Unit -1

What is Security?

Security in cryptography and network security is the protection of data and networks from unauthorized access, attacks, and other threats.

Categories Of Security:

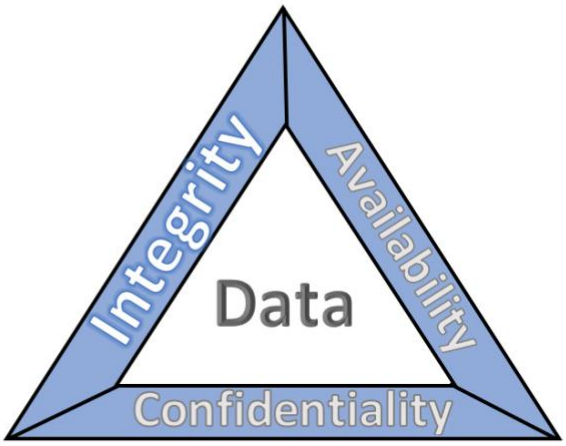
• **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers

• **Network Security** - measures to protect data during their transmission

• **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks

SECURITY GOALS (OR) CIA TRIAD

- The CIA triad is a common model that forms the basis for the development of security systems. They are used for finding vulnerabilities and methods for creating solutions.
- The three letters in "CIA triad" stand for
    i. Confidentiality,
    ii. Integrity,
    iii. Availability.



• **Confidentiality:** Ensuring that sensitive data is only accessible to authorized users (e.g., encryption, access controls).

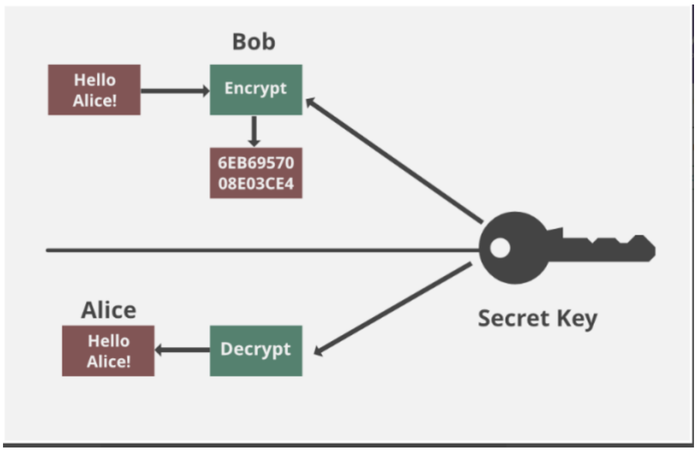
This term covers two related concepts:

Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

Privacy: Assures that individuals control what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Explanation:

The data being sent over the network should not be accessed by unauthorized individuals. The attacker may try to capture the data using different tools available on the Internet and gain access to your information. A primary way to avoid this is to use encryption techniques to safeguard your data so that even if the attacker gains access to your data, he/she will not be able to decrypt it. Encryption standards include **AES**(Advanced Encryption Standard) and **DES** (Data Encryption Standard). Another way to protect your data is through a VPN tunnel. VPN stands for Virtual Private Network and helps the data to move securely over the network.



- **Integrity**: Protecting data from unauthorized modification or corruption (e.g., hashing, digital signatures).

This term covers two related concepts:

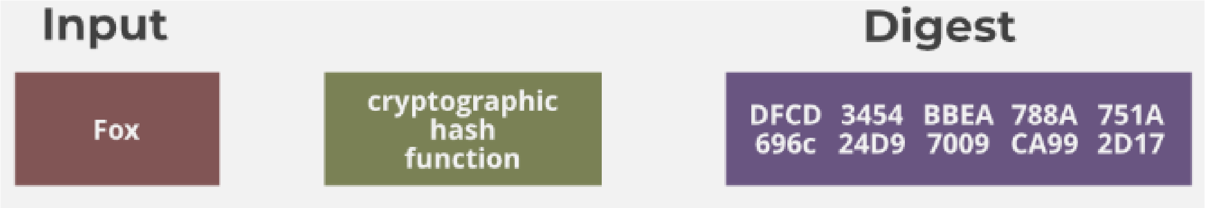
Data integrity: Assures that information (both stored and in transmitted packets) and programs are changed only in a specified and authorized manner.

System integrity refers to the assurance that a computer system and its components (hardware, software, data, and processes) are functioning **correctly, reliably, and as intended** without unauthorized alteration or disruption.

Explanation:

We have two common types: SHA (Secure Hash Algorithm) and MD5(Message Direct 5).

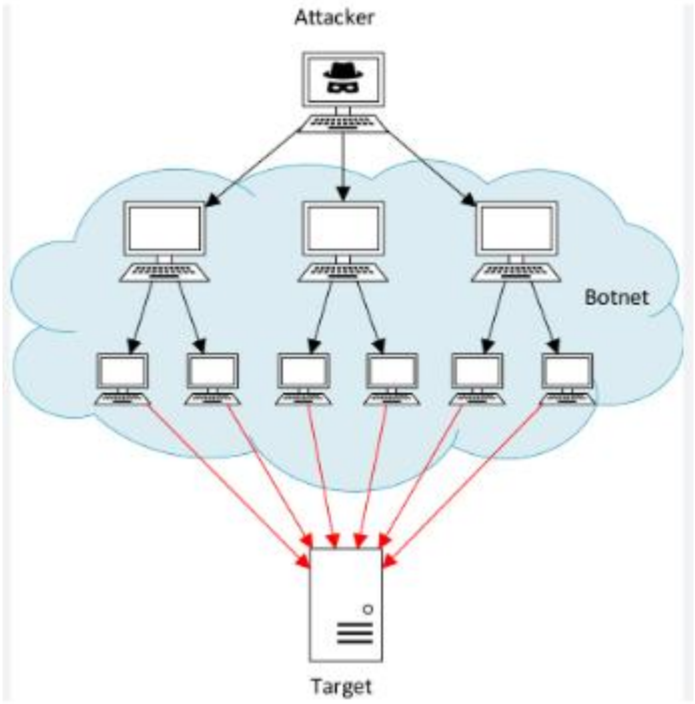
Let’s assume Host ‘A’ wants to send data to Host ‘B’ to maintain integrity. A hash function will run over the data and produce an arbitrary hash value **H1** which is then attached to the data. When Host ‘B’ receives the packet, it runs the same hash function over the data which gives a hash value of **H2**. Now, if **H1 = H2**, this means that the data’s integrity has been maintained and the contents were not modified.


Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696c 24D9 7009 CA99 2D17

• **Availability:** Ensuring that authorized users can access systems and data when needed (e.g., protection against denial-of-service attacks, backups)

To ensure availability, the network administrator should maintain hardware, make regular upgrades, have a plan for fail-over, and prevent bottlenecks in a network.

To protect the network from the Attacks such as DoS or DDoS



Explanation:

A distributed denial-of-service (DDoS) attack is a cybercrime that uses multiple sources to create a fake traffic to a website or network, making it inaccessible to users

A botnet is a collection of internet-connected devices that are infected with malware and **controlled** by a single attacker or group.

- **Authenticity** in cryptography is the process of verifying the source of data and ensuring that it has not been altered or intercepted during transmission.
- **Accountability** in information security refers to the ability to trace actions, operations, or decisions to the individuals or systems responsible for them.

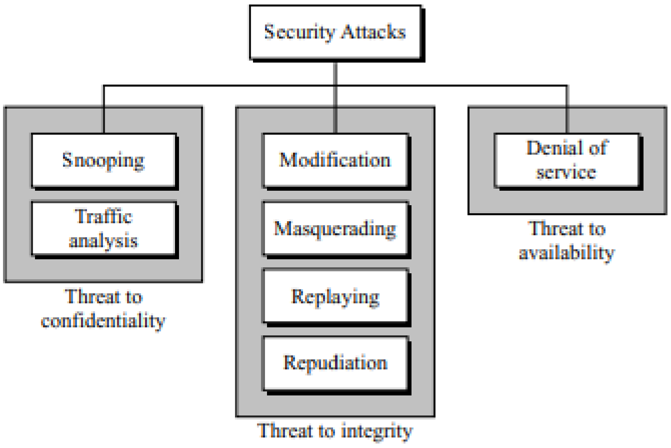
ATTACKS

An attack is a malicious attempt to access or disrupt a computer network or system to steal, change, or destroy data.

Our three goals of security confidentiality, integrity, and availability can be threatened by security attacks.

Figure 1.2 shows the attacks with relation to security goals.

Figure 1.2 *Taxonomy of attacks with relation to security goals*



Attacks Threatening Confidentiality:

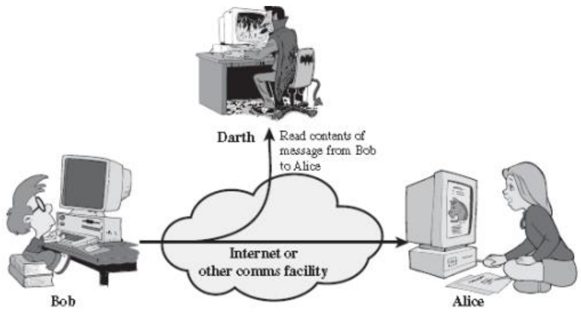
Two types of attacks threaten the confidentiality of information:

- Snooping
- Traffic analysis

Snooping:

Snooping refers to unauthorized access to or interception of data.

For example, a file transferred through the Internet may contain confidential information. An unauthorized entity may intercept the transmission and read the contents of message.


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

(a) Release of message contents

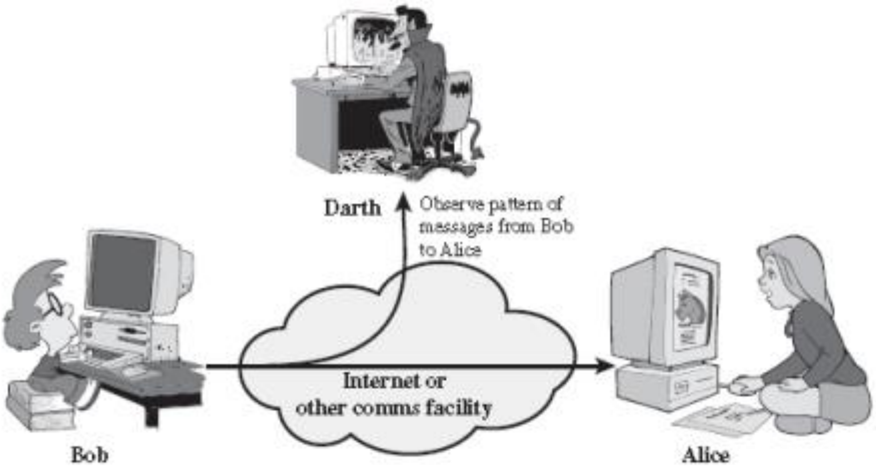
Traffic Analysis:

The attacker does not necessarily intercept or modify the content of the communication. They can obtain some other type information by monitoring online traffic.

They can find the electronic address (such as the e-mail address) of the sender or the receiver.

How Traffic Analysis Works

1. **Observation**: The attacker monitors the network to collect data on communication patterns.
2. **Analysis**: They analyze metadata (e.g., sender/receiver IP addresses, packet sizes, timestamps).


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

(b) Traffic analysis

Attacks Threatening Integrity:

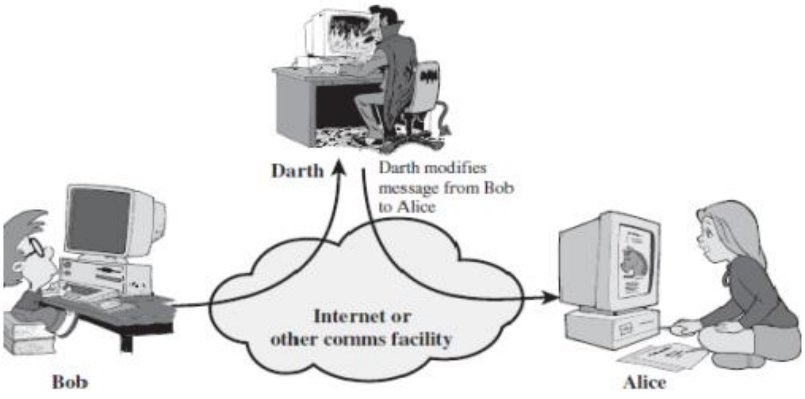
The integrity of data can be threatened by below attacks:

- Modification
- Masquerading
- Replaying
- Repudiation

Modification:

The attacker modifies the information to make it beneficial to herself.

For example, a message meaning “Allow John Smith to read confidential file accounts” is modified to mean “Allow Fred Brown to read confidential file accounts.

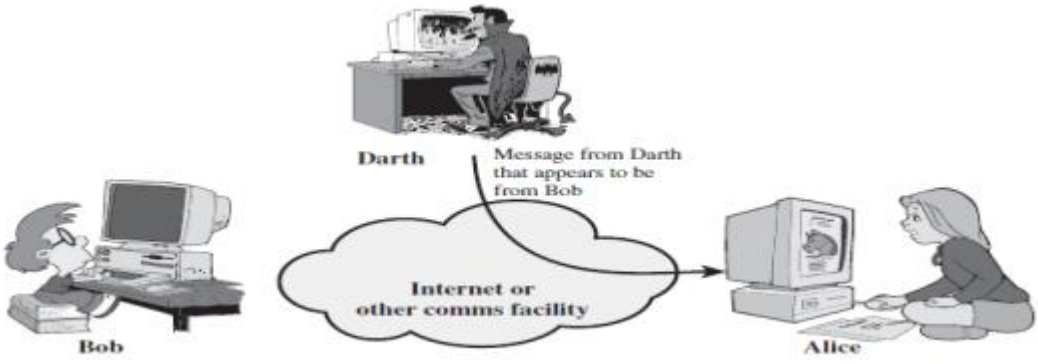

Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

(c) Modification of messages

Masquerading:

Masquerading happens when the attacker impersonates somebody else.

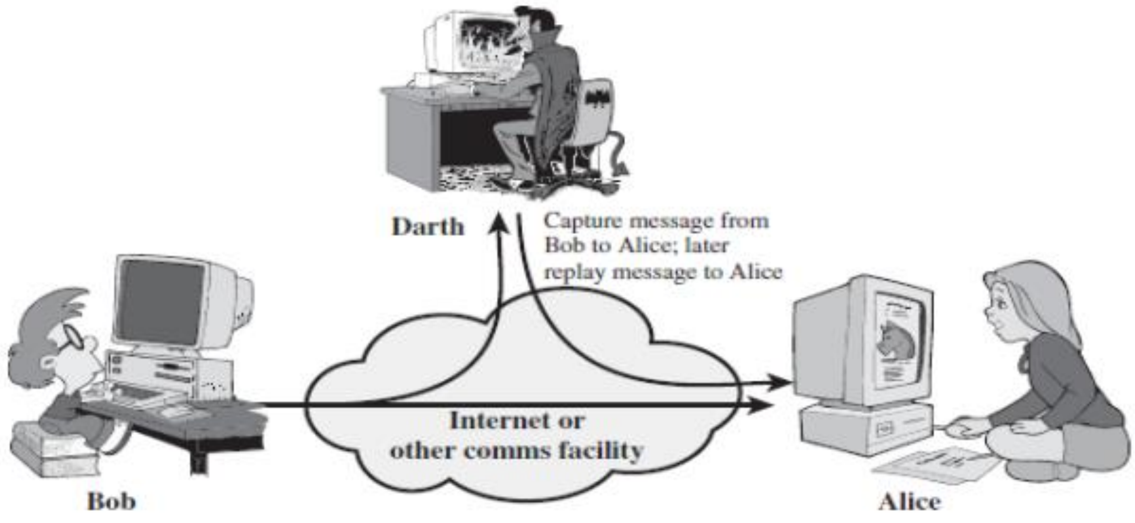
For example, an attacker might steal the bank card and PIN of a bank customer and pretend that she is that customer.


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

(a) Masquerade

Replaying:

The attacker obtains a copy of a message sent by a user and later tries to replay it. For example, a person sends a request to her bank to ask for payment to the attacker, who has done a job for her. The attacker intercepts the message and sends it again to receive another payment from the bank.


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

(b) Replay

Repudiation:

It is performed by one of the two parties in the communication: the sender or the receiver. The sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.

An example of denial by the sender would be a bank customer asking her bank to send some money to a third party but later denying that she has made such a request. An example of denial by the receiver could occur when a person buys a product from a manufacturer and pays for it electronically, but the manufacturer later denies having received the payment and asks to be paid.

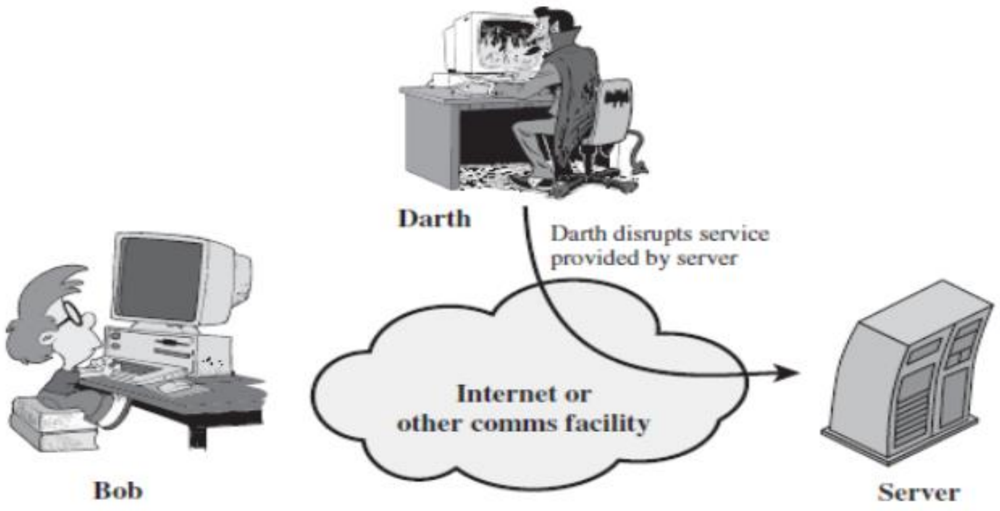
Attacks Threatening Availability:

Only one attack threatening availability:

- Denial of service

Denial of service:

- It may slow down or totally interrupt the service of a system.
- The attacker might send so many bogus requests to a server that the server crashes because of the heavy load.
- The attacker might intercept and delete a server’s response to a client, making the client to believe that the server is not responding.
- The attacker may also intercept requests from the clients, causing the clients to send requests many times and overload the system.


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

(d) Denial of service

Passive versus Active Attacks

The attacks into two groups:

- Passive Attacks
- Active Attacks

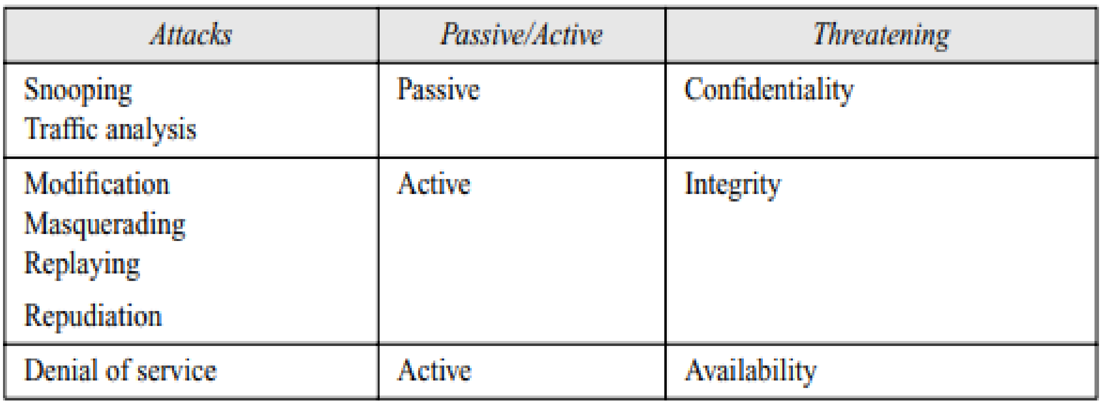
Passive Attacks:

In a **passive attack**, the attacker's goal is just to obtain information. This means that the attack does not modify data or harm the system.

Active Attacks:

An **active attack** may change the data or harm the system. Attacks that threaten the integrity and availability are active attacks.

Table 1.1 *Categorization of passive and active attacks*



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

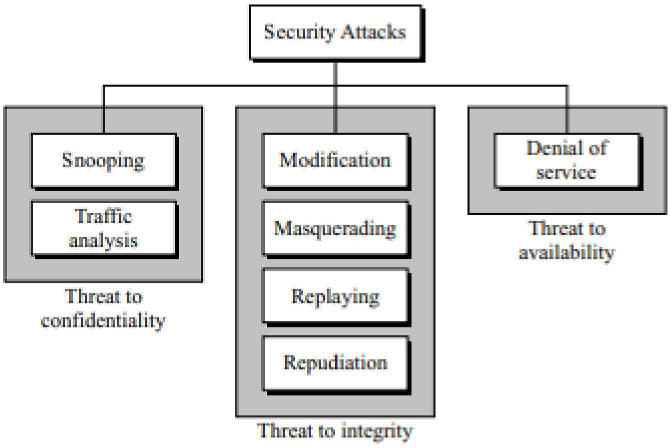
ATTACKS

An attack is a malicious attempt to access or disrupt a computer network or system to steal, change, or destroy data.

Our three goals of security confidentiality, integrity, and availability can be threatened by security attacks.

Figure 1.2 shows the attacks with relation to security goals.

Figure 1.2 *Taxonomy of attacks with relation to security goals*



Attacks Threatening Confidentiality:

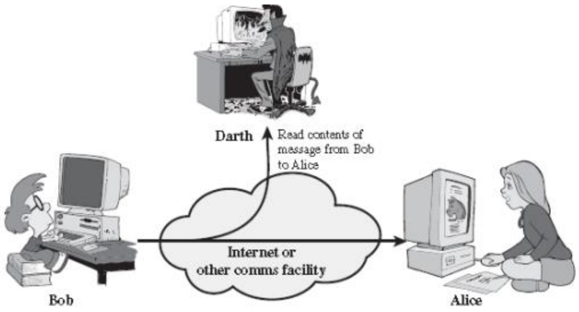
Two types of attacks threaten the confidentiality of information:

- Snooping
- Traffic analysis

Snooping:

Snooping refers to unauthorized access to or interception of data.

For example, a file transferred through the Internet may contain confidential information. An unauthorized entity may intercept the transmission and read the contents of message.


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

(a) Release of message contents

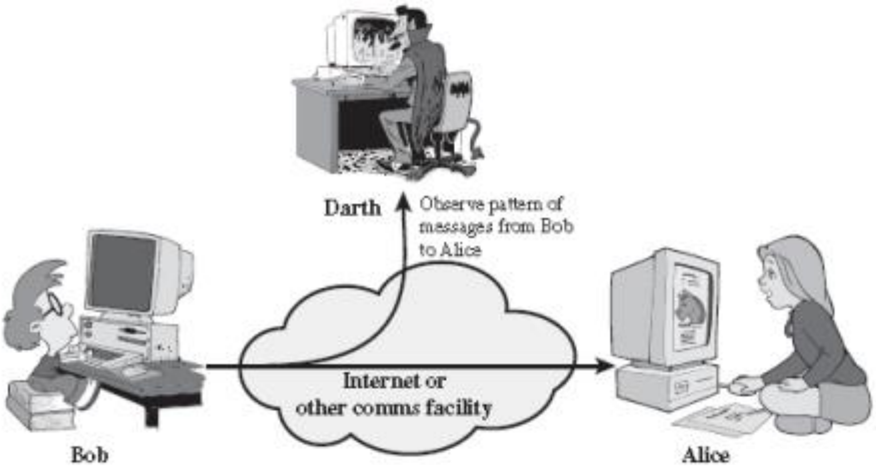
Traffic Analysis:

The attacker does not necessarily intercept or modify the content of the communication. They can obtain some other type information by monitoring online traffic.

They can find the electronic address (such as the e-mail address) of the sender or the receiver.

How Traffic Analysis Works

3. **Observation**: The attacker monitors the network to collect data on communication patterns.
4. **Analysis**: They analyze metadata (e.g., sender/receiver IP addresses, packet sizes, timestamps).


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

(b) Traffic analysis

Attacks Threatening Integrity:

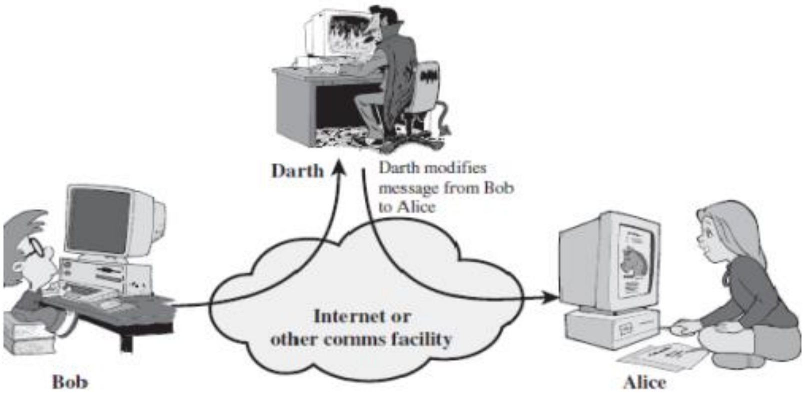
The integrity of data can be threatened by below attacks:

- Modification
- Masquerading
- Replaying
- Repudiation

Modification:

The attacker modifies the information to make it beneficial to herself.

For example, a message meaning “Allow John Smith to read confidential file accounts” is modified to mean “Allow Fred Brown to read confidential file accounts.

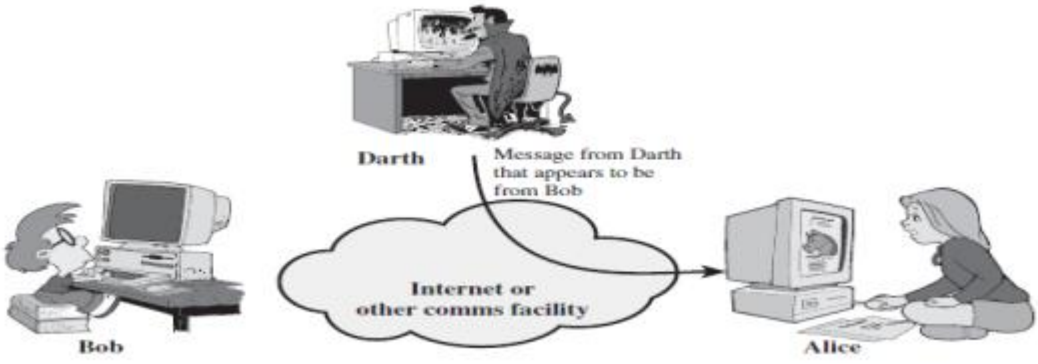

Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

(c) Modification of messages

Masquerading:

Masquerading happens when the attacker impersonates somebody else.

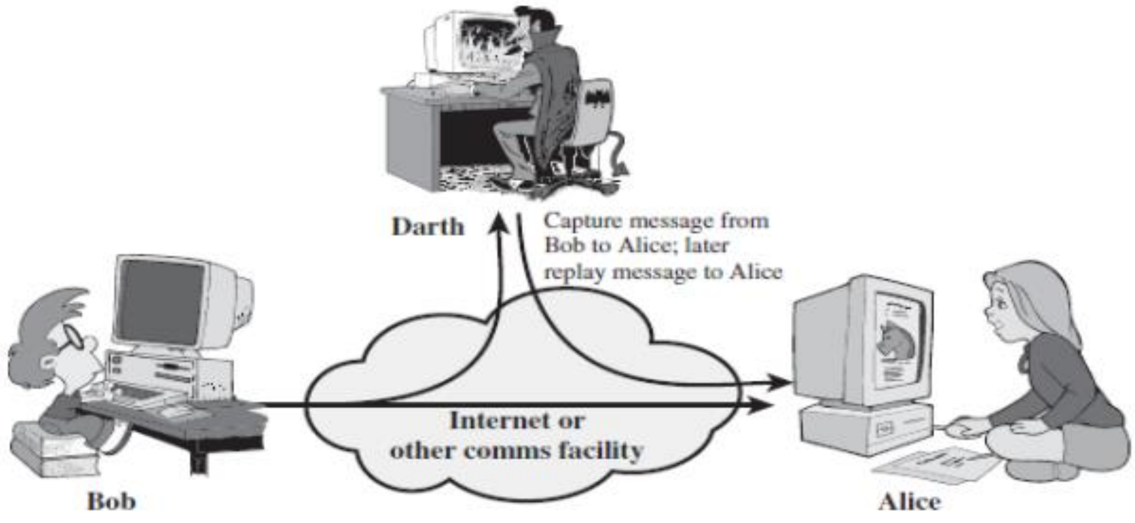
For example, an attacker might steal the bank card and PIN of a bank customer and pretend that she is that customer.


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

(a) Masquerade

Replaying:

The attacker obtains a copy of a message sent by a user and later tries to replay it. For example, a person sends a request to her bank to ask for payment to the attacker, who has done a job for her. The attacker intercepts the message and sends it again to receive another payment from the bank.


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

(b) Replay

Repudiation:

It is performed by one of the two parties in the communication: the sender or the receiver. The sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.

An example of denial by the sender would be a bank customer asking her bank to send some money to a third party but later denying that she has made such a request. An example of denial by the receiver could occur when a person buys a product from a manufacturer and pays for it electronically, but the manufacturer later denies having received the payment and asks to be paid.

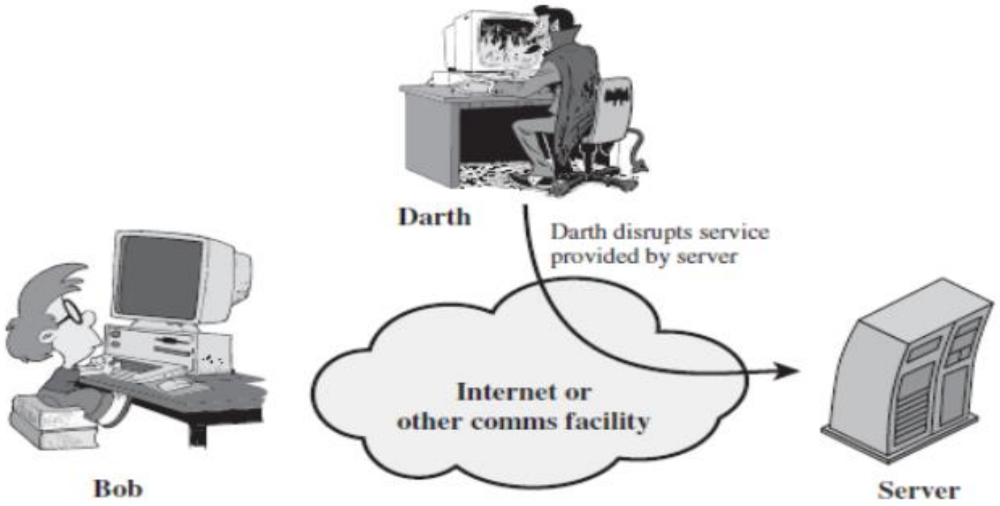
Attacks Threatening Availability:

Only one attack threatening availability:

- Denial of service

Denial of service:

- It may slow down or totally interrupt the service of a system.
- The attacker might send so many bogus requests to a server that the server crashes because of the heavy load.
- The attacker might intercept and delete a server’s response to a client, making the client to believe that the server is not responding.
- The attacker may also intercept requests from the clients, causing the clients to send requests many times and overload the system.


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

(d) Denial of service

Passive versus Active Attacks

The attacks into two groups:

- Passive Attacks
- Active Attacks

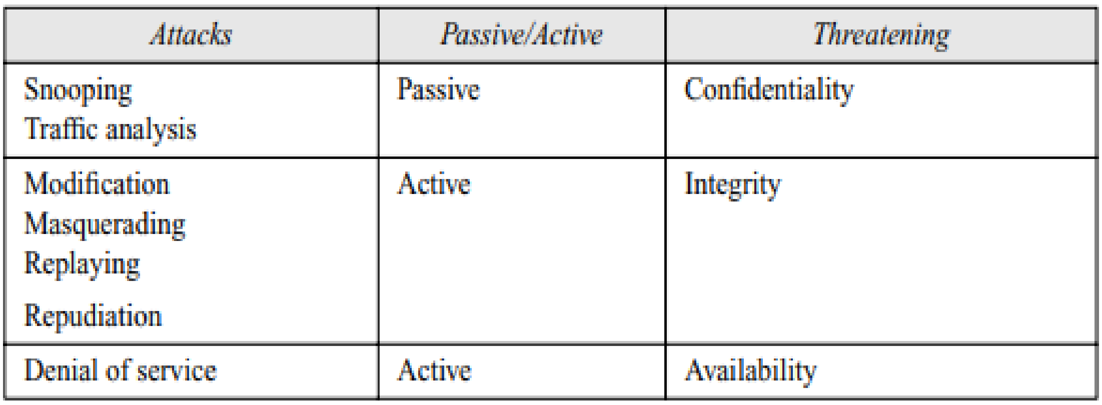
Passive Attacks:

In a **passive attack**, the attacker's goal is just to obtain information. This means that the attack does not modify data or harm the system.

Active Attacks:

An **active attack** may change the data or harm the system. Attacks that threaten the integrity and availability are active attacks.

Table 1.1 *Categorization of passive and active attacks*



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

SERVICES AND MECHANISMS

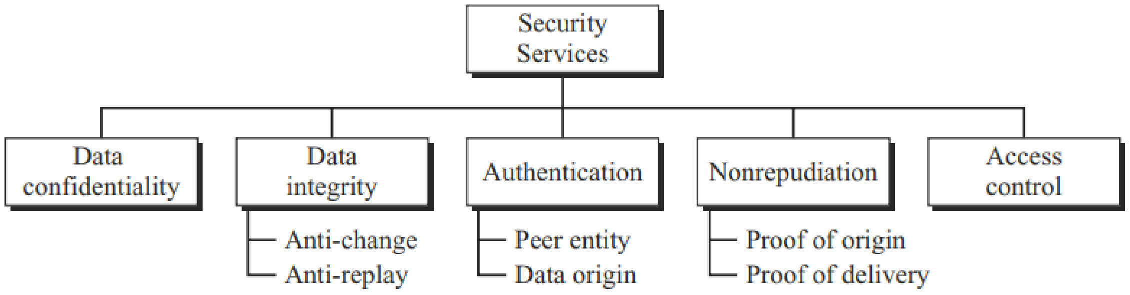
The International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) provides some security services and some mechanisms to implement those services. Security services and mechanisms are closely related because a mechanism or combinations of mechanisms are used to provide a service. A mechanism can be used in one or more services.

A **security service** is a set of measures designed to enhance the security of data and communications

Security Services:

ITU-T (X.800) has defined five services related to the security goals and attacks.

Figure 1.3 *Security services*



Data Confidentiality:

- Data confidentiality is designed to protect data from unauthorized attack.
- Data confidentiality ensures that only authorized users have access to sensitive data.
- The service as defined by X.800 is providing confidentiality of the whole message or part of a message and also protection against traffic analysis.
- It is designed to prevent snooping and traffic analysis attack.

Data Integrity:

- Data integrity is designed to protect data from modification, insertion, deletion, and replaying by an attacker. It may protect the whole message or part of the message.

Authentication:

- This service provides the authentication of sender or receiver.
- In connection-oriented communication, it provides authentication of the sender or receiver during the connection establishment (peer entity authentication).
- In connectionless communication, it authenticates the source of the data (data origin authentication).

Nonrepudiation:

- Nonrepudiation service protects against repudiation by either the sender or the receiver of the data.
- In nonrepudiation with proof of the origin, the receiver of the data can later prove the identity of the sender if denied.
- In nonrepudiation with proof of delivery, the sender of data can later prove that data were delivered to the intended recipient.

Access Control:

- Access control provides protection against unauthorized access to data.
- The term access can involve reading, writing, modifying, executing programs, and so on.

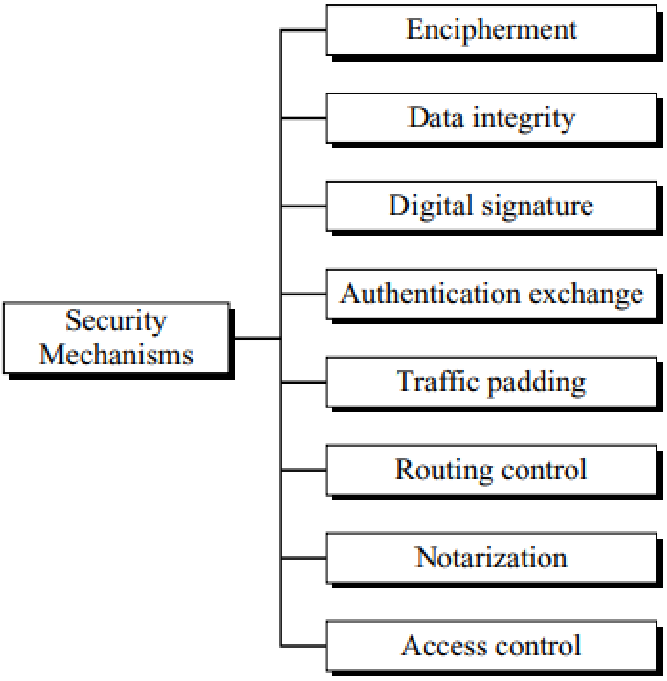
Security Mechanisms

A **mechanism** is a tool, process, or technique used to implement security services and achieve desired security goals.

A **security service** is a set of measures designed to enhance the security of data and communications

ITU-T (X.800) also recommends some security mechanisms to provide the security services

Figure 1.4 *Security mechanisms*



Encipherment:

Encipherment, hiding or covering data, can provide confidentiality.

Two techniques **cryptography and steganography** are used for enciphering.

Data Integrity:

The data integrity mechanism appends to the data a short checkvalue that has been created by a specific process from the data itself. The receiver receives the data and the checkvalue. He creates a new checkvalue from the received data and compares the newly created checkvalue with the one received. If the two checkvalues are the same, the integrity of data has been preserved.

Digital Signature:

The sender can electronically sign the data and the receiver can electronically verify the signature.

Authentication Exchange:

In authentication exchange, two entities exchange some messages to prove their identity to each other.

Traffic Padding:

Traffic padding means inserting some bogus data into the data traffic to thwart the attacker's attempt to use the traffic analysis.

Routing Control:

Routing control means selecting and continuously changing different available routes between the sender and the receiver to prevent the opponent from eavesdropping on a particular route.

Notarization:

Notarization means selecting a third trusted party to control the communication between two entities.

For example, to prevent repudiation. The receiver can involve a trusted party to store the sender request in order to prevent the sender from later denying that she has made such a request.

Access Control:

Access control uses methods to prove that a user has access right to the data or resources owned by a system. Examples of proofs are passwords and PINs.

Relation between Services and Mechanisms

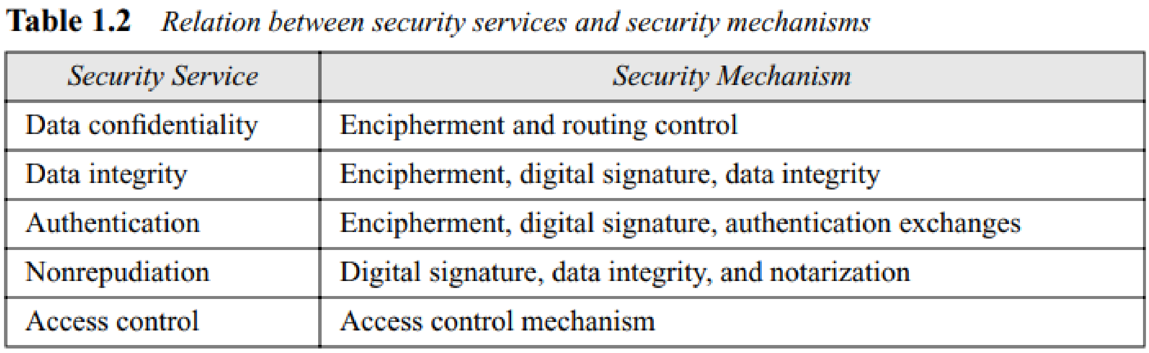


Table 1.2 *Relation between security services and security mechanisms*

Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

Steganography

Steganography is the practice of hiding secret data within a non-secret medium.

The term comes from the Greek words *steganos* (covered or concealed) and *graphia* (writing), meaning "concealed writing."

Steganography can use various **mediums** as carriers to conceal hidden information.

- Text
- Image
- Audio
- Video
- Network Protocols
- File Systems
- Software/Code
- DNA

Here we discuss only two mediums

- Text
- Image

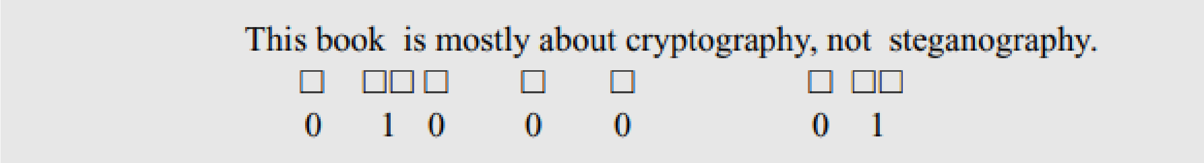
Text Cover:

“Text cover" refers to the use of textual data as a **carrier medium** for hiding information.

There are several ways to insert binary data into an innocuous text.

- **Whitespace Manipulation**:
- **Semantic Steganography**:
- **Font-Based Encoding**:
- **Grammar and Punctuation Manipulation**
- **Text Encoding Algorithms**

For example, we can use single space between words to represent the binary digit 0 and double space to represent binary digit 1. The following short message hides the 8-bit binary representation of the letter A in ASCII code (01000001).

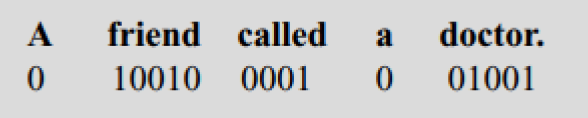


```
This book  is mostly about cryptography, not  steganography.
    □    □□ □      □      □              □  □□
    0     1 0      0      0              0   1
```

Another Example of Text Cover:

The pattern **"article-noun-verb-article-noun"** represents a basic structure in English grammar

The secret binary data can be divided into 16-bit chunks. The first bit of binary data can be represented by an article (for example, 0 for a and 1 for the). The next five bits can be represented by a noun (subject of the sentence), the next four bits can be represented by a verb, the next bit by the second article, and the last five bits by another noun (object). For example, the secret data "Hi", which is 01001000 01001001 in ASCII, could be a sentence like the following:



A	**friend**	**called**	**a**	**doctor.**
0	10010	0001	0	01001

Image Cover:

An **image cover** refers to an image file that acts as the **carrier medium** for embedding hidden data or secret messages.

Least Significant Bit (LSB) Manipulation:

Each pixel uses 24 bits (three bytes). Each byte represents one of the primary colors (red, green, or blue).

We can hide a binary data in the image by keeping or changing the least significant bit. If our binary digit is 0, we keep the bit; if it is 1, we change the bit to 1

For example, a pixel `(120, 200, 255)` in binary is:

- Red: `01111000`
- Green: `11001000`
- Blue: `11111111`

Embed the Binary Data:

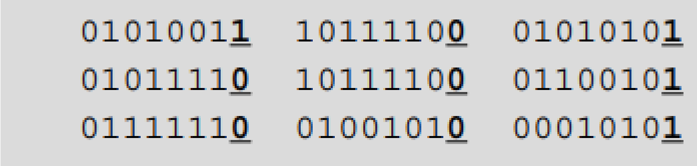
- Binary sequence: `01010011 10111100 01010101`
- First three bits (`010`) will be embedded in the first pixel:

- Original pixel: (120, 200, 255)
- Binary values:
  - Red: 01111000 → 0111100**0 (embed 0)
  - Green: 11001000 → 1100100**1 (embed 1)
  - Blue: 11111111 → 1111111**0 (embed 0)
- Modified pixel: (120, 201, 254)

For example, the following three pixels can represent the letter M.

The ASCII value of the character **M** is:

Decimal: 77
Binary: 01001101



```
01010011  10111100  01010101
01011110  10111100  01100101
01111110  01001010  00010101
```

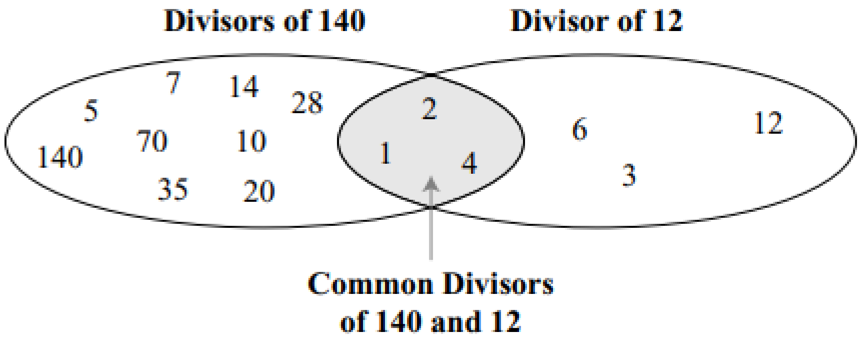
Part - 2

Greatest common divisor

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

For example, the common divisors of 12 and 140 are 1, 2, and 4. However, the greatest common divisor is 4.

Figure 2.6 *Common divisors of two integers*



Relatively prime numbers

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

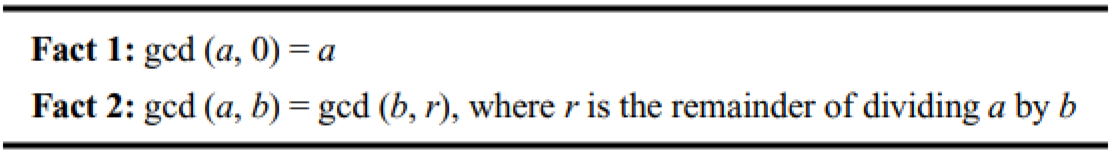
This means that if two numbers a and b are relatively prime, any other number can not evenly divide both a and b except for 1.

For example 7 and 20 are relatively prime numbers. The factors of 7 include 1 & 7 while factors of 20 include 1, 2, 4, 5 and 20.

For example 8 and 15 are relatively prime because the only divisor they share is 1.

Euclidean Algorithm

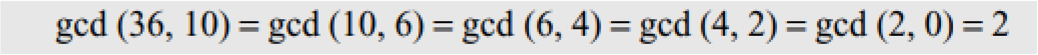
The Euclidean algorithm is based on the following two facts.



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

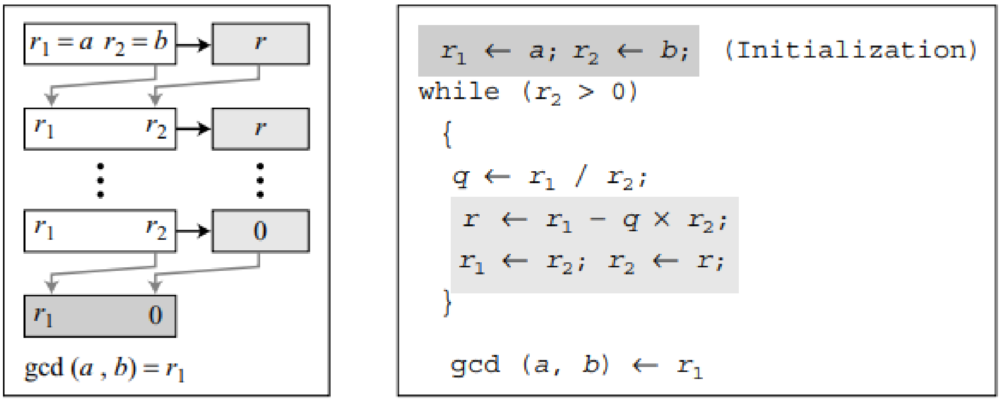
Fact 2: gcd $(a, b) =$ gcd (b, r), where r is the remainder of dividing a by b

For example, to calculate the gcd (36, 10), we can use the second fact several times and the first fact once, as shown below.



gcd (36, 10) = gcd (10, 6) = gcd (6, 4) = gcd (4, 2) = gcd (2, 0) = 2

Figure 2.7 *Euclidean algorithm*



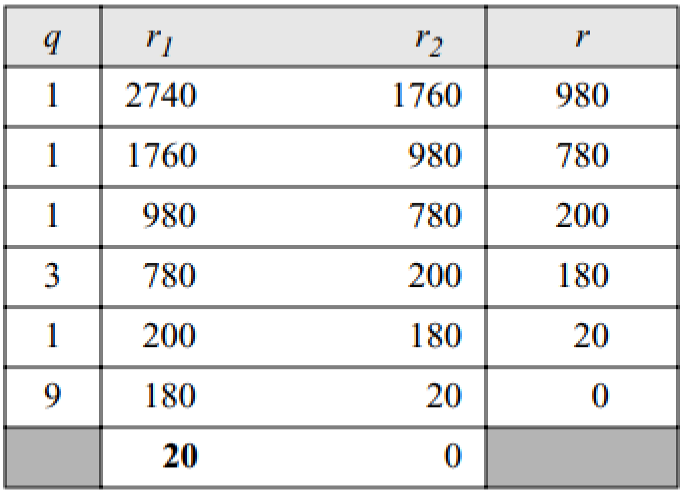
```
r₁ ← a; r₂ ← b;   (Initialization)
while (r₂ > 0)
 {
   q ← r₁ / r₂;
    r ← r₁ − q × r₂;
    r₁ ← r₂; r₂ ← r;
 }

  gcd (a, b) ← r₁
```

a. Process

b. Algorithm

Example 2.7

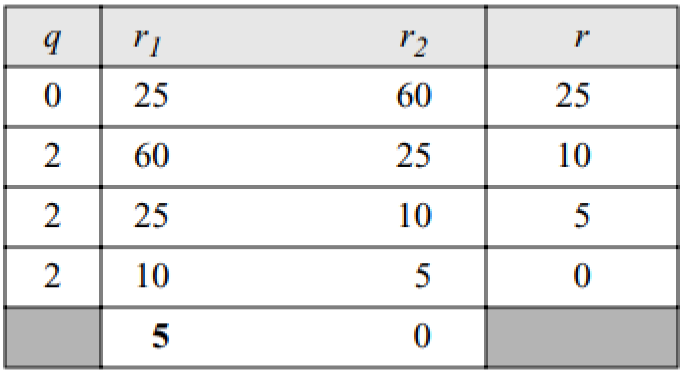
Find the greatest common divisor of 2740 and 1760.



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
	20	0	

Example 2.8

Find the greatest common divisor of 25 and 60.



q	r_1	r_2	r
0	25	60	25
2	60	25	10
2	25	10	5
2	10	5	0
	5	0	

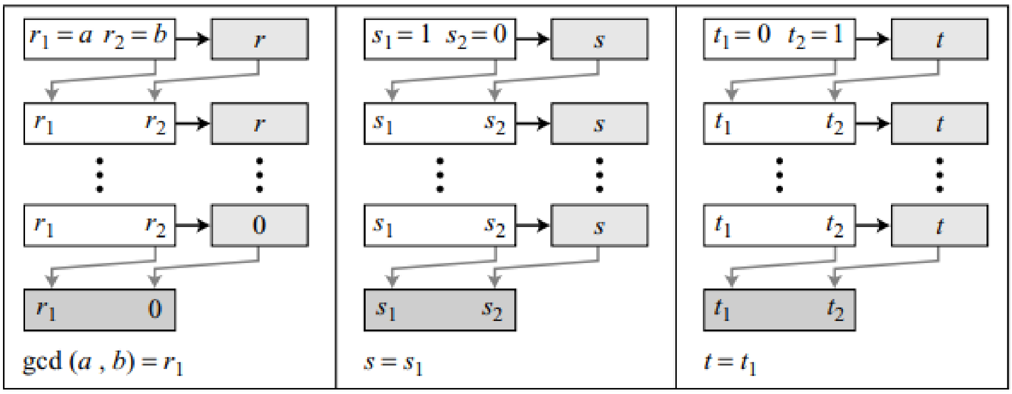
The Extended Euclidean Algorithm

Given two integers a and b, we often need to find other two integers, s and t, such that

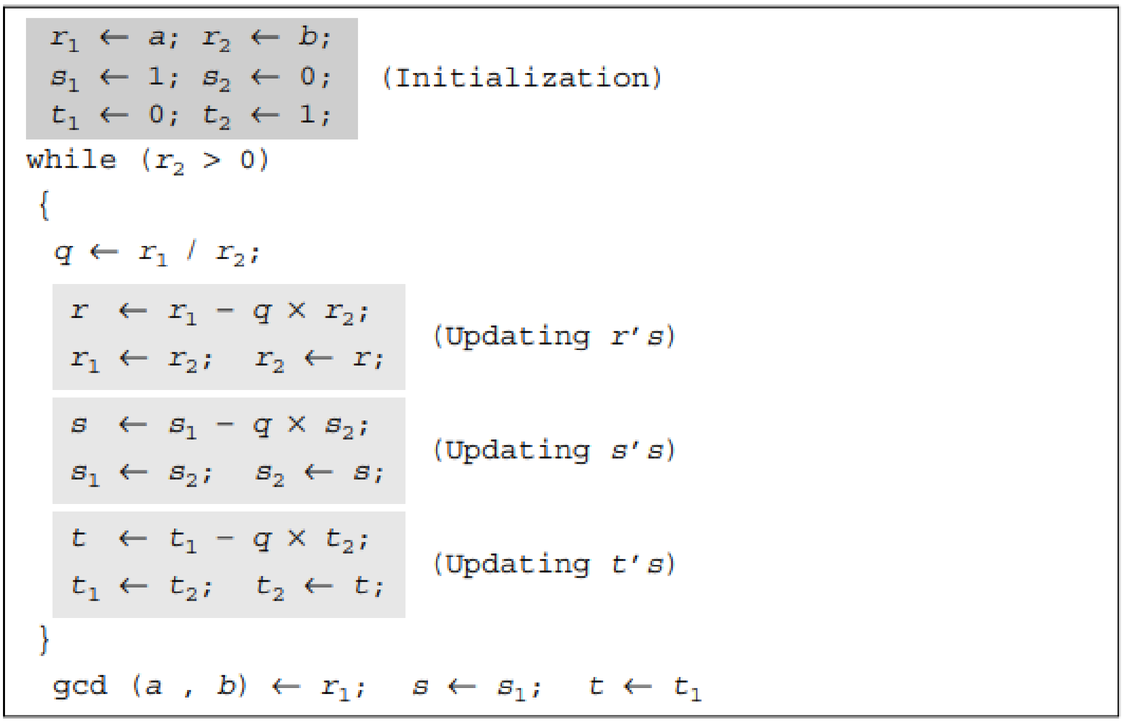
s × a + t × b = gcd (a, b)

The extended Euclidean algorithm can calculate the gcd (a, b) and at the same time calculate the value of s and t.

Figure 2.8 *Extended Euclidean algorithm*



a. Process



```
$r_1 \leftarrow a$; $r_2 \leftarrow b$;
$s_1 \leftarrow 1$; $s_2 \leftarrow 0$;      (Initialization)
$t_1 \leftarrow 0$; $t_2 \leftarrow 1$;
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)
}
  gcd ($a$ , $b$) $\leftarrow r_1$;   $s \leftarrow s_1$;   $t \leftarrow t_1$
```

b. Algorithm

Example 2.9

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

Solution

Figure 2.8 Extended Euclidean algorithm

$r = r1 - q \times r2$; $s = s1 - q \times s2$; $t = t1 - q \times t2$

We use a table to follow the algorithm.

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	

We get gcd (161, 28) = 7, $s = -1$ and $t = 6$. The answers can be tested because we have

$$(-1) \times 161 + 6 \times 28 = 7$$

Example 2.10

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

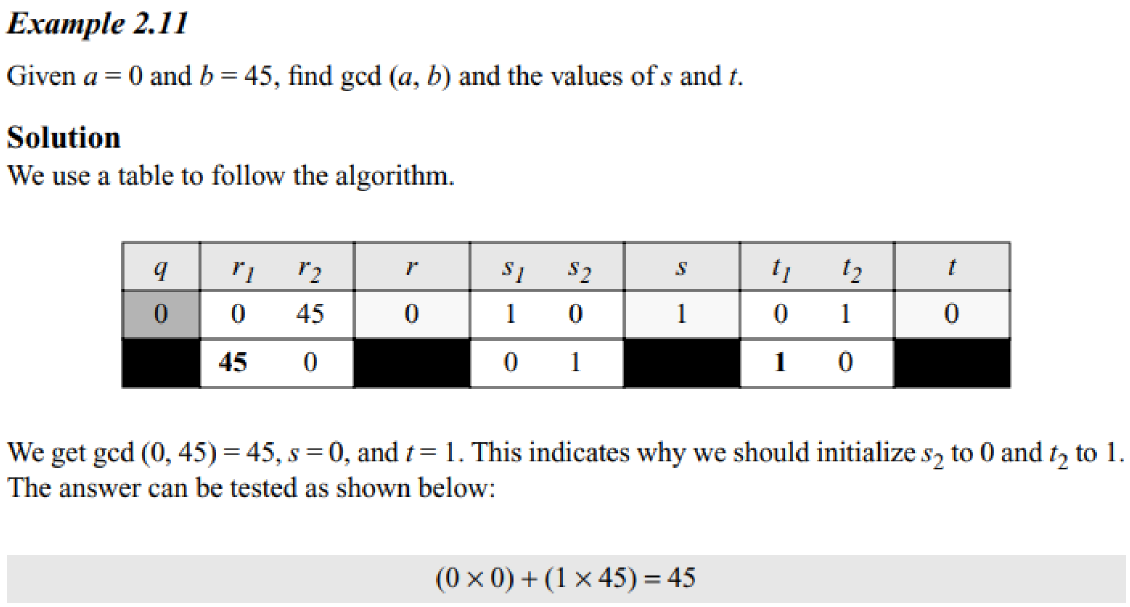
Solution

We use a table to follow the algorithm.

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
	17	0		**1**	**0**		**0**	**1**	

Note that we need no calculation for q, r, and s. The first value of r_2 meets our termination condition. We get gcd (17, 0) = 17, $s = 1$, and $t = 0$. This indicates why we should initialize s_1 to 1 and t_1 to 0. The answers can be tested as shown below:

$$(1 \times 17) + (0 \times 0) = 17$$



Example 2.11

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

Solution

We use a table to follow the algorithm.

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
	45	0		0	1		**1**	0	

We get gcd $(0, 45) = 45$, $s = 0$, and $t = 1$. This indicates why we should initialize s_2 to 0 and t_2 to 1. The answer can be tested as shown below:

$$(0 \times 0) + (1 \times 45) = 45$$

Divisibility

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

a = q × n

that n divides a (or n is a divisor of a).

We can also say that a is divisible by n. When we are not interested in the value of q, we can write the above relationship as a|n. If the remainder is not zero, then n does not divide a and we can write the relationship as a|n.

Example 2.4

a. The integer 4 divides the integer 32 because 32 = 8 × 4. We show this as 4|32.

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

Linear Diophantine Equations

- A linear Diophantine equation of two variables is ax + by = c.
- We need to find integer values for x and y that satisfy the equation.
- This type of equation has either no solution or an infinite number of solutions.
- Let d = gcd (a, b). If d does not divides c, then the equation has no solution. If d divides c, then we have an infinite number of solutions. One of them is called the particular; the rest, general.

Particular Solution:

If d divides c, a particular solution to the above equation can be found using the following steps:

1. Reduce the equation to a1x + b1y = c1 by dividing both sides of the equation by d.

2. Solve for s and t in the relation a1s + b1t = 1 using the extended Euclidean algorithm.

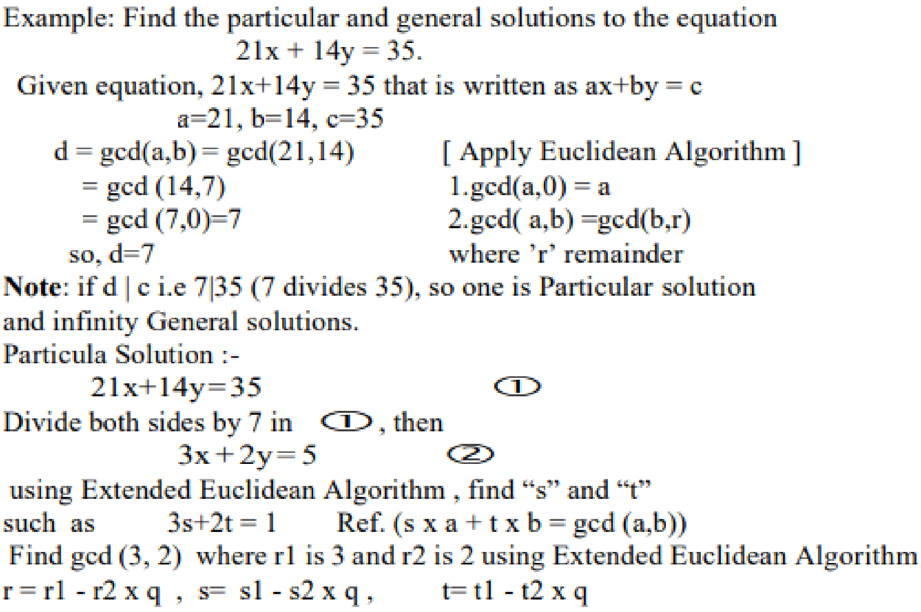
3. The particular solution can be found

Particular solution: x0 = (c/d)s and y0 = (c/d)t

General Solutions:

General solutions:

x = x0 + k (b/d) and y = y0 − k (a/d) where k is an integer



Example: Find the particular and general solutions to the equation

21x + 14y = 35.

Given equation, 21x+14y = 35 that is written as ax+by = c

a=21, b=14, c=35

d = gcd(a,b) = gcd(21,14) [Apply Euclidean Algorithm]

= gcd (14,7) 1.gcd(a,0) = a

= gcd (7,0)=7 2.gcd(a,b) =gcd(b,r)

so, d=7 where 'r' remainder

Note: if d | c i.e 7|35 (7 divides 35), so one is Particular solution and infinity General solutions.

Particula Solution :-

21x+14y=35 ①

Divide both sides by 7 in ①, then

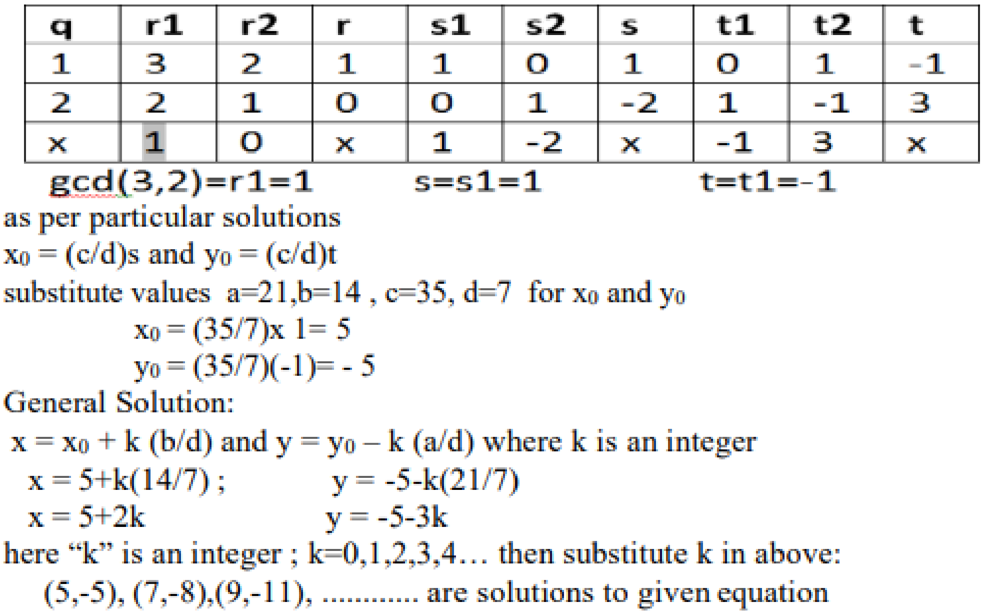
3x + 2y = 5 ②

using Extended Euclidean Algorithm , find “s” and “t”

such as 3s+2t = 1 Ref. (s x a + t x b = gcd (a,b))

Find gcd (3, 2) where r1 is 3 and r2 is 2 using Extended Euclidean Algorithm

r = r1 - r2 x q , s= s1 - s2 x q , t= t1 - t2 x q



q	r1	r2	r	s1	s2	s	t1	t2	t
1	3	2	1	1	0	1	0	1	-1
2	2	1	0	0	1	-2	1	-1	3
x	1	0	x	1	-2	x	-1	3	x

gcd(3,2)=r1=1 s=s1=1 t=t1=-1

as per particular solutions

$x_0 = (c/d)s$ and $y_0 = (c/d)t$

substitute values a=21,b=14 , c=35, d=7 for x_0 and y_0

$x_0 = (35/7)x\ 1= 5$

$y_0 = (35/7)(-1)= - 5$

General Solution:

$x = x_0 + k\ (b/d)$ and $y = y_0 – k\ (a/d)$ where k is an integer

$x = 5+k(14/7)$; $y = -5-k(21/7)$

$x = 5+2k$ $y = -5-3k$

here “k” is an integer ; k=0,1,2,3,4… then substitute k in above:

(5,-5), (7,-8),(9,-11), ... are solutions to given equation

Modulo operator (mod)

The modulo operator (mod) takes an integer (a) from the set Z and a positive modulus (n). The operator creates a nonnegative residue (r).

a mod n = r

Example:

- Dividing 27 by 5 results in r = 2. This means that 27 mod 5 = 2.
- Dividing 36 by 12 results in r = 0. This means that 36 mod 12 = 0.
- Dividing −18 by 14 results in r = −4. However, we need to add the modulus (14) to make it nonnegative. We have r = −4 + 14 = 10. This means that −18 mod 14 = 10.
- Dividing −7 by 10 results in r = −7. After adding the modulus to −7, we have r = 3. This means that −7 mod 10 = 3.

Set of Integers: Z

The set of integers, denoted by Z, contains all integral numbers (with no fraction) from negative infinity to positive infinity.

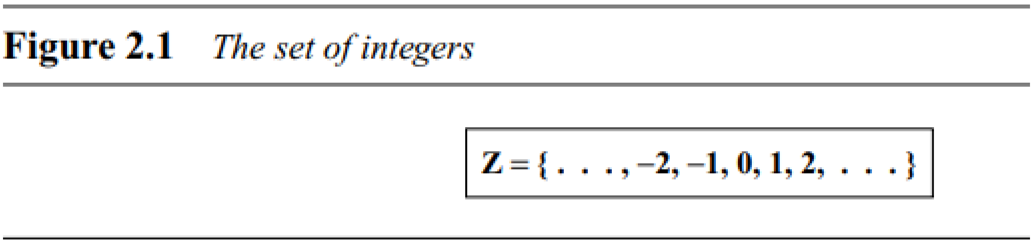


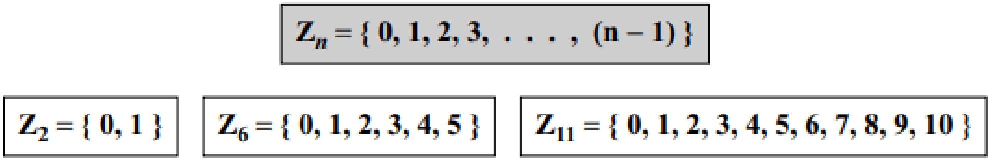
Figure 2.1 *The set of integers*

$$Z = \{ \ldots, -2, -1, 0, 1, 2, \ldots \}$$

Set of Residues: Zn

- The result of the modulo operation with modulus n is always an integer between 0 and n − 1.
- In other words, the result of a mod n is always a nonnegative integer less than n.
- we have infinite instances of the set of residues (Zn), one for each value of n. Figure 2.10 shows the set Zn and three instances, Z2, Z6, and Z11.

Figure 2.10 *Some Z_n sets*



$\mathbf{Z}_n = \{ 0, 1, 2, 3, \ldots, (n-1) \}$

$\mathbf{Z}_2 = \{ 0, 1 \}$

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

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

Congruence:

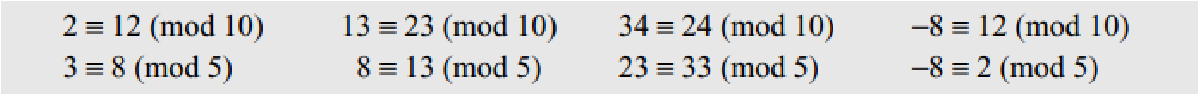
We often used the concept of congruence instead of equality.

Mapping from Z to Zn is not one-to-one.

Infinite members of Z can map to one member of Zn.

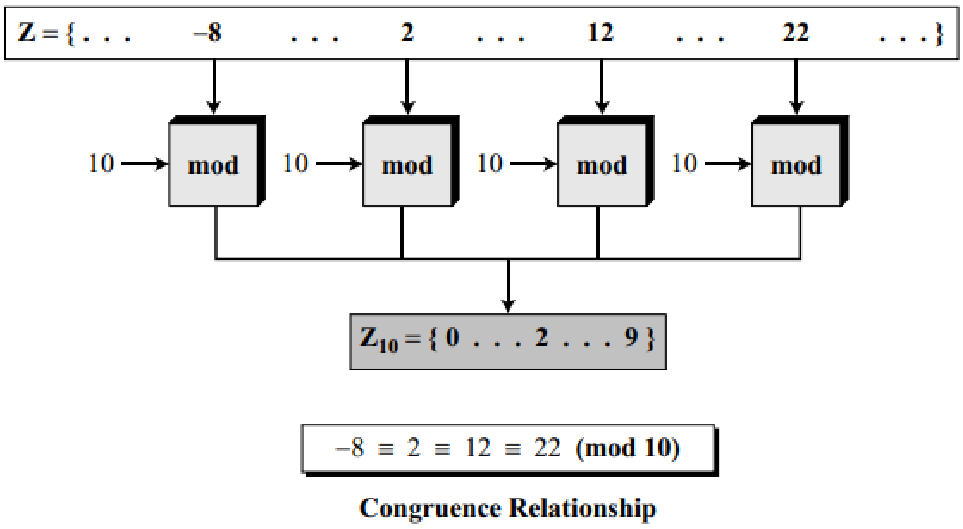
For example, the result of 2 mod 10 = 2, 12 mod 10 = 2, 22 mod 2 = 2, and so on. In modular arithmetic, integers like 2, 12, and 22 are called congruent mod 10. To show that two integers are congruent, we use the congruence operator (≡).

For example, we write:



$2 \equiv 12 \pmod{10}$	$13 \equiv 23 \pmod{10}$	$34 \equiv 24 \pmod{10}$	$-8 \equiv 12 \pmod{10}$
$3 \equiv 8 \pmod{5}$	$8 \equiv 13 \pmod{5}$	$23 \equiv 33 \pmod{5}$	$-8 \equiv 2 \pmod{5}$

Figure 2.11 *Concept of congruence*


Z = { . . . −8 . . . 2 . . . 12 . . . 22 . . . }
10
mod
10
mod
10
mod
10
mod
Z10 = { 0 . . . 2 . . . 9 }
−8 ≡ 2 ≡ 12 ≡ 22 (mod 10)
Congruence Relationship

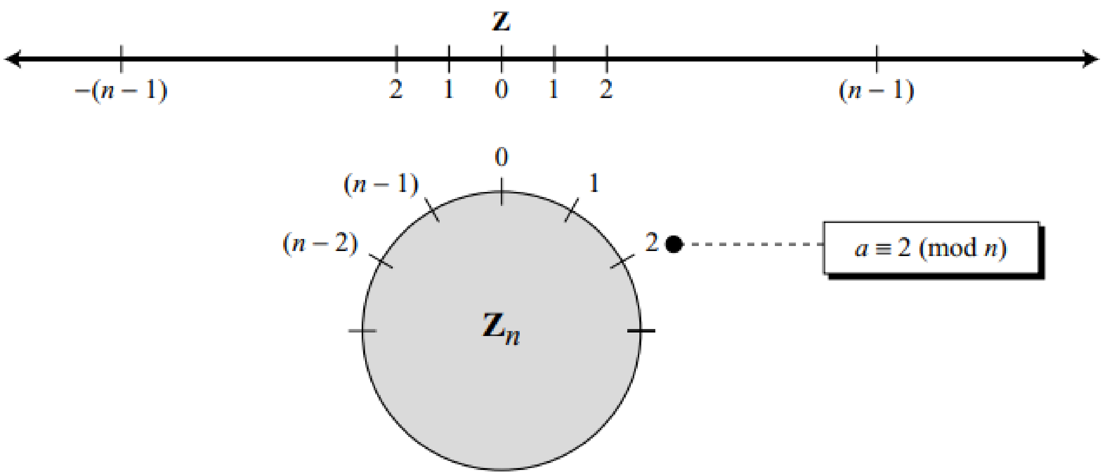
Residue Classes:

A residue class [a] or [a]n is the set of integers congruent modulo n. In other words, it is the set of all integers such that x = a (mod n). For example, if n = 5, we have five sets [0], [1], [2], [3], and [4] as shown below:

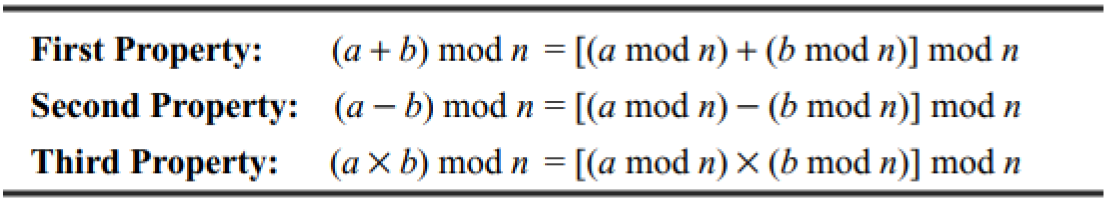
$$
\begin{aligned}
[0] &= \{\ldots, -15,\ -10,\ -5, 0,\ \ 5, 10, 15, \ldots\}\\
[1] &= \{\ldots, -14,\ \ -9,\ -4, 1,\ \ 6, 11, 16, \ldots\}\\
[2] &= \{\ldots, -13,\ \ -8,\ -3, 2,\ \ 7, 12, 17, \ldots\}\\
[3] &= \{\ldots, -12,\ \ -7,\ -5, 3,\ \ 8, 13, 18, \ldots\}\\
[4] &= \{\ldots, -11,\ \ -6,\ -1, 4,\ \ 9, 14, 19, \ldots\}
\end{aligned}
$$

Circular Notation:

Figure 2.12 *Comparison of **Z** and $\mathbf{Z}_n$ using graphs*



Properties:



First Property:	$(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$
Second Property:	$(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$
Third Property:	$(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

Inverses:

Two types of inverses:

- Additive inverse
- Multiplicative inverse

Additive Inverse:

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

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

In Zn, the additive inverse of a can be calculated as **b = n − a**.

For example, the additive inverse of 4 in Z10 is 10 − 4 = 6.

Note:

Each number has an additive inverse and the inverse is unique; each number has one and only one additive inverse.

Example:

Find all additive inverse pairs in Z10.

Solution

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

Multiplicative Inverse:

In Zn, two numbers a and b are the multiplicative inverse of each other if

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

For example, if the modulus is 10, then the multiplicative inverse of 3 is 7. In other words, we have (3 × 7) mod 10 = 1

Example:

Find all multiplicative inverses in Z10.

Solution :

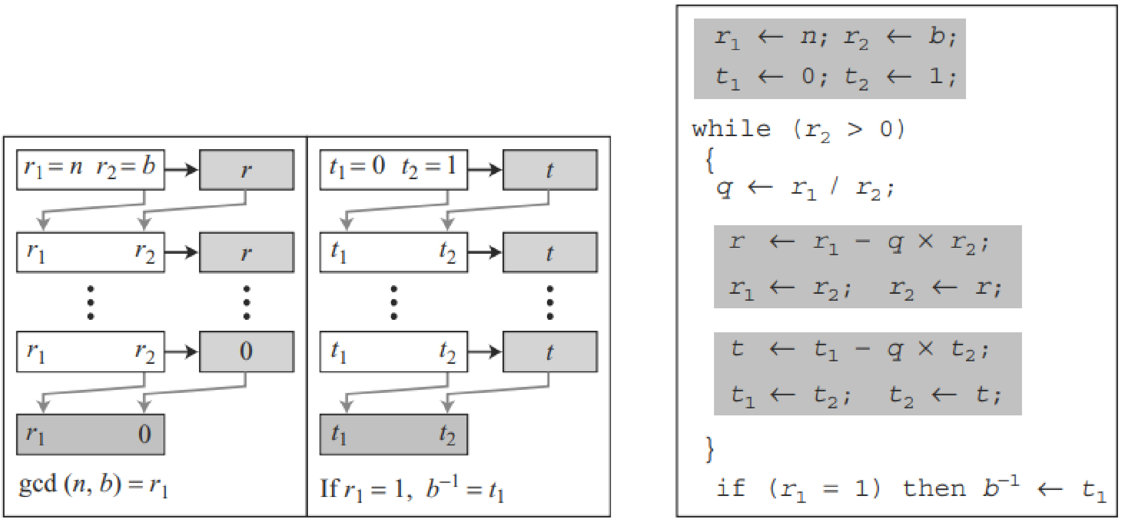
There are only three pairs: (1, 1), (3, 7) and (9, 9).

$$(1 \times 1) \bmod 10 = 1 \qquad (3 \times 7) \bmod 10 = 1 \qquad (9 \times 9) \bmod 10 = 1$$

The extended Euclidean algorithm finds the multiplicative:

The extended Euclidean algorithm finds the multiplicative **inverse**s of b in Zn when n and b are given and gcd (n, b) = 1.

Figure 2.15 *Using the extended Euclidean algorithm to find the multiplicative inverse*



```
$r_1 \leftarrow n$; $r_2 \leftarrow b$;
$t_1 \leftarrow 0$; $t_2 \leftarrow 1$;

while ($r_2 > 0$)
{
  $q \leftarrow r_1 / r_2$;

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

  $t \leftarrow t_1 - q \times t_2$;
  $t_1 \leftarrow t_2$;  $t_2 \leftarrow t$;
}
if ($r_1 = 1$) then $b^{-1} \leftarrow t_1$
```

a. Process

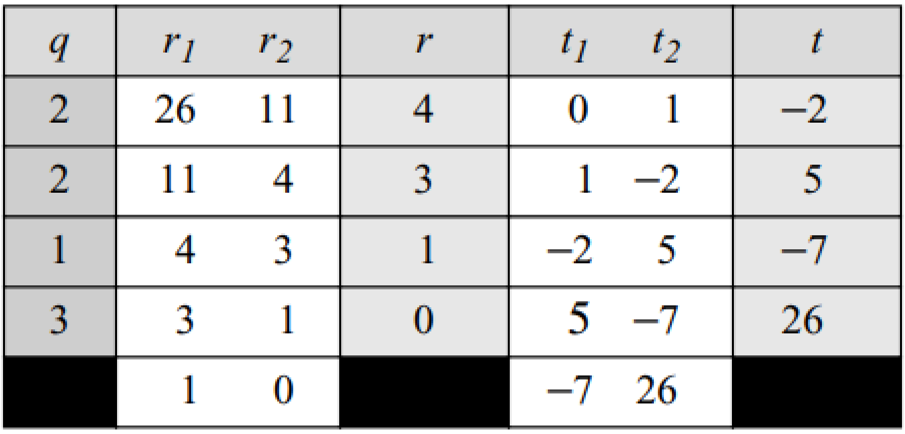
b. Algorithm

Example:

Find the multiplicative inverse of 11 in Z26?

Solution:

We use a table similar to the one we used before with r1 = 26 and r2 = 11. We are interested only in the value of t.



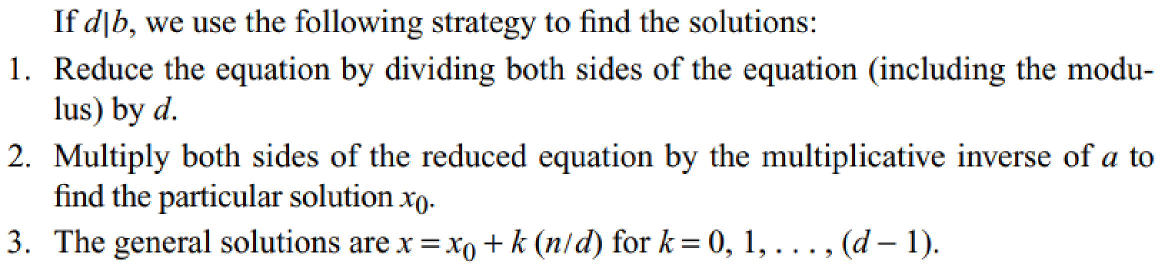
q	r_1	r_2	r	t_1	t_2	t
2	26	11	4	0	1	−2
2	11	4	3	1	−2	5
1	4	3	1	−2	5	−7
3	3	1	0	5	−7	26
	1	0		−7	26	

- The gcd (26, 11) is 1, which means that the multiplicative inverse of 11 exists.
- The extended Euclidean algorithm gives t1 = −7. The multiplicative inverse is (−7) mod 26 = 19.
- In other words, 11 and 19 are multiplicative inverse in Z26.
- We can see that (11 × 19) mod 26 = 209 mod 26 = 1.

LINEAR CONGRUENCE

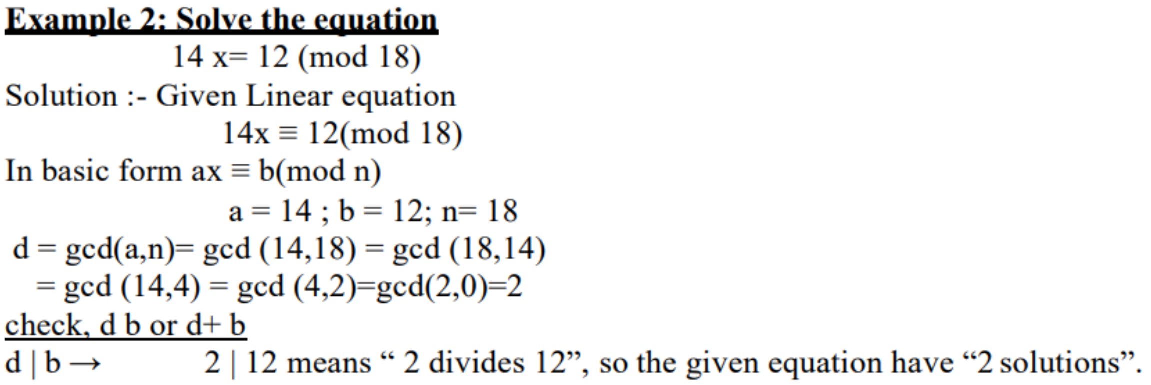
Single-Variable Linear Equations:

- The **Single-Variable Linear Equations** of the form ax ≡ b (mod n).
- An equation of this type might have no solution or a limited number of solutions.
- Assume that the gcd (a, n) = d.
- If d does not divide b, there is no solution.
- If d divides b, there are d solutions.



If $d|b$, we use the following strategy to find the solutions:

1. Reduce the equation by dividing both sides of the equation (including the modulus) by d.
2. Multiply both sides of the reduced equation by the multiplicative inverse of a to find the particular solution x_0.
3. The general solutions are $x = x_0 + k\,(n/d)$ for $k = 0, 1, \ldots, (d-1)$.



Example 2: Solve the equation

14 x= 12 (mod 18)

Solution :- Given Linear equation

14x ≡ 12(mod 18)

In basic form ax ≡ b(mod n)

a = 14 ; b = 12; n= 18

d = gcd(a,n)= gcd (14,18) = gcd (18,14)
= gcd (14,4) = gcd (4,2)=gcd(2,0)=2

check, d b or d+ b

d | b → 2 | 12 means " 2 divides 12", so the given equation have "2 solutions".

Given equation 14 x 12 (mod 18)

divides ‘d’ on both sides of equation

7x 6 (mod 9)

multiply 7^{-1} on both sides of above to get particular solution ‘x_0’.

$7^{-1} \times 7 * x_0 \equiv 6 * 7^{-1} \pmod 9$

$x_0 \equiv 6x\ 7^{-1} \pmod 9$ i.e $7^{-1} \bmod 9 \equiv 4$

$x_0 \equiv 6 \times 4 \pmod 9$

$x_0 \equiv 24 \bmod 9$

$x_0 \equiv 6$

solutions are $x = x_0 + k\ (n/d)$ where $k = 0,1$

(d = 2)

if $k = 0$ $x = x_0 + 0\ (n/\ d)$

$x = 6+ 0\ (\ 18/2) = 6$

$x = 6$

if $k = 1$ $x = x_0 +1\ ((n/\ d) = 6+1\ (\ 18/2)$

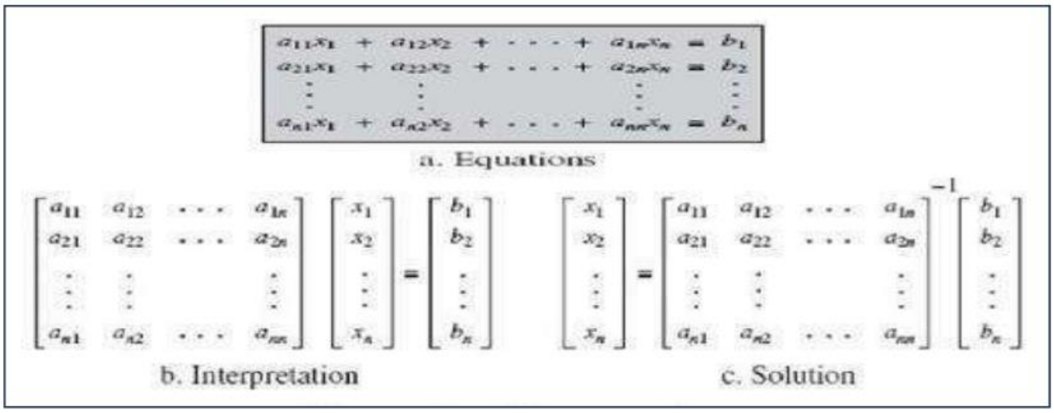
$x = 15$

‘6’ and ‘15’ are solution to 14 x 12 (mod 18)

Set of Linear Equations:

Set of Linear Equations:

Solve the set of linear equations with same modulus by forming three matrices using coefficients.
Matrix 1: square matrix made from coefficients
Matrix 2: Column matrix made from variables
Matrix 3: Column matrix made from values at right side of equations
Consider the matrix as



$$\begin{matrix} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \cdots & + & a_{2n}x_n & = & b_2 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ a_{n1}x_1 & + & a_{n2}x_2 & + & \cdots & + & a_{nn}x_n & = & b_n \end{matrix}$$

a. Equations

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

b. Interpretation

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}^{-1} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

c. Solution

Example

Solve the following sets of Linear equations?

3x + 2y ≡ 5 (mod 7)

4x + 6y ≡ 4 (mod 7)

Solution:

Matrix format of above equations is

$\begin{bmatrix}3 & 2\\4 & 6\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix} = \begin{bmatrix}5\\4\end{bmatrix}$(mod 7)

$\begin{bmatrix}x\\y\end{bmatrix}=\begin{bmatrix}3 & 2\\4 & 6\end{bmatrix}^{-1}\begin{bmatrix}5\\4\end{bmatrix}$(mod 7)

Let A=$\begin{bmatrix}3 & 2\\4 & 6\end{bmatrix}$ then A-1= $\begin{bmatrix}3 & 2\\4 & 6\end{bmatrix}^{-1}= \frac{1}{10}\begin{bmatrix}6 & -2\\-4 & 3\end{bmatrix}$

$\begin{bmatrix}x\\y\end{bmatrix}=\frac{1}{10}\begin{bmatrix}6 & -2\\-4 & 3\end{bmatrix}\begin{bmatrix}5\\4\end{bmatrix}$(mod 7) = $\frac{1}{10}\begin{bmatrix}30-8\\-20+12\end{bmatrix}$(mod 7)

= $\frac{1}{10}\begin{bmatrix}22\\-8\end{bmatrix}$(mod 7) =$\begin{bmatrix}22/10\\-8/10\end{bmatrix}$(mod 7)

x≡ 22/10 (mod 7)

y≡ -8/10 (mod 7)

Check the answer by inserting values:

3x + 2y ≡ 5 (mod 7)

3(22/10) + 2(-8/10)≡(66/10)-(16/10)≡5 (mod 7)

4x + 6y ≡ 4 (mod 7)

4(22/10) + 6(-8/10)≡(88/10)-(48/10)≡4 (mod 7)