R. C. Patel Institute of Technology, Shirpur

Department of Computer Engineering

Presentation
on
Sub: Information Security (IS) (22PCCO6030T)
by

Mr. Vishal S. Thakare

B.E. (Computer Engg.)

M.E. (Computer Engg.)

Unit I –Introduction and Number Theory

8 Hrs.

Security

- Security means safety as well as measures taken to be safe or protected.
- Security is about protection of assets.
- Assets generally include hardware (e.g. servers and switches), software (e.g. mission critical applications and support systems) and confidential information.

Computer Security

- Computer Security is the process of detecting and preventing any unauthorized actions of users of computer system.
- Prevention measures help user to stop unauthorized users from accessing any part of computer system.
- Detection help user to determine whether or not someone attempted to break in to any system.

Computer Security

"the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources" (includes hardware, software, firmware, information/ data, and telecommunications)

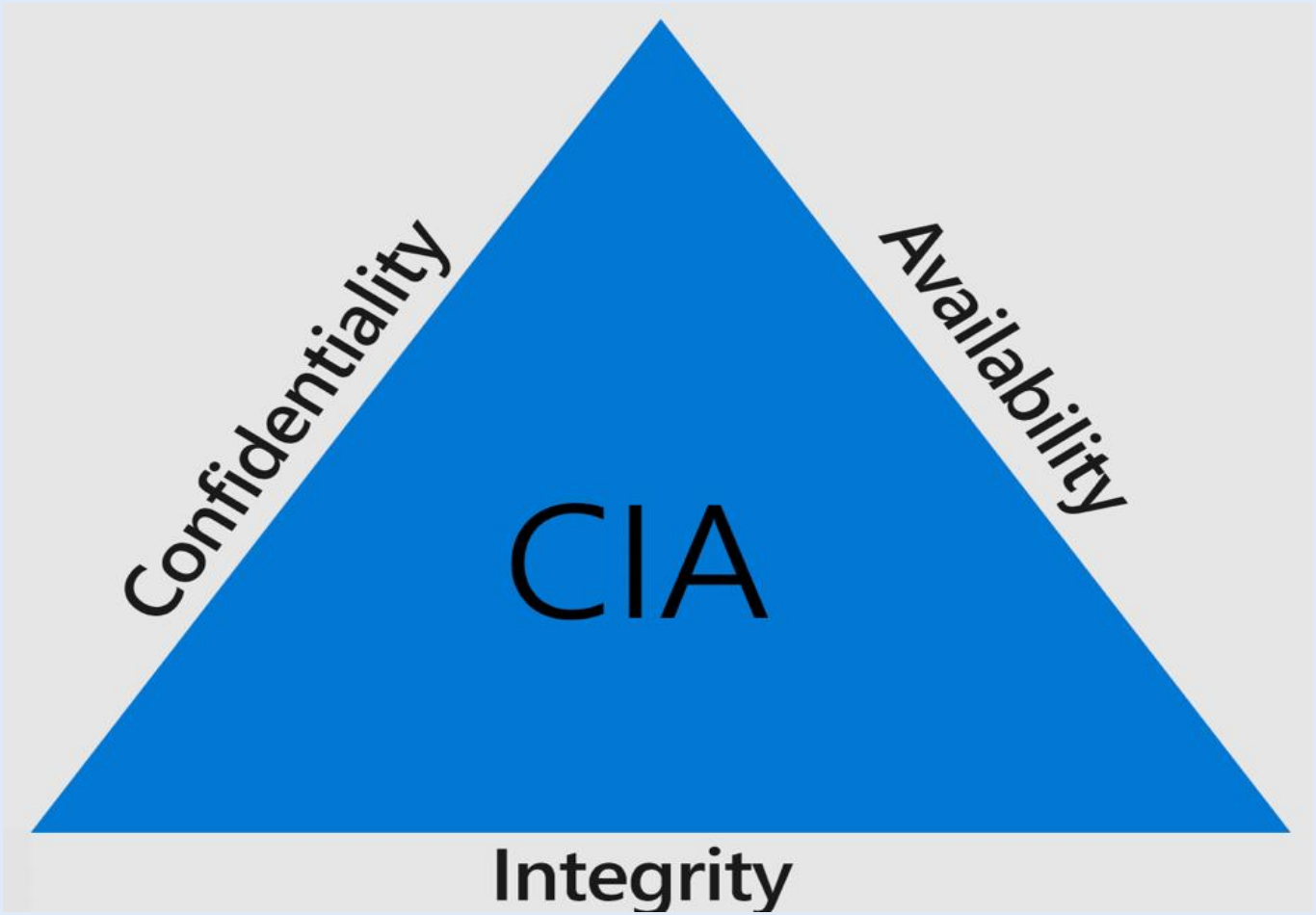
Need for security

- Computer security is necessary to secure data from unauthorized access.
- The user information must remain confidential and only authorized user can access it.
- The assets must remain safe and no one can change or modify it.
- The data or information should be available to the user when they need it.
- The computer security prevents the theft of or damage to the resources.

Computer Security Basics/Objectives

- Security of computers refers to the protection given to computers and the information contained in them from unauthorized access.
- The principal of security is to protect the confidentiality, integrity and availability of information.
- These principles together are known as CIA triad

CIA Triad



Security Basics/Essential Network and Computer Security Requirements

- There are following principles of security.

1) Confidentiality,

2) integrity,

3) availability

4) Accountability,

5) Non repudiation,

6) Reliability,

7) Authenticity

1) Confidentiality

- The principle of confidentiality specifies that only the sender and intended recipient should be able to access the contents of message.
- Confidentiality gets compromised if an unauthorized person is able to access a message.

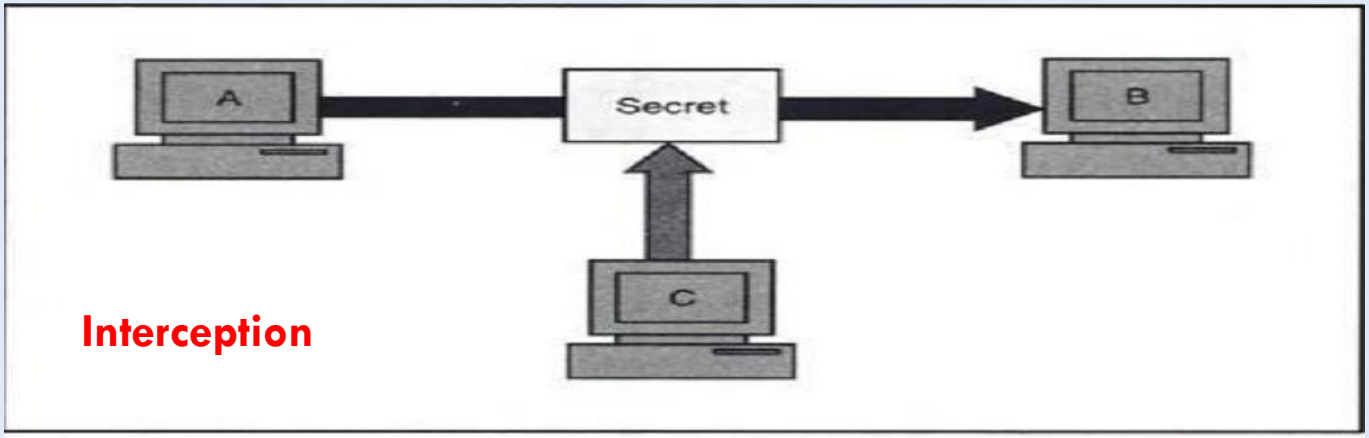


Fig. 1.2 *Loss of confidentiality*

2) Integrity

- It is the concept of ensuring that data has not been altered by an unknown entity during the transfer or storage.
- When the contents of a message are changed after sender sends it but before it reaches the intended recipient then we say that the integrity of message is lost.

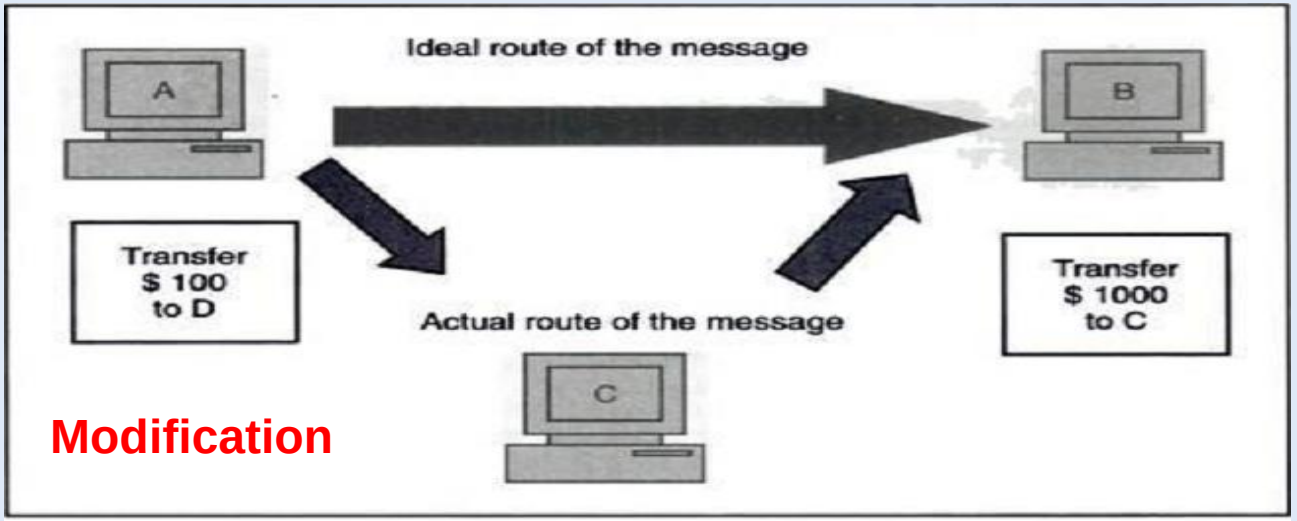


Fig. 1.4 *Loss of integrity*

3) Availability

- The principle of availability states that resources (information) should be available to authorized user at all times.
- For example due to intentional action of an unauthorized user C the authorized user A is not able to access the server computer B

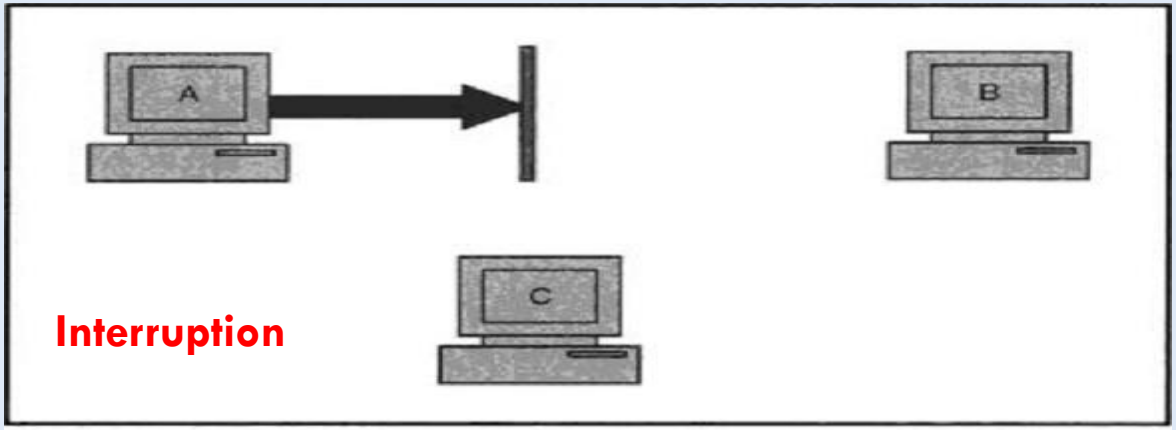


Fig. 1.5 *Attack on availability*

4) Accountability

- Accountability ensures that the audit information must be selectively kept and protected so that actions affecting security can be traced.
- It helps to find that authorized actions that can lead to a security violation.
- Also we can find the loopholes in our security system that allows unauthorized user to access the system.

5) Non repudiation

- It is a way to guarantee that sender of a message cannot later deny having sent the message and the recipient cannot deny having received the message.
- There are situation where a user sends a message, and later on refuses that he had sent that message .

5) Non repudiation

- For example:-
  - User A could send fund transfer request to bank over internet.
  - After the bank performs the fund transfer as per A's instructions, A could claim that he never sent such the fund transfer instruction to the bank.
  - Thus A denies his fund transfer instruction.
- The principle of non-repudiation eliminate such possibilities of denying something after having done it.

6) Reliability

- Reliability deals with the situations where a system has to perform properly in adverse conditions.
- It indicates that the computer system should consistently perform according to its specifications.

7) Authenticity

- The property of being genuine and being able to be verified and trusted.
- This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

Computer Security Challenges

- Security is not simple
- Potential attacks on the security features need to be considered
- Procedures used to provide particular services are not proper.
- It is necessary to decide where to use the various security mechanisms
- Requires constant monitoring
- Little benefit from security investment is perceived until a security failure occurs.
- Strong security is often viewed as an obstacle to efficient and user-friendly operation

OSI Security Architecture

- To assess effectively the security needs of an organization and to evaluate and choose various security products and policies.
- The manager that are responsible for security, needs some systematic way of defining the requirements for security.
- This is difficult enough in a centralized data processing environment and with the use of local and wide area networks, the problems increases.
- ITU-T3 Recommendation X.800, *Security Architecture for OSI*, defines such a systematic approach.
- The OSI security architecture is useful to managers as a way of organizing the task of providing security.

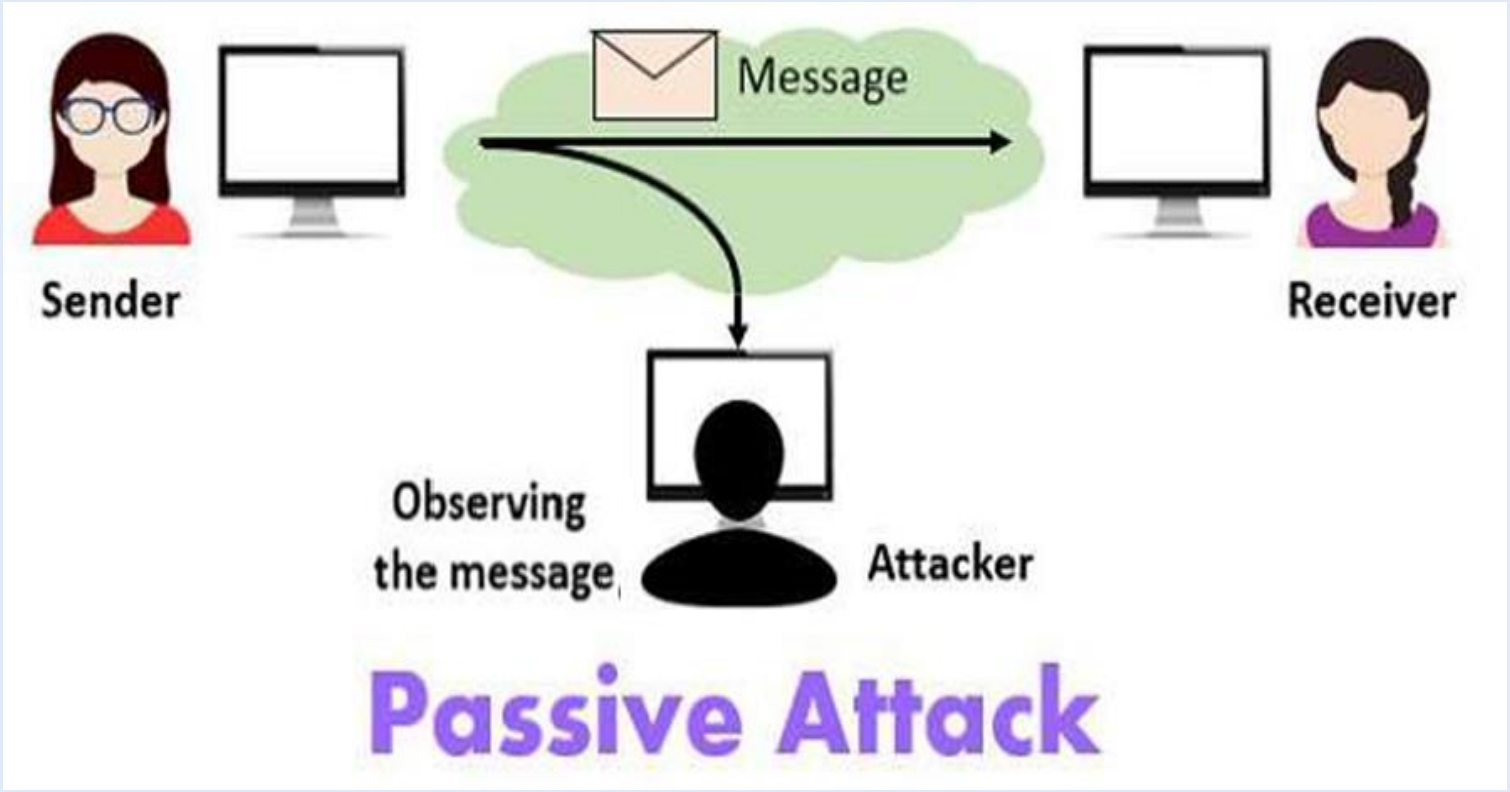
OSI Security Architecture

- The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as
  A. **Security attack:** Any action that compromises the security of information owned by an organization.
  B. **Security mechanism:** A process that is designed to detect, prevent, or recover from a security attack.
  C. **Security service:** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to defend security attacks, and they make use of one or more security mechanisms to provide the service.

A) Security Attacks

- A security attacks, can be classified as:
  - ***1) passive attacks*** and
  - ***2) active attacks.***

1) Passive Attacks



1) Passive Attacks

- Passive attack tries to read or make use of information from the system but does not influence system resources.
- Passive attacks are those, wherein the attacker performs in eavesdropping or monitoring of data transmission.
- In other words, the attacker aims to obtain information that is in transit.
- The term passive indicates that the attacker does not attempt to perform any modifications to the data.
- Due to this passive attacks are harder to detect.

1) Passive Attacks

- Two types of passive attacks are
  1. release of message contents and
  2. traffic analysis.

1. Release of message contents:

- In this attack when a confidential email or message is sent to another user then only that user be able to access it.
- If that message is released to another user then this attack occurs.
- It can be avoided by encoding a message.

1) Passive Attacks

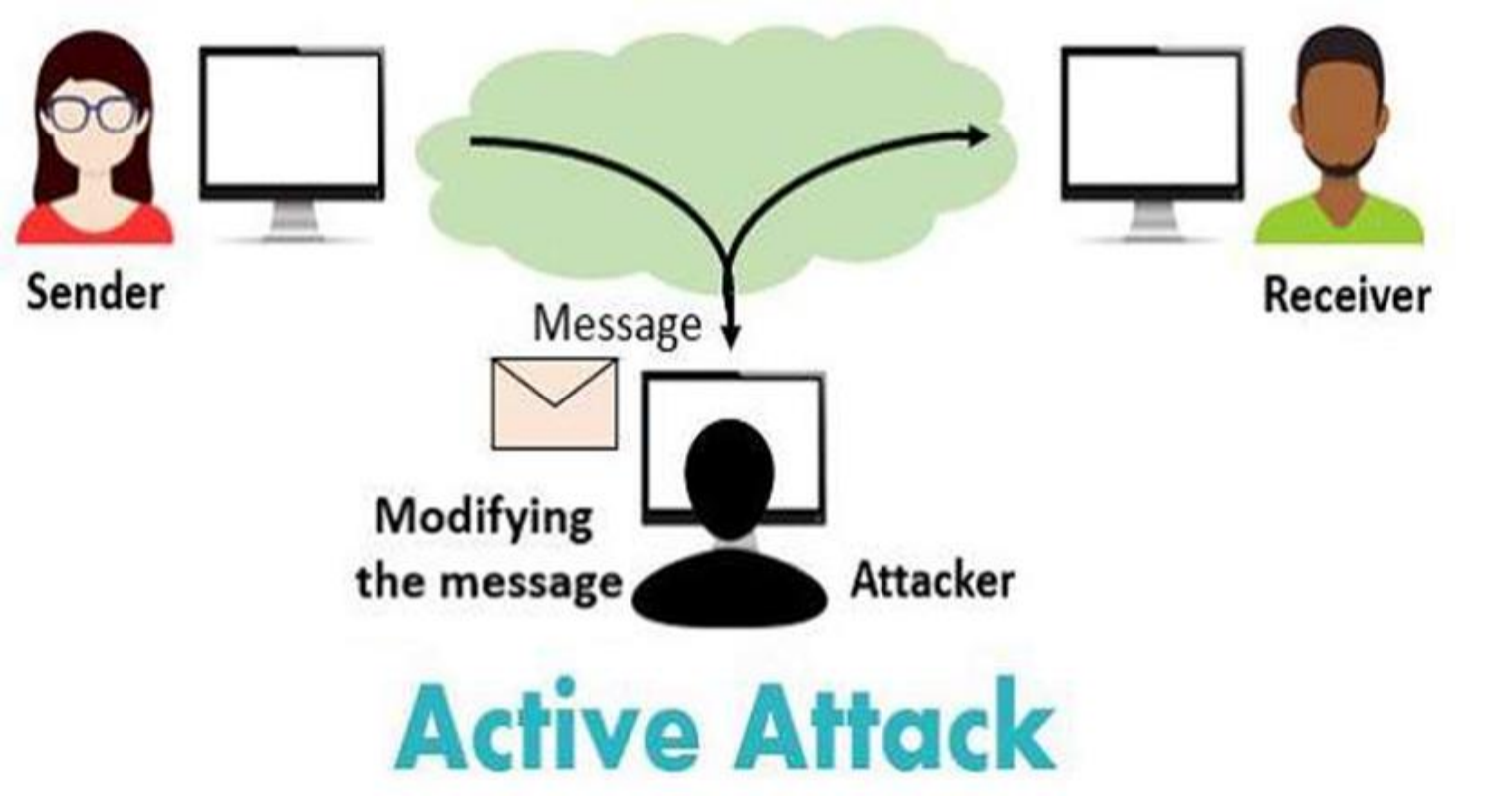
2. Traffic analysis.

- Suppose that we have encoded the contents of messages using encryption, so that opponents, even if they captured the message, could not extract the information from the message.
- In this attack if the message is encoded then also the attacker finds out the clues regarding the communication that is taking place.

1) Passive Attacks

- 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 a 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.

2) Active Attacks

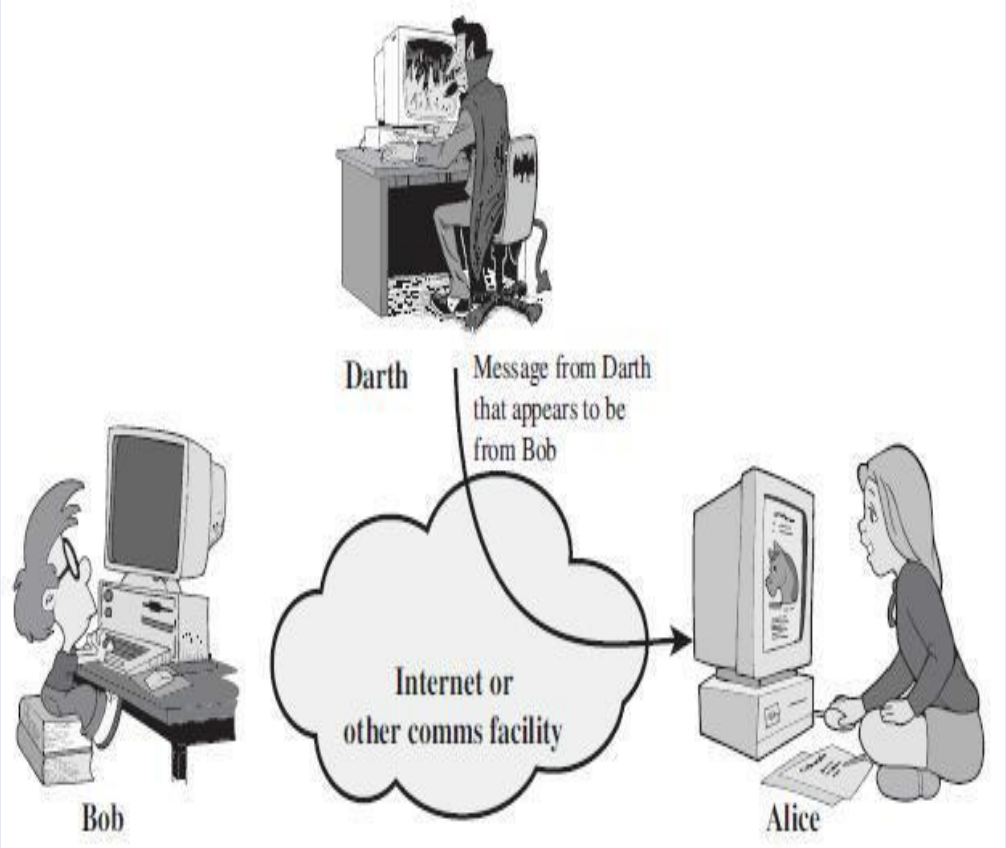


2) Active Attacks

- Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories:

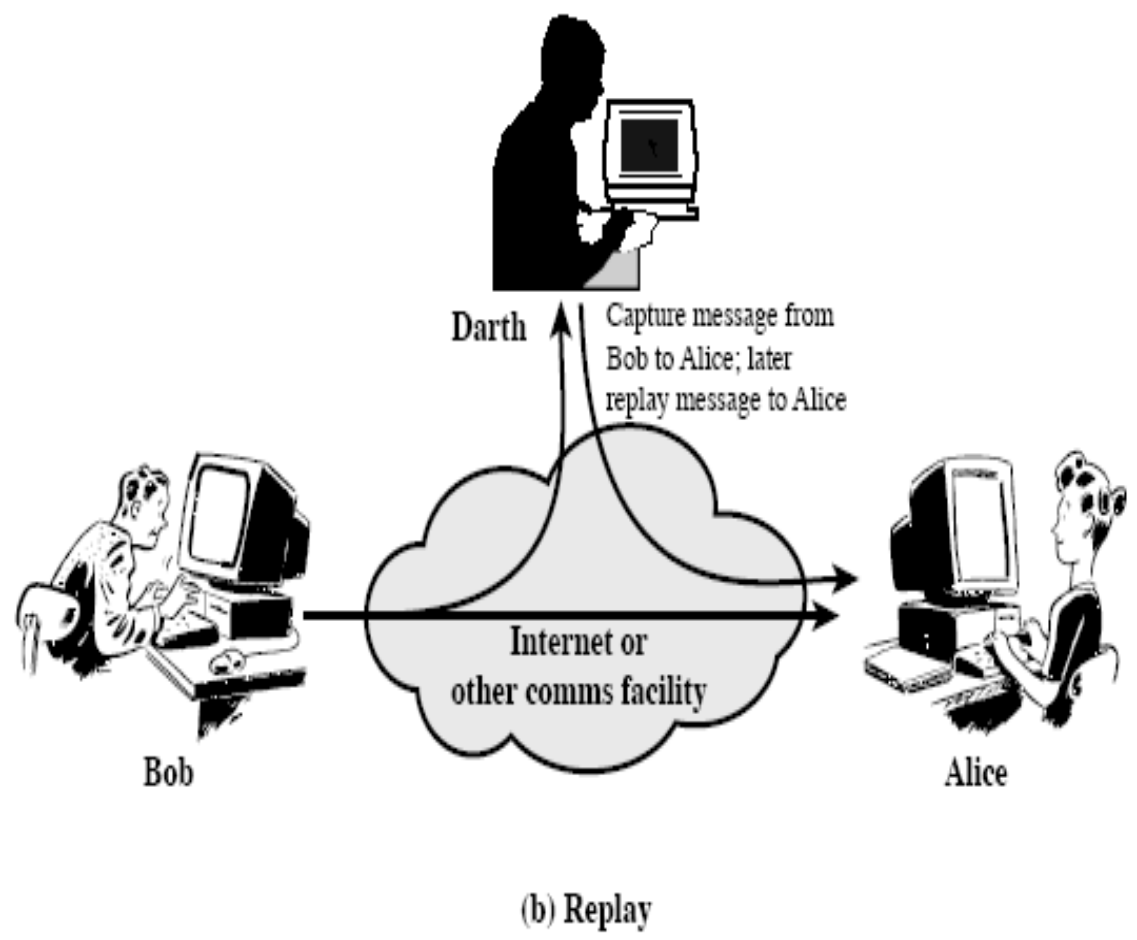
1. masquerade,
2. replay,
3. modification of messages, and
4. denial of service.

1) Masquerade



- A **masquerade** takes place when one entity pretends to be a different entity
- A masquerade attack is one in which the attacker poses as an authorized user of a system to gain access to it or greater privileges than they are authorized for.

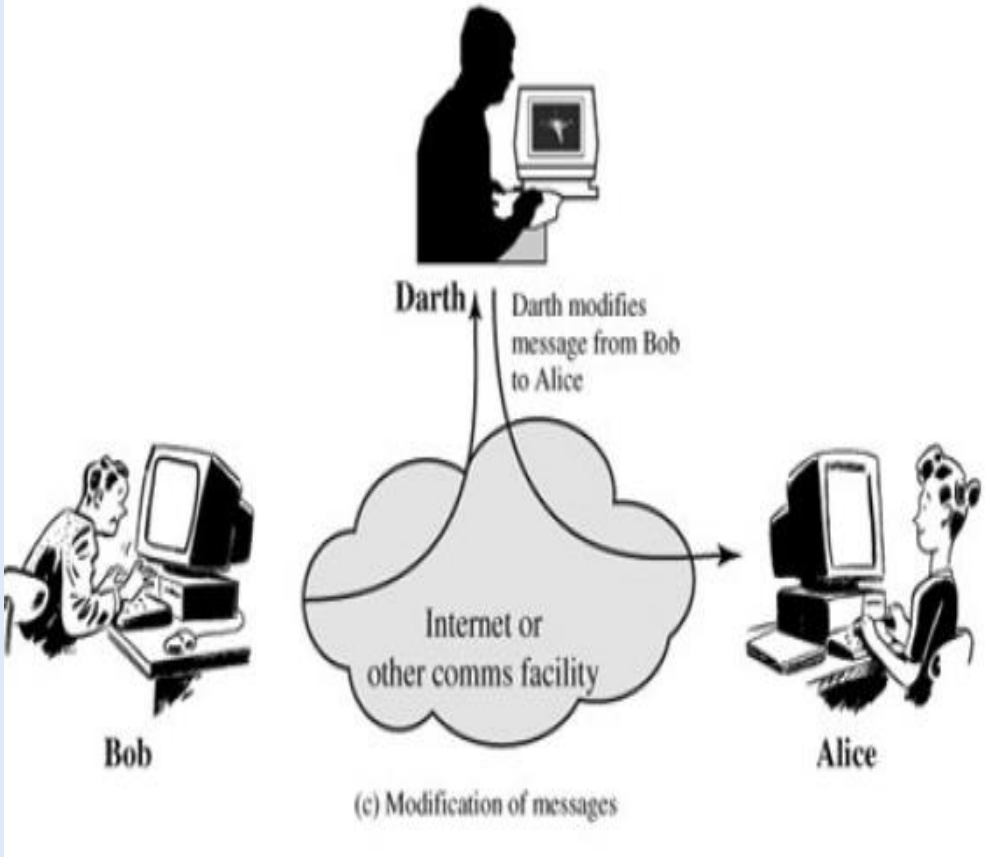
2) Replay



(b) Replay

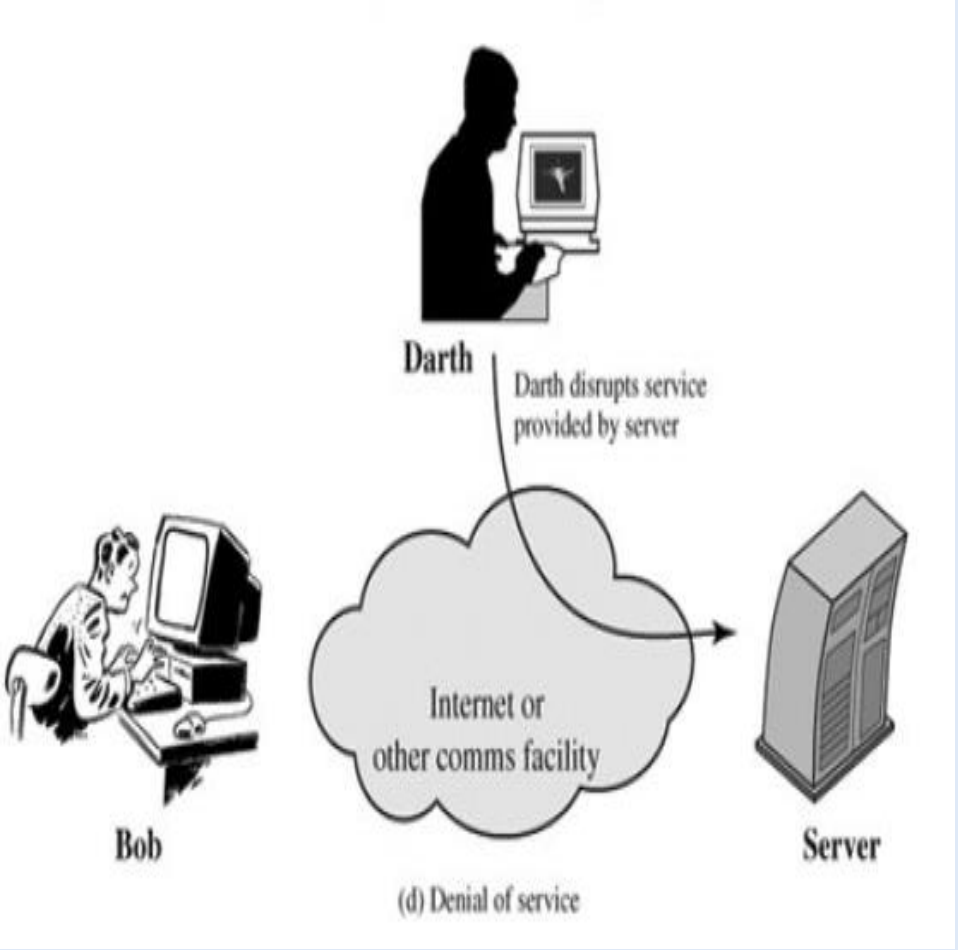
- Replay Attack is a type of security attack to the data sent over a network.
- In this attack, the hacker or any person with unauthorized access, captures the traffic and sends communication to its original destination, acting as the original sender.
- The receiver feels that it is an authenticated message but it is actually the message sent by the attacker.
- The main feature of the Replay Attack is that the client would receive the message twice, hence the name, **Replay Attack**.

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" is modified to mean "Allow Fred Brown to read confidential file."

4) Denial of service



- The **denial of service** prevents 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.
- 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.

B) Security Services

- X.800 defines a security service as a service that is provided by a protocol layer of communicating systems and that ensures adequate security of the systems and data transfers.
- It is defined as a processing or communication service that is provided by a system to give a specific kind of protection to system resources;
- Security services implement security policies and are implemented by security mechanisms.
- X.800 divides these services into five categories and fourteen specific services.

1) AUTHENTICATION

- The authentication service is concerned with assuring that a communication is authentic.
- It provides the assurance that, the communicating entity is the one that it claims to be.
  - **Peer Entity Authentication**
    - Provides for the confirmation of the identity of a peer entity in an association.
  - **Data-Origin Authentication**
    - Provides for the confirmation of the source of a data unit.

2) Access Control

- The prevention of unauthorized use of a resource
- 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.

3) Data Confidentiality

- The protection of data from unauthorized disclosure.
  - **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.

4) DATA INTEGRITY

- The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).
  - **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, with recovery attempted.
  - **Connection Integrity without Recovery**
    - As above, but provides only detection without recovery.
  - **Selective-Field Connection Integrity**
    - Provides for the integrity of selected fields within the data block transferred over a connection.
  - **Connectionless Integrity**
    - Provides for the integrity of a single connectionless data block.
  - **Selective-Field Connectionless Integrity**
    - Provides for the integrity of selected fields within a single connectionless data block;

5) NONREPUDIATION

- Provides protection against denial by one of the entities involved in a communication of having participated in communication.
  - **Nonrepudiation, Origin**
    - Proof that the message was sent by the specified party.
  - **Nonrepudiation, Destination**
    - Proof that the message was received by the specified party.

C) SECURITY MECHANISMS

- There are two types of security Mechanisms
- 1. Specific Security Mechanisms
- 2. Pervasive Security Mechanisms

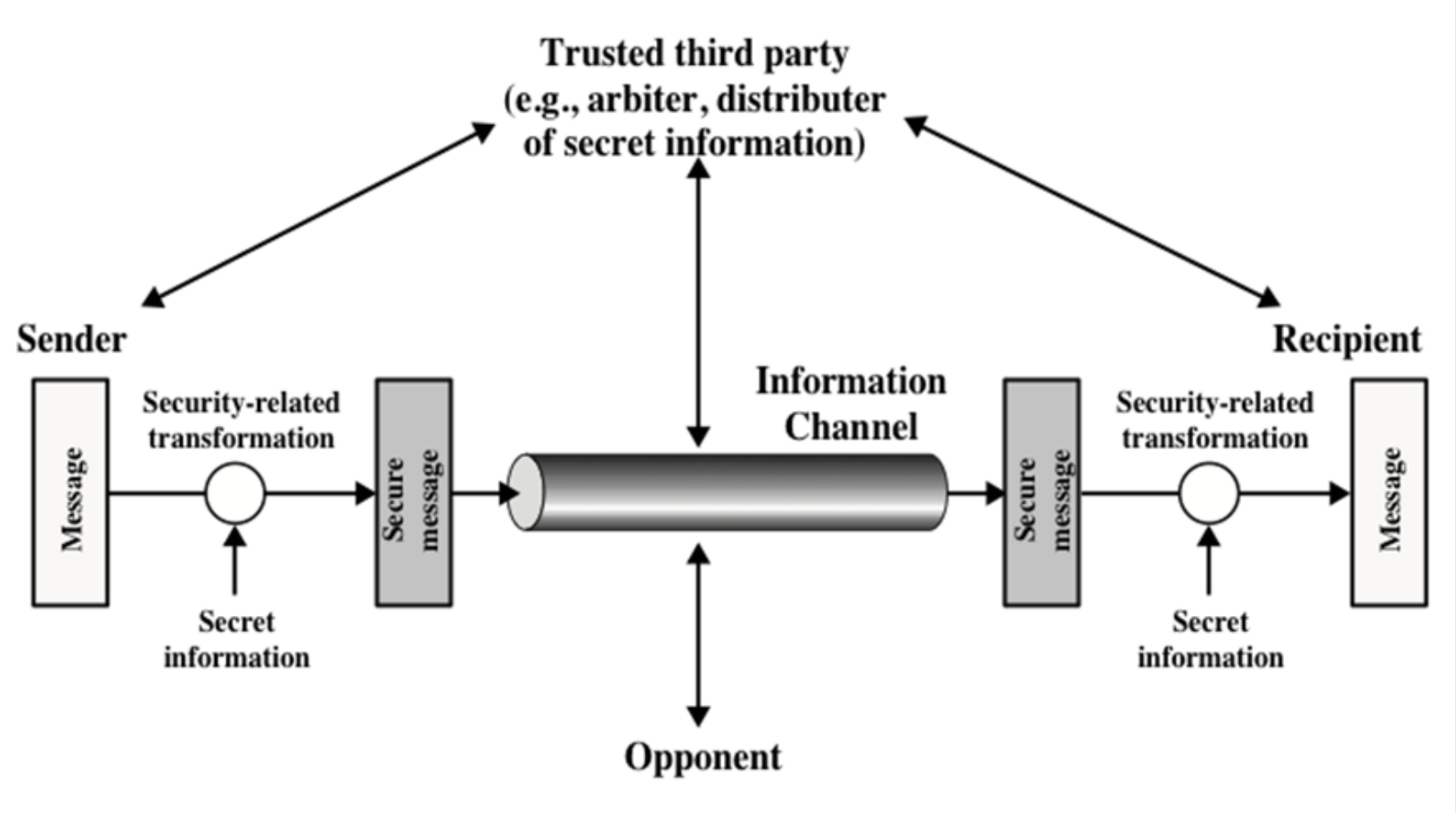
1. Specific Security Mechanisms

- May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.
- **Encipherment**
  - The use of mathematical algorithms to transform data into a form that is not readable.
  - The transformation and recovery of the data depend on an algorithm encryption keys.
- **Digital Signature**
  - It 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**
  - A variety of mechanisms that enforce access rights to resources.
- **Data Integrity**
  - A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

2. Pervasive Security Mechanisms

- Mechanisms that are not specific to any particular OSI security service or protocol layer.
- **Trusted Functionality**
  - That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
- **Security Label**
  - The label to a resource (may be a data unit) that assigns the security attributes to 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.

A MODEL FOR NETWORK SECURITY



A MODEL FOR NETWORK SECURITY

- A message is to be transferred from one party to another across Internet.
- The two parties, who are the *principals* in this transaction, must cooperate for the exchange to take place.
- A logical information channel is established by defining a route through the Internet from source to destination.
- Security aspects come into play when it is required to protect the information from an opponent who may present a threat to confidentiality, authenticity, and so on.

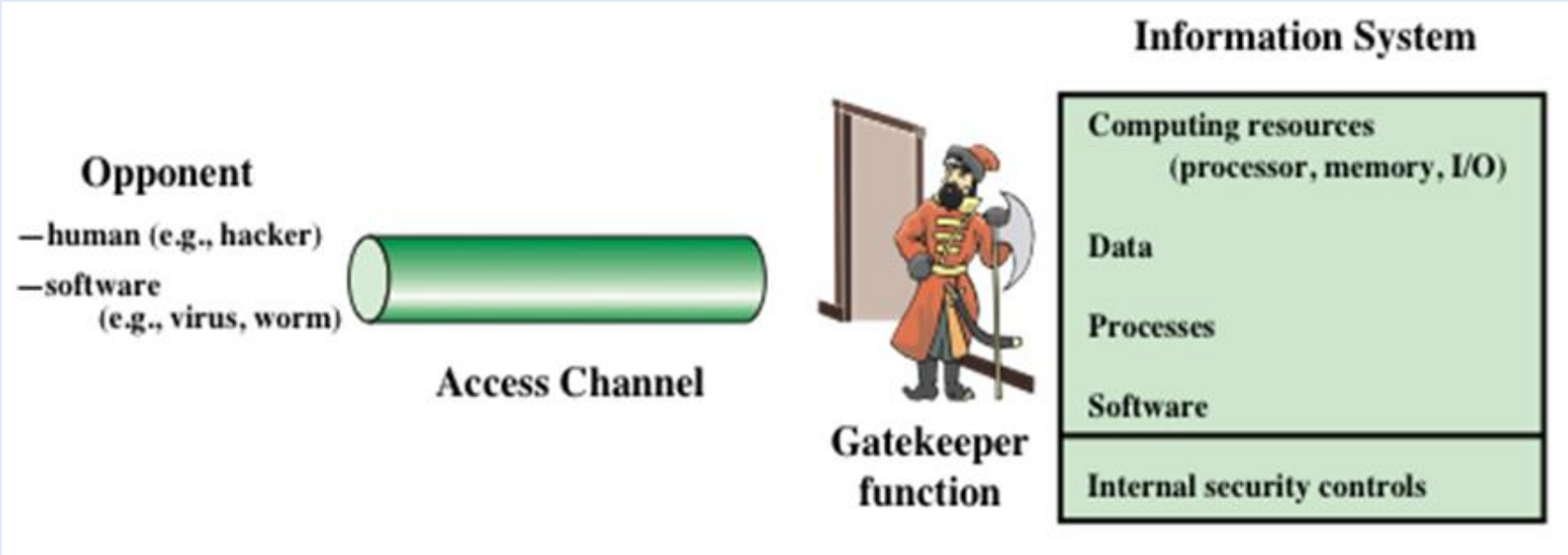
A MODEL FOR NETWORK SECURITY

- All the techniques for providing security have two components:
  - A security-related transformation on the information to be sent. (encryption)
  - Some secret information shared by the two principals and, it is unknown to the opponent. (encryption key)

A MODEL FOR NETWORK SECURITY

- A trusted third party may be needed to achieve secure transmission.
- For example, a third party may be responsible for distributing the secret information to the two principals.
- This general model shows that there are four basic tasks in designing a particular security service:
  - **1.** Design a strong algorithm for performing the security-related transformation.
  - **2.** Generate the secret information (key) to be used with the algorithm.
  - **3.** Develop methods for the distribution and sharing of the secret information.
  - **4.** Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

Network Access Security Model



Network Access Security Model

- Figure shows the Network Access Security Model which reflects a concern for protecting an information system from unwanted access.
  - There are hackers, who attempt to penetrate systems.
  - The hacker can be someone who is not having harmful intent, but simply gets satisfaction from breaking and entering a computer system.
  - Or there can be an intruder, a disappointed employee who wishes to do damage or a criminal who seeks to exploit computer assets for financial gain.

Network Access Security Model

- Another type of unwanted access is the placement of logic in a computer system that exploits vulnerabilities in the system and that can affect application programs(viruses).
- Programs can present two kinds of threats:
  - **Information access threats:** Intercept or modify data on behalf of users who should not have access to that data.
  - **Service threats:** Exploit service flaws in computers to Stop use by authorized users.

Network Access Security Model

- Viruses and worms are two examples of software attacks.
- Such attacks can be introduced into a system by means of a disk or useful software.
- They can also be inserted into a system across a network.
- The security mechanisms needed to cope with unwanted access fall into two broad categories as shown in figure.

Network Access Security Model

- The first category might be termed a gatekeeper function.
- It includes password-based login procedures that are designed to deny access to all unauthorized users and a screening logic that is designed to detect and reject worms, viruses, and other similar attacks.
- Once either an unwanted user or unwanted software gains access, the second line of defense consists of a variety of internal controls that monitor activity and analyze stored information to detect the presence of unwanted intruders.

Plain text

- Plaintext is the term used to refer to the information in plain language that the sender desires to send to receiver.
- It is referred to as cleartext.
- plaintext is commonly referred to as the input to a cipher or encryption algorithm.

Hello Welcome to the Lecture

Cipher text

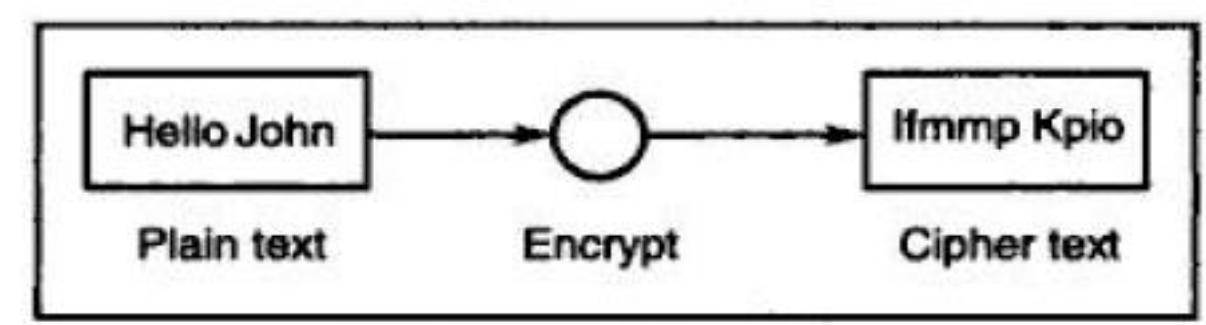
- Ciphertext is encrypted text transformed from plaintext using an encryption algorithm.
- Ciphertext can't be read until it has been converted into plaintext (decrypted) with a key.

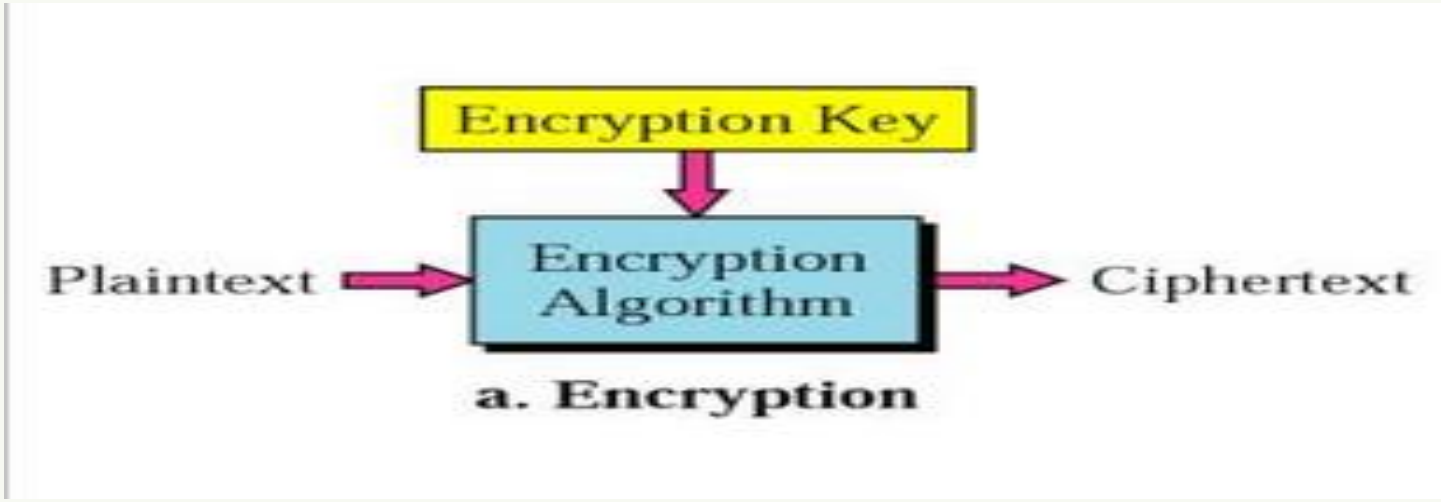
Dbcgfg
Dfdgff
Kjhkhjg
Ngghg

Encryption

- The process of encoding plain text messages into cipher text messages is called as encryption.
- Encryption is the conversion of data in a form called cipher that cannot be understood by unauthorized people.
- In encryption the original message is encrypted using an algorithm called encryption algorithm.

Encryption

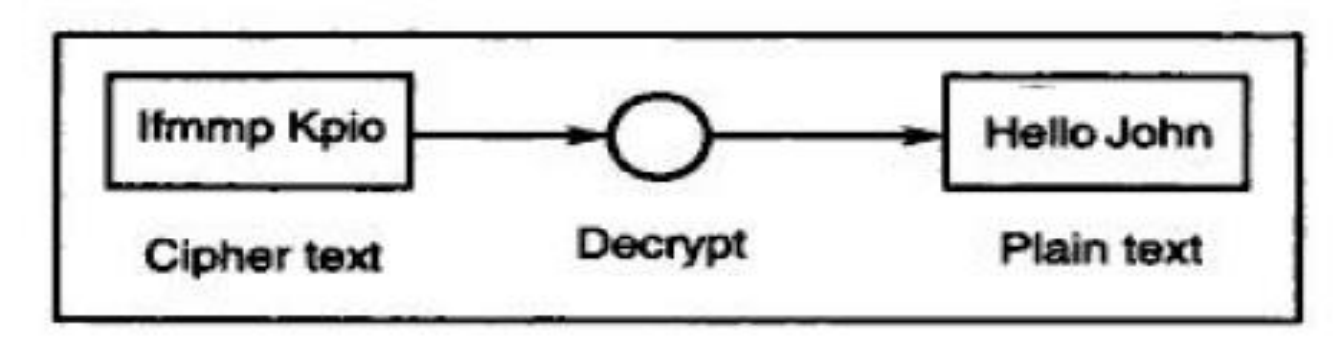

Hello John
Plain text
Encrypt
Ifmmp Kpio
Cipher text

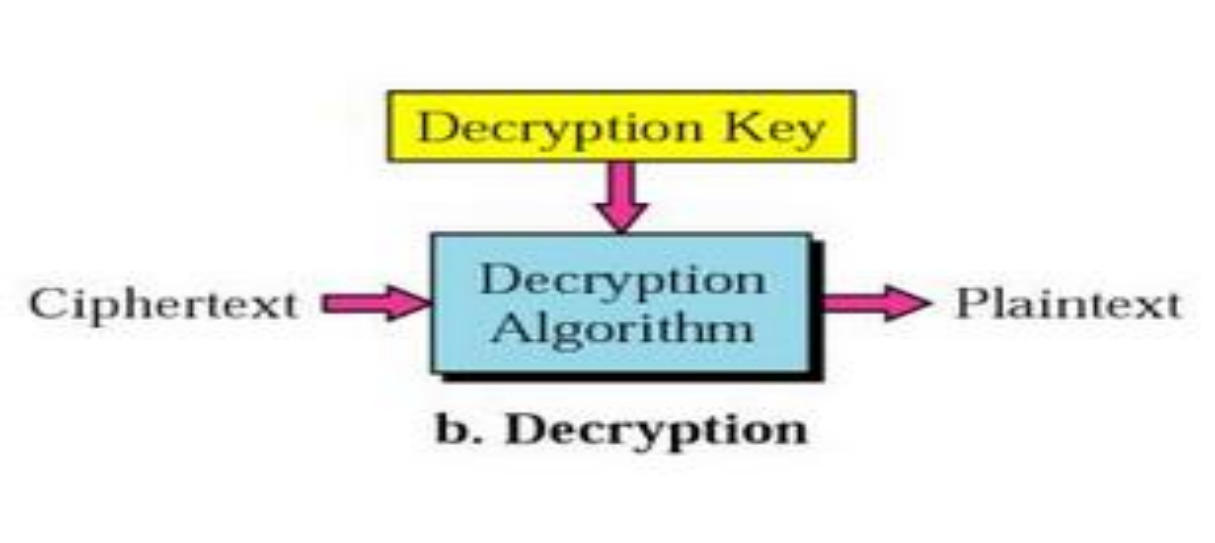

Encryption Key
Plaintext
Encryption Algorithm
Ciphertext
a. Encryption

Decryption

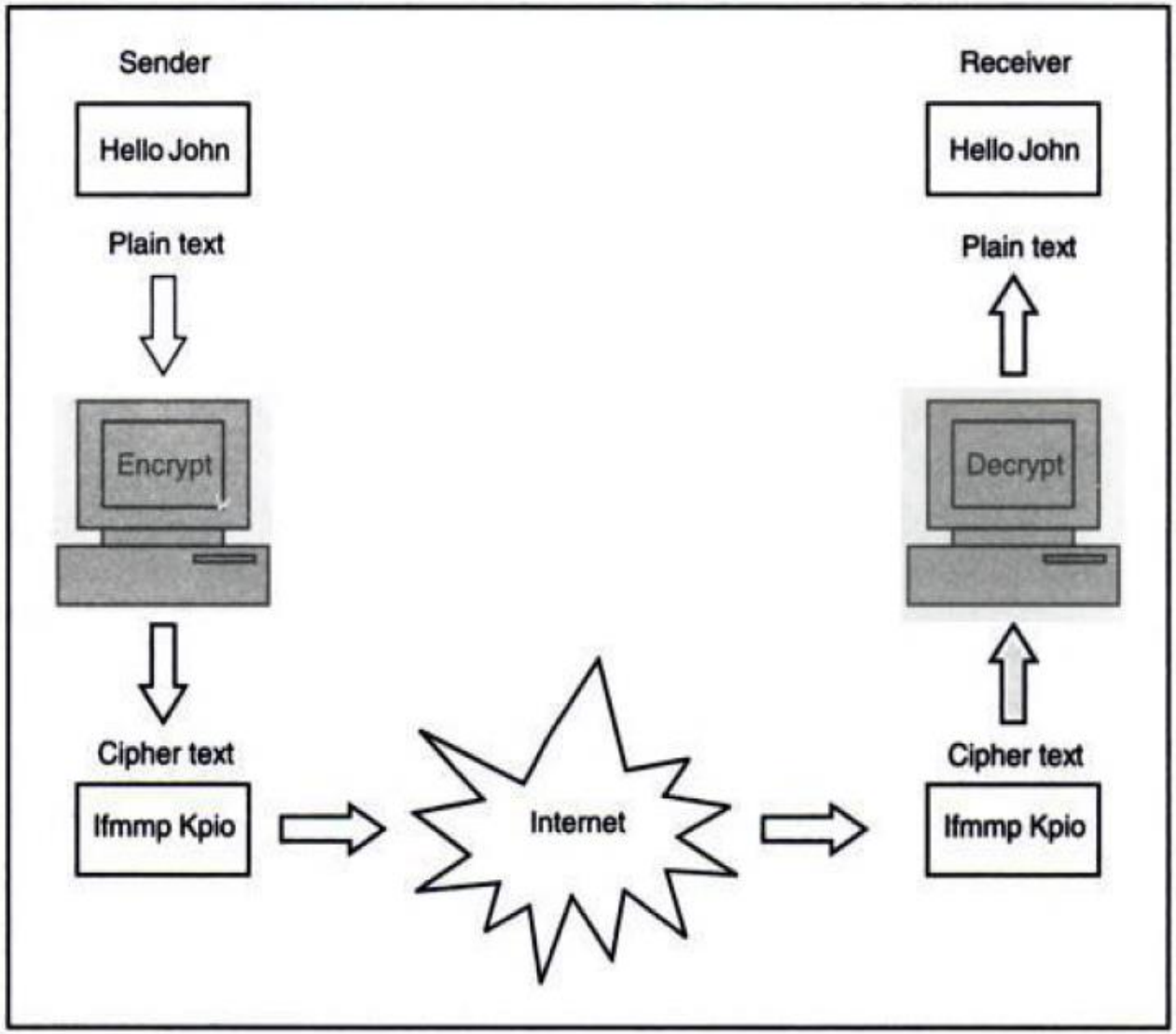
- The reverse process of transforming cipher text messages back to plain text messages is called as decryption.
- *Decryption is exactly opposite of encryption.*
- *Decryption transforms a cipher text message back into plain text using decryption algorithm.*

Decryption

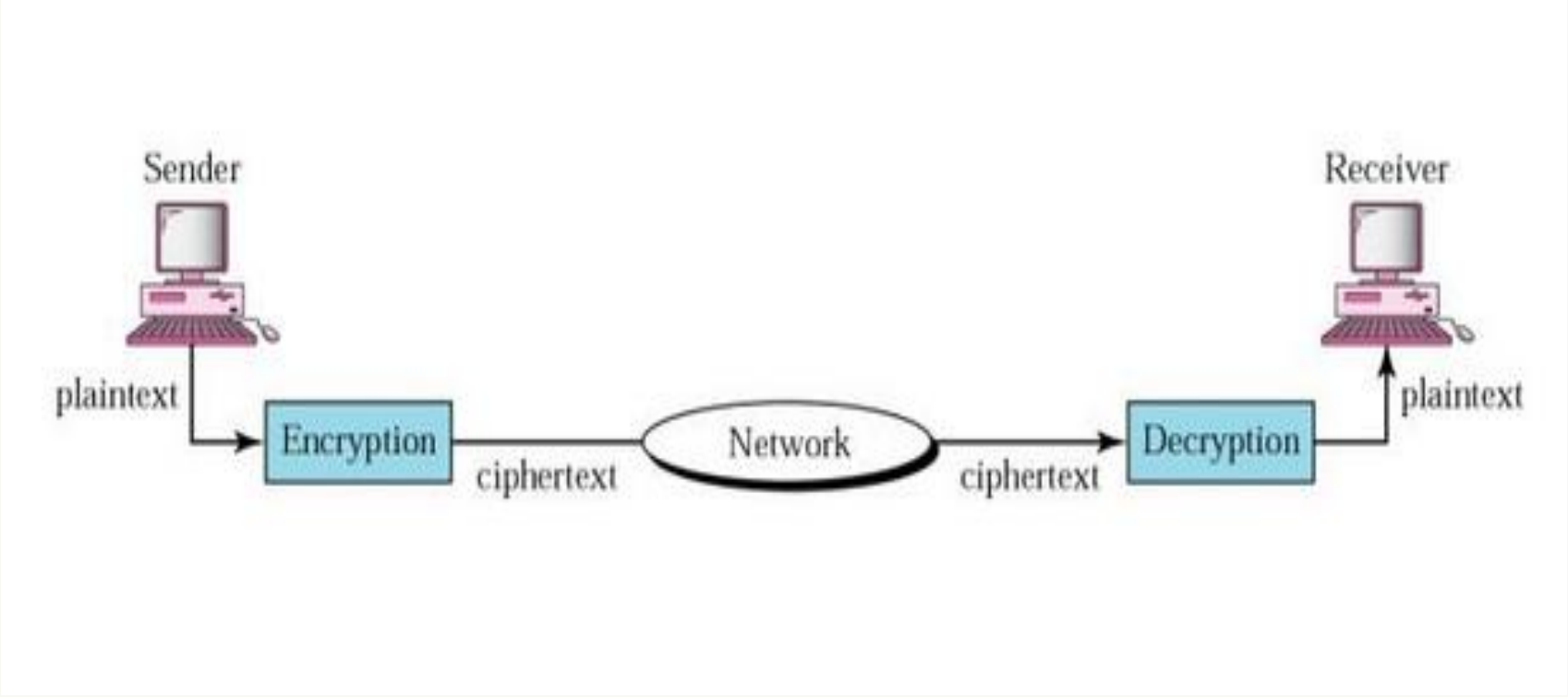

Ifmmp Kpio
Cipher text
Decrypt
Hello John
Plain text


Decryption Key
Ciphertext
Decryption Algorithm
Plaintext
b. Decryption

Cryptography



Cryptography



Cryptography

- *Cryptography is the art and science of achieving security by encoding messages to make them non-readable.*
- It enables to store sensitive information or transmitted across insecure network so that it cannot be read by anyone except the intended receiver.
- Cryptography uses the encryption at sending end to encrypt the message from plain text to cipher text.
- At the receiving end the ciphertext message is decrypted into original form by using decryption.
- Encryption and decryption usually make use of a key and the data cannot be decrypted without knowing the proper key.

Cryptanalysis

- Cryptanalysis is the study of methods for obtaining the meaning of encrypted information, without access to the secret information that is typically required to do so.
- Typically, this involves knowing how the system works and finding a secret key.
- Cryptanalysis is also referred to as codebreaking or cracking the code.
- The areas of cryptography and cryptanalysis together are called **Cryptology.**

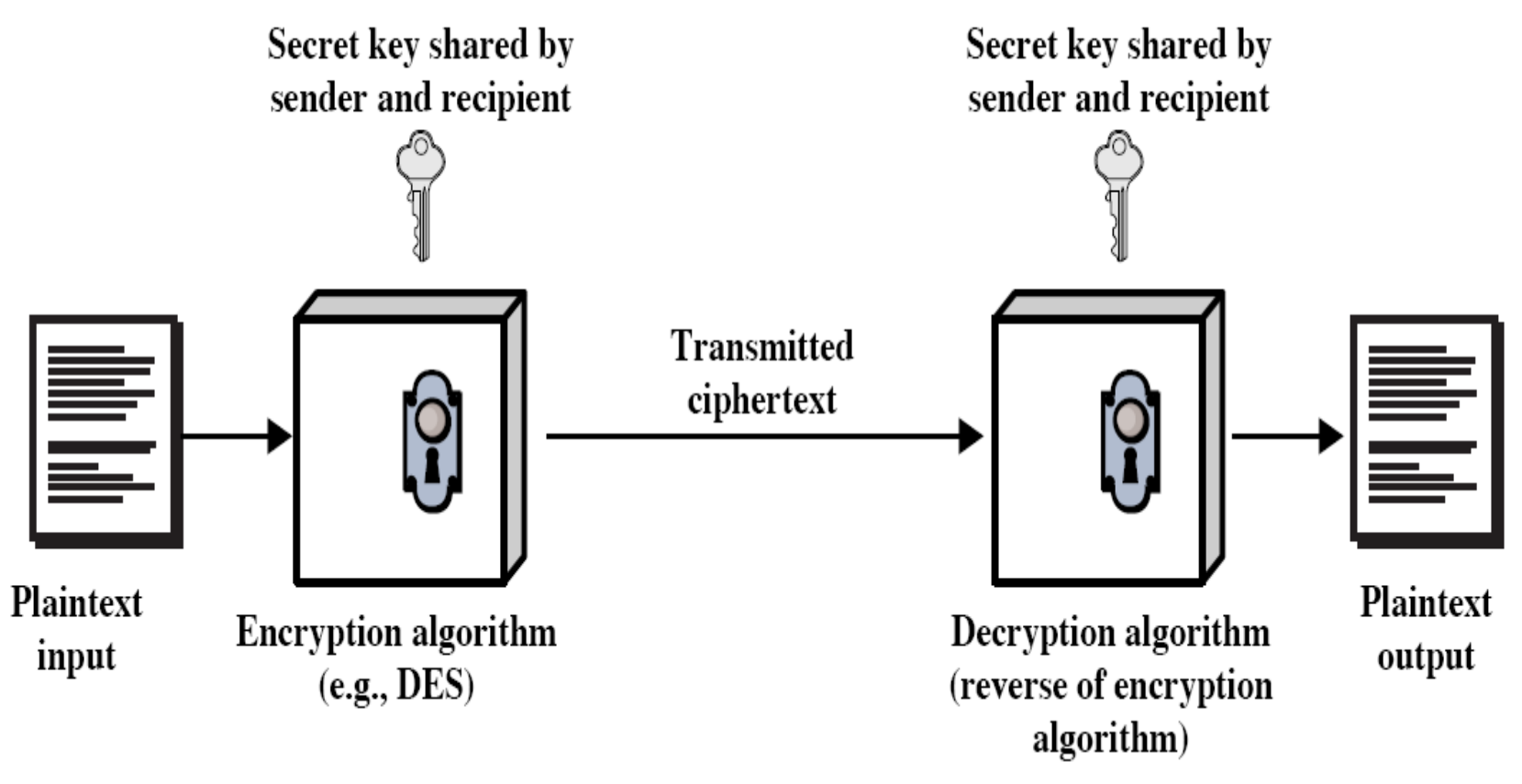
CLASSICAL ENCRYPTION TECHNIQUES

- Symmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the same key.
- It is also known as conventional encryption.
- Symmetric encryption transforms plaintext into cipher text using a secret key and an encryption algorithm.
- Using the same key and a decryption algorithm, the plaintext is recovered from the cipher text.
- The two types of attack on an encryption algorithm are cryptanalysis, based on properties of the encryption algorithm, and brute-force, which involves trying all possible keys.

CLASSICAL ENCRYPTION TECHNIQUES

- Traditional symmetric ciphers use substitution and/or transposition techniques.
- Substitution techniques map plaintext elements (characters, bits) into ciphertext elements.
- Transposition techniques systematically transpose the positions of plaintext elements.

SYMMETRIC CIPHER MODEL



SYMMETRIC CIPHER MODEL

- A symmetric encryption scheme has five ingredients as shown in fig.
  1. **Plaintext:** This is the original message or data that act as input to the algorithm.
  2. **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.
  3. **Secret key:** The secret key is also input to the encryption algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

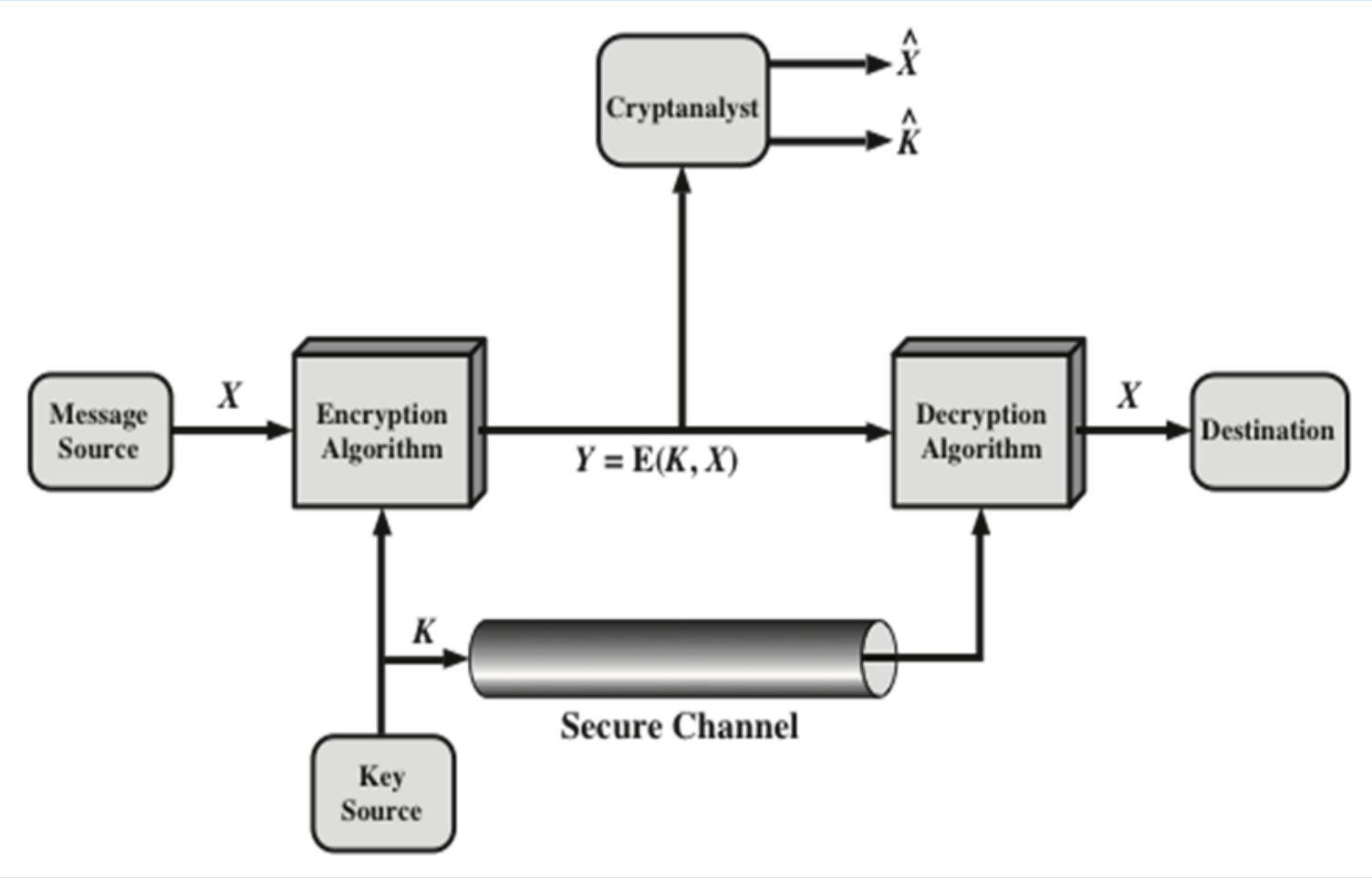
SYMMETRIC CIPHER MODEL

4. **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts.
5. **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key as input and produces the original plaintext.

SYMMETRIC CIPHER MODEL

- There are two requirements for secure use of conventional encryption:
- **1.** We need a strong encryption algorithm. such that an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key.
- **2.** Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable.

Model of Symmetric Cryptosystem



Model of Symmetric Cryptosystem

- Let us take a closer look at the essential elements of a symmetric encryption scheme, using Figure.
- A source produces a message in plaintext,

$$X = [X1, X2, \ldots\ldots, XM].$$

- For encryption, a key of the form $K = [K1, K2, \ldots\ldots, KJ]$ is generated.
- If the key is generated at the message source, then it must also be provided to the destination by means of some secure channel.
- Alternatively, a third party could generate the key and securely deliver it to both source and destination.
- With the message X and the encryption key K as input, the encryption algorithm forms the ciphertext

$$Y = [Y1, Y2, \ldots\ldots\ldots\ldots, YN].$$

- We can write this as $Y = E(K, X)$

Model of Symmetric Cryptosystem

- The intended receiver, in possession of the key, is able to invert the transformation:

$$X = D(K, Y)$$

- An opponent, observing Y but not having access to K or X, may attempt to recover X or K or both X and K.
- It is assumed that the opponent knows the encryption (E) and decryption (D) algorithms.
- If the opponent is interested in only this particular message, then the focus of the effort is to recover X.
- Often, however, the opponent is interested in being able to read future messages as well, in which case an attempt is made to recover K

Cryptography

- Cryptographic systems are characterized along three independent dimensions:

1. The type of operations used for transforming plaintext to ciphertext.

  - All encryption algorithms are based on two general principles:
  - substitution, in which each element in the plaintext is mapped into another element, and
  - transposition, in which elements in the plaintext are rearranged.
  - The fundamental requirement is that no information be lost.
  - Most systems, involve multiple stages of substitutions and transpositions.

Cryptography

2. The number of keys used.

- If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption.
- If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption.

3. The way in which the plaintext is processed.

- **A *block cipher*** processes the input one block of elements at a time, producing an output block for each input block.
- **A *stream cipher*** processes the input elements continuously, producing output one element at a time, as it goes along.

Cryptanalysis and Brute-Force Attack

- Typically, the objective of attacking an encryption system is to recover the key in use rather than simply to recover the plaintext of a single ciphertext.
- There are two general approaches to attacking a conventional encryption scheme:

■ **Cryptanalysis:**

- Cryptanalytic attacks rely on the nature of the algorithm plus some knowledge of the general characteristics of the plaintext or even some sample plaintext–ciphertext pairs.
- This type of attack exploits the characteristics of the algorithm to attempt to identify a specific plaintext or the key being used.

■ **Brute-force attack:**

- The attacker tries every possible key on a piece of ciphertext until plaintext is obtained.
- On average, half of all possible keys must be tried to achieve success.

SUBSTITUTION TECHNIQUES

- A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.
- If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.

Caesar Cipher

- In cryptography, a **Caesar cipher, also known shift cipher is one of the** simplest and oldest encryption techniques.
- It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet.
- The method is named after Julius Caesar, who used it in his private correspondence.
- He used a shift of 3, so that the plain text letter is converted into cipher text letter.
- For example, with a left shift of 3, A would be replaced by D, B would become E, and so on.
- Note that the alphabet is wrapped around, so that the letter following Z is A.

1) Caesar Cipher

- Can define transformation as:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- Mathematically give each letter a number

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Then the algorithm can be expressed as follows. For each plaintext letter *p*, substitute the ciphertext letter C:

$$C = E(3, p) = (p + 3) \bmod (26)$$

- A shift may be of any amount, so that the general Caesar algorithm is

$$C = E(k, p) = (p + k) \bmod 26$$

1)Caesar Cipher

- where *k* takes on a value in the range 1 to 25.
- The decryption algorithm is simply

  $p = D(k, C) = (C - k) \bmod 26$

- cryptanalysis is easily performed: simply try all the 25 possible keys
- Three important characteristics of this problem enabled us to use a brute force cryptanalysis:
- **1.** The encryption and decryption algorithms are known.
- **2.** There are only 25 keys to try.
- **3.** The language of the plaintext is known and easily recognizable.

1)Caesar Cipher

- Example:

  a b c d e f g h i j k l m n o p q r s t u v w x y z

  D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

- **The plaintext of "COMPUTER" with key 3 can be calculated as:**
- **C becomes F**
- **O becomes R**
- **M becomes P**
- **P becomes S**
- **U becomes X**
- **T becomes W**
- **E becomes H**
- **R becomes U**

- **So the cipher text is "FRPSXWHU"**

2) Monoalphabetic Ciphers

- Monoalphabetic substitution cipher is a cipher in which each occurrence of a plaintext symbol is replaced by a corresponding ciphertext symbol to generate ciphertext.
- The key for such a cipher is a table of the correspondence or a function from which the correspondence is computed.
- Each plaintext letter maps to a different random ciphertext letter, hence key is 26 letters long.
- If the "cipher" line can be any permutation of the 26 alphabetic characters, then there are 26! or greater than 4×10^{26} possible keys

2) Monoalphabetic Ciphers

- Example:

  a b c d e f ..... Z

  P X J T Q N ..... G

- **The plaintext of "CAB" can be calculated as:**
- **C becomes J**
- **A becomes P**
- **B becomes X**
- **The Encrypted text is "JPX"**

2) Monoalphabetic Ciphers

- Monalphabetic substitution ciphers are easy to break using a decryption method called **letter frequency analysis.**
- This is done by studying the text in the language of the cipher, and the frequency of each letter can be determined.
- For example, in the English language, the most frequent letter is E followed by T
- By substituting the most frequent letter in the ciphertext with the letter E the second most frequent with the letter T and so on it will end up with the original plaintext.

3) Playfair Cipher

- This algorithm was invented by Charles Wheatstone, but it was named after Lord Playfair who promoted the use of the cipher.
- The best-known multiple-letter encryption cipher is the Playfair,
- It treats digraphs in the plaintext as single units and translates these units into ciphertext digraphs.
- The Playfair algorithm is based on the use of a 5 * 5 matrix of letters constructed using a keyword.

3) Playfair Cipher

- In example below, the keyword is *monarchy*.
- The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top tobottom.
- And then filling in the remainder of the matrix with the remaining letters in alphabetic order.
- The letters I and J count as one letter.

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

3) Playfair Cipher

- Plaintext is encrypted two letters at a time, according to the following rules:
  - **1.** Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x, so that **hello** would be treated as **he lx lo**.
  - **2.** Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last. For example, **ar** is encrypted as **RM**.
  - **3.** Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. For example, **mu** is encrypted as **CM**.
  - **4.** Otherwise, form a rectangle for which the two plaintext letter are at two opposite corners. Then replace each plaintext letter with the letter that forms the other corner of the rectangle that lies on the same row as that plaintext letter. Thus, **hs** becomes **BP** and **ea** becomes **IM** (or JM, as the encipherer wishes).

- Write down the steps to convert the plaintext into cipher text using Playfair Cipher. Also generate the Ciphertext from the following plaintext using Play fair cipher:
  - Plaintext = MY NAME IS ATUL
  - KEY = PLAYFAIR EXAMPLE
  - **Cipher Text: XF OL IX MK PV LR**
- Solve the following Example using PlaYfair cipher:
  - 1) Key = THIRDCO, Plaintext = COMPUTER
  - 2) Key = PLAYFAIR EXAMPLE Plaintext = hide gold in tree stump
  - Ciphertext= BM OD ZB XD NA BE KU EX MO UV IF
- Describe the algorithm to convert the plaintext into cipher text using Playfair Cipher. Also Derive the Ciphertext from the following plaintext using Play fair cipher:
  - Plaintext = instrument
  - KEY = monarchy
  - in = GA, st = TL , ru = MZ, me = CL, nt = RQ

4) Hill Cipher

- The hill cipher is a polygraphic substitution cipher based on linear algebra.
- It was invented by Lester Hill and it operate on digraphs, trigraphs (3 letter blocks).
- To encrypt a message using hill cipher first convert the keyword in to a key matrix (2X2 or 3X3)
- Also convert the plaintext in to digraphs or trigraphs.
- Then perform matrix multiplication and apply modulo 26 on the vectors obtained.
- These vectors are then converted back into letters to produce the cipher text.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- For example consider 2X2 block example.
- Plain text = comp
- Key = bace
- Turn the keyword in to a matrix. If it is longer then 4 letters then take only first 4 letters and if it was shorter fill it up with alphabet in order

  B A

  C E
- Now convert each alphabet in key in to a number by its position in the alphabet

  1 0

  2 4
- Now split the plaintext into digraphs and write these as column vectors.

  C M

  O P

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Now convert the plaintext column vectors into numbers

C M = $\begin{bmatrix} 2 & 12 \\ 14 & 15 \end{bmatrix}$

O P

- Now perform the matrix multiplication. Multiply key matrix by each column vector.

$\begin{bmatrix} 1 & 0 \\ 2 & 4 \end{bmatrix}$ $\begin{bmatrix} 2 \\ 14 \end{bmatrix}$

1X2 + 0X14 =2+0=2

2X2 + 4X14 = 4 + 56=60 mod 26 =8

$\begin{bmatrix} 1 & 0 \\ 2 & 4 \end{bmatrix}$ $\begin{bmatrix} 12 \\ 15 \end{bmatrix}$

12X1 + 0X15 = 12 + 0 =12

12X2 + 4X15 = 24 + 60 = 84 mod 26 =6

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Now we get numbers as

$$\begin{bmatrix} 2 & 12 \\ 8 & 06 \end{bmatrix}$$

- Convert it into letters

$$\begin{bmatrix} C & M \\ I & G \end{bmatrix}$$

- Final cipher text is CIMG

- Solve using Hill Cipher:
  - Encrypt the plaintext message "PIET" using the keyword “hill” and a 2 x 2 matrix.
  - Cipher Text = NTYT

5) Polyalphabetic Cipher

- A poly-alphabetic cipher is any cipher based on substitution, using several substitution alphabets.
- In polyalphabetic substitution ciphers, the plaintext letters are enciphered differently based upon their installation in the text.
- Rather than being a one-to-one correspondence, there is a one-to-many relationship between each letter and its substitutes.
- For example, ‘a’ can be enciphered as ‘d’ in the starting of the text, but as ‘n’ at the middle.
- The polyalphabetic ciphers have the benefit of hiding the letter frequency of the basic language.
- Therefore attacker cannot use single letter frequency statistic to break the ciphertext.

6) Vigenere cipher

- The best known and one of the simplest, polyalphabetic ciphers.
- The set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25.
- Each cipher is denoted by a key letter, which is the ciphertext letter that substitutes for the plaintext letter ‘a’.
- For performing the encryption and decryption, a matrix known as the Vigenere table is constructed

KEY

Plaintext

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	D
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	C
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	B
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

6) Vigenere cipher

- Each of the 26 ciphers is laid out horizontally, with the key letter for each cipher to its left vertically.
- A normal alphabet for the plaintext runs across the top.
- The process of encryption is simple: Given a key letter x and a plaintext letter y, the ciphertext letter is at the intersection of the row labeled x and the column labeled y; in this case the ciphertext is ‘V’.
- To encrypt a message, a key is needed that is as long as the message.
- Usually, the key is a repeating keyword.
- For example, if the keyword is deceptive, the message "we are discovered save yourself" is encrypted as follows:

```
key:          deceptivedeceptivedeceptive
plaintext:    wearediscoveredsaveyourself
ciphertext:   ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

t y c o t y c o -key
c o m p u t e r -pt

6) Vigenere cipher

- Decryption is equally simple.
- The key letter indicates the row.
- The position of the ciphertext letter in that row determines the column, and the plaintext letter is at the top of that column.
- The strength of this cipher is that there are multiple ciphertext letters for each plaintext letter, one for each unique letter of the keyword.
- Thus, the letter frequency information is almost concealed.

- **Evaluate the ciphertext from the plaintext using Vigenere cipher.**
  - Plain Text : **TO BE OR NOT TO BE**
  - Keyword: **Relations**
  - Cipher Text: KS ME HZ BBL KS ME
- **Apply the Vigenere cipher to find the ciphertext from the given plaintext.**
  - Plain text : COMPUTER
  - Keyword: TYCO
  - Ciphertext = **VM OD NR GF**

7) Vernam cipher

- The ultimate defense against such a cryptanalysis is to choose a keyword that is as long as the plaintext and has no statistical relationship to it.
- System works on binary data (bits) rather than letters.
- The system can be expressed as follows

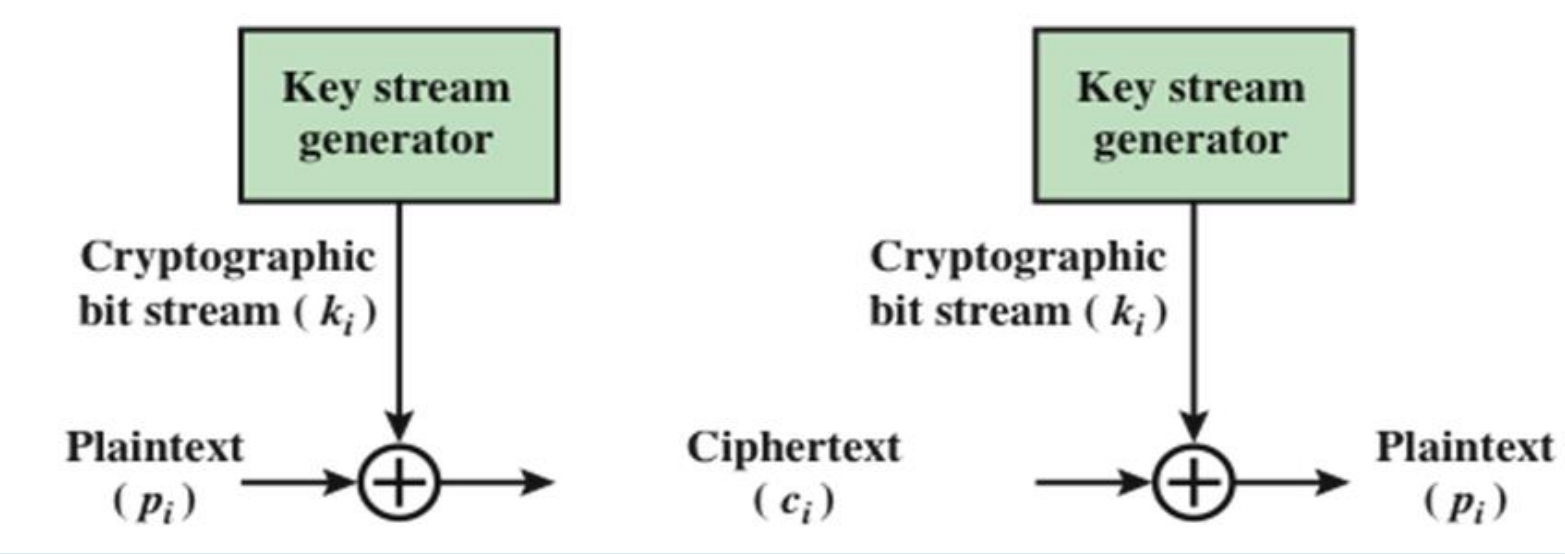
$$c_i = p_i \oplus k_i$$

- where
- *pi* = *i*th binary digit of plaintext
- *ki* = *i*th binary digit of key
- *ci* = *i*th binary digit of ciphertext
- $\oplus$ = exclusive-or (XOR) operation

7) Vernam cipher

- Thus, the ciphertext is generated by performing the bitwise XOR of the plaintext and the key.
- Because of the properties of the XOR, decryption simply involves the same bitwise operation:

$$p_i = c_i \oplus k_i$$



Example:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Plain-Text: O A K Key: S O N
  - O ==> 14 = 0 1 1 1 0
  - S ==> 18 = 1 0 0 1 0
- Bitwise XOR Result: 1 1 1 0 0 = 28
- Since the resulting number is greater than 26, subtract 26 from it.
- Then convert the Cipher-Text character number to the Cipher-Text character.
  - 28 - 26 = 2 ==> C
  - CIPHER-TEXT: C

X-OR

0 0 = 0
0 1 = 1
1 0 = 1
1 1 = 0

- Similarly, do the same for the other corresponding characters,
  - PT: O A K KEY: S O N
  - NO: 14 00 10 NO: 18 14 13
- New Cipher-Text is after getting the corresponding character from the resulting number.
- Cipher Text -NO: 02 14 07
- Cipher Text : **C O H**

- Evaluate the ciphertext from plaintext using the Vernam cipher where plaintext : **COMP** Use Key as : **TYCO**
- Ciphertext = **RWOB**

8) ONE – TIME PAD

- An improvement to the Vignere cipher that yields the ultimate security.
- It uses a random key that is as long as the message, so that the key need not be repeated.
- The key is used to encrypt and decrypt a single message, and then is discarded.
- Each new message requires a new key of the same length as the new message.
- Such a scheme, known as a one-time pad is considered to be unbreakable.
- It produces random output that bears no statistical relationship to the plaintext.
- Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code.

8) ONE – TIME PAD

- If the key is truly random the cipherext will also be random.
- Hence there won't be any patterns or regularities in the ciphertext.
- This makes the code simply unbreakable.
- Two limitations in the implementation of one-time pad is :
  - Practical difficulty in the generation of large number of random keys
  - Distribution and protection of this keys
- Because of these difficulties, the one-time pad is of limited utility and is useful primarily for low-bandwidth channels requiring very high security.
- The one-time pad is the only cryptosystem that exhibits what is referred to as perfect secrecy

TRANSPOSITION TECHNIQUES

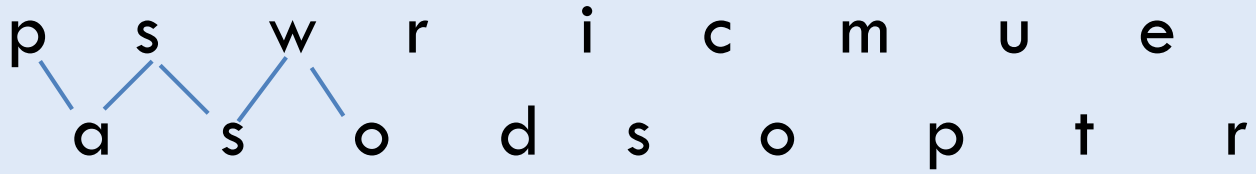
- A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters.
- This technique is referred to as a transposition cipher.
- Transposition Cipher is a cryptographic algorithm where the order of alphabets in the plaintext is rearranged to form a cipher text.
- They perform some permutations over the plain text alphabets.

Plain text: C O M P

Cipher Text: M P O C

Rail Fence Cipher

- The simplest such cipher is the **rail fence** technique, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.
- For example, to encipher the message "password is computer" with a rail fence of depth 2, we write the following:



- The encrypted message is
- PSWRICMUEASODSOPTR

Row Transposition Cipher/Simple Columnar Transposition

- In this method the message is written in rows of fixed length and then read out column by column.
- Column are selected in some scrambled order.
- The number of columns are defined by the length of key.

Algorithm:

- Write the plain text message row by row in a rectangle of predefined size.(length of key)
- Read the message column by column according to the selected order thus obtained message is a cipher text.

Row Transposition Cipher/Simple Columnar Transposition

plain text: welcome home

Order : 6 3 2 4 1 5

1	2	3	4	5	6
W	E	L	C	O	M
E	H	O	M	E	

Cipher text: MLOEHCMWEOE

- Convert plain text to cipher text using rail Fence technique. Plaintext = “INFORMATION SECURITY” use depth =3
  - Ciphertext : **IRIEINOMTOSCRTFANUY**
- Solve using Row Transposition :
  - **Example:** Plain Text: — **“Come Home Tomorrow”**
  - **Keyword: 6,4,3,1,5,2**
  - Cipher text = **OO EOW MTO CMR HM OER**

Steganography

- Steganography means covered of hidden writing.
- Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message.
- The word steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphein meaning "writing".
- "Steganography means hiding one piece of data within another".

Steganography

- The goal of steganography is to hide the data from a third person where as the goal of cryptography is to make data unreadable to a third person.
- It is often combined with cryptography so that even if the message is discovered it cannot be read.
- Historical steganography involves techniques such disappearing ink or microdots while modern steganography involves hiding data in computer files.
- The message can be hidden in text, image, audio or video file.

Steganography

- Various other techniques have been used historically; some examples are:
  - **Character marking:** Selected letters of printed text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held at an angle to bright light.
  - **Invisible ink:** A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.
  - **Pin punctures:** Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light.

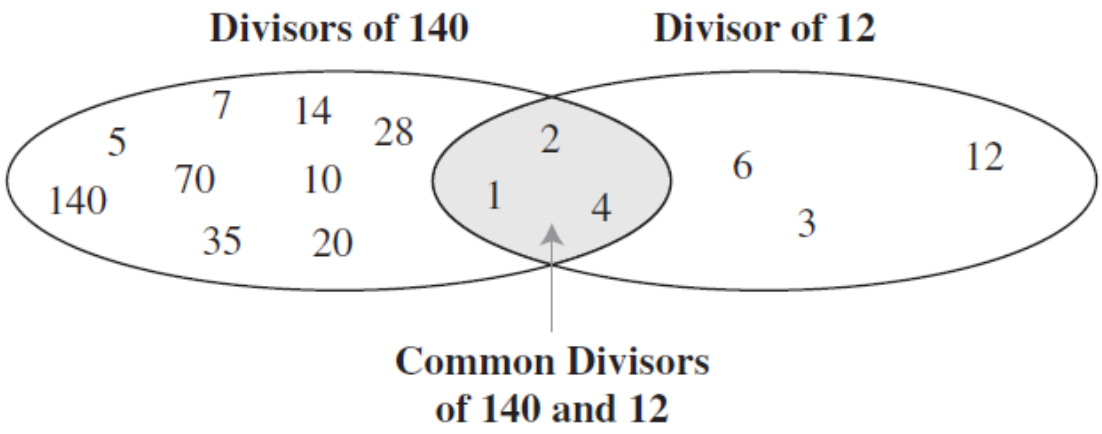
Quotient Remainder Theorem:

- It states that, for any pair of integers a and b (b is positive), there exist two unique integers q and r such that $a = b \times q + r$ where $0 <= r < b$
- In this relation, a is called the dividend; q, the quotient; b, the divisor; and r, the remainder.
- Suppose 7/2 we get q=3,r=1,a=7 and b=2
- So we can write
  - a=bxq+r
  - 7=2*3+1

Greatest Common divisor (GCD)

- One integer often needed in cryptography is the **greatest common divisor** of two positive integers.
- Two positive integers may have many common divisors, but only one greatest common divisor.
- For example, the common divisors of 12 and 140 are 1, 2, and 4.
- However, the greatest common divisor is 4.

Common divisors of two integers



How to Calculate GCD

- 1) 12,140

	12	140
2	6	70
2	3	35

GCD = 2x2=4

2) 13 31

1	13	31
	13	31

GCD = 1

3) 12 33

3	12	33
	4	11

GCD = 3

4) 25 150

	25	150
5	5	30
5	1	6

GCD = 5x5 = 25

Euclidean/Euclid Algorithm

- Finding the greatest common divisor (gcd) of two positive integers by listing all common divisors is not practical when the two integers are large.
- Fortunately, a mathematician named Euclid developed an algorithm that can find the greatest common divisor of two positive integers.
- 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

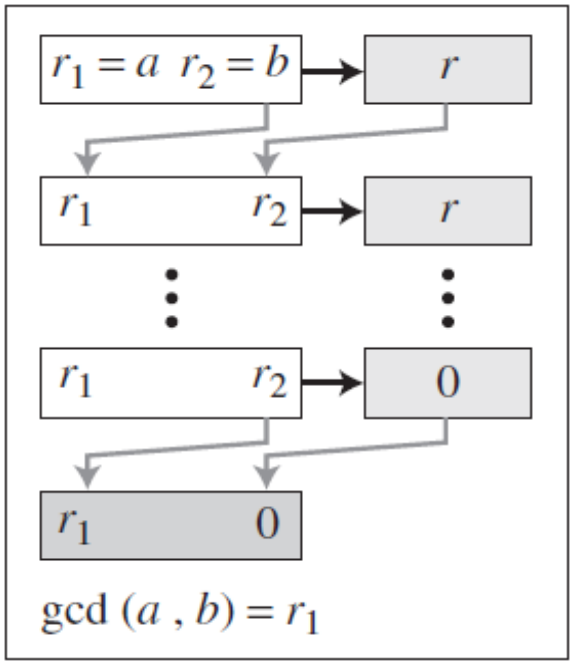
Euclidean Algorithm

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

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

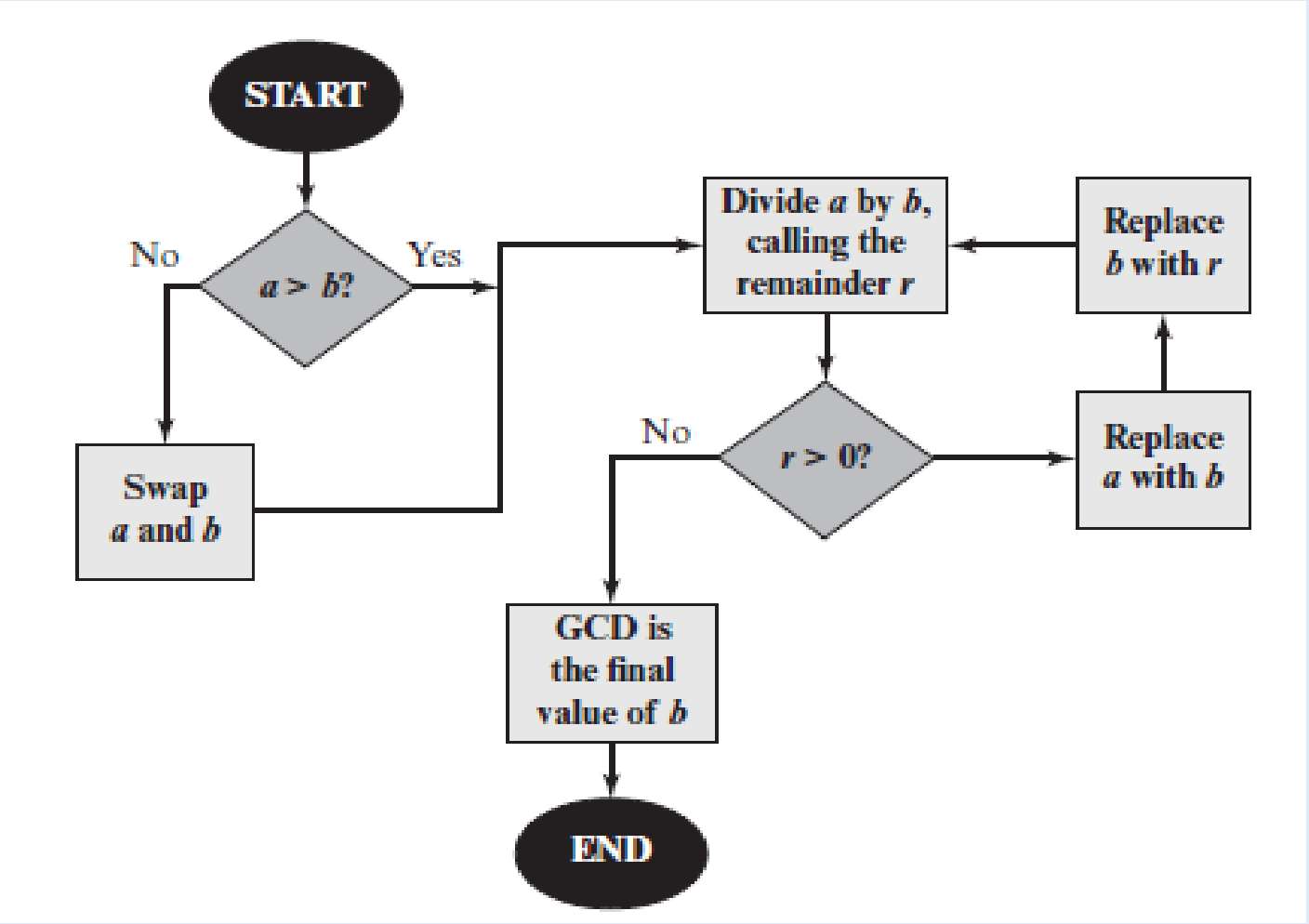
- In other words, gcd (36, 10) = 2, gcd (10, 6) = 2, and so on.
- This means that instead of calculating gcd (36, 10), we can find gcd (2, 0).

- Figure shows how the above two facts are used to calculate gcd (*a*, *b*).



- We use two variables, *r*1 and *r*2, 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
- *r*1 divided by *r*2 and store the result in the variable *r*. We then replace *r*1 by *r*2 and *r*2 by *r*.
- The steps are continued until *r*2 becomes 0. At this moment, we stop. The gcd (*a*, *b*) is *r*1.
- **When gcd (*a*, *b*) = 1, we say that *a* and *b* are relatively prime.**

Euclidean Algorithm



Example

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	

- Find the greatest common divisor of 2740 and 1760.
- We apply the above procedure using a table. We initialize $r1$ to 2740 and $r2$ to 1760.
- We have also shown the value of q in each step. We have gcd (2740, 1760) = 20.

Example

- Find the greatest common divisor of 25 and 60.
- We immediately get our correct ordering. We have gcd (25, 60) = 5.

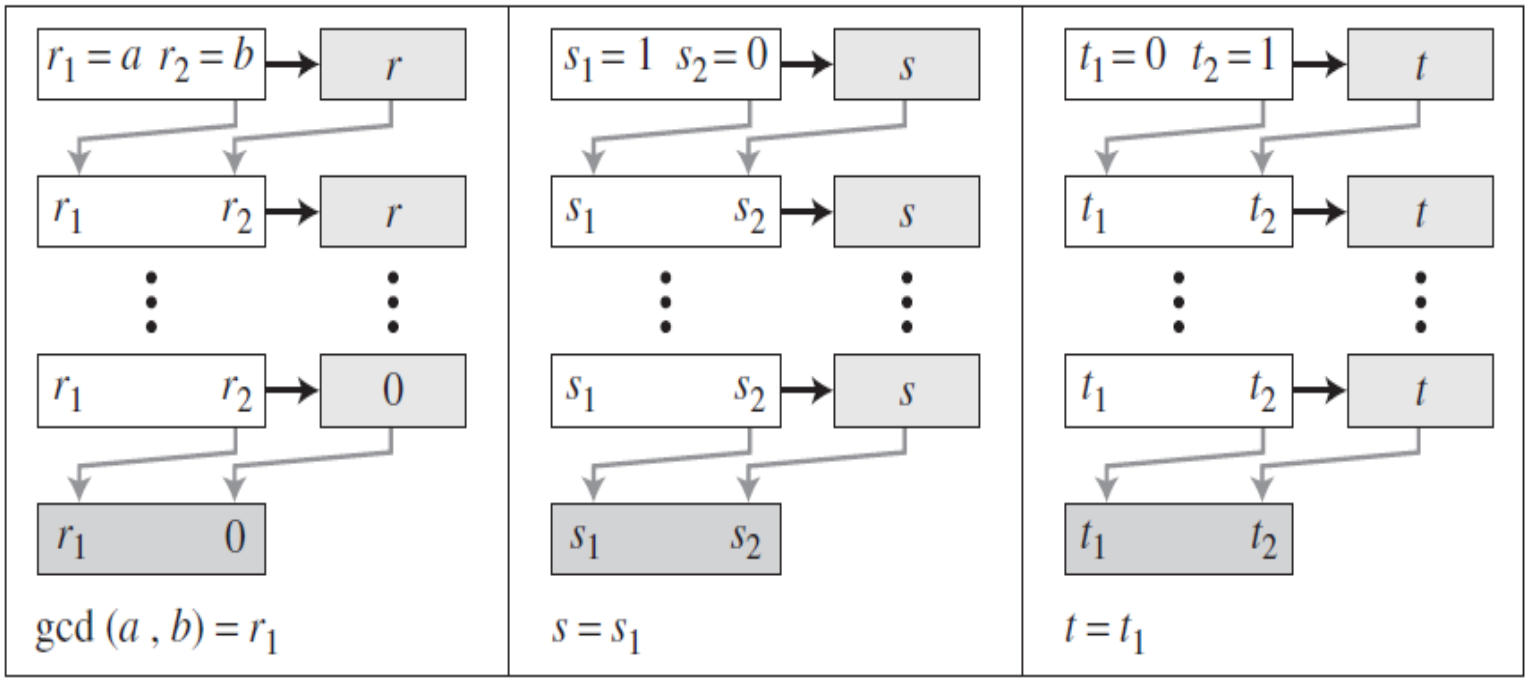
q	r_1	r_2	r
0	25	60	25
2	60	25	10
2	25	10	5
2	10	5	0
	5	0	

The Extended Euclidean Algorithm

- *Extended Euclidean algorithm also finds integer coefficients s and t such that: as + bt = gcd(a, b)*
- 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*.
- The algorithm and the process is shown in Figure.

The Extended Euclidean Algorithm

- As shown in Figure, the extended Euclidean algorithm uses the same number of steps as the Euclidean algorithm.
- However, in each step, we use three sets of calculations and exchanges instead of one.
- The algorithm uses three sets of variables, *r*'s, *s*'s, and *t*'s



The Extended Euclidean Algorithm

- In each step, $r1$, $r2$, and r have the same values in the Euclidean algorithm.
- The variables $r1$ and $r2$ are initialized to the values of a and b, respectively.
- The variables $s1$ and $s2$ are initialized to 1 and 0, respectively.
- The variables $t1$ and $t2$ are initialized to 0 and 1, respectively.
- The calculations of r, s, and t are similar, with one warning.
- Although r is the remainder of dividing $r1$ by $r2$, there is no such relationship between the other two sets.
- There is only one quotient, q, which is calculated as $r1 \mid r2$ and used for the other two calculations.

Example

- Given $a = 161$ and $b = 28$, find gcd (a, b) and the values of s and t.
  - $r = r1 - q \times r2$ $\quad s = s1 - q \times s2$ $\quad t = t1 - q \times t2$

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 **$s \times a + t \times b = \gcd(a, b)$**
  - $(-1) \times 161 + 6 \times 28 = 7$

MODULAR ARITHMETIC

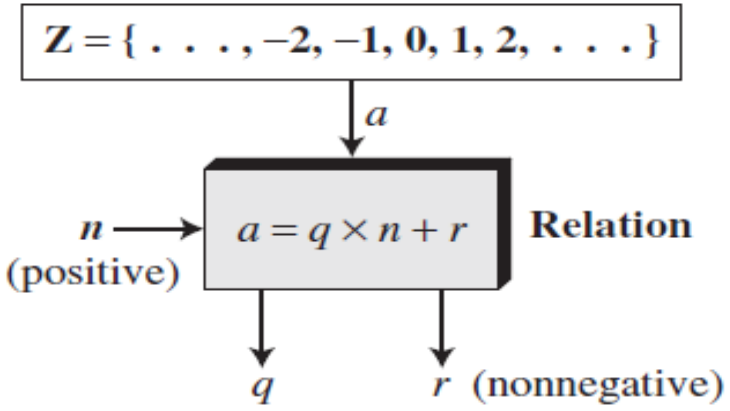
- When we divide two integers we will have an equation that looks like the following:

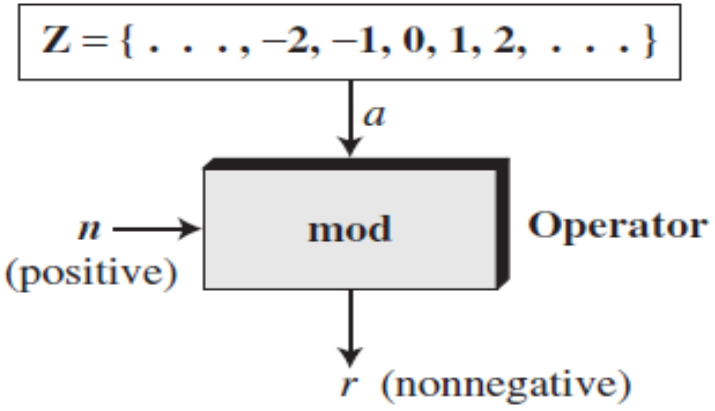
  $$a/n = q \text{ and remainder } r$$

  - a is the dividend, n is the divisor, q is the quotient and r is the remainder
- Sometimes, we are only interested in what the **remainder** is when we divide a by n
- For these cases there is an operator called the modulo operator (abbreviated as mod).
- Using the same a, n, q, and r as above, we would have: a mod n= r
- We would say this as a *modulo* n *is equal to r*. Where n is referred to as the **modulus** and r is called residue.

MODULAR ARITHMETIC

- Fig. 1 shows the division relation compared with the modulo operator.
- Fig. 2 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***





- Find the result of the following operations:
- a. 27 mod 5
  - We are looking for the residue r. We can divide the a by n and find q and r.
  - We can then disregard q and keep r.
  - Dividing 27 by 5 results in $r = 2$. This means that 27 mod 5 = 2.
- b. 36 mod 12
  - Dividing 36 by 12 results in $r = 0$. This means that 36 mod 12 = 0.
- c. −18 mod 14
  - 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.
- d. −7 mod 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.

Congruence

- If n is a positive integer, we say the integers a and b are congruent modulo n , and write a≡ b(mod n), if they have the same remainder on division by n.
- or equivalently if a − b is divisible by n
- 5 ≡ 17 mod 3 (since 5 and 17 both have remainder 2 when divided by 3, or equivalently, since 17 − 5 = 12 is divisible by 3).
- 10 ≡ −4 mod 7 (since 10 − (−4) = 14 is divisible by 7)

Properties of Congruences

- Congruences have the following properties:
  1. $a \equiv b \pmod{n}$ if $n \mid (a - b)$ *that is* *n divides (a-b)*
  2. $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$
  3. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply $a \equiv c \pmod{n}$

Modular Arithmetic Properties

- Modular arithmetic exhibits the following properties:
  1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
  2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
  3. $[(a \bmod n) * (b \bmod n)] \bmod n = (a * b) \bmod n$

$11 \bmod 8 = 3;\ 15 \bmod 8 = 7$

$[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 = 10 \bmod 8 = 2$

$(11 + 15) \bmod 8 = 26 \bmod 8 = 2$

$[(11 \bmod 8) - (15 \bmod 8)] \bmod 8 = -4 \bmod 8 = 4$

$(11 - 15) \bmod 8 = -4 \bmod 8 = 4$

$[(11 \bmod 8) * (15 \bmod 8)] \bmod 8 = 21 \bmod 8 = 5$

$(11 * 15) \bmod 8 = 165 \bmod 8 = 5$

Modular Arithmetic

- 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 can say that the modulo operation creates a set, which in modular arithmetic is referred to as the set of least residues modulo n, or Zn
- Properties of Modular Arithmetic for Integers in Z_n

Property	Expression
Commutative Laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Associative Laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive Law	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$

Prime Numbers

- A positive integer is a prime if and only if it is exactly divisible by two integers, 1 and itself.
- **Prime numbers** play a critical role in number theory.
- Eg: 5 divisible by 1 and 5
- Any integer $a > 1$ can be factored in a unique way as:

$$a = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_t^{a_t}$$

- $36 = 2^2 \times 3^3$
- where $p_1 < p_2 < \ldots < p_t$ are prime numbers and where each a_i is a positive integer.
- This is known as the fundamental theorem of arithmetic.

Relatively Prime/Co-prime

- a and b are said to be relatively prime or co-prime if a and b does not have common factors.
- That is gcd (a, b)=1 then a and b are relative prime.
- E.g a=15 and b=28
- Factors of a= 1, 3, 5
- Factors of b = 1, 2, 4, 7,14
- The above factors of 15 and 28 does not contain common factor.
- So a and b are relative prime.

Fermat's Theorem/ Fermat's little theorem

- Fermat's little theorem plays a very important role in number theory and cryptography.
- It state that if p is a prime number and 'a' is any +ve integer not divisible by p, (gcd(a,p)=1) then

$$a^{p-1} \equiv 1 \bmod p.$$

$$\text{or} \quad a^p / a \equiv 1 \bmod p.$$

$$a^p \equiv a \bmod p.$$

  - E.g. 1) To calculate $5^{18} \bmod 19$
  - gcd(5,19)=1
  - **by $a^{p-1} \equiv 1 \bmod p$.** We get $5^{19-1} \equiv 1 \bmod 19$
  - That is $5^{19-1} \bmod 19 \equiv 1 \bmod 19$
  - Therefore **$5^{19-1} \bmod 19 = 1$**

Fermat's Theorem/ Fermat's little theorem

- Fermat's little theorem sometimes is helpful for quickly finding a solution to some exponentiations.
  - **E.g. 2) To calculate 5^{19}mod 19**
  - gcd(5,19)=1
  - **by $a^p \equiv a \bmod p$.** We get $5^{19} = 5 \bmod 19$
  - that is : $5^{19} \bmod 19 \equiv 5 \bmod 19 = 5$
  - **E.g. 3) To calculate 5^{20}mod 19 (a=5,p=19)**
  - $a^{p-1} \equiv 1 \bmod p$ that is $5^{19-1} \equiv 5 \bmod 19$
  - $5^{18} \times 5^2 \equiv 1 \times 5^2 \bmod 19$
  - $5^{18+2} \equiv 25 \bmod 19$
  - $5^{20} \equiv 25 \bmod 19 \equiv 6 \bmod 19$
  - **5^{20}mod 19 = 6**

Euler's Totient Function

- Euler's Phi function $\phi(n)$ is sometimes called **Euler's Totient Function** plays a very important role in cryptography.
- This function is denoted by $\phi(n)$ where n>=1 is defined as the set of number of positive integers less than *n* and relatively prime to *n*. (that is GCD =1)
  - $\phi(5) = \{1, 2, 3, 4\} = 4$ (No of elements)
  - co-prime = gcd of (5,1) , (5,2), (5,3), (5,4) =1
  - $\phi(6) = \{1, 5\} = 2$
  - As GCD (6,1) =1, (6,2) =2, (6,3) = 3, (6,4) = 2, (6,5) = 1
- By convention, $\phi(1) = 1$.
- **Case 1:** When n is a prime number ,

  $\phi(p) = p - 1$

  $\phi(23) = 23 - 1 = 22$

Euler's Totient Function

- **Case 2:** Now suppose that we have two prime numbers p and q with $p \neq q$.
- Then we can show that, for $n = pq$,

  $\phi(n) = \phi(p*q) = \phi(p) * \phi(q) = (p - 1) * (q - 1)$
- Euler's theorem **underlies the RSA cryptosystem, which is widely used in Internet communications.**
- Euler's theorem allows us to convert complex problems into simpler, computationally less expensive problems.

$$\phi(21) = \phi(3) \times \phi(7) = (3 - 1) \times (7 - 1) = 2 \times 6 = 12$$

where the 12 integers are $\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$.

Euler's Theorem

- Euler's theorem states that for every *a* and *n* that are relatively prime (GCD (a , n)=1): then we can write

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

- Where ø(n) Euler's totient function, which counts the number of positive integers less than n that are relatively prime to n.
- Consider the set of such integers, labeled as
- $R = \{x_1, x_2, \ldots\ldots\ldots, x_{\phi(n)}\}$
- Now multiply each element by *a* and modulo *n*:
- $S = \{(ax_1 \bmod n), (ax_2 \bmod n), \ldots\ldots\ldots, (ax_{\phi(n)} \bmod n)\}$

Euler's Theorem

- Now by observation we can say that set *S* is a permutations of *R* , by the following line of reasoning:
  - **1.** Because *a* is relatively prime to *n* and x_i is relatively prime to *n*,
  - *Then* ax_i must also be relatively prime to *n*. Thus, all the members of *S* are integers that are less than *n* and that are relatively prime to *n*.
- Therefore, equation of Set S = Set R
- $S = \{(ax_1 \bmod n), (ax_2 \bmod n), \ldots\ldots\ldots, (ax_{\phi(n)} \bmod n)\}$
- $R = \{x_1, x_2, \ldots\ldots\ldots, x_{\phi(n)}\}$

$$\prod_{i=1}^{\phi(n)} (ax_i \bmod n) = \prod_{i=1}^{\phi(n)} x_i$$

$$\prod_{i=1}^{\phi(n)} ax_i = \prod_{i=1}^{\phi(n)} x_i \pmod n$$

$$a^{\phi(n)} \times \left[\prod_{i=1}^{\phi(n)} x_i\right] = \prod_{i=1}^{\phi(n)} x_i \pmod n$$

$$a^{\phi(n)} = 1 \pmod n$$

THE CHINESE REMAINDER THEOREM

- The Chinese remainder theorem states that, if one knows the remainders of the division of an integer n by several integers, then one can determine uniquely the remainder of the division of n by the product of these integers, under the condition that the divisors are pairwise coprime.
- The Chinese remainder theorem is widely used for computing with large integers.

- The Chinese remainder theorem (CRT) is used to solve a set of congruent equations with one variable but different moduli, which are relatively prime, as shown below:

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\cdots$$
$$x \equiv a_k \pmod{m_k}$$

- The Chinese remainder theorem states that the above equations have a unique solution if the moduli are relatively prime.

Statement

- Let $m_1, m_2,...,m_k$ be integers with $\gcd(m_i, m_j)=1$ where i != j.
- Let M be the product $M = m_1 m_2 \ldots\ldots m_k$.
- Let $a_1,a_2...,a_k$ be integers.
- Consider the system of congruences:
- $x \equiv a_1 \pmod{m_1}$
- $x \equiv a_2 \pmod{m_2}$
- ……
- $x \equiv a_k \pmod{m_k}$.
- Then there exists exactly one $x \in Z_m$ satisfying this system.
- Formula to find x:

$$x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + ... + a_k \times M_k \times M_k^{-1}) \bmod M$$

THE CHINESE REMAINDER THEOREM

- Example: Solve the following example using Chinese remainder theorem:
  - $X \equiv 2 \pmod 3$
  - $X \equiv 3 \pmod 5$
  - $X \equiv 2 \pmod 7$

  Solution:

  Formula =

  $x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \text{ Mod } M$

  $a_1 = 2 , a_2 = 3 , a_3 = 2$

  $m_1 = 3, m_2 = 5, m_3 = 7$

- $M = m_1 \times m_2 \times m_3 = 3 \times 5 \times 7 = 105$
- $M_1 = M / m_1 = 105/3 = 35$
- $M_2 = M / m_2 = 105/5 = 21$
- $M_3 = M / m_3 = 105/7 = 15$
- $M_1 \times M_1^{-1} = 1 \bmod m_1 = 35 \times M_1^{-1} = 1 \bmod 3$ put $M_1^{-1} = 1,2,3$ to satisfy condition. So 2 satisfies condition as $35 \times (2) = 1 \bmod 3$
- $M_1^{-1} = 2$
- $M_2 \times M_2^{-1} = 1 \bmod m_2$ so $M_2^{-1} = 1$
- $M_3 \times M_3^{-1} = 1 \bmod m_3$ so $M_3^{-1} = 1$
- $x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$
- $x = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105$
- $= (140 + 63 + 30) \bmod 105 = 233 \bmod 105 = 23$

Groups, rings, and fields

- Groups, rings, and fields are the fundamental elements of a branch of mathematics known as abstract algebra, or modern algebra.
- In abstract algebra, we are concerned with sets on whose elements we can operate algebraically;
- that is, we can combine two elements of the set, perhaps in several ways, to obtain a third element of the set.
- These operations are subject to specific rules, which define the nature of the set

Groups

- A **group** G, sometimes denoted by {G, • }, is a set of elements with a binary operation denoted by • such that it satisfies following CAIN properties:
  - (A1) Closure:
    - If *a* and *b* belong to G, then *a* • *b* is also in G
  - (A2) Associative:
    - *a* • (*b* • c) = (*a* • *b*) • c for all *a*, *b*, c in G
  - (A3) Identity element:
    - There is an element e in G such that *a* • e = e • *a* = *a* for all *a* in G
  - (A4) Inverse element:
    - For each *a* in G, there is an element *a* in G such that *a*•*a*' = *a*' • *a* = e

Groups

- If a group has a finite number of elements, it is referred to as a **finite group**, and the **order** of the group is equal to the number of elements in the group.
- Otherwise, the group is an **infinite group**.

Abelian Group

- A group is said to be **abelian** if it already a group and satisfies the following additional condition:
  - (A5) Commutative:
    - $a \bullet b = b \bullet a$ for all a, b in G

Example

Question: Is (Z, +) a group?

Solution:

Z = { ...., -3, -2, -1, 0, 1, 2, 3, ...}

CAIN Property	Explanation	Satisfied?
Closure	If a, b ∈ G, then (a • b) ∈ G. If a = 5, b = -2 ∈ Z then (a + b) = -3 ∈ Z	✓
Associative	a • (b • c) = (a • b) • c for all a, b, c ∈ G. 5 + (3 + 7) = (5 + 3) + 7 ∈ Z	✓
Identity element	(a • e) = (e • a) = a for all a ∈ G. (5 + 0) = (0 + 5) = 5 for all a ∈ G.	✓
Inverse element	(a • a') = (a' • a) = e for all a, a' ∈ G. (5 + -5) = (-5 + 5) = 0 for all 5, -5 ∈ Z	✓
Commutative	(a • b) = (b • a) for all a, b ∈ G. (5 + 9) = (9 + 5) for all 9, 5 ∈ Z.	✓

e is identity element

Cyclic Group

- A Group <G,*> is said to be cyclic group if it contains at least one generator element.
- A Group <G,*> is called Cyclic if 'a' belongs to G and integral powers of 'a' that is $\{a^1, a^2, a^3 \ldots\ldots\ldots a^n\}$ generates all elements of Group G.
- Then element 'a' is called Generating Element.
- A cyclic group is always abelian and may be finite or infinite.

Ring

- A ring R denoted by {R , + , * }, is a set of elements with two binary operations, called addition and multiplication, such that for all a , b , c in R the following properties are obeyed:
- Group (A1-A4), Abelian Group (A5)
- (M1) Closure under multiplication:
  - If a and b belong to R , then ab is also in R
- (M2) Associativity of multiplication:
  - a (bc) = (ab)c for all a , b , c in R
- (M3) Distributive laws:
  - a (b + c) = ab + ac for all a , b , c in R
  - (a + b)c = ac + bc for all a , b , c in R
- In essence, a ring is a set in which we can do addition, subtraction and multiplication

Note: Substraction can be done as [a - b = a + (-b)]

Ring

- A ring is said to be commutative if it satisfies the following additional condition:
- (M4) Commutativity of multiplication:
  - ab = ba for all a, b in R
- An integral domain is a commutative ring that obeys the following.
- (M5) Multiplicative identity:
  - There is an element 1 in R such that a1 = 1a = a for all a in R
- (M6) No zero divisors:
  - If a , b in R and ab = 0, then either a = 0 or b = 0

FIELDS

- A field F , sometimes denoted by {F, +,* }, is a set of elements with two binary operations, called addition and multiplication, such that for all a, b, c in F the following axioms are obeyed:
- (A1–M6)
  - F is an integral domain; that is, F satisfies axioms A1 through A5 and M1 through M6
- (M7) Multiplicative inverse:
  - For each a in F, except 0, there is an element a^{-1} in F such that
  - $aa^{-1} = (a^{-1})a = 1$
- In essence, a field is a set in which we can do addition, subtraction, multiplication, and division without leaving the set.
- Division is defined with the following rule: $a / b = a (b^{-1})$

Finite Fields

- A finite field, a field with a finite number of elements, are very important structures in cryptography.
- Galois showed that for a field to be finite, the number of elements should be p^n, where p is a prime and n is a positive integer.
- The finite fields are usually called Galois fields and denoted as GF(p^n).
- As with any field, a finite field is a set on which the operations of Addition, Multiplication, Substraction and division are defined and satisfy certain basic rules.
- The most common example of finite fields are given by integers (mod p) when p is a prime number.

- What are the basic security goals. Explain various threats to basic security goals.(5 marks)
- What are ITU-T(X.800) recommended security mechanism. Explain any three of them.(5 Marks)
- Prove using Playfair Encryprion and Decryption techniques works for plaintext-"instrument" using key as "MONARCHY". (10 Marks)
- Evaluate the ciphertext from plaintext using the Vernam cipher where plaintext : **COMP** Use Key as : **TYCO**
- Evaluate the ciphertext from the plaintext using Vigenere cipher.
  - Plain Text : **TO BE OR NOT TO BE**
  - Keyword: **Relations**
- Describe the encryption process of simple columnar transposition ipher. Include the steps involved and perform encryption using plaintext : **THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG,** Key = **COLUMN (ignore space)**

Assignment No 1

1) Convert the Plain text "COMPUTER SECURITY" using Caesar cipher.

2) Solve the following Example using PlaYfair cipher:

- 1) Key = THIRDCO, Plaintext = COMPUTER
- 2) Key = PLAYFAIR EXAMPLE

  Plaintext = hide gold in tree stump

3) Solve using Hill Cipher:

- Encrypt the plaintext message "PIET" using the keyword "hill" and a 2 x 2 matrix.

Assignment no 1:

4) Solve using Row Transposition :

- **Example:** Plain Text: — **"Come Home Tomorrow"**
- **Keyword: 6,4,3,1,5,2**

5) Convert plain text to cipher text using rail Fence technique "INFORMATION SECURITY"

Assignment no 1

6) Find GCD of Following using Euclidean Algorithm

- gcd(60, 24)
- gcd(1180, 482)
- gcd(270, 192)
- gcd (2740, 1760)

7) Solve following using Fermats Theorem

- 1) Find 3^{31} mod 7 Answer = (3)
- 2) Find 2^{35} mod 7 Answer = (4)
- 3) Find 128^{129} mod 17 . Answer = (9)
- 4) 2^{1000} is divided by 13. What is the remainder? (3)

Reference

- 1. William Stallings, “Cryptography and Network Security Principles and Practice”, 7th Edition, Pearson Education, June 2017.
- 2. Behrouz A. Ferouzan, “Cryptography & Network Security”, Tata Mc-Graw Hill, 2007