1.) Explain the three security goals.

Security Goals

The three security goals: confidentiality, integrity, and availability

1. Confidentiality:

- It is the most common aspect of information security. We need to protect our confidential information.
- An organization needs to guard against those malicious actions that endanger the confidentiality of its information.
- In the military, concealment of sensitive information is the major concern.
- In industry, hiding some information from competitors is crucial to the operation of the organization.
- In banking, customer's accounts need to be kept secret.
- Confidentiality not only applies to the storage of the information, is also applies to the transmission of information.

2. Integrity:

- Information needs to be changed constantly. In a bank, when a customer deposits or withdraws money, the balance of her account needs to be changed.
- Integrity means that changes need to be done only by authorized entities and through authorized mechanisms.
- Integrity violation is not necessarily the result of a malicious act: an interruption in the system, such as a power surge (up and down), may also create unwanted changes in some information.

3. Availability:

- The third component of information security is availability.
- The information created and stored by an organization needs to be available to authorized entities. Information is useless, if it is not available.
- The unavailability of information is just as harmful for an organization as the lack of confidentiality or integrity.

2.) Explain about Cryptographic Attacks.

Security Attacks/ Cryptographic Attacks:

- Security attacks refer to the sets of actions that the threat actors perform to gain any unauthorised access, cause damage to systems/computers, steal data, or compromise the computer networks.
- An attacker can launch a cyber-attack from any location.
- The attacker can also be an individual or even a group.

security attacks can be of the following two types:

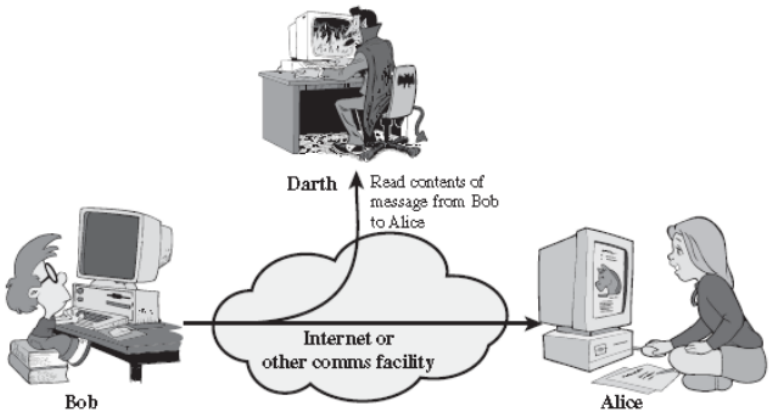
- ❖ Passive attacks
- ❖ Active attacks

Passive Attacks

- A passive attack attempts to learn or make use of information from the system but does not affect or harm system resources.
- Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions.
- The goal of the opponent is to obtain information that is being transmitted.
- Two types of passive attacks are:
    1. Release of message contents
    2. Traffic analysis

1. Release of message contents:

- The release of message contents is easily understood .
- A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information.
- We would like to prevent an opponent from learning the contents of these transmissions.
- In this type of passive attack, the information transmitted from one person to another gets into the hands of a third person/hacker.
- It jeopardises the confidentiality factor in a conversation.



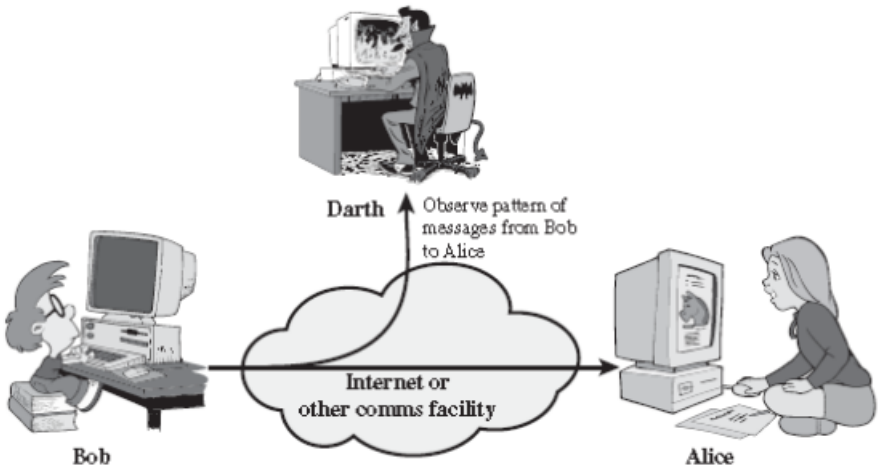
(a) Release of message contents

2. Traffic analysis:

- Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message.
- The common technique for masking contents is encryption.
- If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages.
- The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged.
- This information might be useful in guessing the nature of the communication that was taking place.

- Passive attacks are very difficult to detect, because they do not involve any alteration of the data.
- Typically, the message traffic is sent and received in an apparently normal fashion, and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern.
- However, it is feasible to prevent the success of these attacks, usually by means of encryption.
- Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.
- Active attacks can be subdivided into five categories:

    1. masquerade
    2. replay
    3. modification of messages
    4. Denial of service
    5. Repudiation



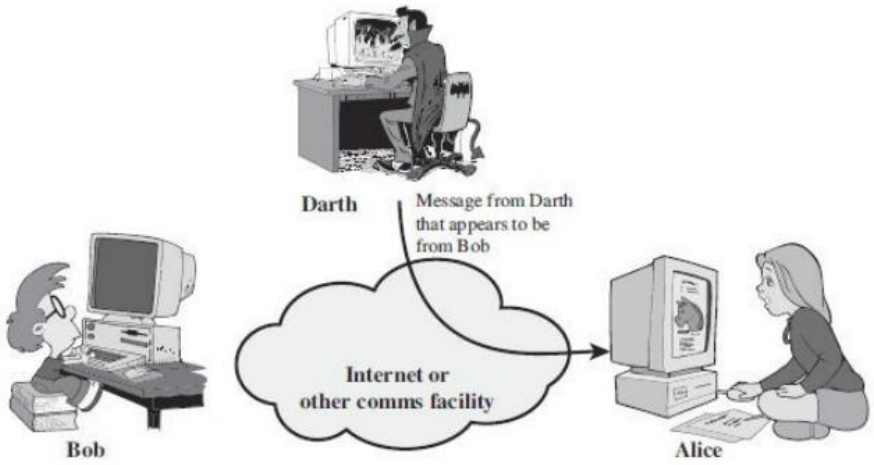
(b) Traffic analysis

Active attack:

- An active attack attempts to alter or harm system resources or affect their operation.
- Active attacks involve some modification of the data stream or the creation of a false stream.

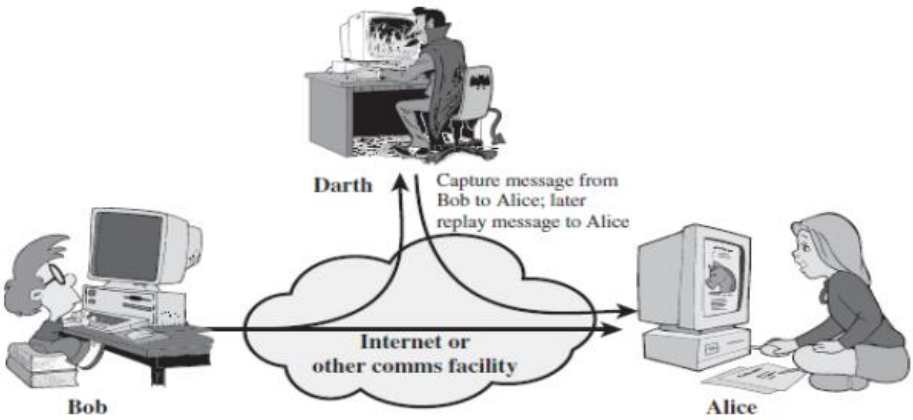
1. Masquerade:

- A masquerade takes place when one entity pretends to be a different entity.
- 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.



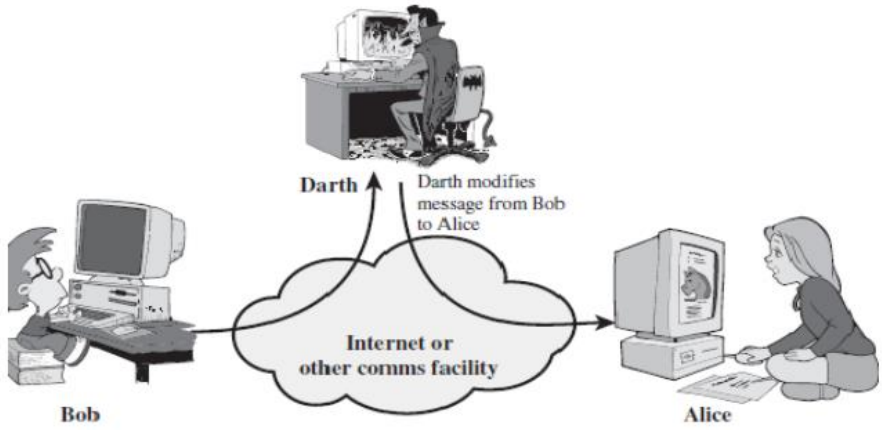
(a) Masquerade

2. **Replay:**
   - It involves the passive capture of a message and its subsequent transmission to produce an authorized effect.
   - In this attack, the basic aim of the attacker is to save a copy of the data originally present on that particular network and later on use this data for personal uses.
   - Once the data is corrupted or leaked it is insecure and unsafe for the users.
   - 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.



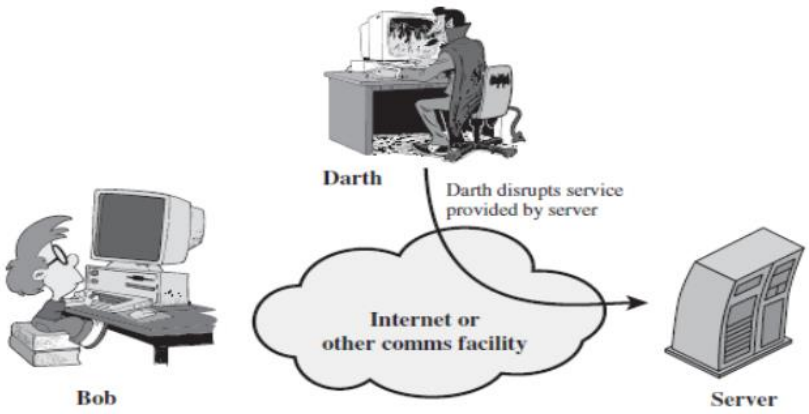
(b) Replay

3. **Modification of messages:**
   - Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect .
   - 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”.
   - Note that sometimes the attacker simply deletes or delays the message to harm the system or to benefit from it.



(c) Modification of messages

4. **Denial of service:**
   - Denial of Service (DoS) is a very common attack.
   - It may slow down or totally interrupt the service of a system.
   - The denial of service prevents or inhibits the normal use or management of communications facilities.
   - This attack may have a specific target.
   - For example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service).
   - Another form of service denial is the disruption of an entire network—either by disabling the network or by overloading it with messages so as to degrade performance.



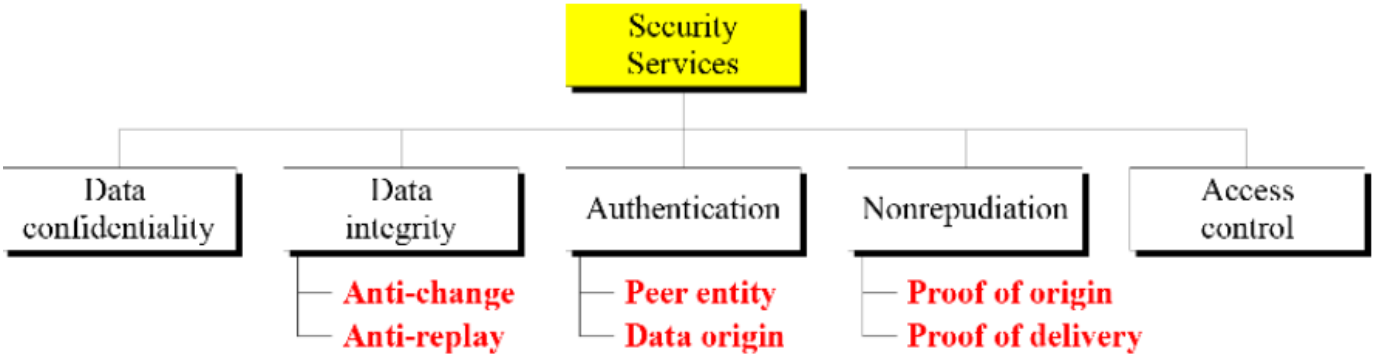
(d) Denial of service

5. **Repudiation**
   - Repudiation attacks are a type of cybersecurity attack in which an attacker attempts to deny or repudiate actions that they have taken, such as making a transaction or sending a message.
   - These attacks can be a serious problem because they can make it difficult to track down the source of the attack or determine who is responsible for a particular action.

3.) Explain about security services.

Security Services

- A service that enhances the security of data processing systems and information transfers.
- A security service makes use of one or more security mechanisms.
- ITU-T (X.800) has defined five services related to the security goals and attacks we defined in the previous sections.
- Figure shows the taxonomy of those five common services.



- It is easy to relate one or more of these services to one or more of the security goals.
- It is also easy to see that these services have been designed to prevent the security attacks that we have mentioned.

1. Data Confidentiality:

- Data confidentiality is designed for information is not made available to unauthorized individual.
- Confidentiality is the protection of transmitted data from passive attacks
- It is designed to prevent snooping and traffic analysis attacks.
- For example, when a TCP connection is set up between two systems, this broad protection prevents the release of any user data transmitted over the TCP connection.

2. Data Integrity:

- Ensures that only authorized parties are able to modify computer system assets and transmitted information.
- It is designed to protect data from modification, changing status, insertion, deletion, and replaying by an adversary.
- It may protect the whole message or part of the message.

3. Authentication:

- The authentication service is concerned with assuring that a communication is Authentic.
- The assurance that the communicating entity is the one that it claims to be.
- Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.
- This service provides the authentication of the party at the other end of the line.
- In connection oriented communication, it provides authentication of the sender and receiver during the connection establishment.
- In connection-less communication, it authenticates the source of the data (data origin authentication).

4. Nonrepudiation:

- Requires that neither the sender nor the receiver of a message be able to deny the transmission.
- when a message is sent, the receiver can prove that the alleged sender in fact sent the message.

- Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.
- Nonrepudiation service protects against repudiation (refuse to accept) by either the sender or the receiver of the data.
    - **Nonrepudiation, Origin**
      Proof that the message was sent by the specified party.
    - **Nonrepudiation, Destination**
      Proof that the message was received by the specified party.

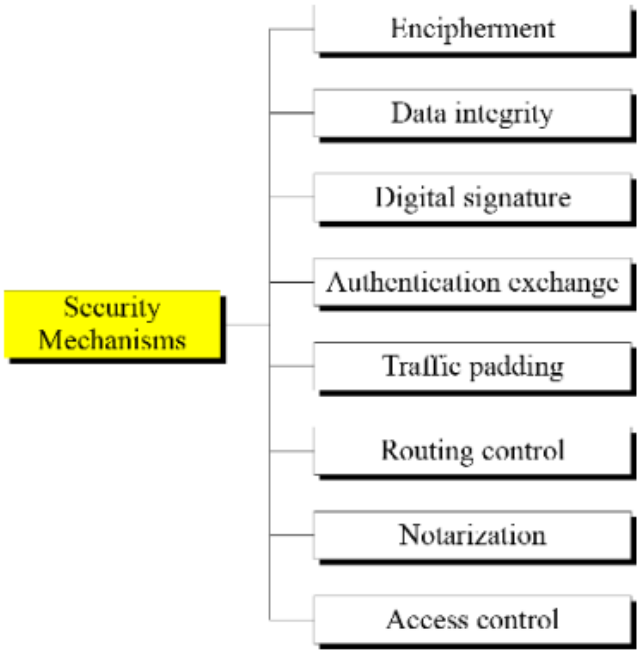
5. Access Control:

- Requires that access to information resources may be controlled by the target system .
- Access control is the ability to limit and control the access to host systems and applications via communications links.
- It provides protection against unauthorized access to data.
- To achieve this, each entity trying to gain access must first be identified, or authenticated
- The term access in this definition is very broad and can involve reading, writing, modifying, executing programs, and so on.

4.) Explain about security mechanisms.

Security Mechanisms

- A security mechanism is any process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
- ITU-T (X.800) also recommends some security mechanisms to provide the security services defined in the previous section.
- Figure gives the taxonomy of these mechanisms.



1. Encipherment:

- Encipherment, hiding or covering data, can provide confidentiality.
- Today two techniques cryptography and steganography are used or enciphering.

2. 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 checks value.
- He creates a new checkvalue from the received data and compares the newly created checkvalue with the one received.
- If two check values are same, the integrity of data has been preserved.

3. Digital signature:

- A digital signature is a means by which the sender can electronically sign the data and receiver can electronically verify the signature.
- The sender uses a process that involves showing that she owns a private key related to the public key that she has announced publicly.
- The receiver uses the sender's public key to prove that the message is indeed signed by the sender who claims to have sent the message.

4. Authentication exchange:

- In this two entities exchange some messages to prove their identity to each other.
- For example, one entity can prove that she knows a secret that only she is supposed to know

5. Traffic Padding:

- This means inserting some bogus data into the data traffic to the adversary's attempt to use the traffic analysis.

6. Routing control:

- It means selecting and continuously changing different available routes between sender and receiver to prevent the opponent from eavesdropping (secretly listen to a conversation) on a particular route.

7. Notarization:

- It means selecting a third trusted party to control the communication between two entities.
- This can be done, for example, to prevent repudiation.

8. Access control:

- It 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.

5.) Write and explain about Euclidean algorithm.

Euclidean Algorithm:

Euclidean algorithm is used to finding the greatest common divisor (gcd) of two positive integers.

GCD of two numbers is the largest number that divides both of them.

When we divide an integer from a non-zero integer, there exists integers q and r such that:

$a=b\ q + r$

where 0<=*r*<=*b* , *q* is known as the *quotient* and *r* is the *remainder*.

The Euclidean Algorithm repeatedly applies the division algorithm to find the GCD of integers *a* and *b*. We repeatedly divide the divisor by the remainder until the remainder is zero. The *last* non-zero remainder is the greatest common divisor.

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

The first fact tells us that if the second integer is 0, the greatest common divisor is the first one.

The second fact allows us to change the value of a, b until b becomes 0.

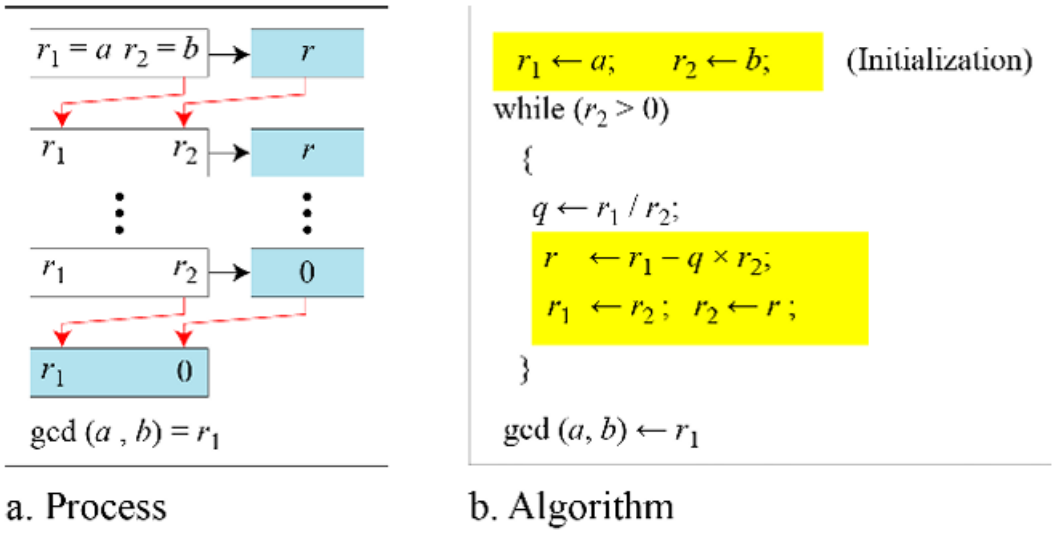


Figure 2.4 Euclidean Algorithm

We use two variables r1 and r2, to hold the changing values during the process of reduction. They are initialized to a and b.

• In each step, we calculate the remainder of r1 divided by r2 and store the result in the variable r. we then replace r1 by r2 and r2 by r.

• The steps are continued until r2 becomes 0. At this moment, we stop. The gcd (a, b) is r1.

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

Example: Find the greatest common divisor of 2740, 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
	20	0	

Example: 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
	5	0	

6.) Explain the extended Euclidean algorithm. Find GCD(a, b) and the values of s and t for given a=161 and b=28.

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

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

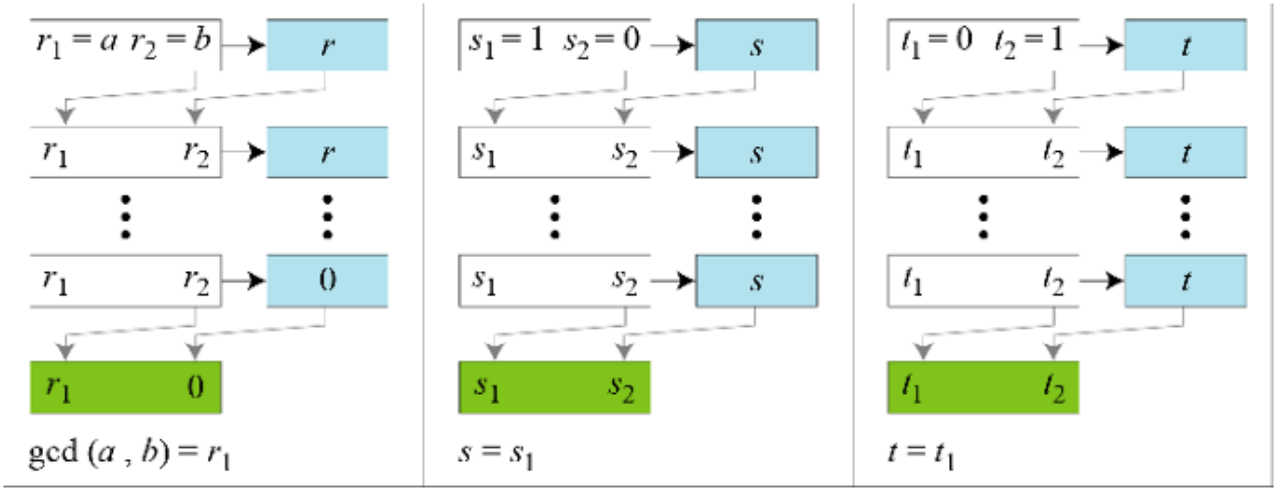
The Extended Euclidean algorithm can calculate the gcd (a, b) and at the same time calculate the value of s and t.

Initially,

$s_1 = 1$, $s_2 = 0$ to compute **s**, use: $s = s_1 - qs_2$

$t_1 = 0$, $t_2 = 1$ to compute **t**, use: $t = t_1 - qt_2$

The algorithm and the process is shown below diagram.



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

Figure 2.5 Extended Euclidian Algorithm

Extended Euclidean algorithm:

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

ex: $\gcd(161, 28)$

q	a	b	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	

$s = s_1 - q s_2$

$t = t_1 - q t_2$

$s = 1 - 5(0) = 1$ $\quad 1 - (-1)(3)$

$0 - 5(1) = -5$ $\quad 1 - (-5)(1)$

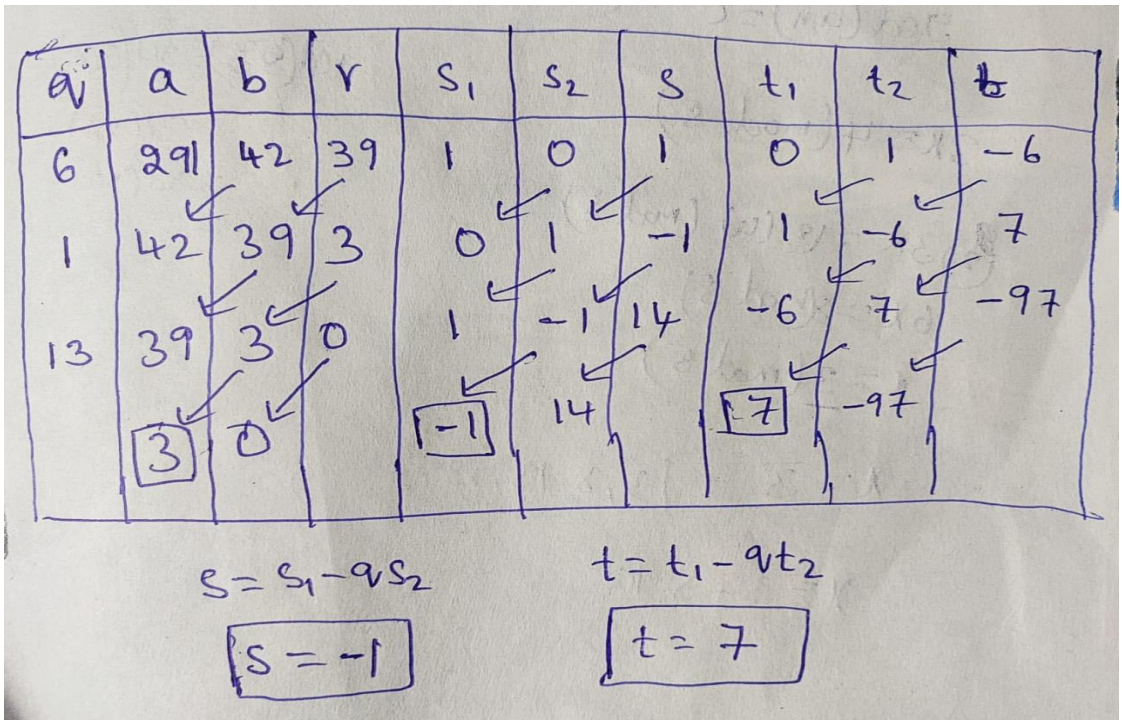
$-5 - (6)(3)$

$\therefore s = -1$ $\quad t = 6$

$$s*a + t*b = (-1)(161) + (6)(28)$$
$$= -161 + 168$$
$$= 7$$

7.) State and prove the properties of modular arithmetic binary operations.

8.) Using the extended Euclidean algorithm, find GCD(291, 42) and the values of s and t.



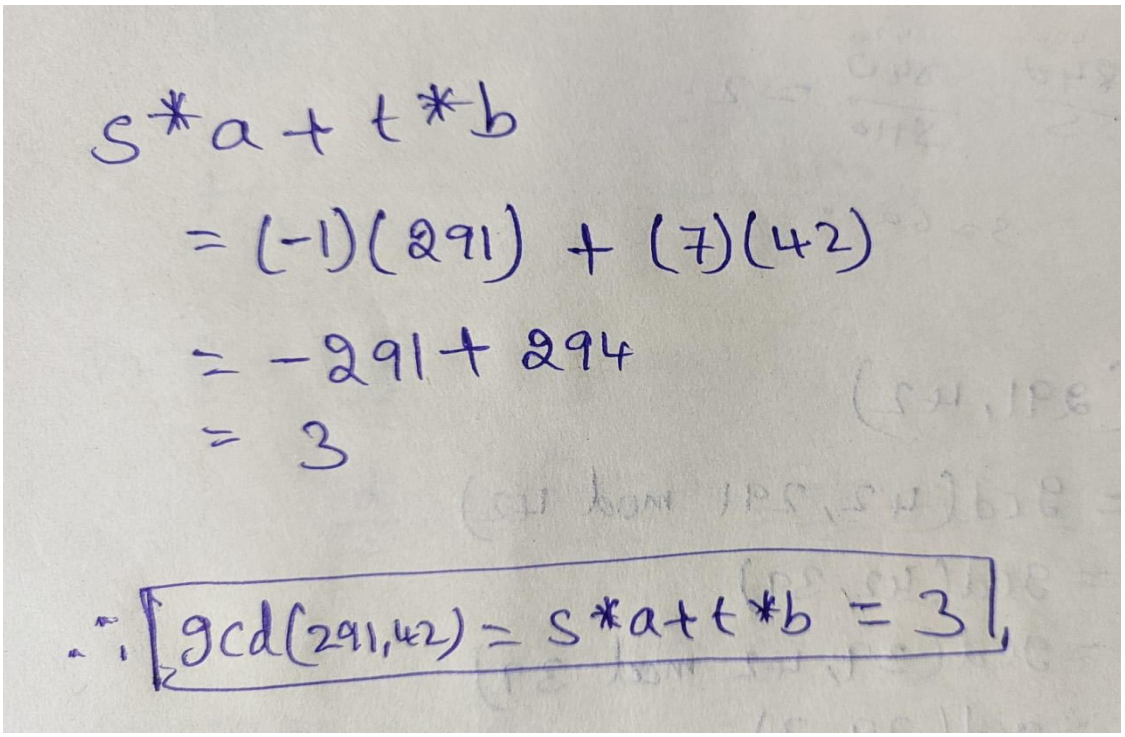
q	a	b	r	s_1	s_2	s	t_1	t_2	t
6	291	42	39	1	0	1	0	1	-6
1	42	39	3	0	1	-1	1	-6	7
13	39	3	0	1	-1	14	-6	7	-97
	3	0		-1	14		7	-97	

$s = s_1 - qs_2$

$\boxed{s = -1}$

$t = t_1 - qt_2$

$\boxed{t = 7}$



$$s*a + t*b$$

$$= (-1)(291) + (7)(42)$$

$$= -291 + 294$$

$$= 3$$

$$\therefore \boxed{gcd(291,42) = s*a + t*b = 3}$$

9.) Distinguish between passive and active security attacks. Name some passive attacks. Name some active attacks.

Active Attack	Passive Attack
In an active attack, Modification in information takes place.	While in a passive attack, Modification in the information does not take place.
Active Attack is a danger to Integrity as well as availability.	Passive Attack is a danger to **Confidentiality**.
In an active attack, attention is on prevention.	While in passive attack attention is on detection.
Due to active attacks, the execution system is always damaged.	While due to passive attack, there is no harm to the system.
In an active attack, Victim gets informed about the attack.	While in a passive attack, Victim does not get informed about the attack.
In an active attack, System resources can be changed.	While in passive attack, System resources are not changing.
Active attack influences the services of the system.	While in a passive attack, information and messages in the system or network are acquired.
In an active attack, information collected through passive attacks is used during execution.	While passive attacks are performed by collecting information such as passwords, and messages by themselves.
An active attack is tough to restrict from entering systems or networks.	Passive Attack is easy to prohibit in comparison to active attack.
Can be easily detected.	Very difficult to detect.
The purpose of an active attack is to harm the ecosystem.	The purpose of a passive attack is to learn about the ecosystem.
In an active attack, the original information is modified.	In passive attack original information is Unaffected.
The duration of an active attack is short.	The duration of a passive attack is long.
The prevention possibility of active attack is High	The prevention possibility of passive attack is low.
Complexity is High	Complexity is low.

- Two types of **passive attacks** are:
    1. Release of message contents
    2. Traffic analysis

- **Active attacks** can be subdivided into five categories:

    1. masquerade
    2. replay
    3. modification of messages
    4. Denial of service
    5. Repudiation

10.) Find the particular and the general solutions to the following linear Diophantine equation: 25x+10y=15

$25x + 10y = 15$

$ax + by = c$

Here, $a = 25$ $b = 10$ $c = 15$

Step-1:

$d = \gcd(a, b)$

$= \gcd(25, 10)$

$= \gcd(10, 5)$

$= \gcd(5, 0)$

$= 5$

Step-2:

Divide the both sides of eqn with value of d

$\Rightarrow \frac{25x + 10y}{5} = \frac{15}{5}$

$5x + 2y = 3$

Step-3:

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
2	5	2	1	1	0	1	0	1	-2
2	2	1	0	0	1	-2	1	-2	5
	1	0		1	-2		-2	5	

$s = s_1 - q s_2$ $t = t_1 - q t_2$

$s = 1$ $t = -2$

Step-4:

Particular solution

$x_0 = (c/d)\, s$

$= (15/5) \cdot (1)$

$= 3$

$y_0 = (c/d)\, t$

$= (15/5) \cdot (-2)$

$= 3(-2)$

$= -6$

Step-5:

General solution

$x = x_0 + k(b/d)$

$= 3 + k(10/5)$

$= 3 + 2k$

$y = y_0 - k(a/d)$

$= -6 - k(25/5)$

$= -6 - 5k$

Here 'k' is an integer ; $k = 0, 1, 2, 3, \ldots$

11.) Define the following terms Modulo operator, Congruence.

Modulo Operator:

• The division relationship (a=q × n + r) has two inputs (a and n) and two outputs (q and r).

• In modular arithmetic, we are interested in only one of the outputs, the remainder r. We don't care about the quotient q.

• In other words, we want to know what is the value of r when we divide a by n.

• This implies that we can change the above relation into a binary operator with two inputs a and n and one output r.

• The above mentioned binary operator is called the **modulo** operator and is shown as **mod**.

• The second input (n) is called the **modulus**. The output r is called the **residue**.

• The below figure shows, the modulo operator (mod) takes an integer (a) from the set z and a positive modulus (n) .The operator creates a nonnegative residue (r).

We can say , **a mod n = r**

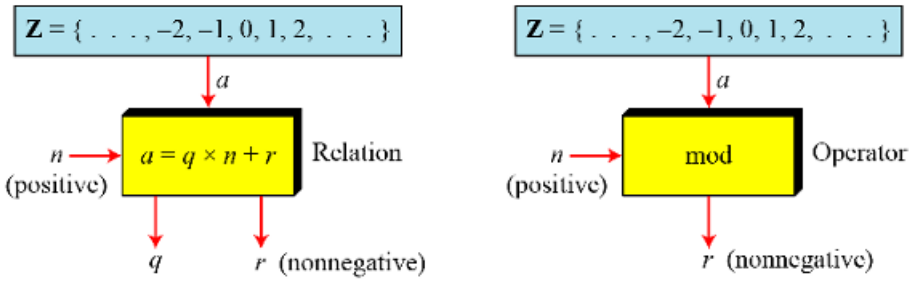


Figure 2.6 Division relation and modulo operator

Set of Residues(Zn):

• The result of 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 can say that modulo operation creates a set, which in modular arithmetic is referred to as the set of least residues modulo n, or Zn.

• We have infinite instances of the set of residues (Zn), one for each value of n.

• The below figure shows the set Zn and three instances, Z2, Z6, and Z11.

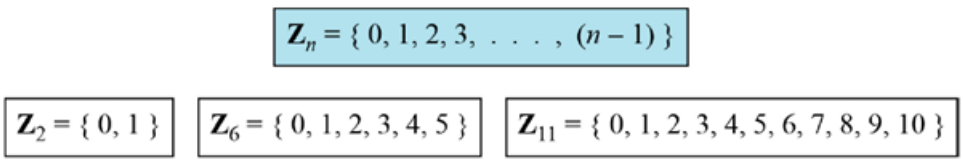


Figure 2.7 Some Z_n sets

Congruence

• In Cryptography, we often used the concept of congruence instead of equality.

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

• For example, the result of 2 mod 10 = 2, 12 mod 10 = 2, 22 mod 10 = 2, and so on.

• In Modular arithmetic, integers like 2, 12, and 22 are called congruent mod 10.

• To show that two integers congruent, we use the congruence operator (≡).

• We add the phrase (mod n) to the right side of the congruence to define the value of modulus that makes the relationship valid.

For example ,we write:

$$2 \bmod 10 = 12 \bmod 10 \rightarrow 2 \equiv 12 \bmod 12$$

We need to explain several points.

• The congruence operator looks like the equality operator, but there are differences. First, an equality operator maps a member of Z to itself; the congruence operator maps a member from Z to member of Zn. Second, the equality operator is one-to-one; the congruence operator is many-to-one.

• The phrase (mod n) that we insert at the right-hand-side of the congruence operator is just an indication of the destination set (Zn).

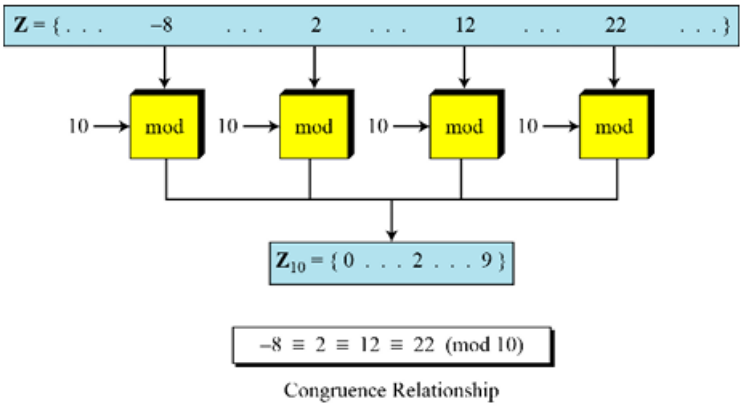


Figure 2.8 Concept of congruence

12.) Find all solutions to linear equation: 3x ≅ 4 (mod 5)

In linear congruence, only positive whole numbers of x are accepted.

Therefore, from the above equation (3x = 4), dividing both sides by 3 cannot be accepted (because it will result to a decimal number, 0.75).

Thus, since 5x - 2x = 3x, we replace 3x with 5x - 2x.

That is, 5x - 2x = 4 (mod5).

Also, in mod5, 5x = 0.

Hence, -2x = 4 (mod5)

Divide both sides by -2

x = 4/-2 (mod5)

x = -2 (mod5)

Since negative are not accepted, we add 5 to -2

$x = -2 + 5$

$x = 3$