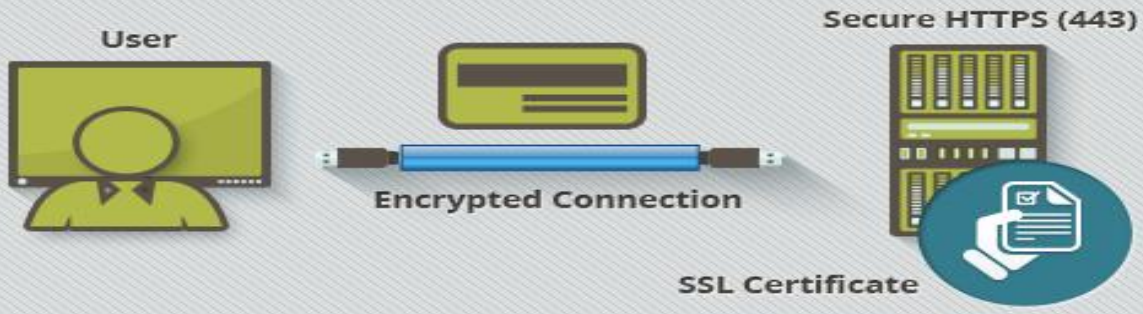
Digital Certificates

- A digital certificate, also known as a *public key certificate*, is used to cryptographically link ownership of a public key with the entity that owns it.
- Digital certificates are for sharing public keys to be used for encryption and authentication.
- Digital certificate consists:
  - public key owner
  - owner name
  - expired public key dates
  - Name of the issuer (the CA that issued the Digital Certificate)
  - Serial number Digital Certificates
  - Publisher logo

Digital Certificates

Digital certificates are used to encrypt online communications between an end-user's browser and a website.

After verifying that a company owns a website, a certificate authority will sign their certificate so it is trusted by internet browsers.



Public Key Infrastructure (PKI)

- **Public Key Infrastructure (PKI):**
- The distribution, authentication and revocation of digital certificates are the primary functions of the public key infrastructure (PKI), the system that distributes and authenticates public keys.

- Source: https://resources.infosecinstitute.com/topic/public-key-infrastructure-pki-3/

Digital Certificates and Certification Authorities

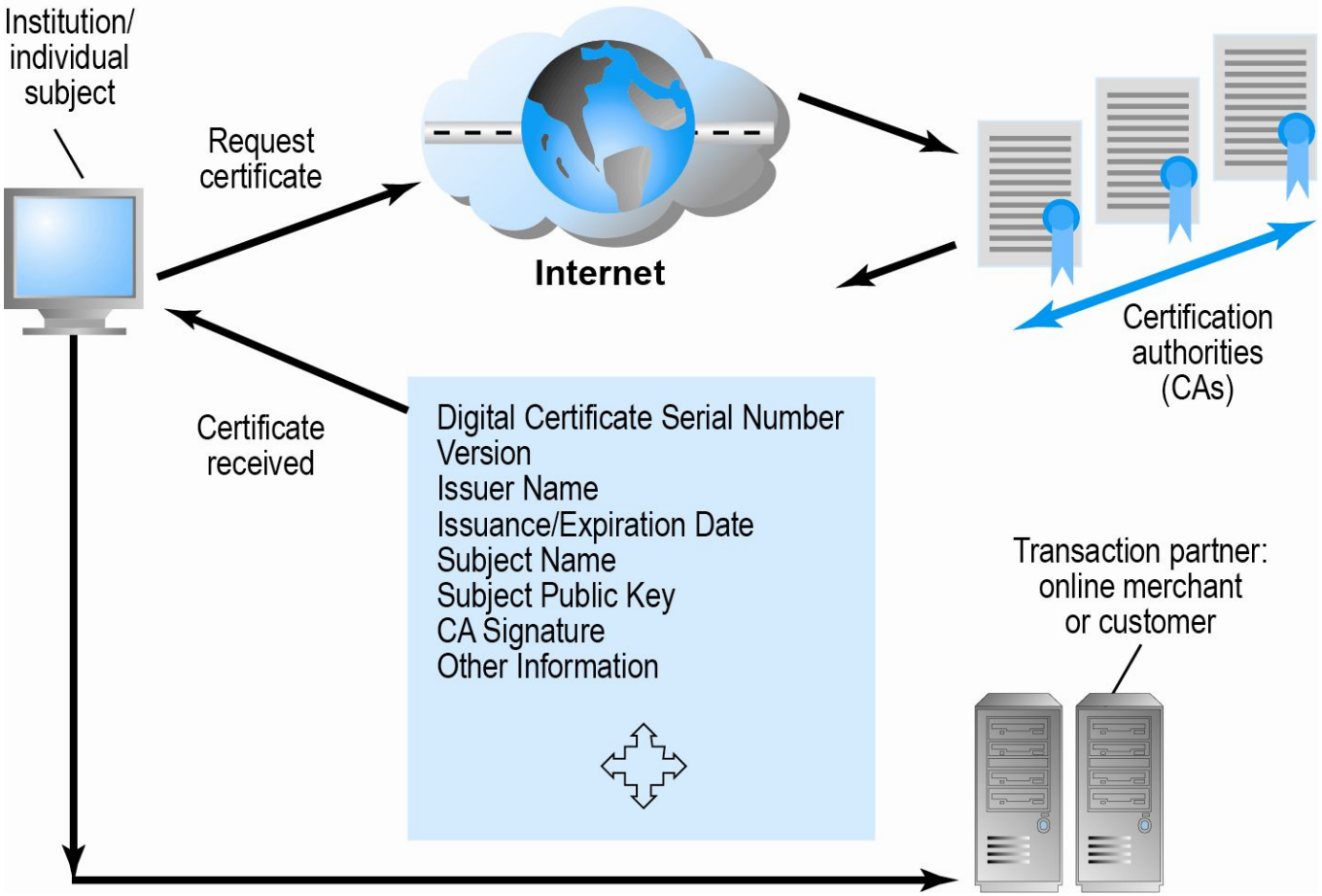
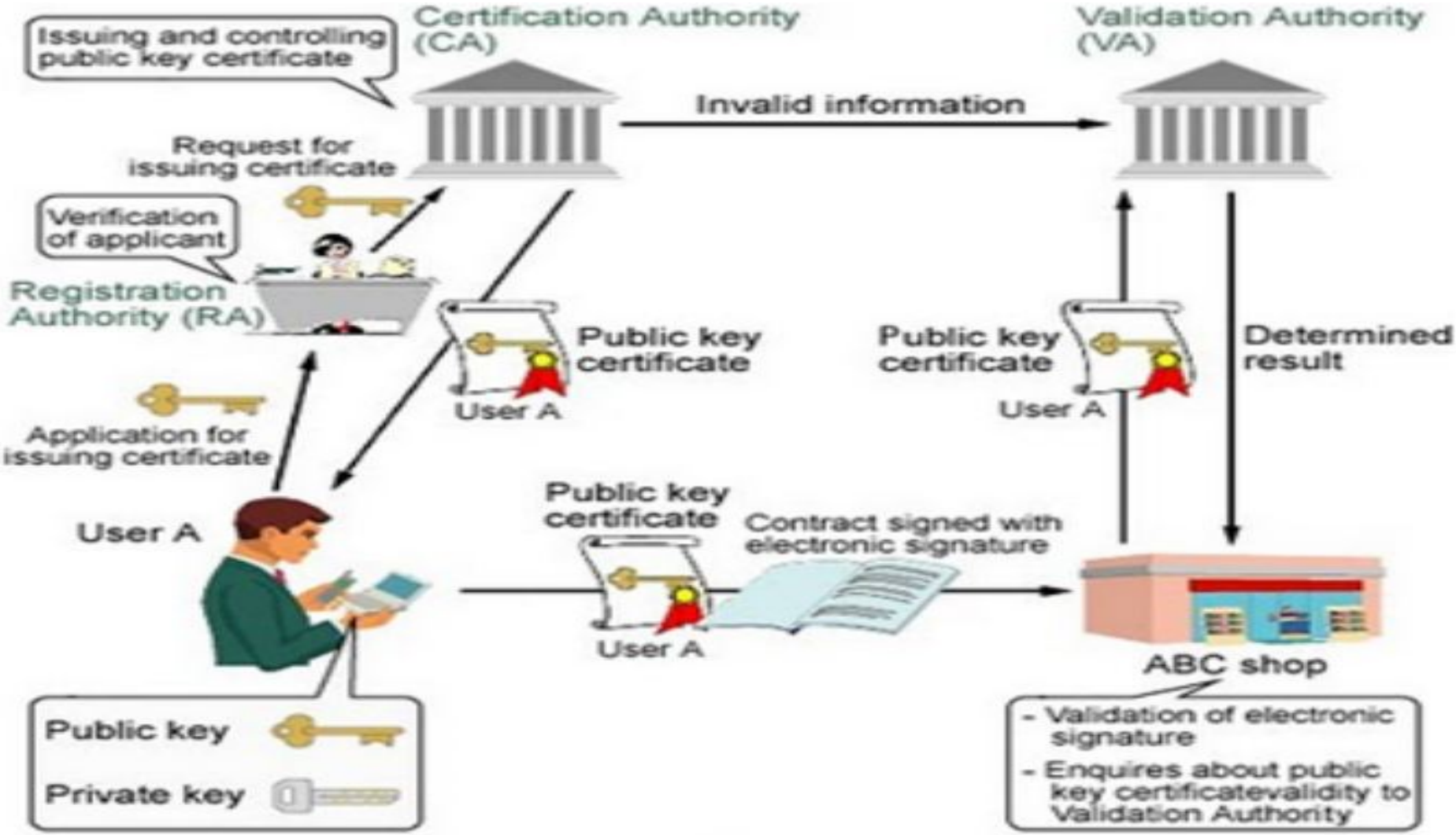


Figure 5.9, Page 283

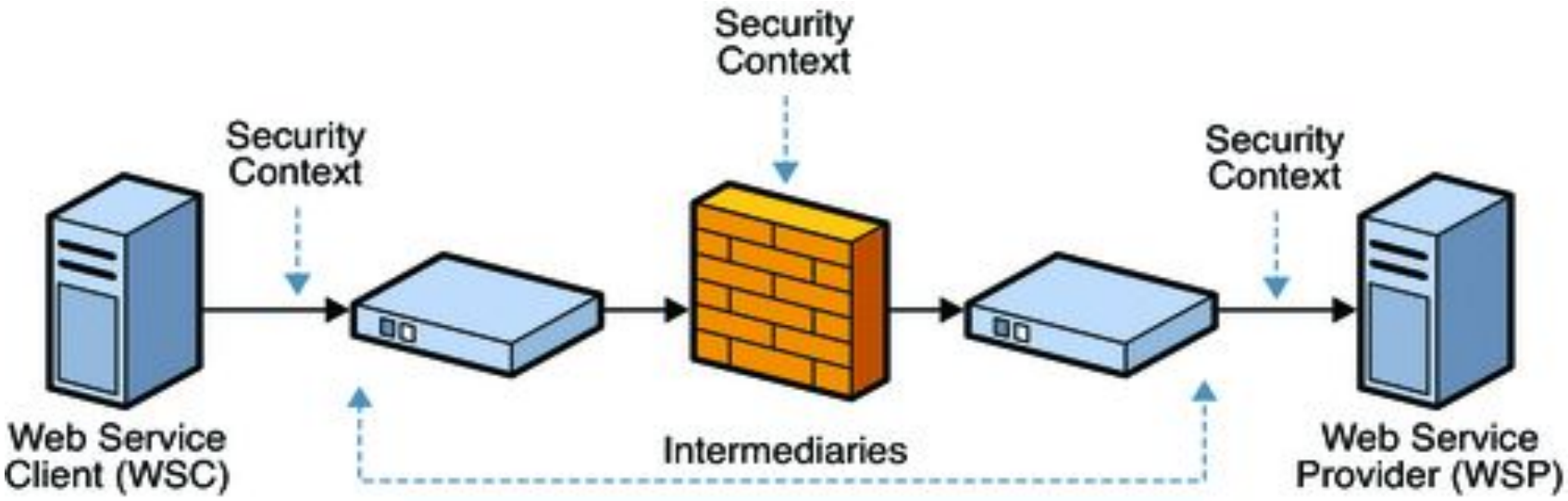
Digital Certificates and Certification Authorities



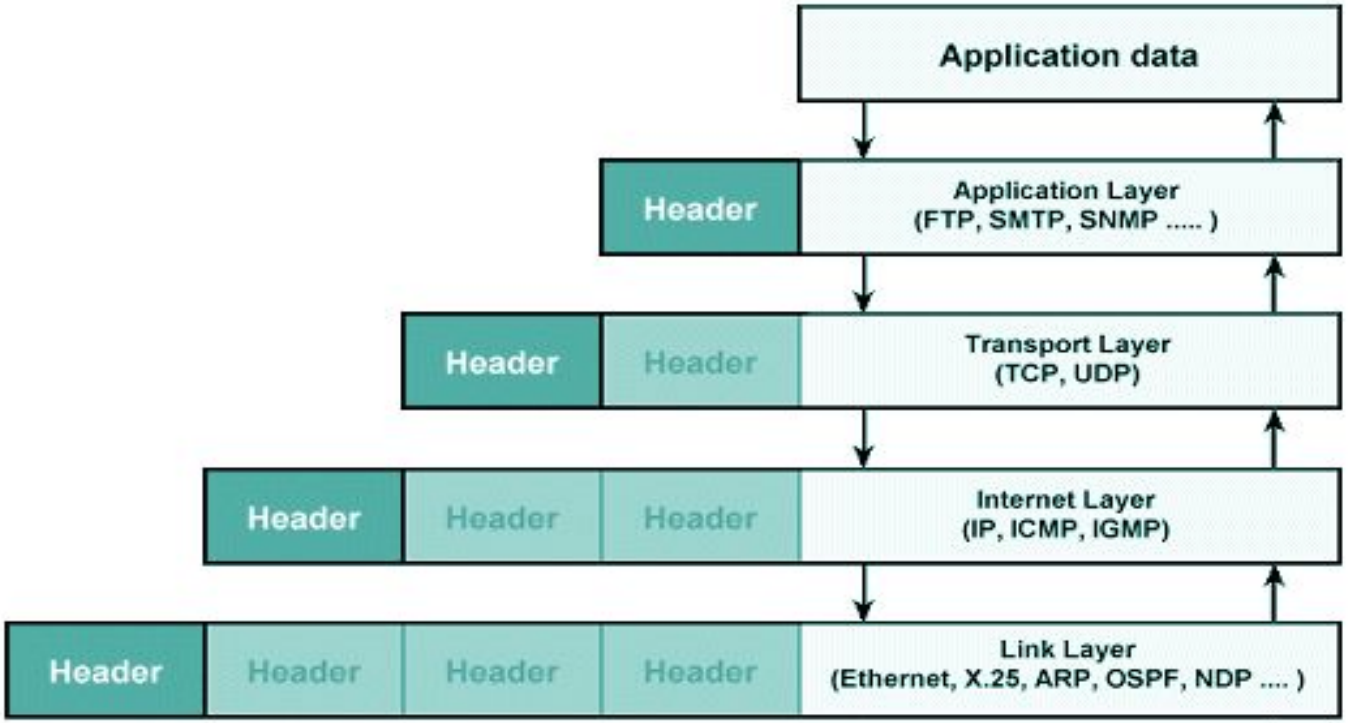
Limits to Encryption Solutions

- **Doesn‘t protect storage of private key**
  - PKI not effective against insiders, employees
  - Protection of private keys by individuals may be haphazard
- **No guarantee that verifying computer of merchant is secure**
- **CAs are unregulated, self-selecting organizations**

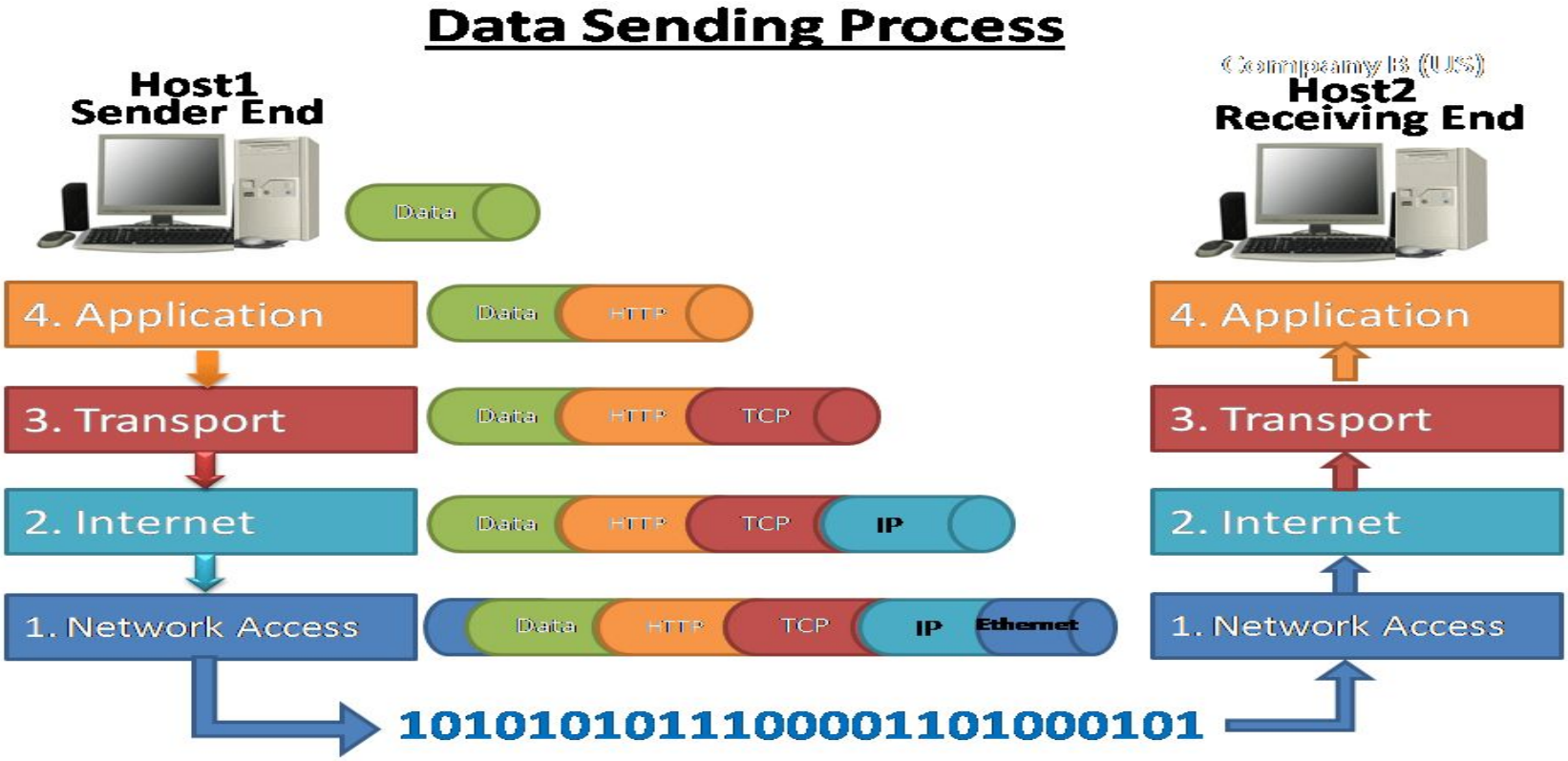
Securing
Communication Protocol &
Communication Channel



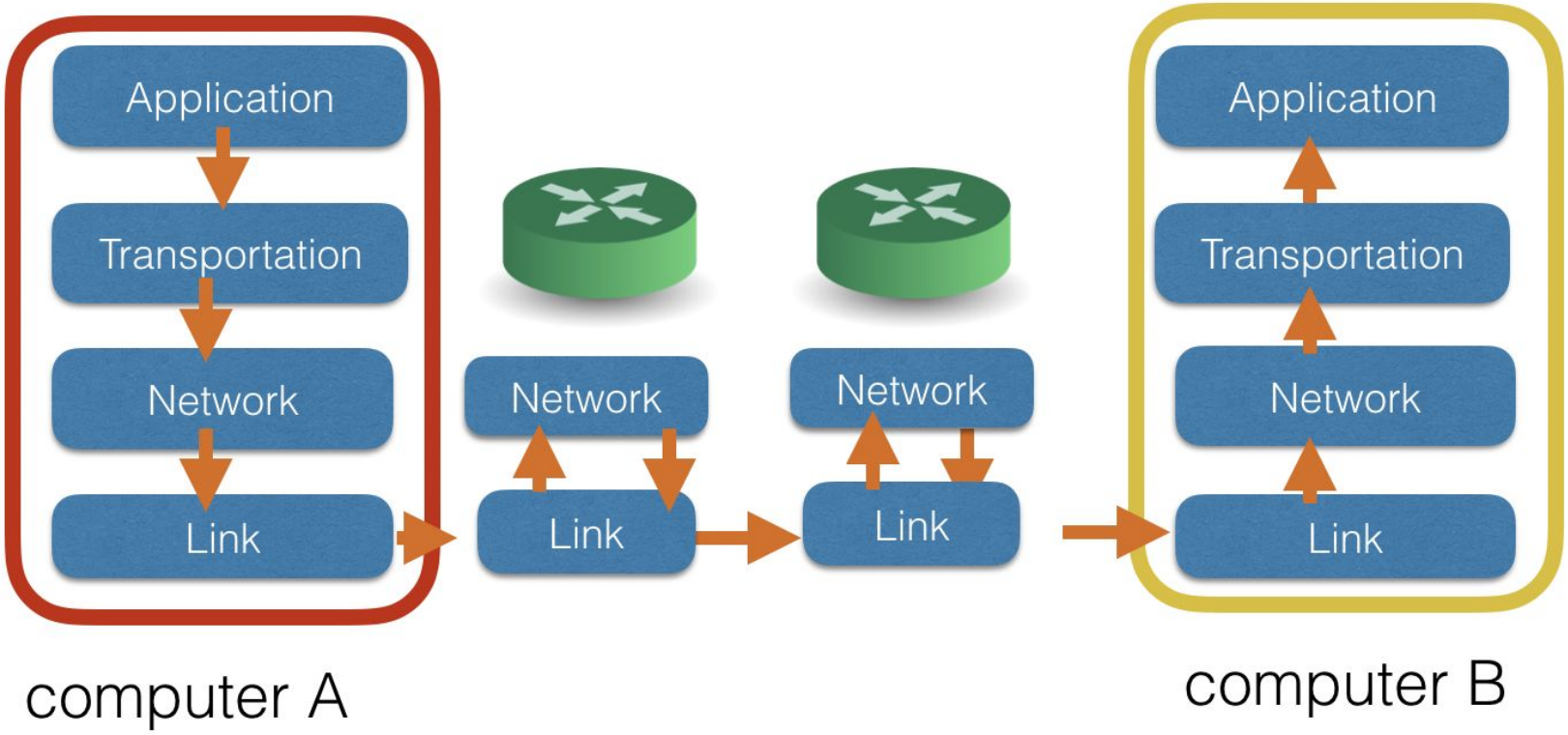
Understanding Communication Protocols



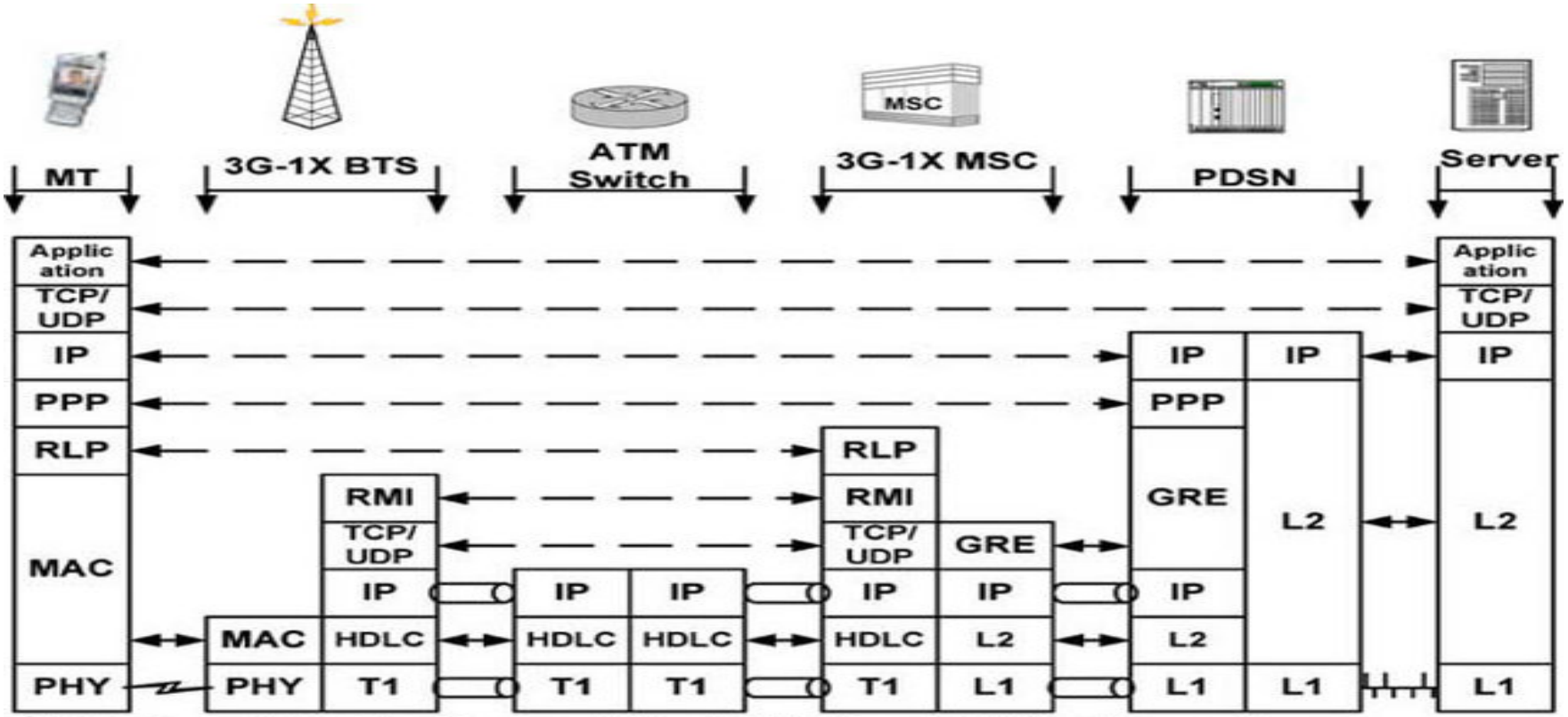
Understanding Communication Protocols



Understanding Communication Protocols



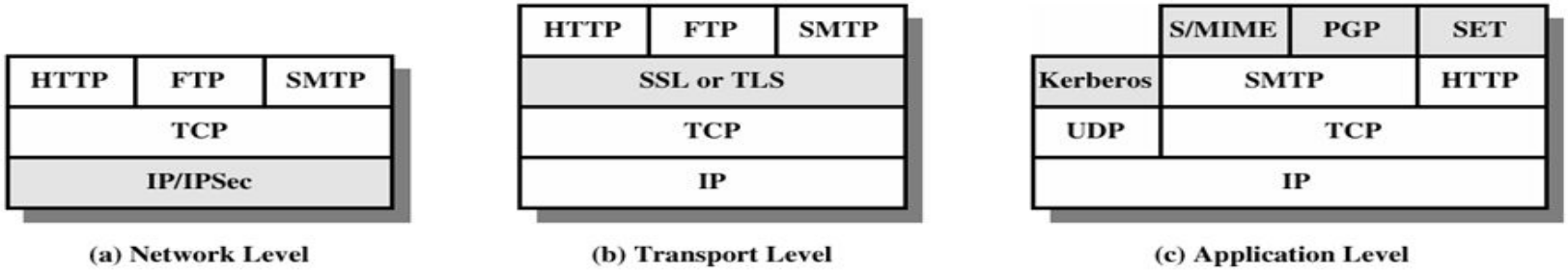
Understanding Communication



GRE - Generic Routing Encapsulation RMI - Remote Method Invocation
HDLC - High Level Data Link Control

Securing Communication Protocols

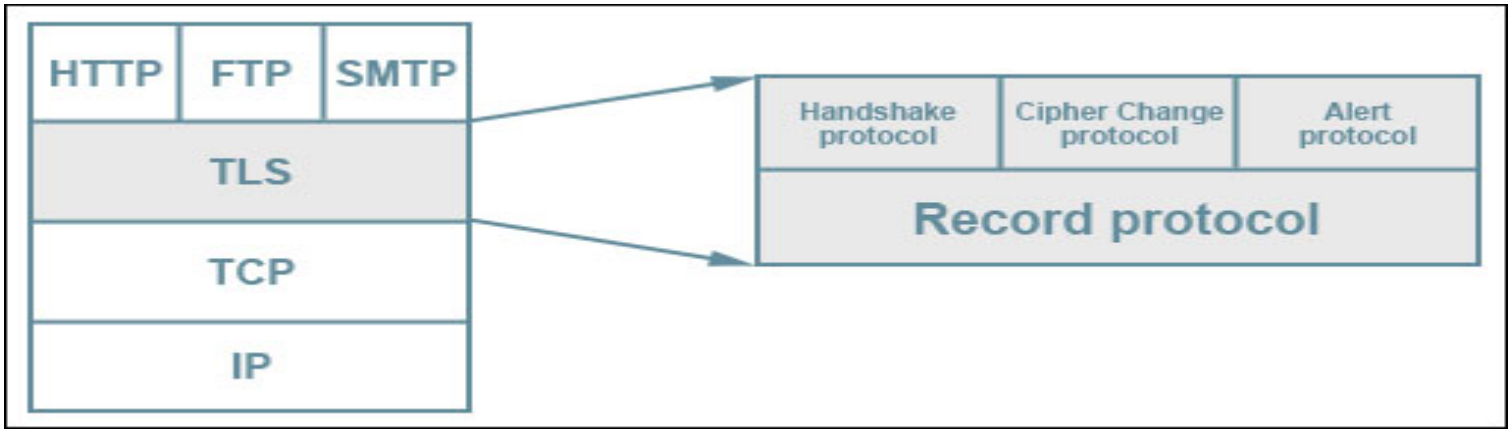
Security facilities in the TCP/IP protocol stack



Securing Communication Protocols

- **Transport Layer Security (TLS)**
  - Establishes secure, negotiated client–server session
  - **Transport Layer Security (TLS),** the **successor of the now-deprecated Secure Sockets Layer (SSL)**
  - **What does TLS do?**
    - **Encryption:** hides the data being transferred from third parties.
    - **Authentication:** ensures that the parties exchanging information are who they claim to be.
    - **Integrity:** verifies that the data has not been forged or tampered with.

Transport Layer Security (TLS) /SSL



Secure Negotiated Sessions Using SSL/TLS

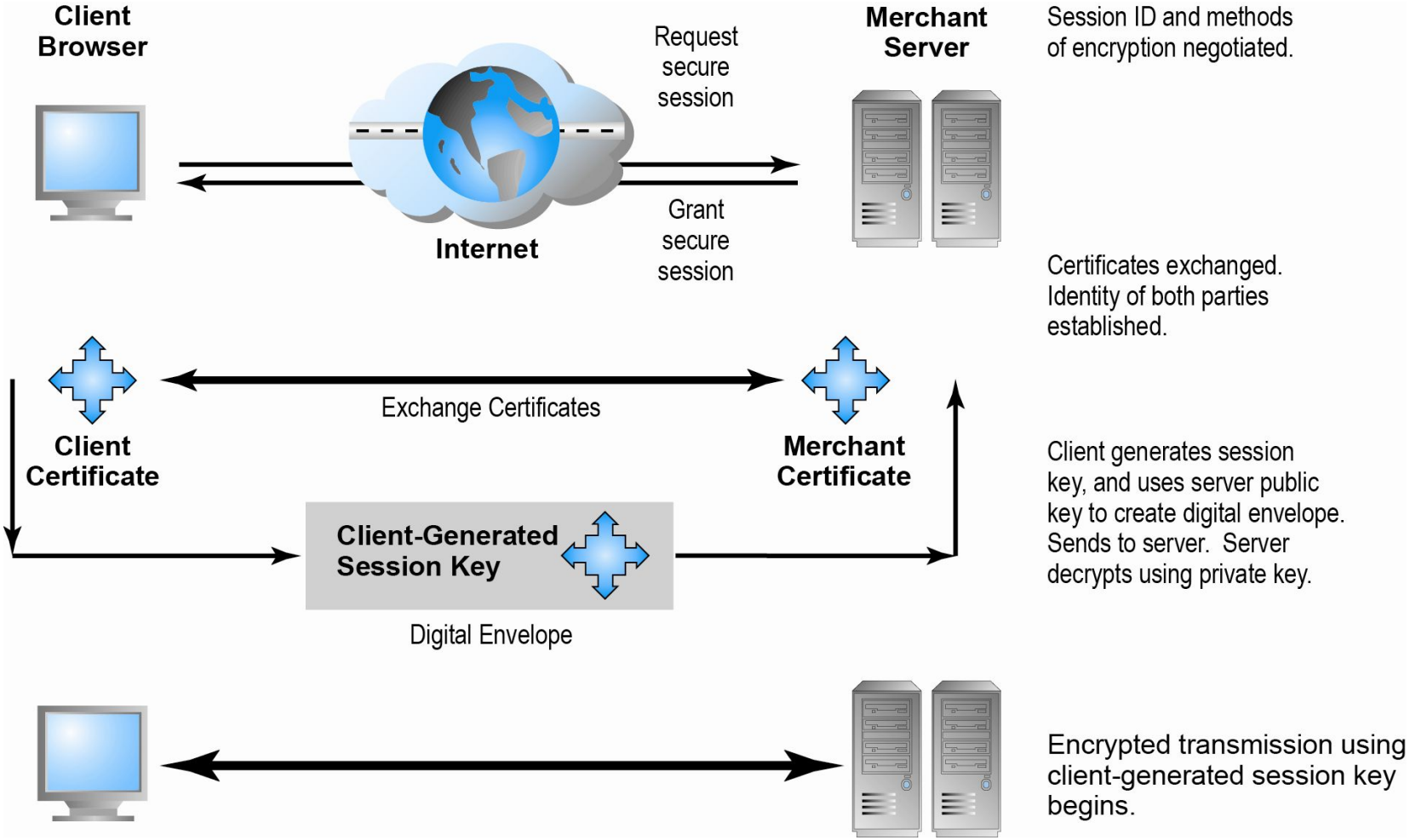
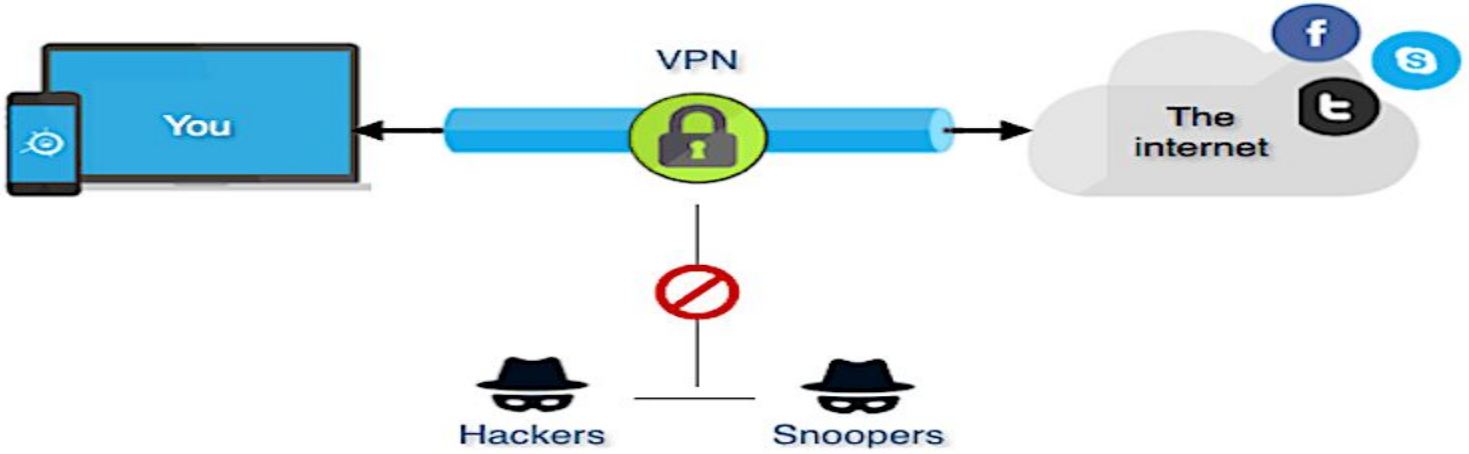


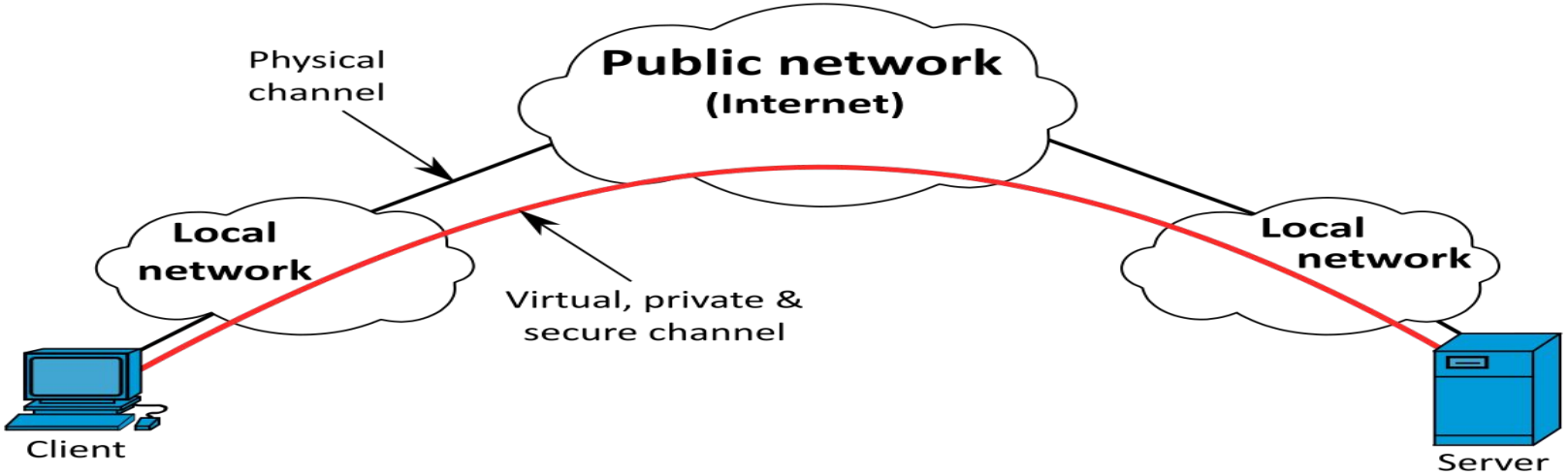
Figure 5.10, Page 286

Securing Channels of Communication

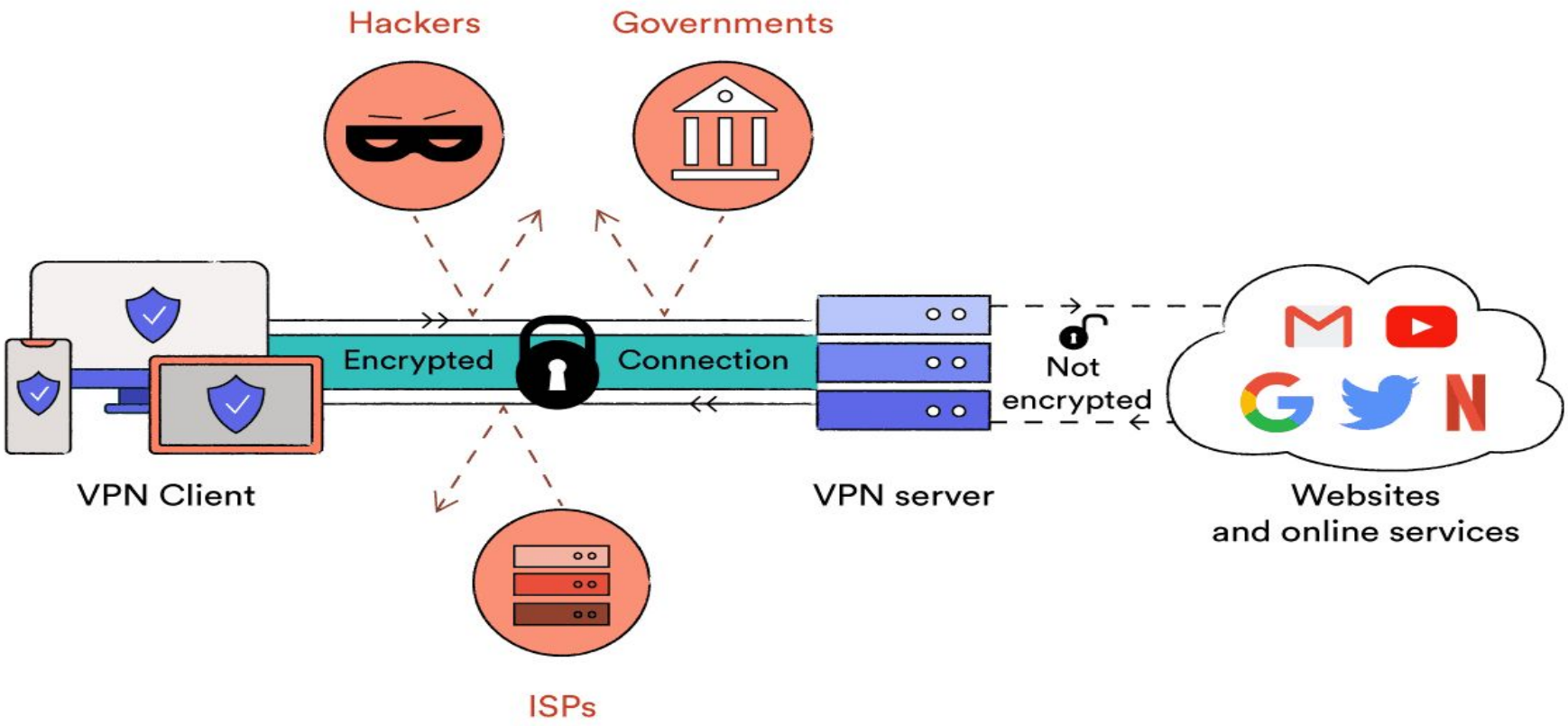
- **Virtual Private Network (VPN)**
  - Allows remote users to securely access internal network via the Internet
  - establish a protected network connection when using public networks.
  - encrypt internet traffic and disguise your online identity.
  - makes it more difficult for third parties to track your activities online and steal data.

Virtual Private Network (VPN)





Virtual Private Network (VPN)



Protecting Networks

- **Firewall**
  - Hardware or software
  - Uses security policy to filter packets
  - Two main methods:
    - Packet filters
    - Application gateways
- **Proxy servers (proxies)**
  - Software servers that handle all communications from or sent to the Internet
- **Intrusion detection systems**
- **Intrusion prevention systems**

Firewalls and Proxy Servers

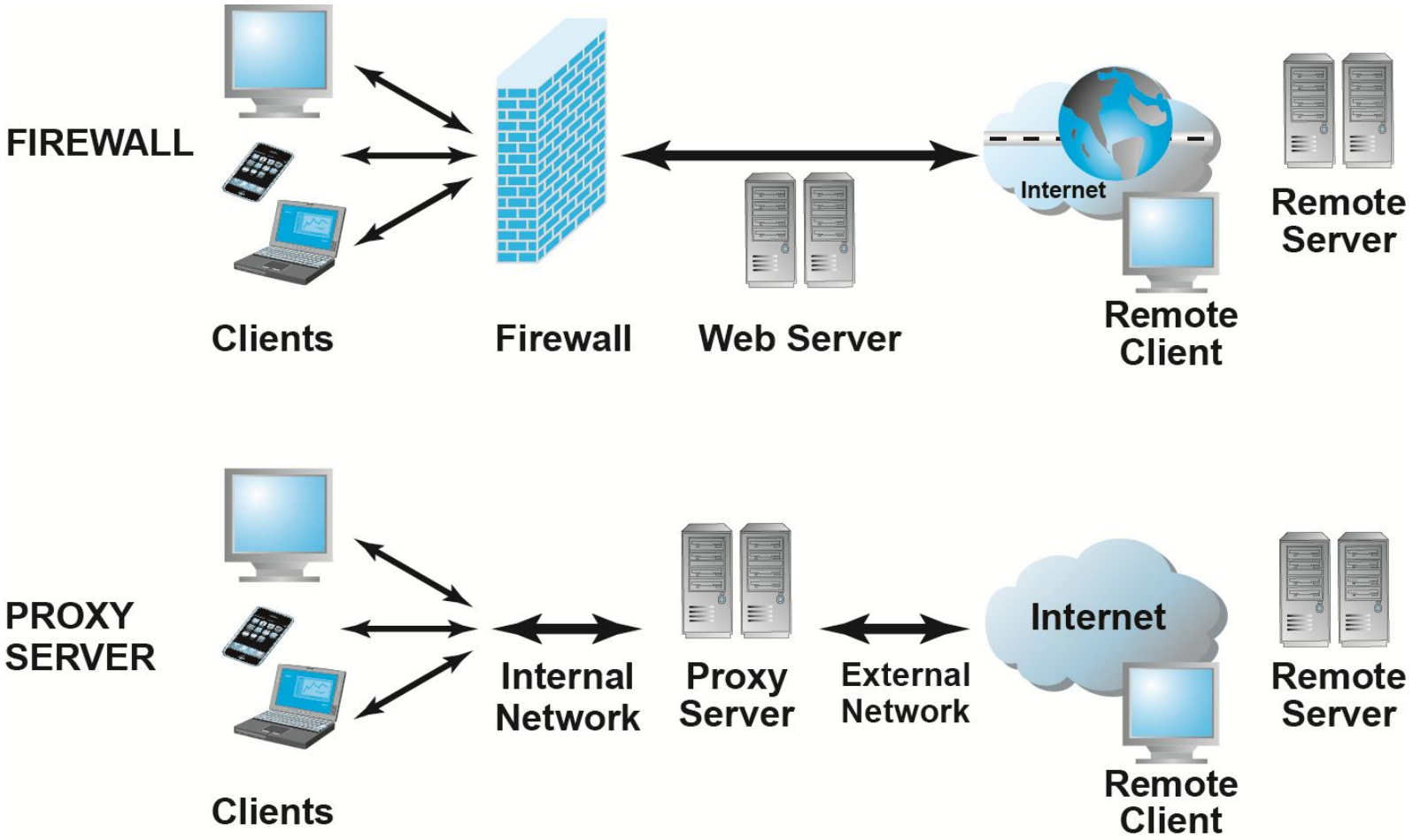
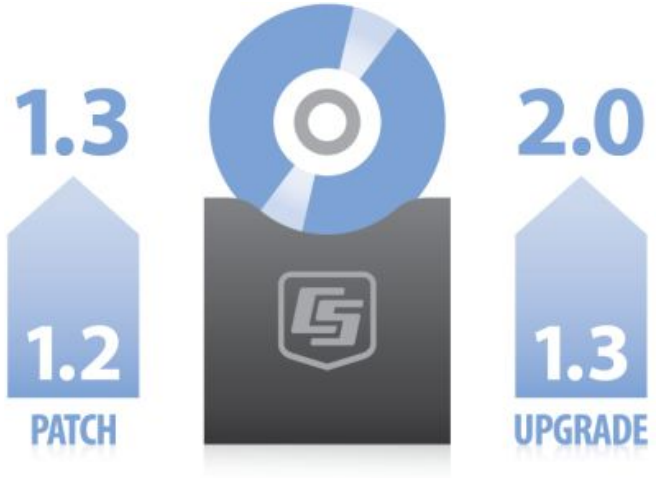


Figure 5.11, Page 289

Protecting Servers and Clients

- **Operating system security enhancements**
  - Upgrades, patches



- **Anti-virus software**
  - Easiest and least expensive way to prevent threats to system integrity
  - Requires daily updates

Management Policies, Business Procedures, and Public Laws

- Worldwide, companies spend more than $65 billion on security hardware, software, services
- Managing risk includes:
  1. Technological Aspect (in Making secure software)
  2. Setting Effective management policies
  3. Public laws and active enforcement

Making secure software

- **Flawed approach**: Design and build software, and ***ignore security at first***
  - Add security once the functional requirements are satisfied

Making secure software

- **Flawed approach**: Design and build software, and ***ignore security at first***
  - Add security once the functional requirements are satisfied

- **Better approach**: ***Build security in*** from the start
  - Incorporate security-minded thinking into all phases of the development process

Development process

Many development processes; **four common phases**:

- **Requirements**
- **Design**
- **Implementation**
- **Testing/assurance**

Where does **security engineering** fit in?

All phases!

Security engineering

Phases

- **Requirements**
- **Design**
- **Implementation**
- **Testing/assurance**

Note that different SD processes have different phases and artifacts, but all involve the basics above. We'll keep it simple and refer to these.

Security engineering

Phases

- **Requirements**
- **Design**
- **Implementation**
- **Testing/assurance**

Note that different SD processes have different phases and artifacts, but all involve the basics above. We'll keep it simple and refer to these.

Activities

Security engineering

Phases

- **Requirements**
- **Design**
- **Implementation**
- **Testing/assurance**

Security Requirements

Note that different SD processes have different phases and artifacts, but all involve the basics above. We'll keep it simple and refer to these.

Activities

Security engineering

Phases

- **Requirements**
- **Design**
- **Implementation**
- **Testing/assurance**

Security Requirements

Abuse Cases

Note that different SD processes have different phases and artifacts, but all involve the basics above. We'll keep it simple and refer to these.

Activities

Security engineering

Phases

- **Requirements**
- **Design**
- **Implementation**
- **Testing/assurance**

Security Requirements

~~***Abuse Cases***~~ ***Architectural Risk Analysis***

Note that different SD processes have different phases and artifacts, but all involve the basics above. We'll keep it simple and refer to these.

Activities

Security engineering

Phases

- **Requirements**
- **Design**
- **Implementation**
- **Testing/assurance**

Security Requirements

Abuse Cases ***Architectural***

Risk Analysis

Security-oriented Design

Note that different SD processes have different phases and artifacts, but all involve the basics above. We'll keep it simple and refer to these.

Activities

Security engineering

Phases

- **Requirements**
- **Design**
- **Implementation**
- **Testing/assurance**

Activities

Security Requirements

~~Abuse Cases~~ Architectural

Risk Analysis

Security-oriented Design

Code Review (with tools)

Note that different SD processes have different phases and artifacts, but all involve the basics above. We'll keep it simple and refer to these.

Security engineering

Phases

- **Requirements**
- **Design**
- **Implementation**
- **Testing/assurance**

Security Requirements

Abuse Cases ***Architectural Risk Analysis***

Security-oriented Design

Code Review (with tools)

Risk-based Security Tests

Note that different SD processes have different phases and artifacts, but all involve the basics above. We'll keep it simple and refer to these.

Activities

Security engineering

Phases

- **Requirements**
- **Design**
- **Implementation**
- **Testing/assurance**

Security Requirements

Abuse Cases ***Architectural Risk Analysis***

Security-oriented Design

Code Review (with tools)

Risk-based Security Tests

Penetration Testing

Activities

Note that different SD processes have different phases and artifacts, but all involve the basics above. We'll keep it simple and refer to these.

Designing secure systems

- **Model** your threats
- Define your **security requirements**
  - What distinguishes a security requirement from a typical “software feature”?
- Apply good security **design principles**

A Security Plan: Management Policies

- **Risk Assessment**
- **Security Policy**
- **Implementation plan**
  - Security organization
  - Access controls
  - Authentication procedures, including biometrics
  - Authorization policies, authorization management systems
- **Security Audit**

Developing an E-commerce Security Plan

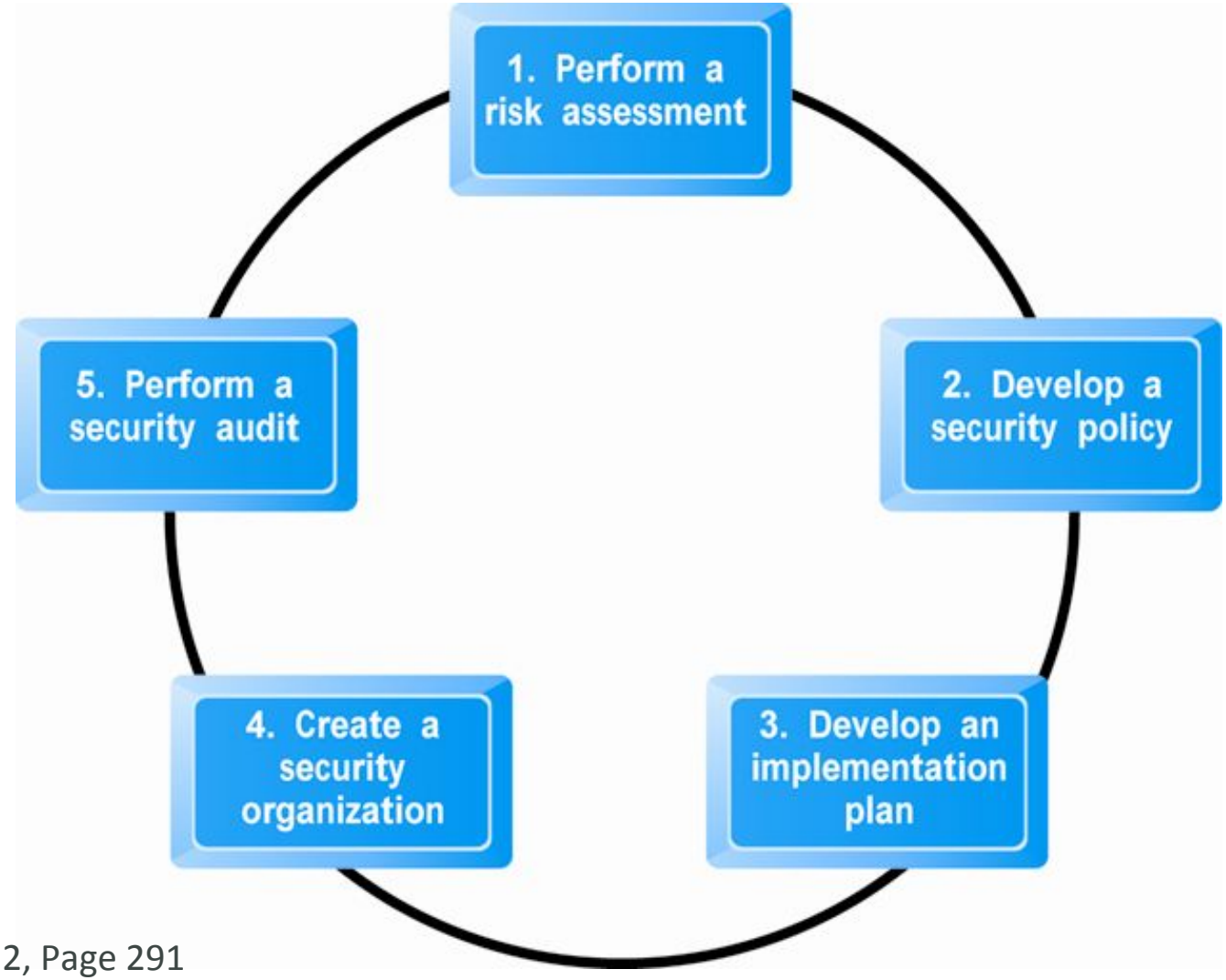


Figure 5.12, Page 291

The Role of Laws and Public Policy

- **Laws that give authorities tools for identifying, tracing, prosecuting cybercriminals:**
  - National Information Infrastructure Protection Act of 1996
  - USA Patriot Act
  - Homeland Security Act
- **Private and private-public cooperation**
  - CERT Coordination Center
  - US-CERT
- **Government policies and controls on encryption software**
  - OECD, G7/G8, Council of Europe, Wassener Arrangement

Reference

- Chapter-5 : E-commerce Security and Payment Systems of E-commerce business. technology. Society--By-Kenneth C. Laudon Carol Guercio Traver