Chapter 13: Electronic Commerce and Information Security

Invitation to Computer Science,
C++ Version, Third Edition

Objectives

In this chapter, you will learn about:

- E-commerce
- Databases
- Information security

Introduction

- E-commerce: financial transactions conducted by electronic means
- Early days (early and mid-1990s) of online commerce
  - A customer fills out an order via the Web and submits it
  - The online order is printed out by the business, and then processed like a “traditional” purchase

Introduction (continued)

- E-business
  - Every part of a financial transaction is handled electronically, including
    - Processing of orders
    - Verification of credit
    - Completion of transactions
    - Issuing debits
    - Alerting shipping
    - Reducing inventory

E-commerce

- Opening an online store requires at least as much planning as building another physical store location

The Vision Thing

- In planning for opening an online store, a company must access:
  - Its objectives
  - Risks involved
  - Costs involved
- The company should go ahead with its plans only if it is determined that its overall bottom line will improve by going online

Decisions, Decisions

- Personnel
  - In-house development or outsourcing
- Hardware
  - Web server machine
  - Additional computers

Decisions, Decisions (continued)

- Software: programs to
  - Process customer orders
  - Interact with accounting, shipping, and inventory control software
  - Manage and store customer information

Anatomy of a Transaction

- Goals for an online business
  - Draw potential customers to your site
  - Keep them there
  - Set up optimum conditions for them to complete a purchase
- A typical online transaction can be divided into nine steps

Step 1: Getting There

- How can you get customers to your Web site?
  - Conventional advertising
  - Obvious domain name
  - Search engine
  - Portal

Step 2: Do I Know You?

- Providing Web site personalization by:
  - Asking the user to register and then log-in on each visit
  - Using cookies
- Providing incentives and benefits for return customers

Step 3: Committing to an Online Purchase

- Must provide security for transmitting sensitive information
  - Encryption: encoding data to be transmitted into a scrambled form using a scheme agreed upon between the sender and the receiver
  - Authentication: verifying the identify of the receiver of your message

Step 3: Committing to an Online Purchase (continued)

- SSL (secure sockets layer)
  - A series of protocols that allow a client and a Web server to:
    - Agree on encryption methods
    - Exchange security keys
    - Authenticate the identity of each party

Steps 4 and 5: Payment Processing

- Most common payment option: credit card
- Option 1
  - Step 4: Online order form communicates with the accounting system
  - Step 5: Accounting system verifies the customer's credit and process the transaction on the fly

Steps 4 and 5: Payment Processing (continued)

- Option 2
  - Step 4: Collect information on the customer's order
  - Step 5: Evaluate the customer's credit and complete the transaction offline

Steps 6–9: Order Fulfillment

- Step 6: Order entry system alerts inventory system to reduce the items in stock
- Step 7: Order entry system contacts shipping system to arrange for shipping
- Steps 8 and 9: Shipping system works with the shipping company to pick up and deliver the purchase to the customer

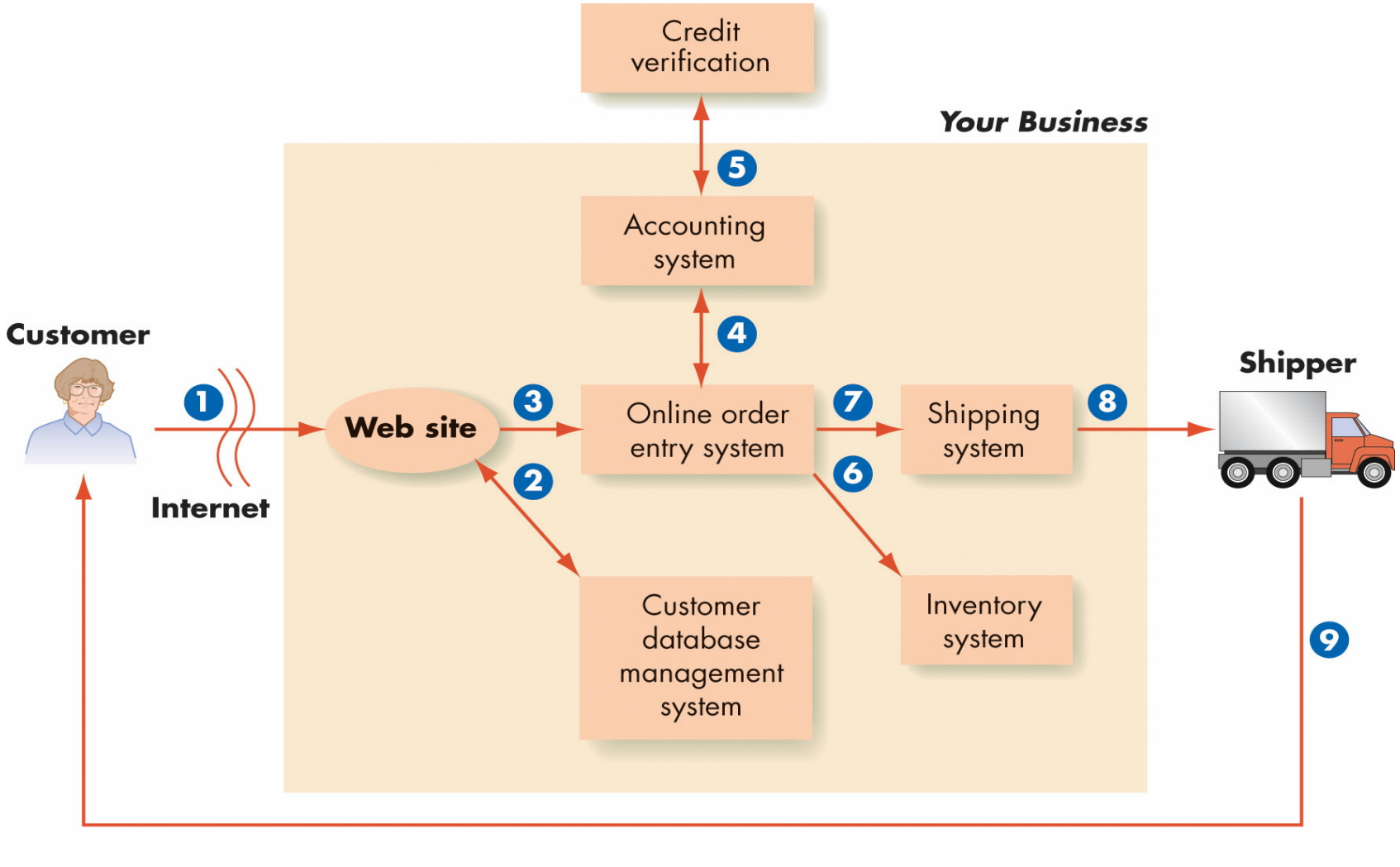

Figure 13.1: A Typical Online Transaction in Nine Steps

Designing Your Web Site

- Web site taxonomy
  - How information will be classified and organized on the Web site
- CRM (customer relationship management)
  - Goals
    - Improve your customer satisfaction
    - Build customer relationships
    - Bring people back to your Web site time and time again

Designing Your Web Site (continued)

- Some important Web site components
  - Site map
  - Navigation bar
  - Shopping carts
  - Order checkout forms
  - Shipping options
  - E-mail confirmations
  - Privacy policy

Designing Your Web Site (continued)

- Web pages should be designed to be displayed on different machines, operating systems, and browsers

- Text-only options should be offered for users with slow connections, the visually impaired, and the hearing-impaired

Databases

- An electronic database
  - Stores data items
  - Data items can be extracted
  - Data items can be sorted
  - Data items can be manipulated to reveal new information

Data Organization

- Byte
  - A group of eight bits
  - Can store the binary representation of a single character or of a small integer number
  - A single unit of addressable memory
- Field
  - A group of bytes used to represent a string of characters

Data Organization (continued)

- Record
  - A collection of related fields
- Data file
  - Related records are kept in a data file
- Database
  - Related files make up a database

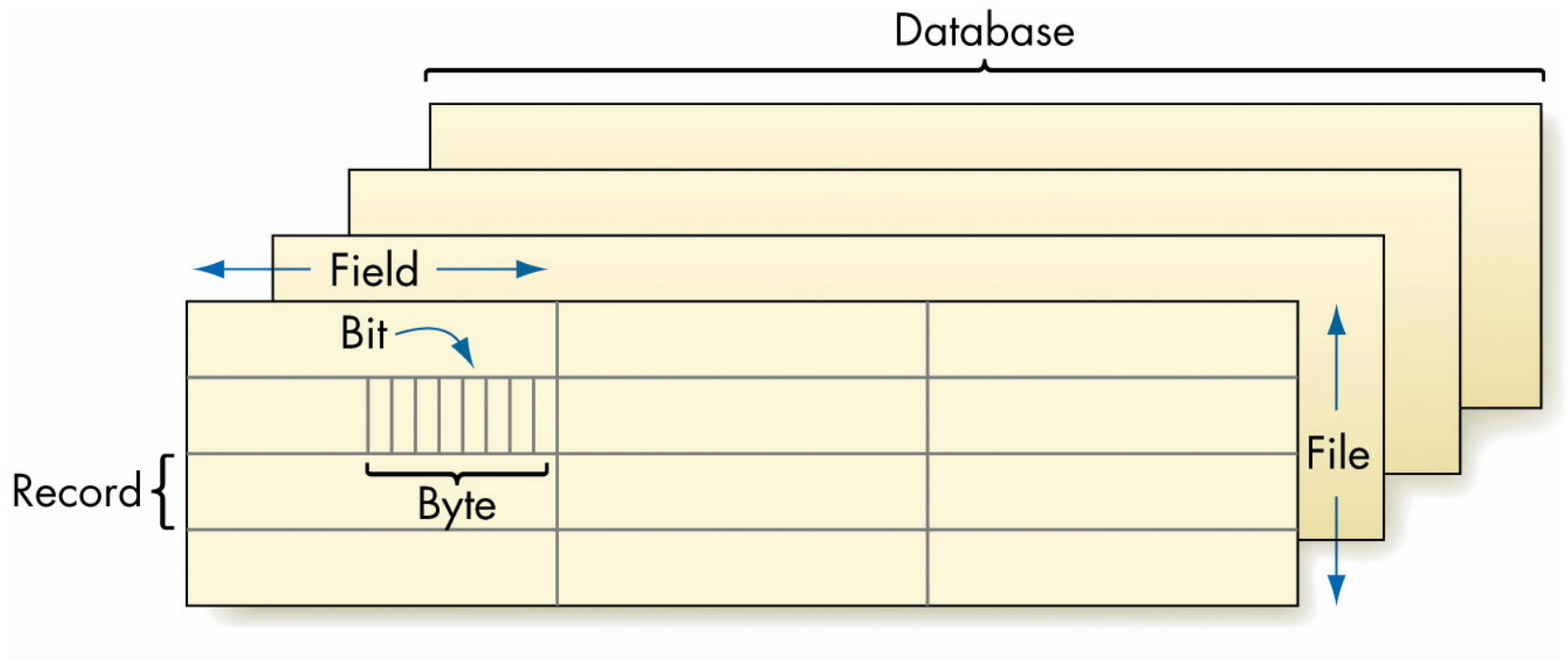

Figure 13.3
Data Organization Hierarchy

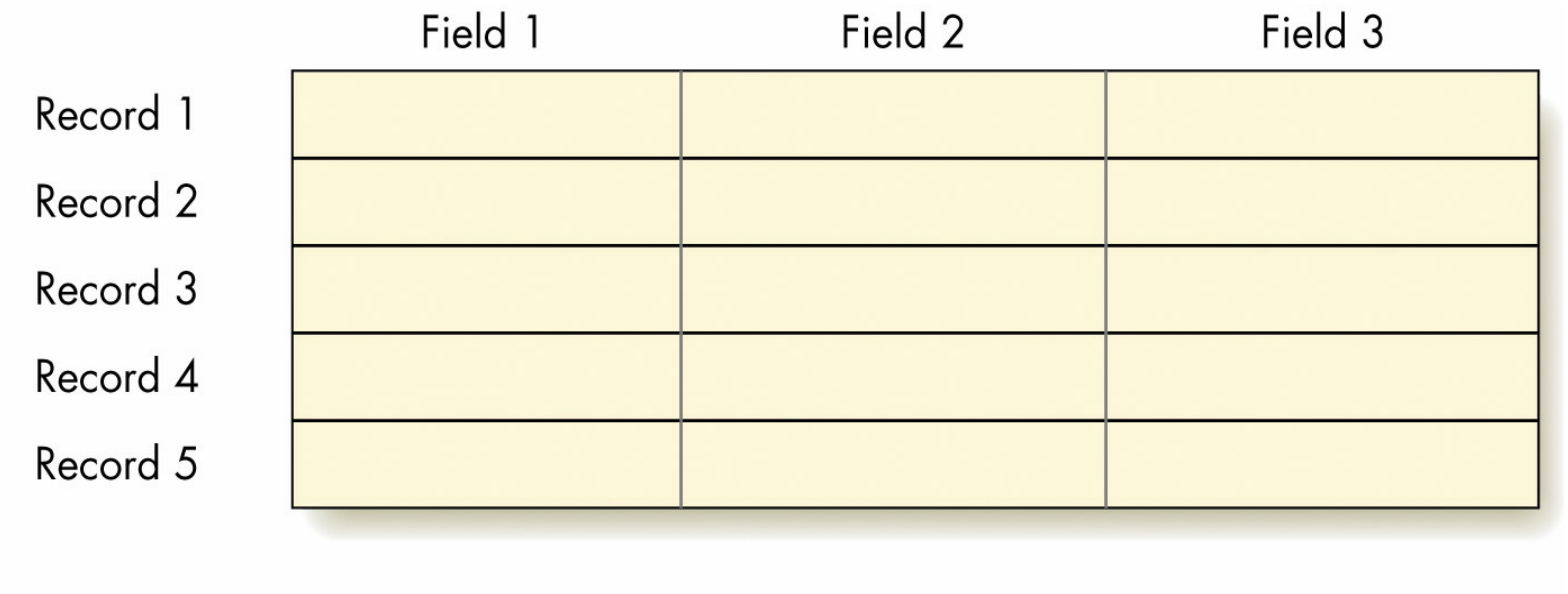

Figure 13.4
Records and Fields in a Single File

ID	LastName	FirstName	Birthdate	PayRate	HoursWorked
149	Takasano	Frederick	5/23/1966	$12.35	250

Figure 13.5
One Record in the Rugs-For-You Employees File

Database Management Systems

- Database management system (DBMS)
  - Manages the files in a database
- Relational database model
  - Conceptual model of a file as a two-dimensional table

Database Management Systems (continued)

- In a relational database
  - A table represents information about an entity
  - A row contains data about one instance of an entity
  - A row is called a tuple
  - Each category of information is called an attribute

EMPLOYEES

ID	LASTNAME	FIRSTNAME	BIRTHDATE	PAYRATE	HOURSWORKED
116	Kay	Janet	3/29/1956	$16.60	94
123	Perreira	Francine	8/15/1987	$ 8.50	185
149	Takasano	Frederick	5/23/1966	$12.35	250
171	Kay	John	11/17/1954	$17.80	245
165	Honou	Morris	6/9/1988	$ 6.70	53

Figure 13.6
Employees Table for Rugs-For-You

InsurancePolicies

EmployeeID	PlanType	DateIssued
171	B2	10/18/1974
171	C1	6/21/1982
149	B2	8/16/1990
149	A1	5/23/1995
149	C2	12/18/1999

Figure 13.7
InsurancePolicies Table for Rugs-For-You

Database Management Systems (continued)

- Specialized query languages
  - Enable the user or another application program to query the database
  - Example: SQL (Structured Query Language)
- Relationships among different entities in a database
  - Established through the correspondence between primary keys and foreign keys

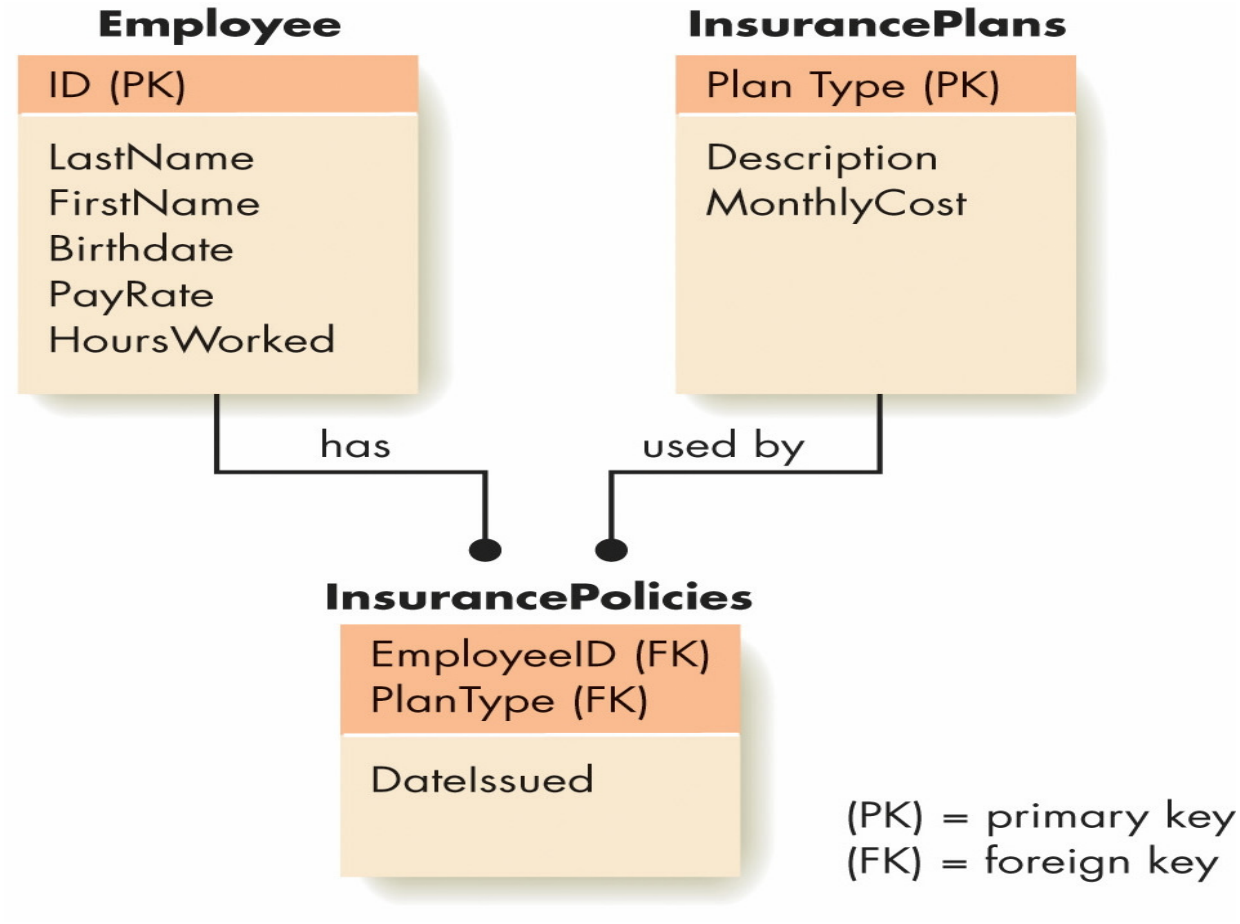

Figure 13.8
Three Entities in the Rugs-For-You Database

Other Considerations

- Performance issues
  - Large files are maintained on disk
  - Organizing record storage on disk can minimize time to access a particular record
  - Creating additional records to be stored with the file can significantly reduce access time

Other Considerations (continued)

- Distributed databases
  - Allow physical data to reside at separate and independent locations that are networked
- Massive, integrated government databases raise legal, political, social, and ethical issues

Information Security

- Information security
  - Data protection, whether on disk or transmitted across a network
  - Authentication: prevent access by hackers
  - Encryption: make data meaningless if they do get it

Encryption Overview

- Cryptography
  - The science of “secret writing”
- Plaintext
  - A message that is not encoded
- Ciphertext
  - An encrypted message

Encryption Overview (continued)

- Process of encryption and decryption
  - Plaintext is encrypted before it is sent
  - Ciphertext is decrypted back to plaintext when it is received
- A symmetric encryption algorithm
  - Requires a secret key known to both the sender and receiver
    - Sender encrypts the plaintext using the key
    - Receiver decrypt the message using the key

Encryption Overview (continued)

- Asymmetric encryption algorithm
  - Also called public key encryption algorithm
  - The key for encryption and the key for decryption are different
    - Person A makes an encryption key public
    - Anyone can encrypt a message using the public key and send it to A
    - Only A has the decryption key and can decrypt the message

Simple Encryption Algorithms: Caesar Cipher

- Caesar cipher
  - Also called a shift cipher
  - Each character in the message is shifted to another character some fixed distance farther along in the alphabet
  - A stream cipher: encodes one character at a time
  - A substitution cipher: a single letter of plaintext generates a single letter of ciphertext

Block Cipher

- A group or block of plaintext letters gets encoded into a block of ciphertext, but not by substituting one at a time for each character

- Each plaintext character in the block contributes to more than one ciphertext character

Block Cipher (continued)

- One ciphertext character is created as a result of more than one plaintext letter
- Diffusion (scattering) of the plaintext within the ciphertext

DES

- Stands for Data Encryption Standard
- Designed to protect electronic information
- A block cipher
- Blocks: 64 bits long
- Key: 64 bit binary key (only 56 bits are actually used)

DES (continued)

- Every substitution, reduction, expansion, and permutation is determined by a well-known set of tables

- The same algorithm serves as the decryption algorithm

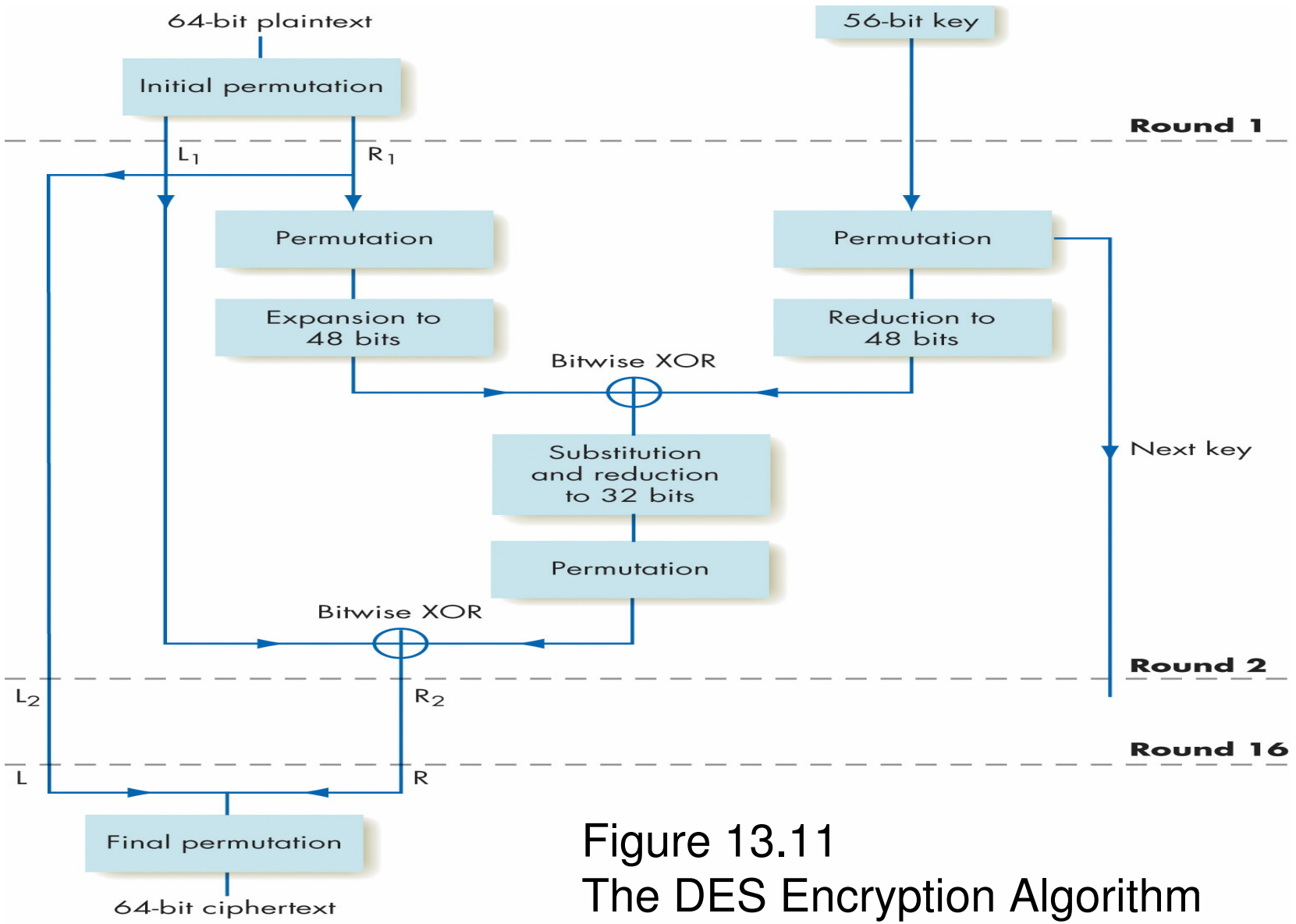

Figure 13.11
The DES Encryption Algorithm

DES (continued)

- Triple DES
  - Improves the security of DES
  - Requires two 56-bit keys
  - Runs the DES algorithm three times
- AES (Advanced Encryption Standard)
  - Uses successive rounds of computations that mix up the data and the key
  - Key length: 128, 192, or 256 bits

Public-Key Systems

- RSA
  - Most common public key encryption algorithm
  - Based on results from number theory
  - If *n* is a large number, it is extremely difficult to find the prime factors for *n*
  - RSA is often used in the initial stage of communication between client and server

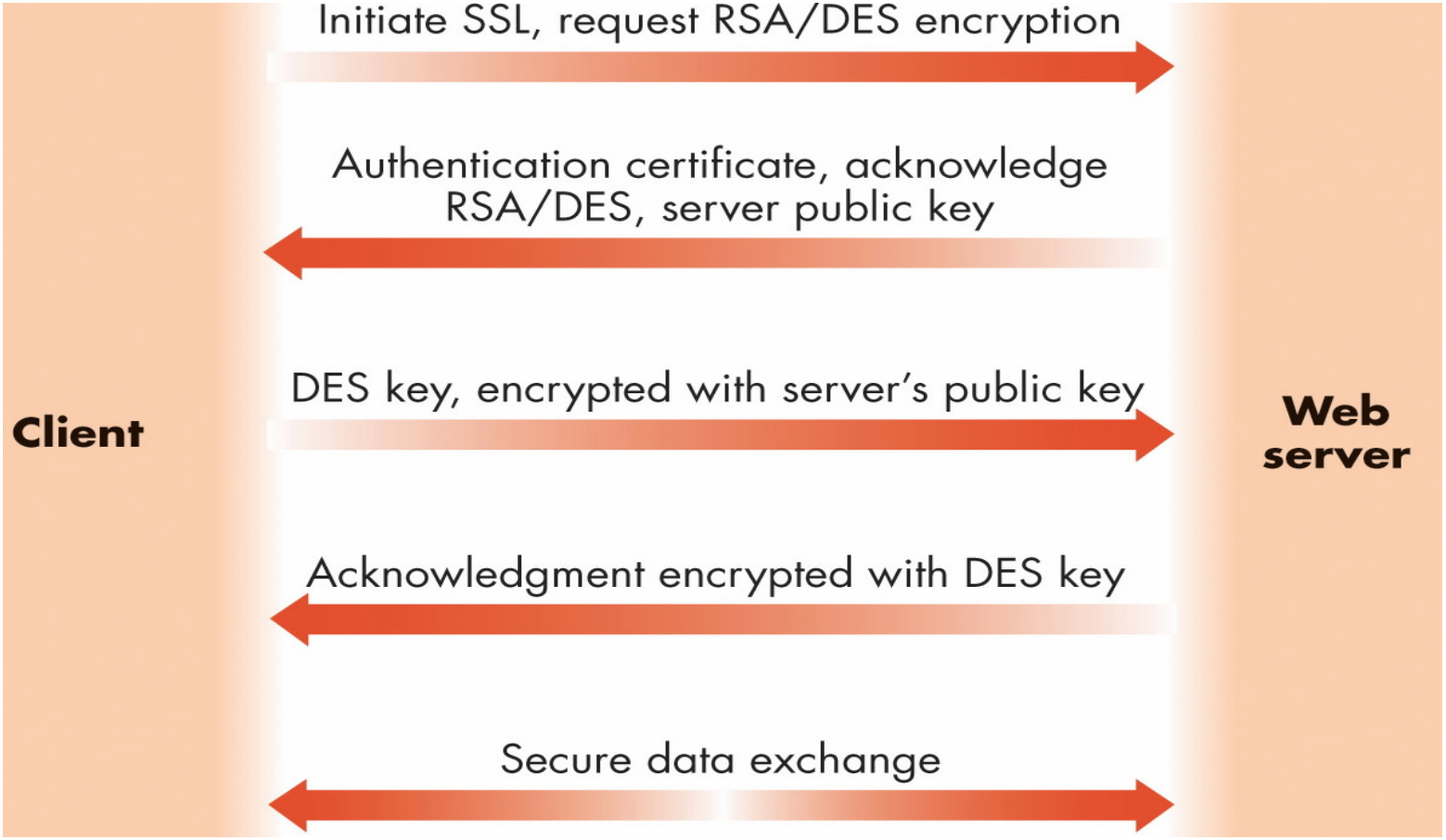

Figure 13.12
An SSL Session

Summary

- E-business: every part of a financial transaction is handled electronically
- Opening an online store requires a significant amount of planning
- Database: allows data items to be stored, extracted, sorted, and manipulated
- Relational database model: conceptual model of a file as a two-dimensional table

Summary

- Main parts of information security: encryption and authentication
- Types of encryption algorithms
  - Symmetric encryption algorithms
  - Asymmetric encryption algorithms (or public key encryption algorithms)
- Encryption algorithms: Caesar cipher, block cipher, DES, Triple DES, AES, RSA