Information Security (CP3404)

Chapter 5 – Basic Cryptography

Based on the Fifth Edition of:

M. Ciampa:. *CompTIA® Security + Guide to Network Security Fundamentals*

Department of Information Technology, College of Business, Law & Governance

Learning Objectives

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

Outline

Preface

- Multilevel approach to information security using physical and technical security
- For high-value data that must be fully protected second level of protection also should be used: encryption
- If attackers penetrate the host and reach data, they still must uncover key to unlock encrypted contents: a virtually impossible task (if encryptions are properly applied)
- As more data taken off-premises it becomes increasingly important to use encryption

Defining Cryptography

Defining Cryptography

- Cryptography – Science of transforming information into secure form so that unauthorized persons cannot access it
- Steganography – Hides 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 (see Figure 5-1)

Defining Cryptography

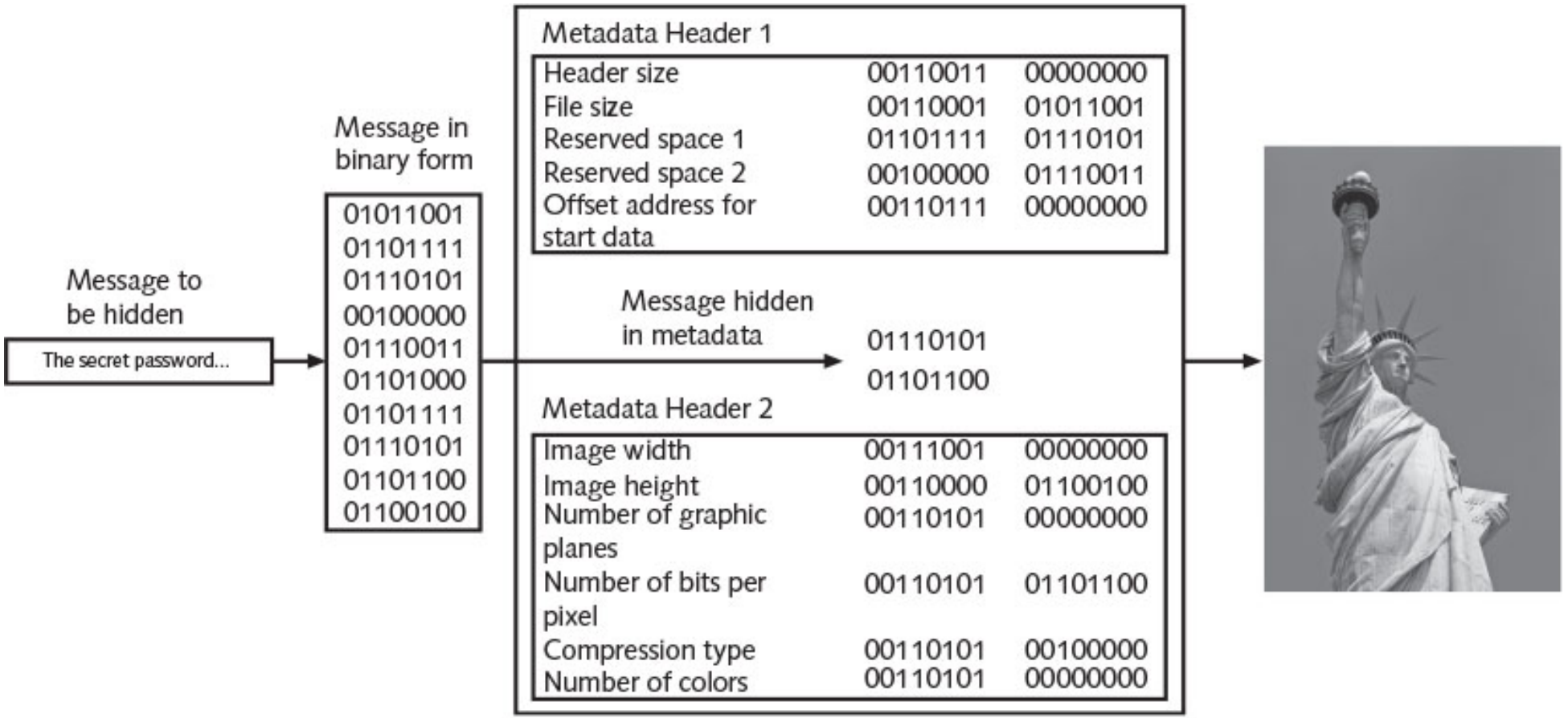

Figure 5-1 Data hidden by steganography

Photo: Chris Parypa Photography/Shutterstock.com

Defining Cryptography

Defining Cryptography (Cont.)

- Origins of cryptography dates back centuries to time of Julius Caesar
- Encryption – Changing original text into secret message using cryptography
- Decryption – Changing secret message back to original form
- Cleartext – Data in unencrypted form
- Plaintext – Cleartext data to be encrypted (and is result of decryption)

Defining Cryptography

Defining Cryptography (Cont.)

- Algorithm – Procedures based on mathematical formula used to encrypt and decrypt data
- Key – Mathematical value entered into cryptographic algorithm to produce encrypted data
- Ciphertext – Data that has been encrypted (see Figure 5-2)

Defining Cryptography

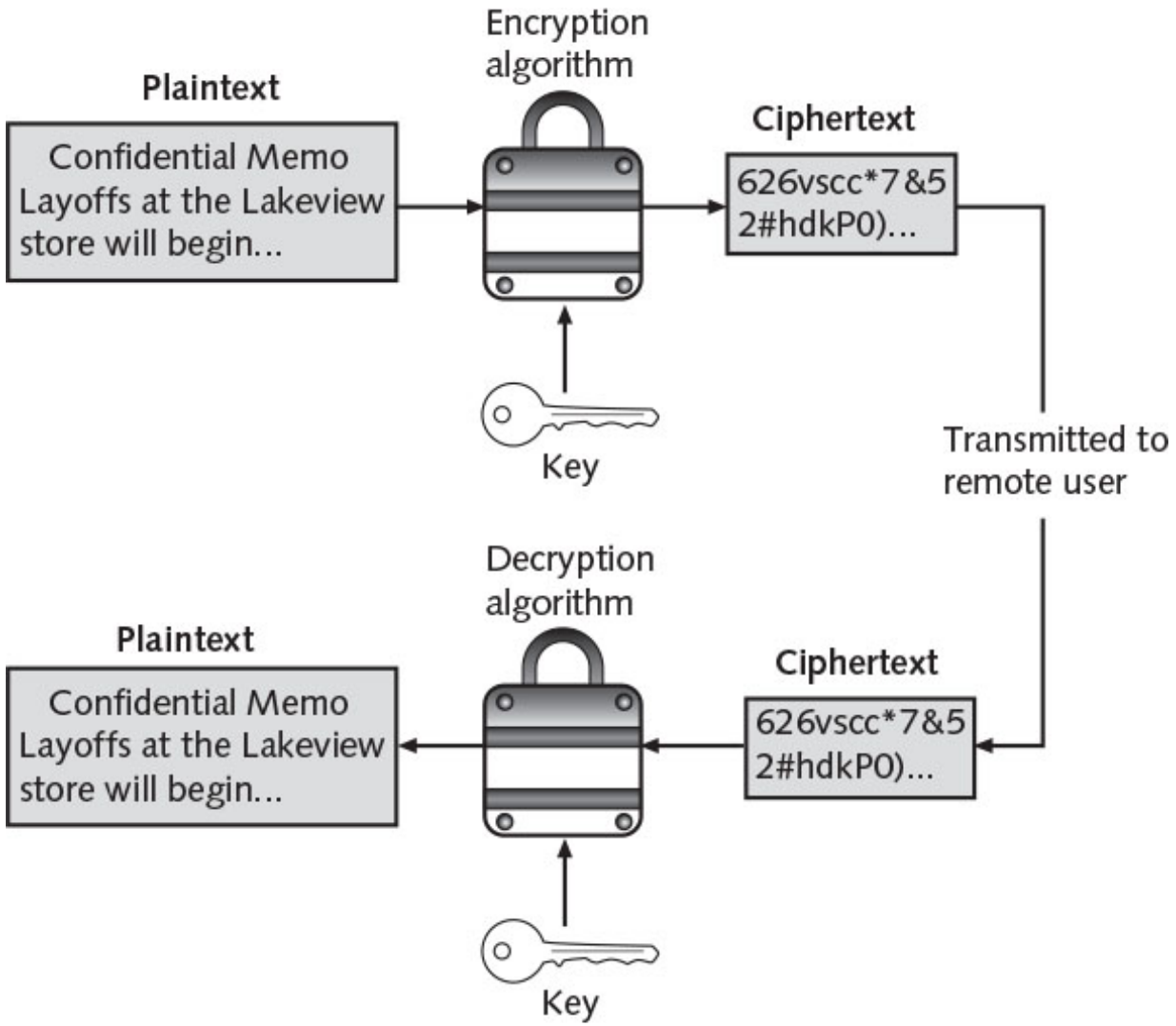

Figure 5-2 Cryptographic process

Defining Cryptography

Cryptography and Security

- Cryptography can provide five (5) basic information protections: (see Table 5-1)
  1. Confidentiality – Insures only authorized parties can view it
  2. Integrity – Insures information is correct and unaltered
  3. Availability – Authorized users can access it
  4. Authentication – Verify sender
  5. Nonrepudiation – Proves that a user performed an action

Defining Cryptography

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.
Authentication	Provides proof of the genuineness of the user	Proof that the sender was legitimate and not an imposter can be obtained.
Non-repudiation	Proves that a user performed an action	Individuals are prevented from fraudulently denying that they were involved in a transaction.

Table 5-1 Information protections by cryptography

Cryptographic Algorithms

Cryptographic Algorithms

- One of fundamental differences in cryptographic algorithms is amount of data that is processed at a time.
- Stream cipher – Takes one character and replaces it with one character (see Figure 5-3)
- The simplest type of stream cipher is a substitution cipher
- A monoalphabetic substitution cipher substitute one letter/character for another (see Figure 5-4)
- A homolaphabetic substitution cipher maps a single plaintext character to multiple ciphertext characters.

Cryptographic Algorithms

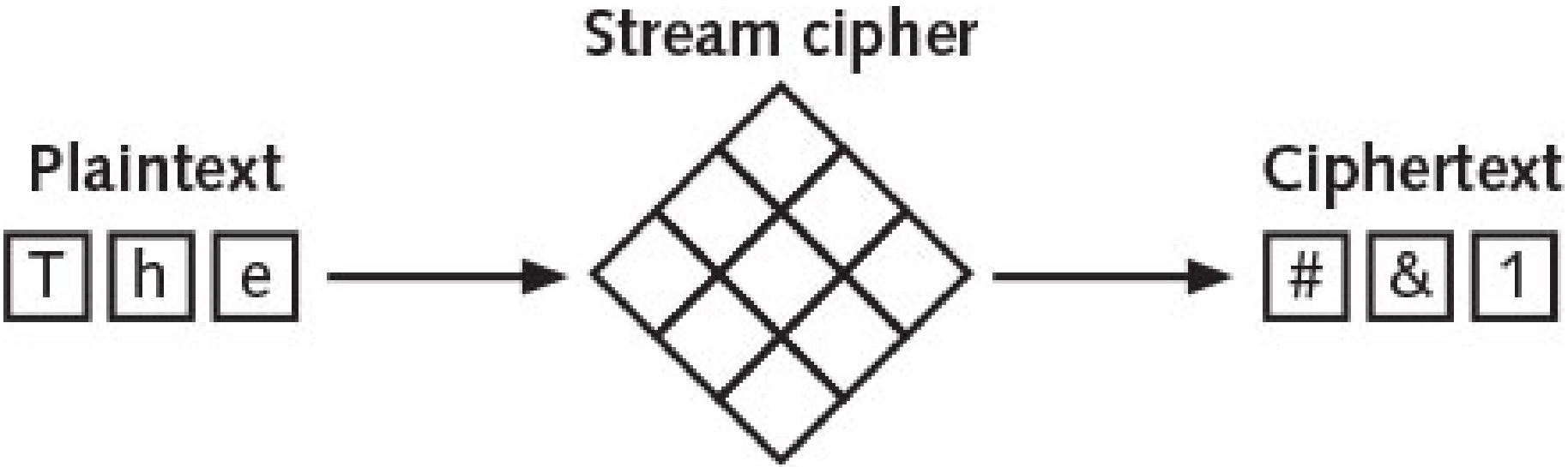

Figure 5-3 Stream cipher

Cryptographic Algorithms

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z — Plaintext letters
Z Y X W V U T S R Q P O N M L K J I H G F E D C B A — Substitution letters

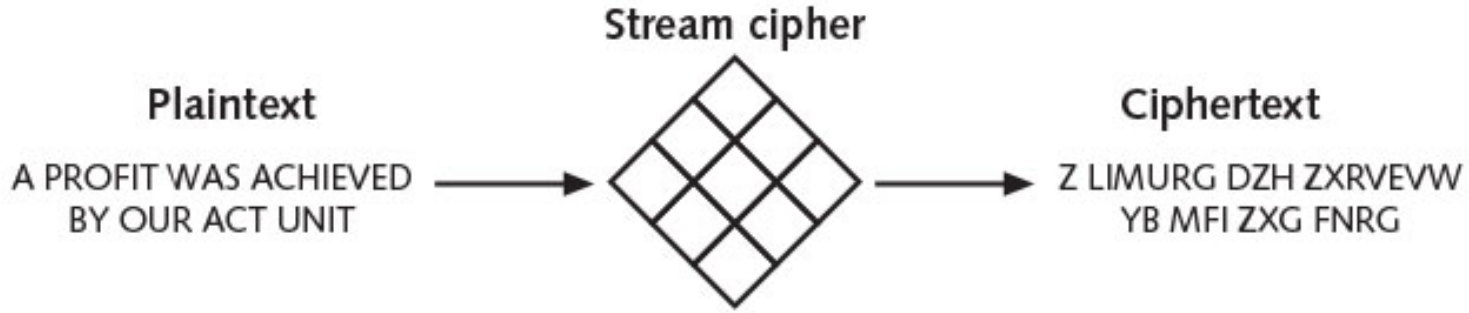

Figure 5-4 Substitution cipher

Cryptographic Algorithms

Cryptographic Algorithms

- Block cipher – Manipulates entire block of plaintext at one time
- After each block is processed, the cipher is reset to its original state –this results in the ciphertext being more difficult to break
- Sponge function – Takes as input a string of any length, and returns a string of any requested variable length
- This function repeatedly applies a process on the input that has been *padded* with additional characters until all characters are used (i.e., absorbed in the spong)

Cryptographic Algorithms

Cryptographic Algorithms

- There are three (3) broad categories of cryptographic algorithms:
  1. Hash algorithms
  2. Symmetric encryption algorithms
  3. Asymmetric encryption algorithms

Cryptographic Algorithms — Hashing

Hash Algorithms

- Hash – Algorithm that creates a unique digital fingerprint of data
- Process called hashing
- Fingerprint called digest (sometimes message digest or simply hash)
- Contents cannot be used to reveal original data set (one-way)
- Primarily used for comparison purposes

Cryptographic Algorithms — Hashing

Hash Algorithms – Secure Hash Algorithms

- 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 — Hashing

Hash Algorithms – Secure Hash Algorithms

- Hashing used to determine message integrity (digests often posted on download sites so user can verify file integrity after download) —see Figure 5-5
- 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

Cryptographic Algorithms — Hashing

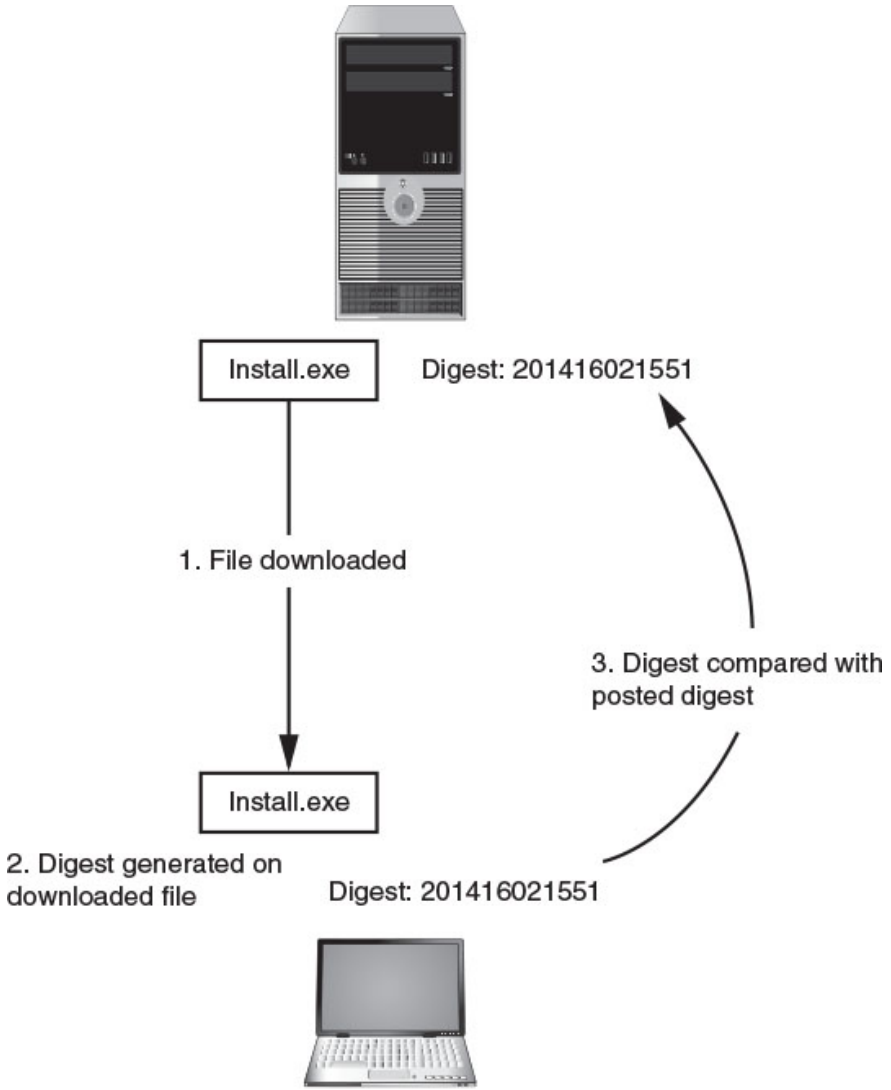

Figure 5-5 Verifying file integrity with digests

Cryptographic Algorithms — Hashing

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

Table 5-2 Information protections by hashing cryptography

Cryptographic Algorithms — Hashing

Hash Algorithms

- Most common hash algorithms:
  - Message Digest, i.e., MD family
  - Secure Hash Algorithm, i.e., SHA family
  - Whirlpool
  - RIPEMD

Cryptographic Algorithms — Hashing

Message Digest (MD)

- One of the most common one-way hash algorithms is the Message Digest (MD), which has three (3) versions:
  1. Message Digest 2 (MD2)
  2. Message Digest 4 (MD4)
  3. Message Digest 5 (MD5)

Cryptographic Algorithms — Hashing

Message Digest 2 (MD2)

- Was developed in 1989
- Divides the message into multiple 128-bit sections –extra padding may needed
- Was optimized to run on Intel-based microcomputers that processed 8 bits at a time
- No longer considered secure

Cryptographic Algorithms — Hashing

Message Digest 4 (MD4)

- Was developed in 1990 for computers that run 32 bits at a time
- Like MD2, MD4 creates a digest of 128 bits
- Message is padded to a length of 512 bits instead of 128 bits as with MD2
- Because of Flaw in the MD4, it was not widely accepted

Cryptographic Algorithms — Hashing

Message Digest 5 (MD5)

- Current MD version and a revision of MD4.
- Was developed in 1991 and designed to address MD4's weaknesses
- Like MD4 the length of a message is padded to 512 bits length
- Weaknesses in compression function could lead to collisions
- Some security experts recommend using a more secure hash algorithm

Cryptographic Algorithms — Hashing

Secure Hash Algorithm (SHA)

- Like MD, the SHA is a family of hashes
- SHA-0 – The first version, which due to a flaw was withdrawn shortly after it was first released
- SHA-1 – Developed in 1993 by the U.S. National Security Agency (NSA) and the National Institute of Standards and Technology (NIST)
- SHA-1 creates a digest of 160 bits instead of 128 bits
- SHA-2 – Currently considered to be secure and comprised of six (6) variations: SHA-224, SHA-256, SHA-384, SHA-512, SHA/512/224, and SHA-512/256 —the last number indicated the length in bits of the digest

Cryptographic Algorithms — Hashing

Secure Hash Algorithm (SHA)

- in 2007, an open competition for a new SHA-3 has algorithm was announced
- Of the 51 entries that were accepted to Round 1, only 14 were selected for Round 2 (one of the entries rejected was a new MD6)
- In late 2012, five finalists moved to Round 3
- In late 2012 the final winner of the competition was announced, Keccak (Pronounced cath-ack)
- SHA-3 uses a sponge function instead of stream or block ciphers

Cryptographic Algorithms — Hashing

Whirlpool

- A relatively recent cryptographic hash function that has received international recognition
- Adopted by standards organizations, including the International Organization for Standardization (ISO)
- Creates a digest of 512 bits
- Being implemented in several new commercial cryptography applications

Cryptographic Algorithms — Hashing

RACE Integrity Primitives Evaluation Message Digest (RIPEMD)

- Was developed by the Research and Development in Advanced Communications Technologies (RACE) —affiliated with the European Union (EU)
- Designed after MD4 and has three (3) variations: RIPEMD-128, RIPEMD-160, and RIPEMD-256
- Two different and parallel chains of computation
- Results are combined at end of process

Cryptographic Algorithms — Hashing

Hash	Digest
MD2	c4b4c4568a42895c68e5d507d7f0a6ca
MD4	9a5b5cec21dd77d611e04e10f902e283
MD5	0e41799d87f1179c1b8c38c318132236
RipeMD160	d4ec909f7b0f7dfb6fa45c4c91a92962649001ef
SHA-1	299b20adfec43b1e8fade03c0e0c61fc51b55420
SHA-256	133380e0ebfc19e91589c2feaa346d3e679a7529fa8d03617fcd661c997d7287
Whirlpool	1db4f64211028432d31ec9f0201244d59c11ff04dcf5c3dc97cc4cef700ad0c20d1943853202 20038ae9680da453f64d0062b09eabd8a157ebe147cd9233dd1d
SHA-3	c298d1ec129b04495f399cbc5c44b8023e213ebe27b78f689046a72e436e0e0 1d47302bbc8a857695594106d63571b95933a6 7b389802ceb2ef9b078297cfcc3

Table 5-3 Digests generated from one-time hash algorithms

Quick Quiz

1. _____ is the science of transforming information into an unintelligible form while it is being transmitted or stored so that unauthorized users cannot access it.
   (a) Hashing
   (b) Steganography
   (c) Message Authentication Code (MAC)
   (d) Cryptography

   Answer:

Quick Quiz

1. _____ is the science of transforming information into an unintelligible form while it is being transmitted or stored so that unauthorized users cannot access it.
   (a) Hashing
   (b) Steganography
   (c) Message Authentication Code (MAC)
   (d) Cryptography

   Answer: (d)

Quick Quiz

1. _____ is the science of transforming information into an unintelligible form while it is being transmitted or stored so that unauthorized users cannot access it.
   (a) Hashing
   (b) Steganography
   (c) Message Authentication Code (MAC)
   (d) Cryptography

   Answer: (d)

2. Whereas cryptography scrambles a message so that it cannot be viewed, _____ hides the existence of the data.

   Answer:

Quick Quiz

1. _____ is the science of transforming information into an unintelligible form while it is being transmitted or stored so that unauthorized users cannot access it.
   (a) Hashing
   (b) Steganography
   (c) Message Authentication Code (MAC)
   (d) Cryptography

   Answer: (d)

2. Whereas cryptography scrambles a message so that it cannot be viewed, _____ hides the existence of the data.

   Answer: steganography

Quick Quiz

1. _____ is the science of transforming information into an unintelligible form while it is being transmitted or stored so that unauthorized users cannot access it.
   (a) Hashing
   (b) Steganography
   (c) Message Authentication Code (MAC)
   (d) Cryptography

   Answer: (d)

2. Whereas cryptography scrambles a message so that it cannot be viewed, _____ hides the existence of the data.
   Answer: steganography

3. Changing the original text to a secret message using cryptography is known as _____.
   Answer:

Quick Quiz

1. _____ is the science of transforming information into an unintelligible form while it is being transmitted or stored so that unauthorized users cannot access it.
   (a) Hashing
   (b) Steganography
   (c) Message Authentication Code (MAC)
   (d) Cryptography

   Answer: (d)

2. Whereas cryptography scrambles a message so that it cannot be viewed, _____ hides the existence of the data.
   Answer: steganography

3. Changing the original text to a secret message using cryptography is known as _____.
   Answer: encryption

Quick Quiz

4. Select below the hashing algorithm that takes plaintext of any length and generates a digest 128 bits in length
   (a) RSA
   (b) SHA1
   (c) MD5
   (d) MD2

Answer:

Quick Quiz

4. Select below the hashing algorithm that takes plaintext of any length and generates a digest 128 bits in length
   (a) RSA
   (b) SHA1
   (c) MD5
   (d) MD2

   Answer: (d)

Quick Quiz

4. Select below the hashing algorithm that takes plaintext of any length and generates a digest 128 bits in length
   (a) RSA
   (b) SHA1
   (c) MD5
   (d) MD2

   Answer: (d)

5. A(n) _____ is a mathematical value entered into the algorithm to produce ciphertext, or text that is *scrambled*.

   Answer:

Quick Quiz

4. Select below the hashing algorithm that takes plaintext of any length and generates a digest 128 bits in length
   (a) RSA
   (b) SHA1
   (c) MD5
   (d) MD2

   Answer: (d)

5. A(n) _____ is a mathematical value entered into the algorithm to produce ciphertext, or text that is *scrambled*.
   Answer: key

Quick Quiz

4. Select below the hashing algorithm that takes plaintext of any length and generates a digest 128 bits in length
   (a) RSA
   (b) SHA1
   (c) MD5
   (d) MD2

   Answer: (d)

5. A(n) _____ is a mathematical value entered into the algorithm to produce ciphertext, or text that is *scrambled*.
   Answer: key

6. A(n) _____ takes as input a string of any length, and returns a string of fixed length.
   Answer:

Quick Quiz

4. Select below the hashing algorithm that takes plaintext of any length and generates a digest 128 bits in length
   (a) RSA
   (b) SHA1
   (c) MD5
   (d) MD2

   Answer: (d)

5. A(n) _____ is a mathematical value entered into the algorithm to produce ciphertext, or text that is *scrambled*.
   Answer: key

6. A(n) _____ takes as input a string of any length, and returns a string of fixed length.
   Answer: hashing algorithm

Cryptographic Algorithms — Symmetric Ciphers

Symmetric Cryptographic Algorithms

- Symmetric cryptographic algorithms – Uses same single key to encrypt and decrypt document
- Unlike hashing, symmetric algorithms are designed to encrypt and decrypt the ciphertext
- Data encrypted with a symmetric cryptographic algorithm will be decrypted when receiver has the key (see Figure 5-6)
- Essential that the key be kept private (confidential)
- Symmetric encryption is also called private key cryptography

Cryptographic Algorithms — Symmetric Ciphers

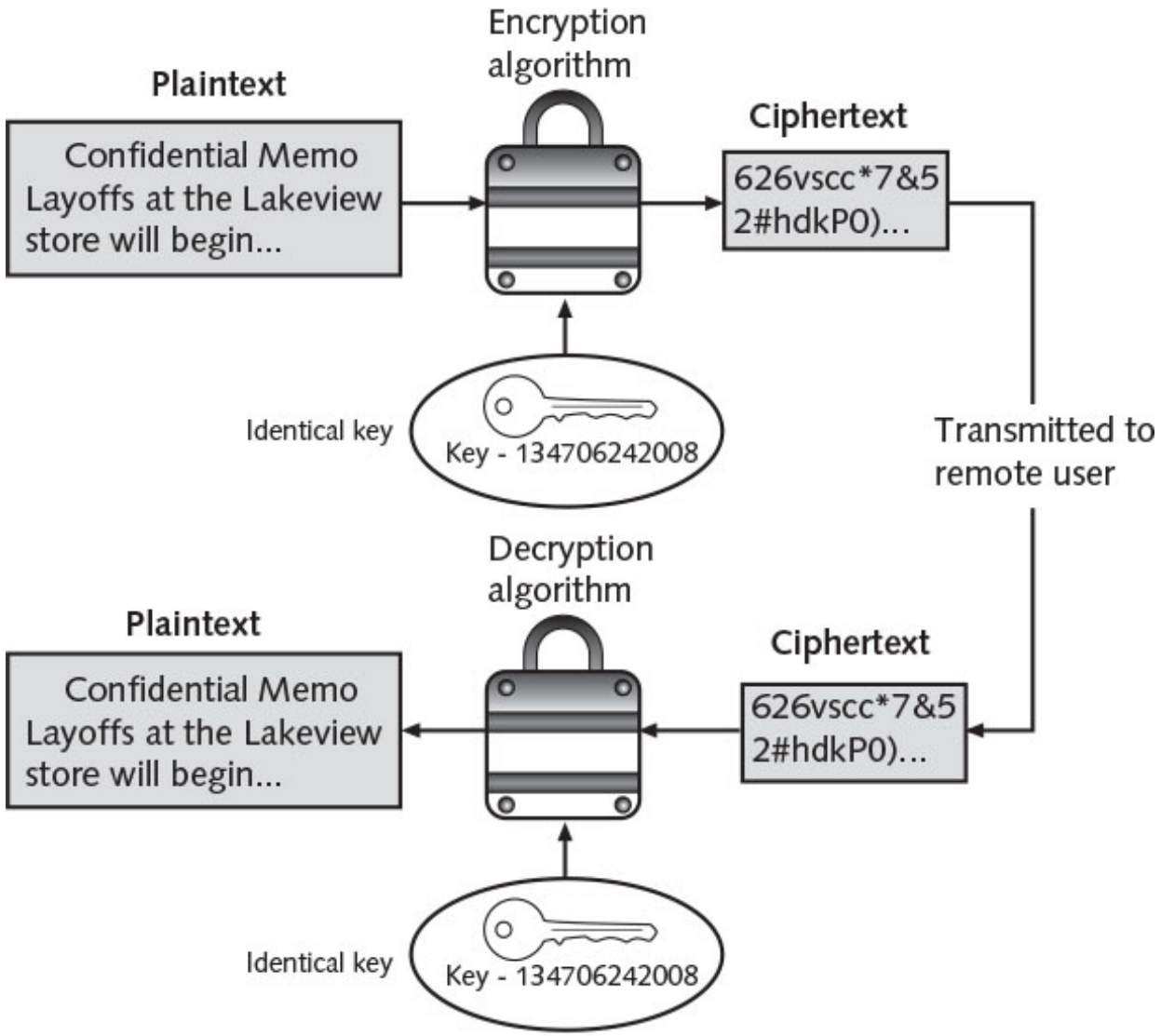

Figure 5-6 Symmetric (private key) cryptography

Cryptographic Algorithms — Symmetric Ciphers

Symmetric Cryptographic Algorithms

- Symmetric cryptography can provide strong protection against attacks as long as the key is kept secure (See Table 5-4)
- Common symmetric cryptographic algorithms include:
  - Data Encryption Standard (DES)
  - Triple Data Encryption Standard (3DES)
  - Advanced Encryption Standard (AES)

Cryptographic Algorithms — Symmetric Ciphers

Characteristic	Protection?
Confidentiality	Yes
Integrity	Yes
Availability	Yes
Authenticity	No
Non-repudiation	No

Table 5-4 Information protections by symmetric cryptography

Cryptographic Algorithms — Symmetric Ciphers

Data Encryption Standard (DES)

- First widely popular symmetric cryptography algorithms
- Predecessor of DES was a product originally designed in the early 1970s by IBM called Lucifer that had key length 128 bits
- Key was later shortened to 56 bits and renamed DES
- The U.S. government officially adopted DES as the standard for encryption non-classified information
- DES is a block cipher that divides plaintext into 64-bit block sand then executes the algorithm 16 times
- Because of short 56-bit key, DES is no longer considered secure

Cryptographic Algorithms — Symmetric Ciphers

Triple Data Encryption Standard (3DES)

- Designed to replace DES
- 3DES uses three rounds of encryption instead of just one (i.e., three iterations times 16 rounds)
- Most secure versions of 3DES use different keys for each round (see Figure 5-7)
- Performs better in hardware than as software
- It is no longer considered the most secure symmetric cryptographic algorithm

Cryptographic Algorithms — Symmetric Ciphers

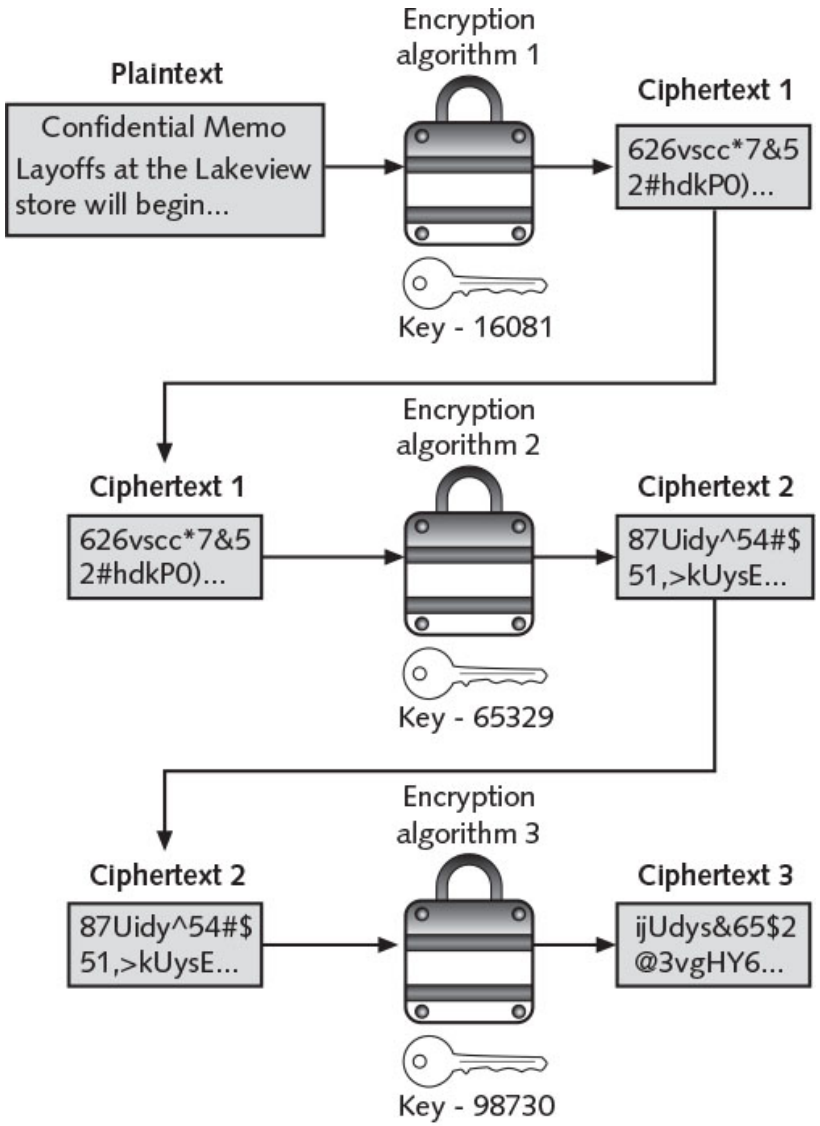

Figure 5-7 3DES

Cryptographic Algorithms — Symmetric Ciphers

Advanced Encryption Standard (AES)

- In 1997, the National Institute of Standard and Technology (NIST), issued a call for candidates to replace DES.
- The requirements was that the system should allow variable key sizes of 128, 192, and 256 bits; should work on different hardwares (e.g., 8-bit, 16-bit, and 32-bit processors); should be fast, and secure.
- In 1998, 15 cryptographic systems have been submitted as the candidates for the new Advanced Encryption Standard (AES).
- Five finalists of AES were: MARS, RC6, Rijndael, Serpent, and Twofish.

Cryptographic Algorithms — Symmetric Ciphers

Advanced Encryption Standard (AES) —Cont.

- The Rijndael cipher, which was designed by researchers from Belgium, competes in the AES race. The cipher works for three block sizes: 128, 192, and 256 bits.
- Rijndael (more often referred to as AES) consists of 9, 11, and 13 rounds, when the key has 128, 192, and 256 bits, respectively.
- To date, no attacks have been successful against AES

Cryptographic Algorithms — Symmetric Ciphers

Other Symmetric Algorithms — RC family

- Rivest Cipher (RC) is a family of cipher algorithms designed by Ron Rivest (one of the designers of RSA)
- RC has six (6) variations, ranging from RC1 to RC6 (Rivest did not release RC1 and RC3)
- RC2 is a block cipher that processes blocks of 64 bits
- RC4 is a stream cipher, accept keys up to 128 bits in length
- RC5 is a block cipher, accept blocks/keys of different lengths
- RC6 has three key sizes (128, 192, and 256 bits) and performs 20 rounds on each block

Cryptographic Algorithms — Symmetric Ciphers

Other Symmetric Algorithms — IDEA

- International Data Encryption Standard (IDEA) dates back to the early 1990s and is used in European nations
- IDEA is a block cipher that processes 64 bits with a 128-bit key with 8 rounds
- IDEA is generally considered to be secure

Cryptographic Algorithms — Symmetric Ciphers

Other Symmetric Algorithms — Blowfish

- A block cipher algorithm that operates on 64-bit blocks and can have a key length from 32 to 448 bits
- Blowfish was designed to run efficiently on 32-bit computers
- To date, no significant weaknesses have been identified
- A later derivation of blowfish knows as Twofish is also considered to be a strong algorithm —not uses as widely as Blowfish

Cryptographic Algorithms — Symmetric Ciphers

Other Symmetric Algorithms — One-Time Pad (OTP)

- One-time pad (OTP) – Combines plaintext with random key/pad of the same size of plaintext
- The pad should be used only one time and then destroyed
- OTP is the only known method to perform encryption that cannot be broken mathematically
- Does not require the use of computer —Table 5-5 illustrates encryption of the plaintext "SECRET" using the pad "CYBFEA"

Cryptographic Algorithms — Symmetric Ciphers

Plaintext	Position in alphabet	Pad	Position in alphabet	Calculation	Result
S	19	C	3	19+3−1=21	U
E	5	B	2	5+2−1=6	F
C	3	Y	25	3+25−1=1	A
R	18	F	6	18+6−1=23	W
E	5	E	5	5+5−1=9	I
T	20	A	1	20+1−1=20	T

Table 5-5 OTP

Cryptographic Algorithms — Asymmetric Ciphers

Asymmetric Cryptographic Algorithms

- The primary weakness of a symmetric encryption algorithm is: *distributing and maintaining a secure single key among multiple users, who are often scattered geographically*
- Asymmetric cryptographic algorithms (a.k.a. public key cryptography) – Developed by Whitfield Diffie and Martin Hellman of the MIT in 1975
- Uses two keys instead of only one (see Figure 5-8)
- Keys are mathematically related:
  - Public key – Known to everyone and can be freely distributed
  - Private key – Known only to the individual to whom it belongs

Cryptographic Algorithms — Asymmetric Ciphers

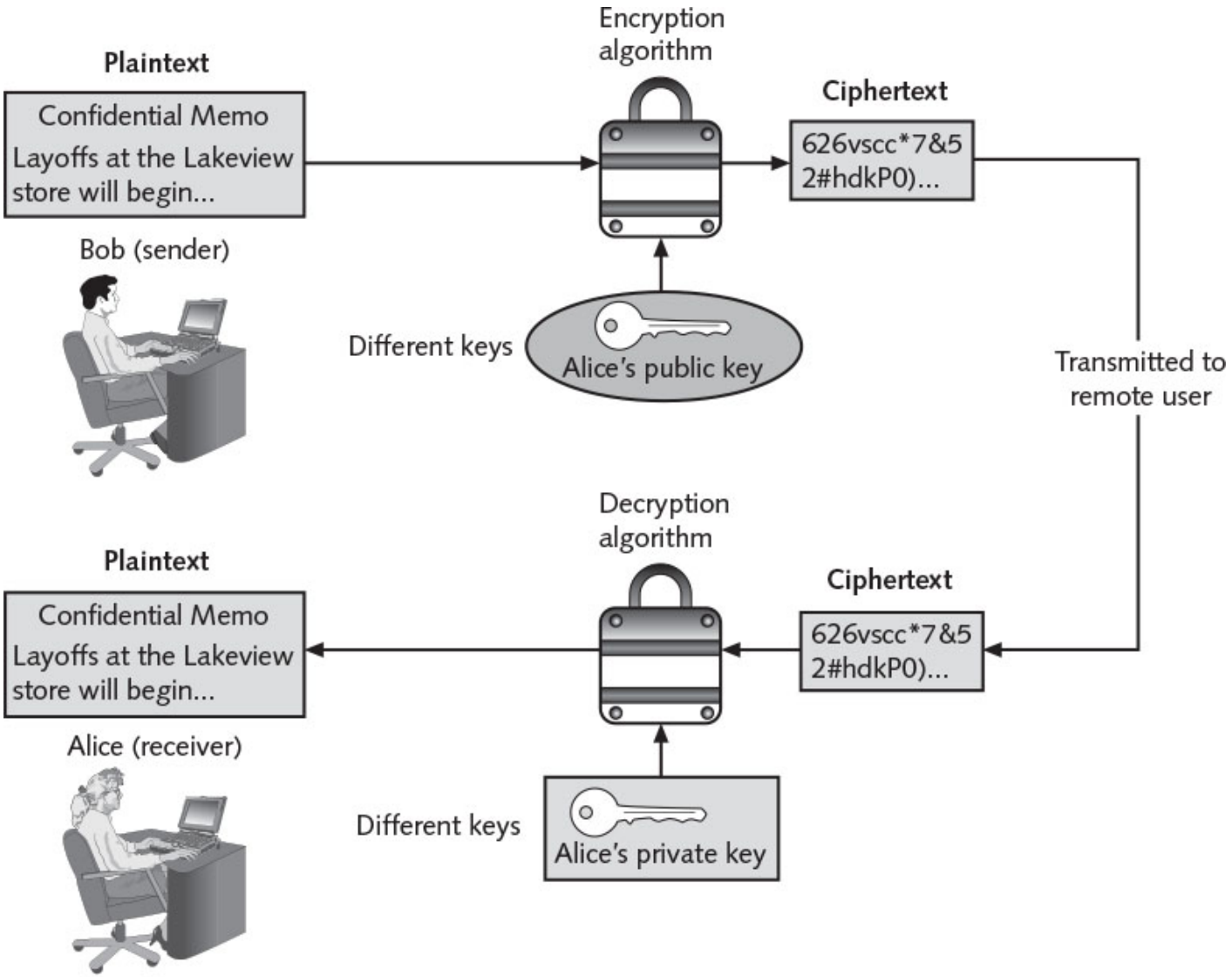

Figure 5-8 Asymmetric (public key) cryptography

Cryptographic Algorithms — Asymmetric Ciphers

Digital Signature

- The basic for a digital signature rests on the ability of asymmetric keys to work in both directions (see Figure 5-9)
- A digital signature can:
  - Verify the sender – Confirm the identity of the person from whom the electronic message originated
  - Nonrepudiation – The sender cannot later attempt to disown it by claiming the signature was forged
  - Integrity of message – Prove that the message has not been altered since it was signed

Cryptographic Algorithms — Asymmetric Ciphers

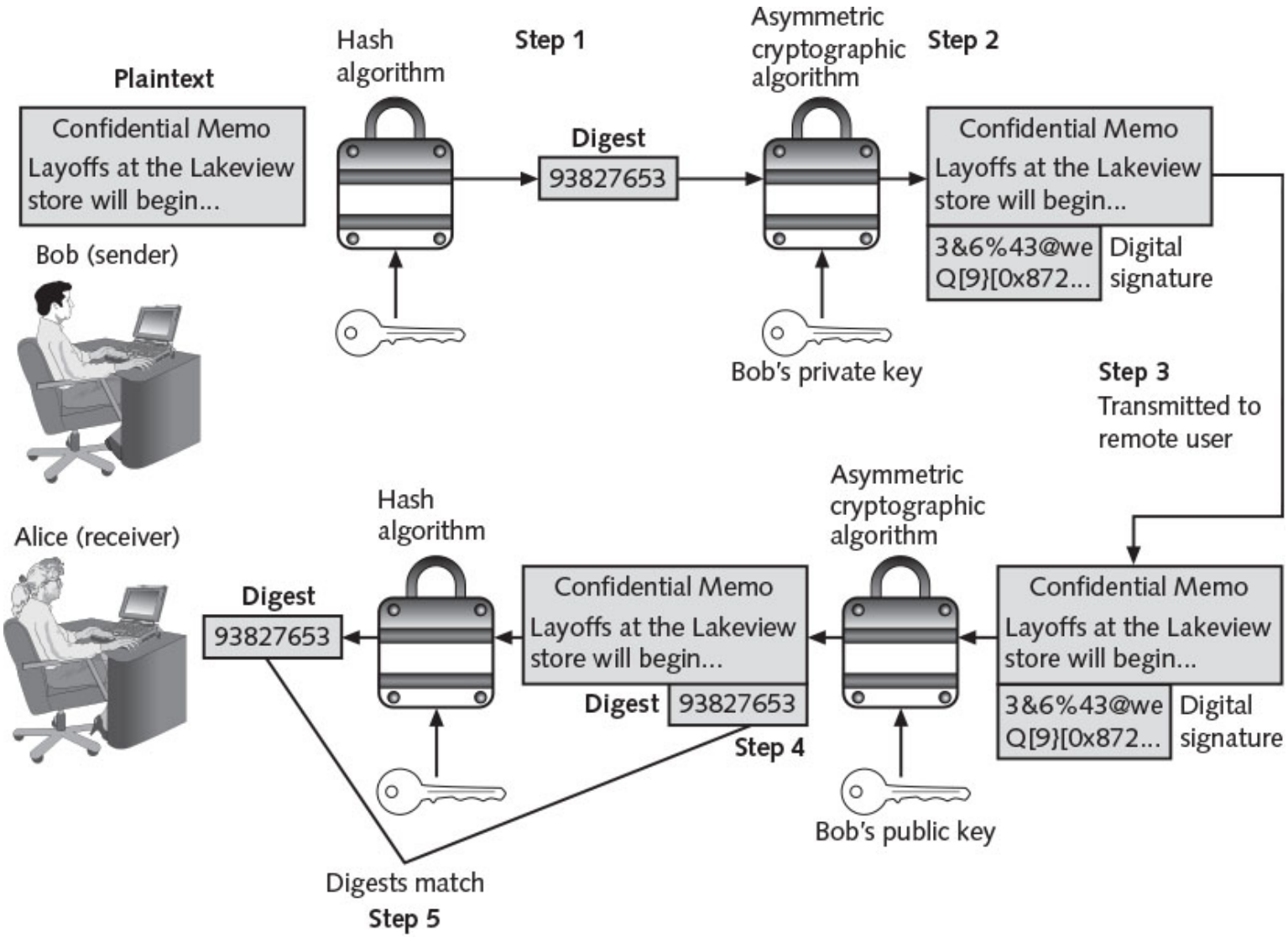

Figure 5-9 Digital signature

Cryptographic Algorithms — Asymmetric Ciphers

Digital Signature

- Simply signing the message does not provide confidentiality of the message (it only provides integrity)
- If the sender/signer wishes to hide the message as well, in addition to using his secret key for signing, he must encrypt the message using the recipient's publick key (see Table 5-6)
- Asymmetric cryptography can provide strong protections (see Table 5-7)

Cryptographic Algorithms — Asymmetric Ciphers

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, and not the sender's, key is used.
Alice wants to read an encrypted message sent by Bob	Alice's key	Private key	An encrypted message can be read only 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 be read only by the recipient's private key. Bob would need to encrypt it with his 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 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 5-6 Asymmetric cryptography practices

Cryptographic Algorithms — Asymmetric Ciphers

Characteristic	Protection?
Confidentiality	Yes
Integrity	Yes
Availability	Yes
Authenticity	Yes
Non-repudiation	Yes

Table 5-7 Information protections by asymmetric cryptography

Cryptographic Algorithms — Asymmetric Ciphers

The RSA Algorithm

- Was first published by Rivest, Shamir and Adleman in 1977 and patented by MIT in 1983.

Cryptographic Algorithms — Asymmetric Ciphers

The RSA Algorithm

- Was first published by Rivest, Shamir and Adleman in 1977 and patented by MIT in 1983.
- The RSA system is set up by the receiver who;
  - chooses two large and distinct primes p and q
  - computes $n = p \times q$ and $\phi(n) = (p-1)(q-1)$
  - selects at random the key $0 \leq e \leq \phi(n)$, such that $\gcd(e,\ \phi(n)) = 1$
  - computes the secret key d, such that $e \times d \equiv 1 \pmod{\phi(n)}$,
  - publishes n, e in a public directory as the public parameters of his RSA system, and keeps p, q, d secret.

Cryptographic Algorithms — Asymmetric Ciphers

The RSA Algorithm

- Messages and cryptograms belong to the set $\{0, 1, \ldots, n-1\}$, where $n = p \times q$ (for large primes p, q)
- Let e and d be the encryption/public and decryption/private keys, respectively
- For a message $0 \leq M < n$:

Cryptographic Algorithms — Asymmetric Ciphers

The RSA Algorithm

- Messages and cryptograms belong to the set $\{0, 1, \ldots, n-1\}$, where $n = p \times q$ (for large primes p, q)
- Let e and d be the encryption/public and decryption/private keys, respectively
- For a message $0 \leq M < n$:

Encryption:

$$C = E_e(M) = M^e \pmod{n}.$$

Decryption:

$$M = D_d(C) = C^d \pmod{n}.$$

Cryptographic Algorithms — Asymmetric Ciphers

Example

Bob chooses $p = 885320963$, $q = 238855417$, and computes,

$$n = p \times q = 211463707796206571.$$

Cryptographic Algorithms — Asymmetric Ciphers

Example

Bob chooses $p = 885320963$, $q = 238855417$, and computes,

$$n = p \times q = 211463707796206571.$$

Bob chooses $e = 9007$, and computes:

$$d = 1/e = 1/9007 = 116402471153538991 \pmod{\phi(n)},$$

Bob publishes e, n as public parameters of his RSA system.

Alice, who wishes to send a message $M = 30120$ to Bob, computes

$$C = M^e = 30120^{9007} = 1135358599035722866 \pmod{n}.$$

Bob uses the decryption key d, and retrieves the message:

$$C^d = 1135358599035722866^{116402471153538991} \equiv 30120 \pmod{n}.$$

Cryptographic Algorithms — Asymmetric Ciphers

Elliptic Curve Cryptography (ECC)

- Elliptic curve cryptography (ECC) — Users share one elliptic curve and one point on curve (see Figure 5-10)
- Considered as an alternative for prime-number-based asymmetric cryptography for mobile and wireless devices
- Because mobile devices are limited in terms of computing power due to their smaller size, ECC offers security that is comparable to other asymmetric cryptography but with smaller key sizes
- Can result in faster computations and lower power consumption

Cryptographic Algorithms — Asymmetric Ciphers

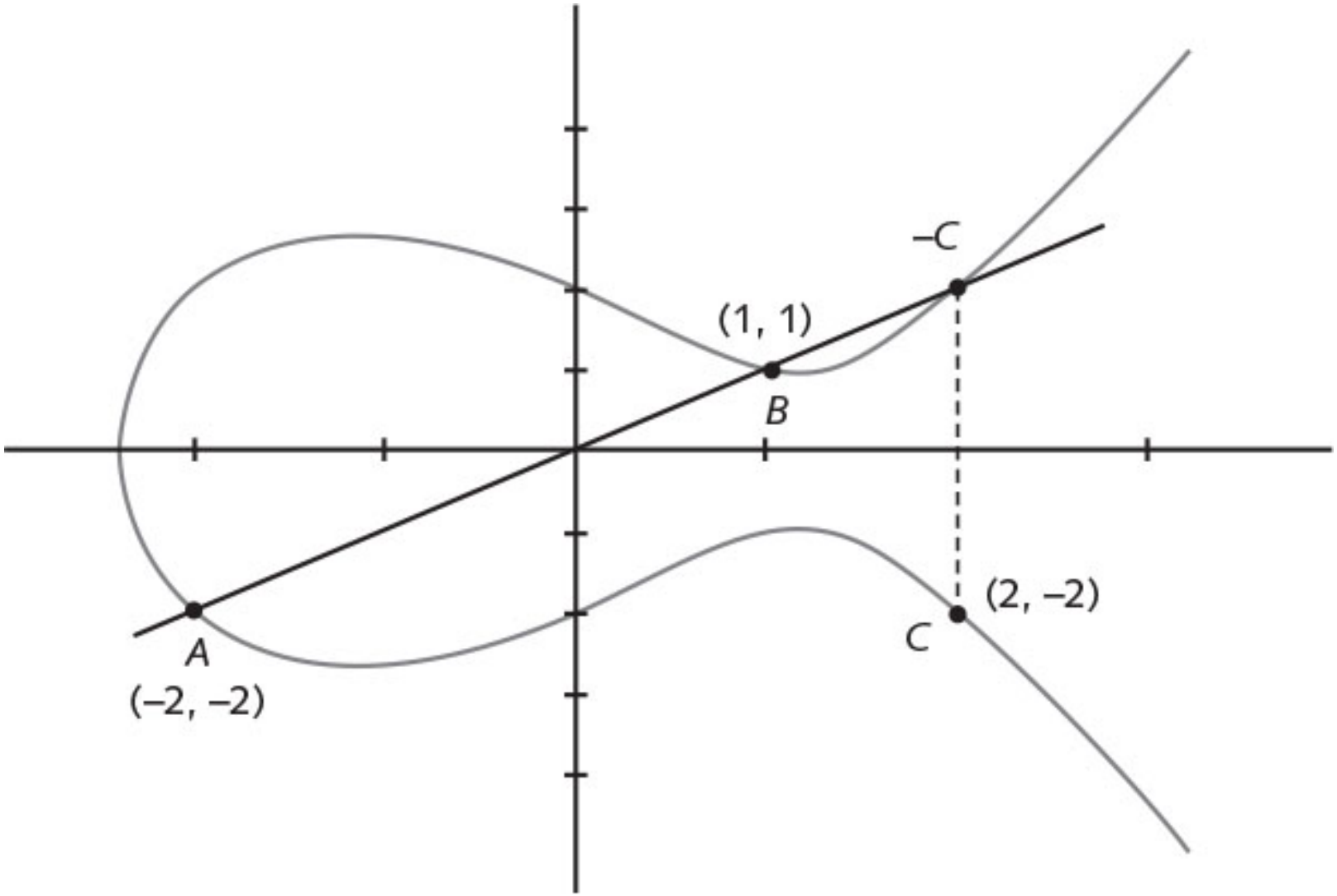

Figure 5-10 Elliptic curve cryptography (ECC)

Cryptographic Algorithms — Asymmetric Ciphers

NTRUEncrypt

- A relatively new asymmetric cryptographic algorithm
- Uses a different foundation than RSA ans ECC
- Uses lattice-based cryptography
- Relies on a set of points in space
- Faster than RSA and ECC
- More resistant to quantum computing attacks

Cryptographic Algorithms — Asymmetric Ciphers

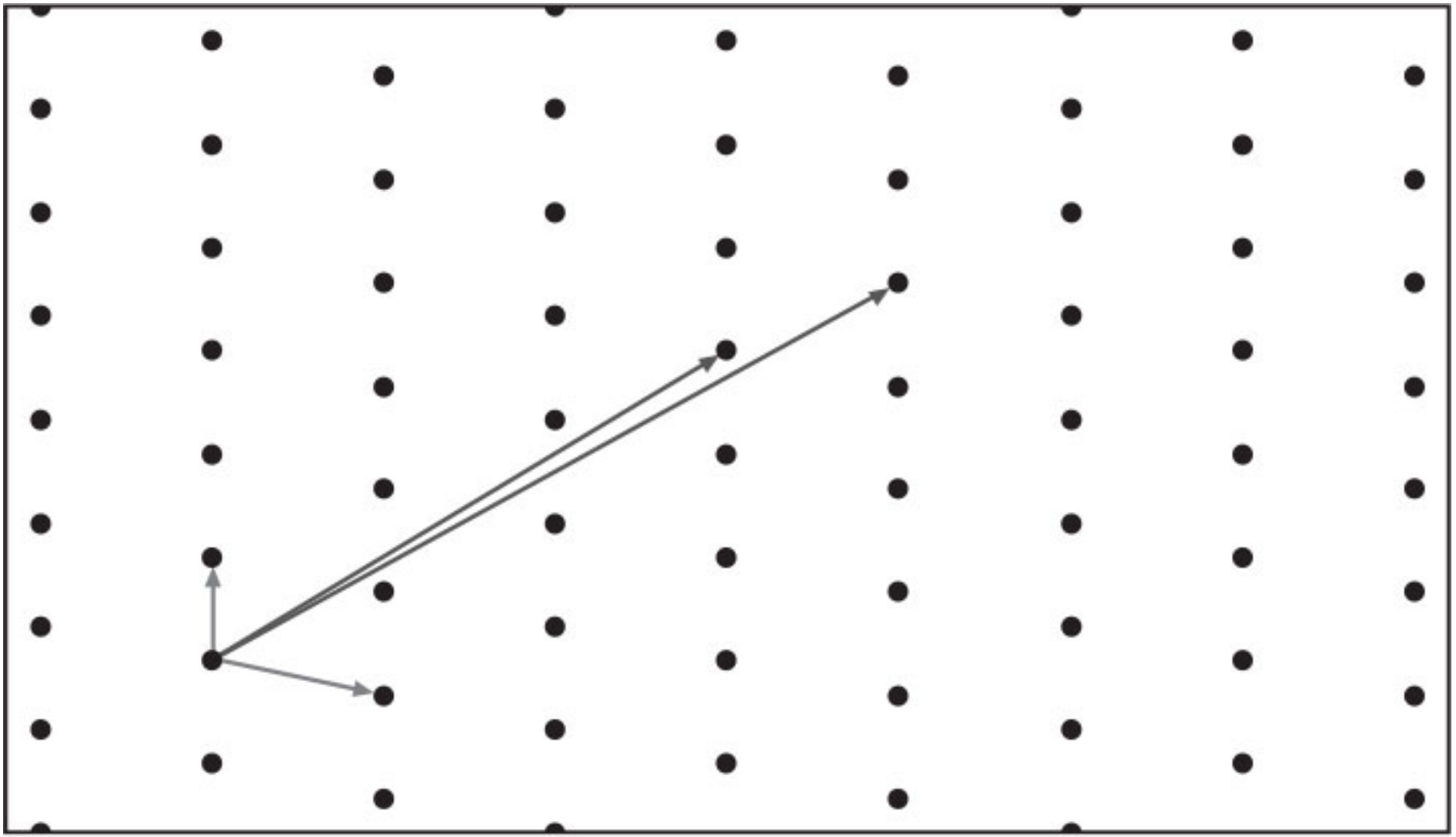

Figure 5-11 Lattice-based cryptography

Cryptographic Algorithms — Asymmetric Ciphers

Quantum Cryptography

- Exploits properties of microscopic objects such as photons
- Does not depend on difficult mathematical problems
- If quantum cryptography is found to be commercially feasible, it may hold the potential for introducing an entirely new type of cryptography

Cryptographic Algorithms — Asymmetric Ciphers

Key Exchange

- Key exchange – Problem of sending and receiving keys
- Out-of-band – Make the exchange outside of normal communication channels
- In-band – Key exchange that occurs within normal communications channel

Cryptographic Algorithms — Asymmetric Ciphers

In-Band Key Exchange — DH and DHE

- Diffie-Hellman (DH) – Requires Alice and Bob to each agree upon a large prime number and related integer; two numbers can be made public, yet Alice and Bob, through mathematical computations and exchanges of intermediate values, can separately create the same key
- Diffie-Hellman Ephemeral (DHE) – Uses different keys (Ephemeral keys are temporary keys that are used only once and then discarded)

Cryptographic Algorithms — Asymmetric Ciphers

In-Band Key Exchange — ECDH and Perfect Forward Security

- Elliptic Curve DiffieHellman (ECDH) – Uses elliptic curve cryptography instead of prime numbers in its computation
- Perfect Forward Secrecy – Public key systems that generate random public keys that are different for each session; value of perfect forward secrecy is that if the secret key is compromised, it cannot reveal the contents of more than one message

Using Cryptography

Using Cryptography

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

Using Cryptography

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 for files and e-mails on Windows systems
- GNU Privacy Guard (GPG) – An open-source product similar to PGP; runs on Windows, UNIX, and Linux
- PGP and GPG use both asymmetric and symmetric cryptography

Using Cryptography — Software Encryption

Microsoft Windows Encryption File System (EFS)

- Cryptography system for Windows OS
- 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

Using Cryptography — Software Encryption

Whole Disk Encryption

- Cryptography can be applied to entire disks
- Protects all data on a hard drive
- One example of whole disk encryption software is that included in Microsoft Windows knows as BitLocker drive encryption software

Using Cryptography

Hardware Encryption

- Software encryption can be subject to attacks to exploit its vulnerabilities
- Cryptography can be embedded in hardware to provide higher degree of security
- Can be applied to USB devices and standard hard drives
- More sophisticated hardware encryption options include the trusted platform module and the hardware security model

Using Cryptography — Hardware Encryption

USB Device Encryption

- 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

Using Cryptography — Hardware Encryption

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

Using Cryptography — Hardware Encryption

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

Using Cryptography — Hardware Encryption

Hardware Security Module (HSM)

- Secure cryptographic processor
- Includes on-board key generator and key storage facility
- Performs accelerated symmetric and asymmetric encryption
- Can provide services to multiple devices over a LAN

Quick Quiz

1. _____ cryptographic algorithms use the same single key to encrypt and decrypt a message.
   Answer:

Quick Quiz

1. _____ cryptographic algorithms use the same single key to encrypt and decrypt a message.
   Answer: Symmetric

Quick Quiz

1. _____ cryptographic algorithms use the same single key to encrypt and decrypt a message.
   Answer: Symmetric

2. The _____ was approved by the NIST in late 2000 as a replacement for DES.
   Answer:

Quick Quiz

1. _____ cryptographic algorithms use the same single key to encrypt and decrypt a message.
   Answer: Symmetric

2. The _____ was approved by the NIST in late 2000 as a replacement for DES.
   Answer: Advanced Encryption Standard (AES)

Quick Quiz

1. _____ cryptographic algorithms use the same single key to encrypt and decrypt a message.
   Answer: Symmetric

2. The _____ was approved by the NIST in late 2000 as a replacement for DES.
   Answer: Advanced Encryption Standard (AES)

3. In cryptography, which of the following basic protections ensures that the information is correct and no unauthorized person or malicious software has altered that data?
   (a) Confidentiality
   (b) Availability
   (c) Encryption
   (d) Integrity

   Answer:

Quick Quiz

1. _____ cryptographic algorithms use the same single key to encrypt and decrypt a message.
   Answer: Symmetric

2. The _____ was approved by the NIST in late 2000 as a replacement for DES.
   Answer: Advanced Encryption Standard (AES)

3. In cryptography, which of the following basic protections ensures that the information is correct and no unauthorized person or malicious software has altered that data?
   (a) Confidentiality
   (b) Availability
   (c) Encryption
   (d) Integrity

   Answer: (d)

Quick Quiz

4. Asymmetric cryptographic algorithms is also known as _____ cryptography.
   Answer:

Quick Quiz

4. Asymmetric cryptographic algorithms is also known as _____ cryptography.
   Answer: public key

Quick Quiz

4. Asymmetric cryptographic algorithms is also known as _____ cryptography.
   Answer: public key

5. Cryptography can also be applied to entire disks. This is known as _____.
   Answer:

Quick Quiz

4. Asymmetric cryptographic algorithms is also known as _____ cryptography.
   Answer: public key

5. Cryptography can also be applied to entire disks. This is known as _____.
   Answer: whole disk encryption

Quick Quiz

4. Asymmetric cryptographic algorithms is also known as _____ cryptography.
   Answer: public key

5. Cryptography can also be applied to entire disks. This is known as _____.
   Answer: whole disk encryption

6. _____ is essentially a chip on the motherboard of the computer that provides cryptographic services.
   Answer:

Quick Quiz

4. Asymmetric cryptographic algorithms is also known as _____ cryptography.
   Answer: public key

5. Cryptography can also be applied to entire disks. This is known as _____.
   Answer: whole disk encryption

6. _____ is essentially a chip on the motherboard of the computer that provides cryptographic services.
   Answer: Trusted Platform Module (TPM)