19Z701 - CRYPTOGRAPHY

19Z701 CRYPTOGRAPHY

COMPUTER SECURITY CONCEPTS : The OSI Security Architecture - Security Attacks - Security Services – Security Mechanisms - A Model for Network Security - Number Theory Concepts: Fermat‘s and Euler‘s Theorems, Euclidean Algorithm - Classical Encryption Techniques (5 + 4)

SYMMETRIC CIPHERS : Block Ciphers and Stream Ciphers - Random Bit Generation and Stream Ciphers: Principles of Pseudorandom Number Generation - Pseudorandom Number Generators:Linear Congruential Generators - Block Cipher Modes - Data Encryption Standard (6 + 6)

PUBLIC-KEY CRYPTOGRAPHY : Principles of Public Key Cryptosystems - The RSA Algorithm - Diffie-Hellman Key Exchange - Elliptic Curve Cryptography (5 + 5)

CRYPTOGRAPHIC HASH FUNCTIONS : Secure Hash Algorithm (SHA) - Message Authentication Codes – Message Authentication Requirements - Message Authentication Functions - Digital Signatures - Digital Signature Standard (DSS) - Blockchain: The growth of blockchain technology - Types, Consensus, and Mining Task - Platforms. (6 + 8)

ROLE OF CRYPTOGRAPHY IN SECURITY PROTOCOLS : Network and Internet Security Protocols: Transport-Level Security -Secure Sockets Layer (SSL) - Email Security: Pretty Good Privacy (PGP) - Firewalls: Characteristics and Types (8 + 7)

Total L: 30 +T: 30 = 60

TEXT BOOKS:

1. Hans, Knebl, Helmut, Delfs , "Introduction To Cryptography Principles And Applications", 3rd Edition, Springer- Verlag, Berlin Heidelberg, 2015.

2. William Stallings , "Cryptography and Network Security: Principles and Practice", 7th Edition, Prentice Hall of India, Pearson Education, New Delhi, 2017.

REFERENCES:

1. Behrouz A Forouzan , "Cryptography and Network Security", 3rd Edition, Tata McGraw Hill Ltd, New Delhi, 2015.

2. Atul Kahate , ", Cryptography and Network Security", 3rd Edition, Tata McGraw Hill Ltd, New Delhi, 2013.

3. Imran Bashir , "Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained", 7th Edition, Packt Publishing Ltd, 2018.

4. Douglas Robert Stinson, Maura Paterson , "Cryptography: Theory and Practice", 4th Edition, Chapman and Hall/CRC, 2018.

Course outcomes

CO1: Understand security threats, services, mechanisms and Techniques and illustrate the working of classical ciphers

CO2: Apply number theory concepts for solving symmetric and asymmetric cryptographic techniques.

CO3: Illustrate the working of asymmetric cryptographic techniques and working of cryptographic hash functions.

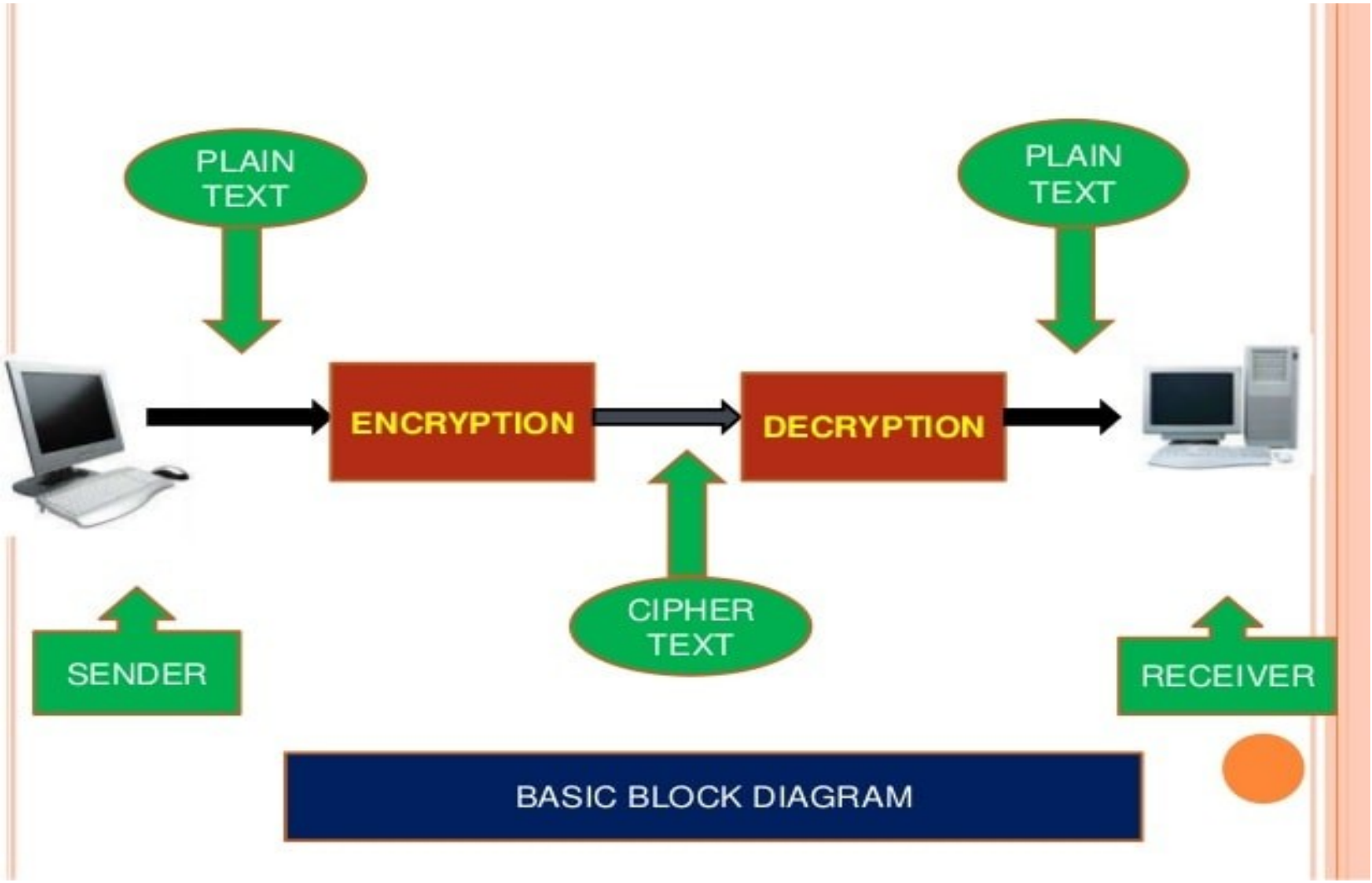
CO4: Describe Message authentication codes, key management and Blockchain

CO5: Explain user authentication protocols, and Network Security protocols

INTRODUCTION

- What is Cryptography?

  - "Hidden Writing"
  - Mainly used to protect Information.


PLAIN TEXT
PLAIN TEXT
ENCRYPTION
DECRYPTION
CIPHER TEXT
SENDER
RECEIVER
BASIC BLOCK DIAGRAM

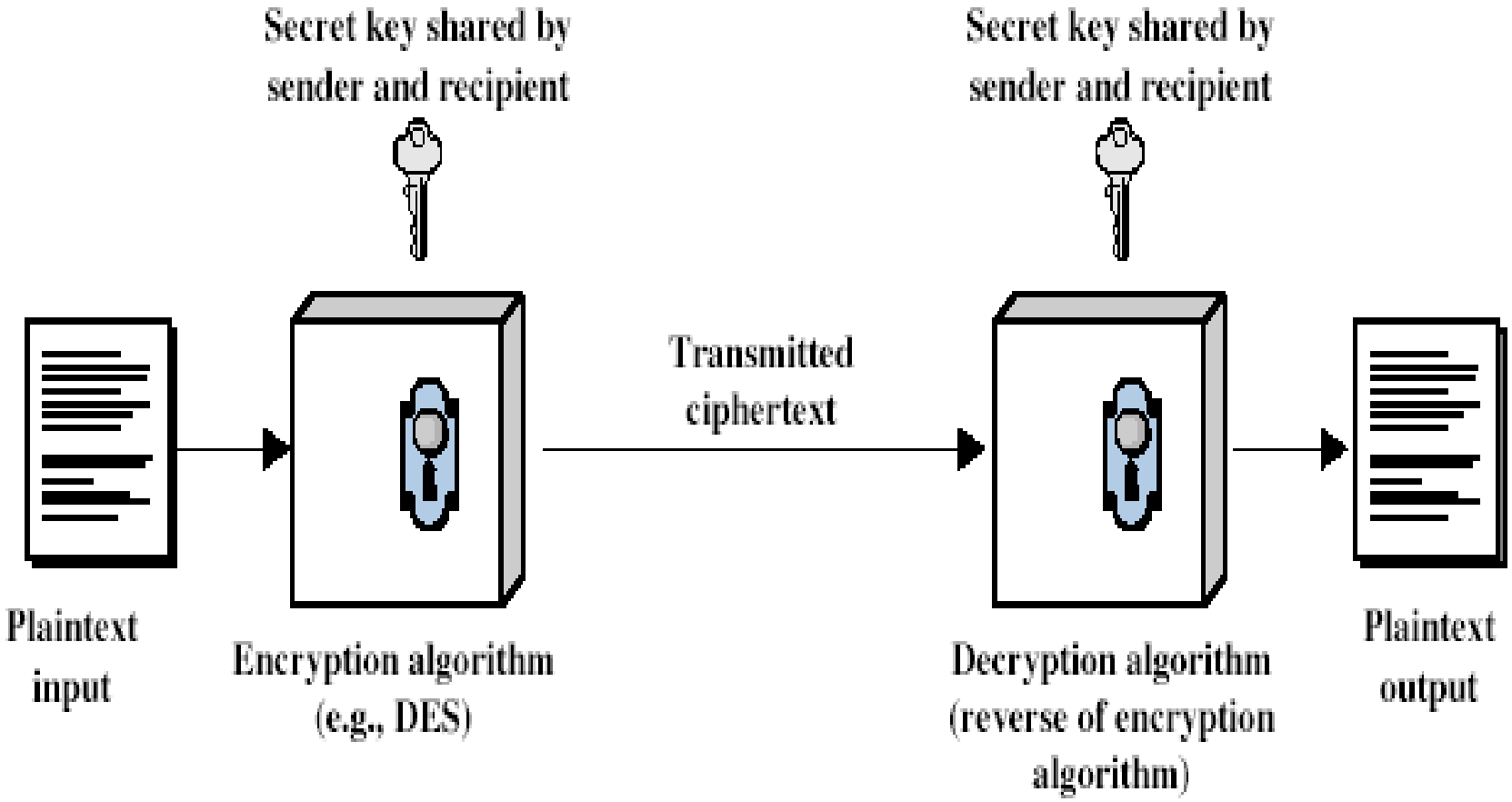
Basic Terminologies

- Encryption
  - Encryption is the process of encoding a message so that its meaning is not obvious
- Decryption
  - Decryption is the reverse process, transforming an encrypted message back into its normal, original form
- Cryptosystem
  - A system for encryption and decryption is called a cryptosystem.

Some Basic 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
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - study of principles/ methods of deciphering ciphertext *without* knowing key
- **cryptology** - field of both cryptography and cryptanalysis

Symmetric Cipher Model



Requirements

- two requirements for secure use of symmetric encryption:
  - a strong encryption algorithm
  - a secret key known only to sender / receiver
- mathematically have:

  $Y = E_K(X)$

  $X = D_K(Y)$
- assume encryption algorithm is known
- implies a secure channel to distribute key

Cryptography

- Cryptographic systems are characterized along three independent dimensions:

1. **The type of operations used for transforming plaintext to ciphertext.** (substitution, transposition).
2. **The number of keys used** (symmetric, public-key encryption)
3. **The way in which the plaintext is processed** (block cipher, stream cipher)

Components of Security

- **Confidentiality, integrity and availability.**
- **CIA triad** is a model designed to guide policies for information security within an organization.
- The model is also sometimes referred to as the AIC triad

The CIA Triad

What is the CIA?		
Confidentiality	**Integrity**	**Availability**
The information is safe from accidental or intentional disclosure.	The information is safe from accidental or intentional modification or alteration.	The information is available to authorized users when needed.
Example		
I send you a message, and no one else knows what that message is.	I send you a message, and you receive exactly what I sent you (without any modification)	I send you a message, and you are able to receive it.
What's The Purpose of the CIA?		
Data is not disclosed	Data is not tampered	Data is available
How Can You Achieve the CIA?		
e.g., Encryption	e.g., Hashing, Digital signatures	e.g., Backups, redundant systems
Opposite of CIA		
Disclosure	Alteration	Destruction

Confidentiality

- Confidentiality is roughly equivalent to privacy.
- Loss of confidentiality :- When information is read or copied by someone not authorized to do so.
- Some information need security like- research data, medical and insurance records, new product specifications, and corporate investment strategies.
- Access must be restricted to those authorized to view the data in question.
- Data to be categorized according to the amount and type of damage that could be done should it fall into unintended hands.

Integrity

- Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle.
- Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people.
- Loss of integrity :- When information is modified in unexpected ways .

Availability

- Availability of information refers to ensuring that authorized parties are able to access the information when needed.
- Information only has value if the right people can access it at the right times.
- Information can be erased or become inaccessible, resulting in loss of availability.
- Availability is often the most important attribute in service-oriented businesses that depend on information .
- When users cannot access the network or specific services provided on the network, they experience a denial of service.

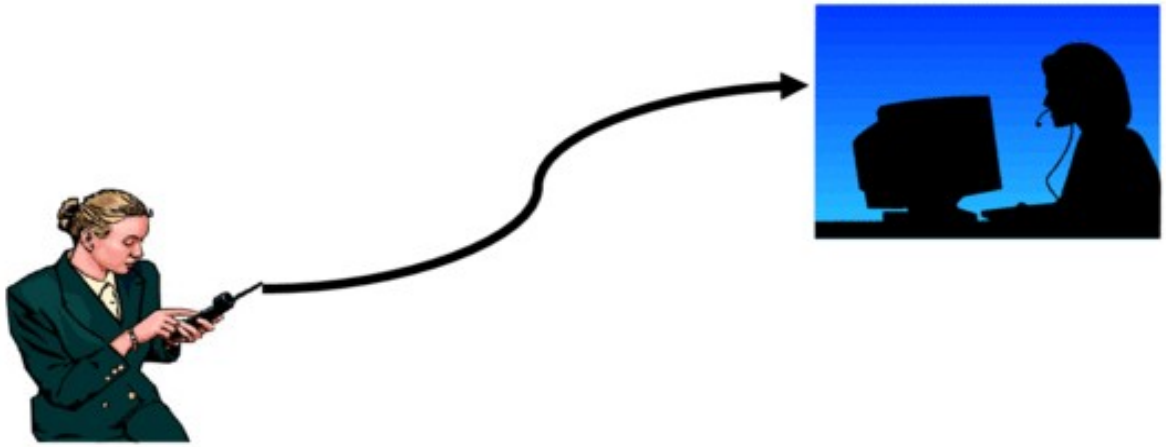
Threat

– **Threat:-** a potential for violation of security

- **Physical threats - weather, natural disaster, bombs, power etc.**
- **Human threats - stealing, trickery, spying, sabotage, accidents.**
- **Software threats - viruses, Trojan horses, logic bombs.**

Network Security

Normal Flow:



Network Security

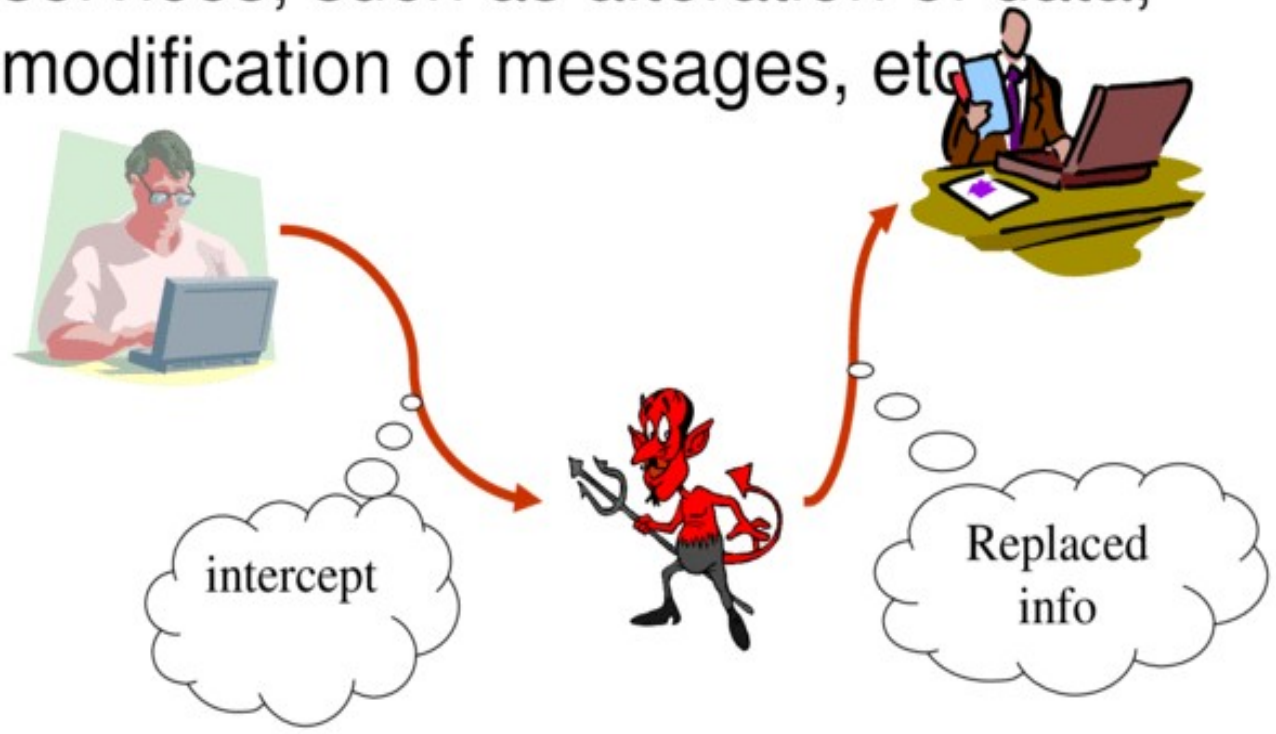
- **Four types of possible attacks are:**

1. ***Interruption***: services or data become unavailable, unusable, destroyed, and so on, such as lost of file, denial of service, etc.

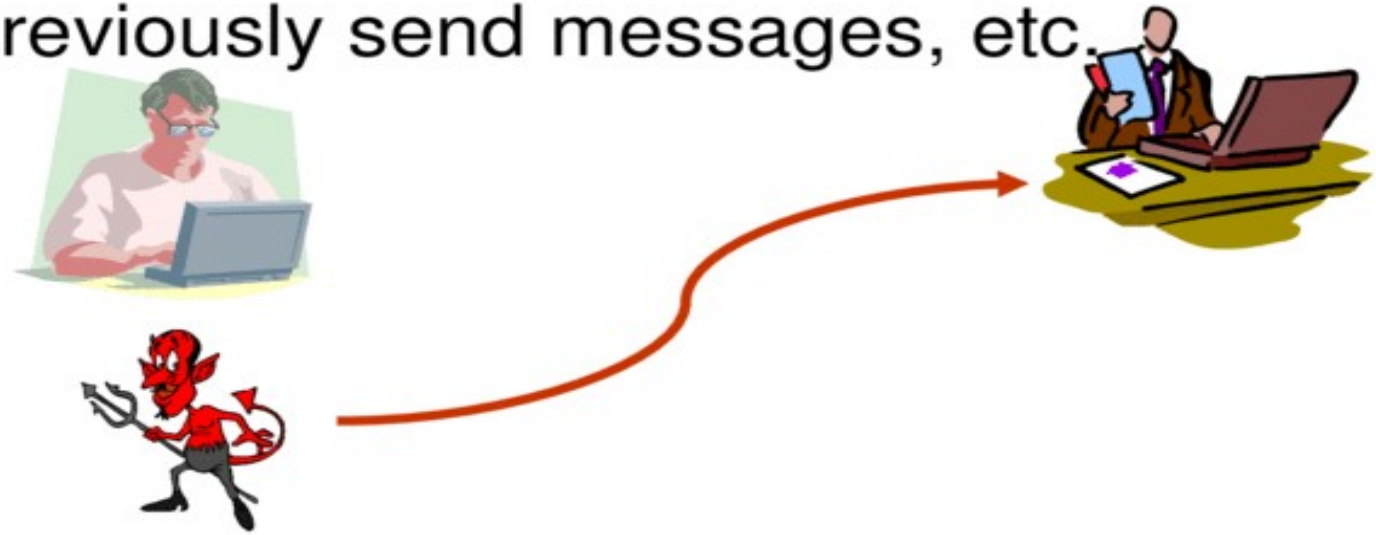
Cut wire lines,
Jam wireless
signals,
Drop packets,

- ***2. Interception:*** an unauthorized subject has gained access to an object, such as stealing data, overhearing others communication, etc.

3. Modification: unauthorized changing of data or tempering with services, such as alteration of data, modification of messages, etc



4. Fabrication: additional data or activities are generated that would normally no exist, such as adding a password to a system, replaying previously send messages, etc.



Also called impersonation

OSI Security Architecture

. OSI : Open System Interconnection
. ITU : International Telecommunication Union

- ITU-T X.800 ªSecurity Architecture for OSIº
- defines a systematic way of defining and providing security requirements
- for us it provides a useful, if abstract, overview of concepts we will study

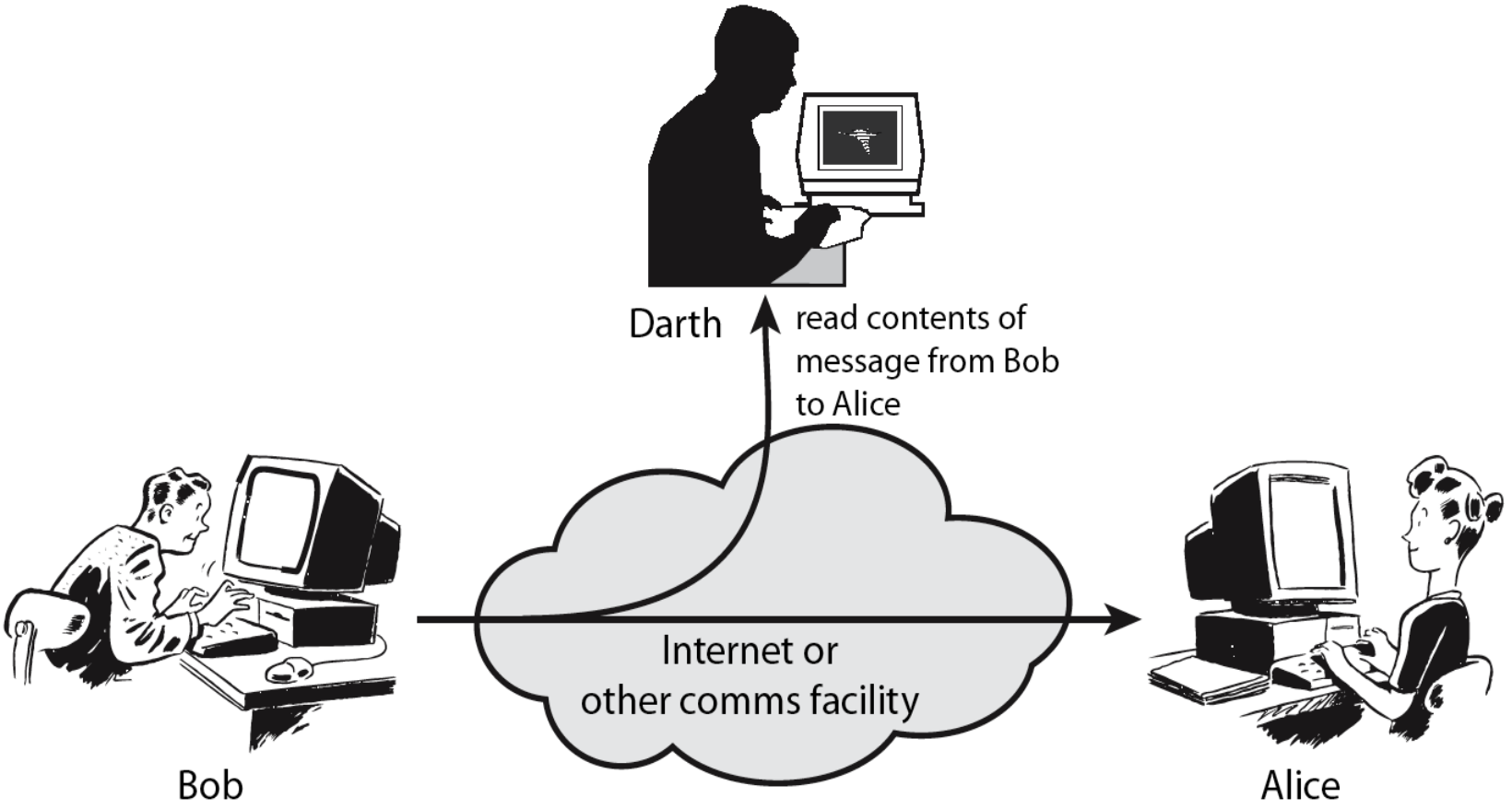
Aspects of Security

- consider 3 aspects of information security:
  - **security attack**
  - **security mechanism**
  - **security service**

Security Attack

- any action that compromises the security of information owned by an organization
- information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- often *threat* & *attack* used to mean same thing
- have a wide range of attacks
- can focus of generic types of attacks
  - passive
  - active

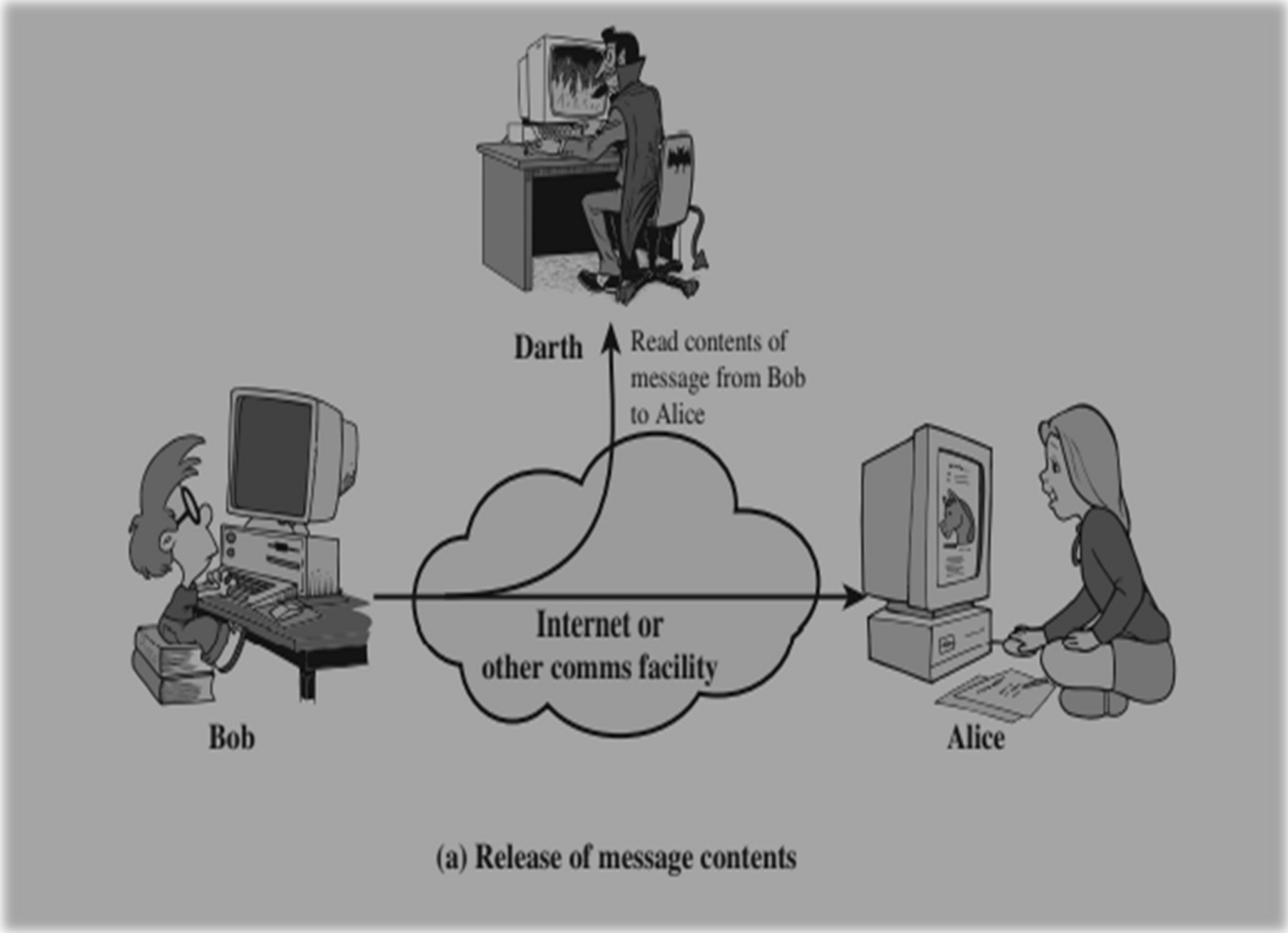
Passive Attacks



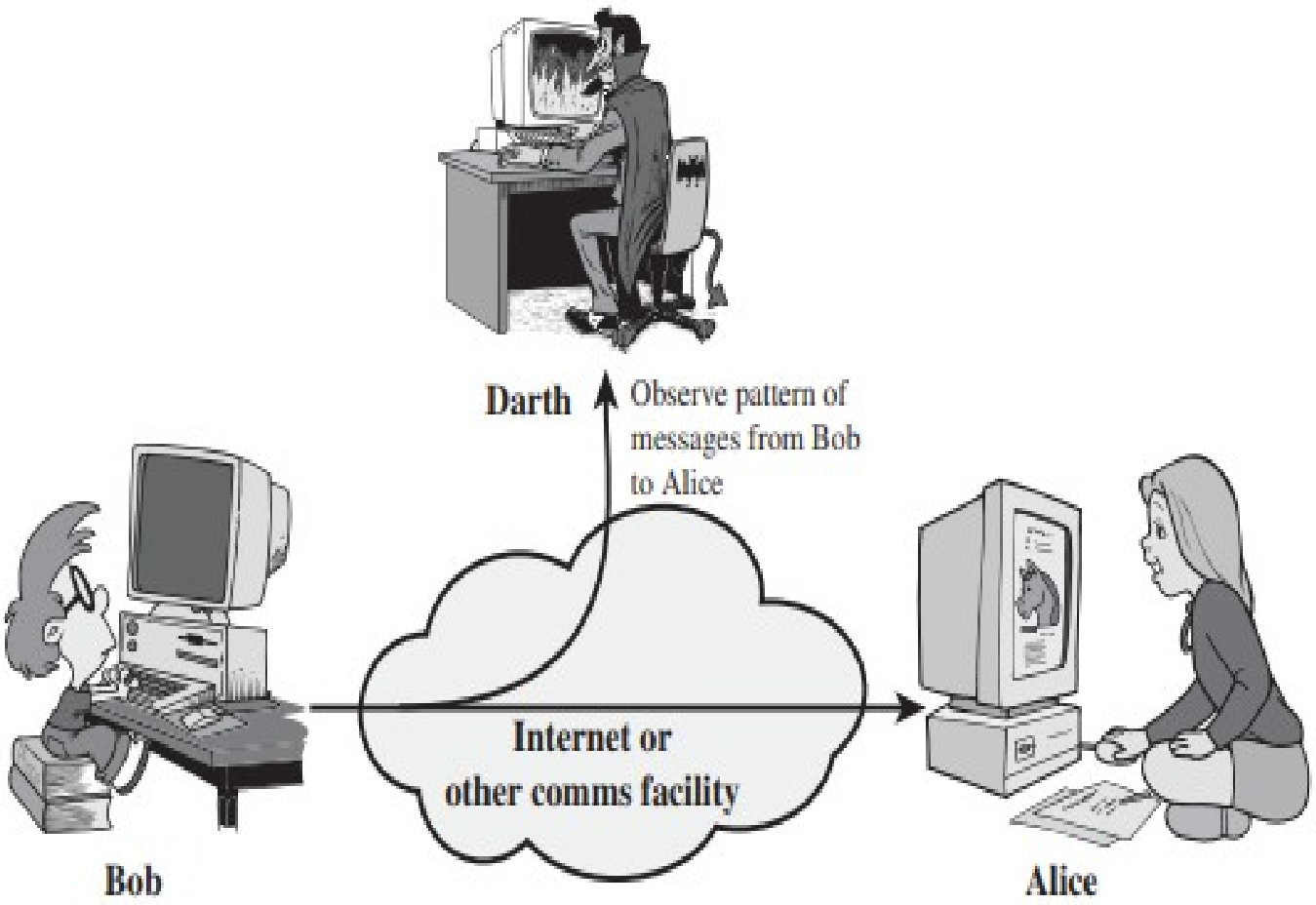
Passive Attacks

- Are in the nature of eavesdropping on, or monitoring of, transmissions
- Goal of the opponent is to obtain information that is being transmitted

- Two types of passive attacks are:
  - The release of message contents
  - Tr[illegible]lysis

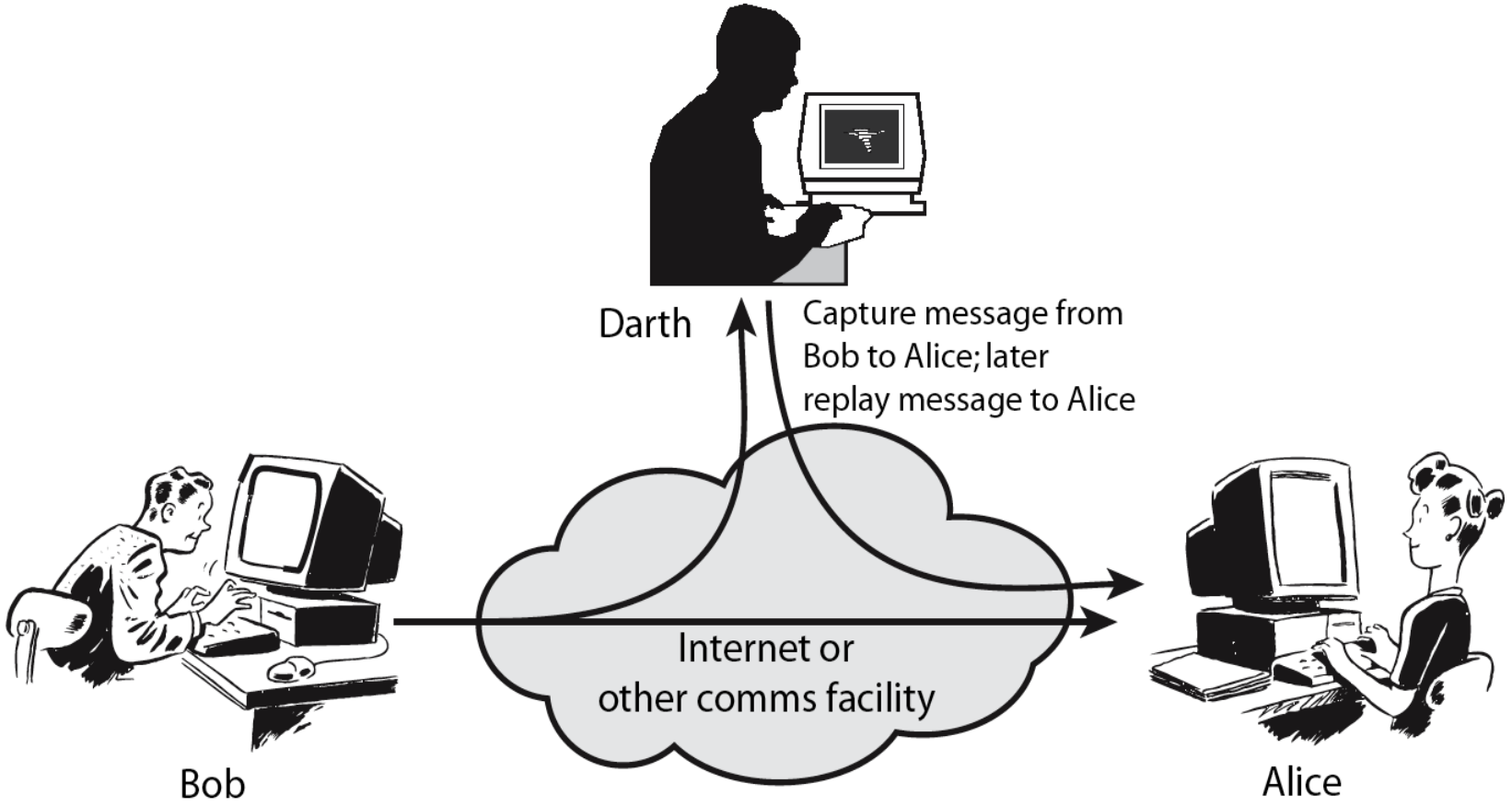


(a) Release of message contents



(b) Traffic analysis

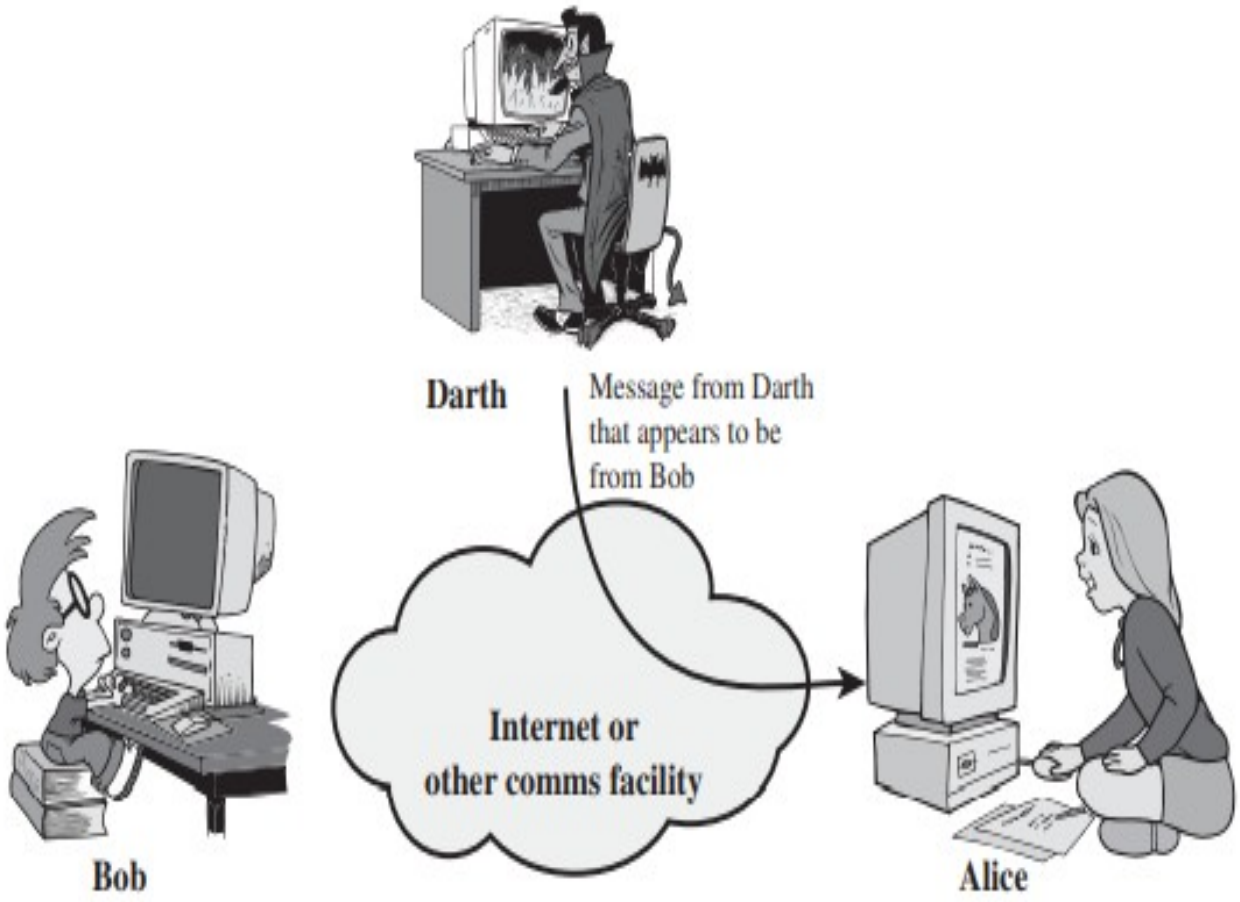
Active Attacks



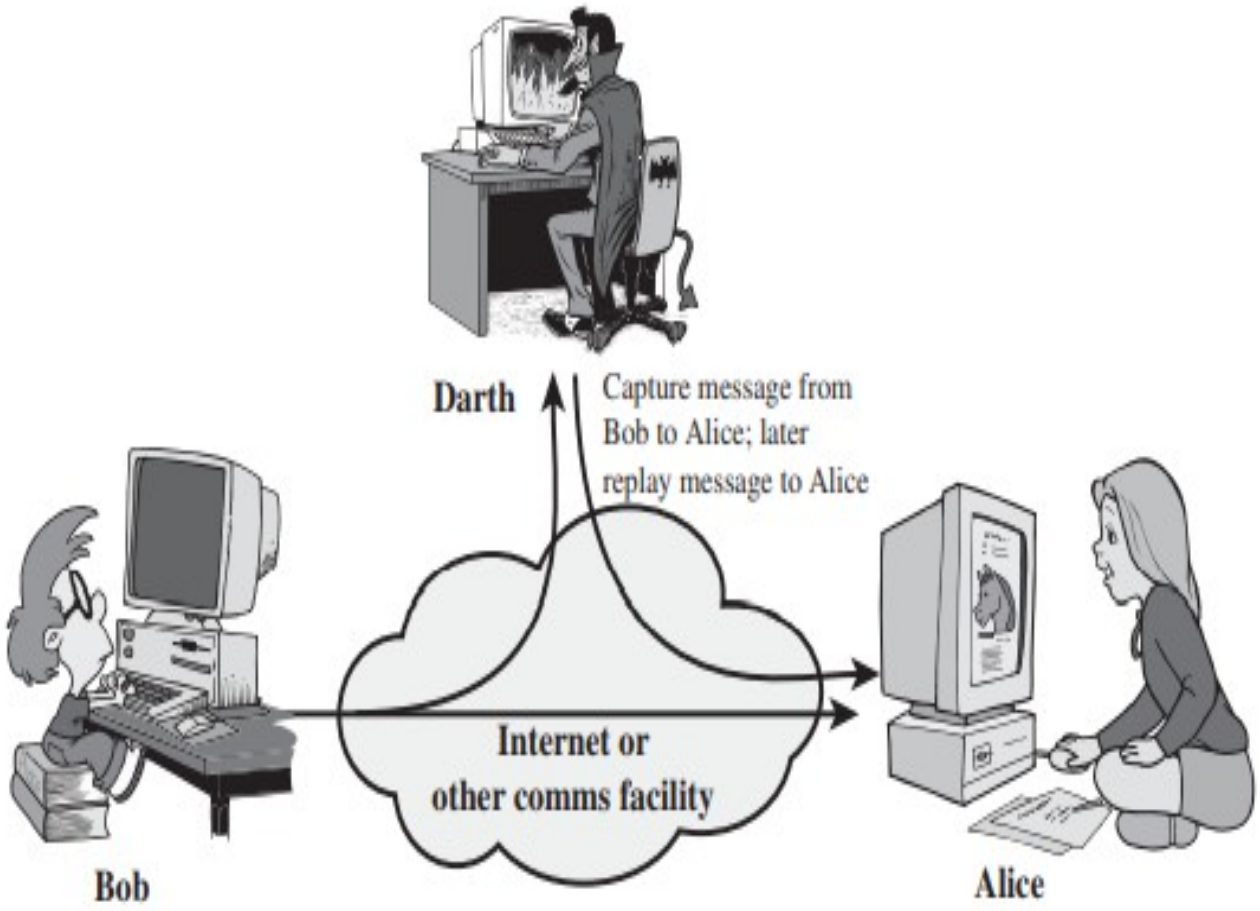
Active Attacks

- Involve some modification of the data stream or the creation of a false stream
- Difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities
- Goal is to detect attacks and to recover from any disruption or delays caused by them

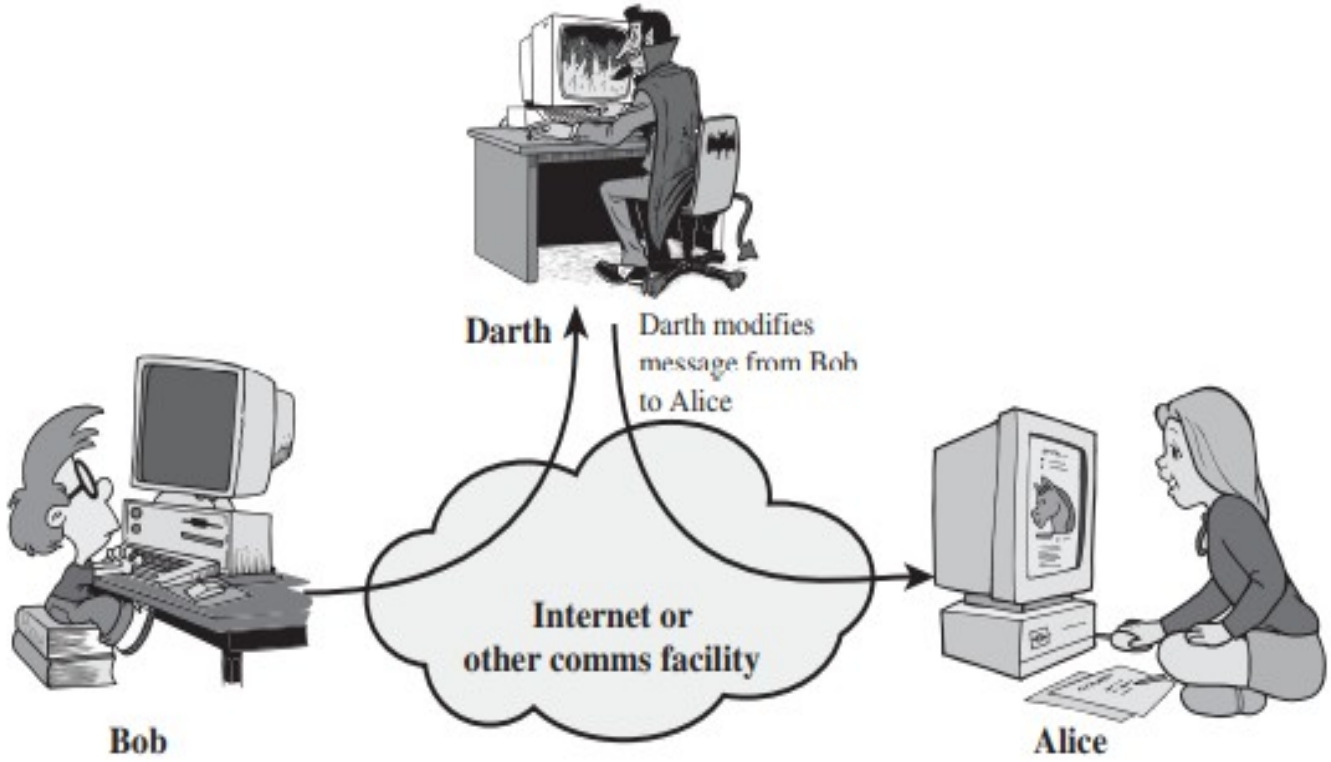
Masquerade	• Takes place when one entity pretends to be a different entity • Usually includes one of the other forms of active attack
Replay	• Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect
Modification of messages	• Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect
Denial of service	• Prevents or inhibits the normal use or management of communications facilities



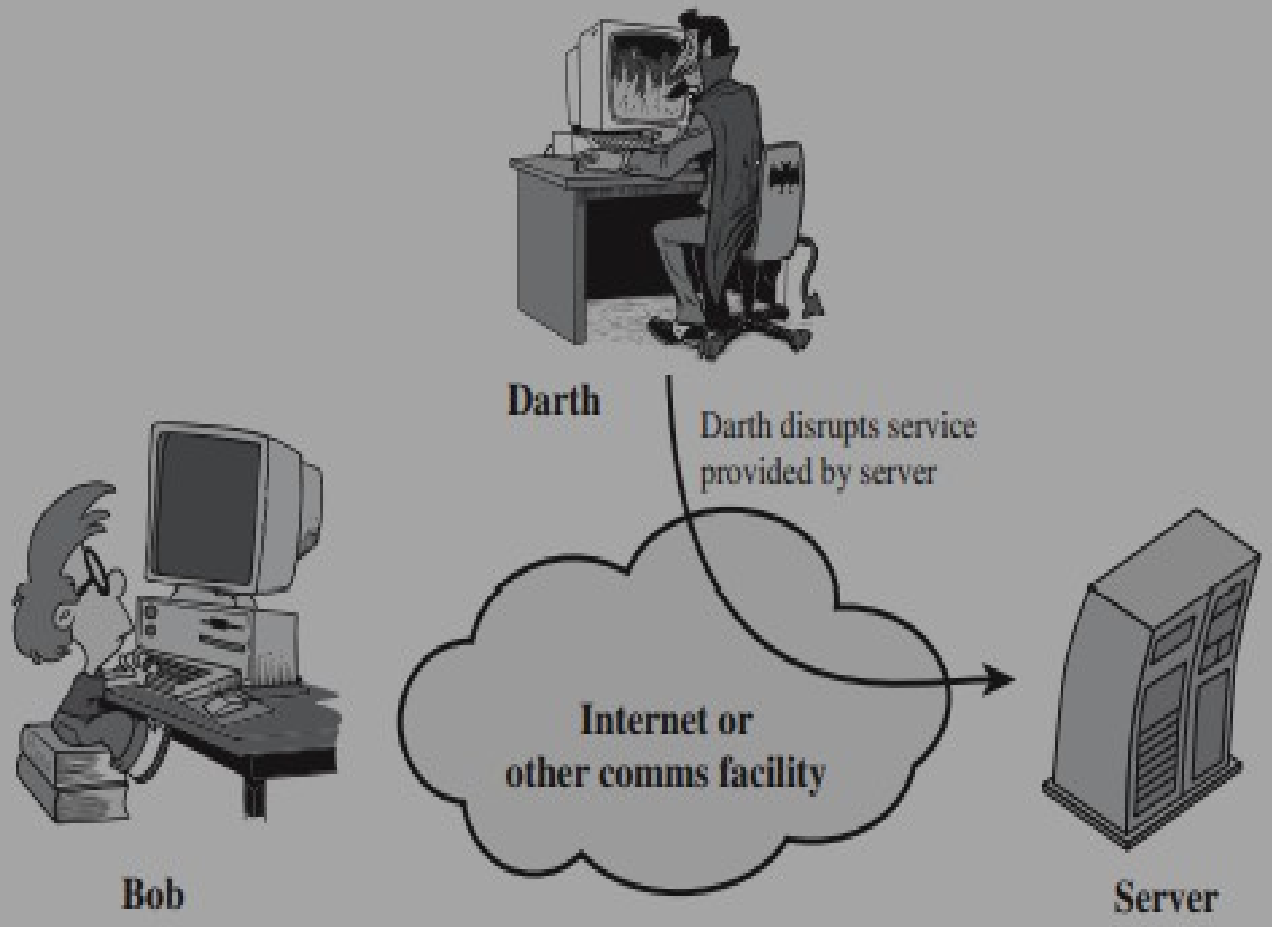
(a) Masquerade


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

(b) Replay



(c) Modification of messages



(d) Denial of service

Security Service

- enhance security of data processing systems and information transfers of an organization
- intended to counter security attacks
- using one or more security mechanisms
- often replicates functions normally associated with physical documents
  - which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

Security Services (X.800)

- **Authentication** - assurance that the communicating entity is the one claimed
- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** –protection of data from unauthorized disclosure
- **Data Integrity** - assurance that data received is as sent by an authorized entity
- **Non-Repudiation** - protection against denial by one of the parties in a communication

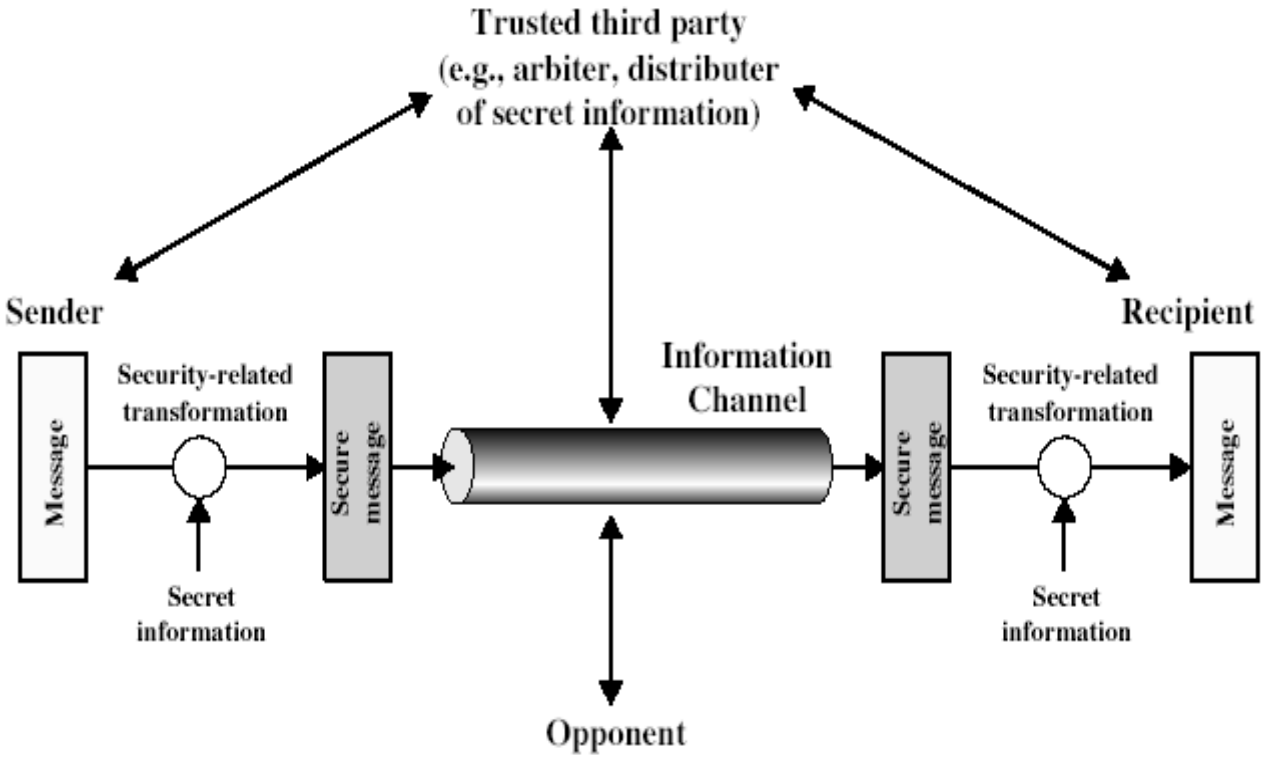
Security Mechanism

- feature designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all services required
- however one particular element underlies many of the security mechanisms in use:
  - **cryptographic techniques**
- hence our focus on this topic

Security Mechanisms (X.800)

- specific security mechanisms:
  - encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
- pervasive security mechanisms:
  - trusted functionality, security labels, event detection, security audit trails, security recovery

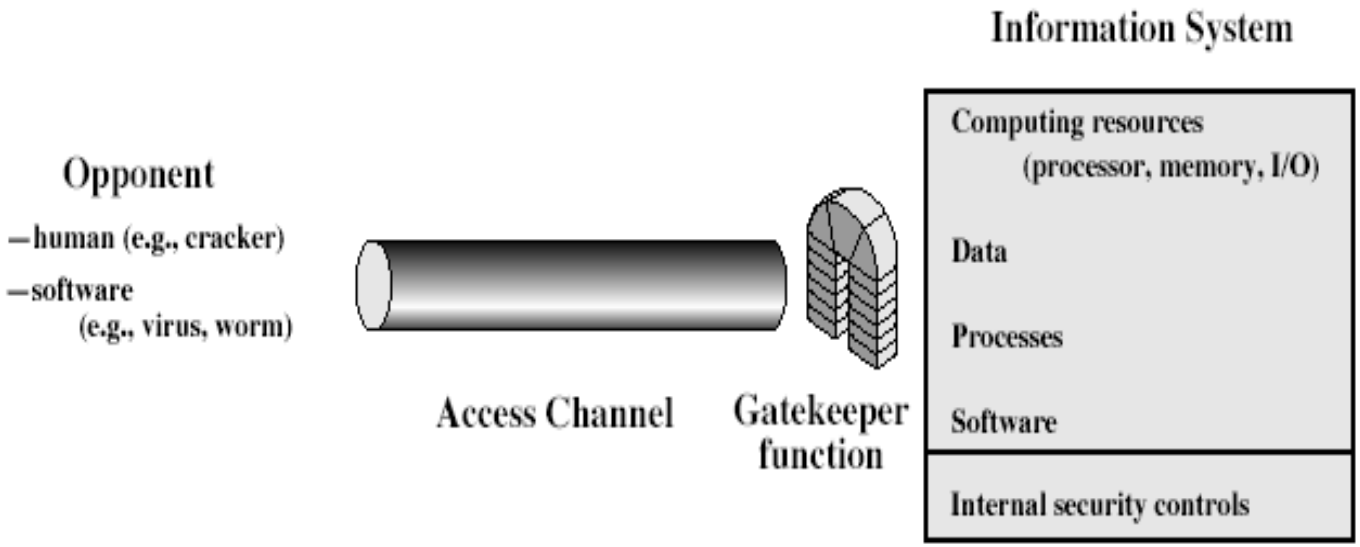
Model for Network Security



Model for Network Security

- using this model requires us to:
  1. design a suitable algorithm for the security transformation
  2. generate the secret information (keys) used by the algorithm
  3. develop methods to distribute and share the secret information
  4. specify a protocol enabling the principals to use the transformation and secret information for a security service

Model for Network Access Security



Model for Network Access Security

- using this model requires us to:
  1. select appropriate gatekeeper functions to identify users
  2. implement security controls to ensure only authorised users access designated information or resources
- trusted computer systems may be useful to help implement this model

Thank You