

What is Security ?

1. "The quality or state of being secure—to be free from danger"
2. A successful organization should have multiple layers of security in place:

- ☒ Physical security
- ☒ Personal security
- ☒ Operations security
- ☒ Communications security
- ☒ Network security
- ☒ Information security

Er Sahil
Ka
Gyan



Introduction : ISS

- ☒ Information systems security, more commonly referred to as INFOSEC, refers to the processes and methodologies involved with keeping information confidential, available, and assuring its integrity.
It also refers to:
- ☒ Access controls, which prevent unauthorized personnel from entering or accessing a system.
- ☒ Protecting information no matter where that information is, i.e. in transit (such as in an email) or in a storage area.
- ☒ The detection and remediation of security breaches, as well as documenting those events.

- Information systems security does not just deal with computer information, but also protecting data and information in all of its forms, such as telephone conversations.
- Risk assessments must be performed to determine what information poses the biggest risk.
- For example, one system may have the most important information on it and therefore will need more security measures to maintain security. Business continuity planning and disaster recovery planning are other facets of an information systems security professional. This professional will plan for what could happen if a major business disruption occurs, but still allow business to continue as usual. INFOSEC is Combination of:

$\text{COMPUSEC} + \text{COMSEC} + \text{TEMPEST} = \text{INFOSEC}$

Where COMPUSEC is computer systems security, COMSEC is communications security, and TEMPEST is compromising emanations.



Characteristics of Information

The value of information comes from the characteristics it possesses:

- Timeliness**

No value if it is too late

- Availability**

No interference or obstruction

Required format

- Accuracy**

Free from mistakes

- Authenticity**

Quality or state of being genuine, i.e., sender of an email

- Confidentiality**

Disclosure or exposure to unauthorized individuals or system is prevented

☒ Integrity

Whole, completed, uncorrupted

Size of the file, hash values, error-correcting codes, retransmission

☒ Utility

Having value for some purpose

☒ Possession

Ownership

Breach of confidentiality results in the breach of possession, not the reverse



Components of an Information System

Information System (IS) is entire set of software, hardware, data, people, procedures, and networks necessary to use information as a resource in the organization

☒ Software

Perhaps most difficult to secure

Easy target

Exploitation substantial portion of attacks on information

☒ Hardware

Physical security policies

Securing physical location important

Laptops

Flash memory

❏ Data

Often most valuable asset

Main target of intentional attacks

❏ People

Weakest link

Social engineering

Must be well trained and informed

❏ Procedures

Threat to integrity of data

❏ Networks

Locks and keys won't work



Security Principles

- ❏ **Confidentiality** – this is the most obvious idea associated with encryption. Data is encrypted using algorithms and secret keys which are only known by the sender and receiver. This makes it hard for attackers to decrypt the message.
 - ❏ **Availability**- meaning that the assets are accessible to the authorized parties in a timely manner (as determined by the systems requirements). The failure to meet this goal is called a denial of service.
 - ❏ **Integrity** – these are the means employed to ensure a receiver gets the message which was intended for them and vice versa. Through integrity, one can ensure that no transmission has been altered or transferred message appears as it was when send.
 - ❏ **Non-repudiation** – these are measures put in place ensure the sender agrees to have sent the message, not an impersonator. This is basically a legal liability. If you agree to the message, it means that you are legally obligated. Non-repudiation can be compared to a signature on the contract.
- Authentication** is the process of making sure that the piece of data being claimed by the user belongs to it.

Security Attack

Basically Attacks are two types:

1. Theoretical Attacks-> (Also Called Active and Passive Attack) It is further divided in 4 parts:

(a) Interception (Passive) (b) Modification (Active)
(c) Fabrication (Active) (d) Interruption (Active)

2. Practical Attacks: It is Divided in 2 Parts

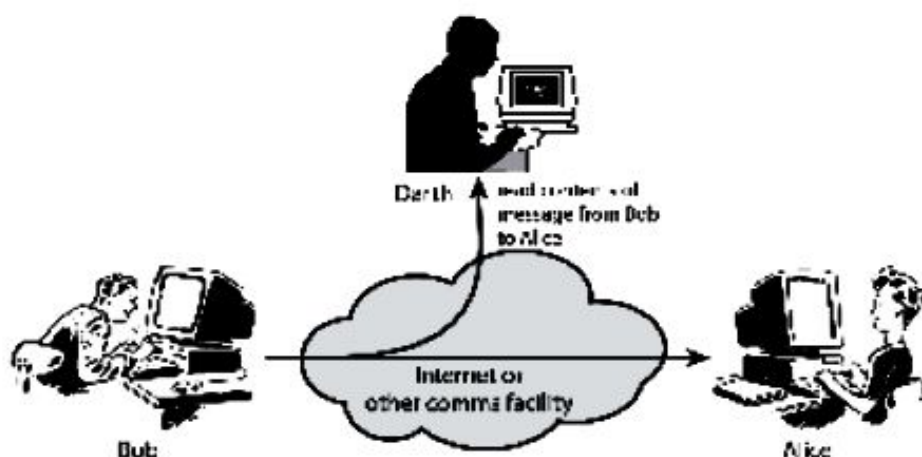
(a) Application Level Attack

(b) Network Level Attack

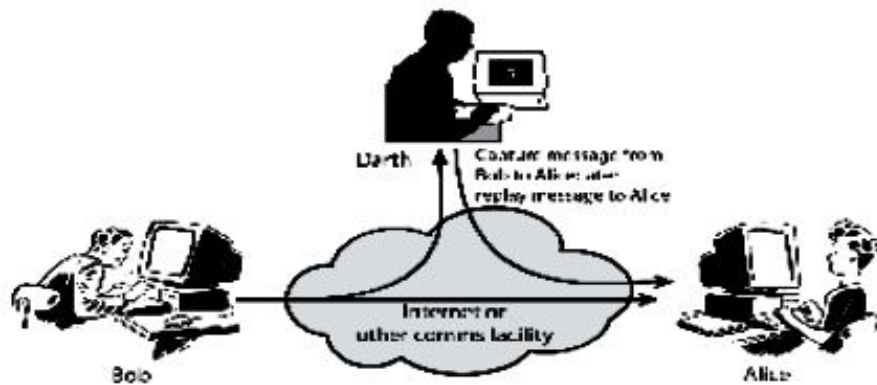


Theoretical Attacks:

Passive Attacks: The attacker observes the content of messages or copy the content of messages. Passive Attack is danger for Confidentiality. Due to passive attack, there is no any harm to the system. The most important thing is that In passive attack, Victim does not get informed about the attack.



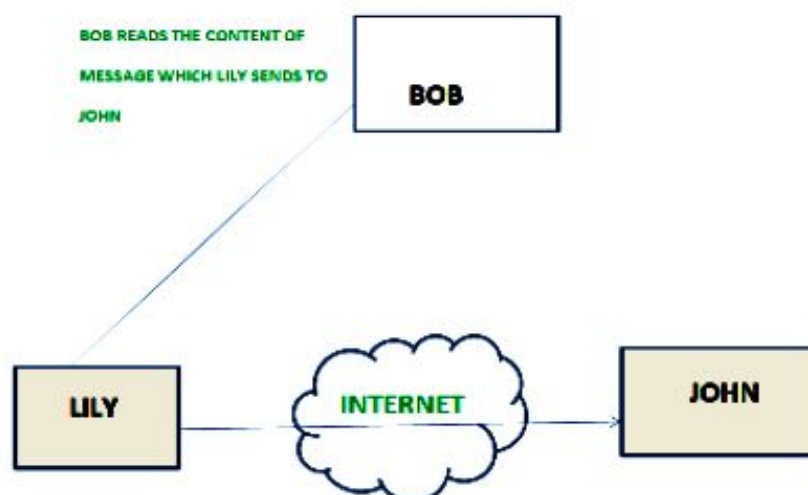
Active Attacks: The attacker efforts to change or modify the content of messages. Active Attack is danger for Integrity as well as availability. Due to active attack system is always damaged and System resources can be changed. The most important thing is that, In active attack, Victim gets informed about the attack.



Passive attacks: A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring of transmission. The goal of the opponent is to obtain information is being transmitted. Types of Passive attacks are as following:

1. The release of message content –

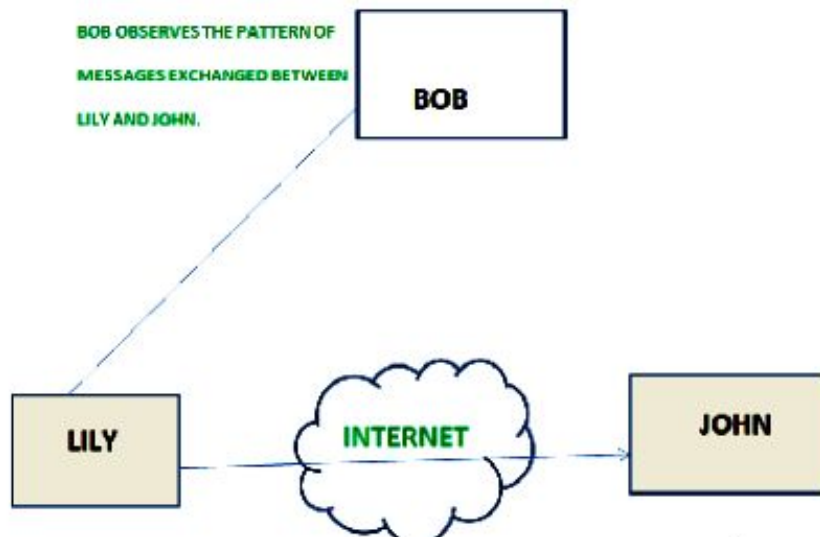
Telephonic conversation, an electronic mail message or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.



Traffic analysis –

Suppose that we had a way of masking (encryption) of information, so that the attacker even if captured the message could not extract any information from the message.

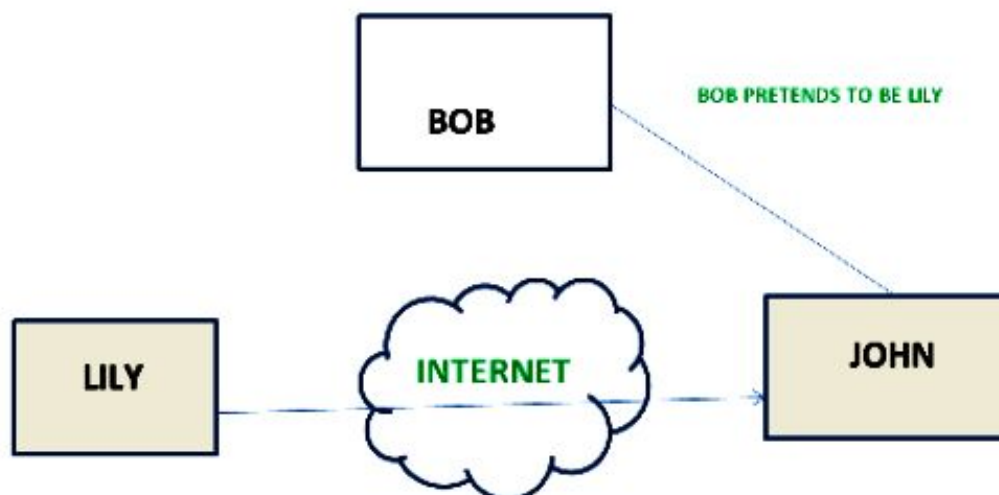
The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.



Active attacks: An Active attack attempts to alter system resources or effect their operations. Active attack involve some modification of the data stream or creation of false statement. Types of active attacks are as following:

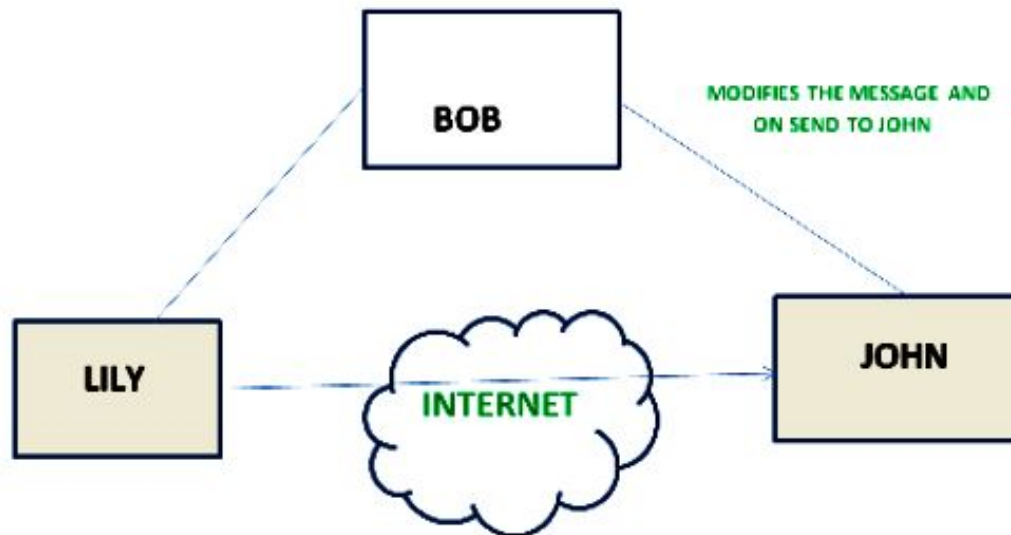
1. Masquerade –

Masquerade attack takes place when one entity pretends to be different entity. A Masquerade attack involves one of the other form of active attacks.



2. Modification of messages –

It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorised effect. For example, a message meaning "Allow JOHN to read confidential file X" is modified as "Allow Smith to read confidential file X".

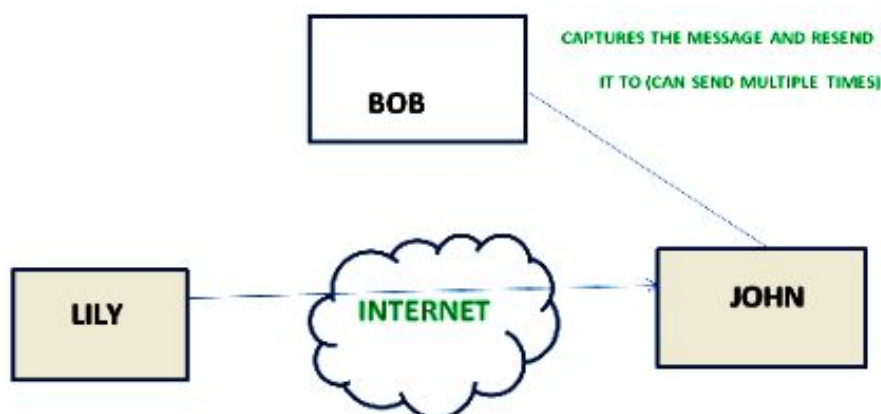


3. Repudiation –

This attack is done by either sender or receiver. The sender or receiver can deny later that he/she has send or receive a message. For example, customer ask his Bank "To transfer an amount to someone" and later on the sender(customer) deny that he had made such a request. This is repudiation.

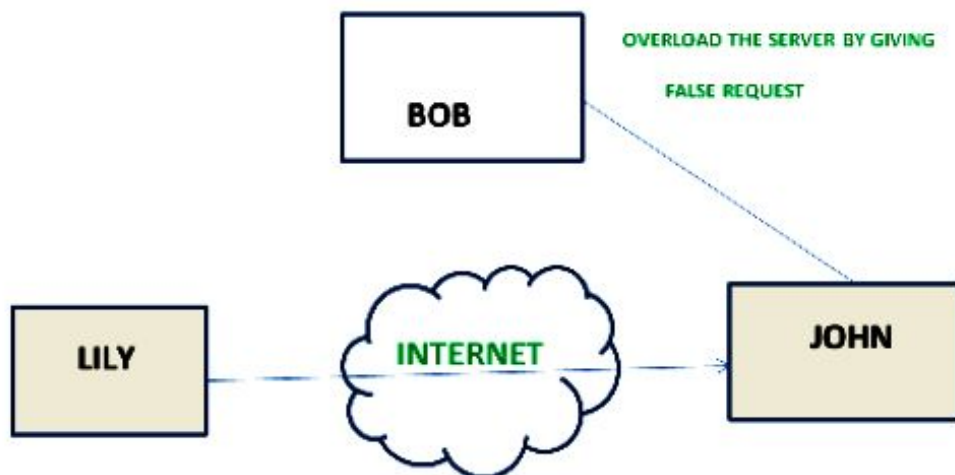
4. Replay –

It involves the passive capture of a message and its subsequent the transmission to produce an authorized effect.



5. Denial of Service –

It prevents normal use of communication 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 wither by disabling the network or by overloading it by messages so as to degrade performance.



18

Difference between Active Attack and Passive Attack

	ACTIVE ATTACK	PASSIVE ATTACK
1.	In active attack, Modification in information take place.	While in passive attack, Modification in the information does not take place.
2.	Active Attack is danger for Integrity as well as availability .	Passive Attack is danger for Confidentiality .
3.	In active attack attention is on detection.	While in passive attack attention is on prevention.
4.	Due to active attack system is always damaged.	While due to passive attack, there is no any harm to the system.
5.	In active attack, Victim gets informed about the attack.	While in passive attack, Victim does not get informed about the attack.
6.	In active attack, System resources can be changed.	While in passive attack, System resources are not change.
7.	Active attack influence the services of the system.	While in passive attack, information and messages in the system or network are acquired.
8.	In active attack, information collected through passive attacks are used during executing.	While passive attack are performed by collecting the information such as passwords, messages by itself.
19	Active attack is tough to restrict from entering systems or networks.	Passive Attack is easy to prohibited in comparison to active attack.

Practical Side Attacks:

It is Divided in 2 parts- (a) Application Level Attack (b) Network Level Attack

- ⌘ ARP Spoofing- ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network.
- ⌘ Botnet- A botnet is a network of compromised computers under the control of a malicious actor. Each individual device in a botnet is referred to as a bot.
- ⌘ Cache Poisoning- Cache poisoning is a type of attack in which corrupt data is inserted into the cache database of the Domain Name System (DNS) name server. The Domain Name System is a system that associates domain names with IP addresses.
- ⌘ Computer Worm- Computer worms are among the most common types of malware. They spread over computer networks by exploiting operating system vulnerabilities.



- ⌘ Keylogger- Keyloggers or keystroke loggers are software programs or hardware devices that track the activities (keys pressed) of a keyboard. Keyloggers are a form of spyware where computer users are unaware their actions are being tracked.
- ⌘ Malware- Malware is short for "malicious software": hostile applications that are created with the express intent to damage or disable mobile devices, computers or network servers.
- ⌘ Man-in-the-Middle Attack- A man-in-the-middle (MITM) attack is a type of cyber attack where a malicious actor inserts him/herself into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other.
- ⌘ Rootkit- A rootkit is a computer program designed to provide privileged access to a computer while actively hiding its presence. Once a rootkit has been installed, the controller of the rootkit has the ability to remotely execute files and change system configurations on the host machine.



- ❏ SQL Injection- SQL Injection is a type of attack that attempts to gain unauthorized access to your database through user input fields.
- ❏ Spoofing Attack-A spoofing attack is when a malicious party impersonates another device or user on a network in order to launch attacks against network hosts, steal data, spread malware or bypass access controls.
- ❏ Spyware-Although it sounds like something James Bond would employ, spyware is all too real. Spyware is any software that installs itself on your computer and starts covertly monitoring your online behavior without your knowledge or permission.

Classical Encryption Techniques

Cryptography is the technique which is used for doing secure communication between two parties in the public environment where unauthorized users and malicious attackers are present.

In cryptography there are two processes i.e. encryption and decryption performed at sender and receiver end respectively.

Encryption is the processes where a simple multimedia data is combined with some additional data (known as key) and converted into unreadable encoded format known as Cipher.

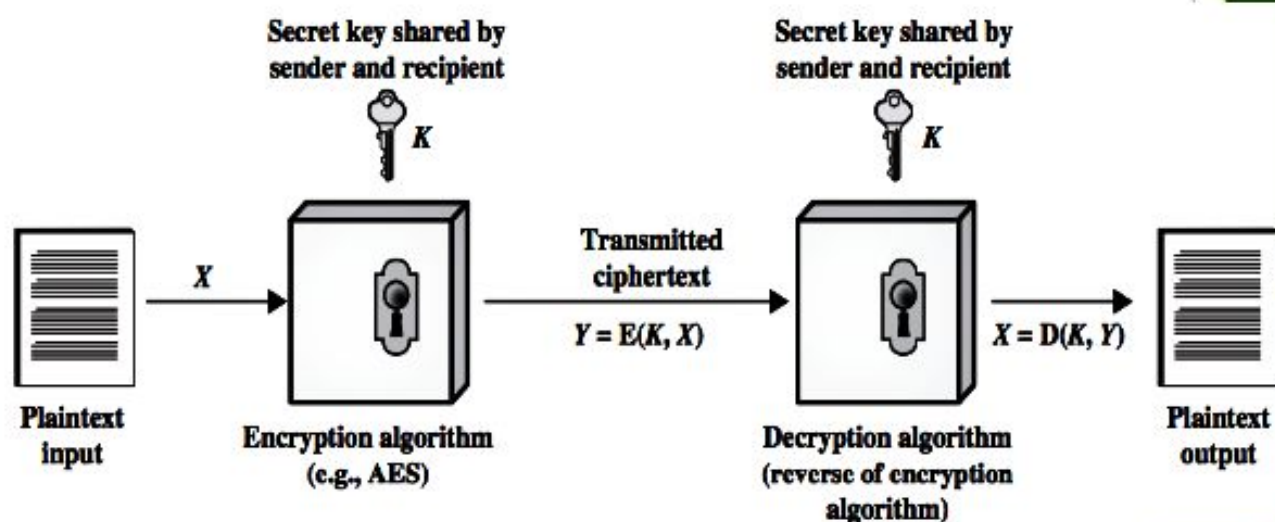
Decryption is the reverse method as that of encryption where the same or different additional data (key) is used to decode the cipher and it is converted in to the real multimedia data.

- ✘ The many schemes used for encryption constitute the area of study known as **cryptography**. Such a scheme is known as a **cryptographic system** (cryptosystem) or a **cipher**.
- ✘ Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of **cryptanalysis**. Cryptanalysis is what the layperson calls "breaking the code".
- ✘ The areas of cryptography and cryptanalysis together are called **cryptology**.

Symmetric Cipher Model

- ✘ **Plaintext:** This is the original intelligible message or data that is fed into the algorithm as input.
- ✘ **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.
- ✘ **Secret key:** The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the 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.
- ✘ **Ciphertext:** This is the scrambled (unintelligible) 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.

- ✘ **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.



Encryption Requirements

- ✘ The encryption algorithm must be strong.
 - ✘ At a minimum, 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.
 - ✘ In a stronger form, the opponent should be unable to decrypt ciphertexts or discover the key even if he or she has a number of ciphertexts together with the plaintext for each ciphertext.
- ✘ 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.

Cryptography

Cryptographic systems are characterized along three independent dimensions:

✘ **Type of operations for transforming plaintext to ciphertext.**

All encryption algorithms are based on two general principles:

- ✘ **Substitution:** each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element,
- ✘ **Transposition:** elements in the plaintext are rearranged.

The fundamental requirement is that no information be lost (all operations are reversible). *Product systems* involve multiple stages of substitutions and transpositions.

Cryptography

Cryptographic systems are characterized along three independent dimensions:

❖ **Type of operations for transforming plaintext to ciphertext.**

All encryption algorithms are based on two general principles:

- ❖ **Substitution:** each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element,
- ❖ **Transposition:** elements in the plaintext are rearranged.

The fundamental requirement is that no information be lost (all operations are reversible). *Product systems* involve multiple stages of substitutions and transpositions.

❖ **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.

❖ **How 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.

Classical Substitution Techniques

- ✘ Where letters of plaintext are replaced by other letters or by numbers or symbols
- ✘ or if plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.

Caesar Cipher

- ✘ It is a simplest form of substitution cipher scheme.
- ✘ It is developed by Julius Caesar.
- ✘ first attested use in military affairs.
- ✘ This cryptosystem is generally referred to as the **Shift Cipher**.
- ✘ For this type of scheme, both sender and receiver agree on a 'secret shift number' for shifting the alphabet.
- ✘ This number which is between 0 and 25 becomes the key of encryption.
- ✘ The name 'Caesar Cipher' is occasionally used to describe the Shift Cipher when the 'shift of three' is used.
- ✘ Replaces each letter by 3rd letter on

Process of Shift Cipher

- ❑ In order to encrypt a plaintext letter, the sender positions the sliding ruler underneath the first set of plaintext letters and slides it to LEFT by the number of positions of the secret shift.
- ❑ The plaintext letter is then encrypted to the ciphertext letter on the sliding ruler underneath. The result of this process is depicted in the following illustration for an agreed shift of three positions. In this case, the plaintext 'tutorial' is encrypted to the ciphertext 'WXWRULDO'. Here is the ciphertext alphabet for a Shift of 3:

Plaintext Alphabet	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
Ciphertext Alphabet	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

- ❑ On receiving the ciphertext, the receiver who also knows the secret shift, positions his sliding ruler underneath the ciphertext alphabet and slides it to RIGHT by the agreed shift number, 3 in this case.
- ❑ He then replaces the ciphertext letter by the plaintext letter on the sliding ruler underneath. Hence the ciphertext 'WXWRULDO' is decrypted to 'tutorial'. To decrypt a message encoded with a Shift of 3, generate the plaintext alphabet using a shift of '-3' as shown below -

Ciphertext Alphabet	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
Plaintext Alphabet	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	w

❑ Security Value/Disadvantage

Caesar Cipher is **not a secure** cryptosystem because there are only 26 possible keys to try out. An attacker can carry out an exhaustive key search with available limited computing resources.

Simple Substitution Cipher/Modified Caesar Cipher

- It is an improvement to the Caesar Cipher.
- Instead of shifting the alphabets by some number, this scheme uses some permutation of the letters in alphabet.
- With 26 letters in alphabet, we have 25 possibilities of replacement.
- The sender and the receiver may choose any one of these possible permutations as a ciphertext alphabet. This permutation is the secret key of the scheme.

Process of Simple Substitution Cipher

- Write the alphabets A, B, C, ..., Z in the natural order.
- The sender and the receiver decide on a randomly selected permutation of the letters of the alphabet.
- For encryption, sender replaces each plaintext letter by substituting the permutation letter that is directly beneath it in the table.
- Example, the chosen permutation is K, D, G, ..., O. The plaintext 'point' is encrypted to 'MJBXZ'.

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

- On receiving the ciphertext, the receiver, who also knows the randomly chosen permutation, replaces each ciphertext letter on the bottom row with the corresponding plaintext letter in the top row. The ciphertext 'MJBXZ' is decrypted to 'point'.

Security Value

- Simple Substitution Cipher is a considerable improvement over the Caesar Cipher.
- However, the Simple Substitution Cipher has a simple design and it is prone to design flaws, say choosing obvious permutation, this cryptosystem can be easily broken.

Monoalphabetic Cipher

- Rather than just shifting the alphabet
- Could shuffle (jumble) the letters arbitrarily
- Each plaintext letter maps to a different random ciphertext letter
- hence key is 26 letters long
- For example, if 'A' is encrypted as 'D', for any number of occurrence in that plaintext, 'A' will always get encrypted to 'D'.

Plain: abcdefghijklmnopqrstuvwxyz

Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN

Plaintext: ifwewishtoreplaceletters

Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA

Monoalphabetic Cipher Security

- Now have a total of $26! = 4 \times 10^{26}$ keys
- With so many keys, might think is secure
- But would be **!!!WRONG!!!**
- Problem is language characteristics

17

Playfair Cipher

- Not even the large number of keys in a monoalphabetic cipher provides security
- One approach to improving security was to encrypt multiple letters
- The **Playfair Cipher** is an example
- Invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair

Playfair Cipher

- Not even the large number of keys in a monoalphabetic cipher provides security
- One approach to improving security was to encrypt multiple letters
- The **Playfair Cipher** is an example
- Invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair

18

Playfair Key Matrix

- A 5X5 matrix of letters based on a keyword
- fill in letters of keyword (sans duplicates)
- fill rest of matrix with other letters
- eg. using the keyword MONARCHY

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

Encrypting and Decrypting

- ⊠ Plaintext is encrypted two letters at a time
 1. if a pair is a repeated letter, insert filler like 'X'
 2. if both letters fall in the same row, replace each with letter to right (wrapping back to start from end)
 3. if both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom)
 4. otherwise each letter is replaced by the letter in the same row and in the column of the other letter of the pair

Security of Playfair Cipher

- ⊠ Security much improved over monoalphabetic
- ⊠ Since have $26 \times 26 = 676$ digrams
- ⊠ Would need a 676 entry frequency table to analyse (verses 26 for a monoalphabetic) and correspondingly more ciphertext
- ⊠ Widely used for many years
 - ⊠ eg. by US & British military in WW1
- ⊠ It **can** be broken, given a few hundred letters
- ⊠ since still has much of plaintext structure

Polyalphabetic Ciphers

- ❑ improve security using multiple cipher alphabets
- ❑ make cryptanalysis harder with more alphabets to guess and flatter frequency distribution
- ❑ use a key to select which alphabet is used for each letter of the message
- ❑ use each alphabet in turn
- ❑ repeat from start after end of key is reached

One-Time Pad/Vernham Cipher

- ❑ It is an unbreakable cipher.
- ❑ The key is exactly same as the length of message which is encrypted.
- ❑ The key is made up of random symbols.
- ❑ As the name suggests, key is used one time only and never used again for any other message to be encrypted.
- ❑ Due to this, encrypted message will be vulnerable to attack for a cryptanalyst. The key used for a one-time pad cipher is called **pad**, as it is printed on pads of paper.

Why One-Time Pad is Unbreakable?

- ✘ The key is as long as the given message.
- ✘ The key is truly random and specially auto-generated.
- ✘ Key and plain text calculated as modulo 10/26/2.
- ✘ Each key should be used once and destroyed by both sender and receiver.
- ✘ There should be two copies of key: one with the sender and other with the receiver.

✘ Encryption

To encrypt a letter, a user needs to write a key underneath the plaintext. The plaintext letter is placed on the top and the key letter on the left. The cross section achieved between two letters is the plain text.

✘ Decryption

To decrypt a letter, user takes the key letter on the left and finds cipher text letter in that row. The plain text letter is placed at the top of the column where the user can find the cipher text letter.

<p>Plain text: T H I S I S S E C R E T</p> <p>OTP-Key : X V H E U W N O P G D Z</p> <p>-----</p> <p>Ciphertext: Q C P W C O F S R X H S</p> <p>In groups : QCPWC OFSRX HS</p>

Transposition Ciphers

- Now consider classical **transposition** or **permutation** ciphers
- These hide the message by rearranging the letter order
- The actual plaintext alphabets are not replaced.
- Can recognise these since have the same frequency distribution as the original text

Rail Fence cipher

- Write message letters out diagonally over a number of rows
- Then read off cipher row by row
- Eg. write message out as:
m e m a t r h t g p r y
e t e f e t e o a a t
- Giving ciphertext
MEMATRHTGPRYETEFETEOAAT

Row Transposition Ciphers

- ⊠ A more complex transposition
- ⊠ Write letters of message out in rows over a specified number of columns
- ⊠ Then reorder the columns according to some key before reading off the rows

Key: 3 4 2 1 5 6 7

Plaintext: a t t a c k p

o s t p o n e

d u n t i l t

w o a m x y z

Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

Product Ciphers

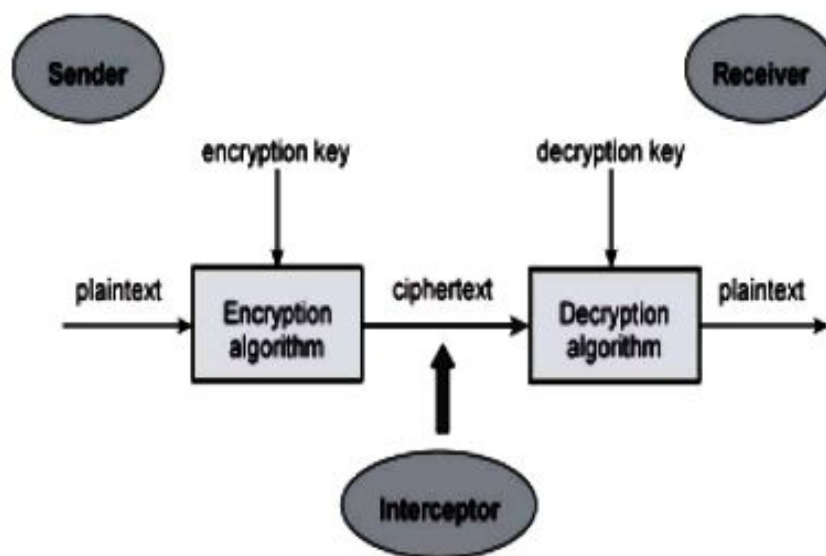
- ⊠ Ciphers using substitutions or transpositions are not secure because of language characteristics
- ⊠ Hence consider using several ciphers in succession to make harder, but:
 - ⊠ two substitutions make a more complex substitution
 - ⊠ two transpositions make more complex transposition
 - ⊠ but a substitution followed by a transposition makes a new much harder cipher
- ⊠ This is bridge from classical to modern ciphers

Difference between Substitution & Transposition Cipher Technique

S.NO	SUBSTITUTION CIPHER TECHNIQUE	TRANSPOSITION CIPHER TECHNIQUE
1.	In substitution Cipher Technique, plain text characters are replaced with other characters, numbers and symbols.	In transposition Cipher Technique, plain text characters are rearranged with respect to the position.
2.	Substitution Cipher's forms are: Mono alphabetic substitution cipher and poly alphabetic substitution cipher.	Transposition Cipher's forms are: Key-less transposition cipher and keyed transposition cipher.
3.	In substitution Cipher Technique, character's identity is changed while its position remains unchanged.	While in transposition Cipher Technique, The position of the character is changed but character's identity is not changed.
4.	In substitution Cipher Technique, The letter with low frequency can detect plaint ext.	While in transposition Cipher Technique, The Keys which are nearer to correct key can disclose plain text.
5.	The example of substitution Cipher is Caesar Cipher.	The example of transposition Cipher is Reil Fence Cipher.

Cryptosystem

- ✧ A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services.
- ✧ A cryptosystem is also referred to as a **cipher system**.
- ✧ The objective of this simple cryptosystem is that at the end of the process, only the sender and the receiver will know the plaintext.



Components of a Cryptosystem

Six Components of cryptosystem:

- ✧ **Plaintext.** It is the data to be protected during transmission.
- ✧ **Encryption Algorithm.** It is a mathematical process that produces a ciphertext for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a ciphertext.
- ✧ **Ciphertext.** It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key. The ciphertext is not guarded. It flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel.

- ❏ **Decryption Algorithm**, It is a mathematical process, that produces a unique plaintext for any given ciphertext and decryption key. It is a cryptographic algorithm that takes a ciphertext and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.
- ❏ **Encryption Key**. It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the ciphertext.
- ❏ **Decryption Key**. It is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the ciphertext in order to compute the plaintext.

For a given cryptosystem, a collection of all possible decryption keys is called a **key space**.

Types of Cryptosystems

Two types of cryptosystem:

- ❏ Symmetric Key Encryption
- ❏ Asymmetric Key Encryption

1. Symmetric Key Encryption: The encryption process where **same keys are used for encrypting and decrypting** the information is known as Symmetric Key Encryption.

The study of symmetric cryptosystems is referred to as **symmetric cryptography**.

Symmetric cryptosystems are also sometimes referred to as **secret key cryptosystems**.

Examples of symmetric key encryption methods are – Digital Encryption Standard (DES), Triple-DES (3DES), IDEA, and BLOWFISH.

1. Symmetric Key Encryption: The encryption process where **same keys are used for encrypting and decrypting** the information is known as Symmetric Key Encryption.

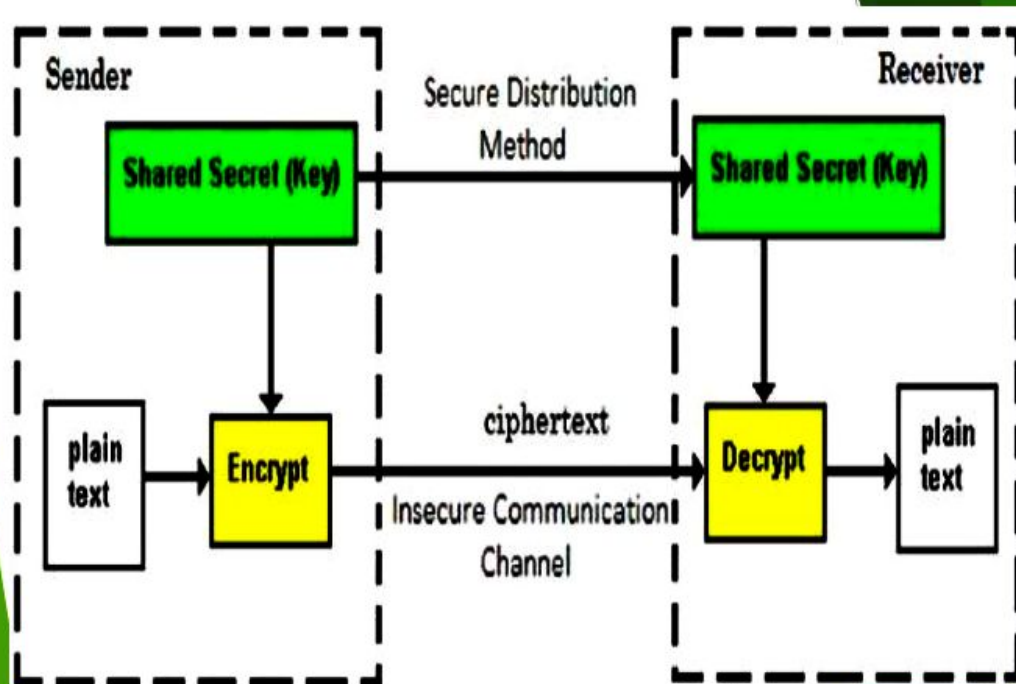
The study of symmetric cryptosystems is referred to as **symmetric cryptography**.

Symmetric cryptosystems are also sometimes referred to as **secret key cryptosystems**.

Examples of symmetric key encryption methods are – Digital Encryption Standard (DES), Triple-DES (3DES), IDEA, and BLOWFISH.

Features of symmetric key encryption :

- Persons using symmetric key encryption must share a common key prior to exchange of information.
 - Keys are recommended to be changed regularly to prevent any attack on the system.
 - A robust mechanism needs to exist to exchange the key between the communicating parties. As keys are required to be changed regularly, this mechanism becomes expensive and cumbersome.
 - In a group of n people, to enable two-party communication between any two persons, the number of keys required for group is $n \times (n - 1)/2$.
 - Length of Key (number of bits) in this encryption is smaller and hence, process of encryption-decryption is faster than asymmetric key encryption.
- Processing power of computer system required to run symmetric algorithm is less.



Challenge of Symmetric Key Cryptosystem

- ⌘ **Key establishment** – Before any communication, both the sender and the receiver need to agree on a secret symmetric key. It requires a secure key establishment mechanism in place.
- ⌘ **Trust Issue** – Since the sender and the receiver use the same symmetric key, there is an implicit requirement that the sender and the receiver 'trust' each other. For example, it may happen that the receiver has lost the key to an attacker and the sender is not informed.

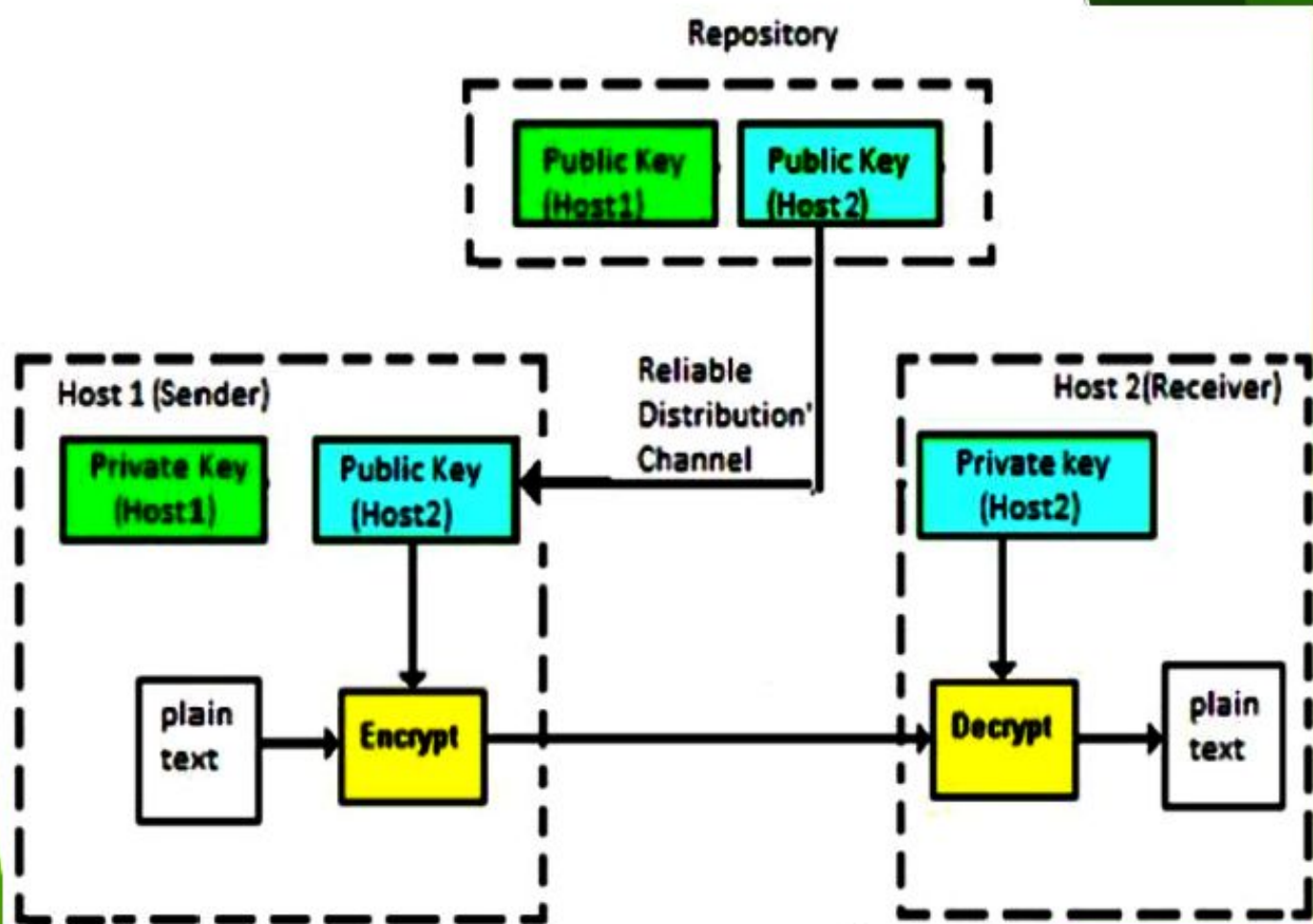
These two challenges are highly restraining for modern day communication. Today, people need to exchange information with non-familiar and non-trusted parties. For example, a communication between online seller and customer.

Asymmetric Key Encryption

- ⌘ The encryption process where **different keys are used for encrypting and decrypting the information** is known as Asymmetric Key Encryption.
- ⌘ Though the keys are different, they are mathematically related and hence, retrieving the plaintext by decrypting ciphertext is feasible.

Features of Asymmetric Key Encryption

- ❑ Every user in this system needs to have a pair of dissimilar keys, **private key** and **public key**. These keys are mathematically related – when one key is used for encryption, the other can decrypt the ciphertext back to the original plaintext.
- ❑ It requires to put the public key in public repository and the private key as a well-guarded secret. Hence, this scheme of encryption is also called **Public Key Encryption**.
- ❑ Though public and private keys of the user are related, it is computationally not feasible to find one from another. This is a strength of this scheme.
- ❑ When *Host1* needs to send data to *Host2*, he obtains the public key of *Host2* from repository, encrypts the data, and transmits.
- ❑ *Host2* uses his private key to extract the plaintext.
- ❑ Length of Keys (number of bits) in this encryption is large and hence, the process of encryption-decryption is slower than symmetric key encryption.
- ❑ Processing power of computer system required to run asymmetric algorithm is higher.



Cryptanalysis

- ❑ Cryptanalysis is the decryption and analysis of codes, ciphers or encrypted text.
- ❑ Simply it is the decryption process.
- ❑ Decryption process is reverse of the encryption process.
- ❑ It is the Part of the cryptology.
- ❑ Cryptanalysis is also used during the design of the new cryptographic techniques to test their security strengths.

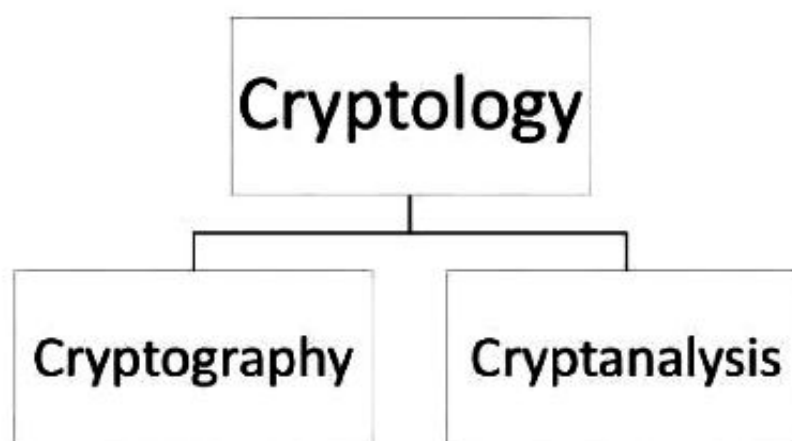
Cryptanalysis attack

- ✘ Known-Plaintext Analysis (KPA): Attacker decrypt ciphertexts with known partial plaintext.
 - ✘ Chosen-Plaintext Analysis (CPA): Attacker uses ciphertext that matches arbitrarily selected plaintext via the same algorithm technique.
 - ✘ Ciphertext-Only Analysis (COA): Attacker uses known ciphertext collections.
 - ✘ Man-in-the-Middle (MITM) Attack: Attack occurs when two parties use message or key sharing for communication via a channel that appears secure but is actually compromised. Attacker employs this attack for the interception of messages that pass through the communications channel. Hash functions prevent MITM attacks.
- Adaptive Chosen-Plaintext Attack (ACPA): Similar to a CPA, this attack uses chosen plaintext and ciphertext based on data learned from past encryptions.

Cryptology

It is Combination of following:

- ✘ Cryptography
- ✘ Cryptanalysis



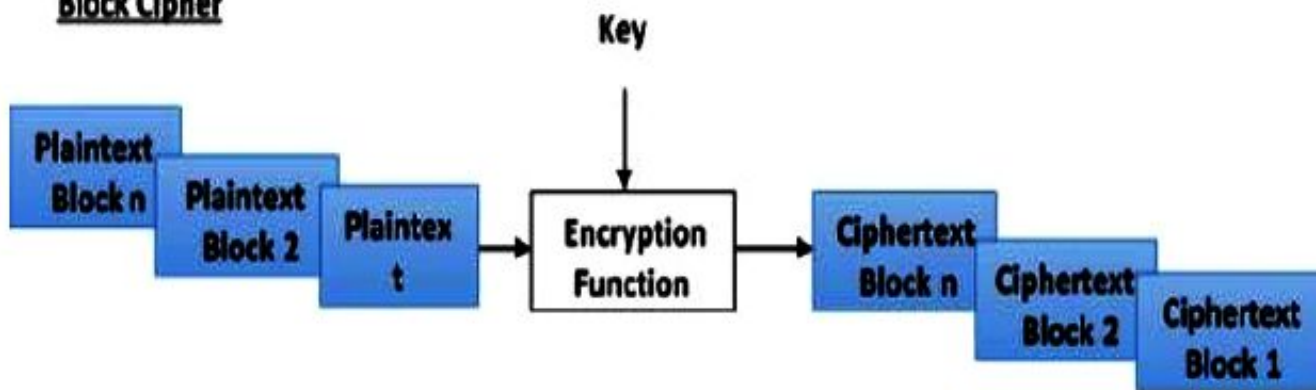
Block Ciphers

- ✘ The plain binary text is processed in blocks (groups) of bits at a time.
- ✘ A block of plaintext bits is selected, a series of operations is performed on this block to generate a block of ciphertext bits.
- ✘ The number of bits in a block is fixed.
- ✘ For example, the schemes DES and AES have block sizes of 64 and 128, respectively.

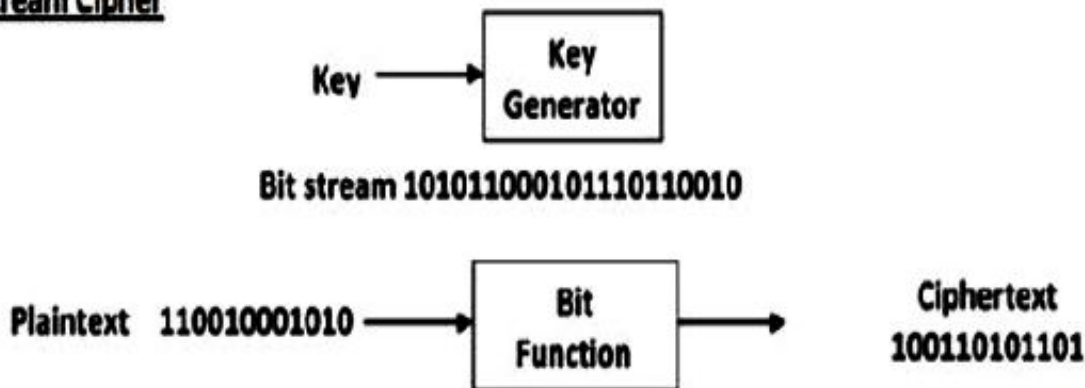
Stream Cipher

- ✘ The plaintext is processed one bit at a time
- ✘ One bit of plaintext is taken, and a series of operations is performed on it to generate one bit of ciphertext.
- ✘ Technically, stream ciphers are block ciphers with a block size of one bit.

Block Cipher



Stream Cipher



Difference between Block Cipher and Stream Cipher

S.NO	BLOCK CIPHER	STREAM CIPHER
1.	Block Cipher Converts the plain text into cipher text by taking plain text's block at a time.	Stream Cipher Converts the plaint text into cipher text by taking 1 byte of plain text at a time.
2.	Block cipher uses either 64 bits or more than 64 bits.	While stream cipher uses 8 bits.
3.	The complexity of block cipher is simple.	While stream cipher is more complex.
4.	Block cipher Uses confusion as well as diffusion.	While stream cipher uses only confusion.
5.	In block cipher, reverse encrypted text is hard.	While in stream cipher, reverse encrypted text is easy.
6.	The algorithm modes which are used in block cipher are: ECB (Electronic Code Book) and CBC (Cipher Block Chaining).	The algorithm modes which are used in stream cipher are: CFB (Cipher Feedback) and OFB (Output Feedback).