UNIT IV

4 Introduction to Network Security

Syllabus

Importance and Need for Security, Network Attacks- Passive, Active Network Security Threats : *Unauthorized access, Distributed Denial of Service (DDoS) attacks, Man in the middle attacks,* ***Concept of Security Principles :*** *Confidentiality and Privacy, Authentication, Authorization and Access Control, Integrity, Non- repudiation, Stream Ciphers : Substitution Cipher - Mono alphabetic Cipher, Polyalphabetic Substitution Cipher., Transposition Cipher : Rail-Fence*

Block Ciphers modes : *Electronic Code Book (ECB) Mode., Cipher Block Chaining (CBC) Mode., Cipher Feedback Mode (CFB) , Output Feedback (OFB) Mode.*

Contents

4.1 Need of Security

- Following are the examples of security violations :
  1. User A transmits a sensitive information file to user B. The unauthorised user C is able to monitor the transmission and capture a copy of the file during its transmission.
  2. A message is sent from a customer to a stockbroker with instructions for various transactions. Subsequently, the investments lose value and the customer denies sending the message.
  3. While transmitting the message between two users, the unauthorised user intercepts the message, alters its contents to add or delete entries and then forwards the message to destination user.
- Security is required because the widespread use of data processing equipment, the security of information felt to be valuable to an organization was provided primarily by physical and administrative means.
- Network security measures are needed to protect data during their transmission.

4.1.1 Business Needs

- Information security performs **four** important organizational functions :
  1. Protects the organization's ability to function.
  2. Safe operation of organizations applications in IT systems.
  3. Protection of organization data.
  4. Safeguards the technology assets in use at the organization.
- Protecting the functionality of an organization : Information security is implemented in organization by IT department management and general management. In some private organization and government offices, some manager level officers are not interested in implementing security because of complex process.
- Enabling the safe operation applications : Some of the resources that important in the organizations. These resources operating system, electronic mail and hardware resources. Organization must provide the security to these resources.
- Protection of organization data : Data is important in any organization. The value of data motivates attackers to steal, delete, or corrupt it. An effective information security program directed by management is essential to the protection of the integrity and value of the organization's data.
- Safeguarding technology assets in organizations : An organization must add secure infrastructure services matching the size and scope of the enterprise. As the

organization's network grows to accommodate changing needs, it may need more robust technology solutions.

4.2 Security Threats

- 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 a vulnerability.
- Threat refers to the source and means of a particular type of attack. A threat assessment is performed to determine the best approaches to securing a system against a particular threat, or class of 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.
- Penetration testing exercises are substantially focused on assessing threat profiles, to help one develop effective countermeasures against the types of attacks represented by a given threat.
- Where risk assessments focus more on analysing the potential and tendency of one's resources to fall prey to various attacks, threat assessments focus more on analysing the attacker's resources.
- Analysing threats can help one develop specific security policies to implement in line with policy priorities and understand the specific implementation needs for securing one's resources.
- Threats come in many forms, depending on their mode of attack. From viruses to trojans, spyware and bots, threats have evolved into sophisticated programs intended to harm computers.

Threat Types	Examples
Compromises to intellectual property.	Piracy, copyright infringement.
Software attacks.	Viruses, worms, macros, DoS.
Deviations in quality of service.	ISP, power, WAN service issues from service providers.
Espionage or trespass.	Unauthorized access and/or data collection.
Forces of nature.	Fire, flood, earthquake, lightning.
Acts of human error or failure.	Accidents, employee mistakes.

4.2.1 Deliberate Software Attacks

- Deliberate software attacks occur when an individual or group designs and deploys software to attack a system. Most of this software is referred to as malicious code or malicious software, or sometimes malware.
- The generic term for threats is malicious software or malware. Malware is software designed to cause damage to or use up the resources of a target computer.
- These threat can be divided into two categories those that need a host program, and those that are independent. Which requires host programs are essentially fragments of programs that cannot exist independently of some actual application program, utility or system program.
- Second category i.e. independent programs are self-contained programs that can be scheduled and run by the operating system.

1. Virus

- A virus is a block of code that inserts copies of itself into other programs. A virus generally carries a payload, which may have nuisance value, or serious consequences. To avoid early detection, viruses may delay the performance of functions other than replication.
- Virus is one type of system threats.
- A virus is any unauthorized program that is designed to gain access to a computer system. Viruses need other programs to spread. Due to its spreading nature, a virus can cause severe damage to a system.
- E-mail viruses : If the recipient opens the email attachment, the Word Macro is activated. The e-mail virus sends itself to everyone on the mailing list in the user's e-mail package. The virus does local damage.
- The first rapidly spreading e-mail viruses, such as Melissa, made use of a Microsoft Word Macro embedded in an attachment.
- Parasitic virus : A parasitic virus attaches itself to executable files and replicates, when the infected program is executed, by finding other executable files to infect.
- Memory-resident virus : Lodges in main memory as part of a resident system program. From that point on, the virus infects every program that executes.
- Boot sector virus : Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus.
- Stealth virus : A form of virus explicitly designed to hide itself from detection by antivirus software.

- Polymorphic virus : A virus that mutates with every infection, making detection by the signature of the virus impossible.
- Metamorphic virus : A metamorphic virus rewrites itself completely at each iteration, increasing the difficulty of detection. Metamorphic viruses may change their behavior as well as their appearance.

2.Worm

- Worm is a program that replicates itself by installing copies of itself on other machines across a network.
- An e-mail virus has some of the characteristics of a worm because it propagates itself from system to system.
- Network worm programs use network connections to spread from system to system. To replicate itself, a network worm uses some sort of network vehicle.

3.Trojan Horse

- Trojan horse is a virus that's disguised as a legitimate or harmless program that sometimes carries within itself the mean to allow the programs creator to secretly access the users system.
- Trojan horse attack may either be passive or active depending on the activities performed by the clandestine code.
- For example, if the clandestine code simply steals information then it is of the **passive** type. But if it does something more harmful like destroying or corrupting files, then it is of the **active** type. A variation of the Trojan horse is a program that emulates a login program.

4.Trap Door

- Secret undocumented entry point into a program used to grant access without normal methods of access authentication.
- Trap doors have been used legitimately for many years by programmers to debug and test programs.
- Trap door can be caused by a flow in the system design or they can be installed there by a system programmer for future use. Trap door including backdoor passwords are unspecified and non-documented entry points to the system. A clever trap door could be included in a compiler.
- The compiler could generate standard object code as well as a trap door regardless of the source code being compiled. Trap door may also be an incorporated into the system by a destructive virus or by a Trojan horse program. Trap door is one type of program threat

4.2.2 Deviations in Quality of Service

- **Internet Service Issues :** Most of the organizations uses the Internet and the World Wide Web to support continued operations, Internet service provider failures can considerably undermine the availability of information.
- **Power Irregularities :** Irregularities from power utilities are common and can lead to fluctuations such as power excesses, power shortages and power losses. This can pose problems for organizations that provide inadequately conditioned power for their information systems equipment.
- Cyber espionage is a form of cyber attack that steals classified, sensitive data or intellectual property to gain an advantage over a competitive company or government entity.
- Types of industrial espionage,
  a) Trespassing onto a competitor's property or accessing their files without permission
  b) Posing as a competitor's employee in order to learn company trade secrets or other confidential information
  c) Wiretapping a competitor
  d) Hacking into a competitor's computers
  e) Attacking a competitor's website with malware.

4.3 Model of Network Security

- A message is to be transferred from source to destination across some sort of internet. Both the sides must cooperate for the exchange of the data.
- A logical information channel is established by defining a route through the internet from source to destination.
- All the techniques for providing security have two components :
  1. A security related transformation on the information to be sent.
  2. Some secret information shared by the two principles, it is hoped, unknown to the opponent.
- Fig. 4.3.1 shows the network security model.
- A trusted third party is needed to achieve secure transmission.
- Basic tasks in designing a particular security service.
  1. Design an algorithm for performing the security related transformation.
  2. Generate the secret information 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 principles that makes use of the security algorithm and the secret information to achieve a particular security service.

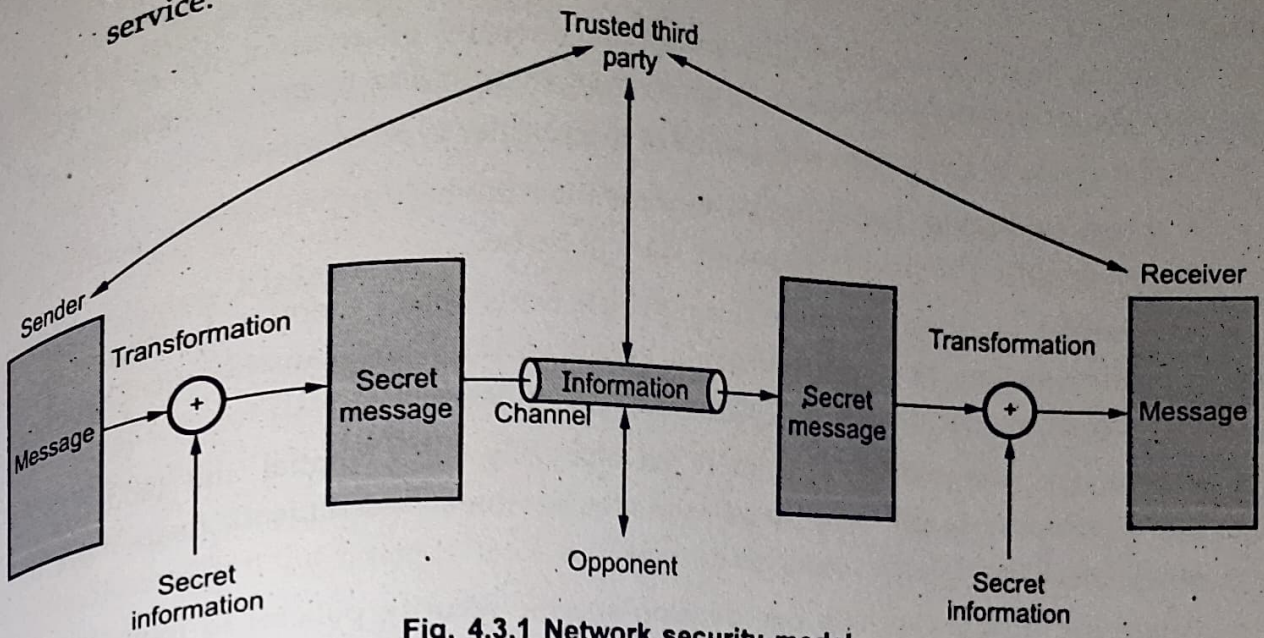


Fig. 4.3.1 Network security model

4.4 Security Attacks

- Computer based systems have three valuable components : **Hardware, software and data.**
- Securities of these components are evaluated in terms of vulnerability, threats, attacks and control.
- An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system.

Asset

- Asset means people, property and information.
- People may include employees and customers along with other invited persons such as contractors or guests.

Vulnerability

- Vulnerability refers to the security flaws in a system that allows an attack to be successful.
- Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset. Vulnerability is a weakness or gap in our protection efforts.

- **Example :** In design, implementation or procedure, that might be exploited to cause loss or harm.

Threat

- Anything that can exploit vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset. A threat is what we're trying to protect against.
- Threat refers to the source and means of a particular type of attack.
- A threat assessment is performed to determine the best approaches to securing a system against a particular threat, or class of 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.
- Where risk assessments focus more on analyzing the potential and tendency of one's resources to fall prey to various attacks, threat assessments focus more on analyzing the attacker's resources.
- Analyzing threats can help one develop specific security policies to implement in line with policy priorities and understand the specific implementation needs for securing one's resources.
- Threats come in many forms, depending on their mode of attack. From viruses to trojans, spyware and bots, threats have evolved into sophisticated programs intended to harm computers.

Risk

- The potential for loss, damage or destruction of an asset as a result of a threat exploiting vulnerability. Risk is the intersection of assets, threats, and vulnerabilities.
- The formula used to determine risk is

$$\text{Risk} = \text{Asset} + \text{Threat} + \text{Vulnerability}$$

$$R = A + T + V$$

- Risk is a function of threats exploiting vulnerabilities to obtain damage or destroy assets. Thus, threats may exist, but if there are no vulnerabilities then there is little/no risk.
- Similarly, you can have vulnerability, but if you have no threat, then you have little/no risk.

Control

- Control is used as proactive measure. Control is a action, device, procedure, or technique that removes or reduces a vulnerability.
- A threat is blocked by control of vulnerability.

- Interception, interruption, modification and fabrication are the system security threats.

4.5 Types of Security Attacks

- An attempt to gain unauthorized access to information resource or services, or to cause harm or damage to information systems.
- Security attacks are of two types : Passive attack and Active attack

4.5.1 Passive Attack

- Passive attacks are those, wherein the attacker indulges in eavesdropping on, or monitoring of data transmission. A passive attack attempts to learn or make use of information from the system but does not affect system resources.
- 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.
- **Passive attacks** are of two types :
  1. Release of message contents 2. Traffic analysis
- **Release of message content** is shown in Fig. 4.5.1. 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 content of these transmissions.

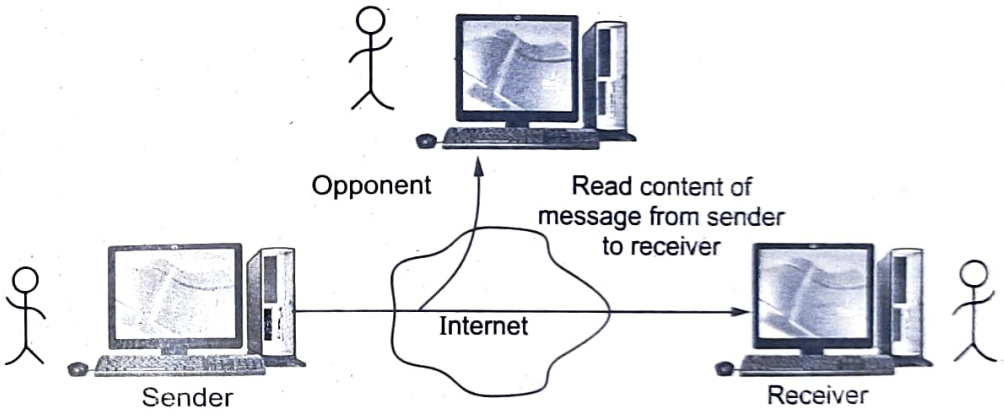


Fig. 4.5.1 Release of message contents

- **Traffic analysis :** Mask the contents of message so that opponents could not extract the information from the message. Encryption is used for masking Fig. 4.5.2 shows the traffic analysis.
- Passive attacks are very difficult to detect because they do not involve any alternation of data. It is feasible to prevent the success of attack, usually by means of encryption.

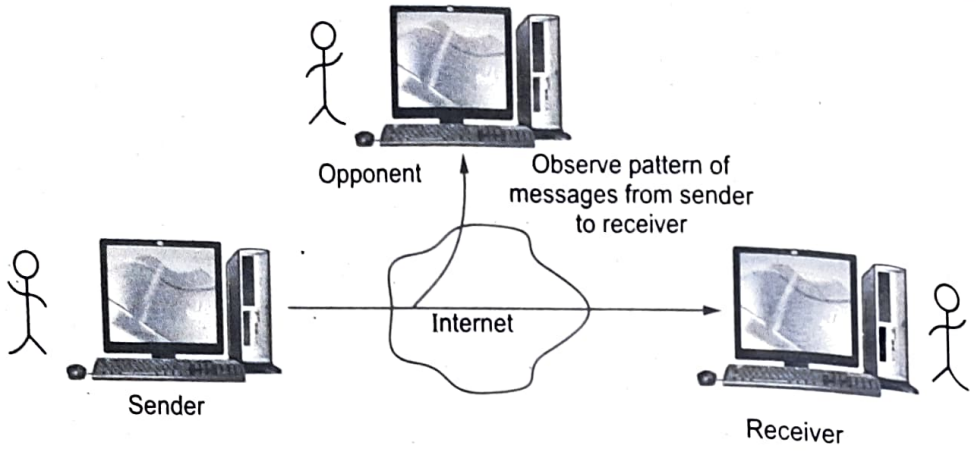


Fig. 4.5.2 Traffic analysis

4.5.2 Active Attack

- Active attacks involve some modification of the data stream or the creation of a false stream. These attacks can not be prevented easily.
- Active attacks can be subdivided into four types :
  1. Masquerade
  2. Replay
  3. Modification of message
  4. Denial of service

1. Masquerade

- It takes place when one entity pretends to be a different entity. Fig. 4.5.3 shows masquerade.

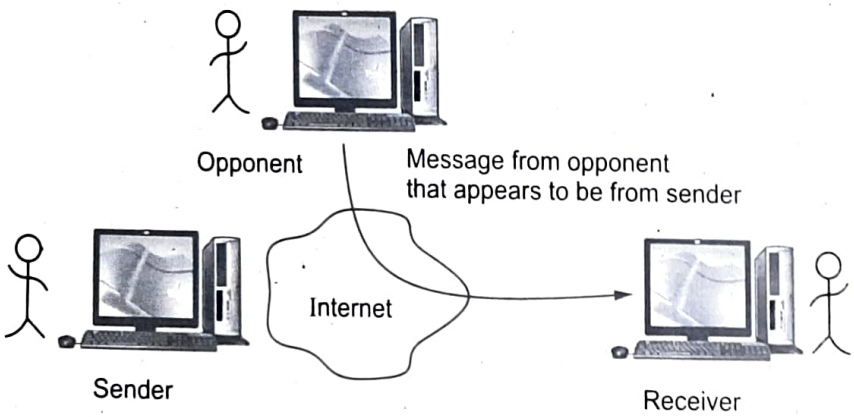


Fig. 4.5.3 Masquerade

- **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.
- **Interruption** attacks are called as masquerade attacks.

2. Replay

- It involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
- Fig. 4.5.4 shows replay attack.

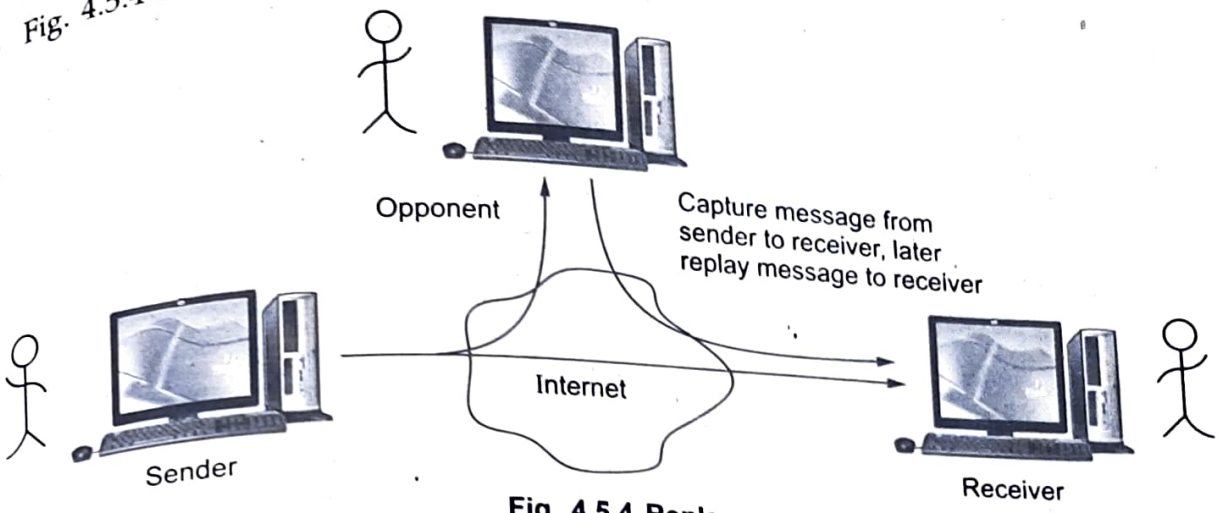


Fig. 4.5.4 Replay

3. Modification of message

- It involves some change to the original message. It produces an unauthorized effect. Fig. 4.5.5 shows the modification of message.
- For example, a message meaning "Allow Rupali Dhotre to read confidential file accounts " is modified to mean "Allow Mahesh Awati to read confidential file accounts".

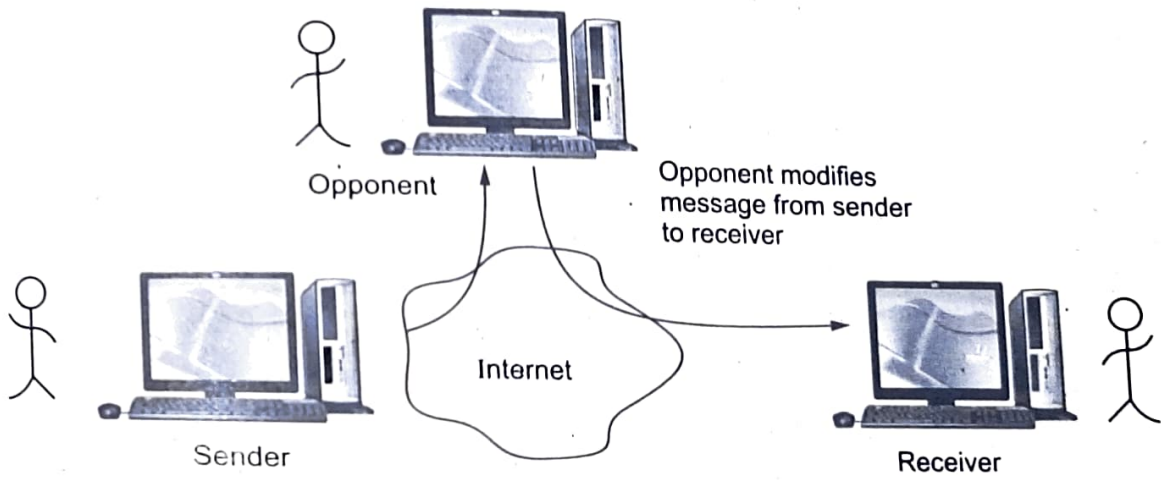


Fig. 4.5.5 Modification of message

4. Denial of service

- Fabrication causes Denial Of Service (DOS) attacks.
- DOS prevents the normal use or management of communications facilities.

- 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.
- Fig. 4.5.6 shows denial of service attack.

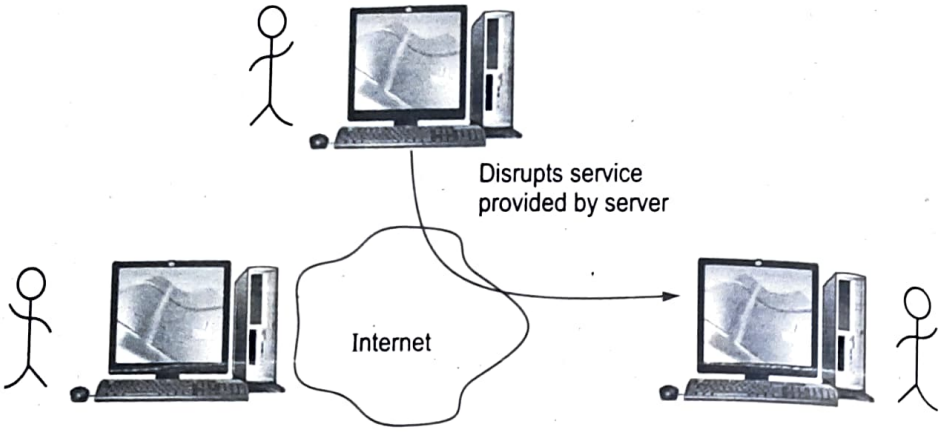


Fig. 4.5.6 Denial of service

- It is difficult to prevent active attack because of the wide variety of potential physical, software and network vulnerabilities.
- The first type of DOS attacks were single source attacks, meaning that a single system was used to attack another system and cause something on that system to fail. SYN flood is the most widely used DOS attack.
- Fig. 4.5.7 shows the SYN flood DOS attack.

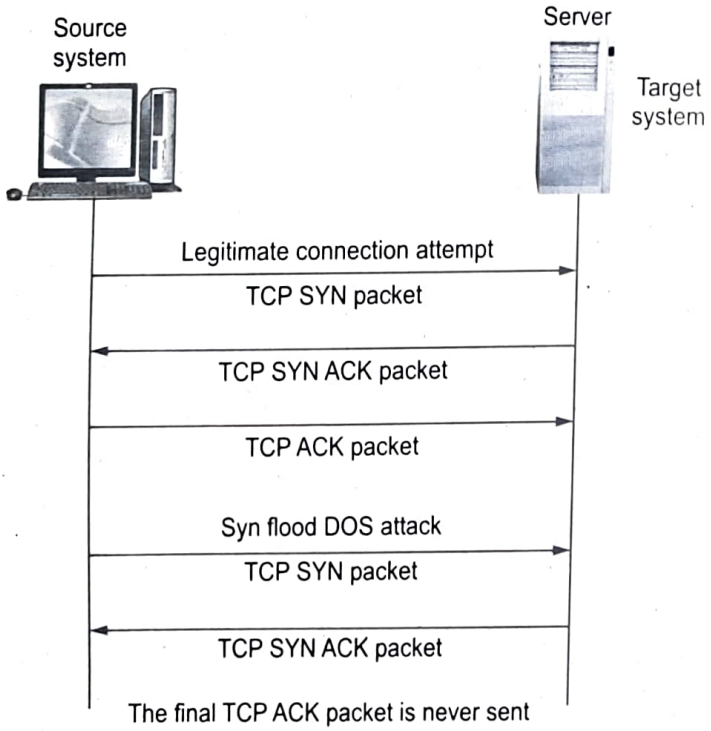


Fig. 4.5.7 SYN flood DOS attack

- Source system sends a large number of TCP SYN packets to the target system. The SYN packets are used to begin a new TCP connection.
- When the target receives a SYN packet, it replies with TCP SYN ACK packet, which acknowledges the SYN packet and sends connection setup information back to the source of the SYN.
- The target also places the new connection information into a pending connection buffer.
- For a real TCP connection, the source would send a final TCP ACK packet when it receives the SYN ACK.
- However, for this attack, the source ignores the SYN ACK and continues to send SYN packets. Eventually, the target's pending connection buffer fills up and it can no longer respond to new connection requests.

4.5.2.1 Difference between Passive and Active Attack

Sr. No.	Passive attacks	Active attacks
1.	Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions.	Active attacks involve some modification of the data stream or the creation of a false stream.
2.	**Types :** Release of message contents and traffic analysis	**Types :** Masquerade, replay, modification of message and denial of service.
3.	Very difficult to detect.	Easy to detect.
4.	The emphasis in dealing with passive attacks is on prevention rather than detection.	It is quite difficult to prevent active attacks absolutely.
5.	It does not affect the system.	It affects the system.

4.5.3 Man-in-the-Middle Attack

- In cryptography, a **Man-In-The-Middle (MITM) attack** is an attack in which an attacker is able to read, insert and modify at will, meassages between two parties without either party knowing that the link between them has been compromised.
- The attacker must be able to observe and intercept messages going between the two victims. The MITM attack can work against public-key cryptography and is also particularly applicable to the original Diffie-Hellman key exchange protocol, when used without authentication.

- The MITM attack may include one or more of
  1. Eavesdropping, including traffic analysis and possibly a known-plaintext attack.
  2. Chosen ciphertext attack, depending on what the receiver does with a message that it decrypts.
  3. Substitution attack
  4. Replay attacks
  5. Denial of service attack. The attacker may for instance jam all communications before attacking one of the parties. The defense is for both parties to periodically send authenticated status messages and to treat their disappearance with paranoia.
- MITM is typically used to refer to active manipulation of the meassages, rather than passively eavesdropping.

Example of a successful MITM attack against public-key encryption

- Suppose Alice wishes to communicate with Bob and that Mallory wishes to eavesdrop on the conversation, or possibly deliver a false message to Bob. To get started. Alice must ask Bob for his public key. If Bob sends his public key to Alice, but Mallory is able to intercept it, a man-in-the-middle attack can begin.
- Mallory can simply send Alice a public key for which she has the private, matching, key. Alice, believing this public key to be Bob's, then encrypts her message with Mallory's key and sends the enciphered message back to Bob.
- Mallory again intercepts, deciphers the message, keeps a copy, and reenciphers it using the public key Bob originally sent to Alice. When Bob receives the newly enciphered message, he will believe it came from Alice.
- This example shows the need for Alice and Bob to have some way to ensure that they are truly using the correct public keys of each other. Otherwise, such attacks are generally possible in principle, against any message sent using public-key technology.

Defenses against the attack

- The possibility of a man-in-the-middle attack remains a serious security problem even for many public-key based cryptosystems. Various defenses against MITM attacks use authentication techniques that are based on :
  1. Public keys
  2. Stronger mutual authentication
  3. Secret keys (high information entropy secrets)
  4. Passwords (low information entropy secrets)
  5. Other criteria, such as voice recognition or other biometrics

- The integrity of public keys must generally be assured in some manner, but need not be secret, whereas passwords and shared secret keys have the additional secrecy requirement. Public keys can be verified by a Certificate Authority, whose public key is distributed through a secure channel.

4.6 Security Services

- X.800 defines a security service as a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers.
- X.800 divides security services into five different categories.
  1. Authentication
  2. Access control
  3. Data confidentiality
  4. Data integrity
  5. Nonrepudiation

1. Authentication

- Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In public and private computer network, authentication is commonly done through the use of login passwords.
- Two specific authentication services are defined in X.800 :
  a. Peer entity authentication
  b. Data origin authentication
- **Peer entity authentication** used in association with a logical connection to provide confidence in the identity of the entities connected.
- Data origin outhentication enables the recepient to verify that the message have not been tempered in transit (data integrity) and they originally from expected sender (authenticity).
- **Data origin authentication** 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.

2. Access control

- It is the ability to limit and control the access to host systems and applications via communications links.
- This service controls who can have access to a resource.

3. Data confidentiality

- Confidentiality is the concealment of information or resources. It is the protection of transmitted data from passive attacks.
- Confidentiality is classified into
  1. **Connection confidentiality :** The protection of all user data on a connection.
  2. **Connectionless confidentiality :** The protection of all user data in a single data block.
  3. **Selective field confidentiality :** The confidentiality of selected fields within the user data on a connection or in a single data block.
  4. **Traffic flow confidentiality :** The protection of the information that might be derived from observation of traffic flows.

4. Data integrity

- Integrity can apply to a stream of messages a single message or selected fields within a message.
- Modification causes loss of message integrity.
- Data integrity can be classified as
  1. Connection integrity with recovery
  2. Connection integrity without recovery
  3. Selective field connection integrity
  4. Connectionless integrity
  5. Selective field connectionless integrity
- 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 within an entire data sequence with recovery attempted.
- Connection integrity without recovery provides only detection without recovery.
- Selective field connection integrity provides for the integrity of selected fields within the user data of a data block transferred over a connection.
- Connectionless integrity provides for the integrity of a single connectionless data block and may take the form of detection of data modification.

5. Nonrepudiation

- Nonrepudiation prevents either sender or receiver from denying a transmitted message.
- When a message is sent, the receiver can prove that the alleged sender in fact sent the message.

- When a message is received, the sender can prove that the alleged receiver in fact received the message.

4.7 Security Mechanism

- A mechanism that is designed to detect, prevent, or recover from a security attack.
- Security mechanisms are technical tools and techniques that are used to implement security services. A mechanism might operate by itself, or with others, to provide a particular service.
- Security mechanisms defined by X.800 are given below:

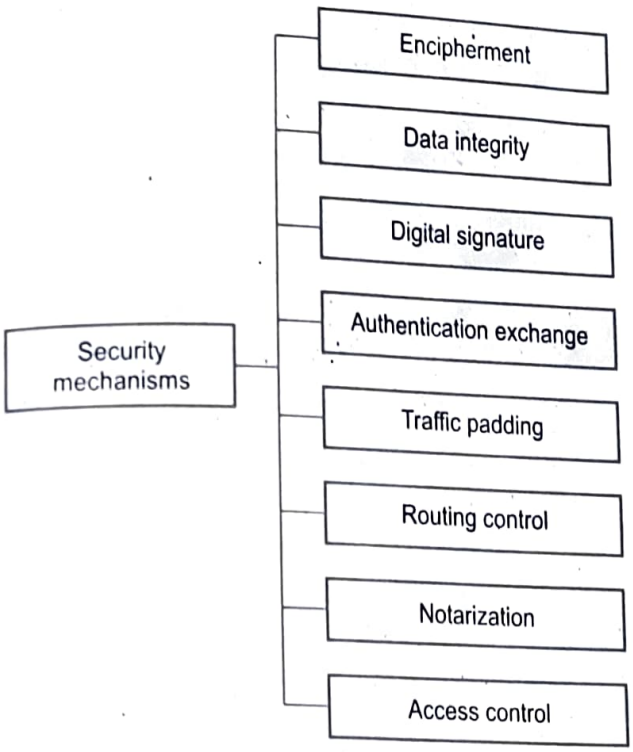


Fig. 4.7.1

- X.800 defined security mechanisms as follows

1. **Specific security mechanisms :** May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

a. **Encipherment :** The use of mathematical algorithms to transform data into a form that is not readily intelligible.

b. **Digital signature :** Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity the data unit and protect against forgery.

c. **Access control :** A variety of mechanisms that enforce access rights to resources.

d. **Data integrity :** A variety of mechanisms used to ensure the integrity of a data unit or stream of data units.

e. **Authentication exchange :** A mechanism intended to ensure the identity of an entity by means of information exchange.

f. **Traffic padding :** The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

g. **Notarization :** The use of a trusted third party to assure certain properties of a data exchange.

2. **Pervasive security mechanisms :** Mechanisms that are not specific to any particular OSI security service or protocol layer.

a. **Trusted functionality :** That which is perceived to be correct with respect to some criteria.

b. **Event detection :** Detection of security relevant events.

c. **Security label :** The marking bound to resource that names or designates the security attributes of that resource.

d. **Security recovery :** Deals with requests from mechanisms, such as event handling and management functions and takes recovery actions.

4.8 Access Control

- Access control is an important tool of security to protect data and other resources. The access control mechanism refers to prevention of unauthorized use of a resource.
- Access control includes :
  1. Authentication of users
  2. Authorization of their privileges
  3. Auditing to monitor and record user actions
- Three types of access controls system are :
  1. Discretionary access control
  2. Mandatory access control
  3. Role-based access control
- A password scheme used to allow access to a user's computer account may be viewed as the simplest instance of an access control matrix : each resource has a list of identities associated with it (e.g. a computer account which authorized entities may access), and successful corroboration of an identity allows access to the authorized resources as listed for that entity.

- The simplest framework for describing a protection system is the access control matrix model. Two fundamental concepts in field authorization are :
  1. Access Control Lists (ACLs) 2. Capabilities (C-lists)

ACLs and Capabilities Lists

- Access Control List (ACL) is a set of rules that define security policy. These ACLs contain one or more Access Control Entries (ACEs), which are the actual rule definitions themselves.
- These rules can restrict access by specific user, time of day, IP address, function (department, management level, etc.), or specific system from which a logon or access attempt is being made.
- Access control matrix is easy to implement. Access matrix contains row and columns. Row is represented by domains and columns represents by objects. Each entry in the matrix consists of a set of access rights.
- The intersection of the row and column contains the access rights for that subject to that objects. Following table shows access control matrix/ protection matrix. Each cell in the matrix specifies the actions that a subject can perform on an object.

4.8.1 Discretionary Access Control (DAC)

- When user set an access control mechanism to allow or deny access to an object (system resource), such a mechanism is a Discretionary Access Control (DAC).
- The Discretionary Access Control (DAC) is also called as an Identity-Based Access Control (IBAC). A DAC policy is a means of assigning access rights based on rules specified by users. Data owners can define access permissions for specific users or groups of users .
- Discretionary Access Control List (DACL) determines which users and groups can access the object (system resource) for operations. It consists of a list of Access Control Entries (ACEs).
- Access permissions for each piece of data are stored in an Access-Control List (ACL). This list can be generated automatically when a user grants access to somebody or can be created by an administrator.
- An ACL includes users and groups that might access data and levels of access they might have. An ACL can also be enforced by a system administrator. In this case, the ACL acts as a security policy, and regular users can't edit or overrule it.
- The DAC is the least restrictive model as compared to the other types because the owner of the list can transfer authenticated access to other users. The end-users have complete control over the system and can determine the access type of other users and transfer ownership.

4.8.2 Mandatory Access Control (MAC)

- When a system mechanism controls access to an object and an individual user cannot alter that access, then such a control is called as Mandatory Access Control (MAC).
- Mandatory Access Control (MAC) is also called as rule-based access control.
- Mandatory access control is a more restrictive scheme that does not allow users to define permissions on files, regardless of ownership. Instead, security decisions are made by a central policy administrator.
- Each security rule consists of a subject, which represents the party attempting to gain access, an object, referring to the resource being accessed, and a series of permissions that define the extent to which that resource can be accessed.
- MAC is used by many governments to secure classified information and to support multilevel security policies and applications. This access control model is mostly used by government organizations, militaries, and law enforcement institutions.
- It is reasonable to use MAC in organizations that value data security more than operational flexibility and costs. Implementing MAC in a private organization is rare because of the complexity and inflexibility of such a system.
- A pure MAC model provides a high and granular level of security. On the other hand, it's difficult to set up and maintain. That's why it's common to combine MAC with other access control models.
- For example, combining it with the role-based model speeds up the configuration of user profiles. Instead of defining access rights for each user, an administrator can create user roles. Each organization has users with similar roles and access rights : employees with the same job position, third-party vendors, etc. An administrator can configure roles for these groups instead of configuring individual user profiles from scratch.
- Another popular combination is MAC and the discretionary access control model. MAC can be used to secure sensitive data, while DAC allows co-workers to share information within a corporate file system.

4.8.3 Role-Based Access Control (RBAC)

- A user is an entity that wishes to access resources of the organization to perform a task. Usually, users are actual human users, but a user can also be a machine or application.
- RBAC entails mapping the different "roles" in an organizational hierarchy and defining a profile of access permissions to the network's resources for each role.

Then each user is assigned one or more roles, providing him/her with the access permissions defined by those roles.

- A user with super-user access may be classified in every role, whereas someone with less need-to know may be classified in only one or two roles.
- A role is defined as a collection of users with similar functions and responsibilities in the organization. Examples of roles in a university may include "student," "alum," "faculty," "dean," "staff," and "contractor." In general, a user may have multiple roles.
- Roles and their functions are often specified in the written documents of the organization.
- The assignment of users to roles follows resolutions by the organization, such as employment actions (e.g. hiring and resignation) and academic actions (e.g., admission and graduation).
- Role-Based Access Control (RBAC) is a method of regulating access to computer or network resources based on the roles of individual users within an enterprise.
- In RBAC, the rights and permissions are assigned to roles instead of individual users.
- RBAC is also called as Non-Discretionary Access Control (NDAC). This added layer of abstraction permits easier and more flexible administration and enforcement of access controls

4.9 Substitution Cipher Techniques

- A substitution cipher changes characters in the plaintext to produce to ciphertext. 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.

4.9.1 Caesar Cipher

- Caesar cipher is a special case of substitution techniques wherein each alphabet in a message is replaced by an alphabet three places down the line.
- Caesar cipher is susceptible to a statistical ciphertext only attack.
- For example,

Plaintext	hellow world
Ciphertext	KHOOR ZRUOG

- List of all possible combination of letters.

Plain	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
Cipher	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V

Plain	t	u	v	w	x	y	z
Cipher	W	X	Y	Z	A	B	C

- Numerical equivalent to each letter is given below.

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

- 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

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

where K = Values from 1 to 25

- The decryption algorithm is simply

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

- If it is known that a given ciphertext is a Caesar cipher, then a brute force cryptanalysis is easily performed : Simply try all the 25 possible keys.
- **Demerits :**

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.

4.9.2 Monoalphabetic Cipher

- Monoalphabetic cipher substitutes one letter of the alphabet with another letter of the alphabet. However, rather than substituting according to a regular pattern, any letter can be substituted for any other letter, as long as each letter has a unique substitute left and vice versa.

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m
Ciphertext	m	n	b	v	c	x	z	a	s	d	f	g	h

Plaintext	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	j	k	l	p	o	i	u	y	t	r	e	w	q

For example

Plaintext message : hello how are you

Ciphertext message : acggk akr moc wky

- Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet.

Homophonic substitution cipher

- It provides multiple substitutes for a single letter. For example, A can be replaced by D, H, P, R; B can be replaced by E, Q, S, T etc.

4.9.3 Playfair Cipher

- The playfair algorithm is based on the use of a 5 × 5 matrix of letters constructed using a keyword.
- **For example :** Monarchy is the keyword.

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

- The matrix is constructed by filling in the letters of the keyword 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.
- The letters I and J count as one letter.

4.9.4 Hill Cipher

- The encryption algorithm takes m successive plaintext letters and substitutor 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, c = 2, ... z = 25), the system can be described as follows :

$$C_1 = (K_{11} P_1 + K_{12} P_2 + K_{13} P_3) \bmod 26$$
$$C_2 = (K_{21} P_1 + K_{22} P_2 + K_{23} P_3) \bmod 26$$
$$C_3 = (K_{31} P_1 + K_{32} P_2 + K_{33} P_3) \bmod 26$$

- This can be expressed in term of column vectors and matrices :

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \bmod 26$$

or $C = KP \bmod 26$

Where C and P are column vectors of length 3, representing the plaintext and ciphertext.

- K is a 3×3 matrix, representing the encrypting key.
- **For example :**

Plaintext = Paymoremoney

$$\text{Key (K)} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

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

$$C = KP \bmod 26$$

$$= \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} \bmod 26 = \begin{pmatrix} 375 \\ 819 \\ 486 \end{pmatrix} \bmod 26 = \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix} = \text{LNS}$$

For plaintext pay, ciphertext is LNS.

The entire ciphertext is **LNSHDLEWMTRW**

- Decryption requires using the inverse of the matrix K.
- The general terms in Hill cipher is

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

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

Advantages

1. It completely hides single letter frequency.
2. Hill cipher is strong against a ciphertext only attack.
3. By using larger matrix, more frequency information hiding is possible.

Disadvantage

1. Easily broken with a known plaintext attack.

4.9.5 Polyalphabetic Substitution

- In polyalphabetic substitution, each occurrence of a character can have a different substitute. The relationship between a character in the plaintext to a character in the ciphertext is one to many.
- An example of polyalphabetic substitution is the **Vigenere cipher.**
- The Vigenere cipher chooses a sequence of keys, represented by a string. The key letters are applied to successive plaintext characters, and when the end of the key is reached, the key start over.
- Fig. 4.9.1 shows a tableall or table to implement this cipher efficiently,

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	N	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

Fig. 4.9.1

- **For example :** Let the message be THE BOY HAS THE BAG and let the key be VIG.

  Key = VIG VIG VIG VIG VIG

  Plaintext = THE BOY HAS THE BAG

  Ciphertext = OPKWWECIYOPKWIM

- The strength of this cipher is that there are multiple ciphertext letters for each plaintext letter, one for each unique letter of the keyword.

4.9.6 One Time Pad

- The key string is chosen at random and at least as long as the message, so it does not repeat.
- Each new message requires a new key of the same length as the new message. It produces random output that bears no statistical relationship to the plaintext.
- **Vernam cipher** uses a one time pad, which is discarded after a single use, and therefore is suitable only for short messages.
- **For example :**

Plaintext :	c	o	m	e	t	o	d	a	y
	2	14	12	4	19	14	3	0	24
Key	N	C	B	T	Z	Q	A	R	X
	13	2	1	19	25	16	0	17	23
Total	15	16	13	23	44	30	3	17	47
Subtract 26 if > 25	15	16	13	23	18	04	3	17	21
Ciphertext	P	Q	N	X	S	E	D	R	V

- The one time pad offers complete security but, in practice, has two fundamental difficulties.
  1. There is the practical problem of making large quantities of random keys.
  2. Key distribution and protection is also major problem with one time pad.
  3. Only possible attack to such a cipher is a brute force attack.

4.9.7 Feistel Cipher

- Fig. 4.9.2 shows the classical Feistel network. The inputs to the encryption algorithm are a plaintext block of length 2w bits and a key K. The plaintext block is divided into two halves i.e. Left (L_0) and Right (R_0).

(See Fig. 4.9.2 on next page)

Parameters and design features

Following parameters are considered :

1. Block size
2. Key size
3. Number of rounds
4. Subkey generation algorithms
5. Round function
6. Fast software encryption / decryption.
7. Ease of analysis

1. Security depends upon the block size. Larger **block size** gives greater security but encryption / decryption speed is reduced normal. Block size is 64-bit and AES uses 128-bit block size.
2. Greater security is achieved by using longer **key size**. Because of longer key size, again speed of algorithm decreases. Key sizes of 64 bits or less are now widely considered to be inadequate and 128 bits have become a common size.
3. **Number of rounds** are 16 in most of the algorithm. In Feistel cipher, single round offers insufficient security and multiple rounds offer greater security.
4. In **subkey generation algorithm**, greater complexity leads to greater difficulty of cryptanalysis.
5. **Round function** is again greater complexity for greater resistance to cryptanalysis.
6. **Fast software encryption / decryption** : The speed of execution of the algorithm becomes a concern.
7. **Ease of analysis** : There is great benefit in making the algorithm easy to analysis.

Decryption algorithm

- Use the ciphertext as input to the algorithm, but use the subkeys K_i in reverse order.
- The output of the first round of the decryption process is equal to a 32 bit swap of the input to the 16^{th} round of the encryption process.
- Consider the encryption process :

$$LE_{16} = RE_{15}$$

$$RE_{16} = LE_{15} \times F(RE_{15}, K_{16})$$

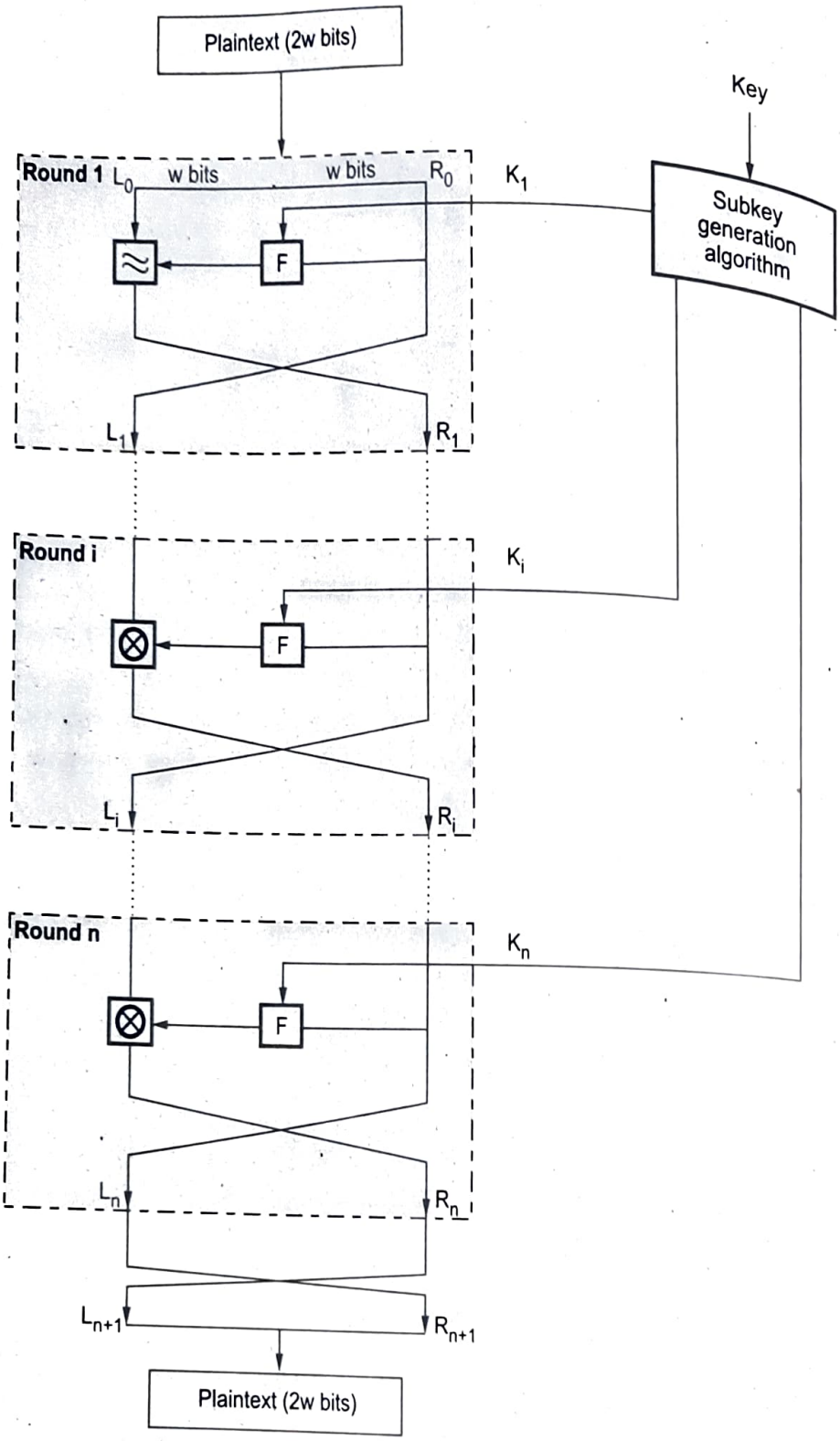


Fig. 4.9.2 Classical feistel network

- On the decryption side

$$LD_1 = RD_0 = LE_{16} = RE_{15}$$

$$RD_1 = LD_0 \times F(RD_0, K_{16}) = RE_{16} \times F(RE_{15}, K_{16})$$

$$= [(LE_{15} \times F(RE_{15}, K_{16})] \times F(RE_{15}, K_{16})$$

$\therefore$ We have $LD_1 = RE_{15}$ and $RD_1 = LE_{15}$

- For the i^{th} iteration of the encryption algorithm,

$$LE_i = RE_{i-1}$$

$$RE_i = LE_{i-1} \times F(RE_{i-1}, K_i)$$

Finally, the output of the last round of the decryption process is $RE_0 \| LE_0$. A 32 bit swap recovers the original plaintext, demonstrating the validity of the Feistel decryption process.

4.9.8 Comparison between Monoalphabetic and Polyalphabetic Cipher

No.	Monoalphabetic cipher	Polyalphabetic cipher
1.	Once a key is chosen, each alphabetic character of a plaintext is mapped onto a **unique** alphabetic character of a ciphertext.	Each alphabetic character of a plaintext can be mapped onto "**m**" alphabetic characters of a ciphertext.
2.	The relationship between a character in the plaintext and the characters in the ciphertext is one-to-one.	The relationship between a character in the plaintext and the characters in the ciphertext is one-to-many.
3.	A stream cipher is a monoalphabetic cipher if the value of *ki* does not depend on the position of the plaintext character in the plaintext stream	A stream cipher is a polyalphabetic cipher if the value of *ki* does depend on the position of the plaintext character in the plaintext stream.
4.	Monoalphabetic cipher includes additive, multiplicative, affine and monoalphabetic substitution cipher.	Polyalphabetic cipher includes autokey, Playfair, Vigenere, Hill, one-time pad, rotor , and Enigma cipher.

Example 4.9.1 *Encrypt the message "PAY" using Hill cipher with the following key matrix and show the decryption to get the original plain text.*

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

Solution :

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

The letters PAY of the plaintext are represented by the vector :

$$\begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} \begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} = \begin{pmatrix} 375 \\ 819 \\ 486 \end{pmatrix} \bmod 26 = \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix} = \text{LNS}$$

Ciphertext = LNS

Example 4.9.2 *Encrypt the following using play fair cipher using the keyword MONARCHY. "SWARAJ IS MY BIRTH RIGHT". Use X for blank spaces.*

Solution :

Key Square :

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

Plain text : SWARAJ IS MY BIRTH RIGHT

SW AR AJ IS MY BI RT HR IG HT

Cipher Text /Encryption Result = QX RM BS XA NC SX ZR OD KE DP

Example 4.9.3 *Convert "COMPUTER SECUIRTY" using caesar cipher.*

Solution : Caesar cipher involves replacing each letter of the alphabet with the letter standing 3 places further down the alphabet.

Plain text : COMPUTER SECUIRTY

Cipher Text : FRPSXWHU VHFXLUWB

Example 4.9.4 *Convert plain text into cipher text by using simple column as techniques of the following sentence : 'ALL IS WELL FOR YOUR EXAM'*

Solution : Consider the six columns. Therefore, we write the message in the rectangle row-by-row :

Column 1	Column 2	Column 3	Column 4	Column 5	Column 6
A	L	L	I	S	W
E	L	L	F	O	R
Y	O	U	R	E	X
A	M				

- Now let us decide the order of columns at some random order, say 5, 2,4,1,6,3. Then read the text in the order of these columns.

Ciphertext = SOELLOMIFRAEYAWRXLLU

Example 4.9.5 *Find out cipher text using Playfair cipher for following given plane text and key.*

Key = GOVERNMENT *Plain text = PLAYFAIR*

Solution : Key = GOVERNMENT

Plain text = PLAYFAIR

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

Plain text = PLAYFAIR ➔ PL AY FA IR

Cipher text = PQHETHBZ

Example 4.9.6 *Find out cipher test using palyfair cipher for following given plane text and key.*

Key = ENGINEERING *Plain text = COMPUTER*

Solution :

Key = ENGINEERING

Plain text = COMPUTER

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

Plain text = COMPUTER ➔ CO MP UT ER

Cipher text = FLTHUPEN

Example 4.9.7 *Consider the following :*

Plaintext : "PROTOCOL" Secret key : "NETWORK"

What is the corresponding cipher text using play fair cipher method ?

Solution : Corresponding cipher text using playfair cipher method :

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

Plaintext : PR OT OC OL

Ciphertext : LA NW NR NS

Example 4.9.8 *Using Playfair cipher encrypt message. "We live in a world full of beauty "use key "ANOTHER ".*

Solution :

Example :

Plaintext : We live in a world full of beauty.

Keyword : Another

Step 1 : Preparing plain text

The plain text matrix is :

we	it	ve	in	aw
or	ld	fu	lx	lo
fb	ea	ut	yz	

Step 2 : Preparing key matrix

The key matrix is :

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

Step 3 : Encryption

By following the above rules for encryption of plain text the cipher text is :

VRFKAFGONVNBULLMIZIHIEFESHZY

Example 4.9.9 *Use polyalphabetic ciphers to encrypt plain text "SHE IS VERY HAPPY AND BEAUTIFUL GIRL" use key 'ANOTHER'*

Solution :

Keyword	anoth	erano	thera	nothe	ranot	heran
Plaintext	sheis	veryh	appya	ndbea	utifu	lgirl
Ciphertext	SUSBZ	ZVRLV	TWTPA	ARULE	LTVTN	SKZRY

Example 4.9.10 *Use play fair cipher to encrypt the following message "This is a columnar transposition" use key - APPLE.*

Solution : Message = This is a columnar transposition

Key = APPLE

Encryption :

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

Message = Th is ac ol um na rt ra ns po si ti on

Ciphertext = UG MQ MQ BH MB SO IE SU MT BK QM NQ KN

Example 4.9.11 *Encrypt the plain text 'COE' using hill cipher, use keyword 'ANOTHERBZ'.*

Solution : Plain text = COE

Key = ANOTHERBZ

For plaintext COE, here C = 2 O = 14 E = 4

Therefore

$$P = \begin{pmatrix} 2 \\ 14 \\ 4 \end{pmatrix}$$

For key ANOTHERBZ the numbers are 0, 13, 14, 19, 6, 4, 17, 1, 25

The numbers in the matrix form :

$$K = \begin{pmatrix} 0 & 13 & 14 \\ 19 & 6 & 4 \\ 17 & 1 & 25 \end{pmatrix}$$

Ciphertext = (Key × Plaintext) Mod 26

Encryption is as follows :

$$C = \begin{pmatrix} 0 & 13 & 14 \\ 19 & 6 & 4 \\ 17 & 1 & 25 \end{pmatrix} \begin{pmatrix} 2 \\ 14 \\ 4 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 238 \\ 138 \\ 148 \end{pmatrix} \bmod 26 = \begin{pmatrix} 4 \\ 8 \\ 18 \end{pmatrix}$$

Ciphertext : = 4 = E, 8 = I and 18 = S

Ciphertext = EIS

Example 4.9.12 *Encrypt the message "PAY" using Hill cipher with the following key matrix and show the decryption to get the original plain text.*

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

Solution : $K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$

The letters PAY of the plaintext are represented by the vector :

$$\begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} \begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} = \begin{pmatrix} 375 \\ 819 \\ 486 \end{pmatrix} \text{ mod } 26 = \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix} = \text{LNS}$$

Ciphertext = LNS

Example 4.9.13 *Using hill cipher encrypt the message 'ESSENTIAL'. The key for encryption is 'ANOTHERBZ'.*

Solution :

$$\text{Key matrix K} = \begin{bmatrix} 0 & 13 & 14 \\ 19 & 6 & 4 \\ 17 & 1 & 25 \end{bmatrix}$$

$$\text{Plaintext matrix P} = \begin{bmatrix} 4 & 4 & 8 \\ 18 & 13 & 0 \\ 18 & 19 & 11 \end{bmatrix}$$

$$\text{Ciphertext matrix C} = \text{K} \times \text{P mod } 26$$

$$C = \begin{bmatrix} 0 & 13 & 14 \\ 19 & 6 & 4 \\ 17 & 1 & 25 \end{bmatrix} \begin{bmatrix} 4 & 4 & 8 \\ 18 & 13 & 0 \\ 18 & 19 & 11 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 486 & 435 & 154 \\ 256 & 230 & 196 \\ 536 & 556 & 411 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 18 & 19 & 24 \\ 22 & 22 & 14 \\ 16 & 10 & 21 \end{bmatrix} \bmod 26$$

$$C = \begin{bmatrix} S & T & Y \\ W & W & D \\ Q & K & V \end{bmatrix} \bmod 26$$

Ciphertext = SWQTWKYD

Example 4.9.14 *Use transposition cipher to encrypt plain text 'I Love my India' and use the key 'HEAVEN'. [Use single columnar transposition]*

Solution :

KEY	→	H	E	A	V	E	N
Key number	→	4	2	1	6	3	5
Plaintext	→	I	L	O	V	E	M
	→	Y	I	N	D	I	A

Arrange the key number as per ascending order

KEY	→	A	E	E	H	N	V
Key number	→	1	2	3	4	5	6
Plaintext	→	O	L	E	I	M	V
	→	N	I	I	Y	A	D

Cithertext = ONLIEIIYMAVD

Example 4.9.15 *Encrypt the message "THIS IS AN EXERCISE" using playfair cipher with key=DOLLARS.*

Solution : Key = DOLLARS

Message = THIS IS AN EXERCISE

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

To encipher a message, divide it into pairs of letters : TH IS IS AN EX ER CI SE

Cipher text = PKGC GC DT CYFAIQBF

4.10 Transposition Cipher Techniques

- A transposition cipher rearranges the characters in the plaintext to form the ciphertext. The letters are not changed.
- The rail fence cipher is composed by writing the plaintext in two rows, proceeding down, then across and reading the ciphertext across, then down.
- For example, to encipher the message "meet me after this party" with a rail fence of depth 2, we write the following :

m	e	m	a	t	r	h	s	a	t
e	t	e	f	e	t	i	p	r	y

- The ciphertext is
  MEMATRHSATETEFETIPRY
- Attacking a transposition cipher requires rearrangement of the letters of the ciphertext.
- A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext.

Plaintext : The book is suitable for self study.

Key : 5 6 4 1 3 2

Key	:	5	6	4	1	3	2
Plaintext	:	t	h	e	b	o	o
		k	i	s	s	u	i
		t	a	b	l	e	f
		o	r	s	e	l	f
		s	t	u	d	y	

Ciphertext : BSLEDOIFFOUELYESBSUTKTOSHIART.

4.10.1 Rail Fence Cipher

- The Rail Fence Cipher is a transposition cipher. It rearranges the plaintext letters by drawing them in a way that they form a shape of the rails of an imaginary fence.
- To encrypt the message, the letters should be written in a zigzag pattern, going downwards and upwards between the levels of the top and bottom imaginary rails. The shape that is formed by the letters is similar to the shape of the top edge of the rail fence.

- Next, all the letters should be read off and concatenated, to produce one line of ciphertext. The letters should be read in rows, usually from the top row down to the bottom one.
- The secret key is the number of levels in the rail. It is also a number of rows of letters that are created during encryption. This number cannot be very big, so the number of possible keys is quite limited.
- Suppose we want to encrypt the message "buy your books in August" using a rail fence cipher with encryption key 3.
  a) Arrange the plaintext characters in an array with 3 rows (the key determines the number of rows), forming a zig-zag pattern :

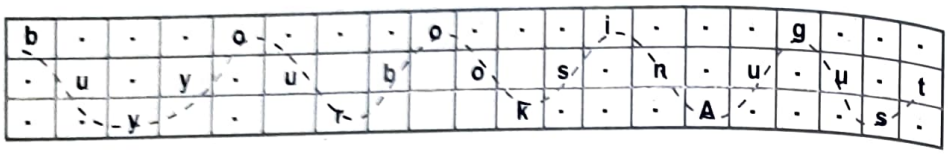


Fig. 4.10.1

  b) Then concatenate the non-empty characters from the rows to obtain the ciphertext : BOOIGUYUBOSNUUTYRKAS

4.10.2 Difference between Substitution Techniques and Transposition Techniques

Parameters	Substitution cipher	Transportation cipher
Definition	A substitution technique is one in which the letters of plain text are replaced by other letters or number or symbols.	Transposition cipher does not substitute one symbol for another instead it changes the location of the symbols
Type	Monoalphabetic and Polyalphabetic substitution cipher.	Keyless and Keyed transportation cipher.
Changes	Each letter retains its position changes its identity	Each letter retains its identity but changes its position
Disadvantage	The last letters of the alphabet which are mostly low frequency tend to stay at the end.	Keys very close to the correct key will reveal long sections of legible plaintext
Example	Ceaser cipher	Rail fence cipher

Example 4.10.1 *Solve the following example using rail fence technique. "COMPUTER SECURITY IS IMPORTANT".*

Solution : Plain text : COMPUTER SECURITY IS IMPORTANT

Arrange the plaintext characters in an array with 3 rows

C	-	-	-	U	-	-	-	S	-	-	-	R	-	-	-	I	-	-	-	P	-	-	-	A	-	-
-	O	-	P	-	T	-	R	-	E		U	-	I	-	Y	-	S	-	M	-	O	-	T	-	N	-
-	-	M	-	-	-	E	-	-	-	C	-	-	-	T	-	-	-	I	-	-	-	R	-	-	-	T

Ciphertext : **CUSRIPAOPTREUIYSMOTNMECTIRT**

Example 4.10.2 *Decipher a message : "TSACT SGCEB HISRM SELNV ISEEE AVITP" using a Rail fence using 10 Columns & 3 rails & retrieve original massage.*

Solution : The number of columns in rail fence cipher remains equal to the length of plaintext message. Hence, rail matrix can be constructed accordingly.

T	S	A	C	T	S	G	C	E	B
H	I	S	R	M	S	E	L	V	N
I	S	E	E	E	A	V	I	T	P

Original Message: - THIS IS A SECRET MESSAGE VCLIEVT BNP

Example 4.10.3 *Convert plain text to cipher text using Rail Fence technique "COMPUTER ENGINEERING".*

Solution : Plain text = COMPUTER ENGINEERING

Step 1 : Write down Plain text as sequence of diagonal.

C	-	-	-	U	-	-	-	E	-	-	-	N	-	-	-	I	-	-
-	O	-	P	-	T	-	R	-	N		I	-	E	-	R	-	N	-
-	-	M	-	-	-	E	-	-	-	G	-	-	-	E	-	-	-	G

Ciphertext : CUENIOPTRNIERNMEGEG

Example 4.10.4 *Convert plain text into cipher text by using simple columnas techniques of the following sentence : 'ALL IS WELL FOR YOUR EXAM'.*

Solution : Consider the six columns. Therefore, we write the message in the rectangle row-by-row :

Column 1	Column 2	Column 3	Column 4	Column 5	Column 6
A	L	L	I	S	W
E	L	L	F	O	R
Y	O	U	R	E	X
A	M				

- Now let us decide the order of columns at some random order, say 5,2,4,1,6,3. Then read the text in the order of these columns.

Ciphertext = SOELLOMIFRAEYAWRXLLU

Example 4.10.5 *Convert plain text to cipher text using Rail Fence technique "COMPUTER SECURITY"*

Solution : Plain text : COMPUTER SECURITY

Arrange the plaintext characters in an array with 3 rows

C	-	-	-	U	-	-	-	S	-	-	-	R	-	-	-
-	O	-	P	-	T	-	R	-	E		U	-	I	-	Y
-	-	M	-	-	-	E	-	-	-	C	-	-	-	T	-

Ciphertext : CUSROPTREUIYMECT

Example 4.10.6 *"Computer Security Technology" using rail fence technique*

Solution : Plain text : Computer Security Technology

Arrange the plaintext characters in an array with 3 rows

C	-	-	-	u	-	-	-	S	-	-	-	r	-	-	-	T	-	-	-	n	-	-	-	g	-
-	o	-	p	-	t	-	r	-	e		u	-	i	-	y	-	e	-	h	-	o	-	o	-	y
-	-	m	-	-	-	e	-	-	-	c	-	-	-	t	-	-	-	c	-	-	-	l	-	-	-

Ciphertext : CuSrtngoptreuiyehooymectcI

4.11 Block Ciphers Modes

- The modes of operation of block ciphers are configuration methods that allow those ciphers to work with large data streams, without the risk of compromising the provided security.
- There are five types of operations in block cipher modes, ECB (Electronic Code Block) mode, CBC (Cipher Block Chaining) mode, CFB (Cipher Feedback) mode, OFB (Output Feedback) mode and CTR (Counter) mode.

- Where ECB and CBC mode works on block ciphers, and CFB and OFB mode works on block ciphers acting as stream ciphers.
- ECB is used for transmitting a single value in secure manner, CBC is used for encrypting blocks of text authentication, CFB is used for transmitting encrypted stream of data authentication, OFB is used for transmitting encrypted stream of data, CTR is used for transmitting block-oriented applications.
- Modes of operation enable the repeated and secure use of a block cipher under a single key. A block cipher by itself allows encryption only of a single data block of the cipher's block length.
- When targeting a variable-length message, the data must first be partitioned into separate cipher blocks. Typically, the last block must also be extended to match the cipher's block length using a suitable padding scheme.
- Modes of operation have primarily been defined for encryption and authentication. While modes of operation are commonly associated with symmetric encryption, they may also be applied to public-key encryption primitives such as RSA in principle.

4.11.1 Electronic Code Book (ECB) Mode

- A block of plaintext encrypts into a block of ciphertext. Block size is 64-bits. Each block is encrypted independently.
- Plaintext patterns are not concealed since identical blocks of plaintext give identical blocks of ciphertext. It is not necessary to encrypt the file linearly.
- User can encrypt the 10 blocks in the middle first, then the blocks at the end, and finally the blocks in the beginning. Because of this, encrypted files are accessed randomly like a data base.
- It is very easy to parallelize the process. Pad the last block with some regular pattern i.e. zeros, ones to make it a complete block.
- End of file character is used to denote the final plaintext byte before padding.
- ECB method is ideal for a short amount of data, such as an encryption key.
- Fig. 4.11.1 shows ECB mode.
- In this mode, the plain text is divided into a block where each block is of 64 bits. Then each block is encrypted separately. The same key is used for the encryption of all blocks. Each block is encrypted using the key and makes the block of ciphertext.

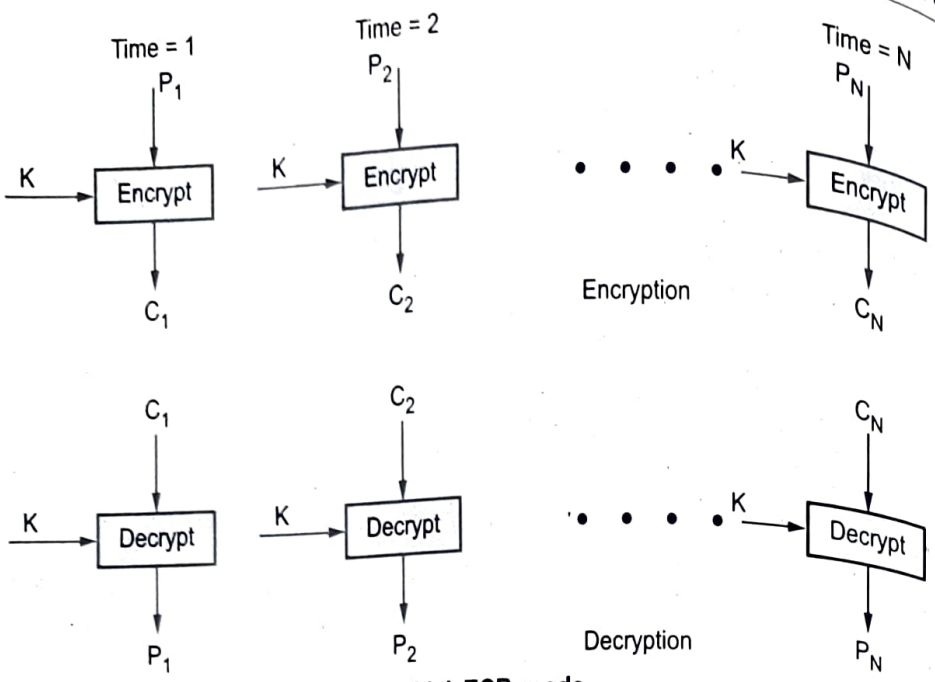


Fig. 4.11.1 ECB mode

- At the receiver side, the data is divided into a block, each of 64 bits. The same key which is used for encryption is used for decryption. It takes the 64-bit ciphertext and by using the key convert the ciphertext into the plain text.
- For lengthy messages, the ECB mode may not be secure.
- Used in secure transmission of single values i.e. an encryption key.
- ECB has security problems that limit its usability.
- Patterns in the plaintext can yield patterns in the ciphertext.
- It is also easy to modify a ciphertext message by adding, removing or switching encrypted blocks.
- Synchronization error is unrecoverable.

4.11.2 Cipher Block Chaining (CBC) Mode

- Cipher block mode at the sender side, the plain text is divided into blocks. In this mode IV(Initialization Vector) is used which can be a random block of text. IV is used to make the ciphertext of each block unique.
- The first block of plain text and IV is combined using the XOR operation and then encrypted the resultant message using the key and form the first block of ciphertext. the first block of ciphertext is used as IV for the second block of plain text. The same procedure will be followed for all blocks of plain text.
- At the receiver side, the ciphertext is divided into blocks. The first block ciphertext is decrypted using the same key which is used for encryption. The decrypted result will be XOR with the IV and form the first block of plain text. The second

block of ciphertext is also decrypted using the same key and the result of the decryption will be XOR with the first block of ciphertext and form the second block of plain text. The same procedure is used for all the blocks.

- The plaintext is XORed with the previous ciphertext block before it is encrypted.
- The CBC mode is iterative mode.
- After a plaintext block is encrypted, the resulting ciphertext is also stored in a feedback register.
- Before the next plaintext block is encrypted, it is XORed with the feedback register to became the next input to the encrypting routine.
- The encryption of each block depends on all the previous blocks.
- A ciphertext block is decrypted normally and also saved in a feedback register.
- After the next block is decrypted, it is XORed with the results of the feedback register.
- Mathematically it is

$$C_i = E_k(P_i \oplus C_{i-1})$$

$$P_i = C_{i-1} \oplus D_k(C_i)$$

- It hides patterns in the plaintext.
- In order to guarantee that there is always some random looking ciphertext to apply to the actual plaintext, the process is started with a block of random bits called the Initialization Vector (IV).
- Fig. 4.11.2 shows cipher block chaining mode.

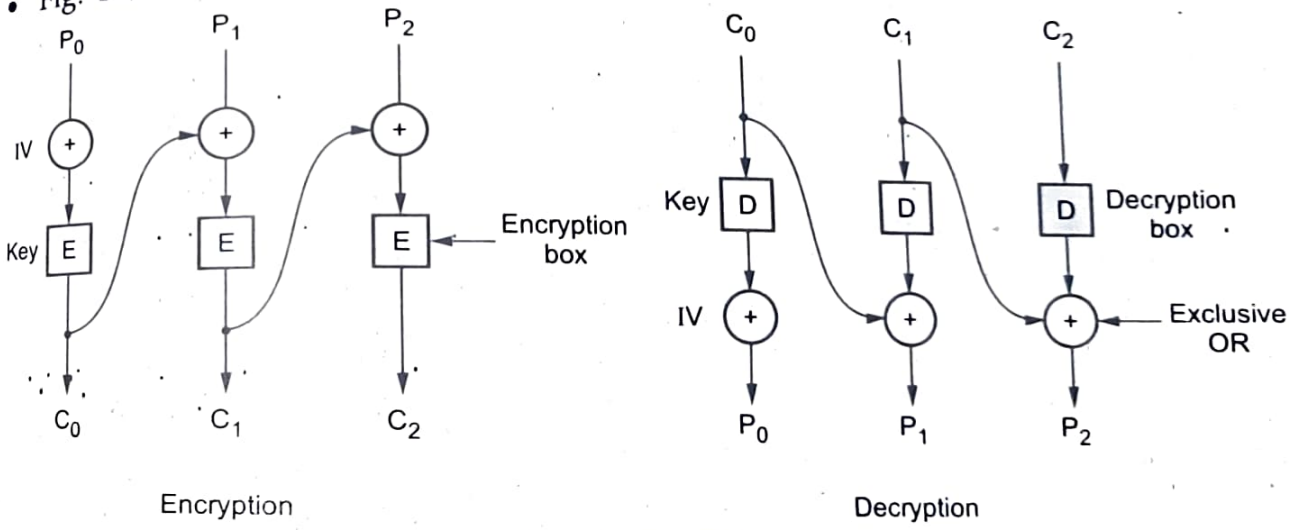


Fig. 4.11.2 CBC

- When used in networking messages, most CBC implementations add the IV to the beginning of the message in plaintext.

- A single bit error in a plaintext block will affect that ciphertext block and all subsequent ciphertext blocks.
- CBC mode is self recovering.
- Two blocks are affected by an error, but the system recovers and continues to work correctly for all subsequent blocks. Synchronization error is unrecoverable.
- Encryption is not parallelizable.
- Decryption is parallelizable and has a random access property.

4.11.3 Cipher Feedback (CFB) Mode

- Data is encrypted in units that are smaller than a defined block size.
- If it possible to convert the DES into stream cipher using cipher feedback mode.
- In this mode, the data is encrypted in the form of units where each unit is of 8 bits.
- Like cipher block chaining mode, IV is initialized. The IV is kept in the shift register. It is encrypted using the key and form the ciphertext.
- Fig. 4.11.3 shows CFB encryption and decryption process.

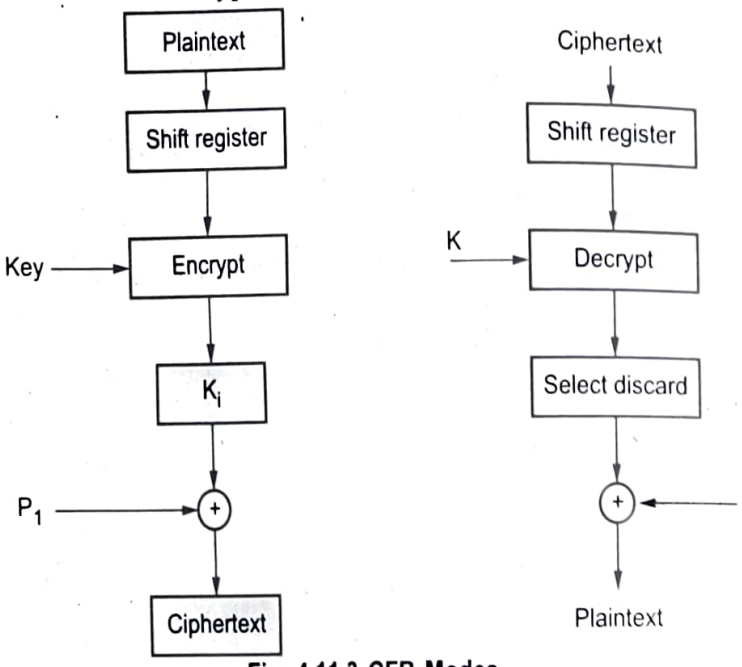


Fig. 4.11.3 CFB Modes

- More than one message can be encrypted with the same key, provided that a different initialization vector is used.
- CFB speed is the same as the block cipher.
- Encryption is not parallelizable, decryption is parallelizable and has a random access property.

- CFB is self recovering with respect to synchronization errors as well.

Advantages :

1. Simplicity
2. Need not be used on a byte boundary.
3. Input to the block cipher is randomized.
4. Ciphertext size is the same size as the plaintext size.

Disadvantages :

1. Encryption is not parallelizable.
2. Plaintext is somewhat difficult to manipulate.

4.11.4 Output Feedback (OFB) Mode

- The Output Feedback (OFB) mode is similar in structure to that of CFB. Fig. 4.11.4 shows output feedback mode.

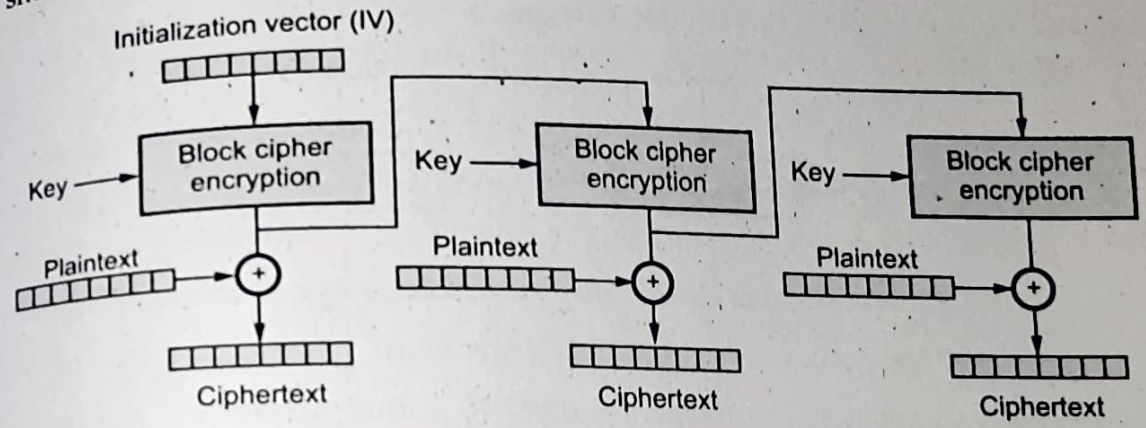


Fig. 4.11.4

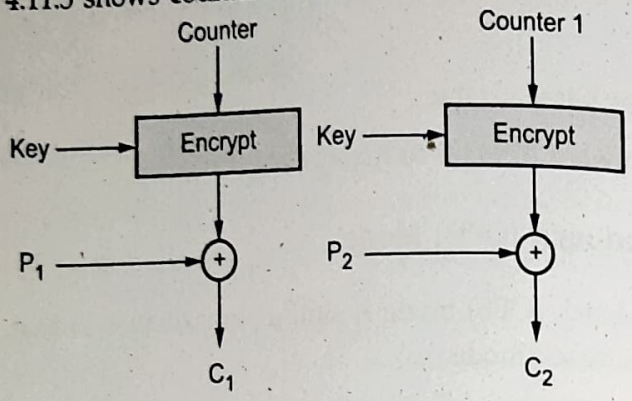
- It is the output of the encryption function that is fed back to the shift register in OFB, whereas in CFB, the ciphertext unit is fed back to the shift register.
- The other difference is that the OFB mode operates on full blocks of plaintext and ciphertext, not on an s-bit subset.

Disadvantages and Limitations of OFB :

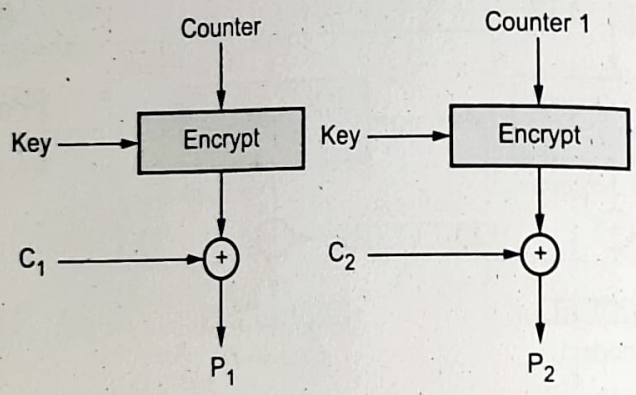
1. Needs an initialization vector which is unique for each use
2. Bit errors do not propagate
3. More vulnerable to message stream modification
4. Sender and receiver must remain in sync
5. Only use with full block feedback

4.11.5 Counter Mode

- Block ciphers in counter mode use sequence numbers as the input to the algorithm.
- More than one message can be encrypted with the same key, provided that a different initialise vector is used.
- Plaintext is very easy to manipulate, any change in ciphertext directly affects the plaintext. Fig. 4.11.5 shows counter mode.



(a) Encryption



(b) Decryption

Fig. 4.11.5 Counter mode

- Synchronization error is unrecoverable.
- A ciphertext error affects only the corresponding bit of plaintext.
- Encryption : The counter is encrypted and then XORed with the plaintext block to produce the ciphertext block.
- **Advantages**
  1. Simple to implement.
  2. It provides confidentiality.
  3. Random access of block is possible.
  4. Efficiency is same as block cipher.

4.12 Short Answered Questions

Q.1 Which are important functions performed by information security for an organization ?

Ans. : Important functions for an organization :

1. Protecting the organization's ability to function
2. Enabling the safe operation of applications running on the organization's IT systems
3. Protecting the data the organization collects and uses
4. Safeguarding the organization's technology assets.

Q.2 Define sniffers.

Ans. : A sniffer is a program or device that can monitor data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information.

Q.3 State the difference between threats and attacks.

Ans. : A threat is anything that can disrupt the operation, functioning, integrity, or availability of a network or system. The attacks actually use the functioning of TCP/IP to defeat the protocol.

Q.4 What is triple encryption ?

Ans. : The function follows an encrypt - decrypt - encrypt (EDE) sequence. There is no cryptographic significance to the use of decryption for the second stage.

Q.5 How many keys are used in triple encryption ?

Ans. : Tuchman proposed a triple encryption method that uses only two keys.

Q.6 Why is the middle portion of 3DES a decryption rather than an encryption ?

Ans. : Decryption requires that the keys be applied in reverse order: P=Dk1[Ek1[P]]. This results in a dramatic increase in cryptographic strength.

Q.7 Why ECB mode is not secure for lengthy message ?

Ans. : For lengthy messages, the ECB mode may not be secure because the message is highly structured, it may be possible for a cryptanalyst to exploit these regularities.

Q.8 Why is access control important ?

Ans. : Access control regulates which users, applications, and devices can view, edit, add, and delete resources in an organization's environment. Controlling access is one of the key practices to protect sensitive data from theft, misuse, abuse, and any other threats. There are two levels of access control : physical and logical.

Q.9 What is mandatory access control ?

Ans. : Mandatory Access Control (MAC) is a model of access control where the operating system provides users with access based on data confidentiality and user clearance levels. In this model, access is granted on a need to know basis : users have to prove a need for information before gaining access.

Q.10 What is discretionary access control ?

Ans. : Discretionary Access Control (DAC) is an identity-based access control model that provides users a certain amount of control over their data. Data owners can define access permissions for specific users or groups of users.

4.13 Multiple Choice Questions

Q.1 _____ is a well-known and broad category of electronic and human activities that can breach the confidentiality of information.

a Espionage
b Attack
c Risk
d All of these

Q.2 _____ can be used both for legitimate network management functions and for stealing information.

a Keylogger
b Hoax
c Sniffers
d None

Q.3 _____ occurs when an attacker or trusted insider steals information from a computer system and demands compensation for its return or for an agreement not to disclose it.

a Information extortion
b Information modification
c Information stolen
d Information exchange

Q.4 _____ is often a chain message telling recipients to forward the mail to all their contacts. The aim is simply to cause alarm and confusion among users.

a Email
b Hoax
c Virus
d Network

Q.5 _____ software attacks occur when an individual or group designs and deploys software to attack a system.

a Deliberate
b System
c Commercial
d Malicious

Q.6 **The process of converting plaintext to ciphertext is called as_____.**

[a] encryption
[b] decryption
[c] substitution
[d] transposition

Q.7 **_____ attacks are very difficult to detect because they do not involve any alternation of data.**

[a] Active
[b] Passive
[c] Active and passive
[d] None of these

Q.8 **Virus is one type of _____ threats.**

[a] program
[b] software
[c] system
[d] all of these

Q.9 **_____ are software programs that hide their true nature and reveal their designed behavior only when activated.**

[a] Worms
[b] Trojan horses
[c] Virus
[d] Trap

Q.10 **The discretionary access control is also called as an _____ access control.**

[a] identity based
[b] rule based
[c] role based
[d] All of these

Q.11 **Components of risk management are _____.**

[a] risk identification
[b] risk assessment
[c] risk control
[d] all of these

Q.12 **Mandatory access control is also called as _____ access control.**

[a] role based
[b] discretionary
[c] rule based
[d] identity based

Q.13 **In _____ access control, each user is assigned one or more roles, and the roles determine which parts of the system the user is allowed to access.**

[a] rule based
[b] role based
[c] task based
[d] none

Q.14 Which of the following is not one of the four access control models ?

a Discretionary
b Mandatory
c Role-based
d Delegated

Q.15 Which of the following access control is used with firewalls and routers ?

a Discretionary access control
b Mandatory access control
c Role-based access control
d Rule-based access control

Q.16 Which of the following is the most expensive means of verifying a user's identity ?

a Single sign-on
b Tokens
c Biometrics
d Passwords

Q.17 What form of authorization is closely associated with labels ?

a Rule-based access control
b Discretionary access control
c Mandatory access control
d Role-based access control

Q.18 ECB mode stands for _____ Mode.

a Electronic Code Block
b Electronic Cyber block
c Encryption Code Block
d Electronic Counter Block

Q.19 How many keys does the Triple DES algorithm use ?

a 2
b 3
c 2 or 3
d 3 or 4

Q.20 Which one of the following DES operating modes can be used for large messages with the assurance that an error early in the encryption/decryption process won't spoil results throughout the communication ?

a Cipher Block Chaining (CBC)
b Electronic Codebook (ECB)
c Cipher Feedback (CFB)
d Output Feedback (OFB)

Q.21 What is the minimum number of cryptographic keys required to achieve a higher level of security than DES with the Triple DES algorithm ?

a 1
b 2
c 3
d 4

Q.22 Double DES has a _____ key and enciphers blocks of 64 bits.

a 32-bit
b 56-bit
c 112-bit
d 128-bit

Answer Keys for Multiple Choice Questions :

Q.1	a	Q.2	c	Q.3	a	Q.4	b
Q.5	a	Q.6	a	Q.7	b	Q.8	c
Q.9	b	Q.10	a	Q.11	d	Q.12	c
Q.13	b	Q.14	d	Q.15	b	Q.16	c
Q.17	c	Q.18	a	Q.19	c	Q.20	d
Q.21	b	Q.22	c				

❑❑❑