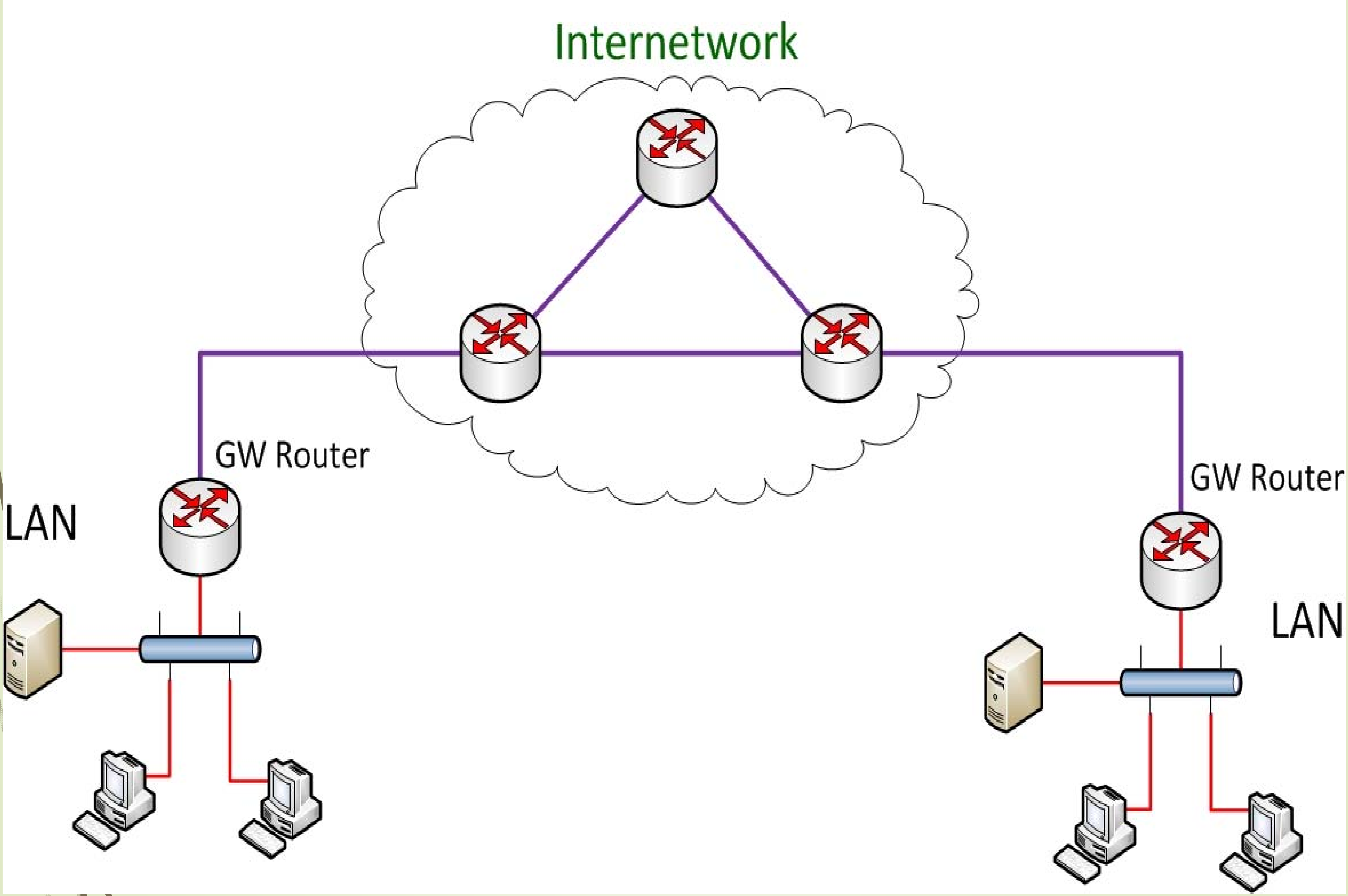
Content Teaching Academy
at
James Madison University

Information Security

DR. MOHAMED ABOUTABL
Department of Computer Science

June 24th, 2014

The Battle Field: Computers, LANs & Internetworks

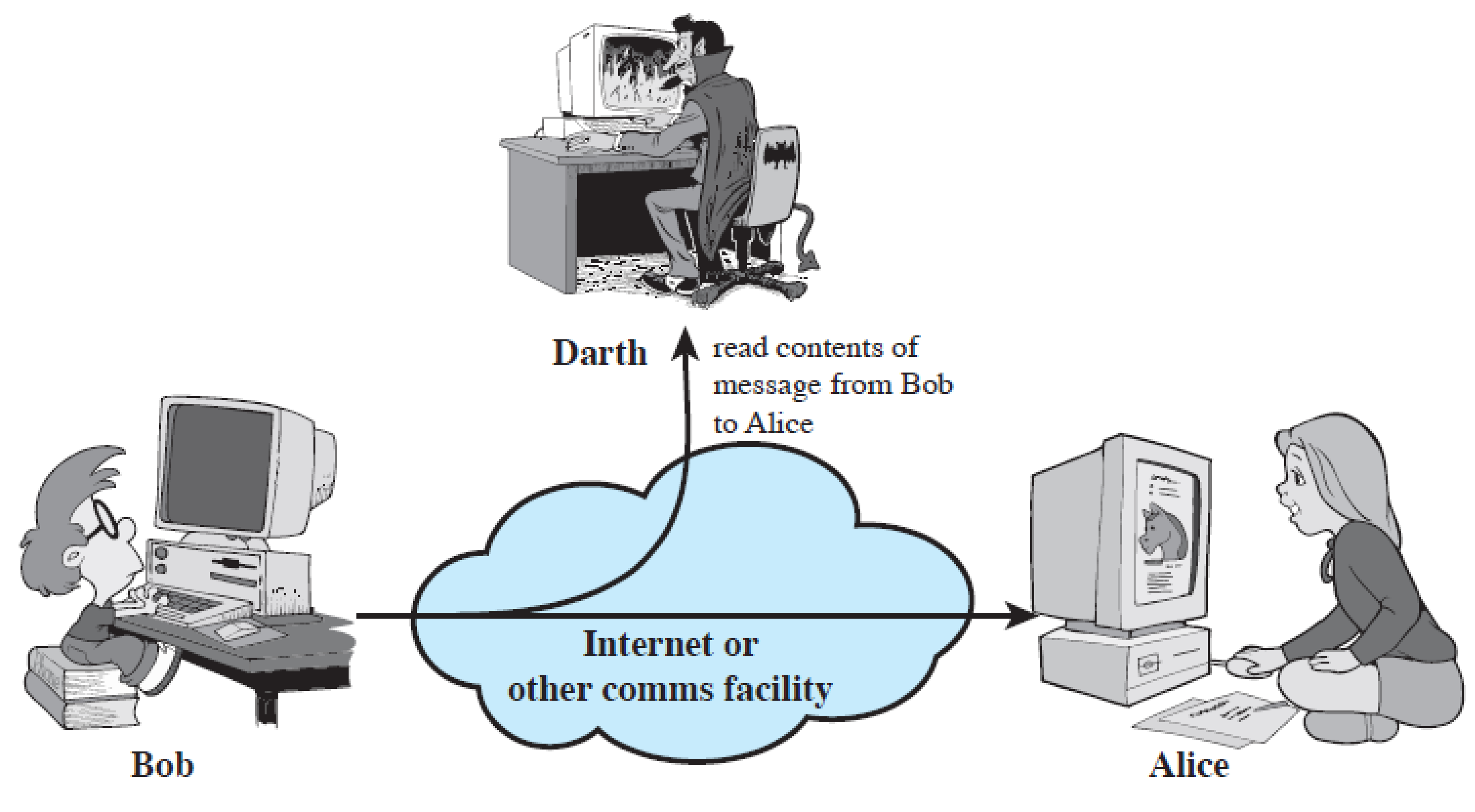


Definitions

- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security** - measures to protect data during their transmission over a collection of interconnected networks
- Traditionally provided by physical and administrative mechanisms
- Security requirements have changed in recent times:
  - computer use requires automated tools to protect files and other stored information
  - use of networks and communications links requires measures to protect data during transmission

Examples of Insecurity: Lack of Confidentiality

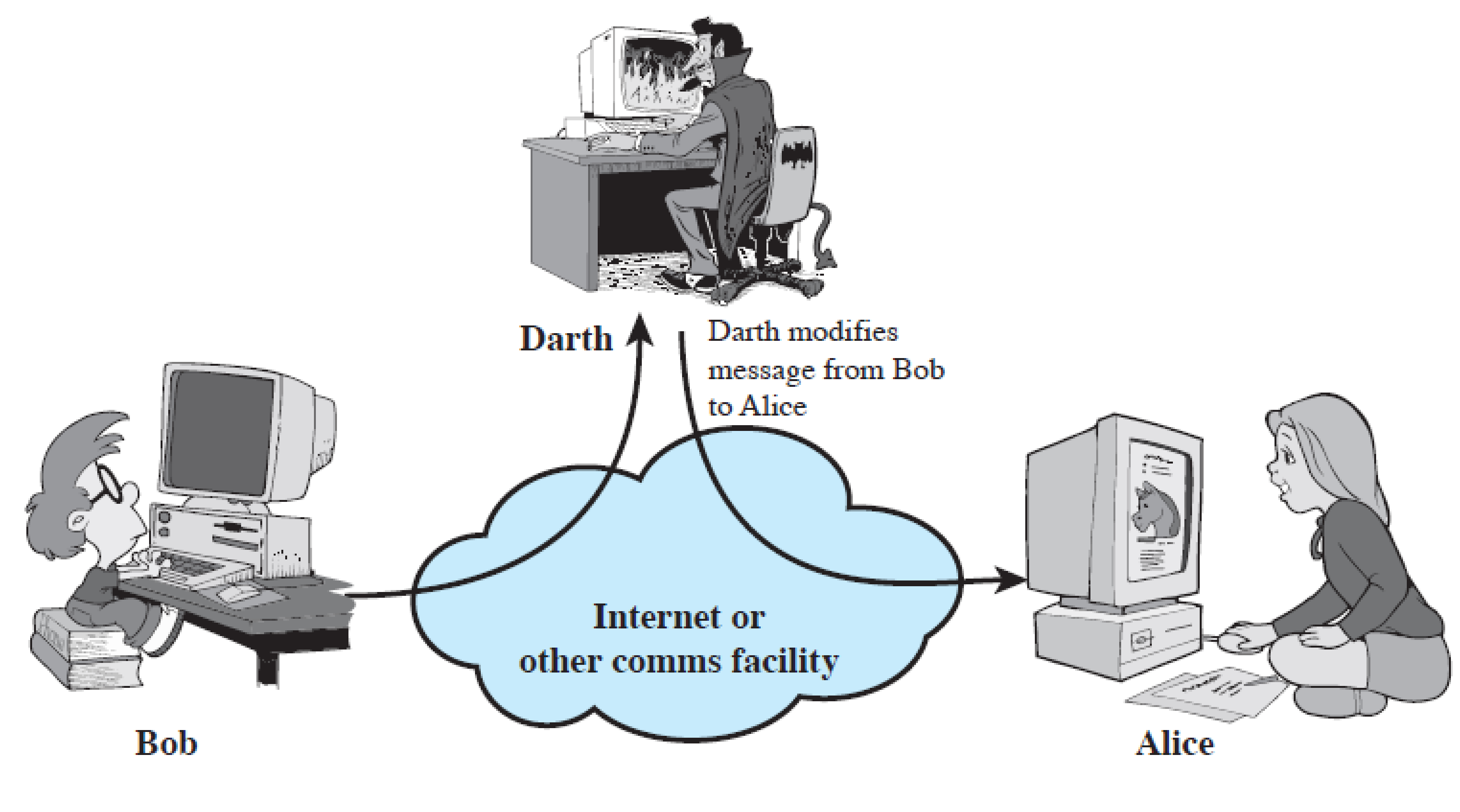
- User C views confidential data transmitted from user A to user B.


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

Source: Network security Essentials, 3rd Ed., by William Stallings

Examples of Insecurity: Lack of Integrity

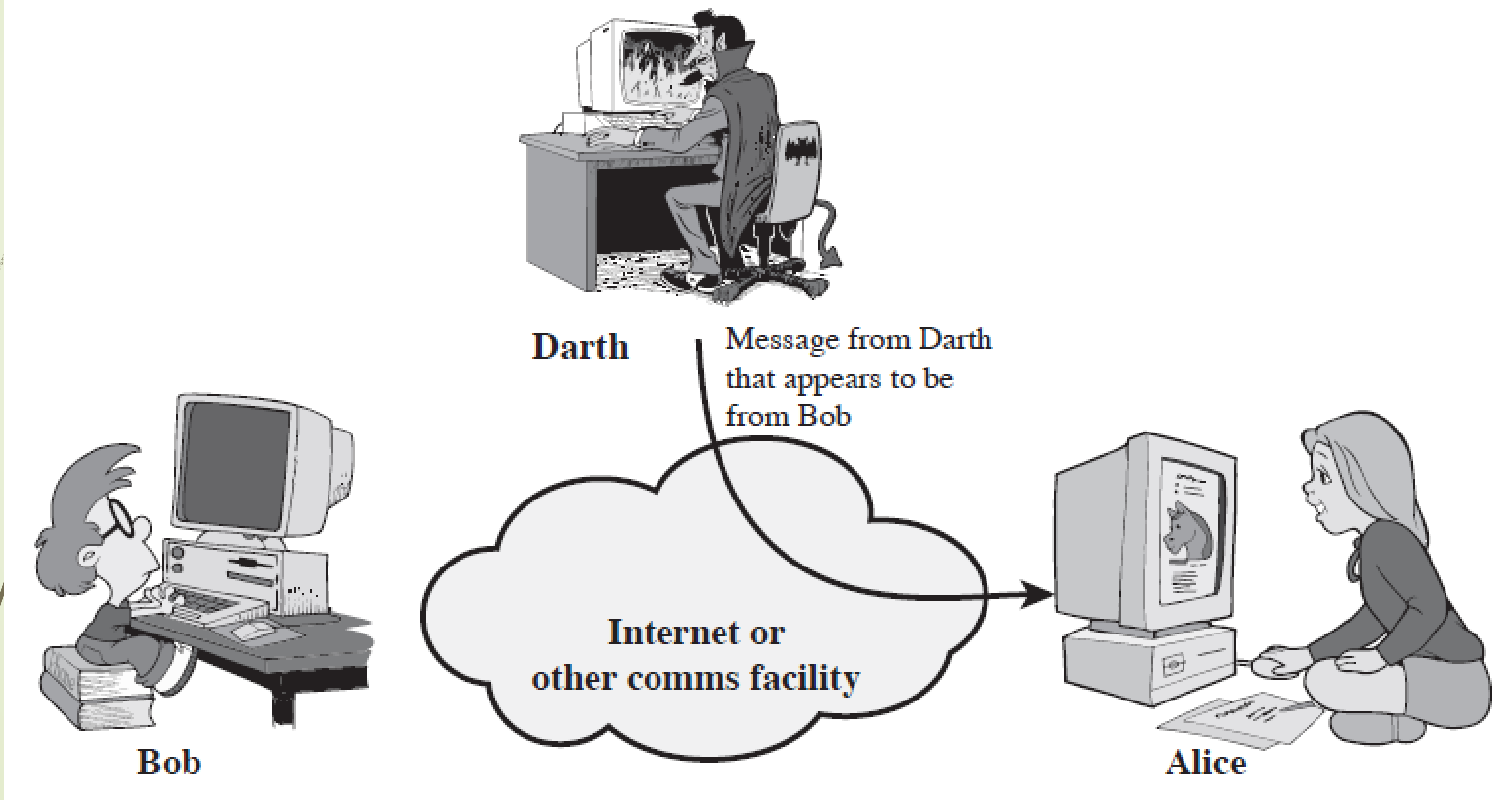
- User C modifies data transmitted from user A to user B.


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

Source: Network security Essentials, 3rd Ed., by William Stallings

Examples of Insecurity: Masquerading

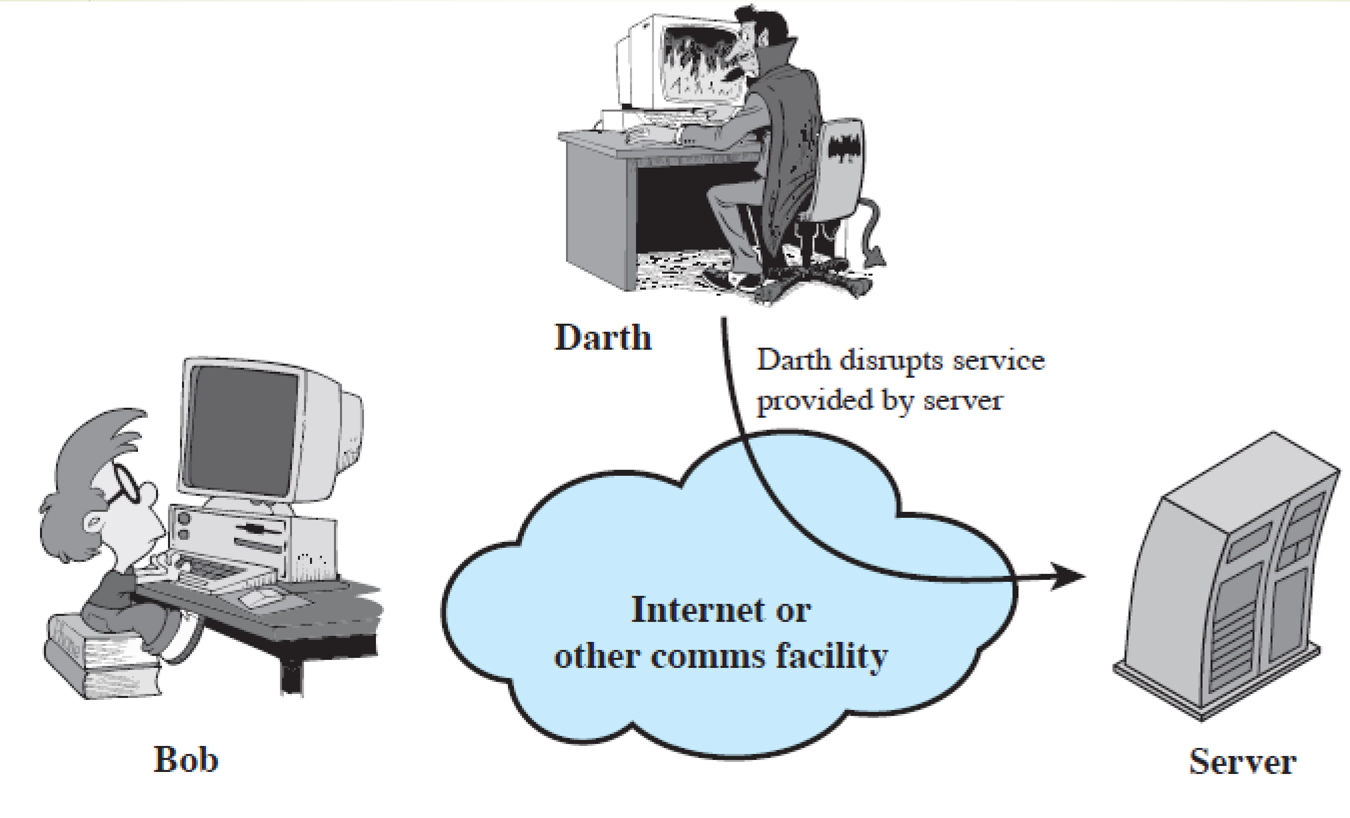
- User C fabricates a message to user B pretending it is from A.


Darth
Message from Darth that appears to be from Bob
Bob
Internet or other comms facility
Alice

Source: Network security Essentials, 3rd Ed., by William Stallings

Examples of Insecurity: Denial of Service

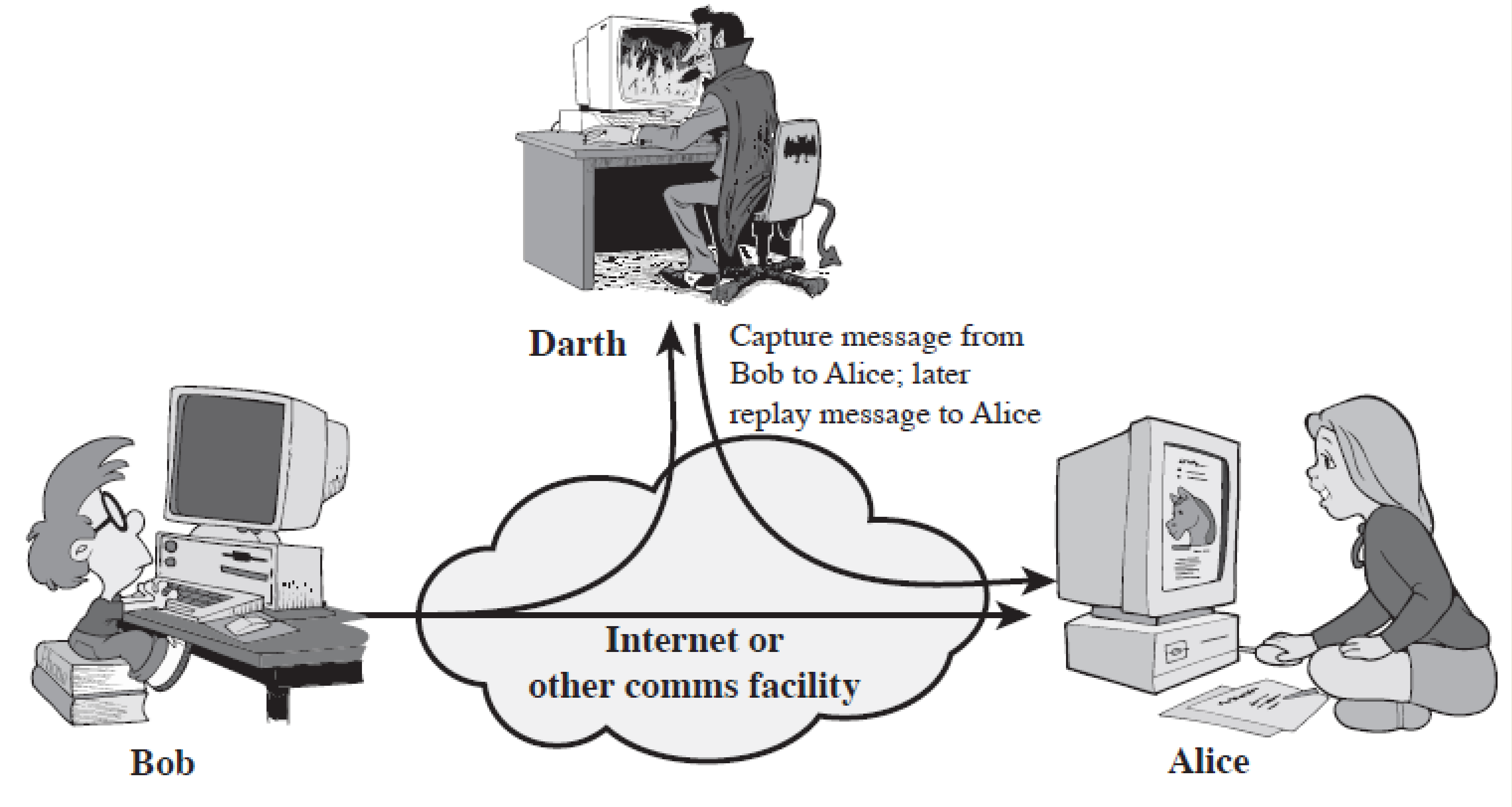
- User A cannot access a server he is authorized to.


Darth
Darth disrupts service provided by server
Bob
Internet or other comms facility
Server

Source: Network security Essentials, 3rd Ed., by William Stallings

Examples of Insecurity: Delay or Replay Attacks

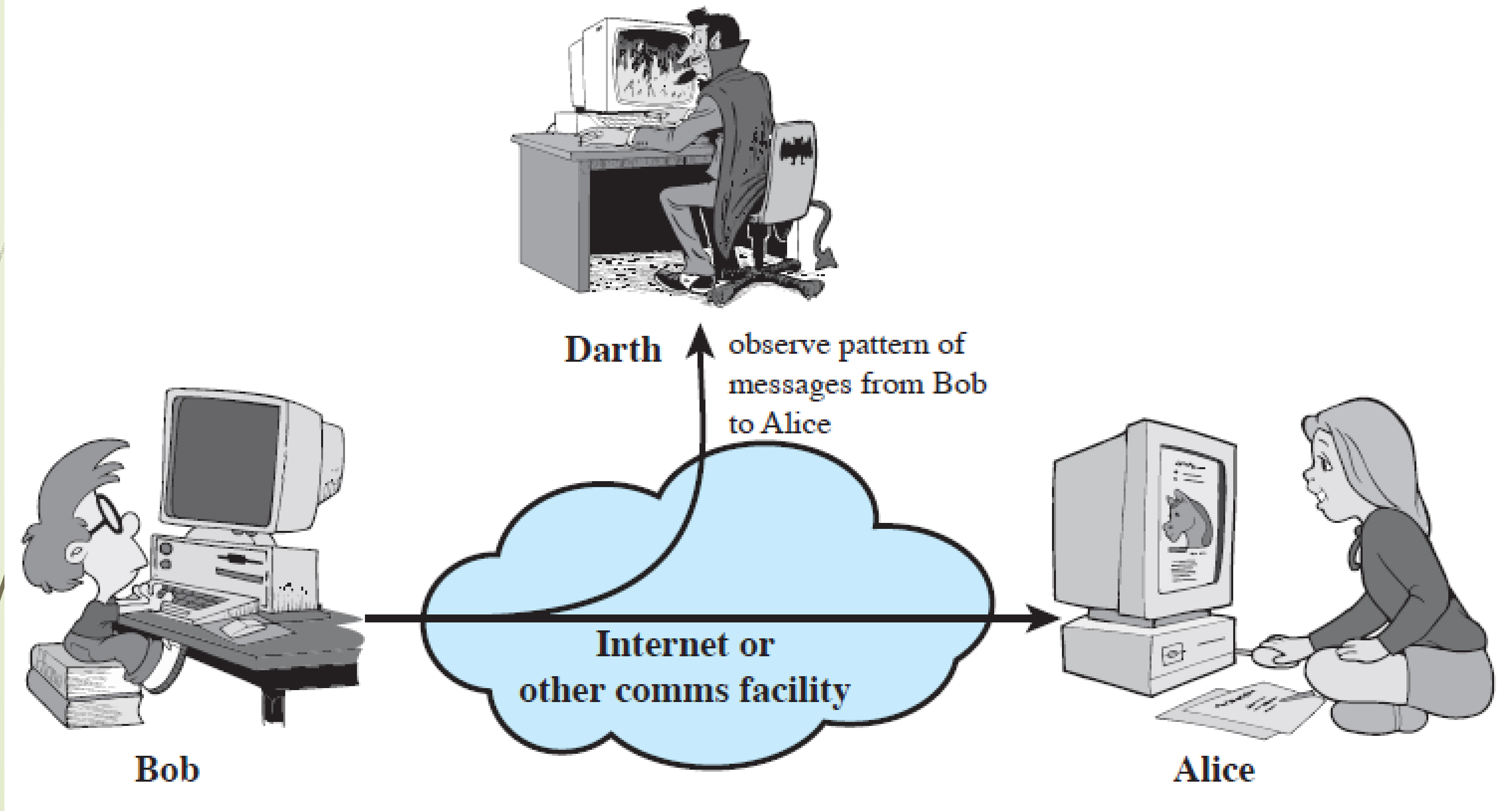
- User C delays, or even duplicates, a message from A to B.


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

Source: Network security Essentials, 3rd Ed., by William Stallings

Examples of Insecurity: Traffic Analysis

- User C analyzes the volume, frequency of messages from A to B.


Darth
observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

Source: Network security Essentials, 3rd Ed., by William Stallings

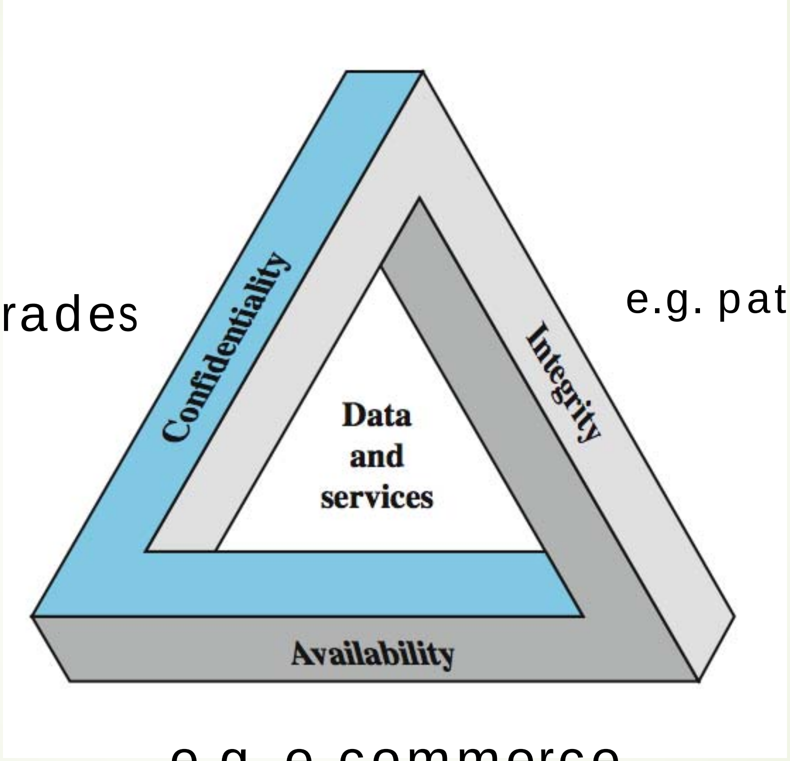
Examples of Insecurity: Repudiation

- User A sends a message to B, but then denies she did.

Key Security Concepts

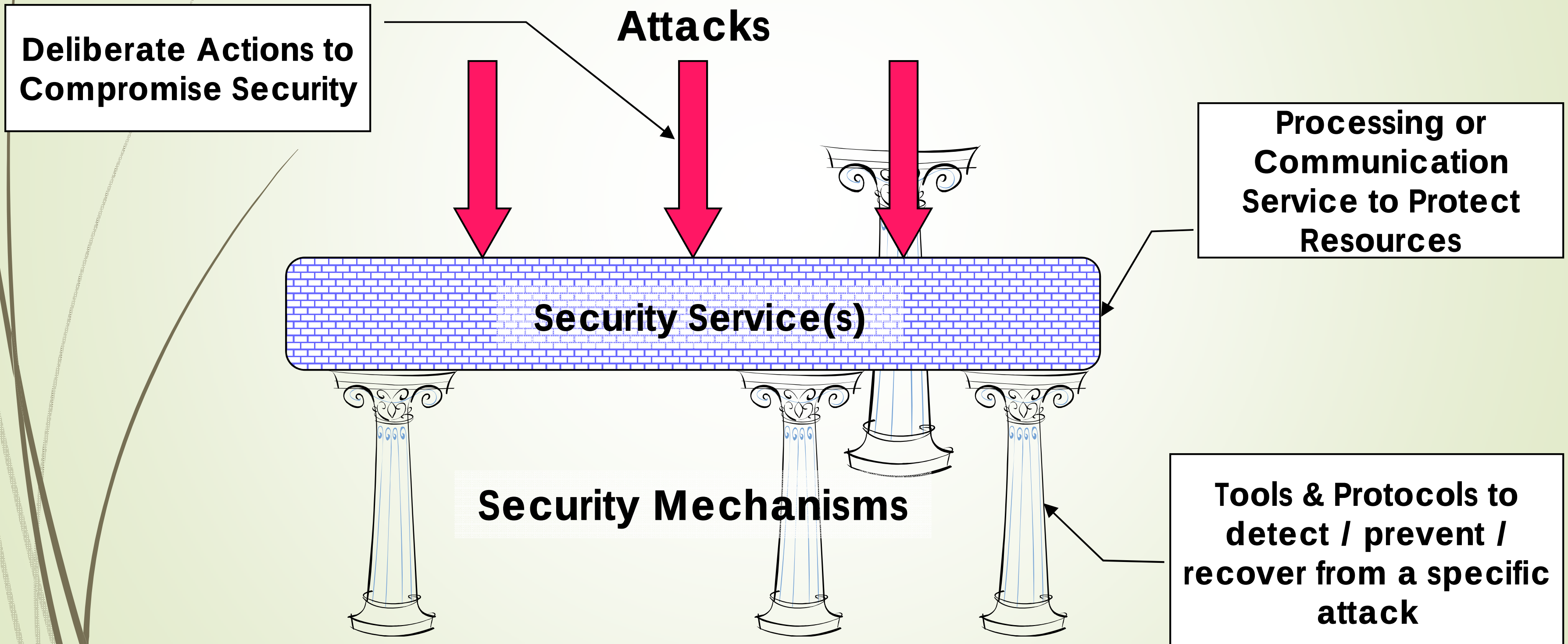
e.g. student grades

e.g. patient information



e.g. e-commerce

Attacks, Services and Mechanisms



Deliberate Actions to Compromise Security
Attacks
Processing or Communication Service to Protect Resources
Security Service(s)
Security Mechanisms
Tools & Protocols to detect / prevent / recover from a specific attack

Security Attacks

- Any action that compromises the security of information owned by an organization. They may be originated from
  - Within the computer itself (Internal Attacks)
  - Outside the computer (External Attacks)
- Security aims to prevent, and detect / recover from, attacks.
- Generic types of attacks:

1. **Passive**:
   - Difficult to detect, yet possible to prevent their success.
2. **Active**:
   - Difficult to prevent, yet possible to detect and recover from.

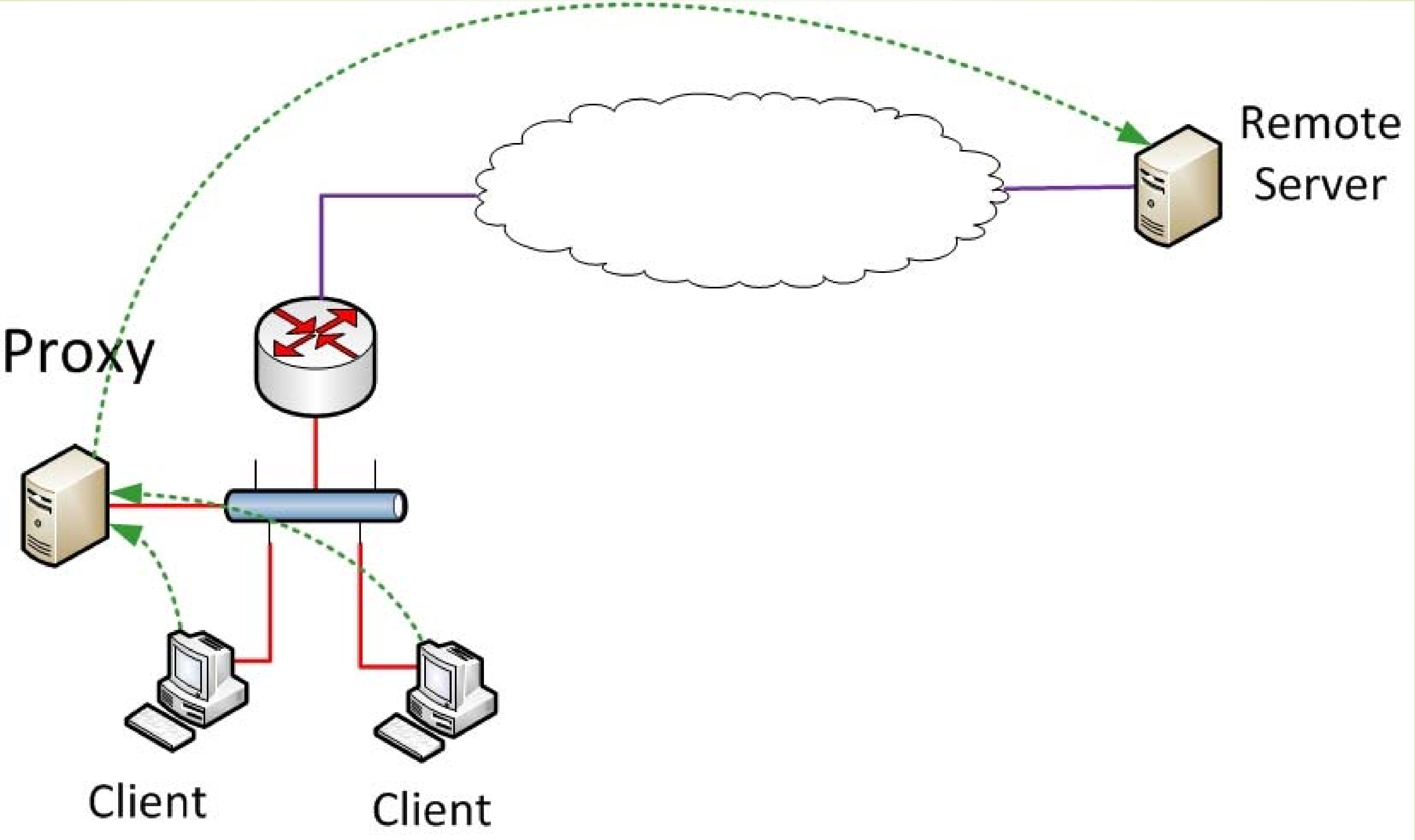
Mitigation of Internal Attacks at the Hardware level

- Regular Users are prohibited from changing the operating parameters of the system: how long they can use the CPU, which memory regions they have access to, what happens when a hardware device needs attention of the O.S., etc.
- CPU Privileges: 2 CPU Modes
  1. Privileged Mode: All instruction can be executed
  2. User Mode: Attempt to execute a privileged instruction (e.g. setting timers, memory management, interrupt handling, communication with devices, changing the privilege level, etc.) is denied by the CPU and control is transferred to the O.S. immediately.
- The O.S. always runs in privileged CPU mode and lowers the level to User Mode just before handing the CPU to a regular user program.
- When User programs are interrupted, say by the timer, the CPU level is automatically elevated to Privileged mode and the CPU is handed to the O.S.

Forms of Attacks

Attack	Description	Mitigation
Virus	Piggyback software attaches itself to local programs	Antivirus software (useless with new viruses)
Worm	Independent programs actively spreading itself across networks	Intrusion Detection Systems
Trojan horse	Infected programs that users download (e.g. games)	Just be wise and pay for the software you use.
Spyware / Sniffers	Collects information on the computer and sends it to the villain attacker.	Auditing the software on your system for abnormal behavior
Phishing	Explicitly asks for your confidential info (Yes, some people proudly give away their secrets)	Authenticate. Spam filters. Proxy Server (next slide)
Denial-of-Service DoS	Flood computers/networks with useless traffic	Traffic filters (Firewalls)

Proxy Servers



Security Services

- A security service is a sort of processing or communication service provided by a system to enhance the security of the system's resources.
- They implement the organization's security polices
- They are implemented by the use of one or more security mechanisms
- Security services are grouped in 5 categories:
  1. Authentication
  2. Access Control
  3. Data Confidentiality
  4. Data Integrity
  5. Nonrepudiation

Security Services: 1- Authentication

The assurance that the communicating entity is the one that it claims to be:

1. ***Peer Entity Authentication***

   - Used in association with an ongoing (established) connection to provide confidence in the identity of the entities connected.

2. ***Data-origin Authentication***

   - In a connectionless transfer, provides assurance that the source of received data is as claimed. No protection against duplication of data. Suitable for e-mail applications.

Security Services: 2- Access Control

The prevention of unauthorized use of a resource (i.e., this service controls

- who can have access to a resource,
- under what conditions access can occur, and
- what those accessing the resource are allowed to do).

Usually, by creating **accounts**: user name + password

- *Administrator* account: Super user who can create, erase, restrict access to the computer
- *Regular user*: has limited access to data, programs, and other resources (e.g. use of printers, network connections, etc.)

Auditing Software

- Record behavior of users and in/out network activity. Helps administrator detect and abnormal behavior

Security Services: 3- Data Confidentiality

The protection of data from unauthorized disclosure.

1. ***Content Confidentiality***
   - The protection of all user data on a connection.
2. ***Traffic-flow Confidentiality***
   - The protection of the information that might be derived from observation of traffic: volume, frequency, peers that are communicating, etc.

Security Services: 4- Data Integrity

The assurance that data received is exactly as sent by an authorized entity (i.e., contain no unauthorized modification, insertion, deletion, or replay).

1. ***Data Integrity with Recovery***

   Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

2. ***Data Integrity without Recovery***

   As above, but provides only detection without recovery.

Security Services: 5- Nonrepudiation

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

1. ***Nonrepudiation, Origin***

   Proof that the message was sent by the specified party even when the sender denies that.

2. ***Nonrepudiation, Destination***

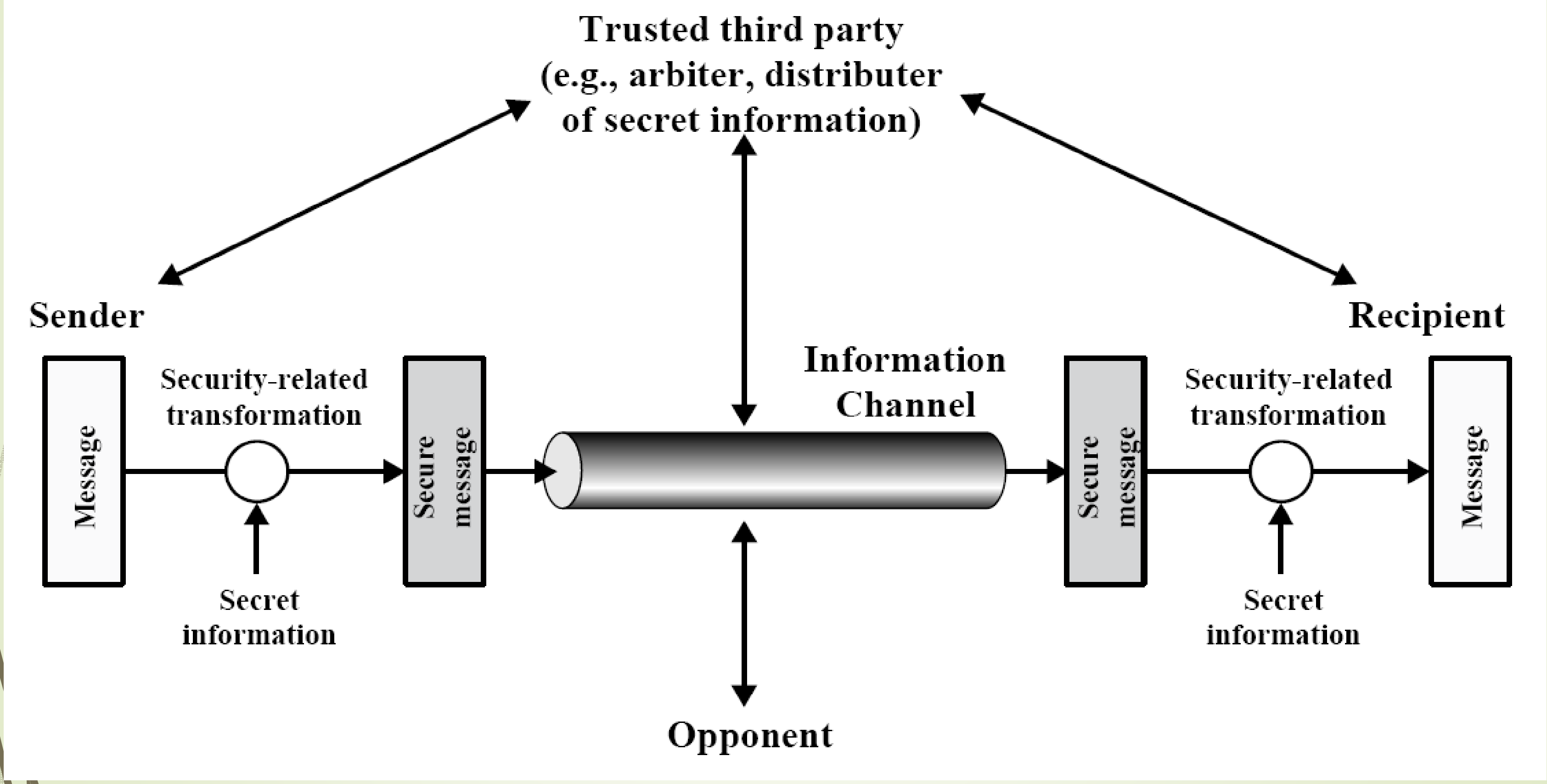
   Proof that the message was received by the specified party even when the receiver denies that.

Security Mechanisms

(*features designed to implement security services*)

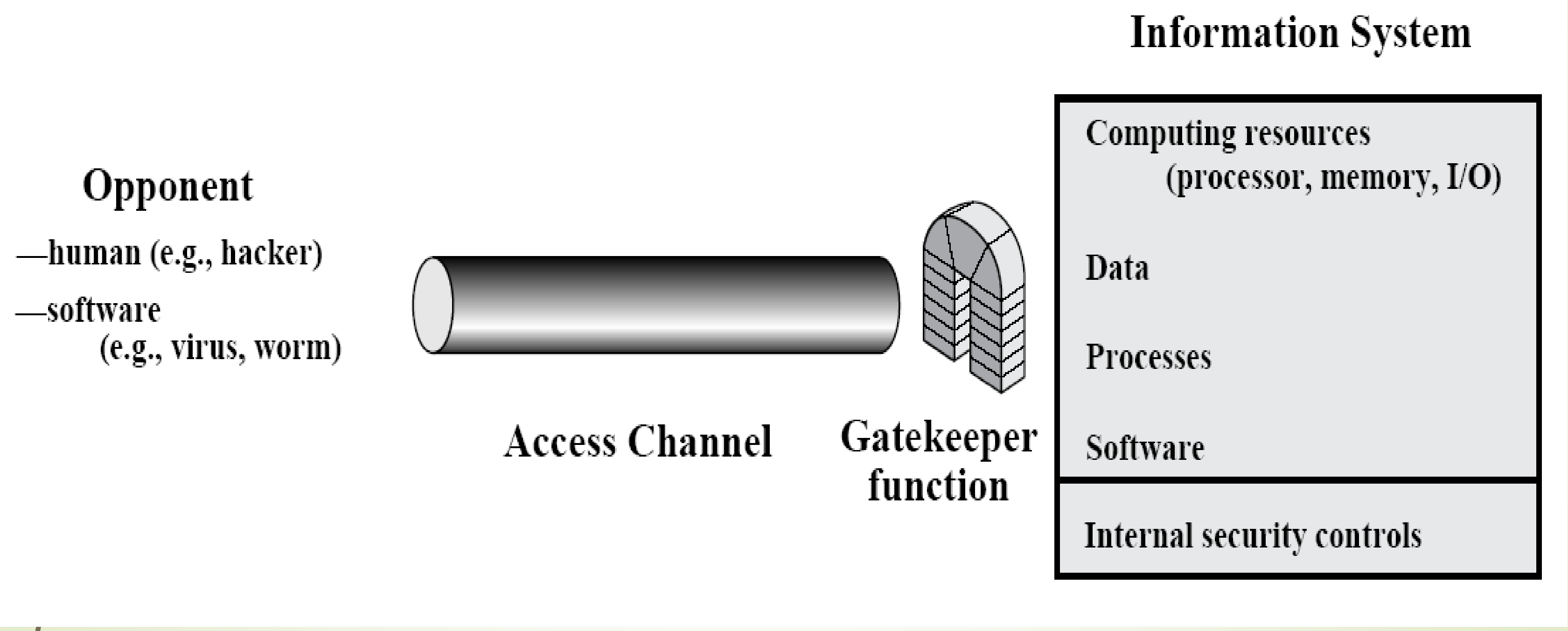
SPECIFIC SECURITY MECHANISMS	
Encryption The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.	**Authentication Exchange** A mechanism intended to ensure the identity of an entity by means of information exchange.
Digital Signature Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).	**Routing Control** Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.
Access Control A variety of mechanisms that enforce access rights to resources.	**Secure Hashing** A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

A Model for Network Security



Source: Network security Essentials, 3rd Ed., by William Stallings

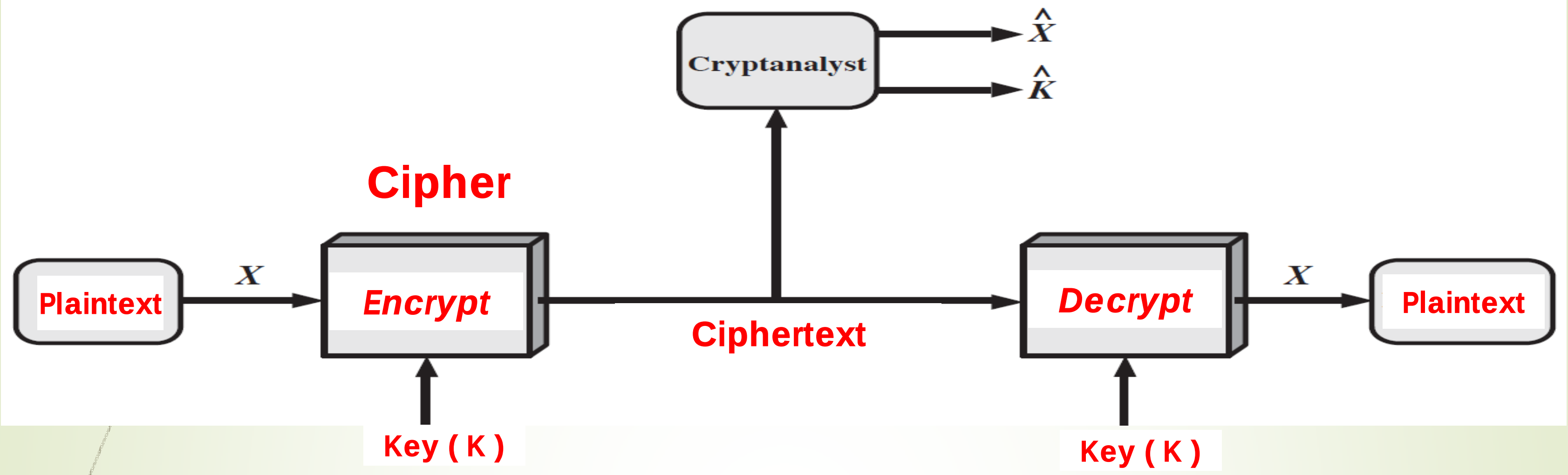
Network Access Security Model



Source: Network security Essentials, 3rd Ed., by William Stallings

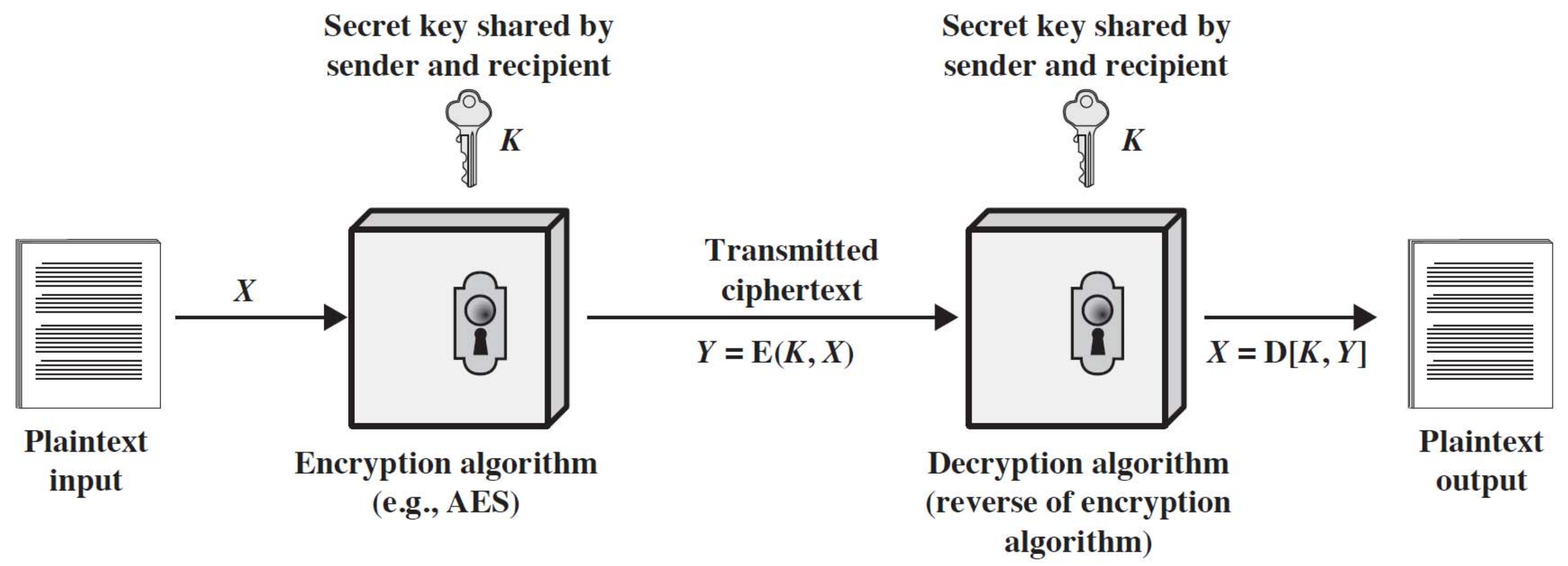
Encryption

Terminology



- **plaintext** - original message
- **ciphertext** - coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering ciphertext from plaintext
- **cryptanalysis (codebreaking)** - study of principles/ methods of deciphering ciphertext *without* knowing key

Symmetric Encryption: A Simplified Model


Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
$Y = E(K, X)$
$X = D[K, Y]$
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

- encryption algorithm is publicly known
- Requirements:

1. a *strong* encryption algorithm
2. a secret key known *only* to sender / receiver

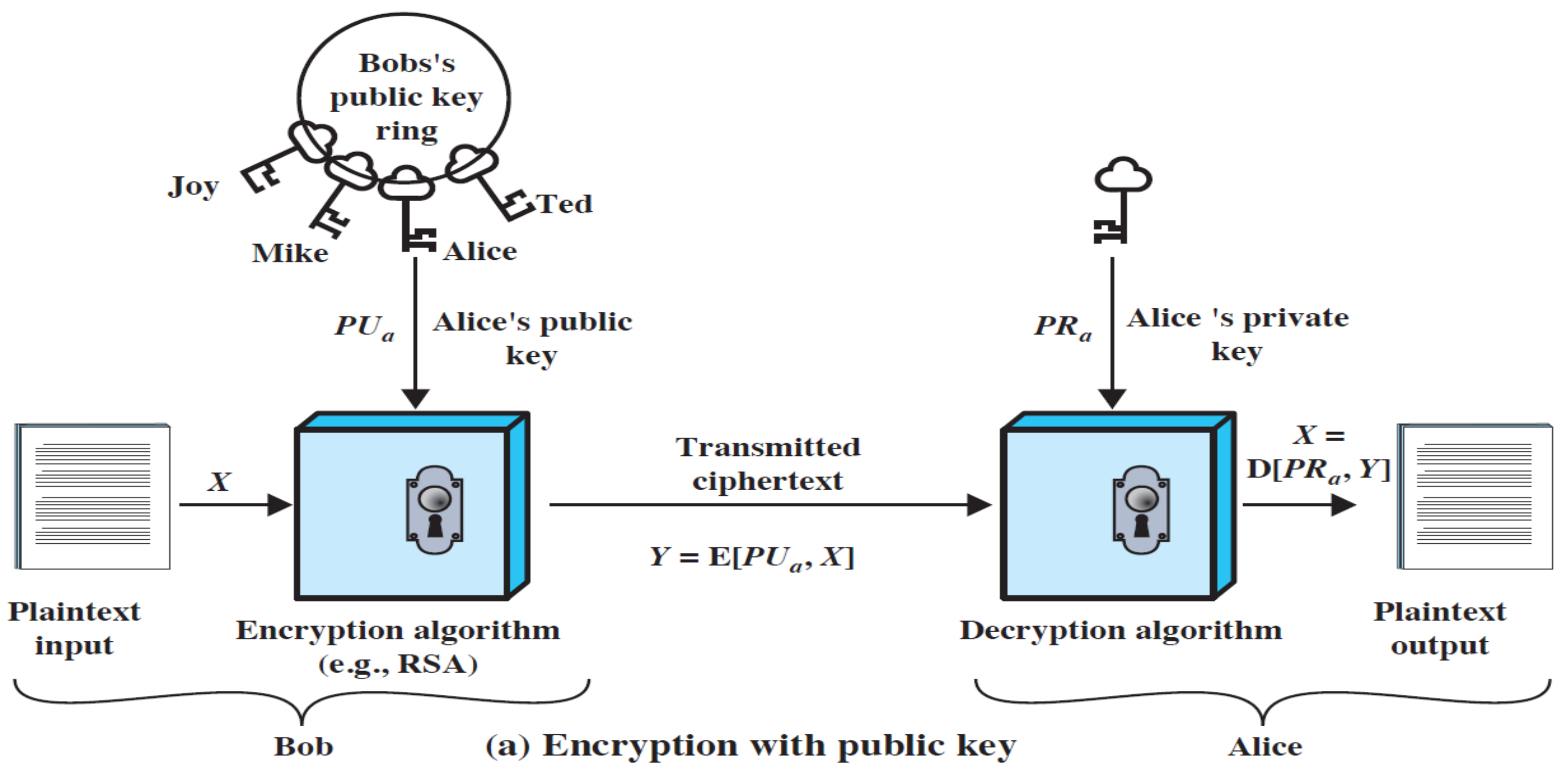
Symmetric Encryption: Characteristics

- Uses **one** key shared by both sender and receiver
- Needs a “secure” *key distribution* mechanism to share the key with *all* involved parties in a group communication.
- In a multi-party session, if one party departs, a *new* key must be used by remaining parties
- If this key is disclosed communications are compromised
- This is a **symmetric**, system, parties, say A and B, are equal
  - hence does not prevent receiver B from forging a message & claiming it was sent by A

Public-Key Encryption

- uses clever application of Number Theory concepts
- complements **rather than** replaces symmetric key encryption
- developed to address two key issues:
  1. **key distribution** – how to have secure communications in general without having to trust a 3rd party (KDC) with your key
  2. **digital signatures** – how to verify a message comes intact from the claimed sender
- You own **two** keys:
  - a **public-key**, which may be known by anyone, and can be used by others to send **encrypt messages** to you, and **verify your signatures** on the message they receive from you.
  - a **private-key**, known only to you, used to **decrypt incoming messages**, and **digitally sign** outgoing messages.
- **asymmetric** since parties are **not** equal
  - Others who encrypt messages for you **cannot** decrypt messages
  - those who verify signatures **cannot** create signatures

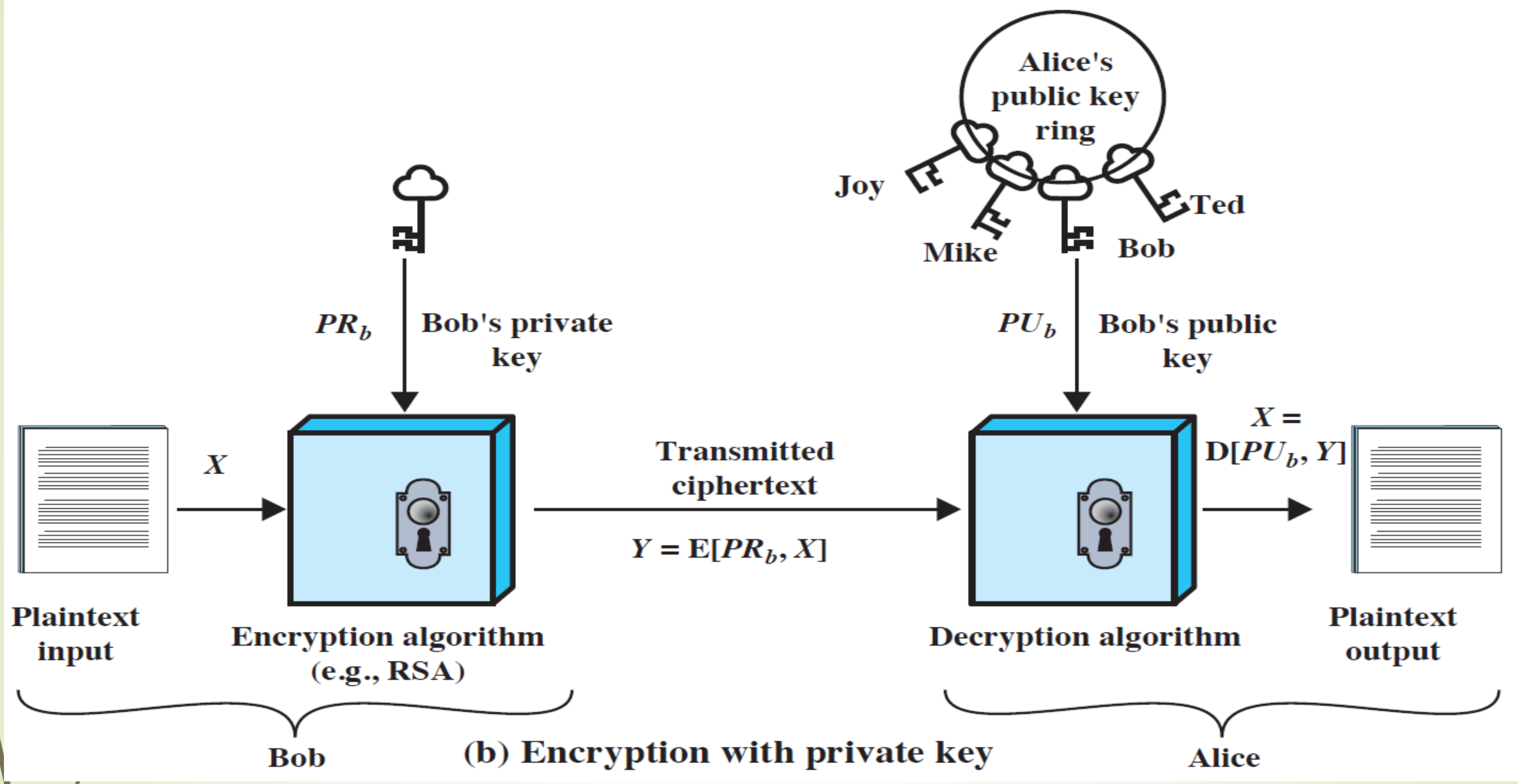
Public-Key Cryptography: Confidentiality



(a) Encryption with public key

1. Can an attacker compromise the secrecy of the document? Why?
2. Can Alice be sure it *is* Bob who sent the message? Why?

Public-Key Cryptography: Authentication



(b) Encryption with private key

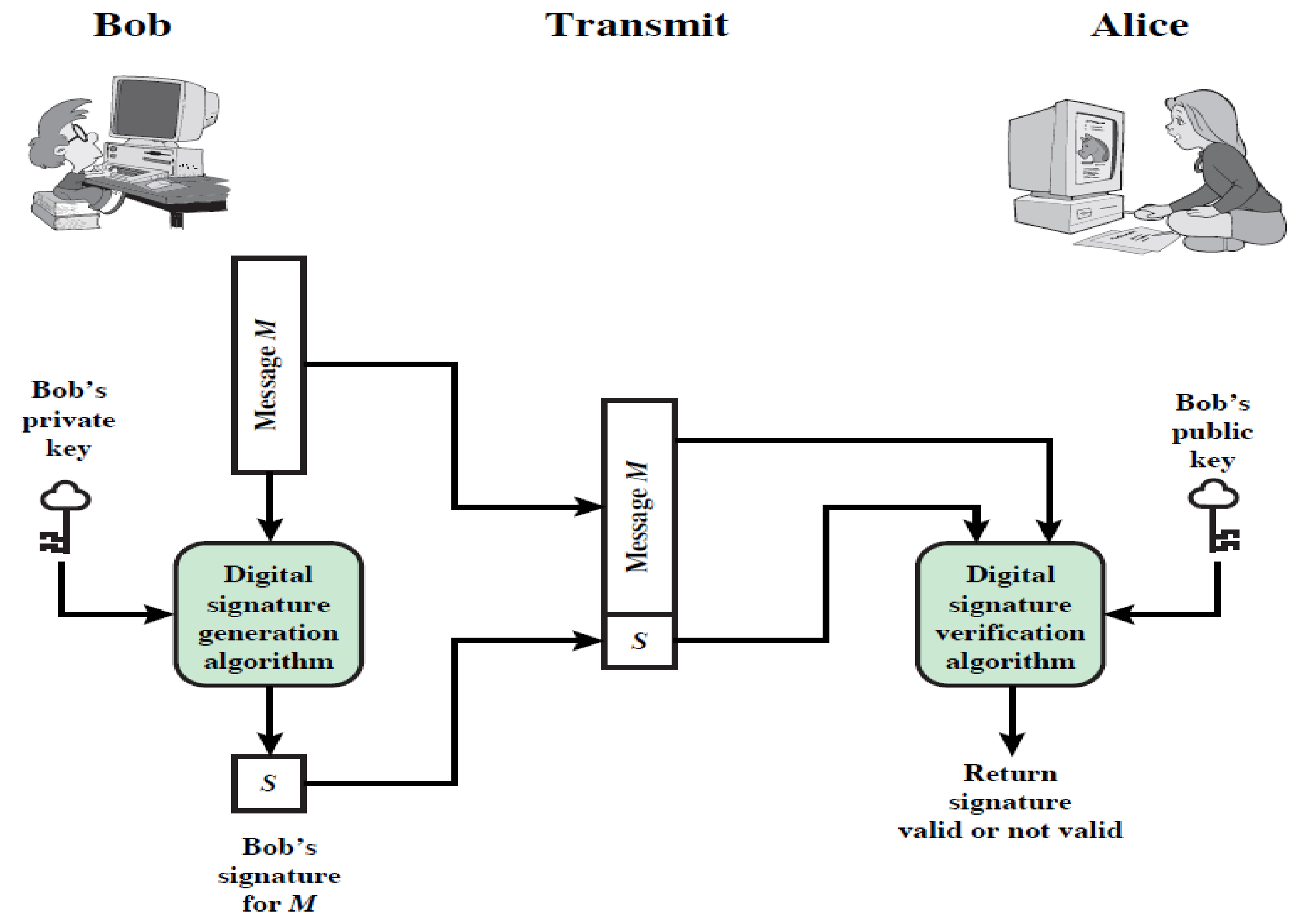
1. Is the secrecy of the document maintained? i.e. is Alice the only one capable of reproducing the plaintext X?
2. Could an attacker alter the Bob's document X without being detected by Alice?

Digital Signatures

Digital Signatures

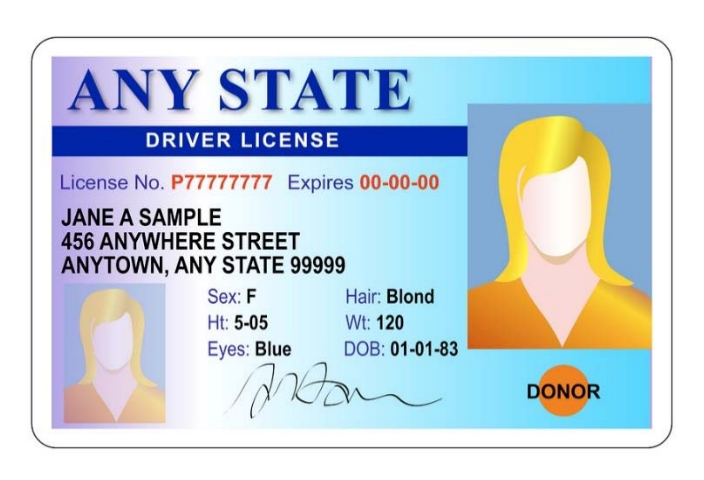
- Similar to handwritten signatures on physical documents
- A **digital signature** indicates the signer's agreement with the contents of an electronic document
- Digital signatures should have these properties:
  - Signer must deliberately sign a document
  - Only the signer can produce his/her signature
  - Cannot move a signature from one document to another document or alter a signed document without invalidating the signature
  - Signatures can be validated by other users, and the signer cannot reasonably claim that he/she did not sign a document bearing his/her signature
  - Signatures can be stored for future dispute resolution

Digital Signatures


Bob
Transmit
Alice
Bob's private key
Message M
Digital signature generation algorithm
S
Bob's signature for M
Message M
S
Bob's public key
Digital signature verification algorithm
Return signature valid or not valid

Source: Network security Essentials, 3rd Ed., by William Stallings

Certificates



ANY STATE

DRIVER LICENSE

License No. P77777777 Expires 00-00-00

JANE A SAMPLE
456 ANYWHERE STREET
ANYTOWN, ANY STATE 99999

Sex: F Hair: Blond
Ht: 5-05 Wt: 120
Eyes: Blue DOB: 01-01-83

DONOR

You say you are My Bank? Prove it!

- How do I know that some public key K really belongs to my bank?
- The bank presents its *public key* and identification information (e.g. name, address, etc.) to a commonly trusted agency (e.g. ViriSign)
- This trusted agency (a.k.a. the *Certification Authority*) generates an electronic document (the *Certificate*) with that information and digitally signs the certificate.
- The Bank presents its name & address + certificate to the client
- The client verifies the CA signature on the certificate,
  - If signature is valid, the client then matches the Bank name, address on the certificate to the information presented by the bank
    - If match, the client uses the Public Key stored inside the certificate to encrypt communication to the Bank
- All of this is done as part of the Secure Sockets Layer (SSL) protocol upon which the HTTPS secure web browsing protocol is built

Network Security and the Law

BCCI SCANDAL: Why Is Washington Stalling?
TIME
Somebody's Watching
How business, government and even the folks next door are tracking your secrets

PopularMechanics
WHO'S SPYING ON YOU?
THE LOOMING THREAT TO YOUR PRIVACY, IDENTITY, AND FAMILY IN THE DIGITAL AGE
Erik Sofge and Davin Coburn

Legal Approaches to Network Security

- Fighting Malware: the **Computer Fraud and Abuse Act of 1984**
  - Prosecuting the introduction of worms and viruses
  - Theft of theft of information
- Protection of Privacy: **Electronic Communication Privacy Act (ECPA) of 1986** and **USA PATRIOT** of 2001
  - Employers monitors employees' communication
  - ISP monitors subscribers
  - government agencies monitor electronic communications under certain restrictions
- Protect against Imposters: **Anticybersquatting Consumer Protection Act of 1999**

Hands-on & On-Line Cryptography Calculators

- Text to Hexadecimal Converter
  http://www.asciitohex.com/
- AES Encryption:
  http://extranet.cryptomathic.com/aescalc/index
- Secure Hashing:
  http://extranet.cryptomathic.com/hashcalc/index
- RSA Encryption:
  http://nmichaels.org/rsa.py