

# 22AIE314 - COMPUTER SECURITY

## UNIT-1

### Basics of Computer Security

February 10, 2025

**Dr.Remya S**  
**Assistant Professor**  
**Department of Computer Science**



School of Computing  
Amritapuri Campus, Clappana P.O., Kollam - 690525, Kerala,  
India. Ph: +91 (476) 280 2100 Email: cs@am.amrita.edu  
[www.amrita.edu/school/computing/amritapuri](http://www.amrita.edu/school/computing/amritapuri)

# Agenda

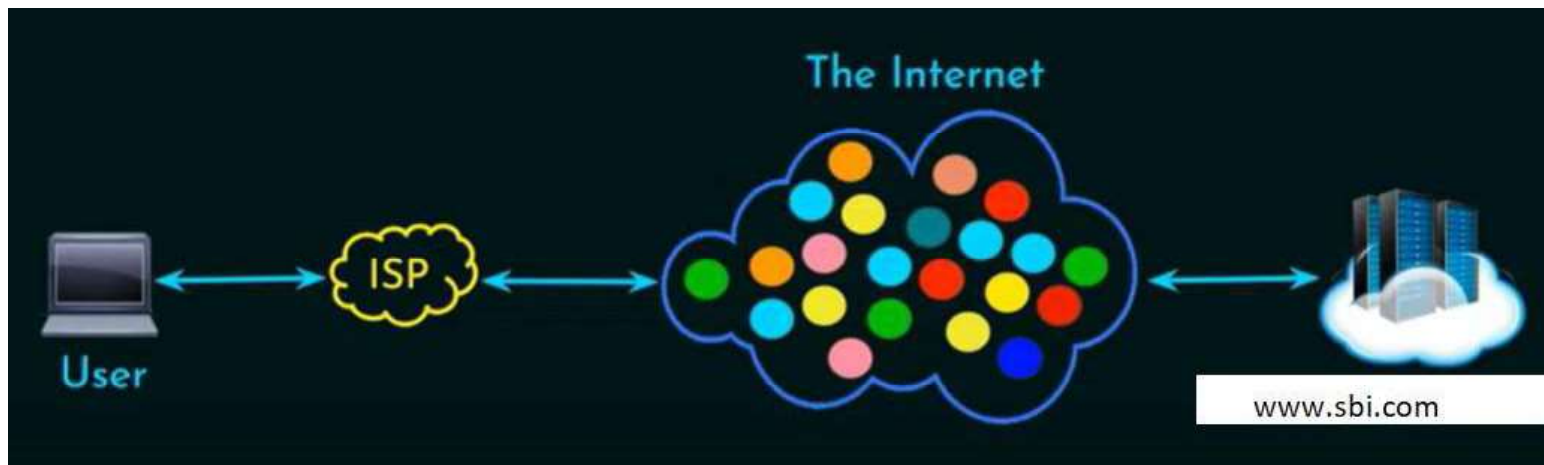
- Introduction to Computer Security
- Mathematical concepts-Algebra & Number Theory
- Block Cipher
- Public Key Cryptography
- Cryptographic Hash functions & Digital Signature
- Security Practices & System security
- Email, IP & Web security

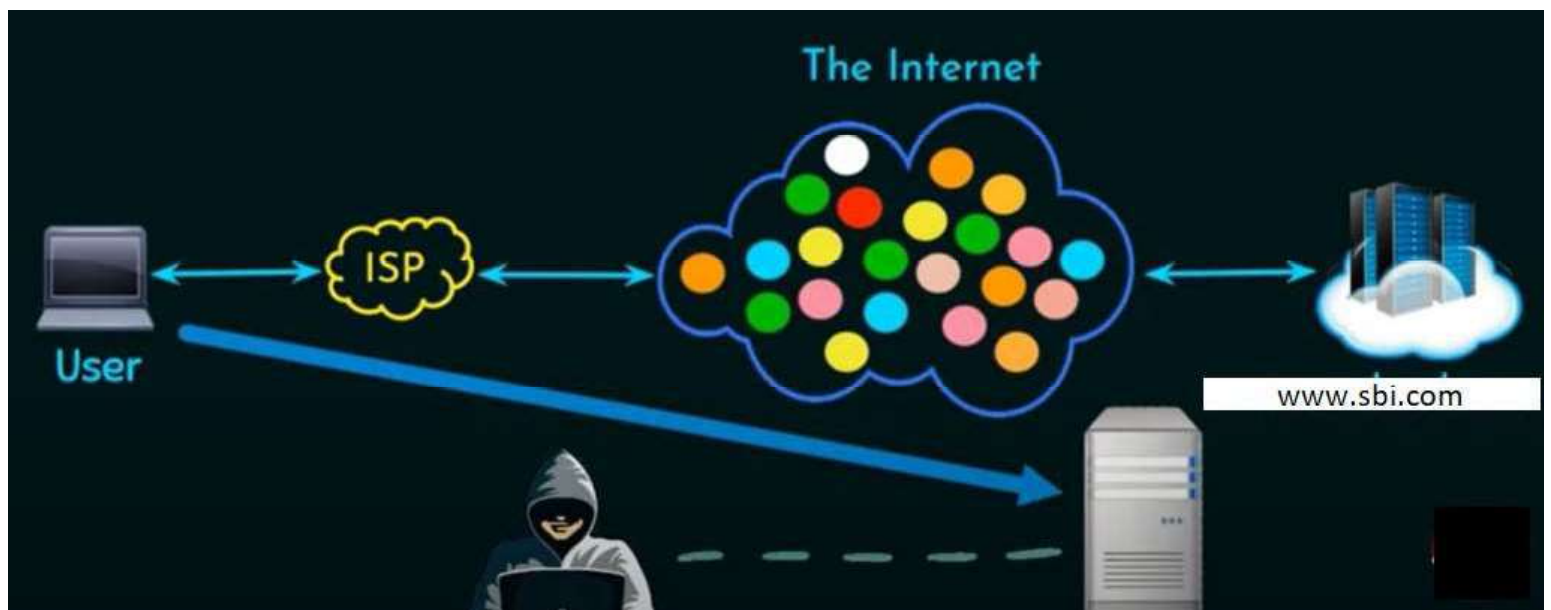
# Introduction

- 1 Understand the need for network security with a real world scenario
- 2 Know various intentions of attacker

## Why Network Security and Cryptography?

- Why are we learning Network Security?
- What would we do with it?
- Understand information security services
- Be aware of vulnerabilities and threats
- Realize why network security is necessary
- What are the elements of a comprehensive security program





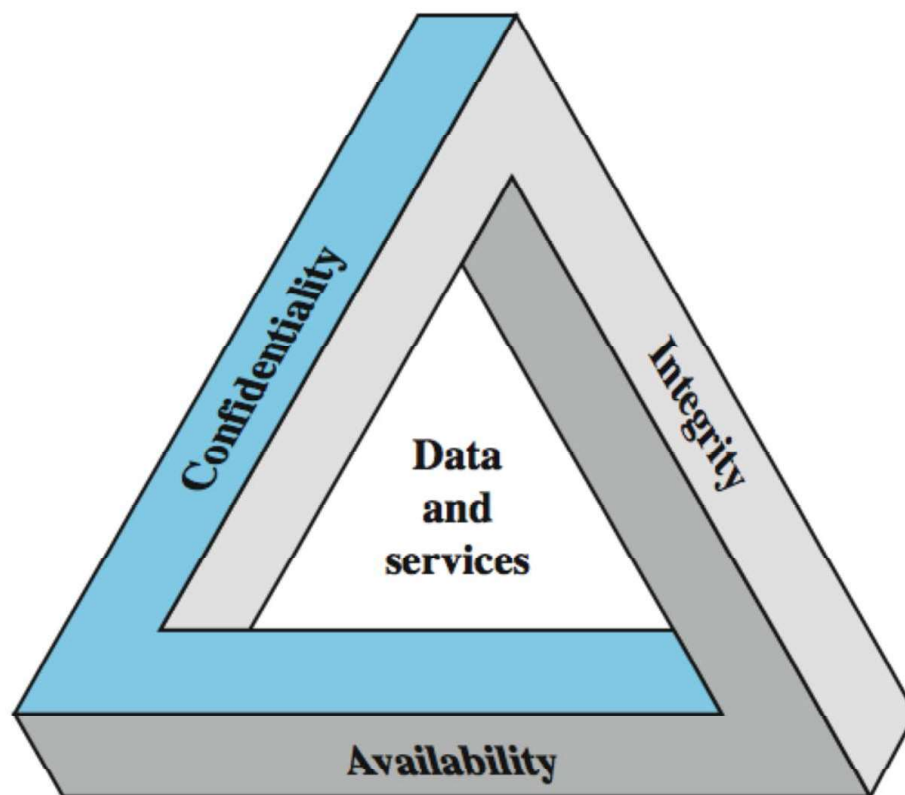
# CIA Triad

- 1 Define Computer Security
- 2 Know the key objectives of computer security
- 3 Understand CIA Triad
- 4 Know various levels of impact of security breach

## Computer Security -Definition

- The protection afforded to an automated information system in order to attain the applicable objectives of preserving the **integrity, availability, and confidentiality** of information system resources (includes hardware, software, firmware, information/ data, and telecommunications)[NIST].
- **3** Key Objectives
  - ① Confidentiality
    - ① Data confidentiality
    - ② Privacy
  - ② Integrity
    - ① Data integrity
    - ② System integrity
  - ③ Availability

# CIA Triad





## ① Confidentiality

- Prevent **unauthorized access and disclosure**
- Unauthorized access: Nobody else can access , except the right entities whom are involved in this transaction
- Disclosure: The message should not be open enough- **encrypted message**
- Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
- Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

## ② Integrity

- **Don't allow any modification of message by unauthorized people**
- sent = Received
- Data integrity: Assures that information and programs are changed only in a specified and authorized manner.
- System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

3

### Availability:

- Ensure the timely and reliable access to the system
- example: google.com

## Levels of impact of Security breaches

- ① Low
  - Limited adverse effect
  - Minor harm or minor damage
- ② Medium
  - Serious adverse effect
- ③ High
  - Catastrophic adverse effect(Severe effect)

## CIA Triad-Additional Elements

- Authenticity
  - Property of being genuine and being able to verify the parties involved
  - Eg: The receiver should verify the message is coming from the right party or trusted authority
- Accountability
  - Every user who works with an organization or information system should have specific responsibilities for information assurance
  - User who accesses the system has their roles and responsibilities and whatever the actions, the user should keep records of their activity
  - Every user is given some responsibilities and every user should only access that level of privilege or it must ensure that users are not misusing their privileges

## Examples of Security Requirements

- confidentiality – student grades, account information
- integrity – patient information
- availability – authentication service, user verification

# OSI Security Architecture

- 3 aspects of information security
  - 1 **Security Attack**: Any action that compromises the security of information owned by an organization
  - 2 **Security Mechanism**: detect, prevent, recover
  - 3 **Security Service**: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.
- ITU-T X.800 “Security Architecture for OSI”
- It defines a systematic way of defining and providing security requirements
- 2 Terms
  - 1 **Threat** – A potential for violation of security
  - 2 **Attack** – An assault on system security, a deliberate attempt to evade security services

## Threats & Attacks

- **Threats:** A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.
- **Attack:** An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

- Security Attack

- 1 Passive Attack
- 2 Active Attack

- Security services

- 1 Authentication
- 2 Access Control
- 3 Data Confidentiality
- 4 Non repudiation

- Security Mechanisms

- 1 Encipherment
- 2 Digital Signature
- 3 Access Control
- 4 Data Integrity
- 5 Authentication Exchange
- 6 Routing Control



# Security Attacks

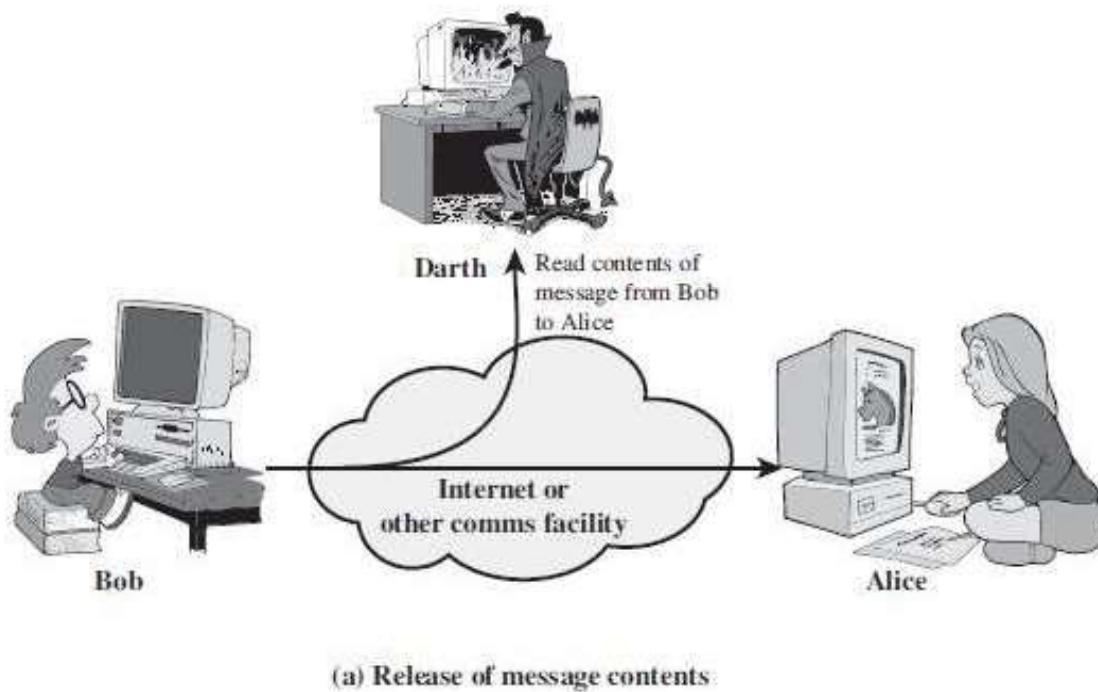
- Attack is an action that comprises the security of an individual or an organization
- Effects-Loss of data, corruption of data, injection of viruses, ransomware attack
- 2 Types
  - ① Passive Attack: Attempts to learn or make use of information from the system but does not affect system resources
    - ① Release of message contents
    - ② Traffic analysis
  - ② Active Attack: attempts to alter system resources or affect their operation.
    - ① Masquerade
    - ② Replay
    - ③ Modification of messages
    - ④ Denial of service

## Passive Attack

- Attempts to learn or make use of information from the system
- Does not affect system resources
- Eavesdropping or monitoring of transmissions
- Goal: Obtain information that is being transmitted

## Passive Attack-Release of Message contents

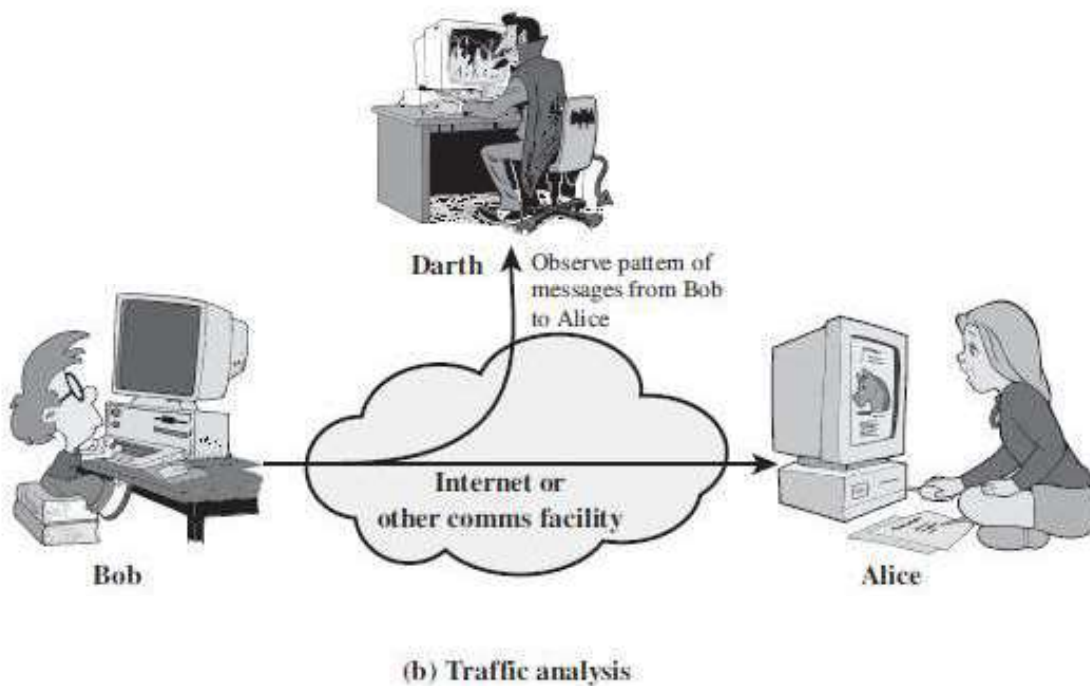
Reads contents from Bob to Alice



Solution: Encryption

## Passive Attack-Traffic Analysis

Observe the pattern of messages from Bob to Alice Encrypted message



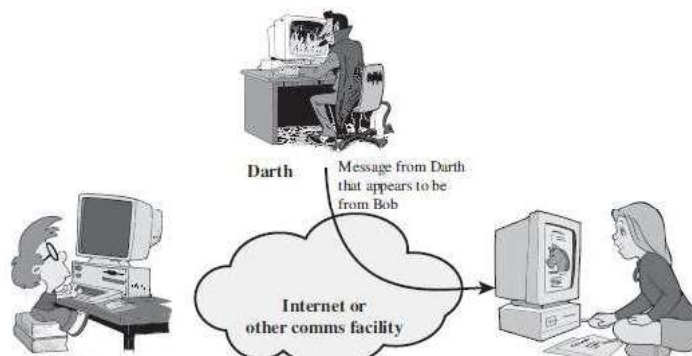
Few information can extract- Location, the identity of communicating host, length of message being transmitted, frequency of message transfer

## Active Attack

- It involves some **modification** of the data stream or the creation of a false stream
- 4 Categories
  - 1 Masquerade
  - 2 Replay
  - 3 Modification of messages
  - 4 Denial of Service(DoS)

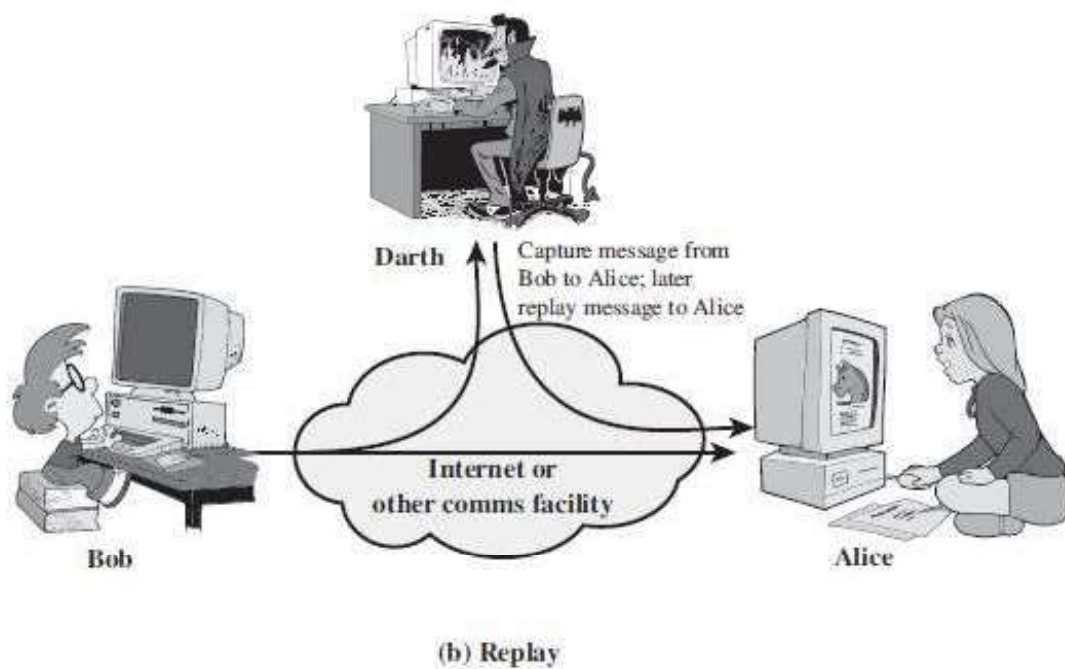
## Active Attack-Masquerade

- Takes place when one entity pretends to be a different entity
- Ex: Steal some one's password and login with that username and pw
- A masquerade attack usually includes one of the other forms of active attack.
- For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.
- **Message from Darth appears to be from Bob**(Darth behaves like Bob)-asking for extra privileges



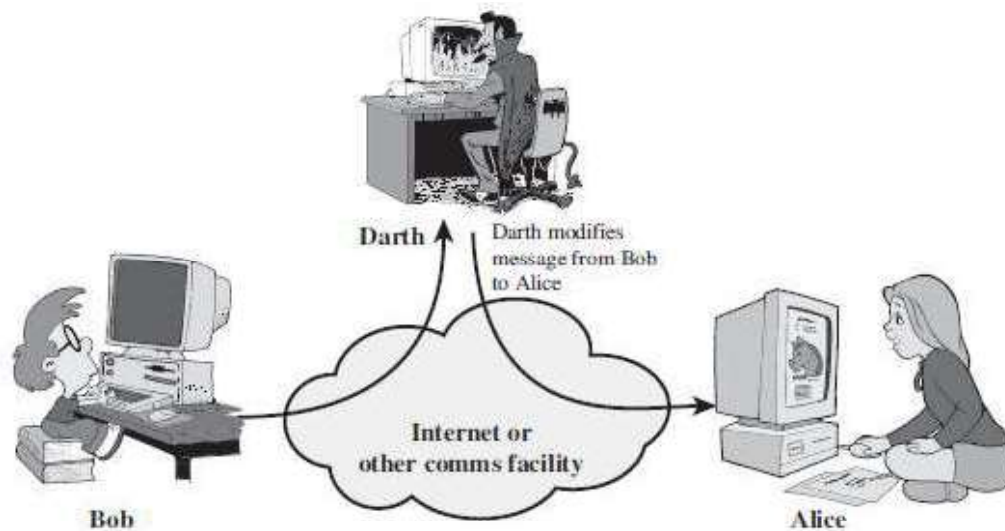
## Active Attack-Replay

- Replay activity
- involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect
- Capture message from Bob to Alice; later replay message to Alice



## Active Attack-Modification of messages

- means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect
- **Darth modifies the message from Bob to Alice**

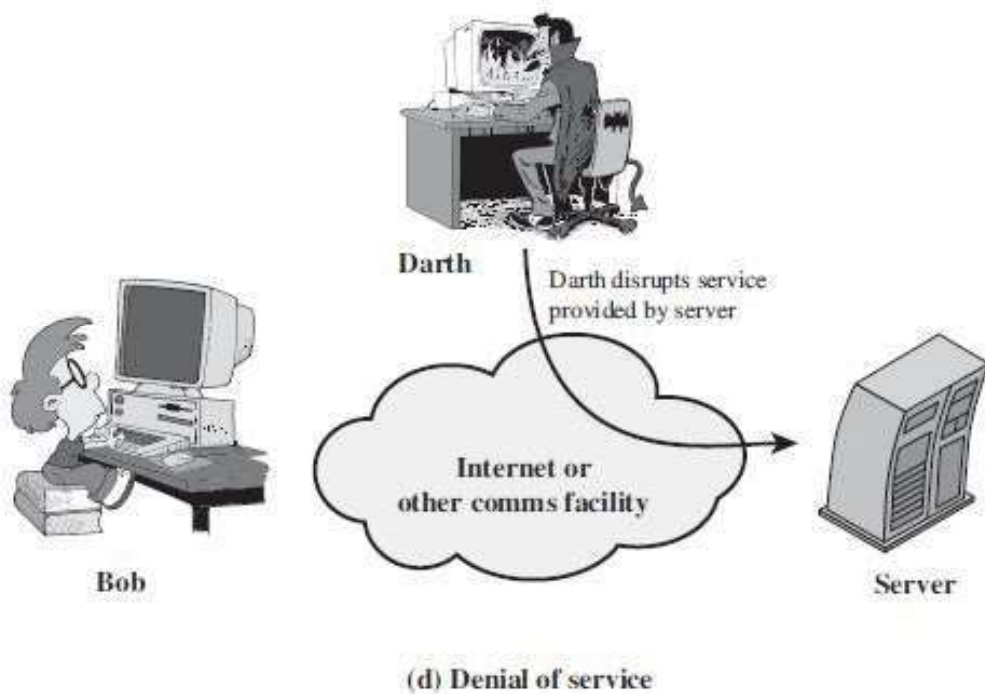


(c) Modification of messages



## Active Attack-Denial of Service(DoS)

- prevents or inhibits the normal use or management of communications facilities
- **Darth disrupts service provided by server**



## Passive Vs Active Attacks

No	Active Attack	Passive Attack
1	Attacker needs to have control media or network.	Attacker observe the communication in media or network.
2	It can be easily detected.	It cannot be easily detected.
3	It affects the system.	It does not affect the system.
4	It involves modification in data.	It involves in monitoring in data.
5	It does not check for loopholes or vulnerabilities.	It scans the ports and network in search for loopholes and vulnerabilities.
6	It is difficult to prevent network from active attack.	Passive attack can be prevented.
7	Types of active attack: Masquerade, replay, denial of service, modification of message.	Types of passive attack: release of message content, Traffic analysis.

# Security Services

- A processing or communication service that is provided by a system to give a specific kind of protection to system resources; security services implement security policies and are implemented by security mechanisms. [\[RFC-2828\]](#)
- 5 Security services
- **Authentication**: Proves the identity of the sender
- 2 types of authentication
  - 1 Peer entity authentication : Provides for the corroboration of the identity of a peer entity in an association
  - 2 Data origin authentication : : Provides for the corroboration of the source of a data unit.

## Access Control:

- Levels of privileges/access
- Ability to limit and control access to host systems and applications via communications links.
- To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.
- **Data Confidentiality**: Protection of transmitted data from passive attacks- Encryption
- **Data Integrity**: Send=Receive
- **Non repudiation**: Nonrepudiation prevents either sender or receiver from denying a transmitted message.

## Security Mechanism:

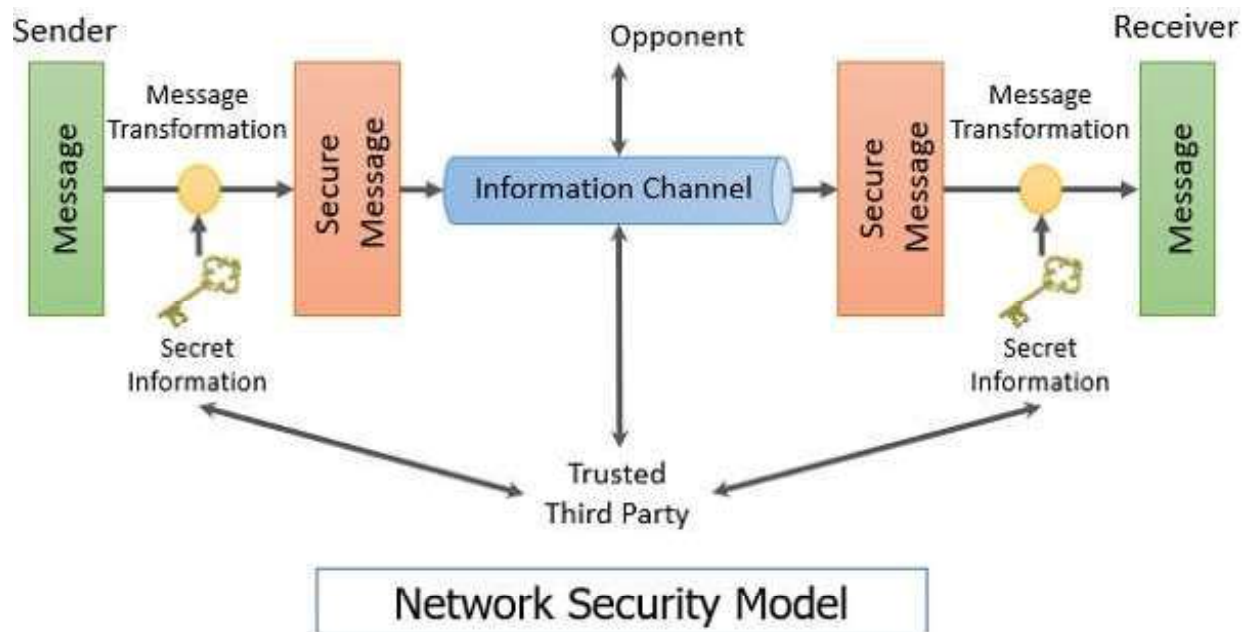
- Security services implement security policies that are implemented by security mechanism
- 2 Types
  - ① **Specific security mechanism**: incorporated into the appropriate protocol layer in order to provide some of the OSI security services.
  - ② **Pervasive security mechanism**: Mechanisms that are not specific to any particular OSI security service or protocol layer.
- **Specific Security Mechanism**
- **Encipherment**: Convert the plain text into cipher text before sending the data- achieve data confidentiality
- **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).-piece of code embedded in message
- **Access Control**: A variety of mechanisms that enforce access rights to resources.

- **Data Integrity:** A variety of mechanisms used to assure the integrity of a data unit or stream of data units.
- **Authentication Exchange:** A mechanism intended to ensure the identity of an entity by means of information exchange.
- **Traffic Padding:** Dummy data in between the gap
- **Routing Control:** Specify the routes to reach destination
- **Notarization:** Trusted third party

**Pervasive Security Mechanism** - Generalized one only-Not incorporated with any layers

- **Trusted Functionality:** perceived to be correct with respect to some criteria
- **Security Label:** The marking bound to a resource that names or designates the security attributes of that resource.
- **Event Detection:** Detection of security-relevant events.
- **Security Recovery:** Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

# Network Security Model



This general model shows that there are four basic tasks in designing a particular security service:

- ① Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
- ② Generate the secret information to be used with the algorithm.
- ③ Develop methods for the distribution and sharing of the secret information.
- ④ Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.



## General Approaches to attack a conventional encryption scheme

- Cryptanalysis: Deals with how the attackers or cryptanalyst find the key based on some information available- Based on info known to the cryptanalyst.
  - 1 Ciphertext only attack(Most difficult)
  - 2 Known plain text attack
  - 3 Chosen plaintext attack
  - 4 Chosen ciphertext attack
  - 5 Chosen text attack
- Brute-force Attack-Attackers or cryptanalyst will be trying all possible values in the key space

Type of Attack	Known to Cryptanalyst
Ciphertext Only	Encryption Algorithm, Ciphertext
Known Plaintext	Encryption Algorithm, Ciphertext, One or more PT-CT pairs formed with secret key
Chosen Plaintext	Encryption Algorithm, Ciphertext, PT message chosen by cryptanalyst together with its CT generated with its secret key
Chosen Ciphertext	Encryption Algorithm, Ciphertext, CT chosen by cryptanalyst together with its corresponding decrypted plaintext generated with the secret key.
Chosen text	Chosen plain text and chosen ciphertext

**Table:** Types of Cryptographic Attacks

### Ciphertext

2D570755676DFF11E71B6C8511EFE7A7D3B02A3CEE63165050AB5  
F4C4D19A4AAB07656A636654C6F39A4AC0FEA2035CCDD7181C0  
EBB482A6EBDAEF2AEB35CB5C325CBF0738AEC27D77BEC3938C  
590CE77F62CBDCC3EA3D03E06A386BD70BC99A843DD6B7B975  
3635C919FA17FC40A3C3DCBD13633D2D56A1A073EA0E73E60C60

### Plaintext

Hello World




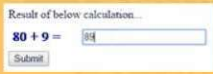

# Brute-Force Attack

- Try every possible keys until an intelligible translation of the cipher text into plain text is obtained
- Guessing
- Exhaustive key search
- Solution: Use a large key space( keys should be large as possible)
- Tools
  - 1 John the Ripper(Use Case: Password recovery, security auditing),
  - 2 Hashcat(Use Case: Password cracking),
  - 3 Aircrack-ng(Use Case: Wi-Fi password cracking),
  - 4 Ophcrack(Use Case: Windows password recovery)

# CAPTCHA

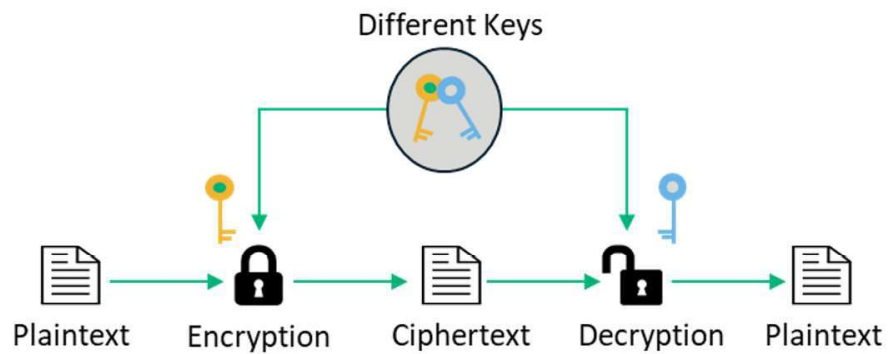
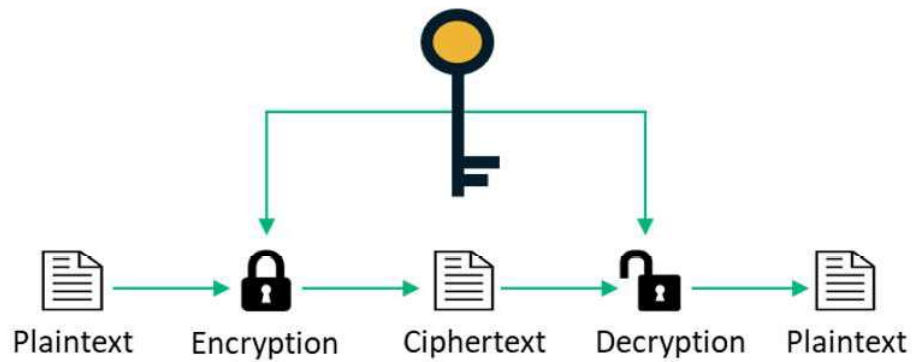
- We can prevent brute force attacks using CAPTCHA
- Completely Automated Public Turing Test to tell Computers and Humans Apart

**What is CAPTCHA and What are its different types?**

 <b>Text-based Captcha</b>	 <b>ReCAPTCHA</b>	 <b>3D Captcha</b>
 <b>Mathematical Captcha</b>		 <b>Image-based Captcha</b>

# Cryptography

- 1 Symmetric Cryptography(Private key cryptography)
- 2 Asymmetric Cryptography(Public key cryptography)



## 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 plaintext from ciphertext
- 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

# Cryptography

- can characterize cryptographic system by:
  - 1 Type of encryption operations used
    - substitution
    - transposition
    - product
  - 2 Number of keys used
    - single-key or private
    - two-key or public
  - 3 Way in which plaintext is processed
    - block
    - stream