



The image shows the cover of the book "CompTIA Security+ Guide to Network Security Fundamentals, Seventh Edition" by Mark Ciampa. The cover is white with a blue header and a yellow and orange abstract pattern at the bottom. The Cengage logo is in the top left corner.




A cluster of icons representing network security, including a cloud with a lock, a server, and a network diagram.

Module 6: Basic Cryptography



Module Objectives



- By the end of this module, you should be able to:
 - Define cryptography
 - Describe hash, symmetric, and asymmetric cryptographic algorithms
 - Explain different cryptographic attacks
 - List the various ways in which cryptography is used

2

What is Cryptography?

■ Cryptography

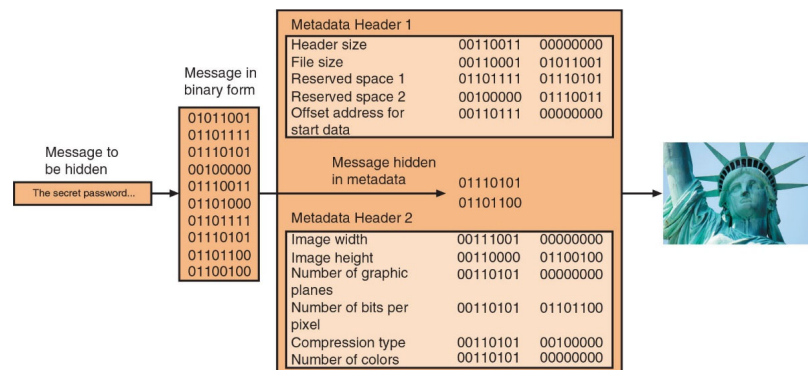
- Scrambling information so it cannot be read
- Transforms information into secure form so unauthorized persons cannot access it

■ Steganography

- Hides the existence of data
- An image, audio, or video file can contain hidden messages embedded in the file
- Achieved by dividing data and hiding in unused portions of the file
- May hide data in the file header fields that describe the file, between sections of the *metadata* (data used to describe the content or structure of the actual data)

3

What is Cryptography?



Source: Chris Panypa Photography/Shutterstock.com

Figure 6-1 Data hidden by steganography

- Figure 6-1 Data hidden by steganography

4

What is Cryptography?

- **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
- **Plaintext**
 - Unencrypted data to be encrypted or is the output of decryption
- **Ciphertext**
 - The scrambled and unreadable output of encryption
- **Cleartext data**
 - Data stored or transmitted without encryption
- **Key**
 - A mathematical value entered into the algorithm to produce ciphertext
 - The reverse process uses the key to decrypt the message

5

What is Cryptography?

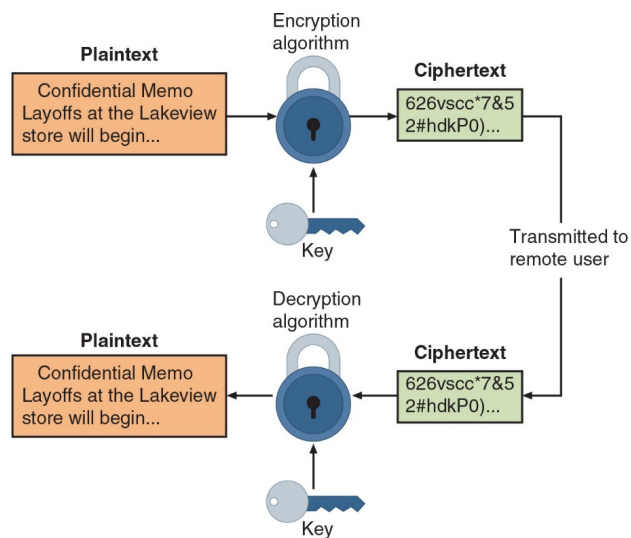
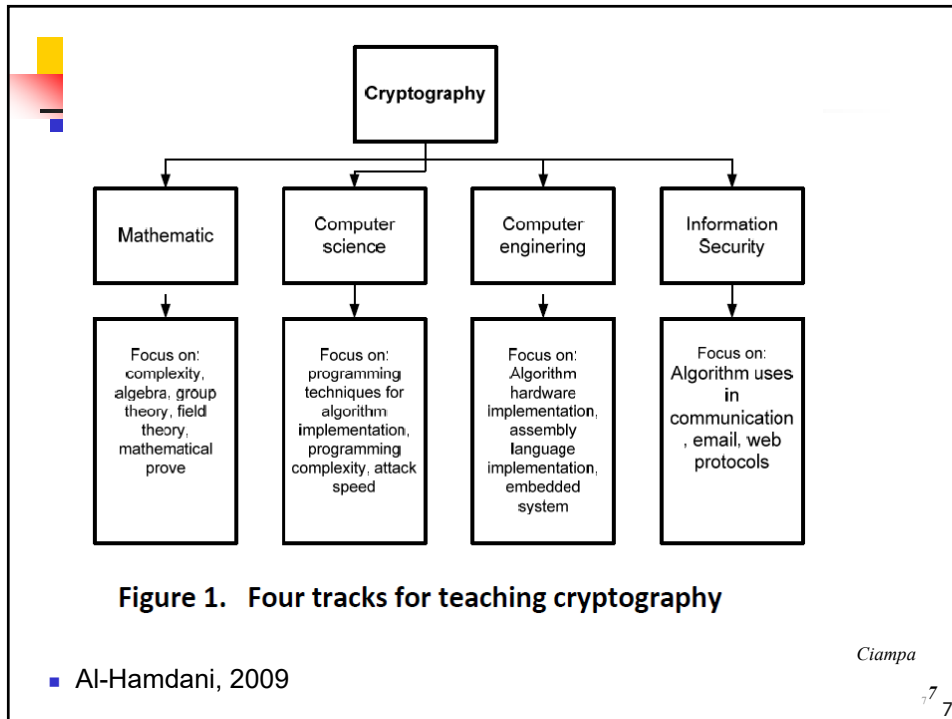


Figure 6-2 Cryptographic process

6



Shift Cipher

- **Shift Cipher:**
 - The algorithm specifies that you offset the alphabet either to the right (forward) or to the left (backward) for another letter
 - The key specifies how many letters the offset should
 - A classic example - Caesar's cipher.
 - Example: Every letter is rotated 19 positions in the alphabet
- **Weakness:** The ease with which it could be broken

8

Transposition

Transposition Cipher:

Same letters are used but the order is changed

Used in Spartans Cipher

Spartans used a ribbon wrapped around a specific gauge cylinder and then wrote on the ribbon



- The order of the letters are changed.

- Ex. THE UNEXAMINED LIFE IS NOT WORTH LIVING

- Written vertically over six columns becomes:

TX SOV
HAL RI
EMINTN
IFOHG
UNET
NE L
EDIWI



Then, written horizontally becomes:

TX SOVHAL RIEMINTN
IFOHGUNET NE LEDIWI

9
9

Cryptography and Security

- Cryptography can provide five basic information protections

- Confidentiality
 - Integrity
 - Availability
 - Authenticity of the sender
 - Nonrepudiation

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

0
10



Goals of Cryptography

Important

- **Confidentiality**

- Most commonly addressed goal
- The meaning of a message is concealed by encoding it
 - The sender encrypts the message using a cryptographic key
 - The recipient decrypts the message using a cryptographic key
 - May or may not be the same as the one used by the sender

- **Integrity**

- When a message is sent, both the sender and recipient need to know that the message was not altered in transmission.
- The hash functions compute the message digests, and this guarantees the integrity of the message

11
11



Goals of Cryptography (continued)

- **Nonrepudiation**

- The message sender cannot later deny that they sent the message.
- This is important in electronic exchanges of data, especially when you are unable to meet face-to-face.
- Based upon public key cryptography and the principle of only you knowing your private key.
 - Tied to asymmetric cryptography and cannot be implemented with symmetric algorithms.

- **Authentication**

- Authentication lets you prove you are who you say you are.
- Asymmetric encryption is better suited than symmetric encryption to prove one's identity
- Authentication can be accomplished in a multitude of ways: Token, digital certificates
- When you log into a secure web site, one-way authentication occurs.
 - Accomplished using digital certificates

12
12

Algorithms

■ Algorithm:

- A step-by-step problem-solving procedure.
- A recursive computational procedure for solving a problem in finite steps.

■ Cryptographic algorithm

- A set of mathematical steps for encrypting and decrypting information.
- Commonly called as encryption algorithm or cipher
- Used to encrypt a message- Change from plaintext to ciphertext
- And then decrypt the message- Change from ciphertext back to plaintext

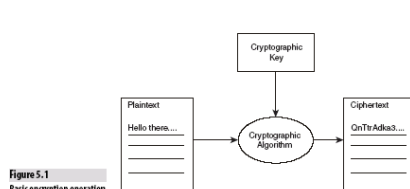


Figure 5.1
Basic encryption operation

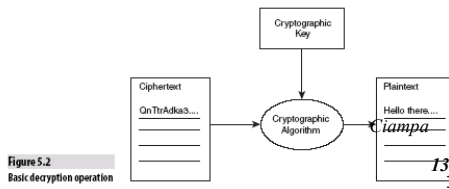


Figure 5.2
Basic decryption operation

Cryptography and Security

- Cryptography can provide protection to data as that data resides in any of three states:

■ Data in-use

- data actions being performed by “endpoint devices”

■ Data in-transit

- actions that transmit the data across a network

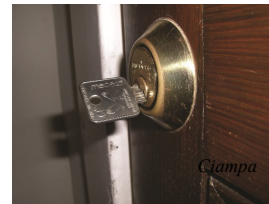
■ Data at-rest

- data this is stored on electronic media

Steps for Encryption

- The steps for encrypting data can be published because of the design of the systems.
 - They are designed to use a key.
- **The algorithms remain the same.**
 - Every implementation uses a **different key**.
 - This ensures that even if other know the algorithm, they cannot break the security.

While everyone knows how to use a knob to open a door, without the key to unlock the knob, that knowledge is useless



15

Limitations of Cryptography



- The number of small electronic devices (**low-power devices**) has grown significantly
 - These devices need to be protected from threat actors
- Applications that require extremely fast response times also face cryptography limitations
- **Resource vs. security constraint**
 - A limitation in providing strong cryptography due to the tug-of-war between available resources (time and energy) and the security provided by cryptography
- It is important that there be **high resiliency** in cryptography
 - High resiliency is the ability to quickly recover from these resource vs. security constraints

16

Cryptographic Algorithms



- A fundamental difference in cryptographic algorithms is the amount of data processed at a time
 - **Stream cipher** - takes one character and replaces it with another
 - **Block cipher** - manipulates an entire block of plaintext at one time
 - **Sponge function** - takes as input a string of any length and returns a string of any requested variable length
- **Three categories of cryptographic algorithms**
 - Hash algorithms
 - Symmetric cryptographic algorithms
 - Asymmetric cryptographic algorithms

17

Hash Algorithms

- **Hash algorithms**
 - Creates a unique “digital fingerprint” of a set of data and is commonly called **hashing**
 - This fingerprint, called a digest (sometimes called a message digest or hash), represents the contents
 - Its contents cannot be used to reveal original data set
 - Is primarily used for comparison purposes
- Hashing is intended to be one way in that its digest cannot be reversed to reveal the original set of data

18
18

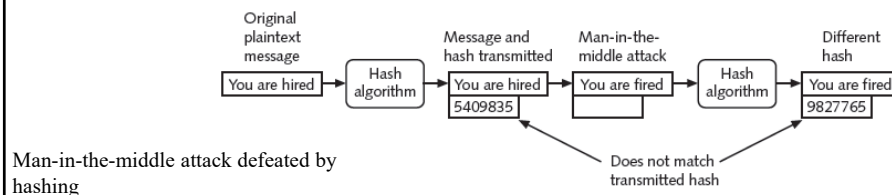
Hash Algorithms

- 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**
 - Data set cannot be created to have a predefined hash
 - **Secure**
 - Resulting hash cannot be reversed to determine original plaintext

19
19

Cryptographic Algorithms


- 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 (shared) 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

Ciampa

20
20




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

Table 5-2 Information protections by hashing cryptography

Ciampa

21
21



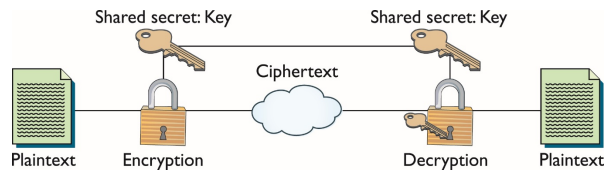
Hash Algorithms
<ul style="list-style-type: none"> ■ Message Digest 5 (MD5) <ul style="list-style-type: none"> ■ Most well-known of the MD hash algorithms ■ Message length padded to 512 bits ■ Weaknesses in compression function could lead to collisions ■ Some security experts recommend using a more secure hash algorithm ■ Secure Hash Algorithm (SHA) <ul style="list-style-type: none"> ■ Refers to four hash algorithms published by the National Institute of Standards and Technology (NIST) and the National Security Agency ■ More secure than MD ■ SHA-1, SHA-256, SHA-384, SHA-512 ■ SHA-2 is currently considered to be a secure hash ■ All have longer hash results, and are more difficult to attack successfully. ■ SHA-3 was announced as a new standard -may be suitable for low-power devices

22
22

Symmetric Encryption

■ Symmetric encryption

- Older and simple method of encrypting information
- Requires the sender and the receiver to have the same key.
 - All symmetric algorithms are based upon this shared secret principle.
- Also called private key cryptography (the key is kept private between sender and receiver)
- Key is called **shared secret key** or **secret key**



- Symmetric encryption involves a cryptographic key, requiring key management.
- The most important lesson - Store and send the key only by known secure means.

23
23

Symmetric Cryptographic Algorithms

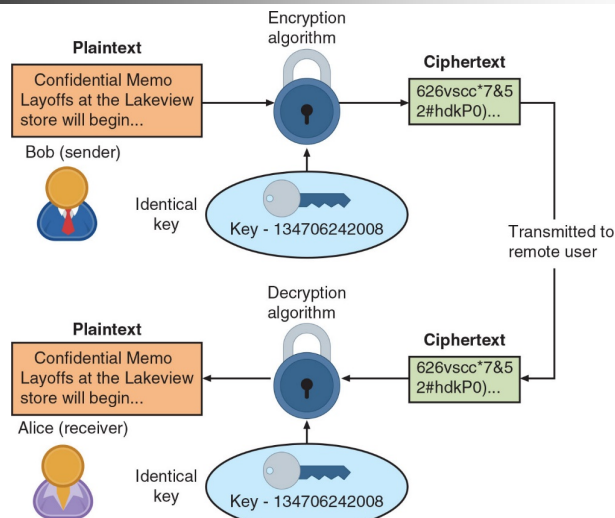



Figure 6-5 Symmetric (private key) cryptography

24
24




Symmetric Cryptographic Algorithms

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

Table 5-4 Information protections by symmetric cryptography

Ciampa

~~25~~
25



Symmetric Cryptographic Algorithms

- **Common algorithms include:**
 - Data Encryption Standard (DES)
 - Triple Data Encryption Standard (3DES)
 - Advanced Encryption Standard (AES)

Ciampa

~~26~~
26

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
- Important principles
 - **Key pairs**
 - **Public key**
 - **Private key**
 - **Both directions** - keys can work in both directions

27
27

Asymmetric Cryptographic Algorithms

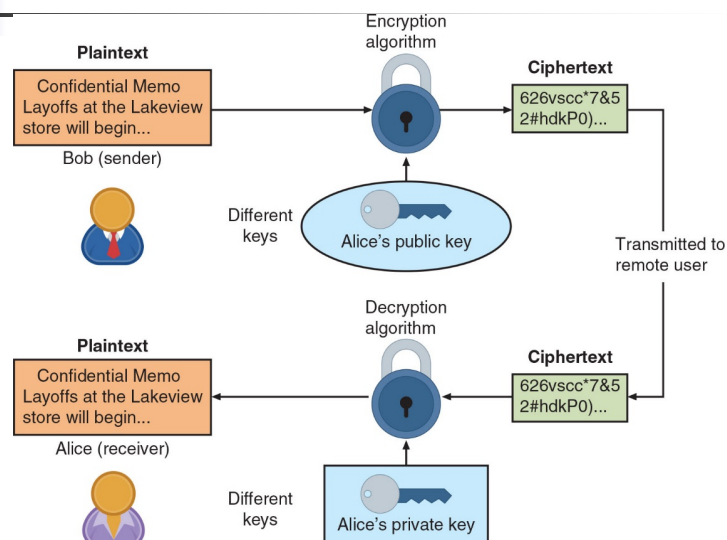


Figure 6-7 Asymmetric (public key) cryptography

28

Asymmetric Cryptographic Algorithms

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

29
29

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

Information protections by asymmetric cryptography

Ciampa

30
30

Asymmetric Cryptographic Algorithms

■ Digital Signature Algorithm (DSA)

- Digital signature - an electronic verification
- Verifies the sender
- Prevents sender from disowning the message
- Proves message integrity

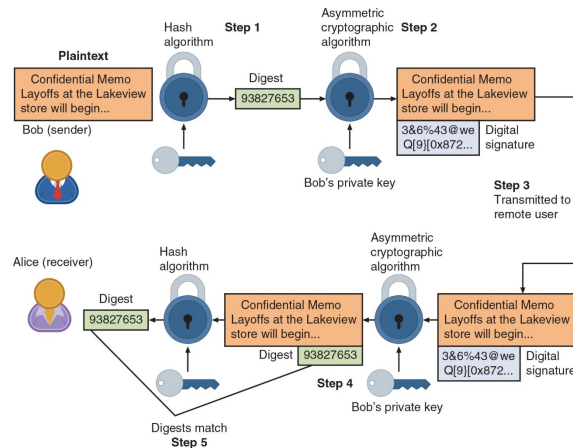


Figure 6-9 Digital signature

31
31

Symmetric Versus Asymmetric Cryptosystems

- Symmetric cryptosystems don't scale well
- Asymmetric cryptosystems are slower than symmetric ones
- Symmetric cryptosystems are excellent for securing the ends of a communication circuit such as a Virtual Private Network
- Asymmetric cryptosystems are more practical when there are a large number of users

Important

Ciampa

32
32

TABLE 5.2 Comparison of Symmetric and Asymmetric Cryptosystems

Symmetric Cryptosystems	Asymmetric Cryptosystems
Provide confidentiality among all participants who share the same secret key	Provide confidentiality between individual users of a cryptosystem
Provide integrity against modification by individuals who do not possess the secret key	Provide integrity against modification by anyone other than the sender of the message
Provide for authentication between two individuals when they are the only ones who possess the secret key	Provide for authentication of any individual user of the cryptosystem
Do not provide for nonrepudiation	Provide for nonrepudiation
Require shorter keys than asymmetric algorithms to achieve the same level of security	Require longer keys than symmetric algorithms to achieve the same level of security
Operate faster than asymmetric algorithms	Operate slower than symmetric algorithms
Are not easily scalable	Scale well to environments with large numbers of users
Do not facilitate the use of digital certificates	Lend themselves well to digital certificate hierarchies
Make the exchange of cryptographic keys difficult (often requiring offline exchange)	Allow for the exchange of public keys over otherwise insecure transmission media

Ciampa

Conklin 33

Cryptographic Attacks and Defenses



- Cryptography remains under attack by threat actors for any vulnerabilities
- The new field of quantum cryptography defenses can aid in making cryptography more secure

Attacks on Cryptography



- Two most common cryptography attacks
 - Algorithm attacks
 - Collision attacks
- **Algorithm Attacks**
 - Methods attackers can use to circumvent strong algorithms:
 - **Known ciphertext attacks**
 - Statistical tools can be used to attempt to discover a pattern in the ciphertexts, which can then be used to reveal the plaintext or key
 - **Downgrade attacks**
 - A threat actor forces the system to abandon the current higher security mode of operation and instead “fall back” to implementing an older and less secure mode
 - **Attacks based on misconfigurations**
 - Selecting weak algorithms should be avoided since they are no longer secure

35

Collision Attack

- **A collision attack**
 - Used to compromise a hash algorithm.
 - Occurs when an attacker finds two different messages that hash to the same value.
- **Hash functions that suffers from collisions lose integrity.**
 - **A good hash function should be resistant to collision**
- An attacker that can make two different inputs hash to the same value, can trick people into running malicious code.
- **This attack is very difficult and requires generating a separate algorithm that attempts to find a text that will hash to the same value of a known hash.**

Ciampa

36
36

Quantum Cryptographic Defenses



- **Quantum cryptography**

- Takes advantage of quantum computing for increasing cybersecurity

- **Quantum communication** (or secure telecommunications)

- A subcategory of quantum cryptography
- Users in a quantum communication exchange can easily detect eavesdroppers

- **Quantum computing also has a drawback for cybersecurity**

- A single quantum computer could perform factoring by using hundreds of atoms in parallel to quickly factor huge numbers
- Renders all current asymmetric cryptographic algorithms useless

37

- https://www.youtube.com/watch?v=6H_9I9N3IXU

38

38



Using Cryptography

- Cryptography should be used to secure:
 - Data-in-transit, data-at-rest, and when possible data-in-use
- This includes:
 - Individual files
 - Databases
 - Removable media
 - Data on mobile devices
- Cryptography can be applied through:
 - Software
 - Hardware

39
39



Encryption through Software



- **File and File System Cryptography**
 - Encryption software can be used to encrypt or decrypt files one-by-one (a cumbersome process)
 - Protecting groups of files can take advantage of the OS's file system
- **Third-party software** tools available for encryption include GNU Privacy Guard (GnuPG), AxCrypt, Folder Lock, and VeraCrypt

40



Encryption through Software



■ Full Disk Encryption (FDE)

- FDE protects all data on a hard drive
- Example: *BitLocker* drive encryption software that is included in Microsoft Windows
 - BitLocker encrypts the entire system volume, including the Windows Registry
 - Prevents attackers from accessing data by booting from another OS or placing the hard drive in another computer

41



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
- Hardware encryption options include:
 - Trusted platform module
 - Hardware security model

42



Hardware Encryption

- **USB device encryption**

- Encrypted hardware-based flash drives can be used
 - 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

- **Self-Encrypting Drives (SEDs)**

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

43
43



Hardware Encryption



- **Hardware Security Module (HSM)**

- HSM is a removable external cryptographic device
- It includes an onboard key generator and key storage facility
- Performs accelerated symmetric and asymmetric encryption
- Malware cannot compromise it

- **Trusted Platform Module (TPM)**

- TPM is a chip on a computer's motherboard that provides cryptographic services
- Includes a true random number generator
- Entirely done in hardware so it 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

44
44

Blockchain

- **A blockchain**

- A shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network

- **Blockchain technology**

- Allows a network of computers to agree at regular intervals on the true state of a distributed ledger
- It is a system in which a record of transactions made is maintained across several computers that are linked in a peer-to-peer network

- **Blockchain relies on cryptographic hash algorithms to records its transactions**

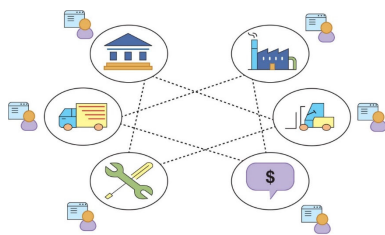


Figure 6-12 Multiple organizations with ledgers

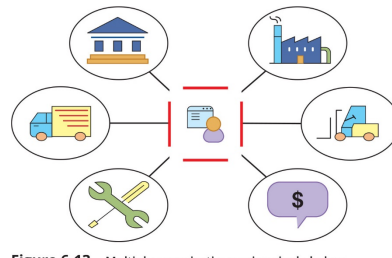


Figure 6-13 Multiple organizations using single ledger

45

Summary (1 of 2)

- Cryptography is the practice of transforming information into a secure form so that unauthorized persons cannot access it
- Cryptography can provide confidentiality, integrity, authentication, nonrepudiation, and obfuscation
- One variation of a cryptographic algorithm is based on the device that is used in the cryptographic process
 - Another variation is the amount of data that is processed at a time
- Hashing creates a unique digital fingerprint called a digest, which represents the contents of the original material
- Symmetric cryptography (also called private key cryptography) uses a single key to encrypt and decrypt a message

46

Summary (2 of 2)

- Asymmetric cryptography (also known as public key cryptography) uses two keys instead of one
- Because cryptography provides a high degree of protection, it remains under attack
- Quantum computing relies on quantum physics using atomic-scale units (qubits) that can be both 0 and 1 at the same time
- Cryptography can be applied through either software or hardware
- Hardware encryption cannot be exploited like software cryptography
- A blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network

47

- InterestingDifficult
- ProposedQuiz

48

48