Security

Objectives

- To discuss security threats and attacks
- To explain the fundamentals of encryption, authentication, and hashing
- To examine the uses of cryptography in computing
- To describe the various countermeasures to security attacks

Outline

- The Security Problem
- Program Threats
- System and network threats
- Cryptography as a Security Tool
- User Authentication
- Implementing Security Defenses
- Firewalling to Protect Systems and Networks
- Computer-Security Classifications

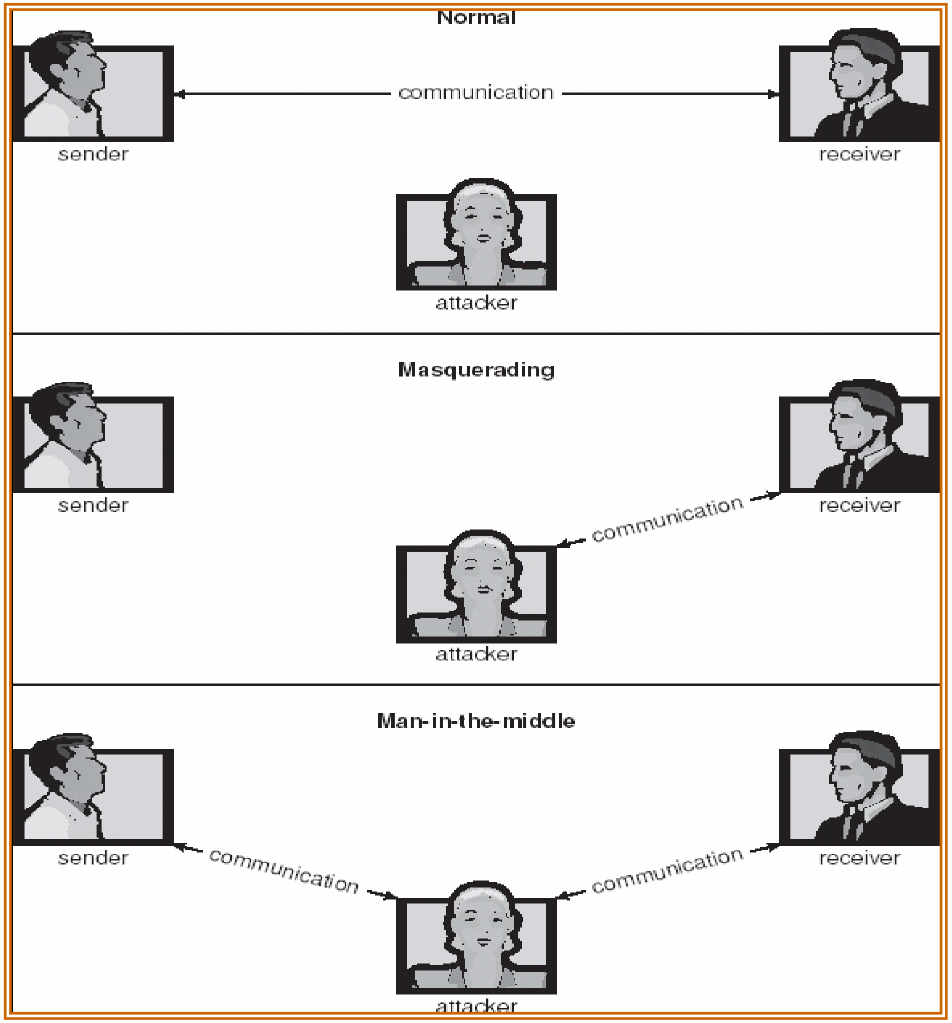
- The Security Problem

- Security must consider external environment of the system, and protect the system resources
- Intruders (crackers) attempt to breach security
- **Threat** is potential security violation
- **Attack** is attempt to breach security
- Attack can be accidental or malicious
- Easier to protect against accidental than malicious misuse

-- Security Violations

- Categories
  - Breach of confidentiality
  - Breach of integrity
  - Breach of availability
  - Theft of service
  - Denial of service
- Methods
  - Masquerading (breach authentication)
  - Replay attack
  - Man-in-the-middle attack

-- Standard Security Attacks



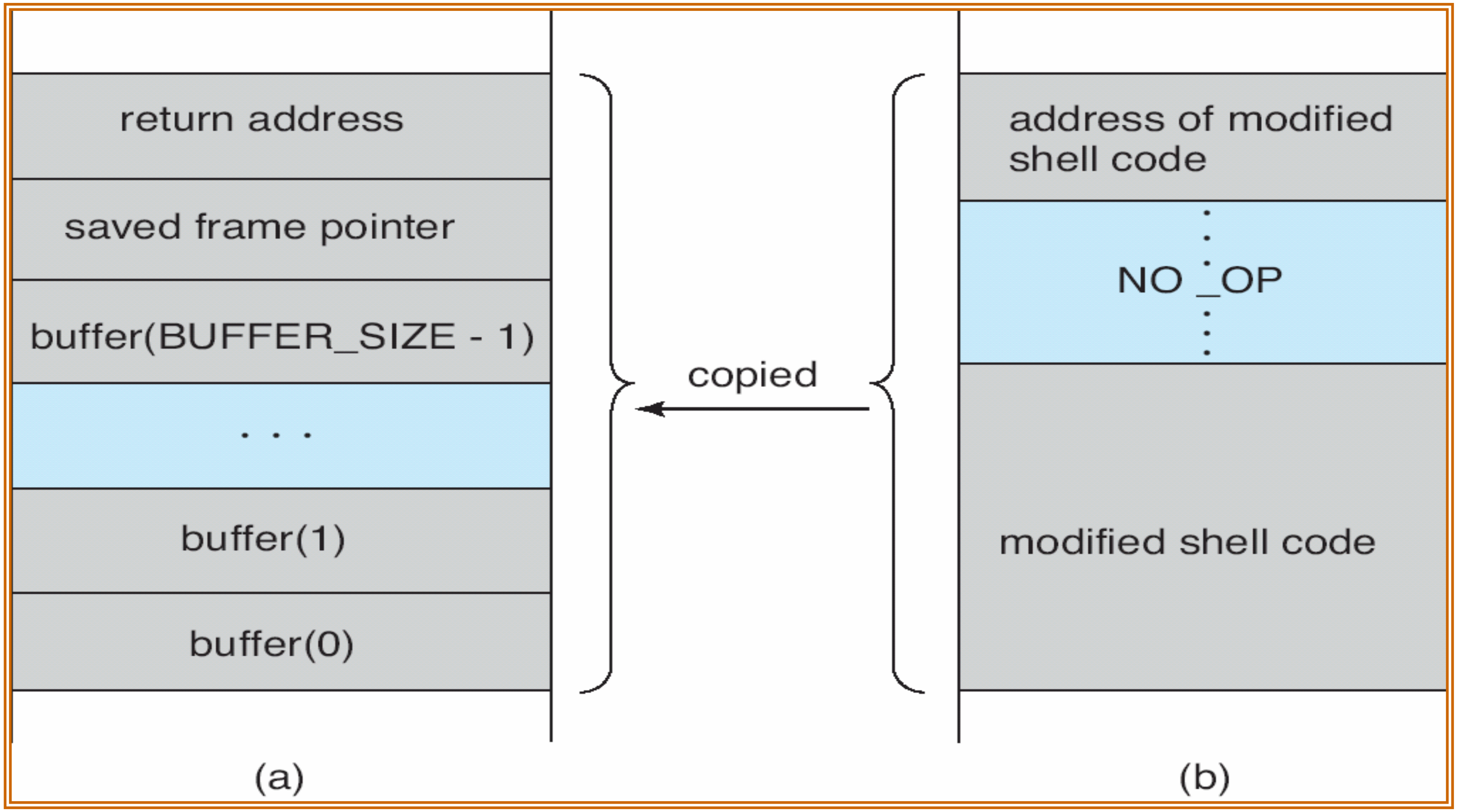
-- Security Measure Levels

- Security must occur at four levels to be effective:
  - Physical
  - Human
    - Avoid **social engineering, phishing, dumpster diving**
  - Operating System
  - Network
- Security as weak as the weakest chain.
- In the remainder of this chapter, we address security at the network and operating-system level.

- Program Threats ...

- Trojan Horse
  - Code segment that misuses its environment
  - Exploits mechanisms for allowing programs written by users to be executed by other users
  - **Spyware, pop-up browser windows, covert channels**
- Trap Door
  - Specific user identifier or password that circumvents normal security procedures
  - Could be included in a compiler
- Logic Bomb
  - Program that initiates a security incident under certain circumstances
- Stack and Buffer Overflow
  - Exploits a bug in a program (overflow either the stack or memory buffers)

-- Hypothetical Stack Frame



Before attack

After attack

... - Program Threats ...

- Virus
  - Executable code often sent as an attachment to an e-mail message or hidden in files such as audio clips, video clips and games
  - Attaches to or overwrites other files to replicate itself
  - Can corrupt files, control applications or even erase a hard drive
  - Can be spread across a network simply by sharing “infected” files embedded in e-mail attachments, documents or programs

... - Program Threats

- Many categories of viruses, literally many thousands of viruses
  - File
  - Boot
  - Macro
  - Source code
  - Polymorphic
  - Encrypted
  - Stealth
  - Tunneling
  - Multipartite
  - Armored

- System and Network Threats

- Worm
  - Executable code that spreads by infecting files over a network
  - Rarely requires any user action to propagate
  - Does not need to be attached to another program or file to spread
- Once a virus or worm is released, it can spread rapidly, often infecting millions of computers worldwide within minutes or hours
- Port scanning
  - Automated attempt to connect to a range of ports on one or a range of IP addresses
- Denial of Service
  - Overload the targeted computer preventing it from doing any useful work
  - Distributed denial-of-service (**DDOS**) come from multiple sites at once

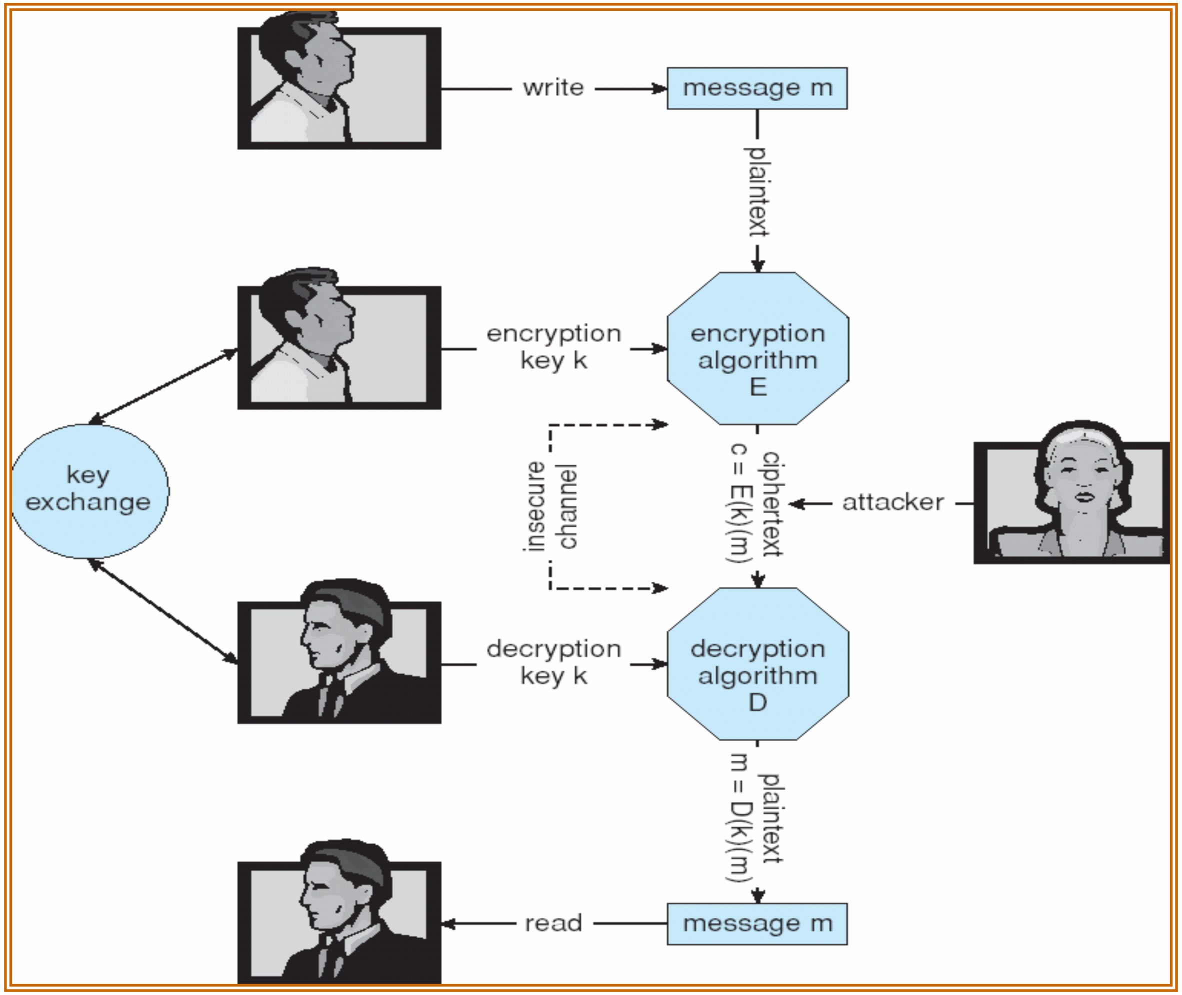
- Cryptography ...

- Broadest security tool available
  - Source and destination of messages cannot be trusted without cryptography
  - Means to constrain potential senders (*sources*) and / or receivers (*destinations*) of *messages*
- Based on secrets (**keys**)
  - Symmetric
  - Asymmetric

… - Cryptography

- Keys are generally distributed selectively to computers in the network.
- A sender can encode its message using the key so that only the computer with a certain key can decode the message. Key becomes the destination.
- A recipient of a message verify that the message was created by some computer possessing a certain key – key is the source of the message.
- Important: It should be computationally infeasible to derive the key from messages used to generate and from any other public information.

-- Secure Communication over Insecure Medium



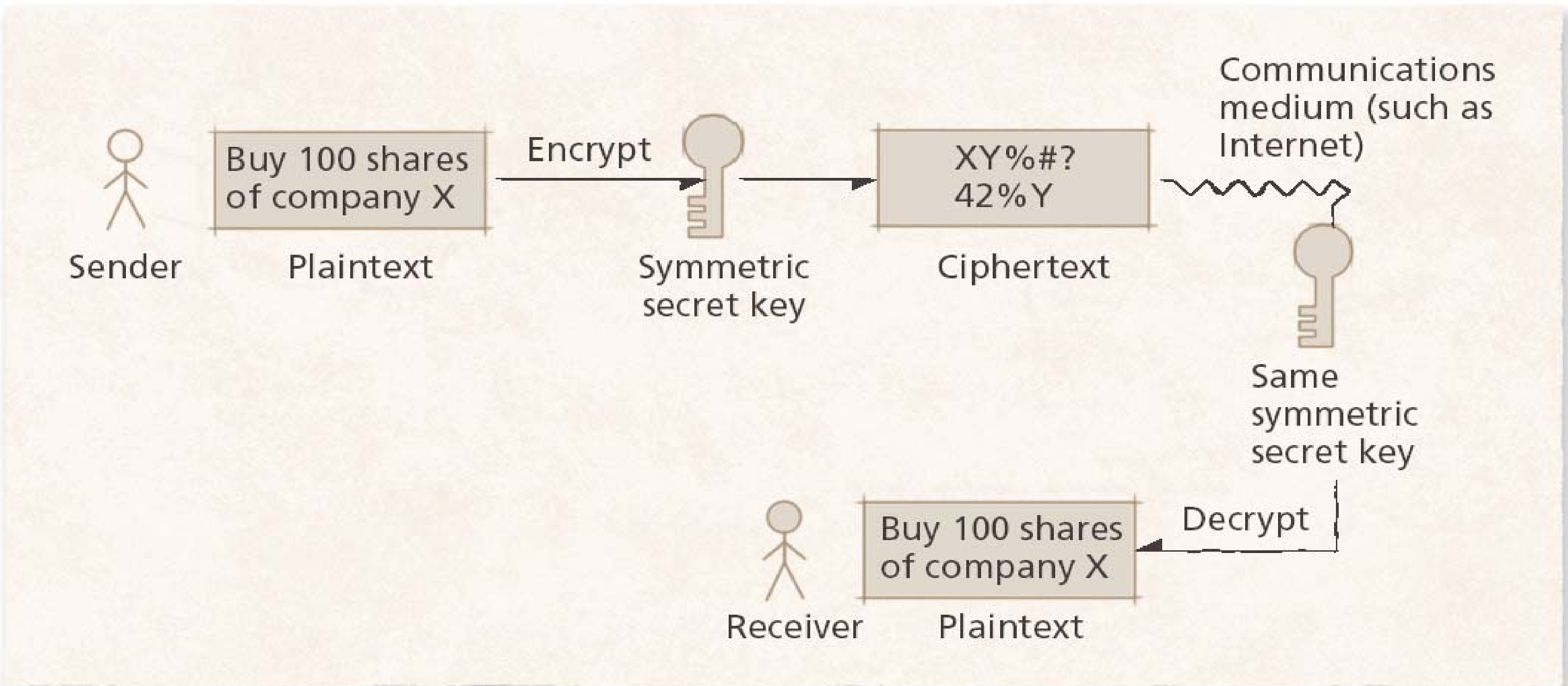
-- Encryption

- Encryption is used to keep sensitive data and information more secure when transmitted over unreliable links as an OS may not offer sufficient protection for such highly sensitive data.
- Encrypt clear text (readable form) into cipher text (internal form).
- Properties of good encryption technique:
  - Relatively simple for authorized users to encrypt and decrypt data.
  - Encryption scheme depends not on the secrecy of the algorithm but on a parameter of the algorithm called the encryption key.
  - Extremely difficult for an intruder to determine the encryption key.

-- Symmetric Cryptography ...

- Uses the same secret key to encrypt and decrypt a message
  - Sender
    - Encrypts a message using the secret key
    - Sends encrypted message to the intended recipient
  - Recipient
    - Decrypts the message using the same secret key

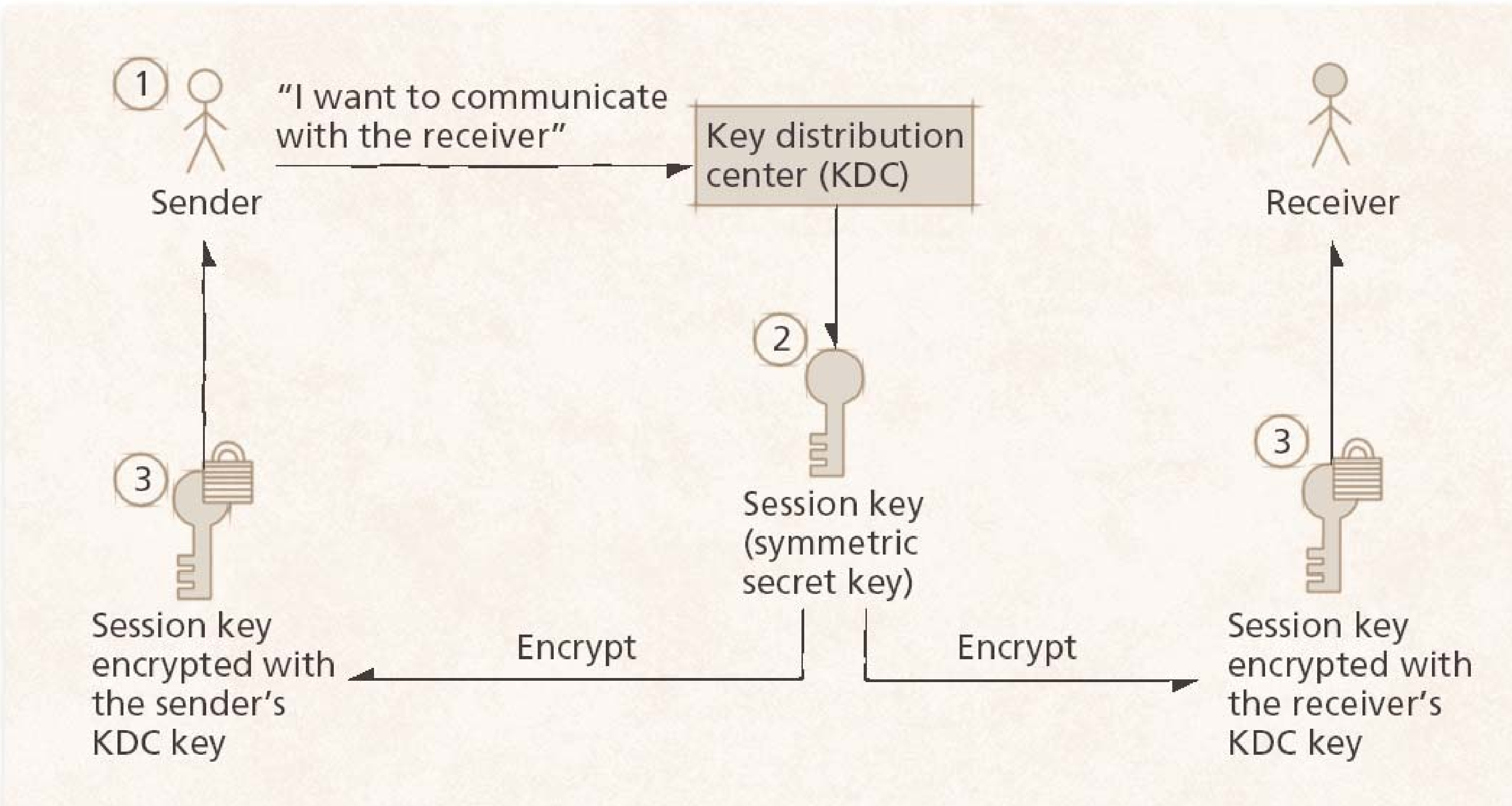
... -- Symmetric ...


Communications medium (such as Internet)
Buy 100 shares of company X
Encrypt
XY%#? 42%Y
Sender
Plaintext
Symmetric secret key
Ciphertext
Same symmetric secret key
Decrypt
Buy 100 shares of company X
Receiver
Plaintext

... --Symmetric

- Limitation of secret-key cryptography
  - Before two parties can communicate securely, they must find a secure way to exchange the secret key
    - Can be done by courier or a key distribution center (KDC)
      - KDCs generate session keys to clients
- Examples of secret-key cryptography:
  - DES
  - 3DES
  - AES

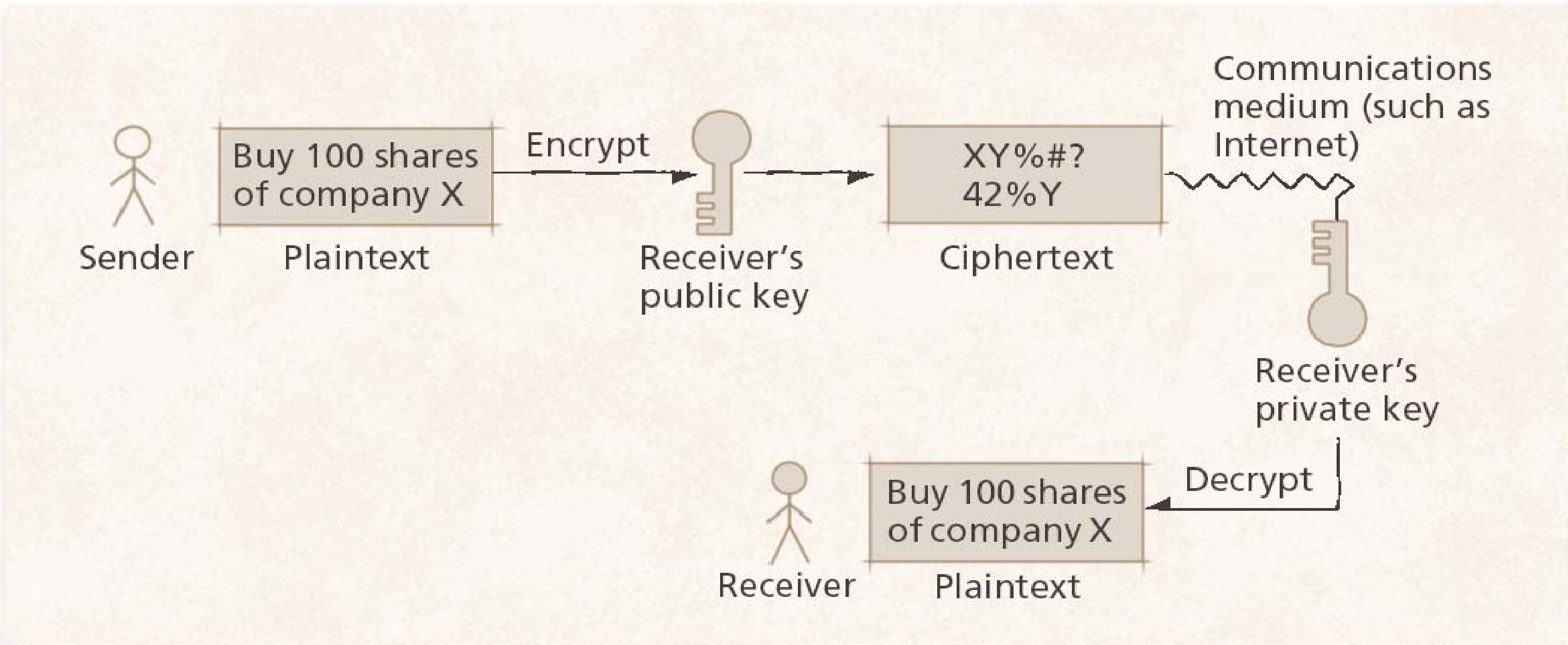
--- Distributing a session key with a key distribution center



-- Asymmetric (public-key) Cryptography ...

- Solves the problem of securely exchanging symmetric keys
- Asymmetric
  - Employs two inversely related keys:
    - Public key
      - Freely distributed
    - Private key
      - Kept secret by its owner
- If the public key encrypts a message, only the corresponding private key can decrypt it

... -- Asymmetric Cryptography ...



... -- Asymmetric Cryptography ...

- If the decryption key is the sender's public key and the encryption key is the sender's private key, the sender of the message can be authenticated
  - Message should be encrypted first using the receiver's public key, then with the sender's secret key
    - Public key provides confidentiality
    - Secret key provides authentication
- Examples of public-key cryptography:
  - RSA
  - Pretty Good Privacy (PGP)

- Secure Communication ...

- Five fundamental requirements for a successful, secure transaction
  - Privacy
    - Ensuring that the information transmitted over the Internet has not been viewed by a third party
  - Integrity
    - Ensuring that the information sent or received has not been altered
  - Authentication
    - Verifying the identities of the sender and receiver
  - Authorization
    - Managing access to protected resources on the basis of user credentials
  - Nonrepudiation
    - Ensuring that the network will operate continuously

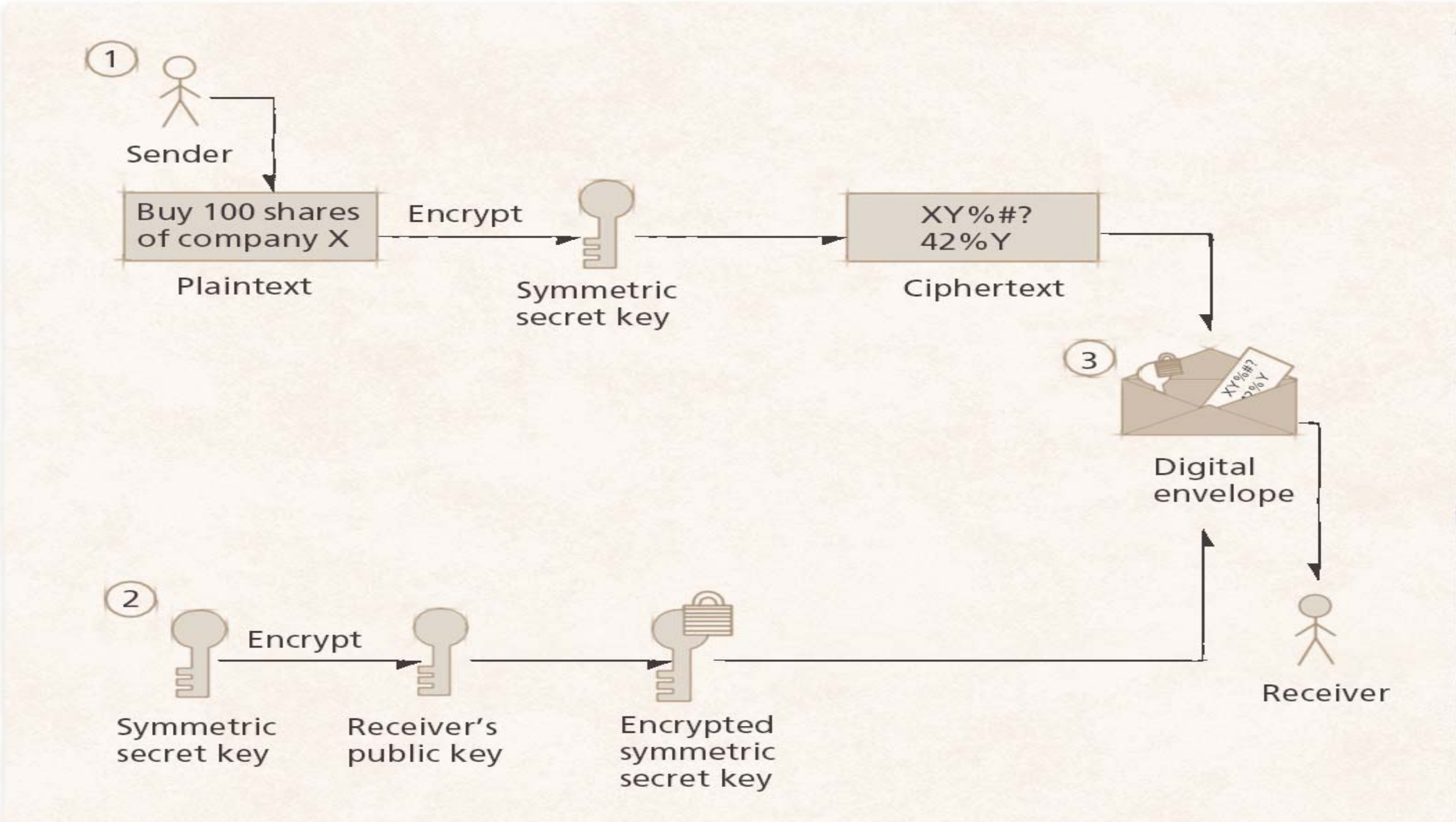
-- key Management

- Maintaining the secrecy of private keys is essential to the maintenance of cryptographic system security
- Most security breaches result from poor key management rather than cryptanalytic attacks
  - For example: The mishandling of private keys, resulting in key theft
- Key generation
  - The process by which keys are created
  - Important to use a key-generation program that can generate a large number of keys as randomly as possible
  - Key security is improved when key length is large enough that brute-force cracking is computationally infeasible

-- Key Agreement protocol ...

- public-key algorithms
  - Most often employed to exchange secret keys securely
- Key agreement protocol
  - The process by which two parties can exchange keys over an unsecure medium
    - Digital envelopes
    - Digital signatures (using the SHA-1 and MD5 hash algorithms

--- Digital Envelop



--- Digital Signatures

- The electronic equivalents of written signatures
- Developed to address the absence of authentication and integrity in public-key (Asymmetric) cryptography
- Authenticate senders' identities
  - Sender Hashes the message to produce message digest
  - Encrypts the message digest and the message before sending
- Difficult to forge
- Hash value uniquely identifies a message
  - Examples
    - Secure Hash Algorithm (SHA-1)
    - MD5 Message Digest Algorithm
    - Digital Signature Algorithm (DSA)

- User Authentication ...

- Identifying users and the actions they are allowed to perform
- A user can be identified by:
  - a unique characteristic of the person (e.g., fingerprints, voiceprints, retina scans and signatures)
  - ownership of an item (e.g., badges, identification cards, keys and smart cards)
  - user knowledge (e.g., passwords, personal identification numbers (PINs) and lock combinations)

-- Basic Authentication

- Simple password protection
  - Most common authentication scheme
  - The user chooses a password, memorizes it and presents it to the system to gain admission to a resource or system
- Weaknesses of password protection
  - Users tend to choose passwords that are easy to remember
    - For example: the name of a spouse or pet
  - Someone who has obtained personal information about the user might try to log in several times using passwords that are characteristic of the user
    - Several repeated attempts might result in a security breach
- Password salting
  - Technique that inserts characters at various positions in the password before encryption
  - Can thwart attempts at recovering passwords from password files

--- Password Salting

Plaintext	Ciphertext
password	cGFzc3dvcmQ=
p**s**as**a**sw**l**or**t**d	cHNhc2Fzd2xvcnRk
newpassword	bmV3cGFzc3dvcmQ=
n**s**ew**a**p**l**a**t**ss**e**wo**d**rd	bnNld2FwbGF0c3Nld29kcmQ=

...- User Authentication

- Encrypted password
- One time password
- Biometrics
  - Uses unique personal information to identify a user
    - Fingerprints
    - Eyeball iris scans
    - Face scans
- Smart cards
  - Often designed to resemble a credit card
  - Can serve many different functions, from authentication to data storage
  - Most popular: memory cards and microprocessor cards

- Implementing Security Defenses

- Firewalls
- Intrusion detection systems
- Antivirus software
- Security patches
- Secure file systems
- Many others

-- Firewalls

- Firewalls
  - Protect a local area network (LAN) from intruders outside the network
  - Police inbound and outbound traffic for the LAN
- Types of firewalls
  - Packet-filtering firewall
    - Inspects packets for inconsistencies such as incorrect source address
  - Application-level gateways
    - Inspect packets for malicious payloads (code)

-- Intrusion-Detection Systems (IDSs)

- IDSs
  - Monitor networks and application log files
    - Logs record information about system behavior, such as:
      - The time at which operating system services are requested
      - The name of the process that requests them
  - Examine log files to alert system administrators of suspicious application and/or system behavior
  - If an application exhibits erratic or malicious behavior, an IDS can halt the execution of that process
- Host-based intrusion detection
  - Specially used to detect Trojan horse
- Network-based intrusion detection
  - Mainly used to detect denial of service (Dos)

-- Antivirus Software ...

- Antivirus software
  - Attempts to protect a computer from a virus and/or identify and remove viruses on that computer
  - Various techniques used to detect and remove viruses from a system
    - None can offer complete protection

... -- Antivirus Software

- Signature-scanning virus detection
  - Relies on knowledge about the structure of the computer virus's code
  - Uses a known virus list
    - Can be particularly ineffective against variants and polymorphic viruses
- Heuristic scanning
  - Can prevent the spread of viruses by detecting and suspending any program exhibiting virus-like behavior:
    - Replication, residence in memory and/or destructive code
  - Primary strength: it can detect viruses that have not yet been identified

-- Security Patches

- Security patches
  - Code releases that address security flaws
  - Simply releasing a patch for a security flaw is insufficient to improve security
  - Developers should address security flaws by:
    - Notifying their users quickly
    - Providing software that facilitates the process of applying security patches
      - Example: Hotfixes
        - Microsoft Automatic Updates

-- Secure File Systems

- Secure file systems
  - Protect sensitive data regardless of how the data is accessed
- Encrypting File System (EFS)
  - Uses cryptography to protect files and folders in an NTFS file system
  - Uses secret-key and public-key encryption to secure files

-- Others

- Auditing, accounting, and logging of all or specific system or network activities
- Example
  - Tripwire

Computer Security Classifications

- U.S. Department of Defense outlines four divisions of computer security: **A**, **B**, **C**, and **D**.
- **D** – Minimal security.
- **C** – Provides discretionary protection through auditing. Divided into **C1** and **C2**. **C1** identifies cooperating users with the same level of protection. **C2** allows user-level access control.
- **B** – All the properties of **C**, however each object may have unique sensitivity labels. Divided into **B1**, **B2**, and **B3**.
- **A** – Uses formal design and verification techniques to ensure security.

End of Chapter 15