

# Cryptography and Network Security

Subject Code:CSC602

# Syllabus-Module 1

## Module 1

### 1

## Introduction - Number Theory and Basic Cryptography

### 1.1

Security Goals, Attacks, Services and Mechanisms, Techniques. Modular Arithmetic: Euclidean Algorithm, Fermat's and Euler's theorem

### 1.2

Classical Encryption techniques, Symmetric cipher model, mono-alphabetic and polyalphabetic substitution techniques: Vigenere cipher, playfair cipher, Hill cipher, transposition techniques: keyed and keyless transposition ciphers

# What is security?

- **Protection of a person, building , organization or country against threats such as crime or attacks by foreign countries.**
- **The quality or state of being secure- to be free from danger**

# What is security(Technically)

- *Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats*

# Multiple layers of security

- Physical security
  - To protect the physical items , objects
- Personal security
  - To protect an individual who are authorized to access an organization
- Operations security
  - Protection of the details of a particular operation
- Communication security
  - Protection of an organization's communication media and technology
- Network security/Internet security
  - Protection of networking components, connections etc
- Information security
  - Protection of information , including the system and the hardware that use store and transmit that information

# Some terms

- Information Security
  - Ensures physical and digital data is protected from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction.
  - Information security differs from cybersecurity in that InfoSec aims to keep data in any form secure, whereas cybersecurity protects only digital data.
- Cyber Security
  - a subset of information security, is the practice of defending your organization's networks, computers and data from unauthorized digital access, attack or damage by implementing various processes, technologies and practices.
- Network Security
  - Network security, a subset of cybersecurity, aims to protect any data that is being sent through devices in your network to ensure that the information is not changed or intercepted. The role of network security is to protect the organization's IT infrastructure from all types of cyber threats including:
    - Viruses, worms and Trojan horses
    - Hacker attacks
    - Denial of service attacks
    - Spyware and adware

# Network Security

- Networks security is concerned with protecting a network from unauthorized accesses.
- The first step of this process is authenticating a user, verifying fingerprints or security tokens.
- After authenticating a user, a firewall is used to make sure that the user accesses only the services that are authorized to her.
- In addition to authenticating users, network should also provide security measures against computer viruses, worms or Trojans.
- As mentioned earlier, different types of networks require different levels of security. For a small network of a home or a small business, a basic firewall, antivirus software and robust passwords would suffice, whereas a network of an important government organization might need to be protected using a strong firewall and proxy, encryption, strong antivirus software and a two- or three-factor authentication system, etc.

# Information Security

- Information security is concerned with protecting information from getting in to the hands of unauthorized parties.
- Main principles of information security are considered as providing confidentiality, integrity and availability.
- Other elements like possession, authenticity and utility were proposed.
- Confidentiality concerns with preventing information from going in to unauthorized parties.
- Integrity makes sure that information cannot be modified secretly.
- Availability is concerned with whether the information is available when they are required.
- Availability also makes sure that the information system is not susceptible to attacks like denial-of-service (DOS).
- Authenticity is important for verifying the identities of two parties involved in a communication (that carry information).
- Information security uses cryptography, especially when transferring information.
- Information would be encrypted such that it would be unusable to anyone other than the authorized users.



# Network and Information Security

- Network security involves methods or practices used to protect a computer network from unauthorized accesses, misuses or modifications,
- Information security prevents unauthorized accesses, misuses and modifications to information systems.
- Software and tools used for achieving network security and information security might overlap.
- For example, antivirus software, firewalls and authentication schemes have to be employed by both the tasks.
- The two tasks complement each other in the sense if you cannot make sure that the network is secure, you can never guarantee that the information in the network is secure.

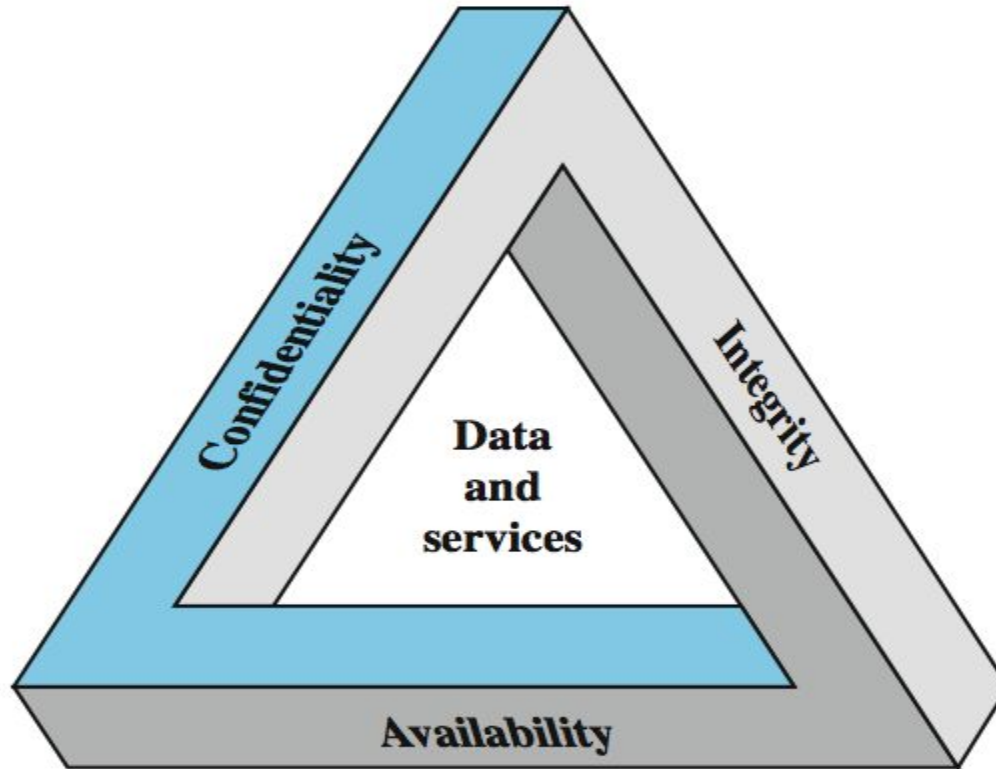
# Cyber vs Information Security

Cyber Security	Information Security
Protection of digital or electronic data	Protection of both physical and digital data
Protects data from unauthorized digital access	Protecting information with CIA triad
It deals with advanced persistent threats like phishing, baiting, data breach etc	It is foundation of data security

# Background- Why Security

- Information Security requirements have changed in recent times
- Traditionally provided by physical and administrative mechanisms
- 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

# Key Security Concepts/Security Goals



# Key Security Concepts

- **Confidentiality**

- (covers both data confidentiality and privacy): preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

- **Integrity**

- (covers both data and system integrity): Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

- **Availability:**

- Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

# Key Security Concepts

## Additionally

- **Authenticity:**

- The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.

- **Accountability:**

- Accountability is an essential information security concept.
- Every individual who works with an information system should have specific responsibilities for information assurance.
- The tasks for which a individual is responsible are part of the overall information security plan and can be readily measurable by a person who has managerial responsibility for information assurance.
- One example would be a policy statement that all employees must avoid installing outside software on a company-owned information infrastructure. The person in charge of information security should perform periodic checks to be certain that the policy is being followed.

# Challenges in security

- The one-word labels: confidentiality, authentication, nonrepudiation, integrity. But the mechanisms used to meet those requirements can be quite complex
- successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism.
- Having designed various security mechanisms, it is necessary to decide where to use them. This is true both in terms of physical placement (e.g., at what points in a network are certain security mechanisms needed) and in a logical sense [e.g., at what layer or layers of an architecture such as TCP/IP (Transmission Control Protocol/Internet Protocol) should mechanisms be placed].

# Challenges in security

- Security requires regular, even constant, monitoring, and this is difficult in today's short-term, overloaded environment
- Computer and network security is essentially a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them. The great advantage that the attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security.
- Many users (and even security administrators) view strong security as an impediment to efficient and user-friendly operation of an information system or use of information



# Security Attacks, Services, and Mechanisms

- **Security Attacks:** 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 attacks
- **Security Services:** A service that enhances the data processing systems and the information transfers of an organization

# Threat/Attack

## Threat

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.

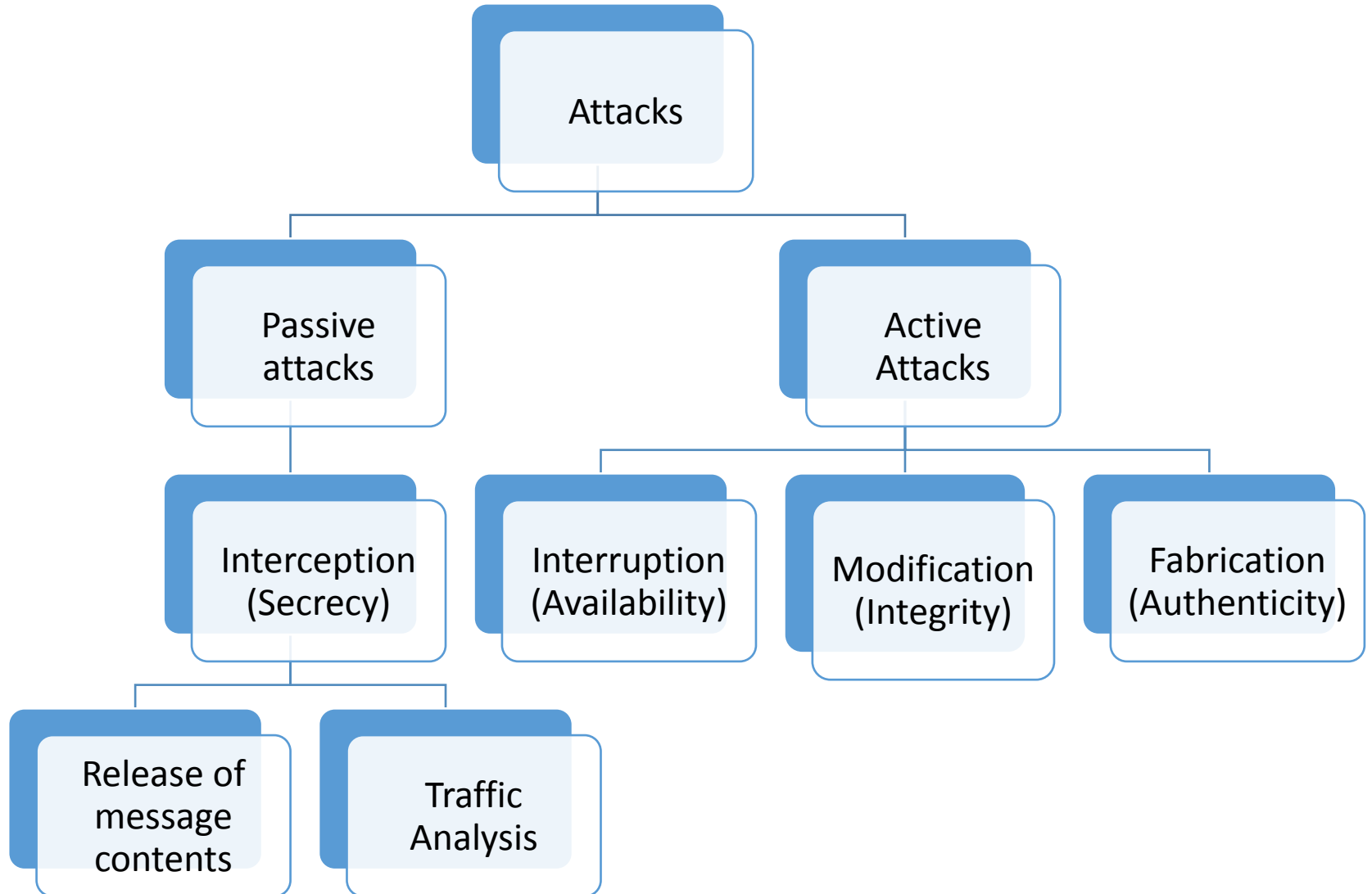
# Security Attack

- 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
- Have a wide range of attacks
- Can focus of generic types of attacks
- Often *threat* & *attack* mean same

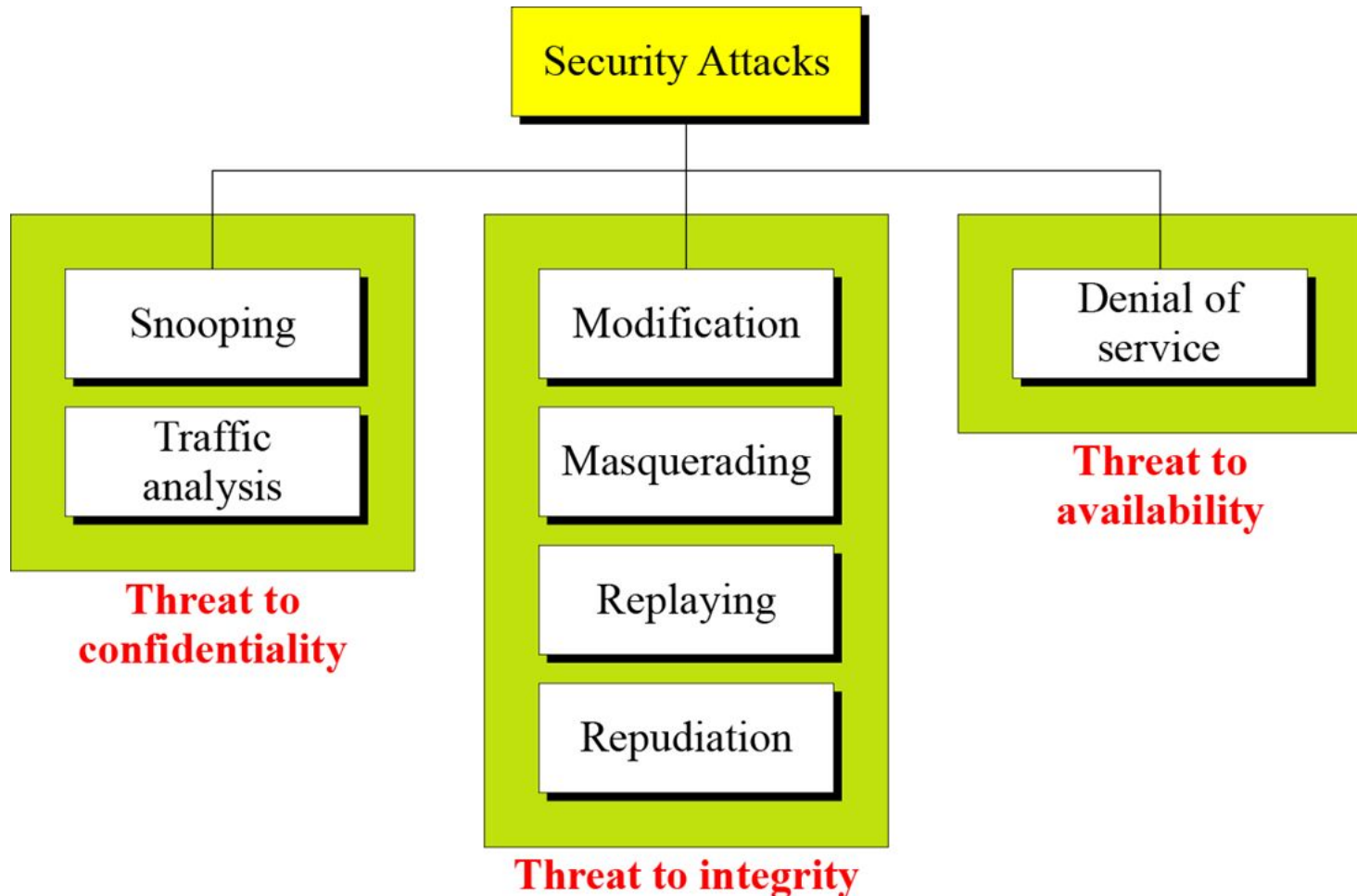
# Cryptographic Attacks

- They are broadly classified as
  - Cryptanalytic attacks
  - Non Cryptanalytic attacks

# Security Attacks



# Taxonomy of Attacks w.r.t. Security Goals



# Classify Security Attacks as

- **passive attacks** - eavesdropping on, or monitoring of, transmissions to:
  - obtain message contents, or
  - monitor traffic flows
- **active attacks** – modification of data stream to:
  - masquerade of one entity as some other
  - replay previous messages
  - modify messages in transit
  - denial of service

# Active Attacks

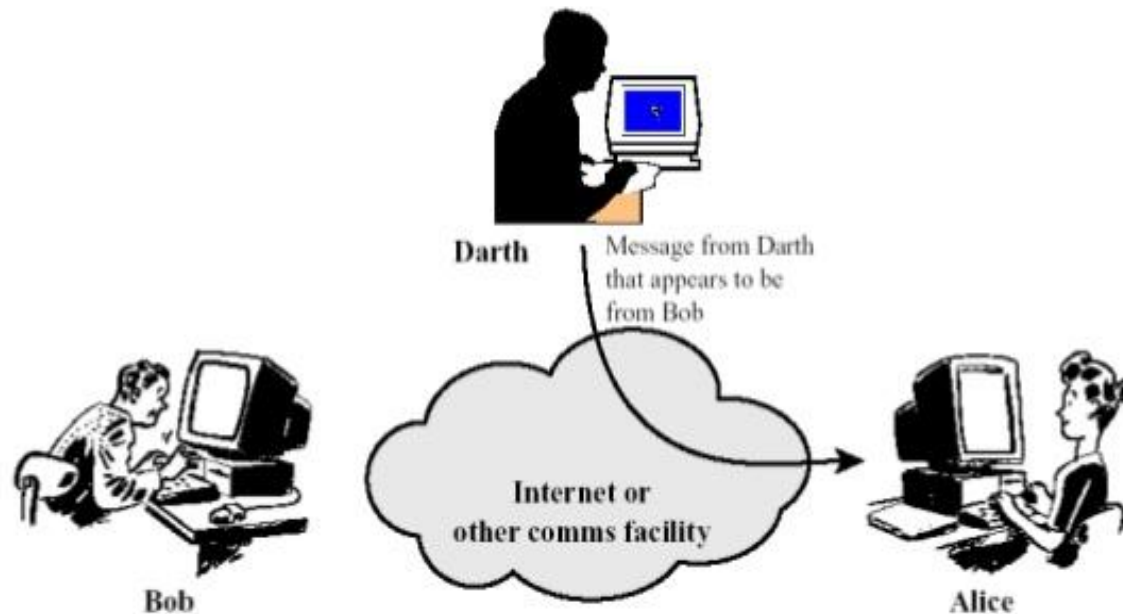
- **Active Attacks**

Active attacks involve some modification of the data stream or the creation of a false stream, and are hard to prevent.

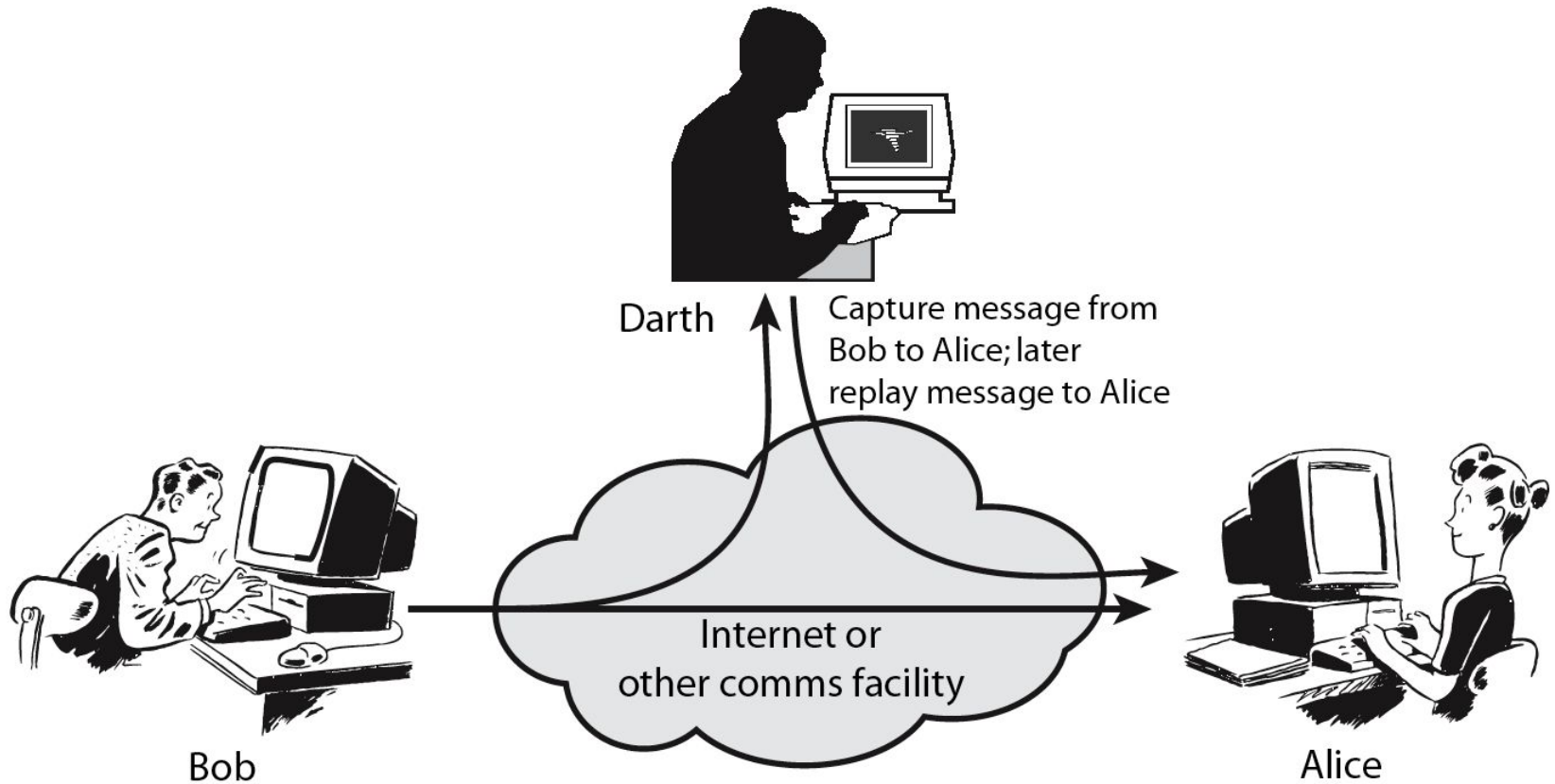
- Masquerade
  - pretends to be a different entity
- Replay
  - passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect
- Modification of messages
  - alters some portion of a legitimate message
- Denial of service
  - prevents or inhibits the normal use or management of communications facilities



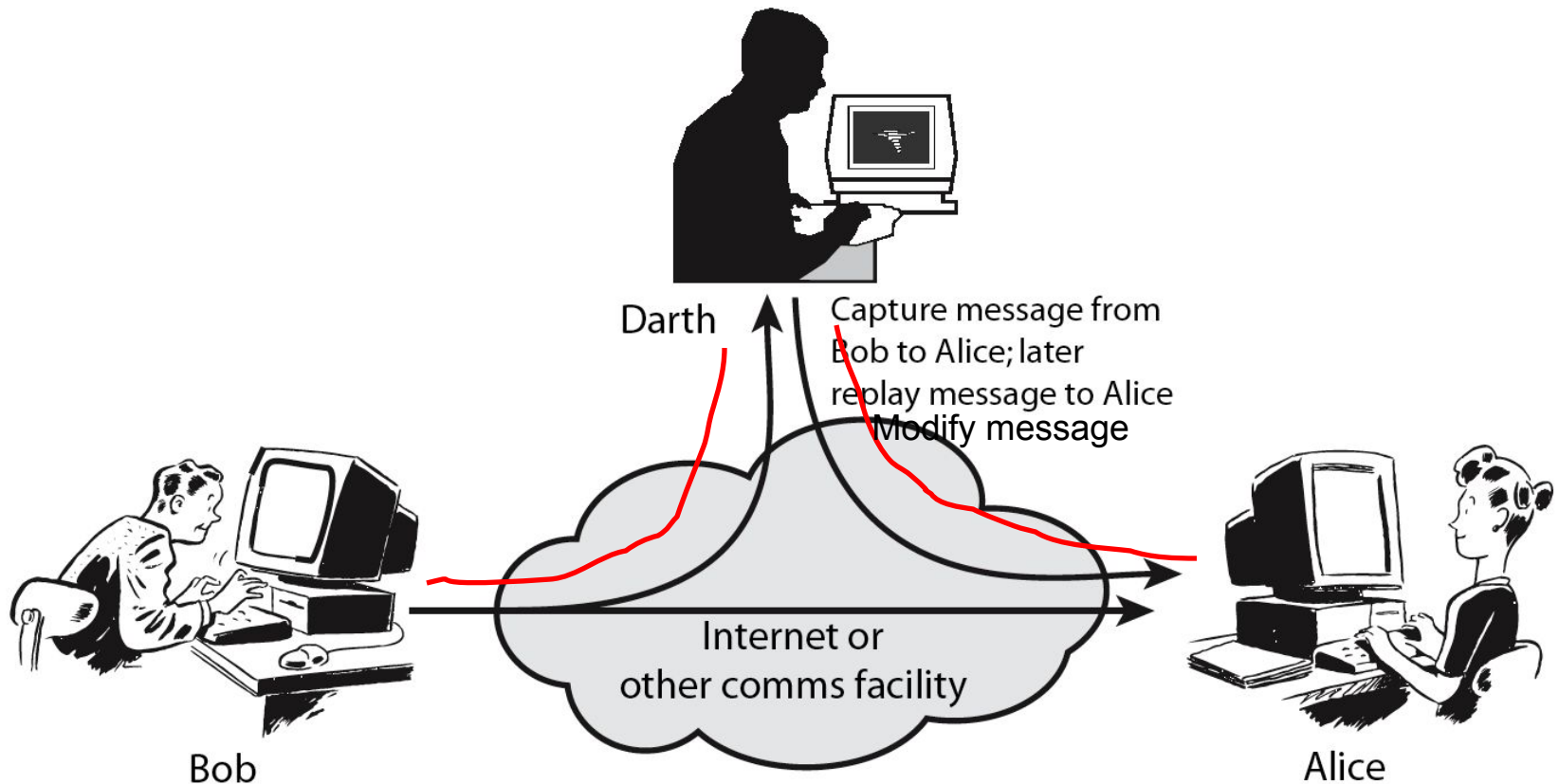
# Active Attack: Masquerade



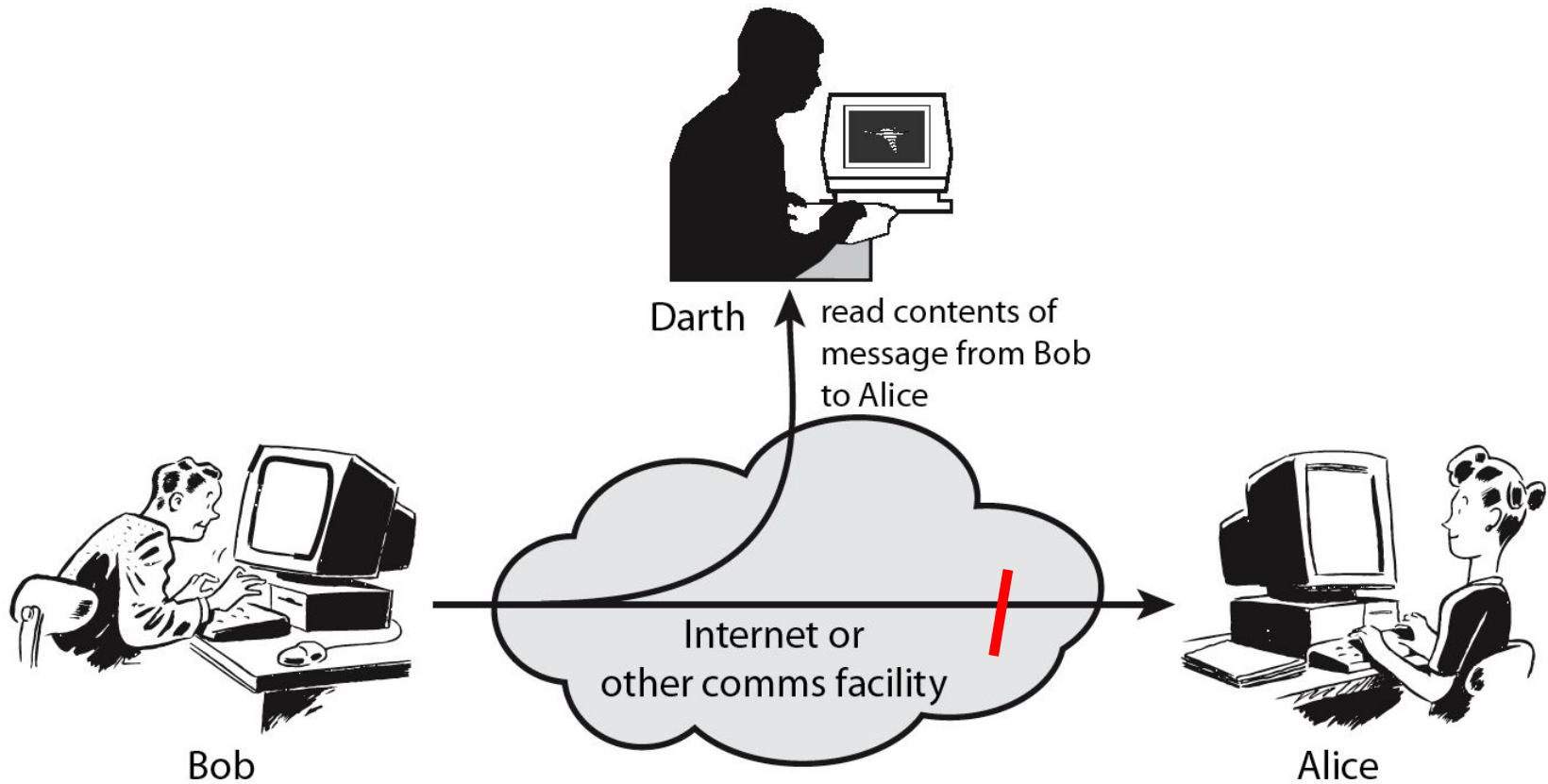
# Active Attack: Replay



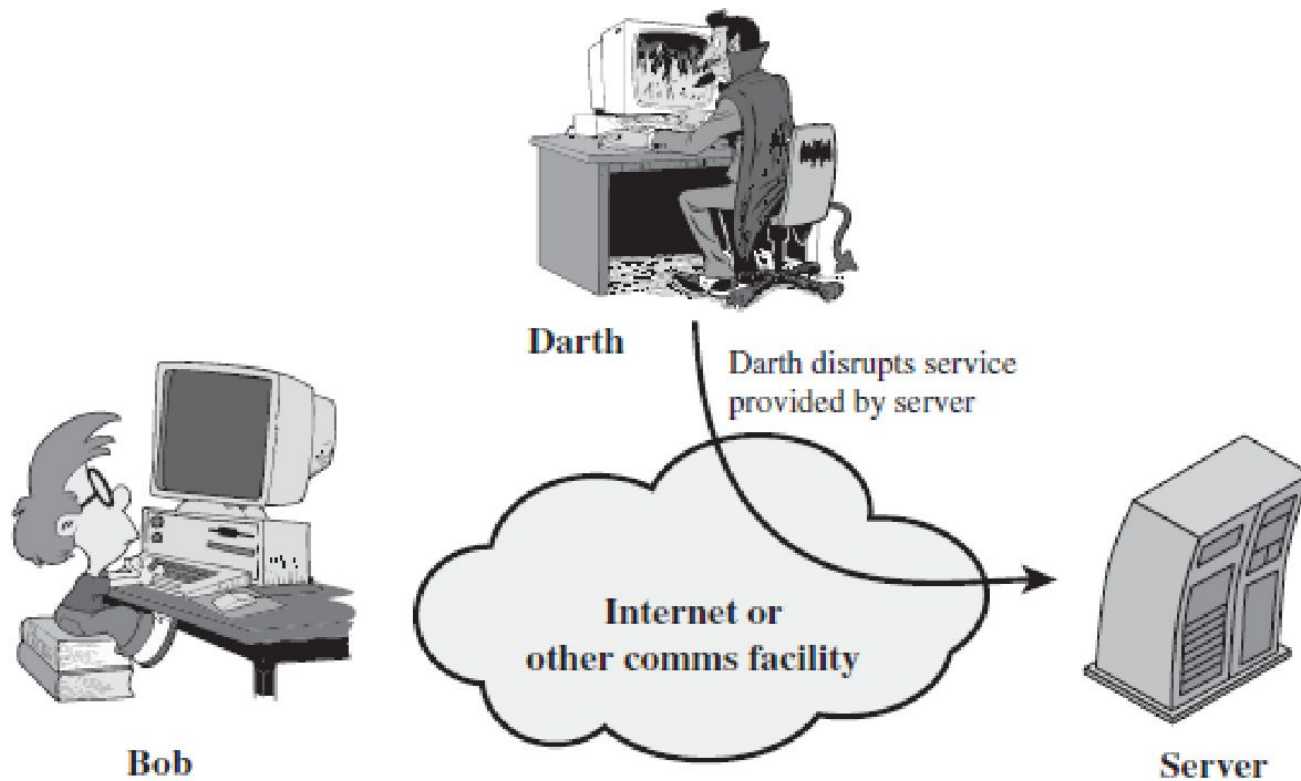
# Active Attack: Modification



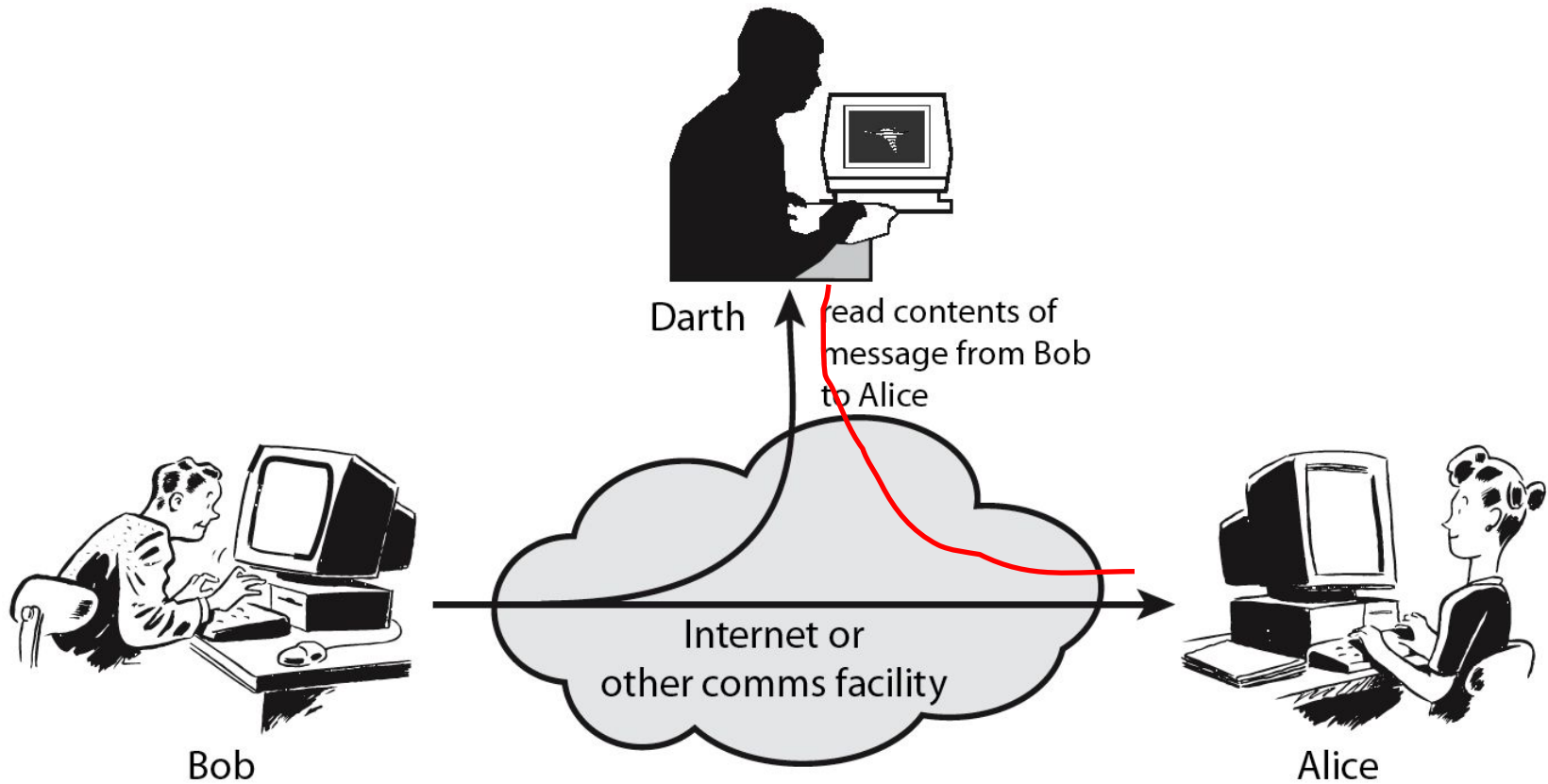
# Active Attack: Interruption



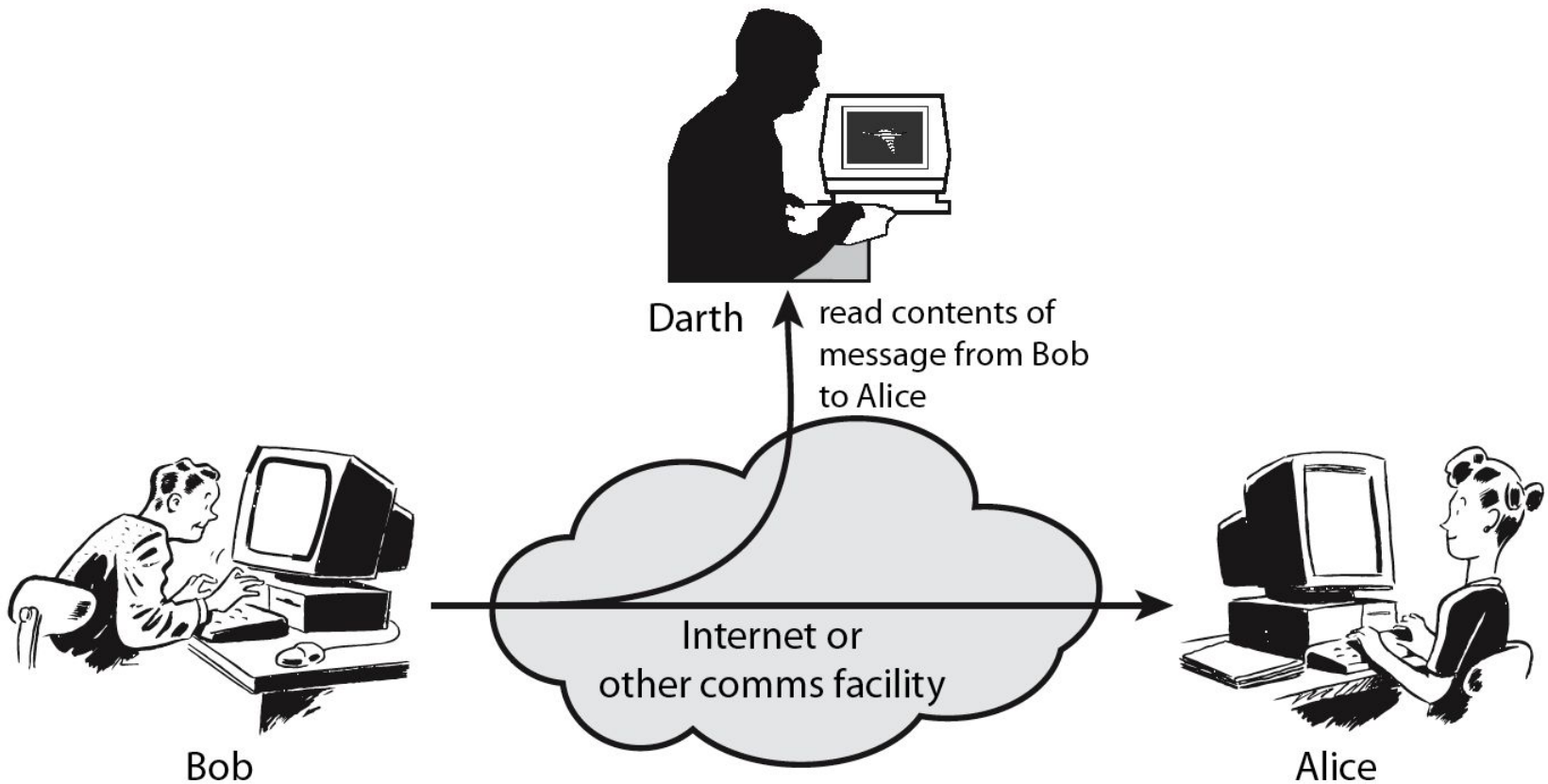
# Active Attack: denial of service attack



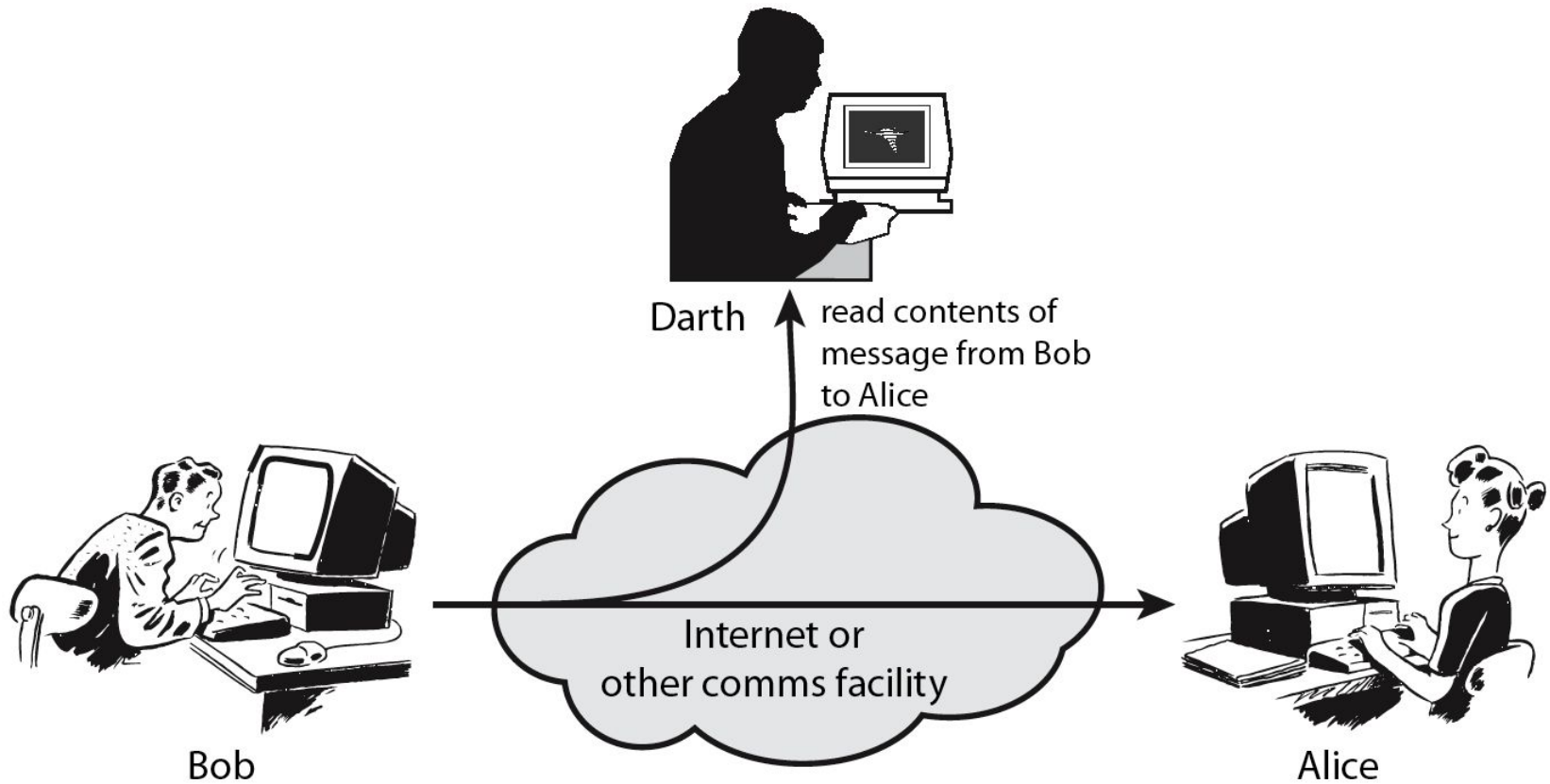
# Active Attack: Fabrication



# Passive Attack - Interception



# Passive Attack: Traffic Analysis





# Handling Attacks

- Passive attacks – focus on Prevention
  - Easy to stop
  - Hard to detect
- Active attacks – focus on Detection and Recovery
  - Hard to stop
  - Easy to detect

# Fabrication and modification difference

- **Fabrication:**

- An unauthorized party inserts counterfeit objects into the system and basically attacks the authenticity of the system.
- the attacker creates data that is to fool the system from scratch. That data does not exist, the attacker produces it.

- **Modification:**

- An unauthorized party modifies the assets of the system and basically attacks the integrity of the system.
- Originally legitimate data is intercepted and changed before it reaches the validating system in order to trick that system into doing something different than the original sender intended

# Categorization of Attacks

<i>Attacks</i>	<i>Passive/Active</i>	<i>Threatening</i>
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability

# X.800

- ITU-T provides some security services and some mechanisms to implement those services. Security services and mechanisms are closely related because a mechanism or combination of mechanisms are used to provide a service..
- 
- This standard defines a security service as a service that is provided by the protocol layer of open systems
- X.800 defines these services into five categories and fourteen specific services

# Security services X.800

Table 1.2 Security Services (X.800)

<p style="text-align: center;"><b>AUTHENTICATION</b></p> <p>The assurance that the communicating entity is the one that it claims to be.</p> <p><b>Peer Entity Authentication</b> Used in association with a logical connection to provide confidence in the identity of the entities connected.</p> <p><b>Data-Origin Authentication</b> In a connectionless transfer, provides assurance that the source of received data is as claimed.</p> <p style="text-align: center;"><b>ACCESS CONTROL</b></p> <p>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).</p> <p style="text-align: center;"><b>DATA CONFIDENTIALITY</b></p> <p>The protection of data from unauthorized disclosure.</p> <p><b>Connection Confidentiality</b> The protection of all user data on a connection.</p> <p><b>Connectionless Confidentiality</b> The protection of all user data in a single data block</p> <p><b>Selective-Field Confidentiality</b> The confidentiality of selected fields within the user data on a connection or in a single data block.</p> <p><b>Traffic-Flow Confidentiality</b> The protection of the information that might be derived from observation of traffic flows.</p>	<p style="text-align: center;"><b>DATA INTEGRITY</b></p> <p>The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).</p> <p><b>Connection Integrity with Recovery</b> 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.</p> <p><b>Connection Integrity without Recovery</b> As above, but provides only detection without recovery.</p> <p><b>Selective-Field Connection Integrity</b> Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.</p> <p><b>Connectionless Integrity</b> Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.</p> <p><b>Selective-Field Connectionless Integrity</b> Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.</p> <p style="text-align: center;"><b>NONREPUDIATION</b></p> <p>Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.</p> <p><b>Nonrepudiation, Origin</b> Proof that the message was sent by the specified party.</p> <p><b>Nonrepudiation, Destination</b> Proof that the message was received by the specified party.</p>
---	--

# Security services-Mechanism (X.800 standard)

Security Service	Security Mechanism
Data Confidentiality	Encipherment and Routing Control
Data Integrity	Encipherment, digital Signature, data integrity
Authentication	Encipherment, digital signature,
Non Repudiation	Digital Signature, data integrity
Access Control	Access control mechanism

# Security Service

- Enhances the security of the data processing systems and the information transfers of an organization
- intended to counter security attacks
- make use of one or more security mechanisms to provide the service
- replicate functions normally associated with physical documents
  - eg have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

# Security services category

- Authentication
  - Peer entity authentication
    - Used in association with a logical connection to provide confidence in the identity of the entities connected.
  - Data-Origin Authentication
    - In a connectionless transfer, provides assurance that the source of received data is as claimed



# Security services category

- Access control
  - The prevention of unauthorized use of a resource
  - It controls who can have access to a resource, under what conditions access can occur,

# Security services category

- Data confidentiality
  - Connection confidentiality
    - The protection of all user data on a connection.
  - Connectionless Confidentiality
    - The protection of all user data in a single data block.
  - Selective-Field Confidentiality
    - The confidentiality of selected fields within the user data on a connection or in a single data block.
  - Traffic-Flow Confidentiality
    - The protection of the information that might be derived from observation of traffic flows.

# Security services category

- Data Integrity
  - Connection Integrity with Recovery
  - Connection Integrity without Recovery
  - Selective field connection integrity
  - Connectionless Integrity
  - Selective field connectionless integrity
- Nonrepudiation
  - Nonrepudiation, Origin
  - Nonrepudiation, Destination

# Security services category

- Data Integrity- data received are exactly as sent by an authorized entity
- **Connection 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.
- **Connection Integrity without Recovery**
  - Provides only detection without recovery.
- **Selective-Field Connection Integrity**
  - Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.
- **Connectionless Integrity**
  - Provides for the integrity of a single connectionless data block and may take the form of detection of data modification.
- **Selective-Field Connectionless Integrity**
  - Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

# Security services category

- NonRepudiation

- Nonrepudiation is the assurance that someone cannot deny something. Typically, nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

- Nonrepudiation, Origin

- Proof that the message was sent by the specified party.

- Nonrepudiation, Destination

- Proof that the message was received by the specified party.

# Security Mechanism

- a mechanism that is designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all functions required
- however one particular element underlies many of the security mechanisms in use: **cryptographic techniques**

# Security mechanisms

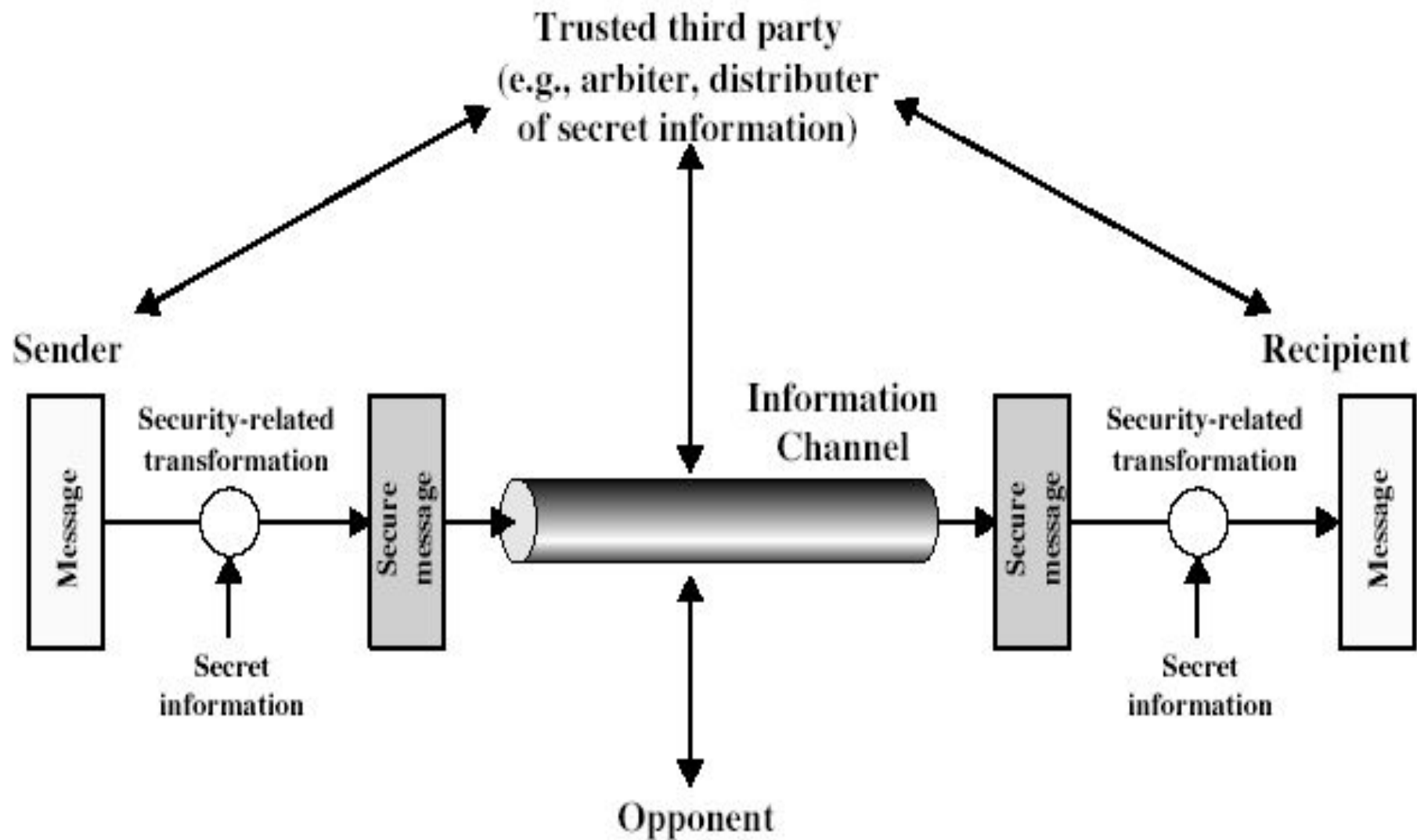
- Encipherment
  - The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.
- Digital signature
  - Data appended to, or a cryptographic transformation 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).
- Access control
- Traffic Padding
  - The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts
- Routing control
- Notarization
  - The use of a trusted third party to assure certain properties of a data exchange.

# Security mechanisms

## Pervasive security mechanisms

- Trusted functionality
  - That which is 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 Audit Trail
  - Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities
- Security Recovery
  - Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

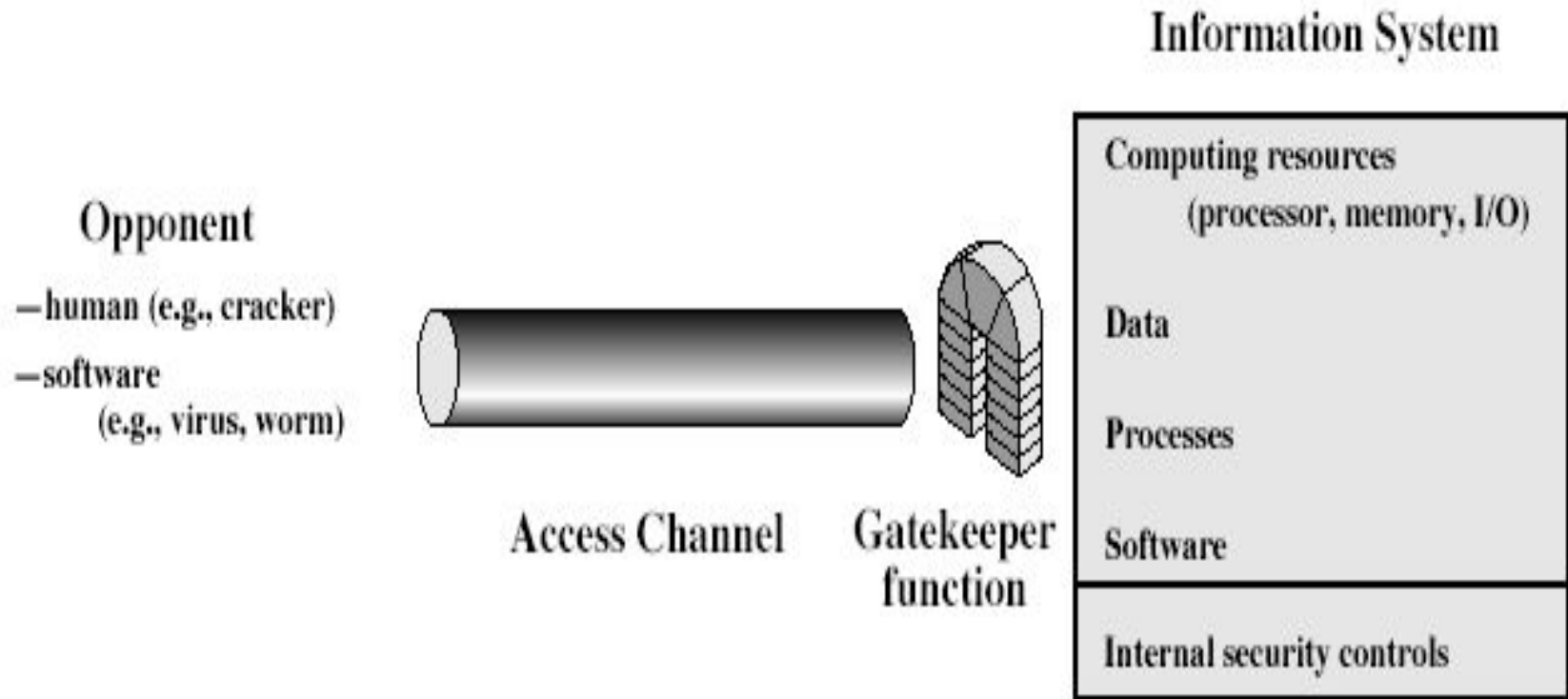




# Model for Network Security

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

# Model for Network Access Security



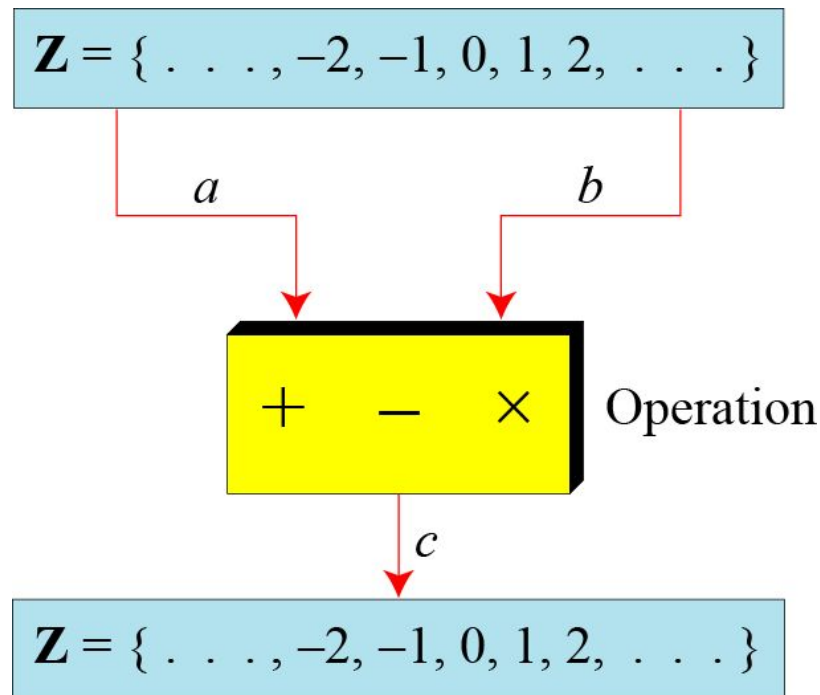
# Modular Arithmetic

The set of integers, denoted by  $\mathbb{Z}$ , contains all integral numbers (with no fraction) from negative infinity to positive infinity

The set of integers

$$\mathbf{Z} = \{ \dots, -2, -1, 0, 1, 2, \dots \}$$

# Binary operation for set of integers



Three Binary operation for set of integers

# Binary operations

The following shows the results of the three binary operations on two integers. Because each input can be either positive or negative, we can have four cases for each operation.

Add:	$5 + 9 = 14$	$(-5) + 9 = 4$	$5 + (-9) = -4$	$(-5) + (-9) = -14$
Subtract:	$5 - 9 = -4$	$(-5) - 9 = -14$	$5 - (-9) = 14$	$(-5) - (-9) = +4$
Multiply:	$5 \times 9 = 45$	$(-5) \times 9 = -45$	$5 \times (-9) = -45$	$(-5) \times (-9) = 45$

# Integer division

In integer arithmetic, if we divide  $a$  by  $n$ , we can get  $q$  and  $r$ . The relationship between these four integers can be shown as

$$a = q \times n + r$$

# Integer Division

Assume that  $a = 255$  and  $n = 11$ . We can find  $q = 23$  and  $R = 2$  using the division algorithm.

$$\begin{array}{r} \textcolor{teal}{n} \longrightarrow 11 \quad \overline{) 255} \\ \underline{22} \phantom{0} \\ 35 \\ \underline{33} \\ 2 \end{array}$$

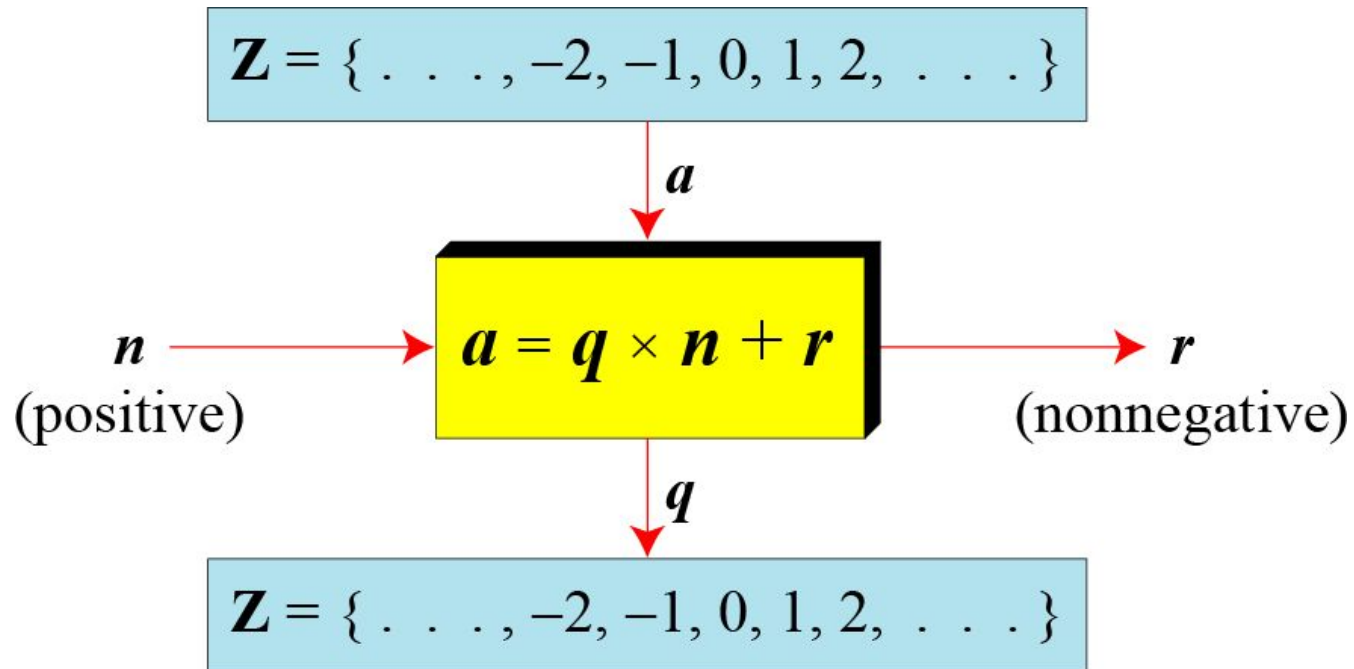
$23 \longleftarrow \textcolor{teal}{q}$

$255 \longleftarrow \textcolor{teal}{a}$

$2 \longleftarrow \textcolor{teal}{r}$



# Restrictions on integer Division



# Restrictions on integer Division

When we use a computer or a calculator,  $r$  and  $q$  are negative when  $a$  is negative. How can we apply the restriction that  $r$  needs to be positive? The solution is simple, we decrement the value of  $q$  by 1 and we add the value of  $n$  to  $r$  to make it positive.

$$-255 = (-\mathbf{23} \times 11) + (-\mathbf{2}) \quad \leftrightarrow \quad -255 = (-\mathbf{24} \times 11) + \mathbf{9}$$

# Integer Division.....

If  $a$  is not zero and we let  $r = 0$  in the division relation, we get

$$a = q \times n$$

If the remainder is zero,  $a | n$

If the remainder is not zero,  $a \nmid n$

- a. The integer 4 divides the integer 32 because  $32 = 8 \times 4$ . We show this as

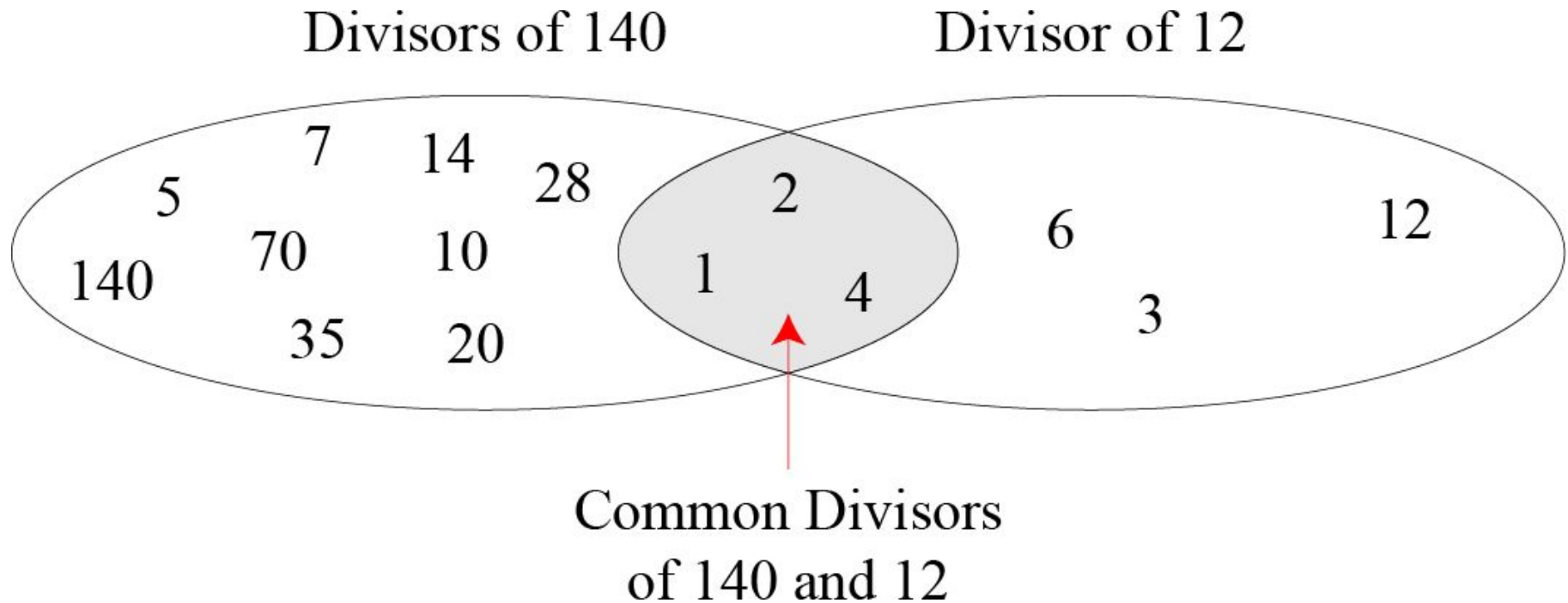
$$4 \mid 32$$

- b. The number 8 does not divide the number 42 because  $42 = 5 \times 8 + 2$ . There is a remainder, the number 2, in the equation. We show this as

$$8 \nmid 42$$

- a. We have  $13|78$ ,  $7|98$ ,  $-6|24$ ,  $4|44$ , and  $11|(-33)$ .
- b. We have  $13 \nmid 27$ ,  $7 \nmid 50$ ,  $-6 \nmid 23$ ,  $4 \nmid 41$ , and  $11 \nmid (-32)$ .

# Common Divisor

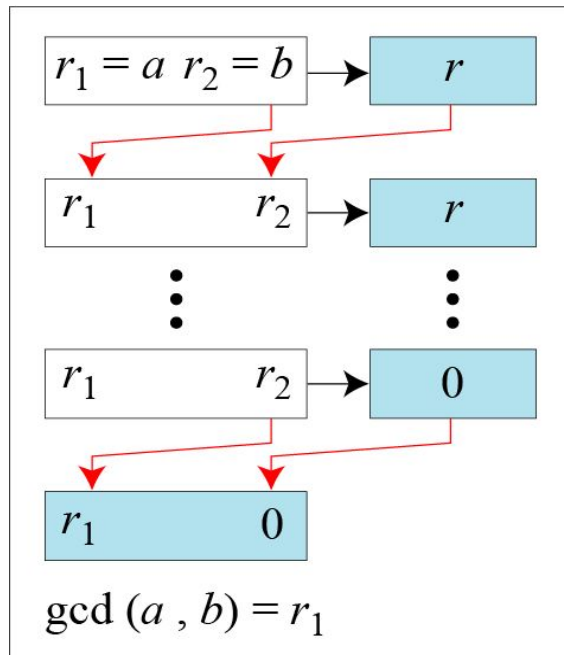


# GCD-Euclidean Algo

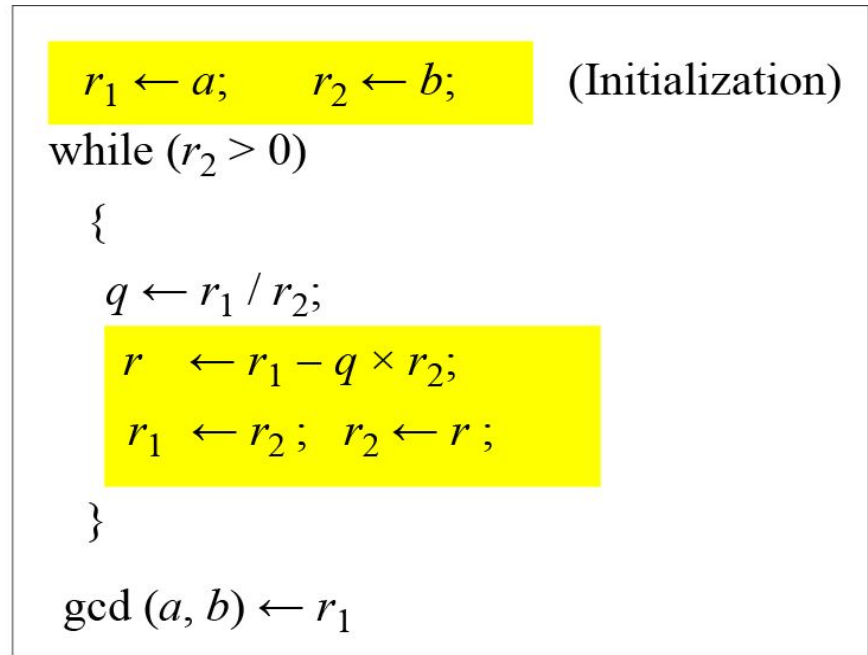
The greatest common divisor of two positive integers is the largest integer that can divide both integers.

Fact 1:  $\gcd(a, 0) = a$

Fact 2:  $\gcd(a, b) = \gcd(b, r)$ , where  $r$  is the remainder of dividing  $a$  by  $b$



a. Process



b. Algorithm

When  $\gcd(a, b) = 1$ , we say that  $a$  and  $b$  are relatively prime.



Find the greatest common divisor of 2740 and 1760. **Solution**

We have  $\gcd(2740, 1760) = 20$ .

$q$	$r_1$	$r_2$	$r$
1	2740	1760	980
1	1760	980	780
1	980	780	200
3	780	200	180
1	200	180	20
9	180	20	0
	<b>20</b>	0	

Find the greatest common divisor of 25 and 60.

**Solution**

We have  $\gcd(25, 60) = 5$ .

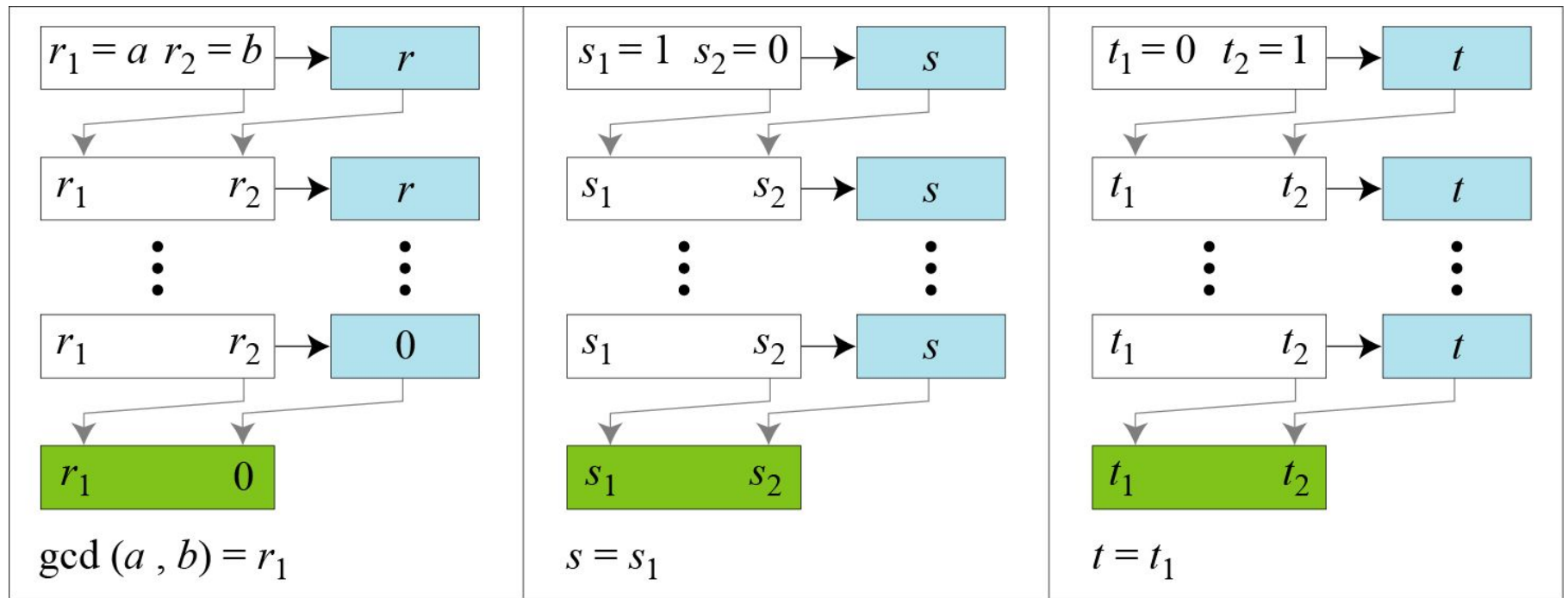
$q$	$r_1$	$r_2$	$r$
0	25	60	25
2	60	25	10
2	25	10	5
2	10	5	0
	<b>5</b>	0	

# Extended Euclidean Algo

It is well known that if the  $\gcd(a, b) = r$  then there exist integers  $p$  and  $s$  so that:

$$s(a) + t(b) = \gcd(a, b).$$

By reversing the steps in the Euclidean Algorithm, it is possible to find these integers  $s$  and  $t$ .



a. Process



## Extended Euclidean algorithm

```
 $r_1 \leftarrow a;$      $r_2 \leftarrow b;$   
 $s_1 \leftarrow 1;$      $s_2 \leftarrow 0;$   
 $t_1 \leftarrow 0;$      $t_2 \leftarrow 1;$ 
```

(Initialization)

```
while ( $r_2 > 0$ )
```

```
{
```

```
   $q \leftarrow r_1 / r_2;$ 
```

```
     $r \leftarrow r_1 - q \times r_2;$ 
```

```
     $r_1 \leftarrow r_2;$   $r_2 \leftarrow r;$ 
```

(Updating  $r$ 's)

```
     $s \leftarrow s_1 - q \times s_2;$ 
```

```
     $s_1 \leftarrow s_2;$   $s_2 \leftarrow s;$ 
```

(Updating  $s$ 's)

```
     $t \leftarrow t_1 - q \times t_2;$ 
```

```
     $t_1 \leftarrow t_2;$   $t_2 \leftarrow t;$ 
```

(Updating  $t$ 's)

```
}
```

```
   $\text{gcd}(a, b) \leftarrow r_1;$   $s \leftarrow s_1;$   $t \leftarrow t_1$ 
```

b. Algorithm

Given  $a = 161$  and  $b = 28$ , find  $\gcd(a, b)$  and the values of  $s$  and  $t$ .

### Solution

We get  $\gcd(161, 28) = 7$ ,  $s = -1$  and  $t = 6$ .

$q$	$r_1$	$r_2$	$r$	$s_1$	$s_2$	$s$	$t_1$	$t_2$	$t$
5	161	28	21	1	0	1	0	1	-5
1	28	21	7	0	1	-1	1	-5	6
3	21	7	0	1	-1	4	-5	6	-23
	7	0		-1	4		6	-23	

Given  $a = 17$  and  $b = 0$ , find  $\gcd(a, b)$  and the values of  $s$  and  $t$ .

### Solution

We get  $\gcd(17, 0) = 17$ ,  $s = 1$ , and  $t = 0$ .

$q$	$r_1$	$r_2$	$r$	$s_1$	$s_2$	$s$	$t_1$	$t_2$	$t$
	<b>17</b>	<b>0</b>		<b>1</b>	<b>0</b>		<b>0</b>	<b>1</b>	

Given  $a = 0$  and  $b = 45$ , find  $\gcd(a, b)$  and the values of  $s$  and  $t$ .

### Solution

We get  $\gcd(0, 45) = 45$ ,  $s = 0$ , and  $t = 1$ .

$q$	$r_1$	$r_2$	$r$	$s_1$	$s_2$	$s$	$t_1$	$t_2$	$t$
0	0	45	0	1	0	1	0	1	0
	<b>45</b>	0		0	1		<b>1</b>	0	



The modulo operation creates a set, which in modular arithmetic is referred to as the set of least residues modulo  $n$ , or  $Z_n$ .


Figure 2.10 Some  $Z_n$  sets

$$Z_n = \{ 0, 1, 2, 3, \dots, (n-1) \}$$

$$Z_2 = \{ 0, 1 \}$$

$$Z_6 = \{ 0, 1, 2, 3, 4, 5 \}$$

$$Z_{11} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \}$$



To show that two integers are congruent, we use the congruence operator ( $\equiv$ ). For example, we write:

$$2 \equiv 12 \pmod{10}$$

$$3 \equiv 8 \pmod{5}$$

$$13 \equiv 23 \pmod{10}$$

$$8 \equiv 13 \pmod{5}$$

# Additive Inverse

In  $Z_n$ , two numbers  $a$  and  $b$  are additive inverses of each other if

$$a + b \equiv 0 \pmod{n}$$

In modular arithmetic, each integer has an additive inverse. The sum of an integer and its additive inverse is congruent to 0 modulo  $n$ .

$$a \times b \equiv 1 \pmod{n}$$

$$\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$$

Multiplicative inverse

$$(3, 3)(1, 1)$$

Find all additive inverse pairs in  $\mathbb{Z}_{10}$ .

### Solution

The six pairs of additive inverses are  $(0, 0)$ ,  $(1, 9)$ ,  $(2, 8)$ ,  $(3, 7)$ ,  $(4, 6)$ , and  $(5, 5)$ .

# Multiplicative Inverse

In  $\mathbb{Z}_n$ , two numbers  $a$  and  $b$  are the multiplicative inverse of each other if

$$a \times b \equiv 1 \pmod{n}$$

In modular arithmetic, an integer may or may not have a multiplicative inverse.

When it does, the product of the integer and its multiplicative inverse is congruent to 1 modulo  $n$ .

Find the multiplicative inverse of 8 in  $\mathbb{Z}_{10}$ .

There is no multiplicative inverse because  $\gcd(10, 8) = 2 \neq 1$ . In

other words, we cannot find any number between 0 and 9 such that when multiplied by 8, the result is congruent to 1.

Find all multiplicative inverses in  $\mathbb{Z}_{10}$ .

### Solution

There are only three pairs: (1, 1), (3, 7) and (9, 9). The numbers

0, 2, 4, 5, 6, and 8 do not have a multiplicative inverse.

## 2.2.5

### Example 2.24

Find all multiplicative inverse pairs in  $\mathbb{Z}_{11}$ .

#### Solution

We have seven pairs:  $(1, 1)$ ,  $(2, 6)$ ,  $(3, 4)$ ,  $(5, 9)$ ,  $(7, 8)$ ,  $(9, 9)$ , and  $(10, 10)$ .

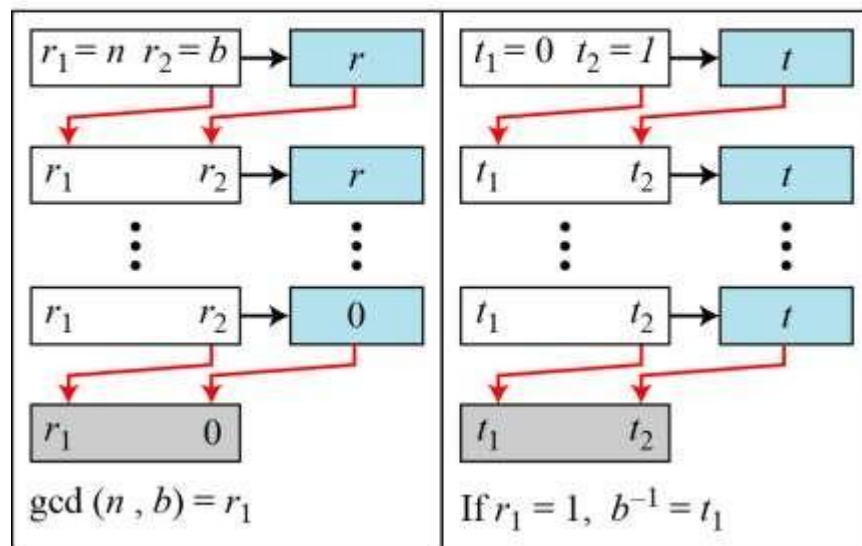


# Multiplicative Inverse using Euclidean algo

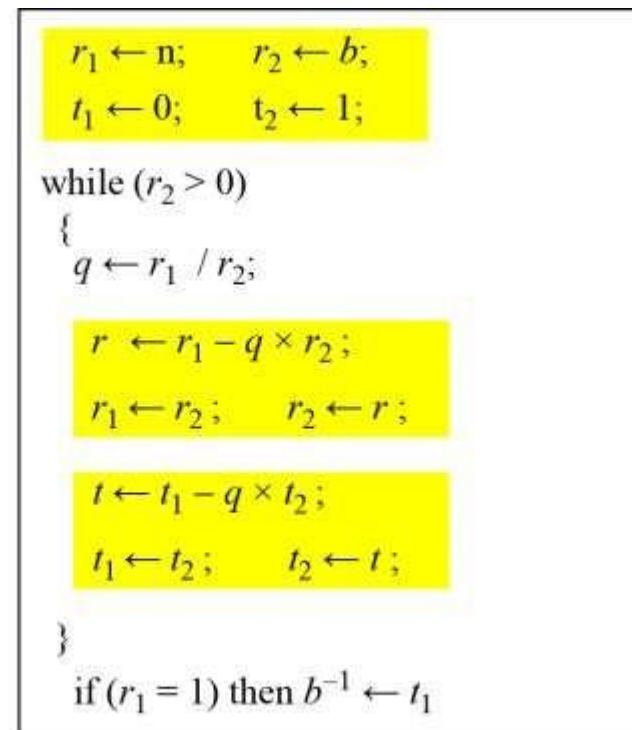
The extended Euclidean algorithm finds the multiplicative inverses of  $b$  in  $Z_n$  when  $n$  and  $b$  are given and

$$\gcd(n, b) = 1.$$

The multiplicative inverse of  $b$  is the value of  $t$  after being mapped to  $Z_n$ .



a. Process



b. Algorithm

Find the multiplicative inverse of 11 in  $\mathbb{Z}_{26}$ .

$q$	$r_1$	$r_2$	$r$	$t_1$	$t_2$	$t$
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	26
	1	0		-7	26	

The gcd (26, 11) is 1; the inverse of 11 is -7 or 19.

Find the multiplicative inverse of 23 in  $\mathbb{Z}_{100}$ .

Solution

$q$	$r_1$	$r_2$	$r$	$t_1$	$t_2$	$t$
4	100	23	8	0	1	-4
2	23	8	7	1	-4	19
1	8	7	1	-4	9	-13
7	7	1	0	9	-13	100
	1	0		-13	100	

The gcd (100, 23) is 1; the inverse of 23 is -13 or 87.

Find the inverse of 12 in  $\mathbb{Z}_{26}$ .

Solution

$q$	$r_1$	$r_2$	$r$	$t_1$	$t_2$	$t$
2	26	12	2	0	1	-2
6	12	2	0	1	-2	13
	2	0		-2	13	

The gcd (26, 12) is 2; the inverse does not exist.

$$\mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\}$$

$$\mathbf{Z}_6^* = \{1, 5\}$$

$$\mathbf{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$$

$$\mathbf{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$$

$$\mathbf{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

$$\mathbf{Z}_{10}^* = \{1, 3, 7, 9\}$$

We need to use  $\mathbf{Z}_n$  when additive inverses are needed; we need to use  $\mathbf{Z}_n^*$  when multiplicative inverses are needed.

# Euler's totient function

Euler's Totient function  $\Phi(n)$  for an input  $n$  is the count of numbers in  $\{1, 2, 3, \dots, n\}$  that are relatively prime to  $n$ , i.e., the numbers whose GCD (Greatest Common Divisor) with  $n$  is 1.

So  $\Phi(n)$  where  $[n \geq 1]$  is defined as the number of positive integers that are less than  $n$  and co prime to  $n$

$$\Phi(n) = n-1$$

# Euler's totient function

$$\Phi(1) = 1$$

$\gcd(1, 1)$  is 1

$$\Phi(2) = 1$$

$\gcd(1, 2)$  is 1, but  $\gcd(2, 2)$  is 2.

$$\Phi(3) = 2$$

$\gcd(1, 3)$  is 1 and  $\gcd(2, 3)$  is 1

$$\Phi(4) = 2$$

$\gcd(1, 4)$  is 1 and  $\gcd(3, 4)$  is 1

$$\Phi(5) = 4$$

$\gcd(1, 5)$  is 1,  $\gcd(2, 5)$  is 1,

$\gcd(3, 5)$  is 1 and  $\gcd(4, 5)$  is 1

$$\Phi(6) = 2$$

$\gcd(1, 6)$  is 1 and  $\gcd(5, 6)$  is 1,



# Properties of totient function

Examples

$$\Phi(5) = 5 - 1 = 4$$

$$\Phi(13) = 13 - 1 = 12$$

# Properties of totient function

Examples

$$\Phi(5) = 5 - 1 = 4$$

$$\Phi(13) = 13 - 1 = 12$$

# Properties of totient function

For two prime numbers **a** and **b**,  $\Phi(a.b) = \Phi(a).\Phi(b)$  used in [RSA Algorithm](#)

**Proof :**

$\Phi(a) = a-1$  ,  $\Phi(b) = b-1$  where **a** and **b** are prime number

**Example:**

$a = 5$ ,  $b = 7$ ,  $ab = 35$

$$\Phi(a*b) = \Phi(a)*\Phi(b)$$

$$\Phi(35) = \Phi(5)*\Phi(7)$$

$$= 4*6$$

$$= 24$$

# Euler's Theorem

## Euler's Theorem

Given integer  $n > 1$ , such that  $\gcd(x, n) = 1$  then

$$x^{\Phi(n)} \equiv 1 \pmod{n}$$

## Corollary

Given integer  $n > 1$ , such that  $\gcd(x, n) = 1$  then

$x^{\Phi(n)-1} \pmod{n}$  is a multiplicative inverse of  $x \pmod{n}$ .

## Corollary

Given integer  $n > 1$ ,  $x$ ,  $y$ , and  $a$  positive integers with  $\gcd(a, n) = 1$ . If  $x \equiv y \pmod{\Phi(n)}$ , then

$$a^x \equiv a^y \pmod{n}.$$

# Euler's Theorem

## Example

Let  $x = 4$  and  $n = 165$

$$\gcd(4, 165) = 1$$

$$4^{\Phi(165)} = 1 \pmod{165}$$

$$\Phi(165) = \Phi(15) * \Phi(11)$$

$$= \Phi(3) * \Phi(5) * \Phi(11)$$

$$= 2 * 4 * 10$$

$$= 80$$

$$4^{80} = 1 \pmod{165}$$

# Fermat's Theorem

This is a special case of Euler's Theorem

$$x^{\Phi(n)} = 1 \pmod{n}$$

$$\Phi(n) = n-1$$

$$x^{n-1} = 1 \pmod{n}$$

$$X = 3 \quad n = 5$$

$$3^{5-1} = 1 \pmod{5}$$

$$3^4 = 1 \pmod{5}$$

# Fermat's Theorem

Another variation

$$x^* x^{\Phi(n)} = x^*(1 \pmod n)$$

$$x^{\Phi(n)+1} = x \pmod n$$

$$x^{n-1+1} = x \pmod n$$

$$\mathbf{x^n = x \pmod n}$$