Table of Contents

1 INTRODUCTION AND CLASSICAL CIPHERS

2 SYMMETRIC CIPHERS

3 ASYMMETRIC CIPHERS

4 CRYPTOGRAPHIC HASH FUNCTIONS AND DIGITAL SIGNATURES

5 AUTHENTICATION

6 NETWORK SECURITY AND PUBLIC KEY INFRASTRUCTURE

7 MALICIOUS LOGIC

CHAPTER 1

INTRODUCTION AND CLASSICAL CIPHERS

CHAPTER OUTLINE

After studying this chapter, the students will be able to

- Security: Computer Security, Information Security, Network Security, CIA Triad, Cryptography, Cryptosystem, Cryptanalysis, Security Threats and Attacks, Security Services, Security Mechanisms
- Classical Cryptosystems: Substitution Techniques: Ceasar, Monoalphabetic, Playfair, Hill, Polyalphabetic ciphers, One-time pad
- Transposition Techniques: Rail Fence Cipher
- Modern Ciphers: Block vs. Stream Ciphers, Symmetric vs. Asymmetric Ciphers

In 1994, the Internet Architecture Board (IAB) issued a report entitled "Security in the Internet Architecture" (RFC 1636). The report stated the general consensus that the Internet needs more and better security, and it identified key areas for security mechanisms. Among these were the need to secure the network infrastructure from unauthorized monitoring and control of network traffic and the need to secure end-user-to-end-user traffic using authentication and encryption mechanisms. Security is said to be preserved when unauthorized, unauthenticated access and modification to the systems are not allowed.

Information security means protecting information and information systems from unauthorized access, use, modification, or destruction. The terms information security, computer security and information assurance are frequently used interchangeably. These fields are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information.

To make a system secure various security dimensions are needed such as; Good physical Security is necessary to protect physical assets like paper records and systems. Communication Security (COMSEC) is necessary to protect information in transit. Emission Security (EMSEC) is needed when the enemy has significant resources to read the electronic emissions from our computer systems. Computer Security (COMPUSEC) is necessary to control access on our computer systems and Network Security (NETSEC) is needed to control the security of our local area networks. Together, all of these concepts provide information security (INFOSEC).

Network Security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users and programs to perform their permitted critical functions within a secure environment over computer networks.

With the introduction of the computer, the need for automated tools for protecting the files and other information stored on the computer became evident. This is especially the case for a shared system as like internet. Thus, ***computer security*** is the generic name for the collection of tools designed to protect data and to prevent attackers.

Computer Security is 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).

Computer Security rests on confidentiality, integrity and availability.

Confidentiality: This term covers two related concepts:

- **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
- **Privacy:** Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Integrity: This term covers two related concepts:

- **Data integrity:** Assures that information and programs are changed only in a specified and authorized manner.
- **System integrity:** Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Availability: Assures that systems work promptly and service is not denied to authorized users.

These three concepts form what is often referred to as the **CIA triad.** The three concepts embody the fundamental security objectives for both data and for information and computing services.

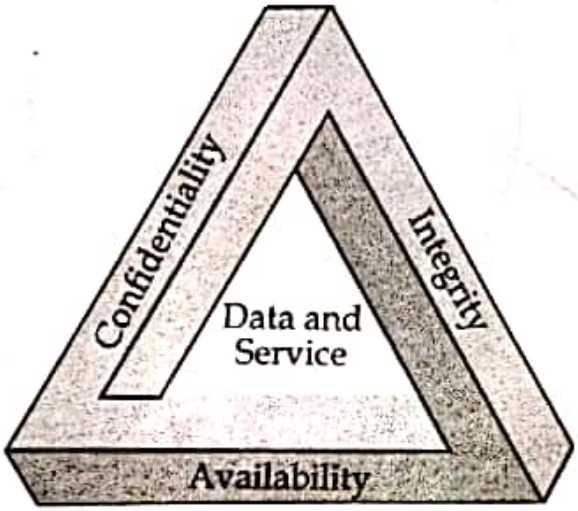

Figure 1.1: The CIA Traid REDRAW

Confidentiality: Confidentiality is the concealment of information or resources. Cryptography can be the better choice for maintaining the privacy of information, which traditionally is used to protect the secret messages. Similarly, privacy of resources, i.e. resource hiding can be maintained by using proper firewalls. Confidentiality is sometimes called **secrecy** or **privacy.**

Integrity: Integrity ensures the correctness as well as trustworthiness of data or resources. For example, if we say that we have preserved the integrity of an item, we may mean that the item is: precise, accurate, unmodified, modified only in acceptable ways, modified only by authorized people, modified only by authorized processes, consistent, meaningful and usable.

Integrity mechanisms fall into two classes; *prevention* mechanisms and *detection* mechanisms. Prevention mechanisms are responsible to maintain the integrity of data by blocking any unauthorized attempts to change the data or any attempts to change data in unauthorized ways. While detection mechanisms; rather than preventing the violations of integrity; they simply analyze the data's integrity is no longer trustworthy. Such mechanisms may analyze the system events or the data itself to see if required constraints still hold.

Availability: Availability refers to the ability to use the information or resource desired. An unavailable system is as bad as no system at all. An object or service is thought to be available if;

- It is present in a usable form.
- It has capacity enough to meet the service's needs.
- It is making clear progress, and, if in wait mode, it has a bounded waiting time.
- The service is completed in an acceptable period of time.

Availability is usually defined in terms of "quality of service," in which authorized users are expected to receive a specific level of service. The aspect of availability that is relevant to security is that someone may intentionally arrange to deny access to data or to service by making it unavailable.

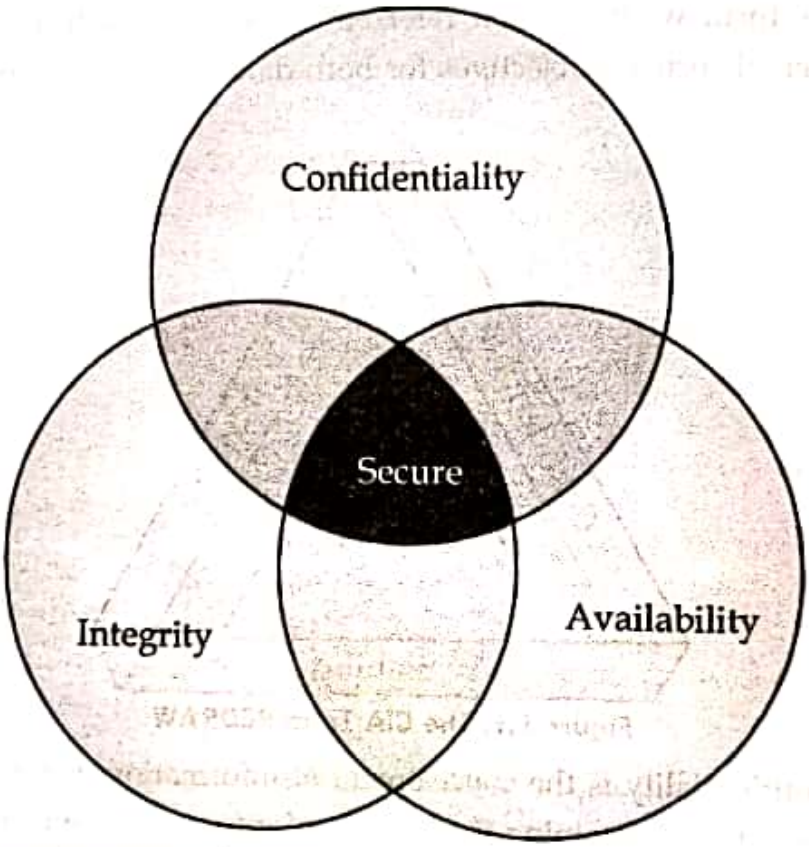

Figure 1.2: Relationship between Confidentiality, Integrity and Availability

Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture. Two of the most commonly mentioned are as follows:

Authenticity: It is the property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

Accountability: Accountability defines the security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party. Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

GOALS OF SECURITY

- **Prevention** is to prevent the attackers from violating security policy. Prevention means that an attack will fail. Typically, prevention involves implementation of mechanisms that users can not override and that are trusted to be implemented in a correct ways so that the attacker cannot defeat the mechanism by changing it.
- **Detection** is to detect attackers' violation of security policy. So it occurs after someone violates the policy. The mechanism determines that a violation of the policy has occurred (or is underway) due to attack, and reports it. The system must then respond appropriately. Detection is most useful when an attack cannot be prevented.
- **Recovery** is to stop attack and to assess and repair any damage caused by attack. With recovery, it should be such that the system continues to function correctly, possibly after a period during which it fails to function correctly, due to attacks. For example if the attacker deletes a file, one recovery mechanism is to restore the file from backup tapes.

CHALLENGES OF COMPUTER SECURITY

Computer and network security is both fascinating and complex. Some of the reasons follow:

1. **Security is not as simple as it might first appear to the novice.** The requirements seem to be straightforward; indeed, most of the major requirements for security services can be given self-explanatory, one-word labels: confidentiality, authentication, nonrepudiation, or integrity. But the mechanisms used to meet those requirements can be quite complex, and understanding them may involve rather subtle reasoning.
2. **In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features.** In many cases, successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism.
3. Because of point 2, the procedures used to provide particular services are often counterintuitive. **Typically, a security mechanism is complex, and it is not obvious from the statement of a particular requirement that such elaborate measures are needed.** It is only when the various aspects of the threat are considered that elaborate security mechanisms make sense.
4. **Having designed various security mechanisms, it is necessary to decide where to use them.** This is true both in terms of physical placement (e.g., at what points in a network are certain security mechanisms needed) and in a logical sense [e.g., at what layer or layers of an architecture such as TCP/IP (Transmission Control Protocol/Internet Protocol) should mechanisms be placed].
5. **Security mechanisms typically involve more than a particular algorithm or protocol. They also require that participants be in possession of some secret information (e.g., an encryption key), which raises questions about the creation, distribution, and protection of that secret information.** There also may be a reliance on communications protocols whose behavior may complicate the task of developing the security mechanism. For example, if the proper functioning of the security mechanism requires setting time limits on the transit time of a message from sender to receiver, then any protocol or network that introduces variable, unpredictable delays may render such time limits meaningless.

6. **Computer and network security is essentially a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them. The** great advantage that the attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security.
7. **There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs.**
8. **Security requires regular, even constant, monitoring, and this is difficult in today's short-term, overloaded environment.**
9. **Security is still too often an afterthought to be incorporated into a system after the design is complete rather than being an integral part of the design process.**
10. **Many users and even security administrators view strong security as an barrier to efficient and user-friendly operation of an information system or use of information.**

CRYPTOGRAPHY

The word *cryptography* comes from two Greek words "Cryptos" and "Graph" meaning *"secret writing"* and is the art and science of information hiding. This field is very much associated with mathematics and computer science with application in many fields like computer security, electronic commerce, telecommunication, etc. In the ancient days, cryptography was mostly referred to as ***encryption*** – the mechanism to convert the readable ***plaintext*** into unreadable (incomprehensible) text i.e. ***ciphertext***, and ***decryption*** – the opposite process of encryption i.e. conversion of ciphertext back to the plaintext. Though the consideration of cryptography was on message confidentiality (encryption) in the past, nowadays cryptography considers the study and practices of authentication, digital signatures, integrity checking, and key management, etc.

Cryptanalysis is the breaking of codes. Cryptanalysis encompasses all of the techniques to recover the plaintext and/or key from the ciphertext.

The combined study of cryptography and cryptanalysis is known as ***cryptology***. Though most of the time we use cryptography and cryptology in the same way.

CRYPTOSYSTEM

Cryptosystem is a 5-tuple/quintuple (E, D, M, K, C), where M set of plaintexts, K set of keys, C set of ciphertexts, E set of encryption functions e: $M \times K \rightarrow C$ and D set of decryption functions d: $C \times K \rightarrow M$.

Example: *Caesar Cipher*

$M = \{\text{sequences of letters}\}$
$K = \{i \mid i \text{ is an integer and } 0 \leq i \leq 25\}$
$E = \{E_k \mid k \in K \text{ and for all letters m, } E_k(m) = (m + k) \bmod 26\}$
$D = \{D_k \mid k \in K \text{ and for all letters c, } D_k(c) = (26 + c - k) \bmod 26\}$
$C = M$

ENCRYPTION AND DECRYPTION

Encryption is the process of encoding a message so that its meaning is not obvious i.e. converting information from one form to some other unreadable form using some algorithm called *cipher* with the help of secret message called *key*. The converting text is called is *plaintext* and the converted text is called *ciphertext*.

Decryption is the reverse process, transforming an encrypted message back into its normal, original form. In decryption process also the use of key is important.

Alternatively, the terms *encode* and *decode* or *encipher* and *decipher* are used instead of *encrypt* and *decrypt*. That is, we say that we encode, encrypt, or encipher the original message to hide its meaning. Then, we decode, decrypt, or decipher it to reveal the original message.

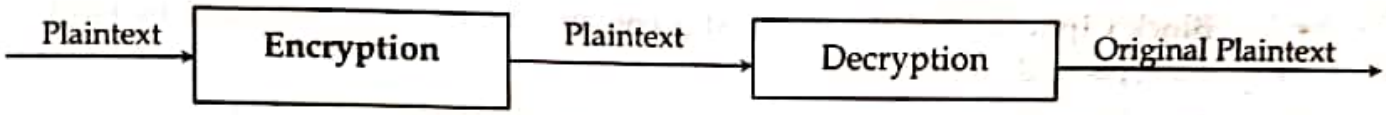

Figure 1.3: Encryption-Decryption

The use of encryption techniques is being used since very long period as it can be noted from the technique called *Caesar's cipher* used by Julius Caesar for information passing to his soldiers. Encryption techniques have also been extensively used in military purposes to conceal the information from the enemy. Nowadays to gain the confidentiality encryption is being used in many areas like communication, internet banking, digital right management, etc.

KEY

A *key* is a parameter or a piece of information used to determine the output of cryptographic algorithm. While doing the encryption, key determines the transformation of plaintext to the cipher text and vice versa. Keys are also used in other cryptographic processes like message authentication codes and digital signatures. Most of the cryptographic systems depend upon the key and thus the secrecy of the key is very important and is one of the difficult problems in practice. Another important issue for the key is its length. Since key is the sole entity that defines the strength of the security (normally algorithm used is public) we need to select the key in a way such that attacker should take long enough to try all possibilities. To prevent the key from being guessed the choice of the key must be random.

CIPHER

A *cipher* is an algorithm for performing encryption and decryption. The operation of cipher depends upon the special information called key. Without knowledge of the key, it should be difficult, if not nearly impossible, to decrypt the resulting cipher into readable plaintext. There are many types of encryption techniques that have advanced from history, however the distinction of encryption technique can be broadly categorized in terms of number of key used and way of converting plaintext to the ciphertext.

TYPES OF CIPHERS

Historical / Classical Ciphers

These ciphers use processes like *substitution* and *transposition* or combination of both called *product ciphers*. These historic ciphers use the single key for both encryption and decryption (symmetric cipher). To reduce the cipher attacks, in substitution instead of *monoalphabetic* - a letter for letter, *polyalphabetic*- one or more letters for single letter substitution can be used.

Modern Ciphers

Modern encryption methods can be divided by two criteria: by type of input data, and by type of key used.

- **Based upon input data: Stream Ciphers:** In this kind of ciphers the plaintext is converted into ciphertext stream by stream. So it encrypts continuous streams of data. Like, character by character conversion.
- **Block Ciphers:** Here the plaintext is converted into ciphertext block by block. So it encrypts of data of fixed size
- **Based upon type of key:** By type of key used ciphers are divided into;

  Symmetric Key Algorithms (Private Key Cryptography): These techniques use single key for encryption as well as decryption.
- **Asymmetric Key Algorithms (Public Key Cryptography):** These techniques use two keys, namely private and public keys. One key is used for encryption and the other is used for decryption.

In a symmetric key algorithm (e.g., DES and AES), the *sender* and *receiver* must have a shared key set up in advance and kept secret from all other parties; the sender uses this key for encryption, and the receiver uses the same key for decryption. In an asymmetric key algorithm (e.g., RSA), there are two separate keys: a *public key* is published and enables any *sender* to perform encryption, while a *private key* is kept secret by the *receiver* and enables only him to perform correct decryption.

CRYPTANALYSIS

Cryptanalysis (from the Greek *kryptós*, "hidden", and *analýein*, "to loosen" or "to untie") is the study of methods for obtaining the meaning of encrypted information, without access to the secret information which is normally required to do so. Typically, this involves finding a secret key.

Cryptanalysis usually excludes methods of attack that do not primarily target weaknesses in the actual cryptography, such as bribery, physical coercion, burglary, keystroke logging, and social engineering, although these types of attack are an important concern and are often more effective than traditional cryptanalysis.

SECURITY THREATS AND ATTACKS

Threat: A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit vulnerability.

Threats can be categorized into four classes:

- *Disclosure*- It leads to an unauthorized access to information. Eg: *Snooping*
- *Deception*- It leads to acceptance of false data. Eg: *Modification, Spoofing, denial of receipt, Repudiation of origin*
- *Disruption*- It leads to an interruption of correct operation. Eg: *Modification*
- **Usurpation**- It leads to an unauthorized control of some part of system. Eg: *Modification, Spoofing, denial of service, delay*

Attack: An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

TYPES OF ATTACKS

Attacks may be classified based on the nature. It may be an **active attack or passive attack.** A passive attack attempts to learn or make use of information from the system but does not affect system resources. An active attack attempts to alter system resources or affect their operation.

PASSIVE ATTACKS

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are the release of message contents and traffic analysis.

The release of message contents is easily understood. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

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

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

ACTIVE ATTACKS

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: **masquerade, replay, modification of messages, and denial of service.**

A **masquerade** takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect. For example, a message meaning "Allow John Smith to read confidential file *accounts*" is modified to mean "Allow Fred Brown to read confidential file *accounts*."

The **denial of service** prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service). Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

The **delay** is a temporal forbiddance of service. E.g.: If delivery of a message or a service requires time *t*; if an attacker can force the delivery time to be more than *t*, then there is delayed delivery.

Active attacks present the opposite characteristics of passive attacks. Whereas passive attacks are difficult to detect, measures are available to prevent their success. On the other hand, it is quite difficult to prevent active attacks absolutely because of the wide variety of potential physical, software, and network vulnerabilities. Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them. If the detection has a deterrent effect, it may also contribute to prevention.

To secure every system from attacks a set of security mechanism are implemented. **Security mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

SECURITY SERVICES

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 counter security attacks, and they make use of one or more security mechanisms to provide the service. Security services include following services;

a. **Authentication**

The authentication service is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from.

- **Peer entity authentication:** Provides for the corroboration of the identity of a peer entity in an association. Two entities are considered peers if they implement to same protocol in different systems; e.g., two TCP modules in two communicating systems. Peer entity authentication is provided for use at the establishment of, or at times during the data transfer phase of, a connection. It attempts to provide confidence that an entity is not performing either a masquerade or an unauthorized replay of a previous connection.
- **Data origin authentication:** Provides for the corroboration of the source of a data unit. It does not provide protection against the duplication or modification of data units. This type of service supports applications like electronic mail, where there are no prior interactions between the communicating entities.

b. **Access Control**

In the context of network security, access control is the ability to limit and control the access to host systems and applications via communications links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

c. **Data Confidentiality**

Confidentiality is the protection of transmitted data from passive attacks. With respect to the content of a data transmission, several levels of protection can be identified. The broadest service protects all user data transmitted between two users over a period of time. The other aspect of confidentiality is the protection of traffic flow from analysis. This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility.

d. **Data Integrity**

Integrity ensures correctness of the data. A connection-oriented integrity service, one that deals with a stream of messages, assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays. The destruction of data is also covered under this service. Thus, the connection-oriented integrity service addresses both message stream modification and denial of service. On the other hand, a connectionless integrity service, one that deals with individual messages without regard to any larger context, generally provides protection against message modification only.

e. **Non repudiation**

Non repudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.

f. **Availability Service**

Availability is the property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system.

SECURITY MECHANISMS

Security mechanism is process or a device incorporating such a process that is designed to detect, prevent, or recover from a security attack. Security mechanisms are used to preserve security in every system and make the system consistent. The mechanisms may include cryptography for ensuring confidentiality and integrity, authentication systems and digital signature schemes for ensuring integrity and access control lists for authorization. Security mechanisms are defined in a system based on security requirements and security policy.

CLASSICAL CRYPTOSYSTEMS

MONOALPHBETIC SUBSTITUTION CIPHER

CAESAR CIPHER

It is the simple shift monoalphabetic classical cipher where each letter is replaced by a letter 3 position (actual Caesar cipher) ahead using the circular alphabetic ordering i.e. letter after Z is A.

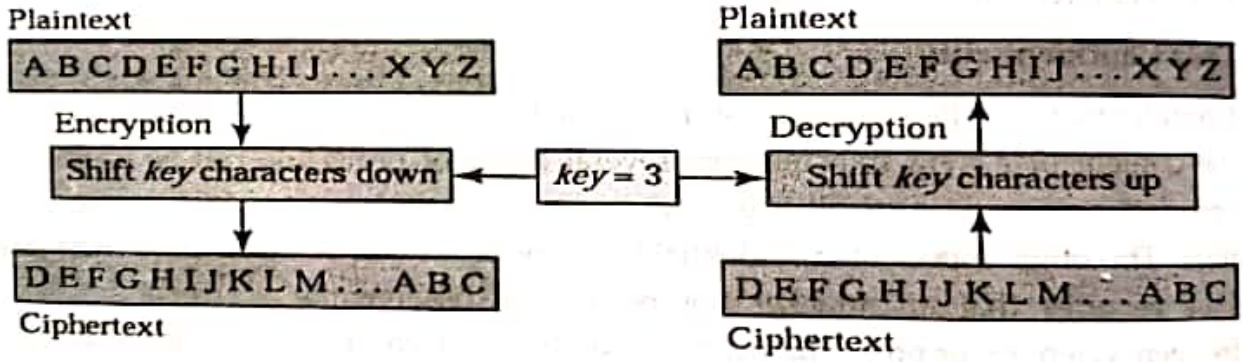

Fig 1.4: Caesar Cipher

So when we encode HELLO WORLD, the cipher text becomes KHOORZRUOG. Here we number each English alphabet starting from 0 (A) to 25 (Z). Each letter of the clear message is replaced by the letter whose number is obtained by adding the key (a number from 0 to 25) to the letter's number modulo 26. See the picture to visualize the Caesar cipher. The encryption can also be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1, ..., Z = 25. Encryption of a letter c by a shift k can be described mathematically as,

$$c = E_k(m) = (m + k) \mod 26$$

Decryption is performed similarly,

$$m = D_k(c) = (c + 26 - k) \mod 26$$

Similarly, consider some examples of Caesar cipher;

Plaintext: meet me after the toga party

Ciphertext: PHHW PH DIWHU WKH WRJD SDUWB

Plaintext: the quick brown fox jumps over the lazy dog

Ciphertext: WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ

Algorithm

Step 1: Start

Step 2: Convert a letter to its corresponding order in alphabet 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
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

Step 3: Compute cipertext as:

$C = E(K, P) = (P + K) \bmod 26$

Where, $0 \leq K \leq 25$

Step 4: Compute plaintext from ciphertext as,

$P = D(K, C) = (C - K) \bmod 26$

Example: p = hello

key (k) = 7

Solution:

h =7, k = 7

$y = e_k(x) = (x + k) \bmod 26$

$= (7 + 7) \bmod 26$

$= 14 \bmod 26$

$= o$

For ℓ, $\ell = 11$

$= (11 + 7) \bmod 26$

$= 18 \bmod 26$

$= 9$

c = o ℓ s s v

For e, e = 4

$= (4 + 7)$ mode 26

$= 11 \bmod 26$

$= 11$

$= \ell$

For o, o = 14

$= (14 + 7) \bmod 26$

$= 21$

$= v$

PLAYFAIR CIPHER

The best-known multiple-letter encryption cipher is the Playfair, which treats digrams in the plaintext as single units and translates these units into ciphertext digrams.

The Playfair algorithm is based on the use of a 5 x 5 matrix of letters constructed using a keyword. Here keyword is MONARCHY then the matrix is:

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

The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetic order. 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 balloon would be treated as ba lx lo on.
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, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, hs becomes BP and ea becomes IM (or JM, as the encipherer wishes).

Example: *Encrypt mathematics is good using your name as keyword & playfair cipher.*

Solution:

Keyword = S A R A H

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

Now, breaking the given plaintext as

ma	th	em	at	ic	si	sg	ox	od
KH	yF	FL	HP	DI	CO	BC	QV	PC

Hill Cipher

Another interesting multi letter cipher is the Hill cipher, developed by the mathematician Lester Hill in 1929. The encryption algorithm takes m successive plaintext letters and substitutes for them m ciphertext letters. The substitution is determined by m linear equations in which each character is assigned a numerical value (a = 0, b = 1 ... z = 25).

For example, consider the plaintext "paymoremoney" and use the encryption key

$$A = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

The first three letters of the plaintext are represented by the vector

$$\begin{pmatrix}15\\0\\24\end{pmatrix} \text{ then } K.\begin{pmatrix}15\\0\\24\end{pmatrix}=\begin{pmatrix}375\\819\\487\end{pmatrix} \bmod 26=\begin{pmatrix}11\\13\\18\end{pmatrix}=LNS$$

The ciphertext for the entire plaintext is LNSHDLEWMTRW. Hence in general the hill cipher can be expressed as

$C = E(K, P) = KP \bmod 26$

$P = D(K, P) = K^{-1}C \bmod 26 = K^{1}KP = P$

As with Playfair, the strength of the Hill cipher is that it completely hides single-letter frequencies. Indeed, with Hill, the use of a larger matrix hides more frequency information. Thus a 3 x 3 Hill cipher hides not only single-letter but also two-letter frequency information.

Example: Let k = $\begin{pmatrix}3 & 6\\1 & 5\end{pmatrix}$ **and plaintext = movie**

Solution:

The key is 2 × 2 matrix, we create 2 × 1 matrix of plain text, grouping 2 letters each.

So, mo vi ez (z is used to complete last pair)

So, for mo

$$= (12\ \ 14)\begin{pmatrix}3 & 6\\1 & 5\end{pmatrix}$$

$= (36 + 14 \quad 72 + 70)$

$= (50 \quad 142)$

$= (24 \quad 12) \bmod 26$

$= y \quad m$

POLYALPHABETIC SUBSTITUTION CIPHER

Vigenere Cipher

It is like Caesar cipher, but uses a phrase for e.g. for the message THE BOY HAS THE BALL and the key VIG, encipher using Caesar cipher for each letter:

Key: VIGVIGVIGVIGVIGV

Plaint Text: THEBOYHASTHEBALL

Cipher Text: OPKWWECIYOPKWIRG

Here, generally, we repeatedly write key above the plaintext and use the Caesar cipher for each letter in the plaintext where key for each letter being processed is taken from the repeated key letter just above it. This process is simplified by using the table as below called Tableau

Plaintext \ Key Word	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	V
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	W
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	X
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

Figure 1.5: Vigenere Ciphers

Period: length of key. In example above it is 3.

Tableau: Table used to encipher and decipher. In tableau Vigènere cipher has key letters on top, plaintext letters on the left or vice versa. It is also possible to have key on top (left) plaintexts in middle and ciphertexts in left (top).

Assuming key on top and the plaintext on left, Decryption is performed by finding the position of the ciphertext letter in a column, corresponding to the key letter, of the table, and then taking the label of the row in which it appears as the plaintext letter. For example, in column V (key letter), the ciphertext letter O appears in row T, which taken as the first plaintext letter. The second letter is decrypted by looking up P in column I of the table; it appears in row H, which is taken as the plaintext letter. This process continues until we find the plaintext letters for all the ciphertext letters.

TRANSPOSITION CIPHER

In transposition ciphers the letters are systematically arranged so that the actual position of letters is gets changed making the text garble.

RAIL-FENCE CIPHER

The Rail Fence Cipher is a form of transposition cipher that derives its name from the way in which it is encoded. In the rail fence cipher, the plaintext is written downwards and diagonally on successive "rails" of an imaginary fence, then moving up when we reach the bottom rail. When we reach the top rail, the message is written downwards again until the whole plaintext is written out. The message is then read off in rows.

For Example, if we have 3 "rails" and a message of THIS IS THE PLAINTEXT, the cipherer writes out (we are not showing diagonal move here just write in down rail a step ahead):

T S T P I E

H I H L N X

I S E A T T

The ciphertext is T S T P I E H I H L N X I S E A T T

The problem with Rail Fence Cipher is that the rail fence cipher is not very strong; the number of practical keys is small enough that a cryptanalyst can try them all by hand. To decrypt we get the number of letters to be skipped. For this if the number of rail is n key is $\lceil total\ letters\ in\ ciphertext\ /\ n \rceil$ so in our e.g. n = 3 and key is 18/3 = 6 i.e. skip 6 letters from the letter you are reading every time to get plaintext (remember to go circular that is if count ends continue from the starting letter leaving the read letter). See below:

T	S	T	P	I	E	H	I	H	L	N	X	I	S	E	A	T	T
1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6

We have selected letter with index 1 THI. Now choose the letter with index 2, see below

T	S	T	P	I	E	H	I	H	L	N	X	I	S	E	A	T	T
1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6

Continue like this until you read off all the characters.

Example: *Encrypt the message "ATTAK AT DOWN" using rail-fence cipher where rail = 3.*

Solution:

a				c				d			
	t		a		k		t		a		n
		t				a				w	

Now, ciphertext a c d t a k t a n t a w

MODERN CIPHERS

Block vs. Stream Ciphers

Stream Cipher

Let E be an encipherment algorithm, and let $E_k(b)$ be the encipherment of message b with key k. Let a message $m = b_1b_2 \ldots$, where each b_i is of a fixed length, and let $k = k_1k_2 \ldots$. Then a stream cipher is a cipher for which $E_k(m) = E_{k1}(b_1)E_{k2}(b_2) \ldots$. If the key stream k of a stream cipher repeats itself, it is a periodic cipher and the length of its period is one cycle of $k_1k_2 \ldots$

Block Cipher: Let E be an encipherment algorithm, and let $E_k(b)$ be the encipherment of message b with key k. Let a message $m = b_1b_2 \ldots$, where each b_i is of a fixed length. Then a block cipher is a cipher for which $E_k(m) = E_k(b_1)E_k(b_2) \ldots$

Examples: Vigenère cipher has b_i = 1 character, $k = k_1k_2 \ldots$where k_i = 1 character and each b_i is enciphered using k_i mod length(k)[stream cipher]. Data Encryption Standard has b_i = 64 bits, k = 56 bits and each b_i enciphered separately using k [block cipher].

Advantages of Stream Ciphers

- **Speed of transformation.** Because each symbol is encrypted without regard for any other plaintext symbols, each symbol can be encrypted as soon as it is read. Thus, the time to encrypt a symbol depends only on the encryption algorithm itself, not on the time it takes to receive more plaintext.
- **Low error propagation.** Because each symbol is separately encoded, an error in the encryption process affects only that character.

Disadvantages of Stream Ciphers

- **Low diffusion.** Each symbol is separately enciphered. Therefore, all the information of that symbol is contained in one symbol of the ciphertext.
- **Susceptibility to malicious insertions and modifications.** Because each symbol is separately enciphered, an active interceptor who has broken the code can splice together pieces of previous messages and transmit a spurious new message that may look authentic.

Advantages of Block Ciphers

- **High diffusion.** Information from the plain-text is diffused into several ciphertext symbols. One ciphertext block may depend on several plaintext letters.
- **Immunity to insertion of symbols.** Because blocks of symbols are enciphered, it is impossible to insert a single symbol into one block. The length of the block would then be incorrect, and the decipherment would quickly reveal the insertion.

Disadvantages of Block Ciphers

- **Slowness of encryption.** The person or machine using a block cipher must wait until an entire block of plaintext symbols has been received before starting the encryption process.
- **Error propagation.** An error will affect the transformation of all other characters in the same block.

SYMMETRIC VS. ASYMMETRIC CIPHERS

Symmetric Ciphers: Symmetric cipher often known as private key cryptography or secret key cryptography is an approach of cryptography where a single same private key is used during both of the encryption and decryption process. The sender and reciever of the message should have shared the pivate key. The examples of symmetric ciphers are Caeser cipher, Data Encryption Standard (DES) etc.

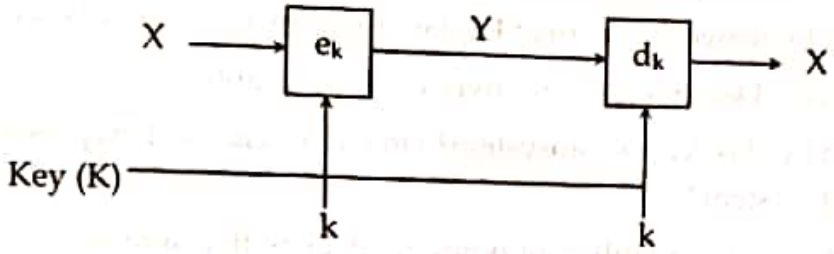

Figure 1.6: Symmetric Cipher REDRAW

Assymetric Ciphers: Assymmetric cipher often known as public key is an approach of cryptography where two different keys are used during process of encryption and decryption. A public key, known to all, is used to encrypt the input message and a private key, which is secret, is used to decrypt the original message from the ciphertext. All of the communicating parties in network should have their pair of public and private keys. The public key is disclosed to others while private key is kept secret. While sending an encrypted message, the sender will encrypt the message using reciever public key and the reciever, upon receiving the ciphertext, will decrypt the message using his/her own private key. The examples of assymmetric ciphers are RSA, Elliptic Ciphers etc.

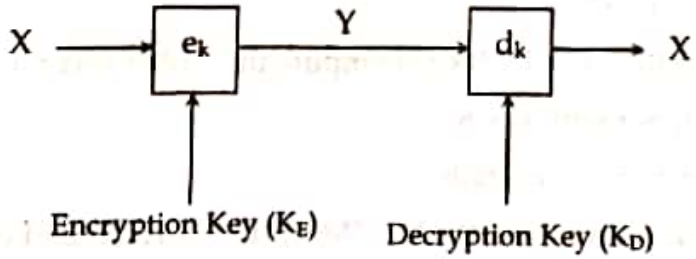

Figure 1.7: Assymetric Cipher

Symmetric v/s Asymmetric Cryptography

	Secret Key (Symmetric)	Public Key (Asymmetric)
Number of keys	1	2
Protection of key	Must be kept secret	One key must be kept secret; the other can be freely exposed
Best uses	Cryptographic workhorse; secrecy and integrity data—single characters to blocks of data, messages, files	Key exchange, authentication
Key distribution	Must be out-of-band	Public key can be used to distribute other keys
Speed	Fast	Slow; typically, 10,000 times slower than secret key

Discussion Exercise

1. What do you mean by computer security? Explain
2. Explain information security with its importance.
3. What do you mean by network security? Explain the threats to network security.
4. What is cryptosystem? Describe the objectives of cryptography.
5. What do you mean by classical cryptosystem? How does classical cryptosystem differ from modern cryptosystem?
6. Define the term attack. Explain different types of attack with example.
7. List and briefly explain types of cryptographic attacks based on attacker.
8. What is stream cipher? Explain the characteristics of stream cipher.
9. Differentiate between stream cipher and b lock cipher.
10. What is symmetric cipher? How does symmetric cipher differ from asymmetric cipher? Explain with block diagram.
11. How does monoalphabetic substitution differs from polyalphabetic substitutions.
12. Describe the two building blocks of all classical ciphers.
13. Explain the importance of CIA triads.
14. Construct playfair matrix with the key "KEYWORD". Using this matrix encrypt the message "CRYPTOGRAPHY".
15. Given a plaintext "ABRA KA DRBRA" compute the cipher text for
    i. The ceaser cipher with key 8
    ii. The railfence cipher with rails=3
16. Construct a play fair matrix with the key "MATHEMATICS" and encrypt the message "FINITE STATE AUTOMATA"
17. Given a plaintext "ARTIFICIAL NEURAL NETWORK" , compute the ciphertext for
    i. The shift cipher with key=5
    ii. The railfence cipher with rails =4
18. Encrypt the message " ATTACK AT DOWN" using the hill cipher with the key $\begin{pmatrix} 2 & 5 \\ 9 & 5 \end{pmatrix}$