Overview

By Purvi Tandel

Information Security

Information security within an organization have undergone two major changes in last decades.

Computer Security:

The generic name for the collection of tools designed to protect data and to thwart hackers is computer security.

Network Security:

Measures that are needed to protect data during transmission.

By Purvi Tandel

The OSI Security Architecture

The OSI (Open Systems Interconnection) security architecture provides a systematic framework for defining security attacks, mechanisms and services.

Mainly 3 aspects for Information Security:

- ✓Security Attack
- ✓Security Mechanisms
- ✓Security Services

By Purvi Tandel

Security Attack: Any action that compromises the security of information owned by an organization.

Security Mechanisms: A process that is designed to detect, prevent, or recover from security attack.

Security Services: A communication service that enhances the security of the data processing systems and the information transfers of an organization.

Attack:

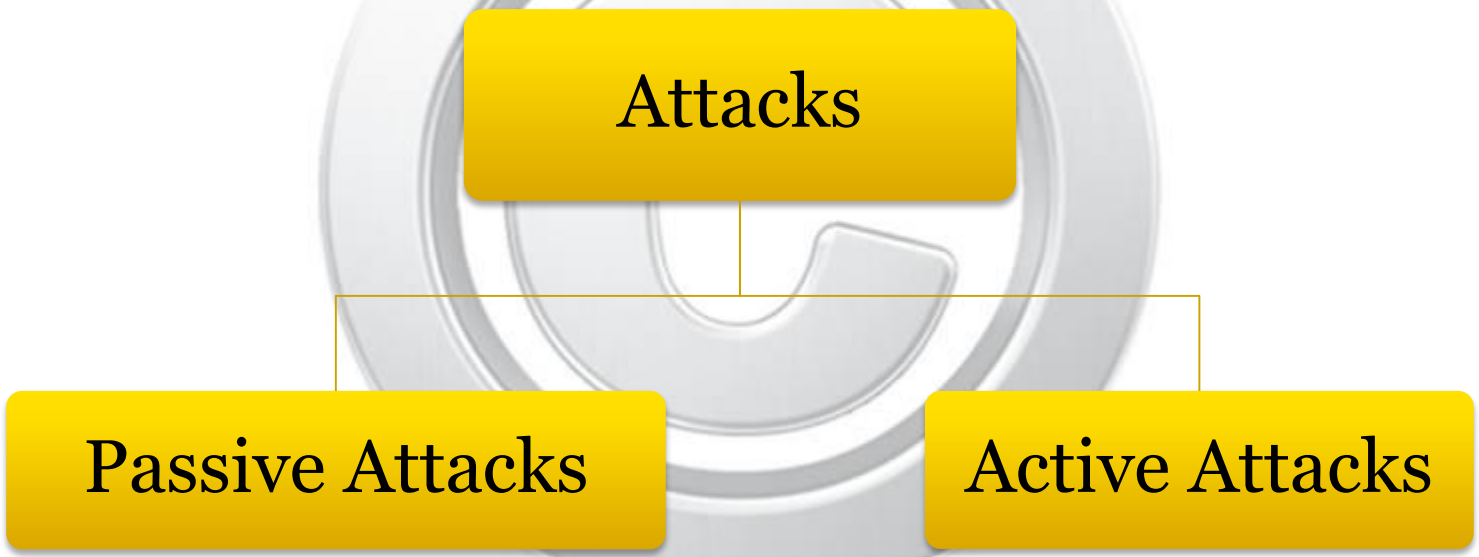
Any action that compromises the security of information owned by an organization.

Threat:

Threat is a possible danger that might exploit a valnerability.

By Purvi Tandel

Security Attacks



By Purvi Tandel

Security Attacks

Passive Attacks

Passive attacks do not involve any modification to the contents of an original message.

- ✓ Release of message contents
- ✓ Traffic analysis

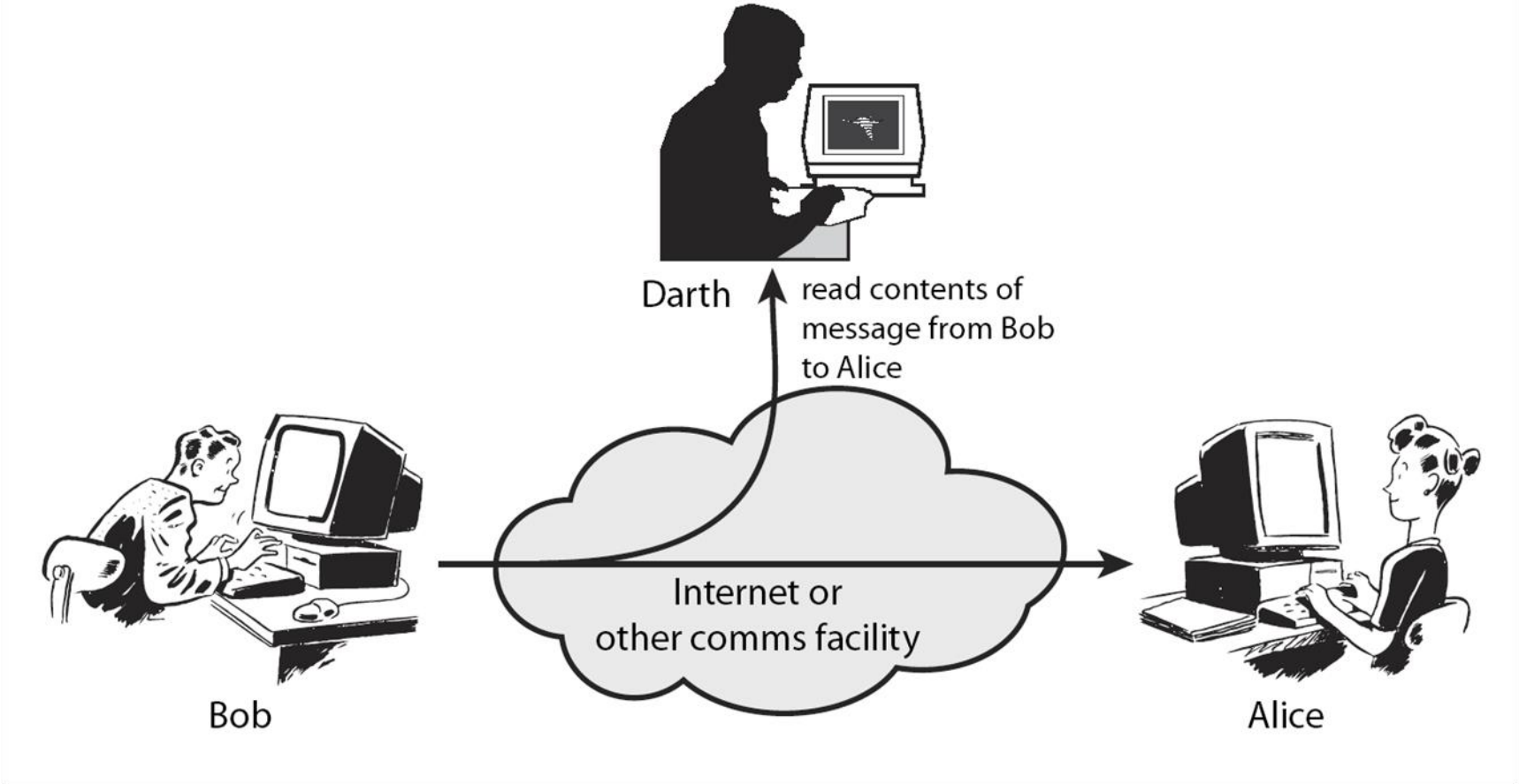
Active Attacks

In Active attacks, the contents of the original message are modified in some way.

- ✓ Masquerade
- ✓ Replay
- ✓ Modification of messages
- ✓ Denial Of Service (DOS)

By Purvi Tandel

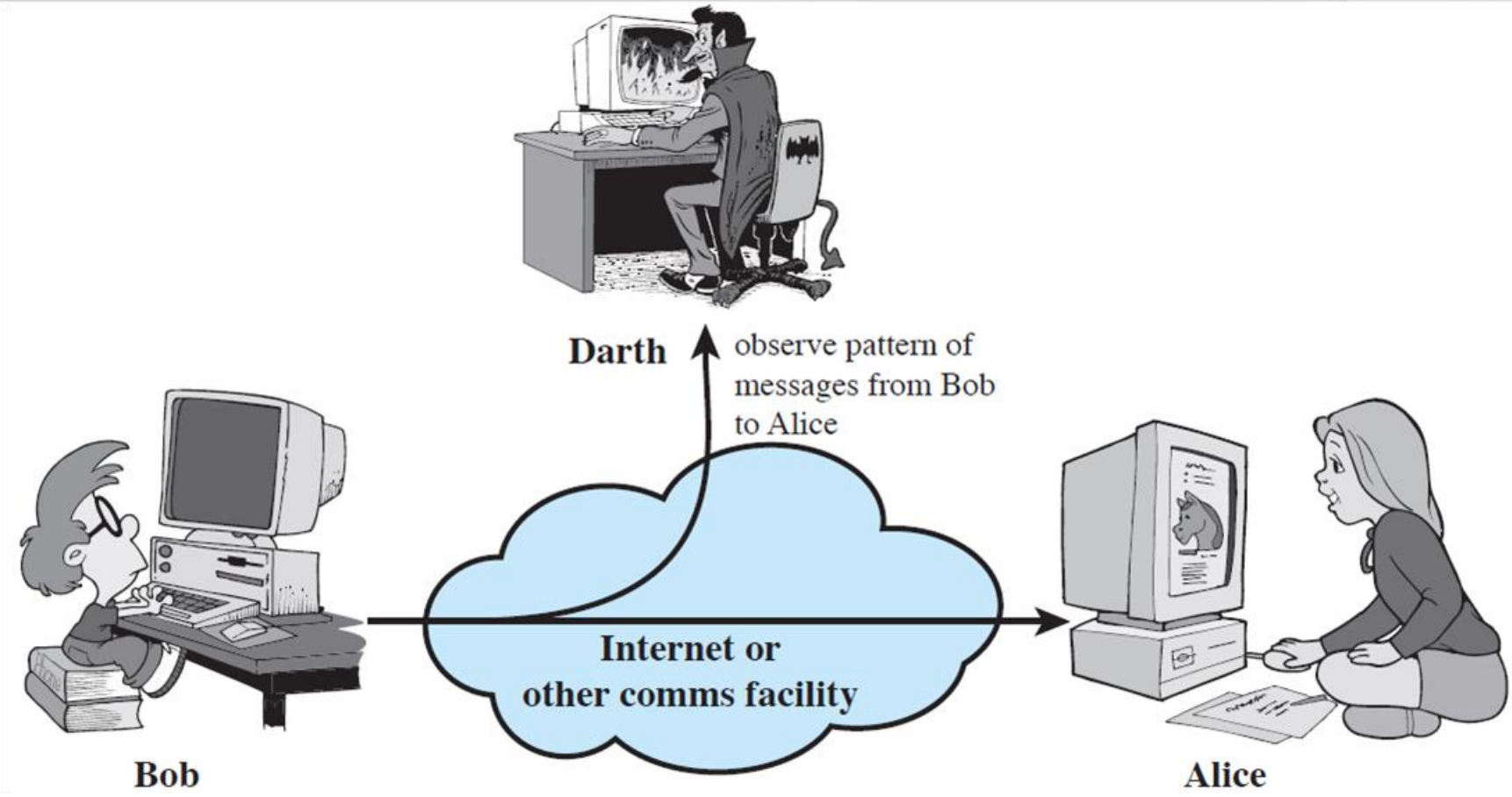
Passive Attacks



Release of message contents

By Purvi Tandel

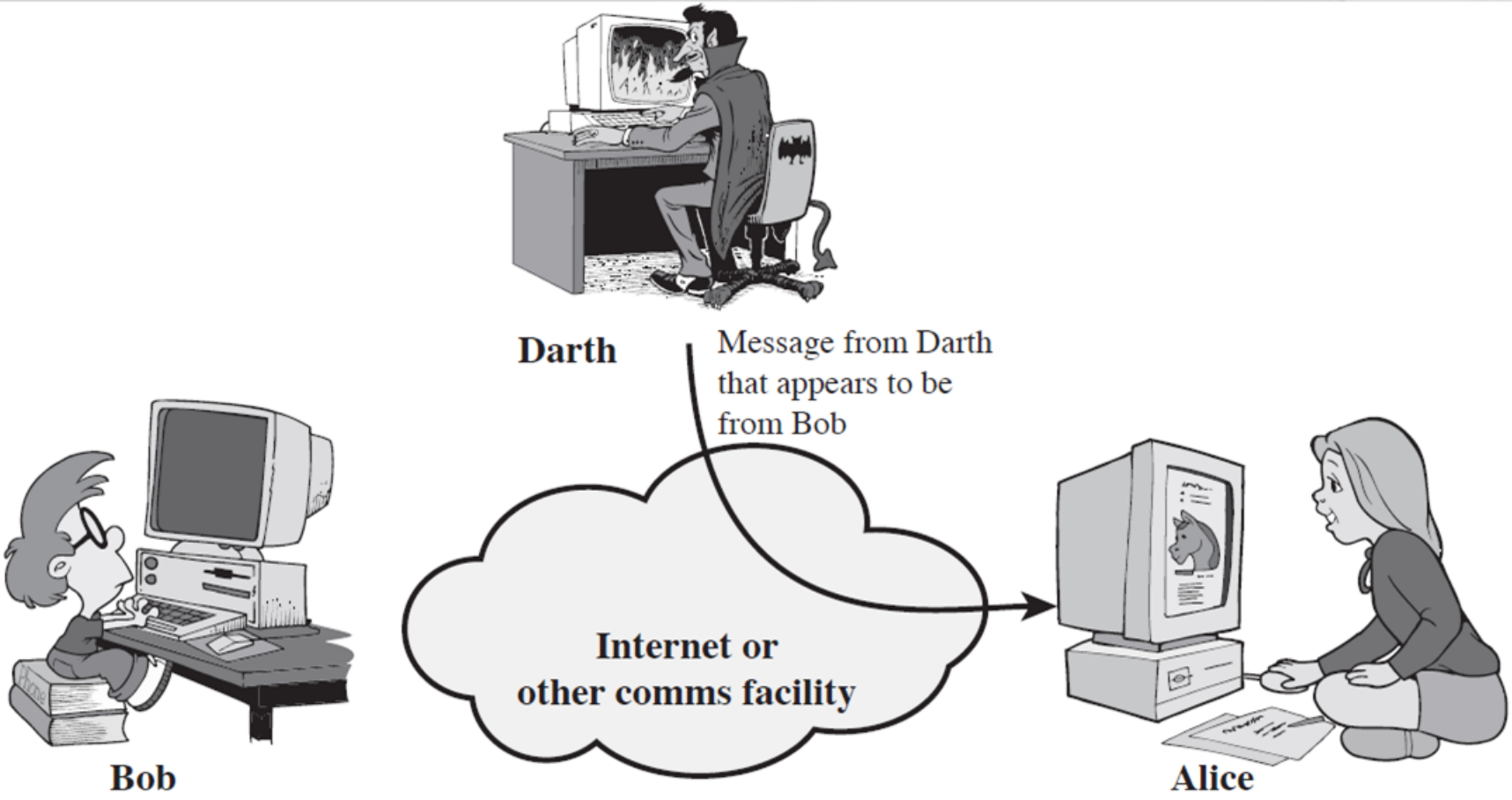
Passive Attacks



Traffic analysis

By Purvi Tandel

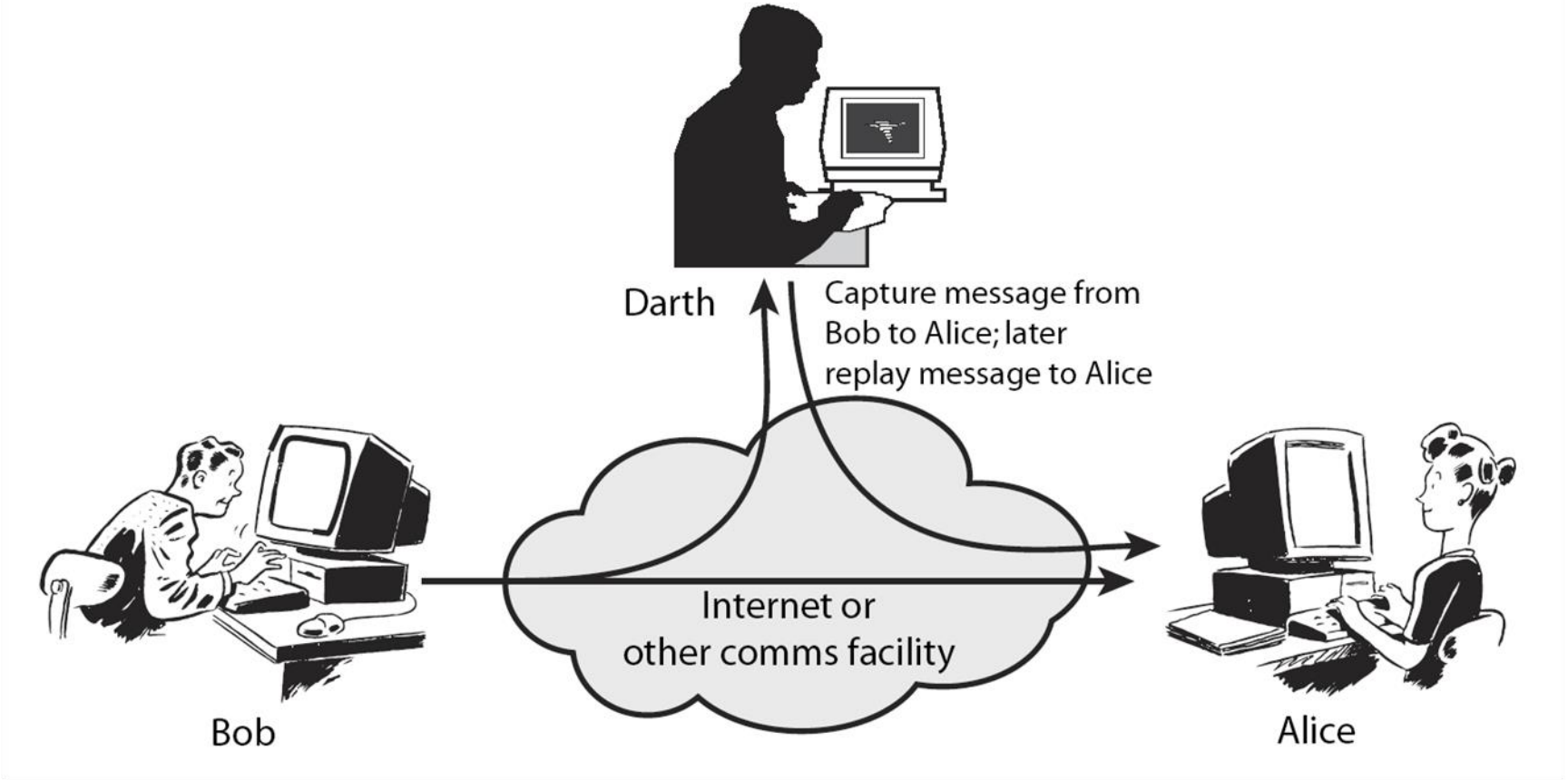
Active Attacks



Masquerade

By Purvi Tandel

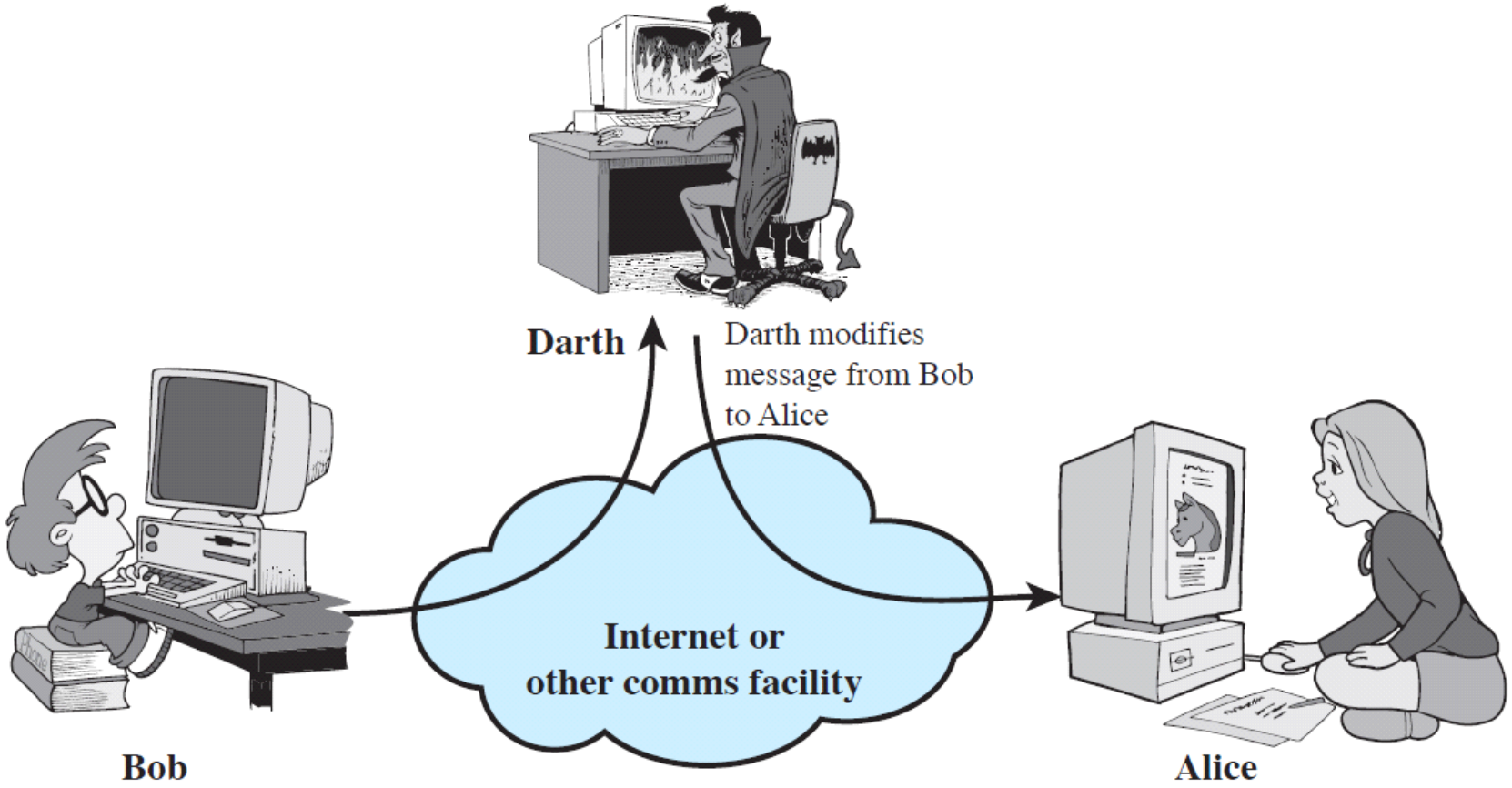
Active Attacks



Replay

By Purvi Tandel

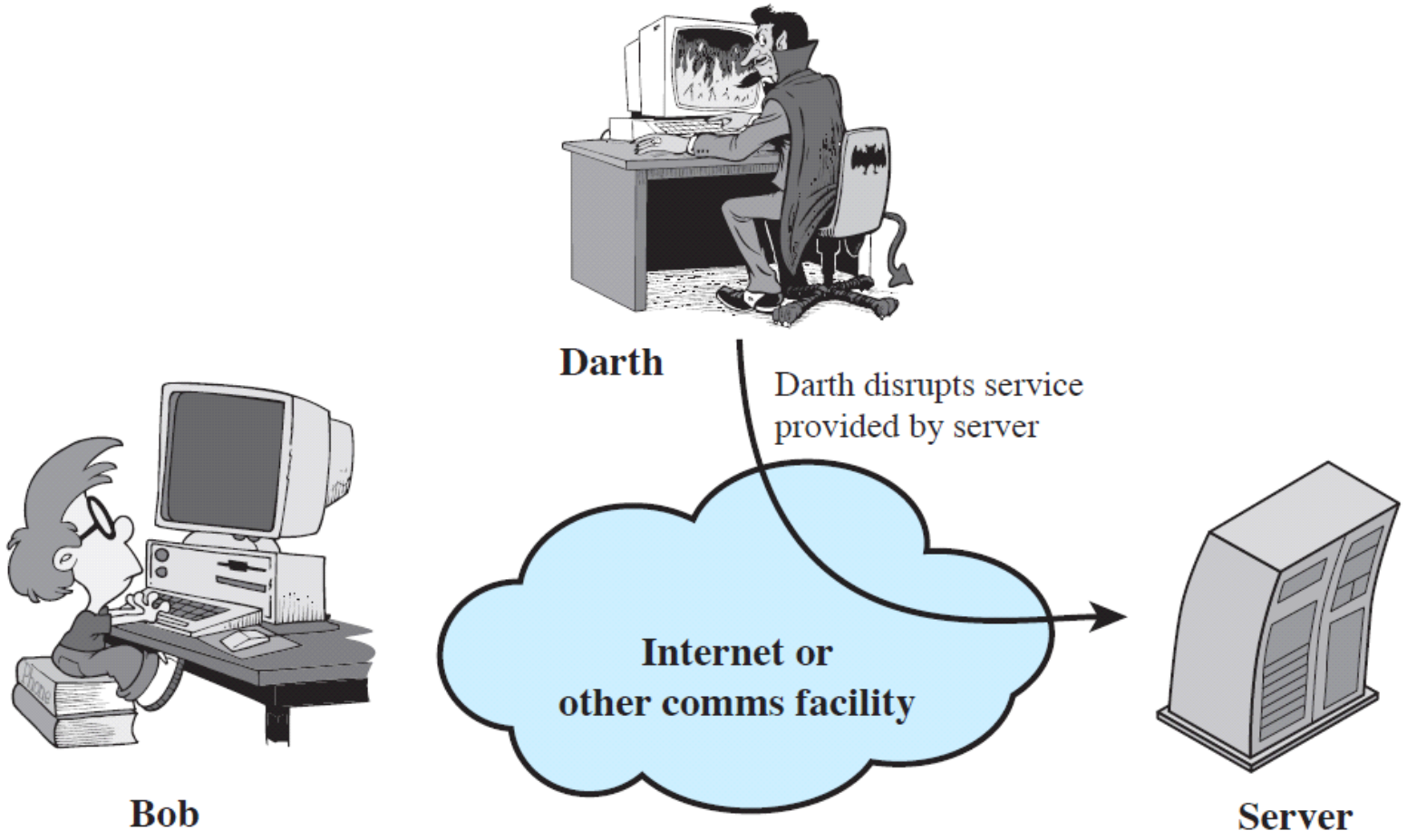
Active Attacks



Modification of messages

By Purvi Tandel

Active Attacks



Denial Of Service

By Purvi Tandel

Security Services

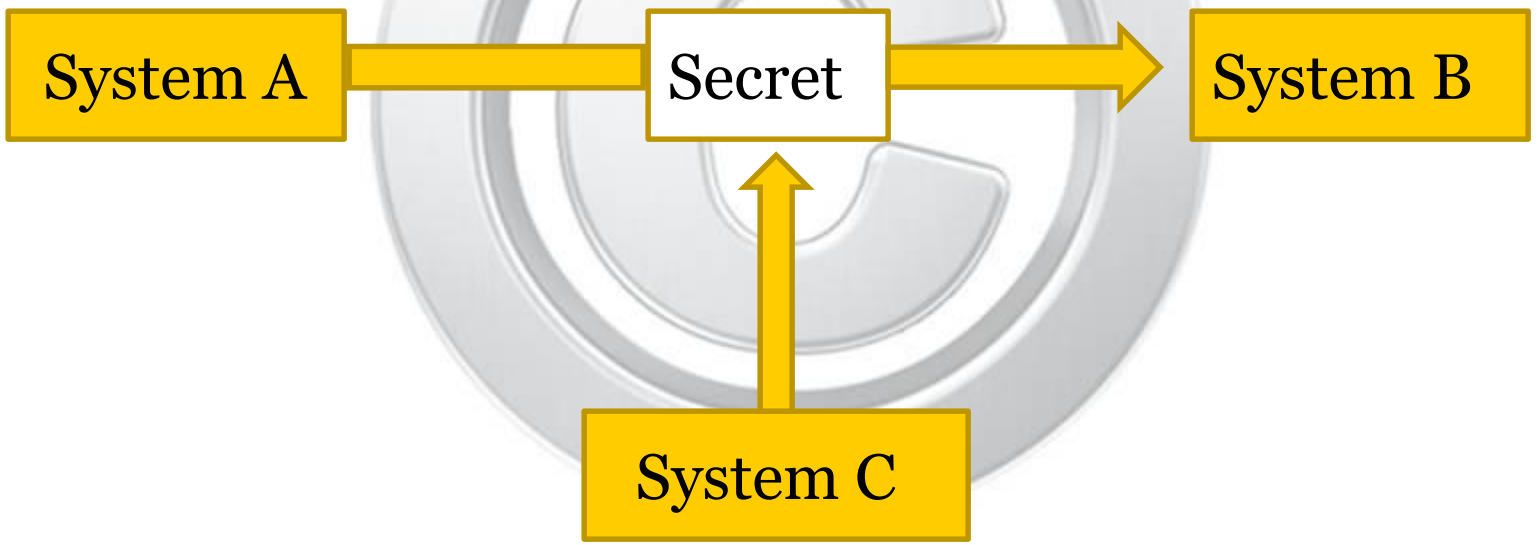
- ✓ Confidentiality
- ✓ Authentication
- ✓ Integrity
- ✓ Non-Repudiation
- ✓ Access Control
- ✓ Availability

By Purvi Tandel

Security Services

Confidentiality:

Protection of the data from unauthorized disclosure.



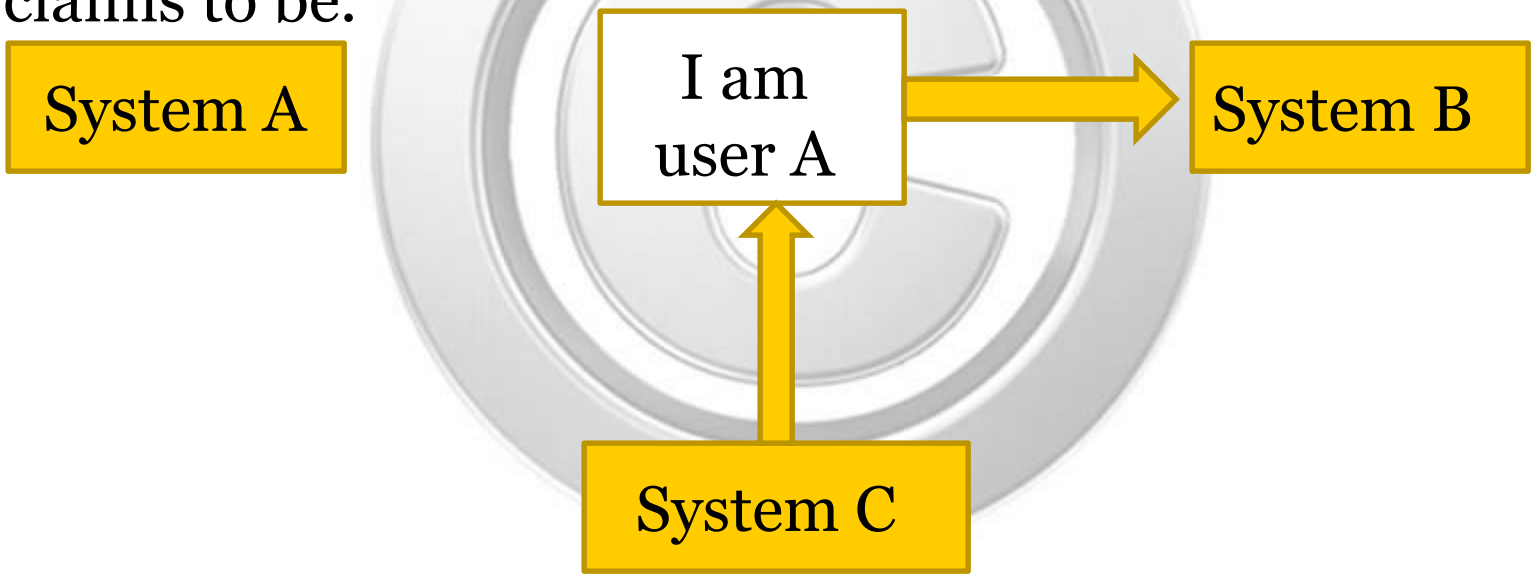
Loss of Confidentiality

By Purvi Tandel

Security Services

Authentication:

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



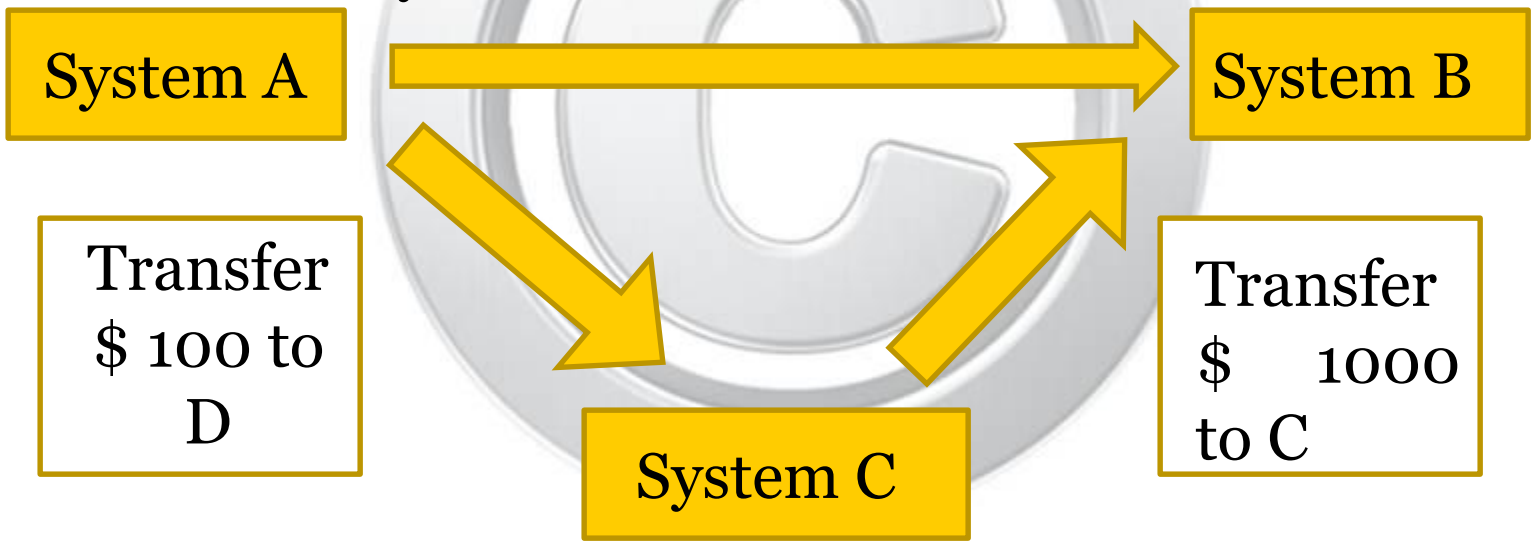
Absence of Authentication

By Purvi Tandel

Security Services

Integrity:

The assurance that data received are exactly as sent by an authorized entity.

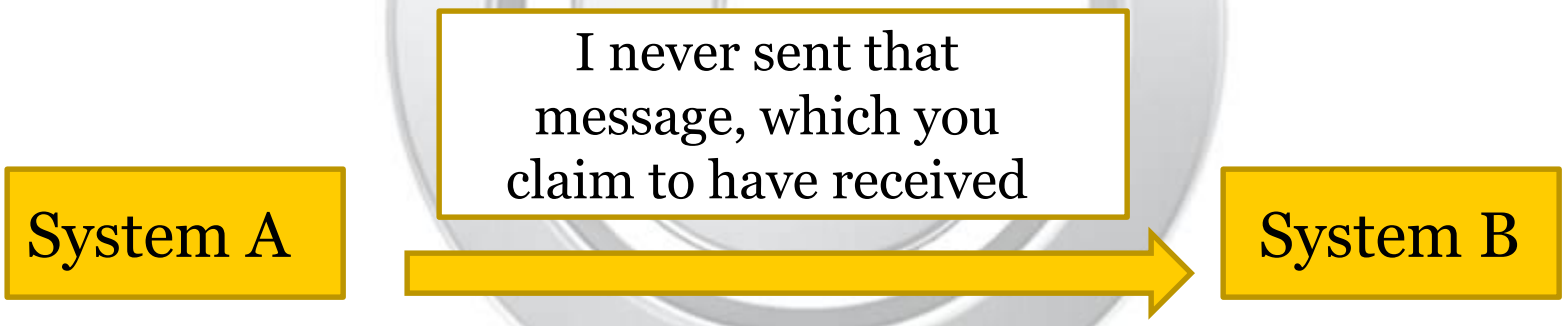


Loss of Integrity

Security Services

Non-Repudiation:

Provision whereby the sender of a message cannot refuse having sent it and receiver of a message cannot refuse having received it.



Establishing non-repudiation

Access Control:

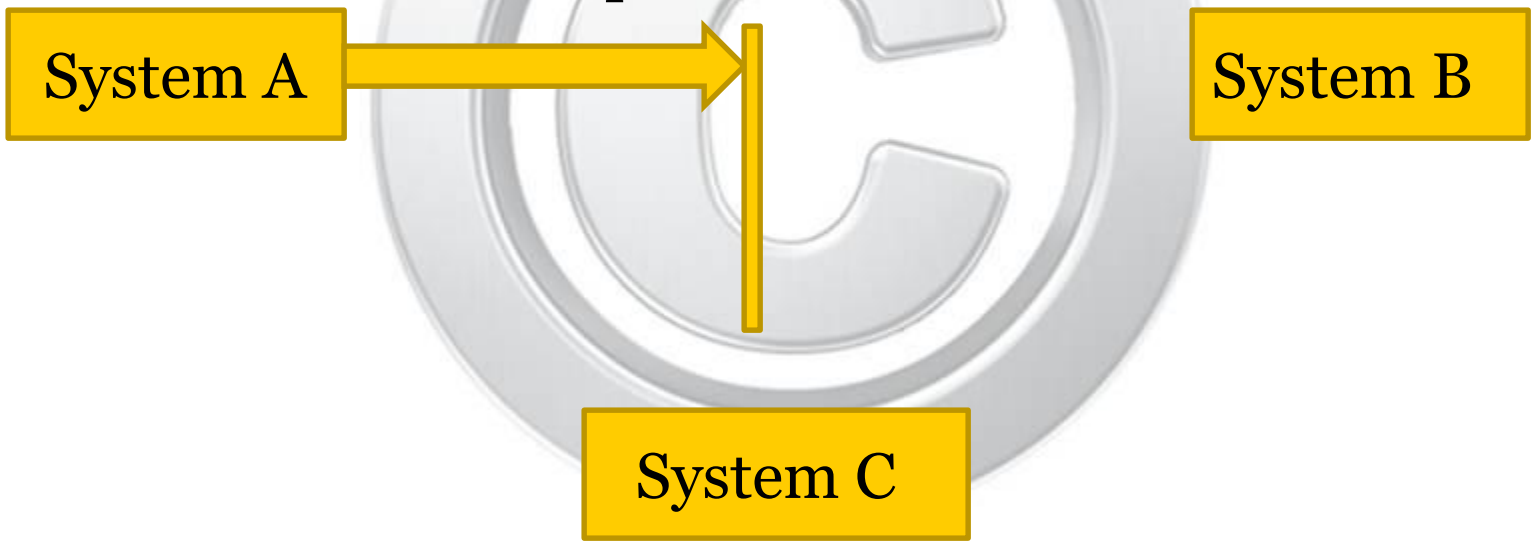
The prevention of unauthorized use of a resource.

By Purvi Tandel

Security Services

Availability:

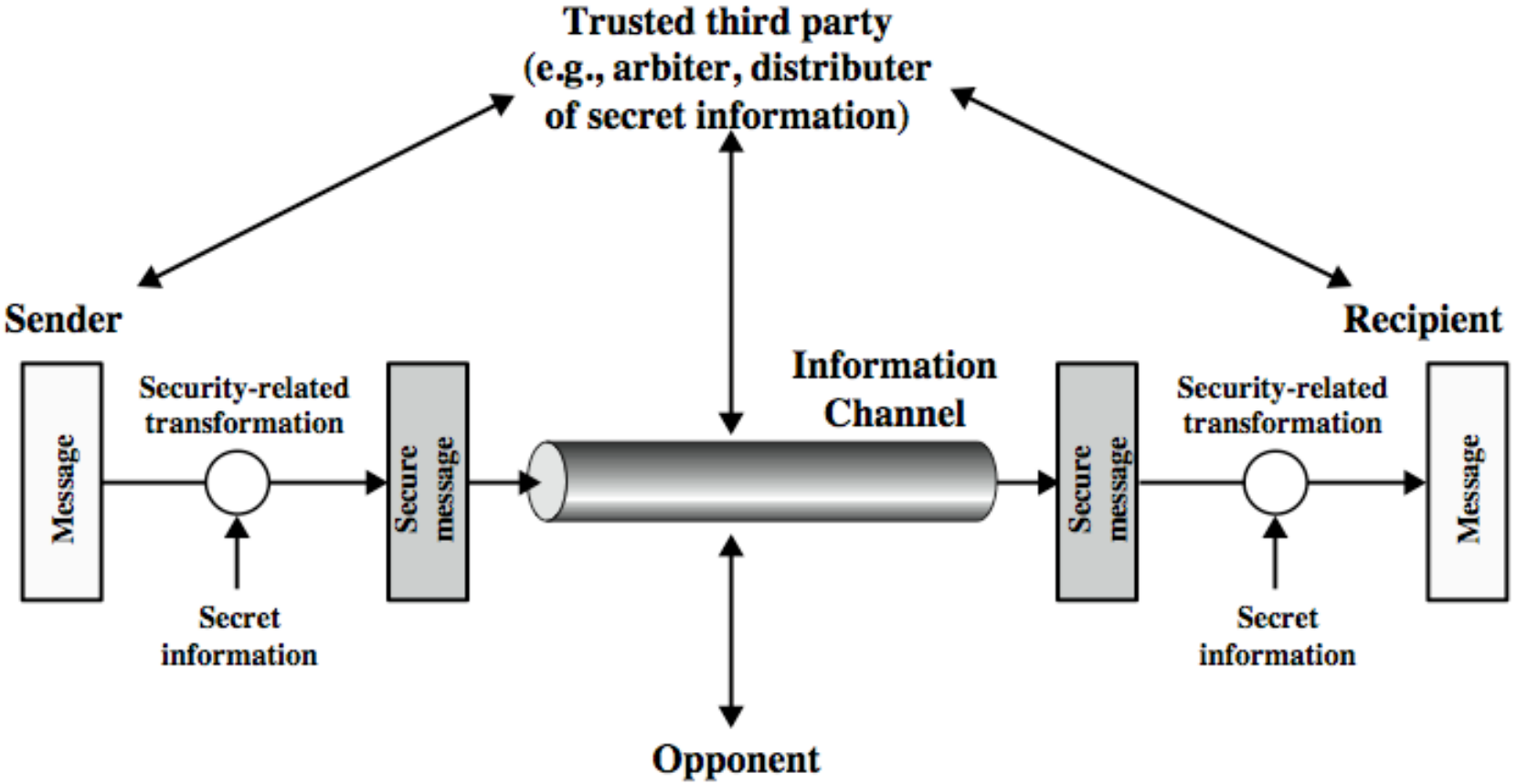
The principle of availability states that resources should be available to authorized parties at all times.



Attack on Availability

By Purvi Tandel

A model for network security



By Purvi Tandel

CLASSICAL ENCRYPTION TECHNIQUES

By Purvi Tandel

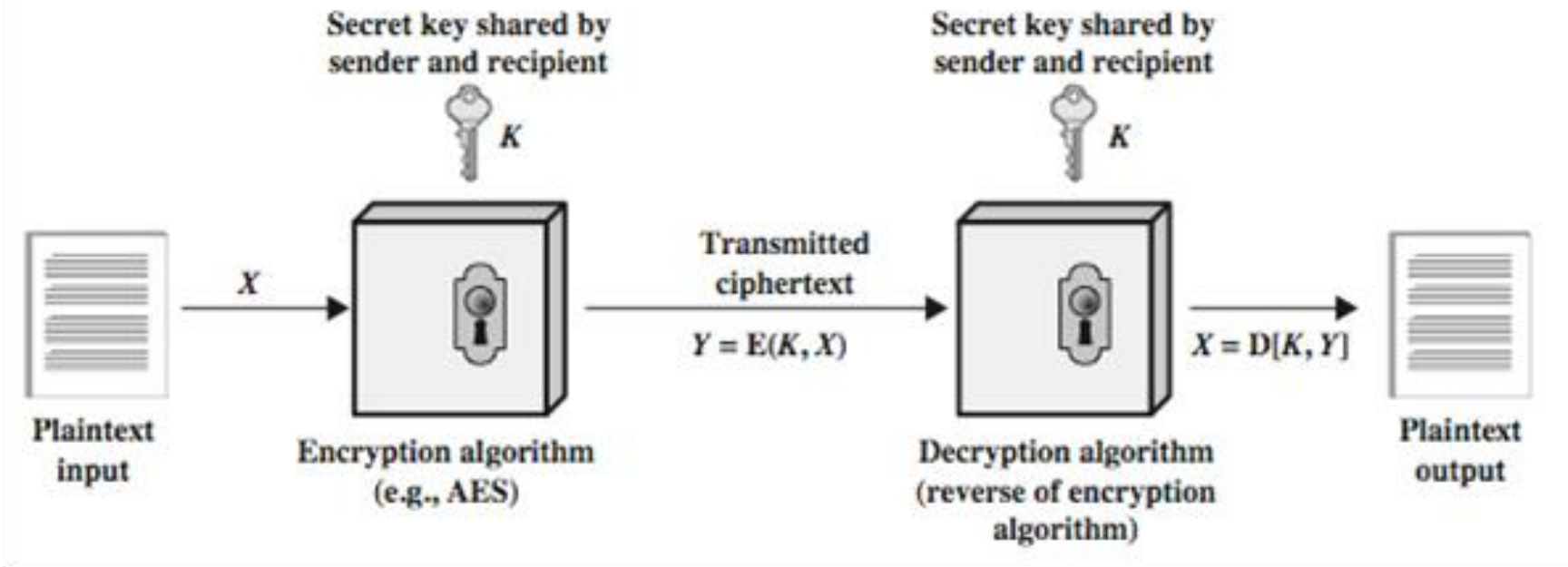
Many schemes used for encryption constitute the area of study known as **cryptography**.

Such a scheme is known as **cryptographic system**.

Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of **cryptanalysis**.

The areas of cryptography and cryptanalysis together are called **cryptology**.

Symmetric cipher model



Simplified model of conventional encryption

Symmetric cipher model

A symmetric encryption scheme has 5 ingredients:

Plain text: Original intelligible message or data.

Encryption algorithm: The encryption algorithm performs various substitution & transformations on the plaintext.

Secret key: The algorithm will produce a different output depending on the specific key being used at the time.

Cipher text: Coded message produced as output.

Decryption algorithm: Essentially the encryption algorithm run in reverse.

By Purvi Tandel

Symmetric cipher model

2 requirements for secure use of conventional encryption:

1) Strong encryption algorithm(Opponent should not find the key)

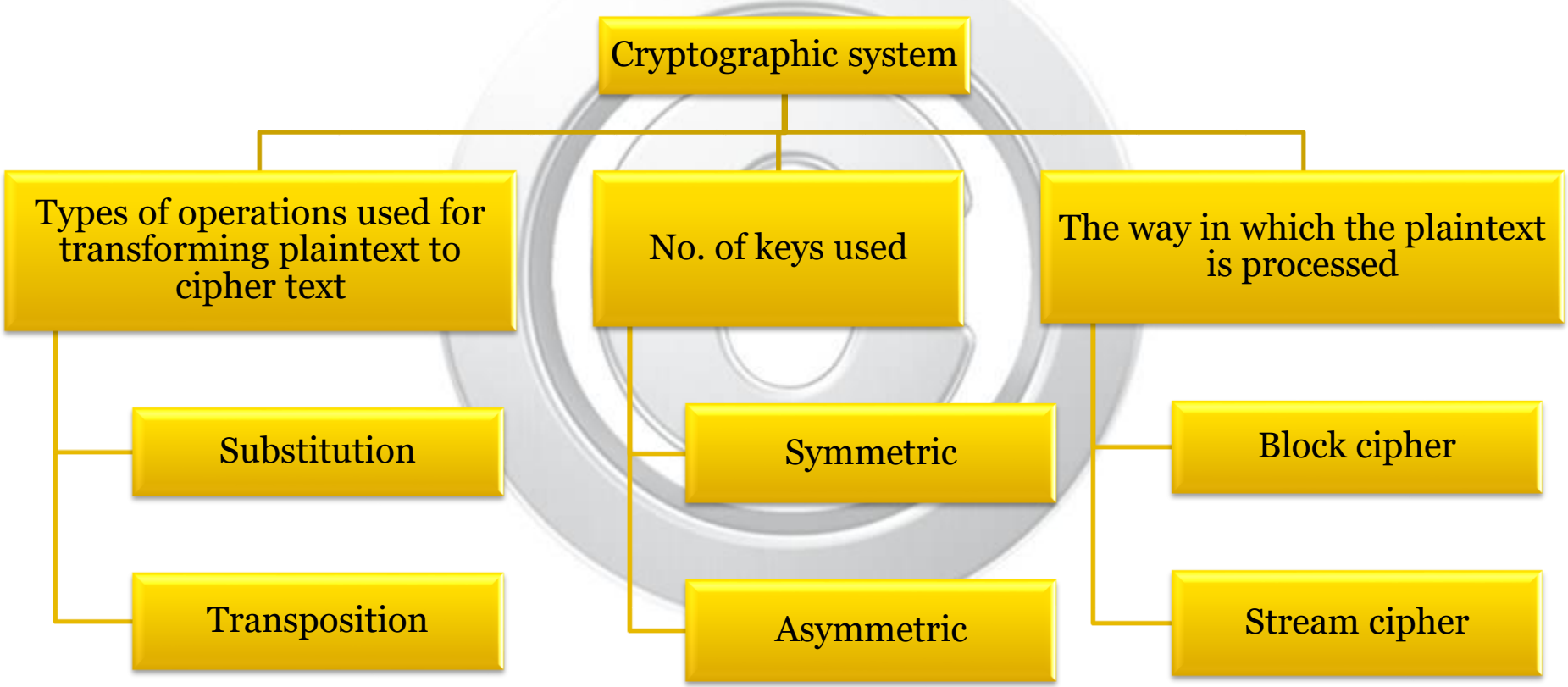
2) Sender and receiver must have obtained copies of the secret key in a secure fashion.

Encryption: Y = E (K , X)

Decryption: X = D (K , Y)

By Purvi Tandel

Cryptographic systems categorized in 3 dimensions:



By Purvi Tandel

Substitution: Each element mapped into another

Transposition: Elements are rearranged

Symmetric: If both sender & receiver use the same key, system referred to as symmetric.

Asymmetric: If both sender & receiver use the different key, system referred to as asymmetric.

Block cipher: Producing an output block for each input block.

Stream cipher: Processes the input elements continuously producing output 1 element at a time.

Cryptanalysis:

Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of general characters of the plaintext.

Brute Force Attack:

Attacker tries every possible key on a piece of cipher text until plaintext is obtained.

By Purvi Tandel

Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/μs	Time required at 10^6 decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} μs = 6.4×10^{12} years	6.4×10^6 years

By Purvi Tandel

Unconditionally Secure: If cipher text generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much cipher text is available.

Computationally Secure: If either of these two criteria are met.

1) The cost of breaking the cipher exceeds the value of the encrypted information.

2) The time required to break the cipher exceeds the useful lifetime of the information.

By Purvi Tandel

Classical encryption techniques

Substitution Technique:

In which the letters of plaintext are replaced by other letters.

- ✓Caesar cipher
- ✓Monoalphabetic cipher
- ✓Playfair cipher
- ✓Hill cipher
- ✓Polyalphabetic cipher

Transposition Technique:

In which the letters of plaintext are re-arranged.

- ✓Rail Fence
- ✓Columnar

By Purvi Tandel

Steganography

- An alternative to encryption
- Hides existence of message

Various techniques:

1) **Character marking:** Letters overwritten in pencil
   Letters are visible unless the paper is held at an angle to bright light.

2) **Invisible ink:** No of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.

By Purvi Tandel

Steganography

3) **Pin punctures:** Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light.

4) **Typewriter correction ribbon:** Used between lines typed with a black ribbon, the result of tying with the correction type are visible only under a strong light.

Drawback: Lot of overhead to hide few bit information

By Purvi Tandel