COURSE TECHNOLOGY
CENGAGE Learning™

Security+ Guide to Network Security Fundamentals, Fourth Edition

Chapter 11
Basic Cryptography

Objectives

- Define cryptography
- Describe hash, symmetric, and asymmetric cryptographic algorithms
- List the various ways in which cryptography is used

Introduction

- Multilevel approach to information security
  - Firewalls
  - Network intrusion detection systems
  - All-in-one network security appliances
- Second level of protection
  - Encryption of document contents

Defining Cryptography

- What is cryptography?
  - Scrambling information so it appears unreadable to attackers
  - Transforms information into secure form
- Steganography
  - Hides the existence of data
  - Image, audio, or video files containing hidden message embedded in the file
  - Achieved by dividing data and hiding in unused portions of the file

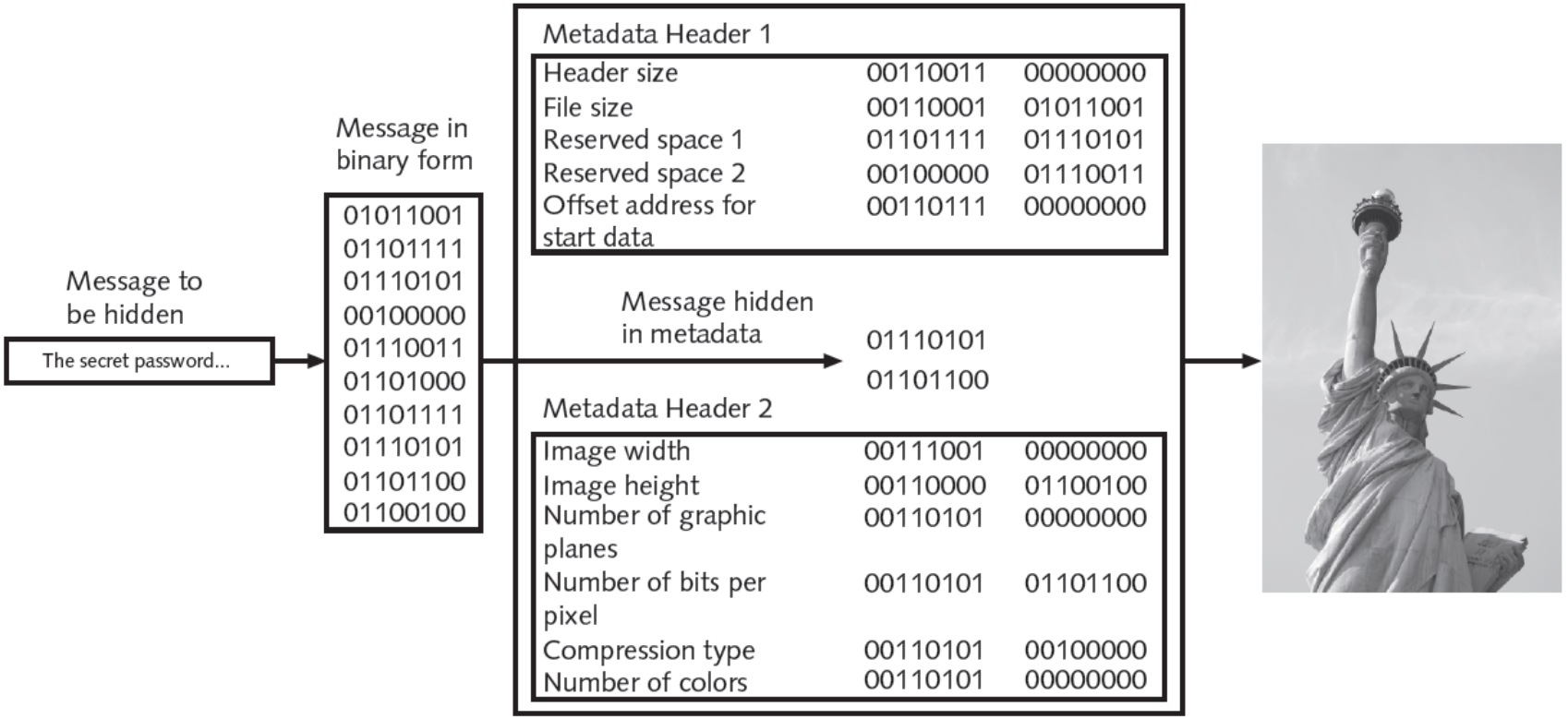

Figure 11-1 Data hidden by steganography

What is Cryptography? (cont'd.)

- Origins of cryptography
  - Used by Julius Caesar
- Encryption
  - Changing original text into a secret message using cryptography
- Decryption
  - Changing secret message back to original form
- Cleartext data
  - Data stored or transmitted without encryption

What is Cryptography? (cont'd.)

- Plaintext
  - Data to be encrypted
  - Input into an encryption algorithm
- Key
  - Mathematical value entered into the algorithm to produce ciphertext (scrambled text)
  - Reverse process uses the key to decrypt the message

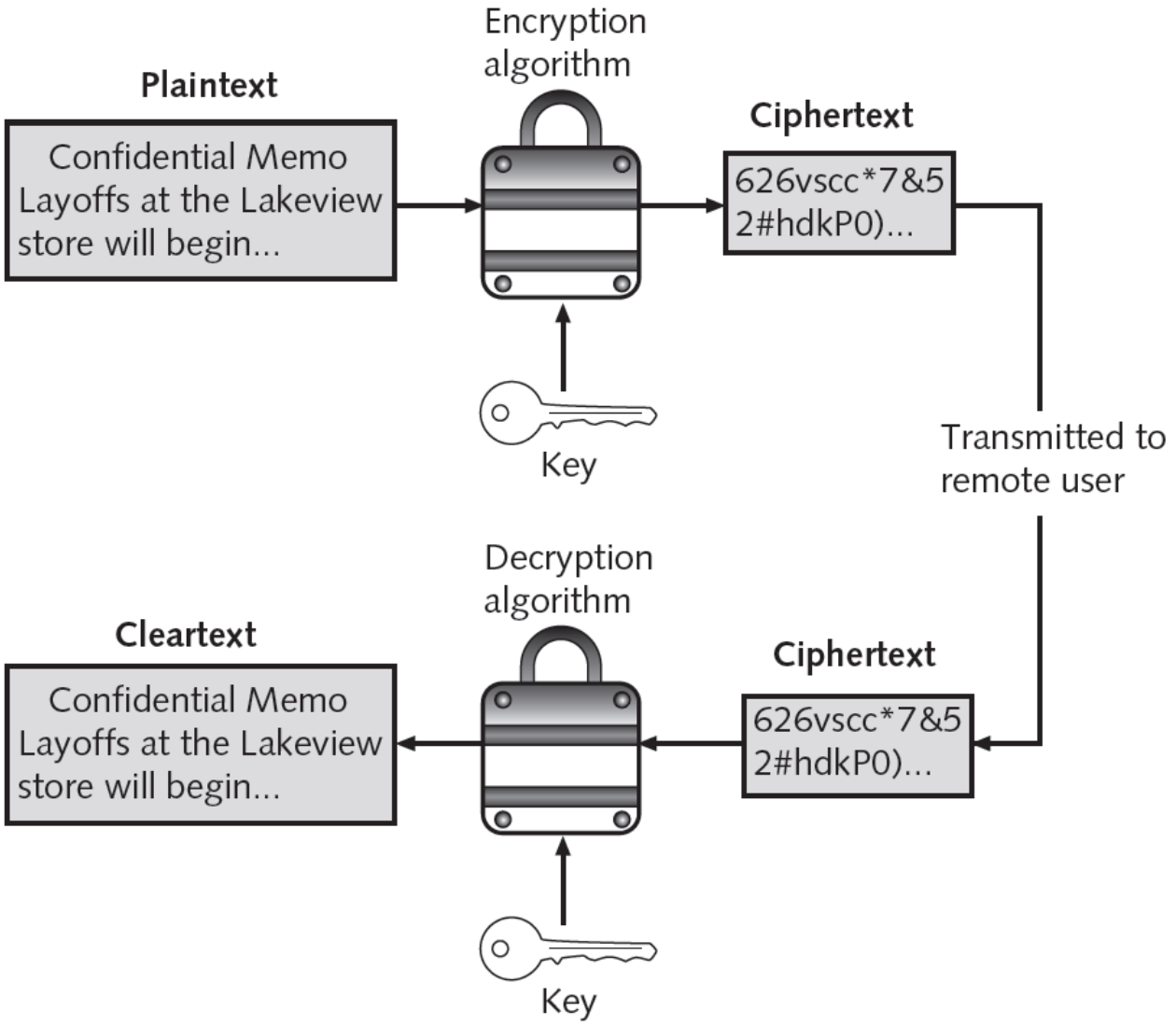

Figure 11-2 Cryptography process

Cryptography and Security

- Cryptography can provide five basic information protections
  - Confidentiality
    - Insures only authorized parties can view it
  - Integrity
    - Insures information is correct and unaltered
  - Availability
    - Authorized users can access it
  - Authenticity of the sender
  - Nonrepudiation
    - Proves that a user performed an action

Characteristic	Description	Protection
Confidentiality	Ensures that only authorized parties can view the information	Encrypted information can only be viewed by those who have been provided the key
Integrity	Ensures that the information is correct and no unauthorized person or malicious software has altered that data	Encrypted information cannot be changed except by authorized users who have the key
Availability	Ensures that data is accessible to authorized users	Authorized users are provided the decryption key to access the information
Authenticity	Provides proof of the genuineness of the user	Cryptography can prove that the sender was legitimate and not an imposter
Nonrepudiation	Proves that a user performed an action	Cryptographic nonrepudiation prevents an individual from fraudulently denying they were involved in a transaction

Table 11-1 Information protections by cryptography

Cryptographic Algorithms

- Three categories of cryptographic algorithms
  - Hash algorithms
  - Symmetric encryption algorithms
  - Asymmetric encryption algorithms
- Hash algorithms
  - Most basic type of cryptographic algorithm
  - Process for creating a unique digital fingerprint for a set of data
  - Contents cannot be used to reveal original data set
  - Primarily used for comparison purposes

Cryptographic Algorithms (cont'd.)

- Example of hashing (ATMs)
  - Bank customer has PIN of 93542
  - Number is hashed and result stored on card's magnetic stripe
  - User inserts card in ATM and enters PIN
  - ATM hashes the pin using the same algorithm that was used to store PIN on the card
  - If two values match, user may access ATM

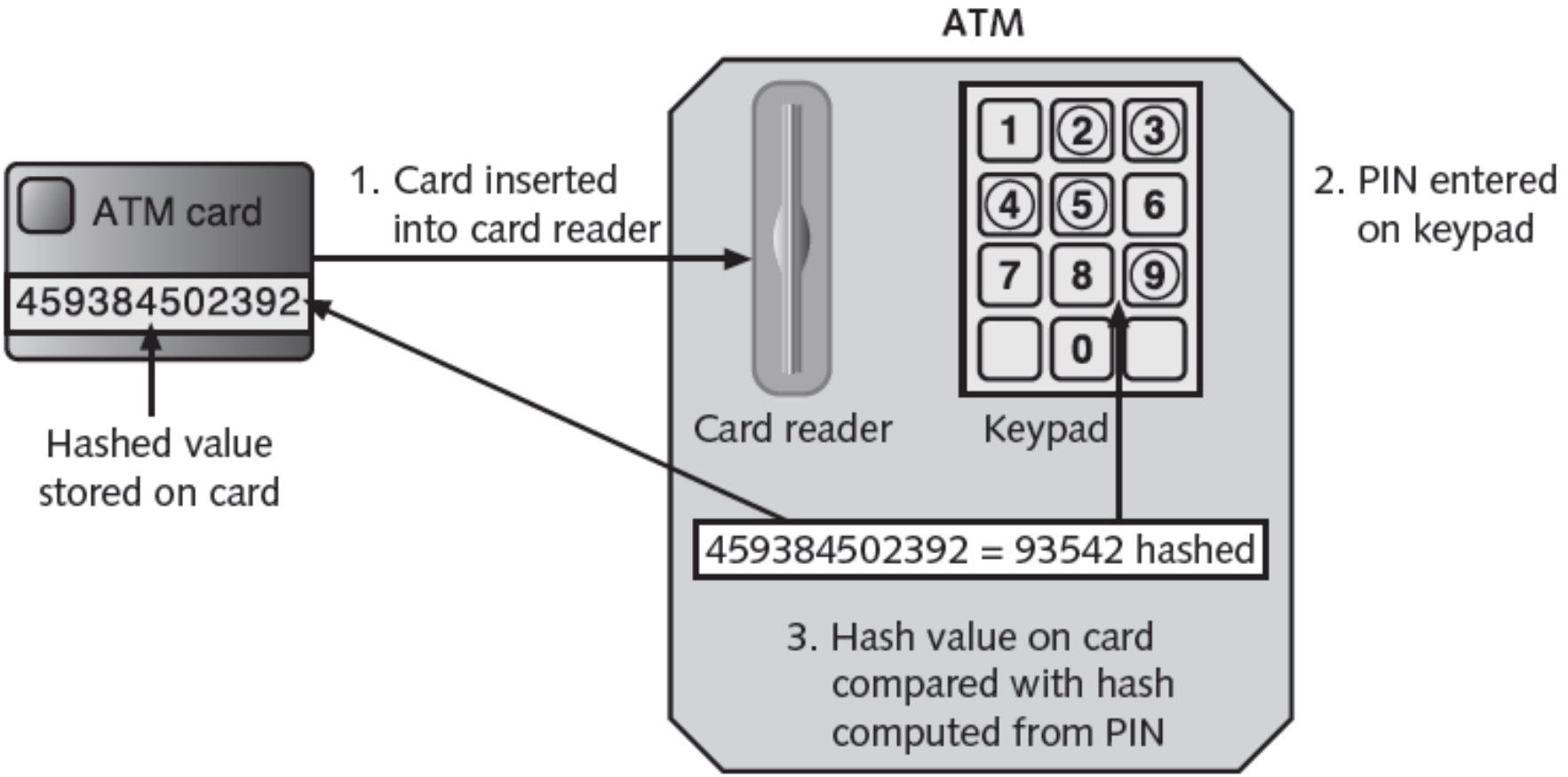

Figure 11-3 Hashing at an ATM

Cryptographic Algorithms (cont'd.)

- Secure hashing algorithm characteristics
  - Fixed size
    - Short and long data sets have the same size hash
  - Unique
    - Two different data sets cannot produce the same hash
  - Original
    - Dataset cannot be created to have a predefined hash
  - Secure
    - Resulting hash cannot be reversed to determine original plaintext

Cryptographic Algorithms (cont'd.)

- Hashing used to determine message integrity
  - Can protect against man-in-the-middle attacks
- Hashed Message Authentication Code (HMAC)
  - Hash variation providing improved security
  - Uses secret key possessed by sender and receiver
  - Receiver uses key to decrypt the hash
- Hash values often posted on download sites
  - To verify file integrity after download

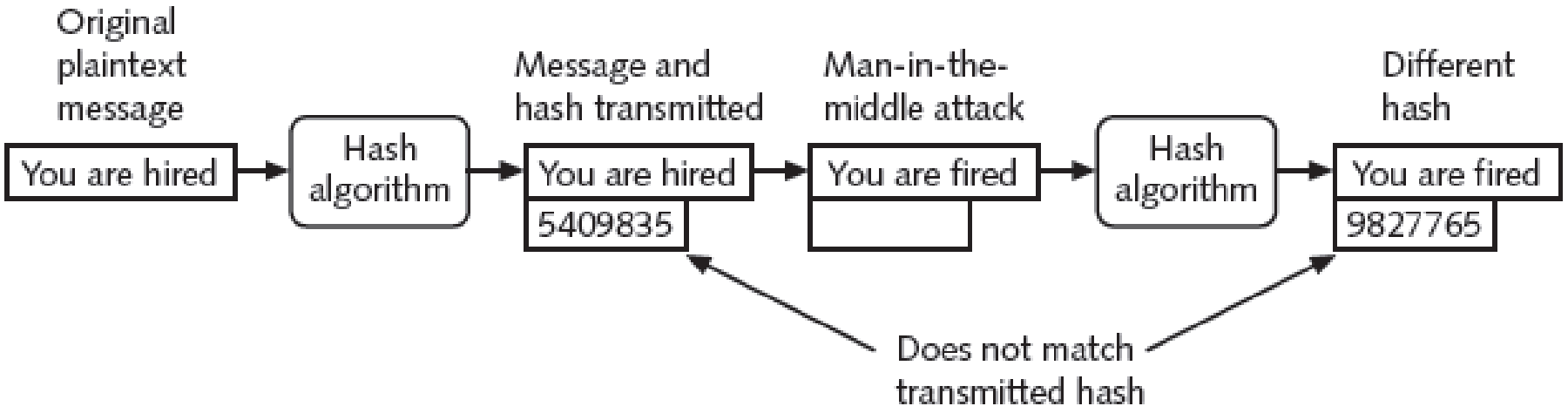

Figure 11-4 Man-in-the-middle attack defeated by hashing

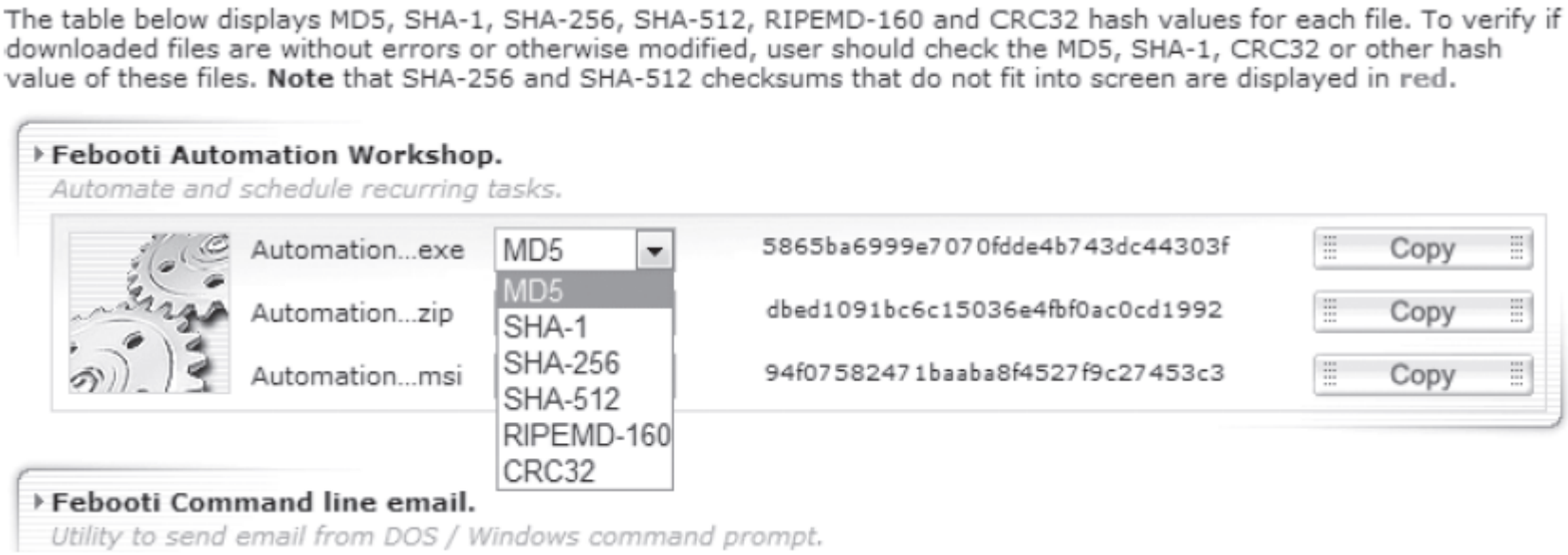

Figure 11-5 Posted hash values

Characteristic	Protection?
Confidentiality	No
Integrity	Yes
Availability	No
Authenticity	No
Nonrepudiation	No

Table 11-2 Information protections by hashing cryptography

Cryptographic Algorithms (cont'd.)

- Most common hash algorithms
  - Message Digest
  - Secure Hash Algorithm
  - Whirlpool
  - RIPEMD
  - Password hashes

Cryptographic Algorithms (cont'd.)

- Message Digest (MD)
  - Three versions
- Message Digest 2
  - Takes plaintext of any length and creates 128 bit hash
  - Padding added to make short messages 128 bits
  - Considered too slow today and rarely used
- Message Digest 4
  - Has flaws and was not widely accepted

Cryptographic Algorithms (cont'd.)

- Message Digest 5
  - Designed to address MD4's weaknesses
  - Message length padded to 512 bits
  - Weaknesses in compression function could lead to collisions
  - Some security experts recommend using a more secure hash algorithm
- Secure Hash Algorithm (SHA)
  - More secure than MD
  - No weaknesses identified

Cryptographic Algorithms (cont'd.)

- Whirlpool
  - Recent cryptographic hash
  - Adopted by standards organizations
  - Creates hash of 512 bits
- Race Integrity Primitives Evaluation Message Digest (RIPEMD)
  - Two different and parallel chains of computation
  - Results are combined at end of process

Cryptographic Algorithms (cont'd.)

- Password hashes
  - Used by Microsoft Windows operating systems
    - LAN Manager hash
    - New Technology LAN Manager (NTLM) hash
- Linux and Apple Mac strengthen password hashes by including random bit sequences
  - Known as a salt
  - Make password attacks more difficult

Symmetric Cryptographic Algorithms

- Original cryptographic algorithms
- Data Encryption Standard
- Triple Data Encryption Standard
- Advanced Encryption Standard
- Several other algorithms
- Understanding symmetric algorithms
  - Same shared single key used to encrypt and decrypt document

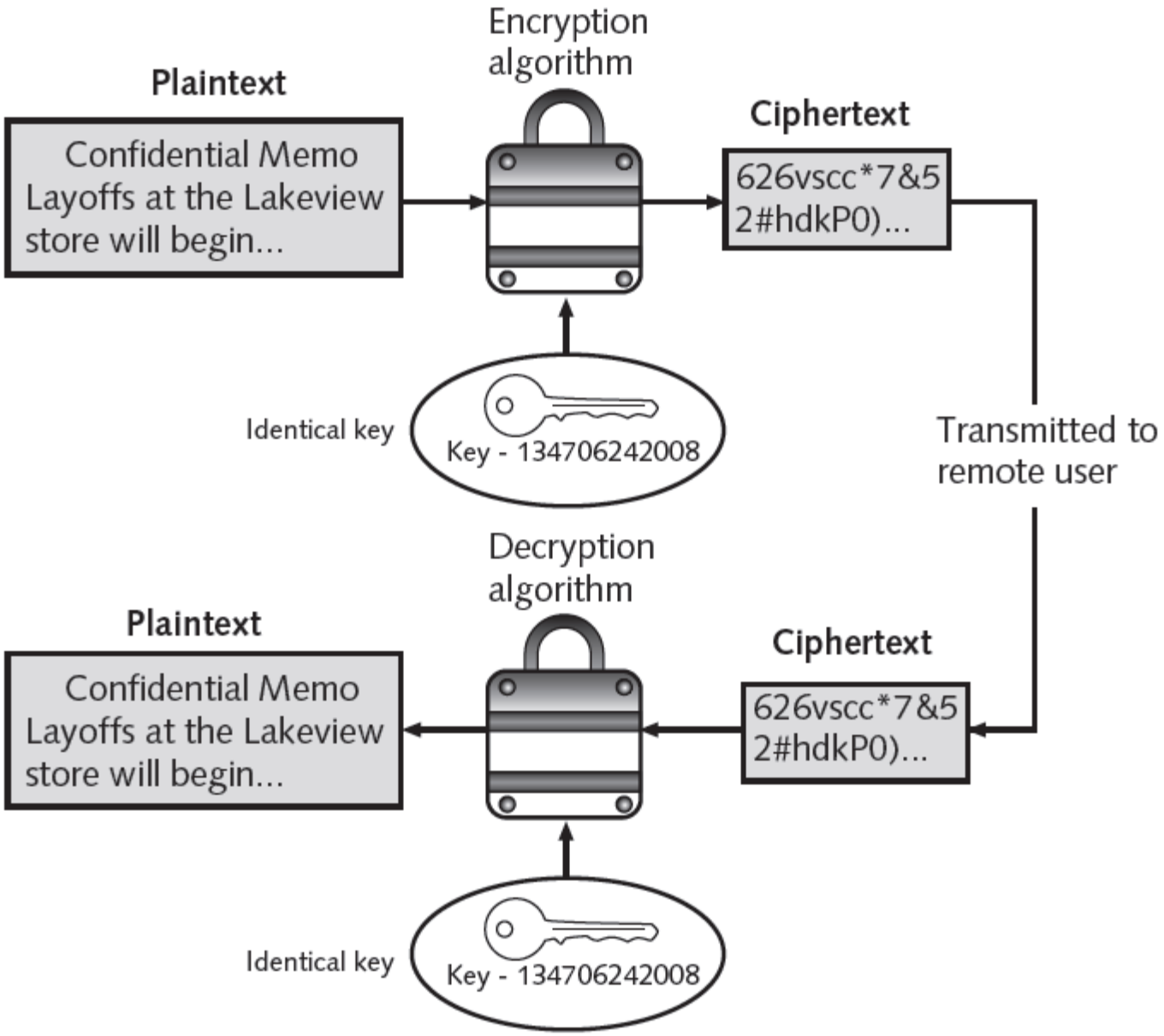

Figure 11-6
Symmetric (private key) cryptography

Symmetric Cryptographic Algorithms (cont'd.)

- Two symmetric algorithm categories
  - Based on amount of data processed at a time
- Stream cipher
  - Takes a character and replaces it with a character
  - Simplest type: substitution cipher
- Monoalphabetic substitution cipher
  - Easy to break

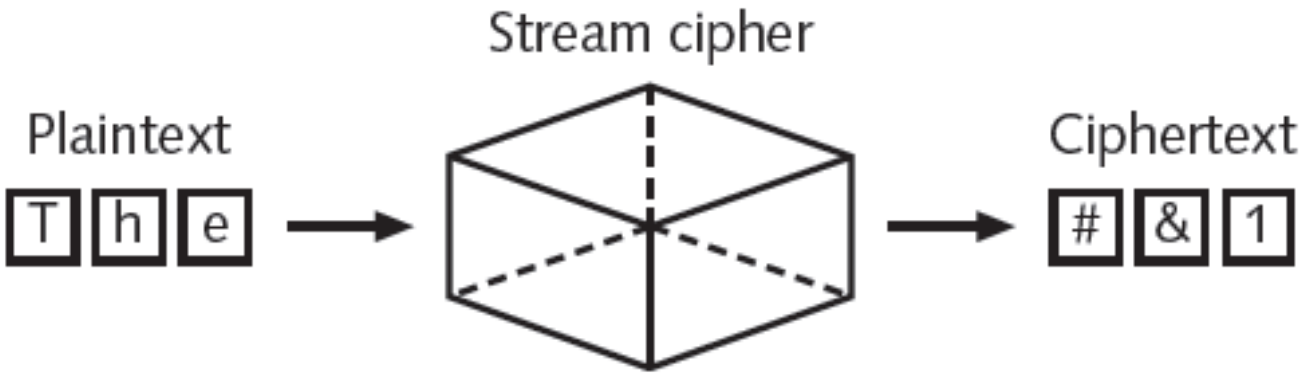

Figure 11-7 Stream cipher

Symmetric Cryptographic Algorithms (cont'd.)

- Homoalphabetic substitution cipher
  - Single plaintext character mapped to multiple ciphertext character

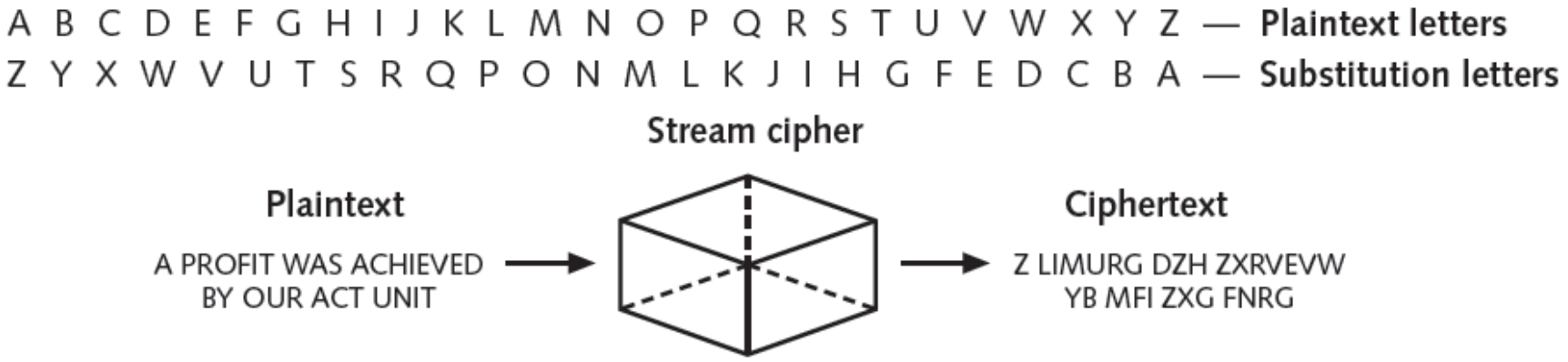

Figure 11-8 Substitution cipher

Symmetric Cryptographic Algorithms (cont'd.)

- Transposition cipher
  - Rearranges letters without changing them

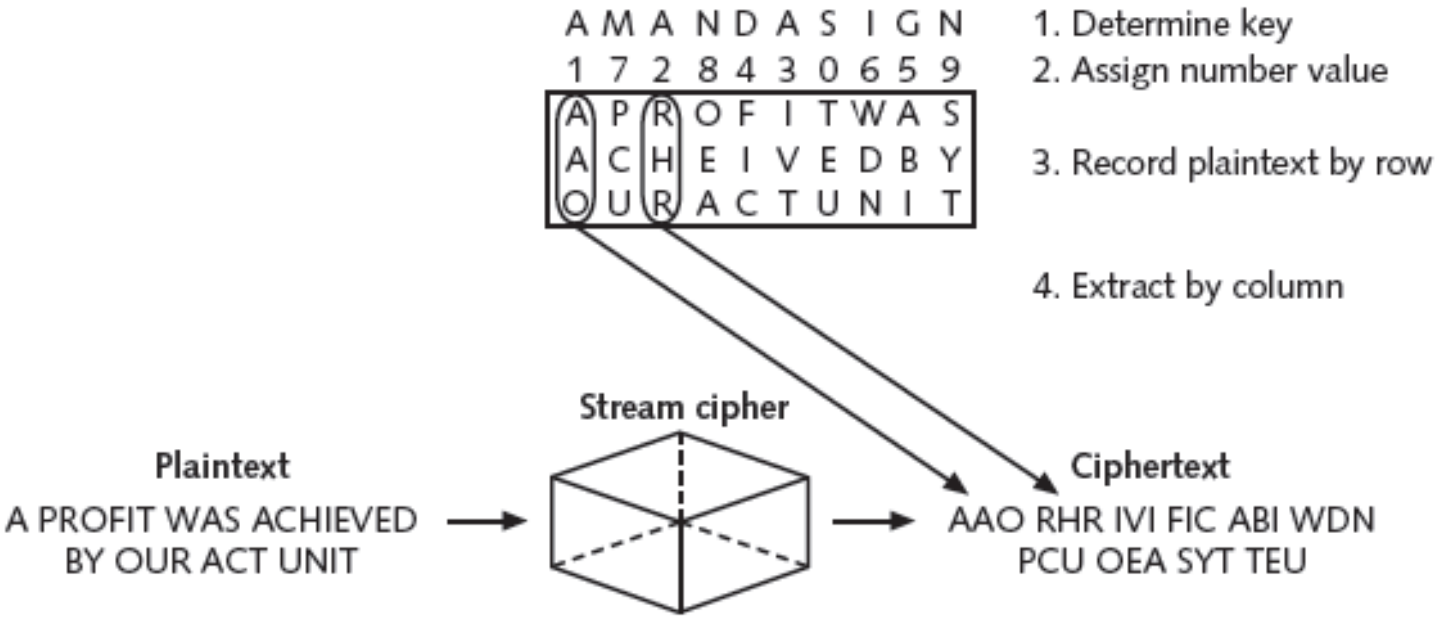

Figure 11-9 Transposition cipher

Symmetric Cryptographic Algorithms (cont'd.)

- Final step in most symmetric ciphers
  - Combine cipher stream with plaintext to create the ciphertext

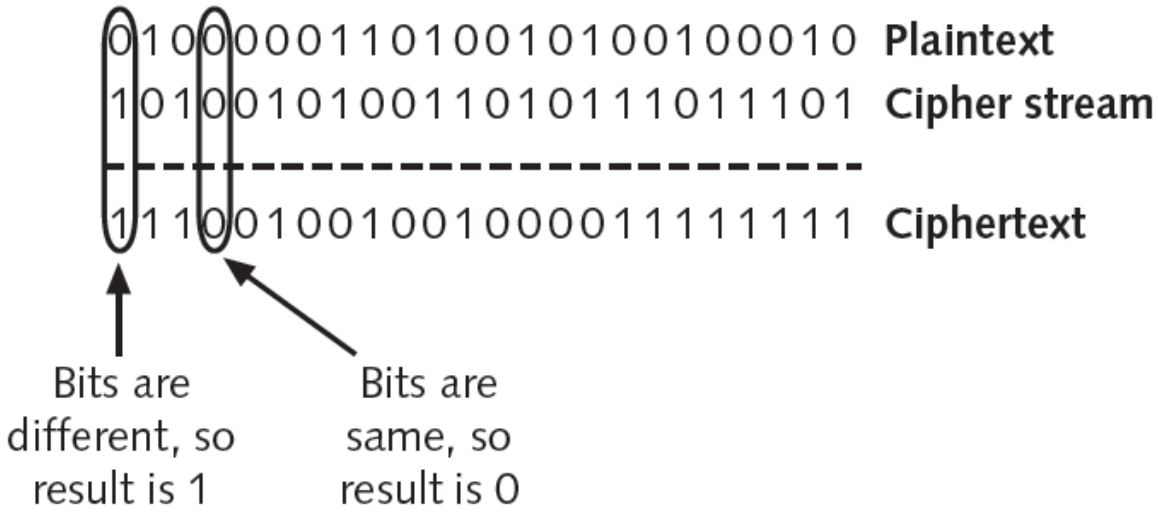

Figure 11-10 Combine ciphertext

Symmetric Cryptographic Algorithms (cont'd.)

- One-time pad (OTP)
  - Creates a truly random key to combine with the plaintext
  - Considered secure if random, kept secret, and not reused
- Block cipher
  - Works on entire block of plaintext at a time
  - Separate blocks of 8 to 16 bytes encrypted independently
  - Blocks randomized for additional security

Symmetric Cryptographic Algorithms (cont'd.)

- Stream cipher advantages
  - Fast if plaintext is short
- Stream cipher disadvantages
  - Consumes much processing power if plaintext is long
  - More prone to attack because engine generating stream does not vary
- Block ciphers considered more secure because output is more random

Characteristic	Protection?
Confidentiality	Yes
Integrity	Yes
Availability	Yes
Authenticity	No
Nonrepudiation	No

Table 11-3 Information protections by symmetric cryptography

Symmetric Cryptographic Algorithms (cont'd.)

- Data Encryption Standard (DES)
  - Based on product originally designed in early 1970s
  - Adopted as a standard by the U.S. government
- Triple Data Encryption standard (3DES)
  - Designed to replace DES
  - Uses three rounds of encryption
  - Ciphertext of first round becomes input for second iteration
  - Most secure versions use different keys used for each round

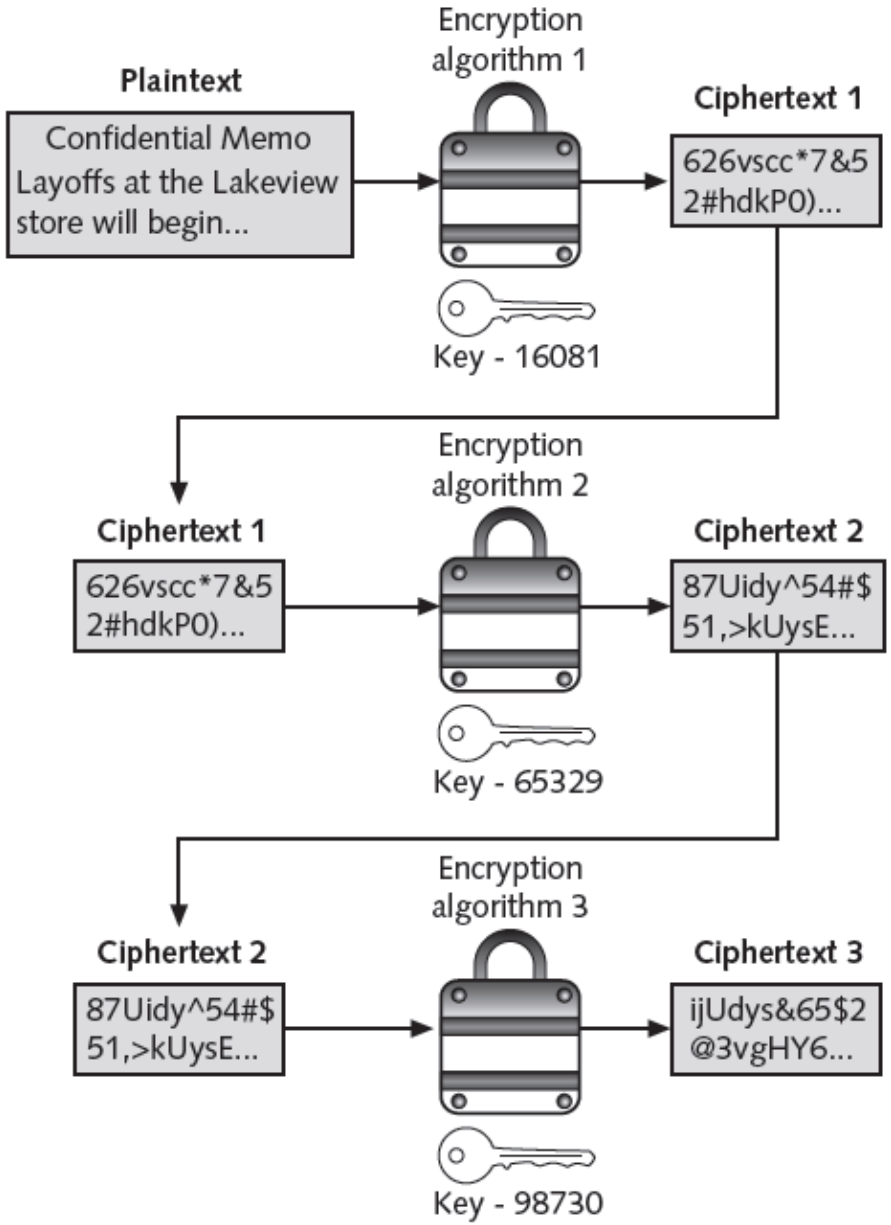

Figure 11-11 3DES

Symmetric Cryptographic Algorithms (cont'd.)

- Advanced Encryption Standard (AES)
  - Symmetric cipher approved by NIST in 2000 as replacement for DES
  - Official encryption standard used by the U.S. government
  - Performs three steps on every block of plaintext
  - Designed to be secure well into the future

Other Algorithms

- Rivest Cipher (RC)
  - Family of cipher algorithms designed by Ron Rivest
- International Data Encryption Algorithm (IDEA)
  - Used in European nations
  - Block cipher processing 64 bits with a 128-bit key with 8 rounds
- Blowfish
  - Block cipher operating on 64-bit blocks with key lengths from 32-448 bits
  - No significant weaknesses have been identified

Asymmetric Cryptographic Algorithms

- Weakness of symmetric algorithms
  - Distributing and maintaining a secure single key among multiple users distributed geographically
- Asymmetric cryptographic algorithms
  - Also known as public key cryptography
  - Uses two mathematically related keys
  - Public key available to everyone and freely distributed
  - Private key known only to individual to whom it belongs

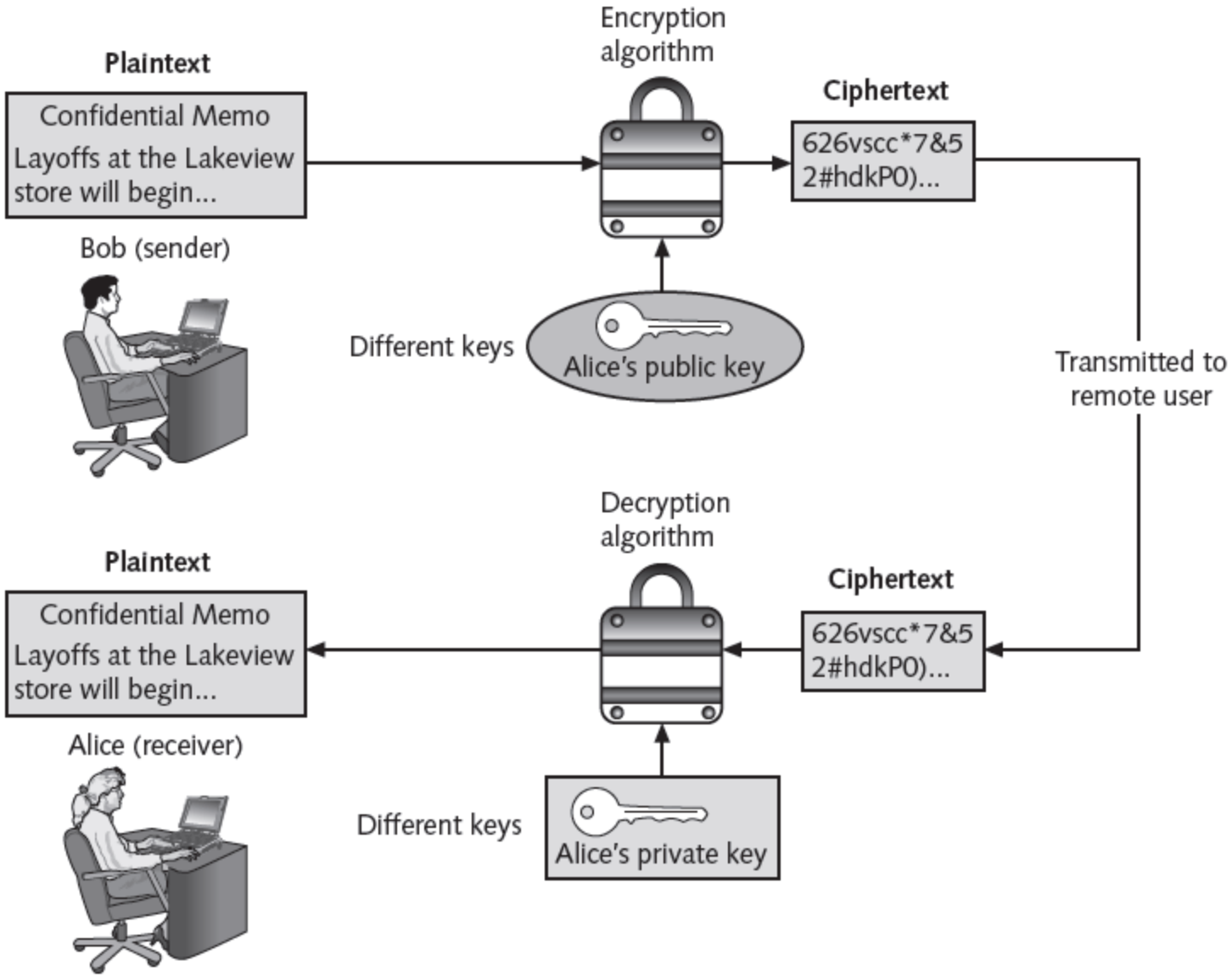

Figure 11-12 Asymmetric (public key) cryptography

Asymmetric Cryptographic Algorithms (cont'd.)

- Important principles
  - Key pairs
  - Public key
  - Private key
  - Both directions
- Digital signature
  - Verifies the sender
  - Prevents sender from disowning the message
  - Proves message integrity

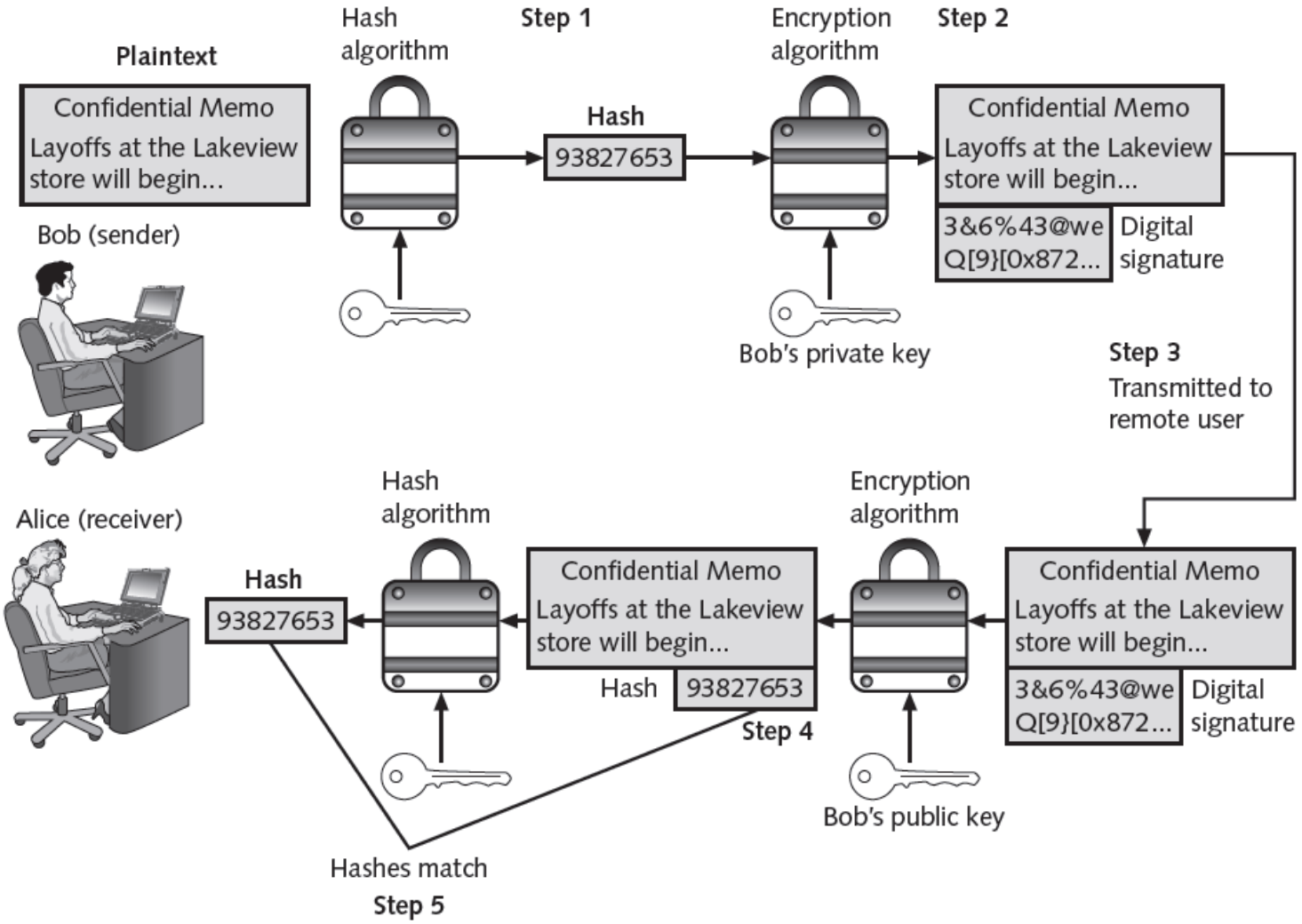

Figure 11-13 Digital signature

Action	Whose key to use	Which key to use	Explanation
Bob wants to send Alice an encrypted message	Alice's key	Public key	When an encrypted message is to be sent, the recipient's key is used and not the sender's keys
Alice wants to read an encrypted message sent by Bob	Alice's key	Private key	An encrypted message can only be read by using the recipient's private key
Bob wants to send a copy to himself of the encrypted message that he sent to Alice	Bob's key	Public key to encrypt Private key to decrypt	An encrypted message can only be read by the recipient's private key; Bob would need to encrypt it with his own public key and then use his private key to decrypt it
Bob receives an encrypted reply message from Alice	Bob's key	Private key	The recipient's private key is used to decrypt received messages
Bob wants Susan to read Alice's reply message that he received	Susan's key	Public key	The message should be encrypted with Susan's key for her to decrypt and read it with her private key
Bob wants to send Alice a message with a digital signature	Bob's key	Private key	Bob's private key is used to encrypt the hash
Alice wants to see Bob's digital signature	Bob's key	Public key	Because Bob's public and private keys work in both directions, Alice can use his public key to decrypt the hash

Table 11-4 Asymmetric cryptography practices

Characteristic	Protection?
Confidentiality	Yes
Integrity	Yes
Availability	Yes
Authenticity	Yes
Nonrepudiation	Yes

Table 11-5 Information protections by asymmetric cryptography

Asymmetric Cryptographic Algorithms (cont'd.)

- RSA
  - Published in 1977 and patented by MIT in 1983
  - Most common asymmetric cryptography algorithm
  - Uses two large prime numbers
- Elliptic curve cryptography (ECC)
  - Users share one elliptic curve and one point on the curve
  - Uses less computing power than prime number-based asymmetric cryptography
    - Key sizes are smaller

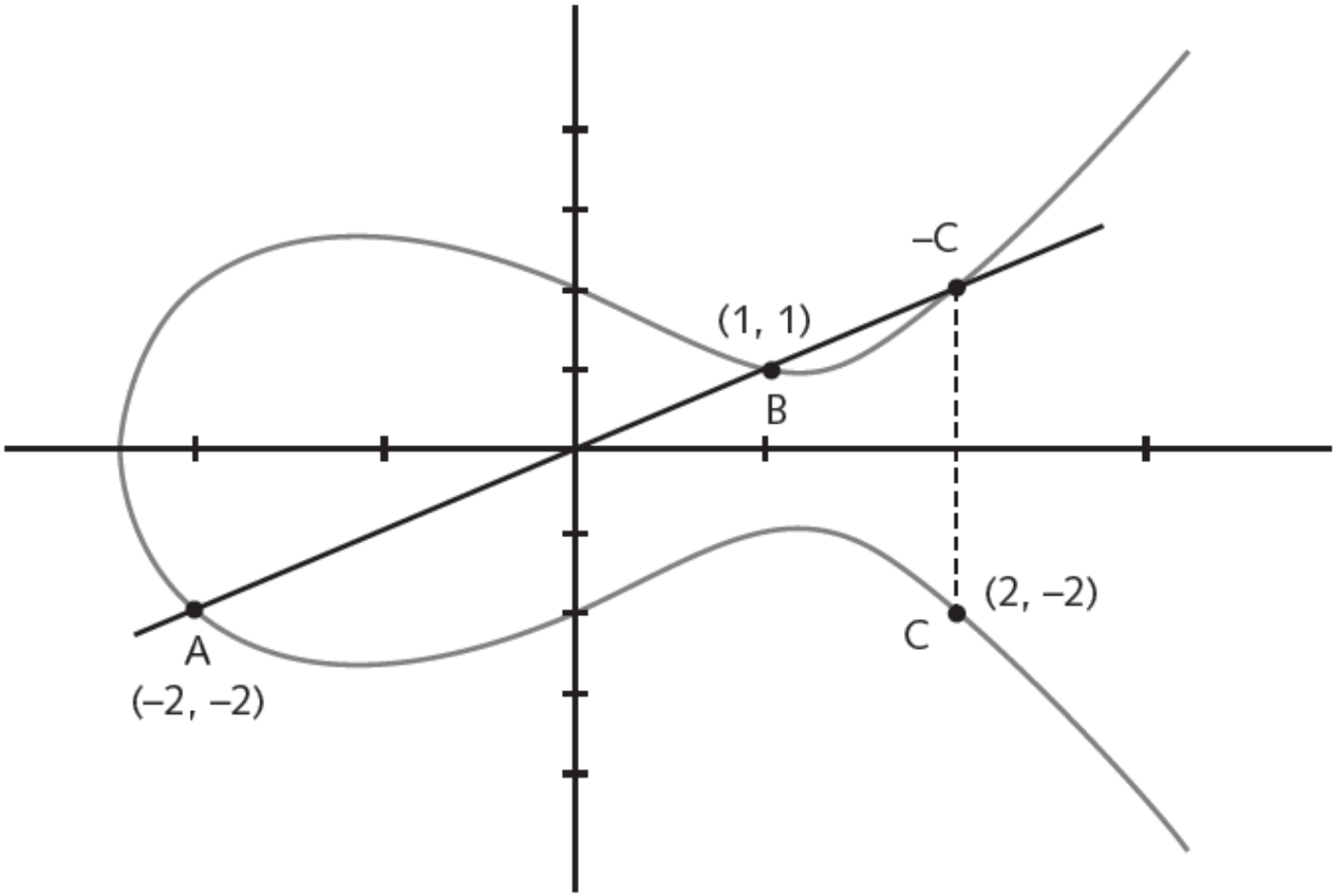

Figure 11-14 Elliptic curve cryptography (ECC)

Asymmetric Cryptographic Algorithms (cont'd.)

- Quantum cryptography
  - Exploits the properties of microscopic objects such as photons
  - Does not depend on difficult mathematical problems
- NTRUEncypt
  - Uses lattice-based cryptography
  - Relies on a set of points in space
  - Faster than RSA and ECC
  - More resistant to quantum computing attacks

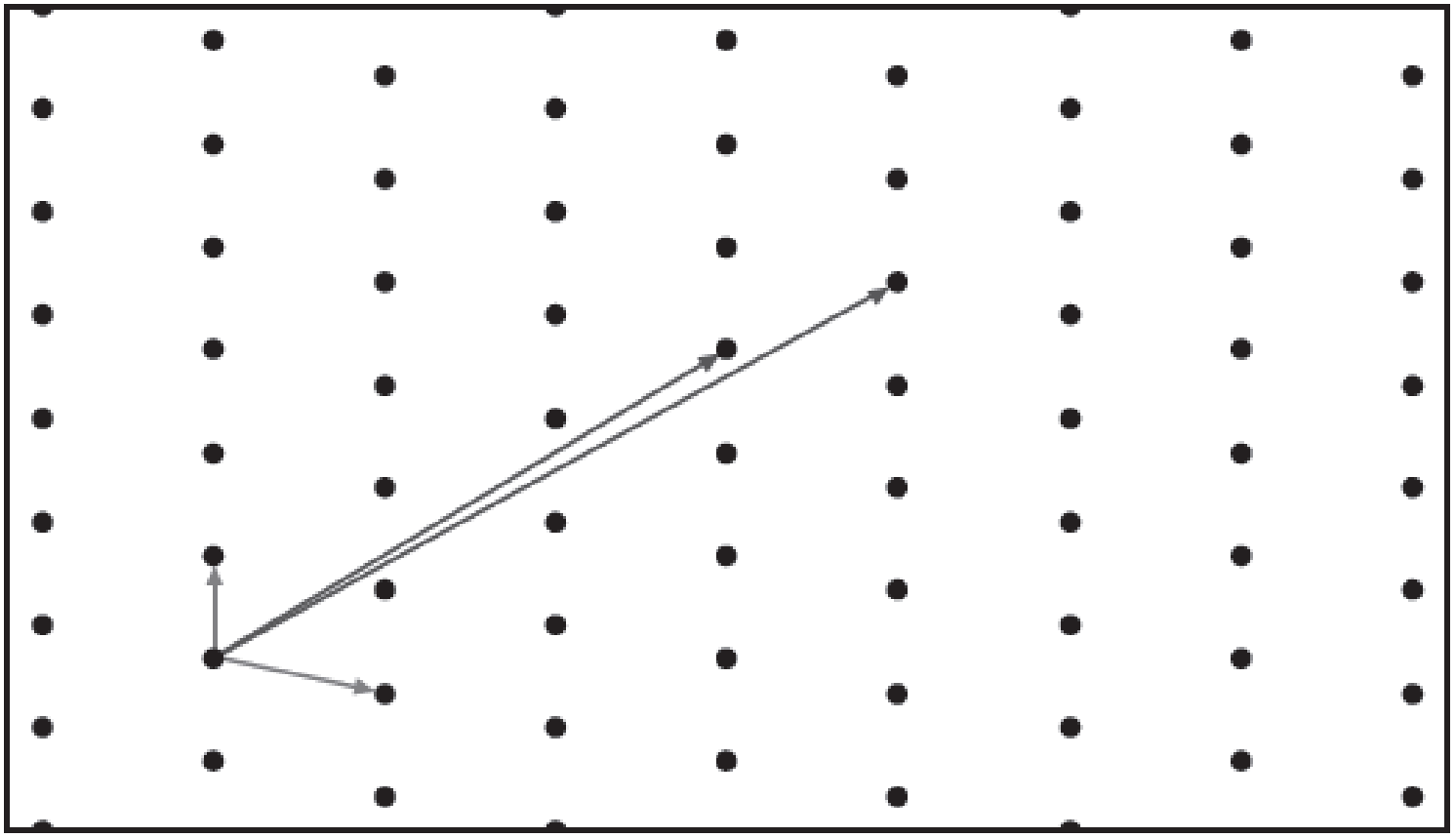

Figure 11-15 Lattice-based cryptography

Using Cryptography

- Cryptography
  - Should be used to secure data that needs to be protected
  - Can be applied through either software or hardware

Encryption Through Software

- File and file system cryptography
  - Encryption software can be applied to one or many files
- Protecting groups of files
  - Based on operating system's file system
- Pretty Good Privacy (PGP)
  - Widely used asymmetric cryptography system
  - Used for files and e-mails on Windows systems
- GNU Privacy Guard (GPG)
  - Runs on Windows, UNIX, and Linux

Encryption Through Software (cont'd.)

- PGP and GPG use both asymmetric and symmetric cryptography
- Microsoft Windows Encrypting File System (EFS)
  - Cryptography system for Windows
  - Uses NTFS file system
  - Tightly integrated with the file system
  - Encryption and decryption transparent to the user
  - Users can set encryption attribute for a file in the Advanced Attributes dialog box

Encryption Through Software (cont'd.)

- Whole disk encryption
  - Protects all data on a hard drive
  - Example: BitLocker drive encryption software

Hardware Encryption

- Software encryption can be subject to attacks to exploit its vulnerabilities
- Cryptography can be embedded in hardware
  - Provides higher degree of security
  - Can be applied to USB devices and standard hard drives
  - Trusted platform module
  - Hardware security model

Hardware Encryption (cont'd.)

- USB device encryption
- Encrypted hardware-based flash drives
  - Will not connect a computer until correct password has been provided
  - All data copied to the drive is automatically encrypted
  - Tamper-resistant external cases
  - Administrators can remotely control and track activity on the devices
  - Stolen drives can be remotely disabled

Hardware Encryption (cont'd.)

- Hard disk drive encryption
  - Self-encrypting hard disk drives protect all files stored on them
  - Drive and host device perform authentication process during initial power up
  - If authentication fails, drive can be configured to deny access or even delete encryption keys so all data is permanently unreadable

Hardware Encryption (cont'd.)

- Trusted Platform Module (TPM)
  - Chip on computer's motherboard that provides cryptographic services
  - Includes a true random number generator
  - Entirely done in hardware so cannot be subject to software attack
  - Prevents computer from booting if files or data have been altered
  - Prompts for password if hard drive moved to a new computer

Hardware Encryption (cont'd.)

- Hardware Security Module (HSM)
  - Secure cryptographic processor
  - Includes onboard key generator and key storage facility
  - Performs accelerated symmetric and asymmetric encryption
  - Can provide services to multiple devices over a LAN

Summary

- Cryptography is science of transforming information into a secure form while being transmitted or stored
- Hashing creates a unique digital fingerprint that represents contents of original material
  - Used only for comparison
- Symmetric cryptography uses a single key to encrypt and decrypt a message
  - Stream ciphers and block ciphers

Summary (cont'd.)

- Asymmetric cryptography
  - Public key cryptography
  - Uses two keys: public key and private key
  - Can be used to create a digital signature
- Cryptography can be applied through hardware or software
- Hardware encryption cannot be exploited like software cryptography