G. Pullaiah College of Engineering & Technology

Cryptography and Network Security. (CNS).

Sub Code - A33117.

UNIT - I Security Concepts

1. Introduction
2. The need for security
3. Security approaches
4. Principles of security
5. Types of Security attacks
6. Security service
7. Security Mechanisms

* A model for Network Security Cryptography Concepts and Techniques :

1. Introduction
2. plain text and cipher text
3. Substitution techniques
4. transposition techniques
5. Encryption and Decryption
6. Symmetric and Asymmetric key cryptography
7. key range and key size
8. Possible type of attacks

Network Security :

⇒ Network security is any action an organization takes to prevent malicious use or accidental damage to the networks private data, its user's or their devices.

⇒ The goal of network security is to keep the network running and safe for all the legitimate users.

⇒ Because there are so many ways that a network can be vulnerable, network security involves a broad range of practices. These include :

1. Deploying active devices:

⇒ Using software to block malicious programs from entering, or running within the network.

⇒ Blocking users from sending or receiving suspicious looking emails.

⇒ Blocking Unauthorized use of the Network.

⇒ Stopping the Network's users accessing websites that are known to be dangerous.

2. Deploying passive devices :

⇒ Using devices and software that report unauthorized intrusions into the network or suspicious activity by authorized users.

3. Using preventative devices :

⇒ Devices that help identify potential security holes, so that network staff can fix them.

4. Ensuring users follow safe practices :

⇒ Even if the software and hardware are setup to be secure, the actions of users can create security holes.

=> Network security staff is responsible for educating members of the organization about how they can stay safe from potential threats.

The Need for Security

=> Most previously computer applications had no (or) very little security.

=> When computer applications were developed to handle financial and personal data, the real need for security was felt.

=> People realized that data on computers is extremely important and need to be protected.

=> Two typical security mechanisms which were implemented to protect computer data were as follows

* Provide a user identification and password to every user and use that information to authenticate a user
* Encode information stored in the database in some fashion, so that it is not visible to users who do not have the right permissions.

=> With the advancement of technology and internet people realized the basic security measures were not quite enough.

=> As business was conducted using these technologies namely over internet network and internet security gained immense importance

=> Information travelling across the internet was subjected to various types of attacks.

=> Some key characteristics of modern attacks are:

1. Automating attacks :-

=) Computers are efficient in doing routine, mundane and repetitive tasks.
=) The speed of computers can make several attacks worthwhile for miscreants.
=) for example, computers can excel in somehow stealing a very low amount (say half a dollar) from a million bank accounts in a matter of a few minutes.
=) This would give the attacker a half million dollars possibly without any major complaints.

2. Privacy Concerns :

=) Companies like banks, airlines, insurers are collecting and processing a mind-boggling amount of information about us, without us realizing when and how it is going to be used.
=) The so-called data mining applications gather, process and tabulate all sorts of information about individuals
=) People can then illegally sell this information.
=) Information that can come out of this are :
  * Which store the person buys more from.
  * Which restaurant he/she eats in.
  * Where he/she goes for vacations frequently and so on.
=) These activities can invade our privacy.

3. Distance :

=) Now a days, money is in digital form inside computers, and moves around by using computer networks.
=) A Robber can easily and cheaply attempt an attack on the computer systems of the bank.

=) The attacker can break into the bank's servers or steal credit card/ATM information from the comforts of his/her home or place of work.
=) for example, in 1995 a Russian hacker broke into citibanks computers remotely, stealing $12 million.

Note :

1. Intruders :-

=) Intruders are the atlackers who attempt to breach the security of a network.
=) They attack the network in order to get unauthorized access.
=) Intruders are of three types namely
    1. Masquerader (outsider)
    2. misfeasor (insider)
    3. clandestine user (inside or outsider)

Masquerader :

=) An external user who is not authorized to use a compoter and yet tries to gain privileges to access a legitimate user's account.
=) Masquerading is generally done either using stolen ID's and passwords or through bypassing authentication mechanisms.

Misfeasor :

=) The category of individuals that are authorized to use the system but misuse the granted access and privilege for stealing data.

Clandestine User :

=) The category of individuals those have administrative control over the system and misuse the [authorization] authoritative power given to them for financial gains.

Authentication & Authorization :

=) Authentication verifies the identity of a user or service and authorization determines their access rights.
=) Authentication is done before authorization.

Miscreant :

=) a person who has done something unlawful.

Security Policy :

=) Security policy is a document that states in writing how a company plans to protect its physical and Information technology assets.

Security Approaches :-

=) Security management issues have been handled by organizations in various ways.
=) Some Security approaches in network security are

* Trusted systems.
* security Models
* security Management Practices

1. Trusted Systems :

=) A Trusted Systems is a computer system that can be trusted to a specified extent to enforce a specified security policy.
=) Trusted systems were initially of primary interest to the military, now a days they are used in banking and financial community.
=) Trusted systems are special systems designed to serve the purpose of providing security.

=) Different models were developed to ensure the safety of trusted system, which are

* Reference monitor
* Trusted computing base (TCB)
* Bell - LaPadula model.

1. Reference monitor :-

=) This can be a software/hardware which is the heart of a computer system.

=) It is mainly responsible to take decisions related to access control.

=) A Reference monitor enforces the system security by preventing normal users from writing to a restricted file through validation mechanisms.

=) following are the expectations from the reference monitor ;

* It should be tamper-proof
* It should always be invoked.
* It should be small enough so that it can be tested independently.

2. Trusted computing base (TCB) :

=) It can be a combination of hardware, software and firmware responsible for [enforcing] enforcing system's security policy.

=) It defines a set of evaluation classes that describes the features and assurances that the user could expect from a trusted system.

=) Lower the TCB, higher the assurance.

3. Bell - LaPadula Model :

=> It was developed by David Bell and leonard LaPadula for enforcing access control in government and military applications.

=> In this model, a highly trustworthy computer system is designed as a collection of objects and subjects.

=> Objects are passive repositories or destinations for data, such as files, disks, printers, etc.

=> Subjects are active entities, such as users processes or threads operating on behalf of users.

=> Subjects cause information to flow among objects

=> labels were attached to objects that represented the sensitivity of data contained within the objects.

Eg : Top secret, secret, confidential, unclassified are a range of security labels.

=> Bell - LaPadula model talks about confidentiality or security of information. It does not talk about problems of integrity of information.

Security Models :-

=> An Organization can take several approaches to implement its security model.

=> Some approaches followed are

1. No Security :

=> In this simplest case, the approach could be a decision to implement no security at all.

2. Security through obscurity :

=) In this model, a system is secure simply because nobody knows about its existence and contents.

=) This approach cannot work for too long, as there are many ways an attacker can come to know about it.

3. Host Security :

=) In this scheme, the security for each host is enforced individually.

=) This is a very safe approach, but harder to achieve as organizations grow.

4. Network Security :

=) In this technique the focus is to control network access to various hosts and their services rather than individual host security.

=) This is very efficient and valuable model.

Security Management Practices

=) Good security management practices always talk of a security policy being in place.

=) A good security policy and its proper implementation go a long way in ensuring security-Management practices

=) A good security policy generally takes care of four key aspects, which are

* Affordability
  => Money and efforts required

* functionality
  → Mechanism of providing security
* Cultural Issues
  → Policy complements with people expectations, working style and beliefs.
* Legality
  → Policy meet the legal requirements.

⇒ Once a security policy is in place, the following points should be ensured.

(a) Explanation of the policy to all concerned
(b) Outline everybody's responsibilities.
(c) Use simple language in all communications
(d) Accountability should be established.
(e) provide for exceptions and periodic reviews.

Principles of Security:

⇒ Security principles are the building blocks to identify the type of attack and solutions for that
⇒ Then chief principle of security are

1. Confidentiality
2. Authentication
3. Integrity
4. Non-repudiation
5. Access control
6. Availability
7. Ethical and legal issues

1. Confidentiality :

⇒ The confidentiality principle of security states that only their intended sender and receiver should be able to access messages.

⇒ If an unauthorized person gets access to this message then the confidentiality gets compromised.

⇒ For example, suppose user x wants to send a message to user y and x does not want someone else to get access to this message.

⇒ But if user z somehow gets access to this secret message, then the purpose of this confidentiality gets fail.

⇒ This type of attack is called Interception.

⇒ "Interception causes loss of message confidentiality."

2. Authentication :

⇒ The Authentication principle of security establishes proof of identity.

⇒ It ensures that the origin of a document or electronic message is correctly identified.

⇒ For example, suppose user z sends a message to user y, however, the trouble is that user z posed as user x while sending a message to user y.

⇒ This type of attack is called fabrication.

⇒ "Fabrication is possible in absence of proper authentication mechanisms."

3. Integrity :

⇒ The integrity principle of security states that the message should not be altered.

⇒ In other words, we can say that when the content of the message changes after the sender sends it, we can say that integrity of the message is lost.

⇒ for example, suppose user x sends a message to user y and attacker z somehow gets access to this message during transmission and changes the content of the message and then sends it to user y.

⇒ This type of attack is called Modification.

⇒ "Modification causes loss of message integrity".

4. Non-repudiation :

⇒ Non-repudiation principle of security does not allow the sender of a message to refute the claim of not sending that message.

⇒ for example, user x sends requests to the bank for fund transfer over the internet.

⇒ After the bank performs fund transfer based on user x request, user x cannot claim that he/she never sent the fund transfer request to the bank.

⇒ This principle of security defeats such possibilities of denying something after having done it.

⇒ "Non-repudiation does not allow the sender of a message to refute the claim of not sending that message."

5. Access control :

=) Access control principles of security determine who should be able to access what : i.e we can specify that what users can access which function

=) for example, we can specify that user x can view the database record but cannot update them, but user y can access both, can view record and can update them.

=) This principle is broadly related to two areas.

- → role management and
- → rule management

=) Role Management concentrates on the users side i.e which user can do what.

=) Where as rule management focuses on the resources side i.e which resource is accessible and under what circumstances.

=) Based on this access control matrix is prepared, which lists the users against a list of items they can access.

=) The access control list is a subset of the access control matrix.

=) "Access control specifies and controls who can access what".

6. Availability :

=) The principle of availability states that resources i.e information should be available to authorized parties at all times.

=) for Example, due to the intentional access of another unauthorized user 2, an authorized user X may not be able to contact a server computer y.

=) This would defeat the principle of availability.

=) such an attack is called interruption.

=) "Interruption puts the availability of resources in damadger".

7. Ethical and legal issues:

=) Ethical issues in the security system are classified into the following categories.

- Privacy
  - => It deals with the individuals right to access the personal information.
- Accuracy
  - => It deals with the responsibility of authentication, fidelity and accuracy of information.
- Accessibility
  - => It deals with what information a oaganization have right to collect and measures to safeguard it.
- Property
  - => It deals with the owner of the information and who controls access.

=) While dealing with legal issues, we must remember that there is a hieraachy of regulatory bodies that govern the legality of information security.

=) It can be classified into the following categories.

=> International, eg. International cybercrime Treaty

* federal, e.g. FERPA, GLB
* state, eg. UCITA
* Organization, e.g. computer use policy.

OSI standard for security Model :

⇒ This defines seven layer of security in the form of

- Authentication
- Access control
- Non repudiation
- Data integrity
- confidentiality
- Assurance or availability
- Notarization or signature

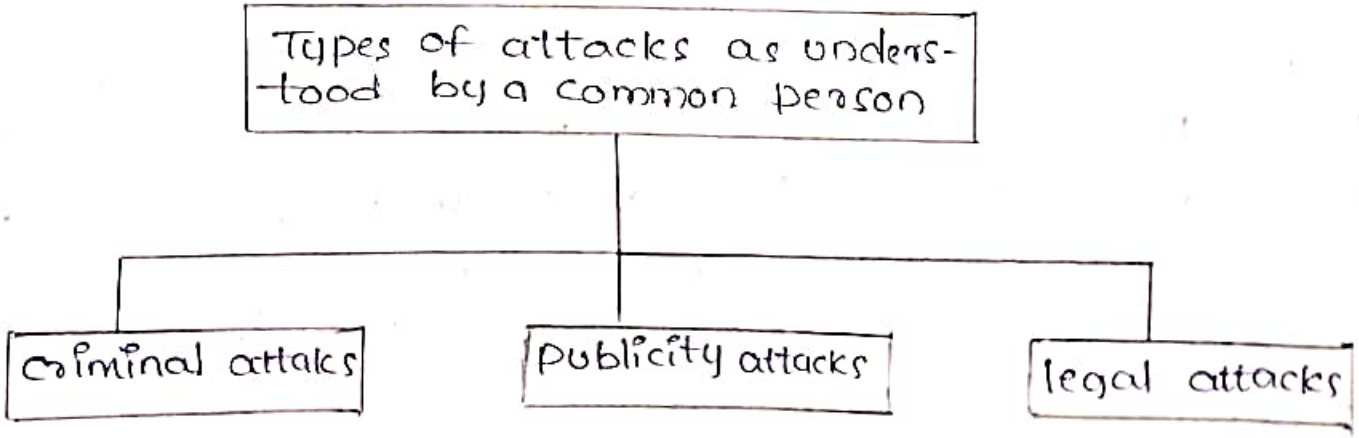
Types of attacks

⇒ Security attacks can be classified with respect to two views

1. The common person's view
2. A Technologist's view

1. A General view of attacks :

⇒ from a common person's point of view, we can classify attack into three categories.



1. Criminal attacks :

=> Criminal attacks are the simplest to understand.
=> Here, the sole aim of the attackers is to maximize financial gain by attacking computer systems.
=> Some forms of criminal attacks are

• Fraud :
=> Fraud attacks concentrate on manipulating some aspects of electronic currency, credit cards, checks, ATM etc.

• Scams :
=> Scams come in various forms, some of the most common ones being sale of services, auctions and business opportunities etc.

=> In this type of attacks people are entered to send money in return of great returns, but end up losing their money.

• Destruction :
=> Example of this type of attacks are unhappy Employee attack their own organization and terrorists strike.

• Identity theft :
=> In this type of attack, the attacker does not steal anything from a legitimate user but becomes that legitimate user.
=> Example obtaining someone's password or credit card.

• Intellectual property theft :

=> This type of attacks ranges from stealing companies trade secrets, databases, electronic documents and books, software and so on.

• Brand theft :

=) In this type of attacks fake web sites are set up that look like real web sites.

=) Innocent users end up providing their secrets and personal details on these fake sites.

=) The attackers use these details to then access the real site, causing an Identity theft.

2. Publicity Attacks :

=) In publicity attacks, the aim of the attacker is to gain publicity.

=) The attackers want to see their names appear on television, news channels and newspapers.

=) They are people such as students in universities or employees in large organizations.

3. legal Attacks :

=) In a legal attack, attackers try to make judge doubtful about the security of the computer system.

=) The attacker attacks on the system and later on tries to convey to the judge that there is a problem within the computer system.

2. A Technical view of attacks:

=)-from a technical point of view, we can classify the types of attacks on computers and networks systems into two categories.

(a) Theoretical concepts behind these attacks and

(b) Practical approaches used by the attackers.

(a) Theoretical concepts:

=)These attacks are generally classified into four categories, which are

* Interception:

=) It means than an Unauthorized party has gained access to a resource.

=)The party can be a person, program or Computer-based system.

=) Examples of interception are coping of data or program and listening to network traffic

* Fabrication:

=)This involves the creation of illegal objects on a computer system.

=)for Example, the attacker may add fake records to a database.

* Modification:

=)Here, the attacker may modify the values in a database.

* Interruption:

=)Here, the resource becomes unavailable, lost or unusable.

=) Examples of interruption are causing problems to a hardware device, erasing program, data or operating system components.

⇒ Theoretical concept attacks are further grouped into two types

(a) passive attacks

(b) active attacks

(a) Passive attacks :

⇒ Passive attacks do not involve any modification to the contents of an original message.

⇒ The attacker aims to obtain information that is in transit.

⇒ These attacks are harder to detect.

⇒ The general approach to deal with passive attacks is to think about prevention rather than detection correction actions.

⇒ Passive attacks are classified into two sub categories.

1. release of message contents
2. traffic analysis.

⇒ Example of Passive attack is interception.

(b) Active attacks :

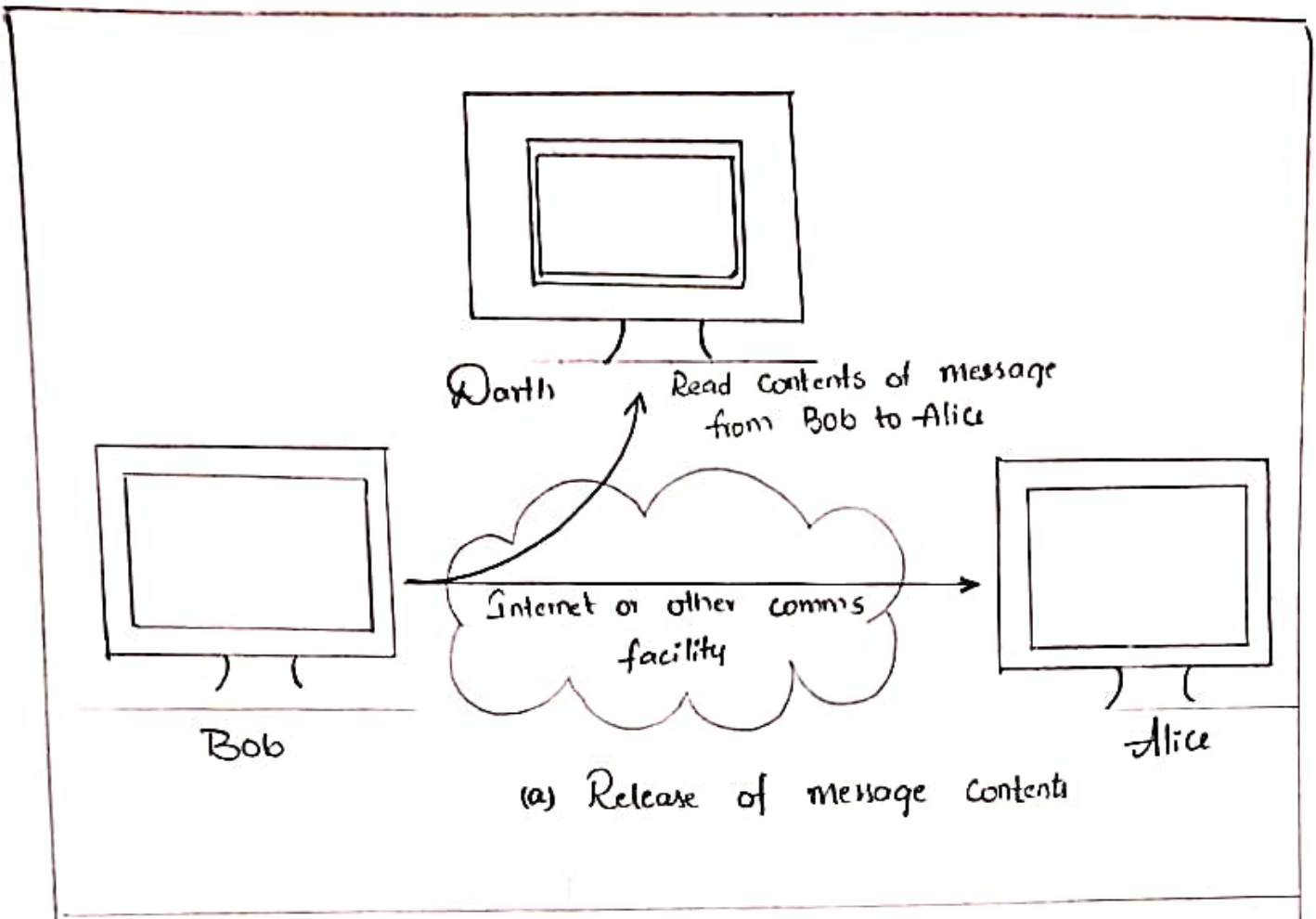
⇒ In active attacks the contents of the original message are modified in some way.

⇒ These attacks cannot be prevented easily.

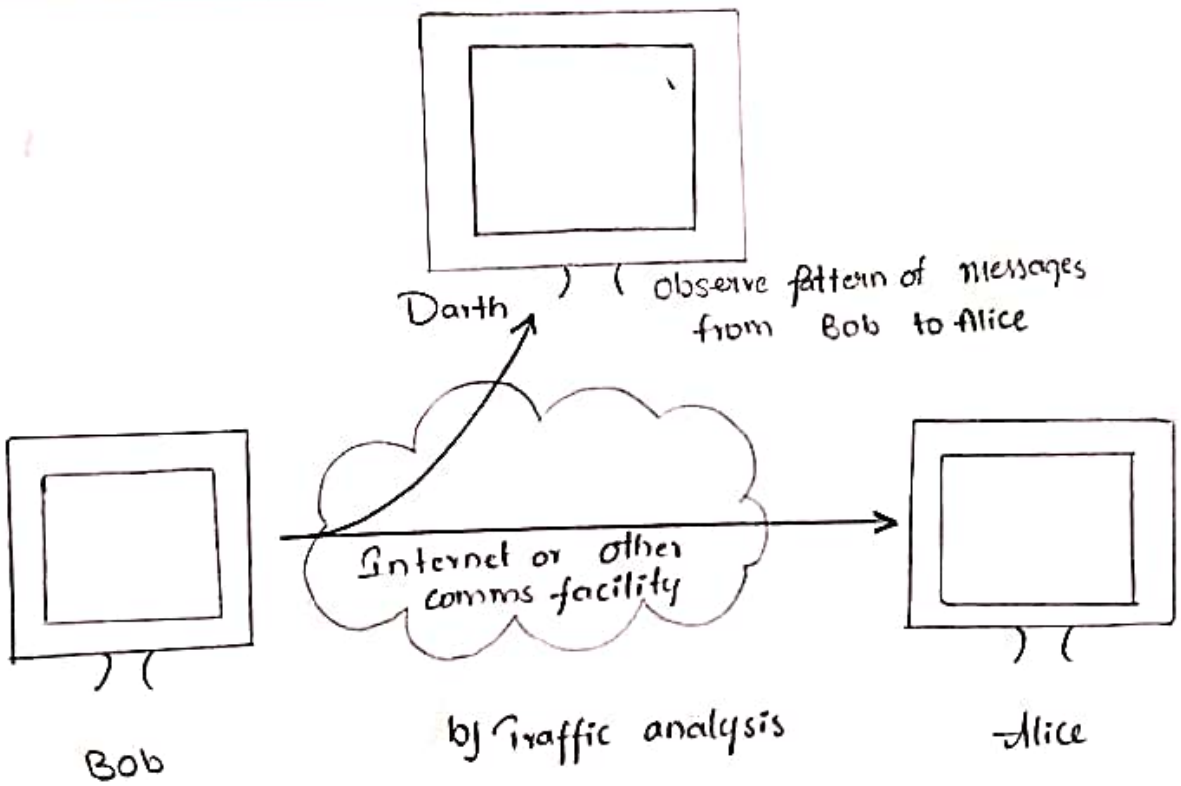
⇒ They can be detected with some effort and attempts can be made to recover from them.

⇒ These attacks can be in the form of interruption, Modification and fabrication.

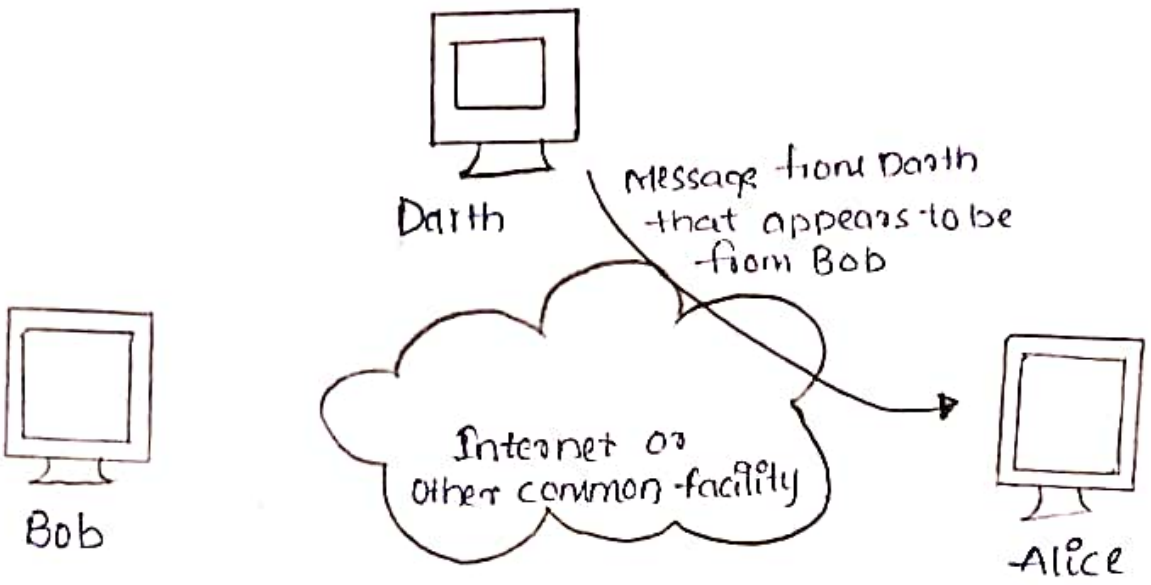
⇒ Active attacks can further be classified as shown below



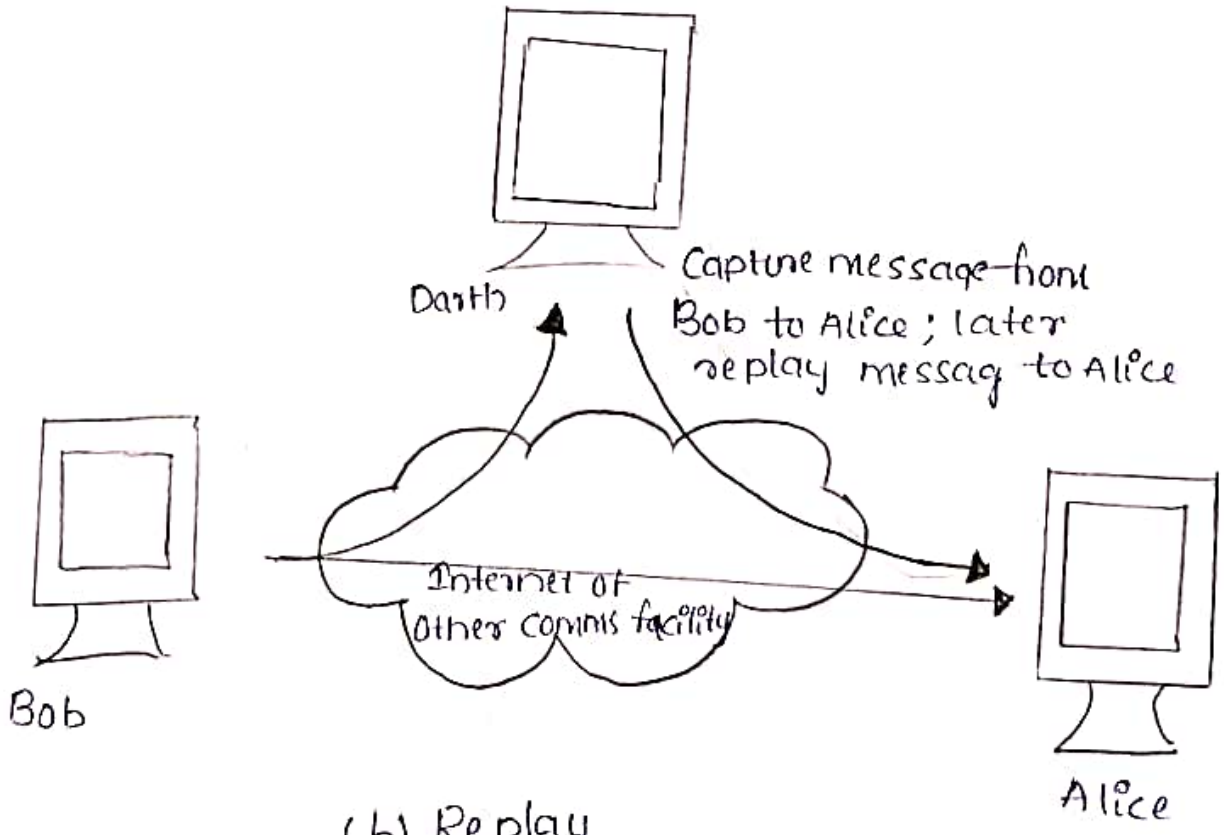
(a) Release of message contents



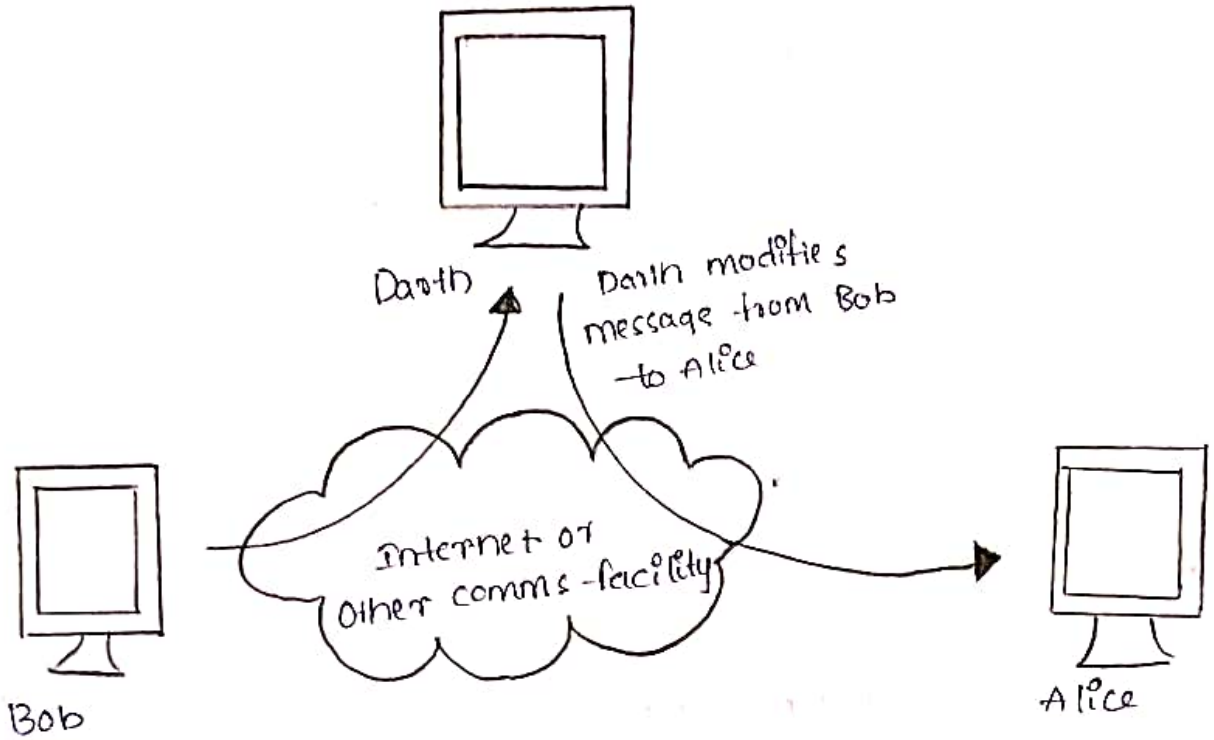
by Traffic analysis



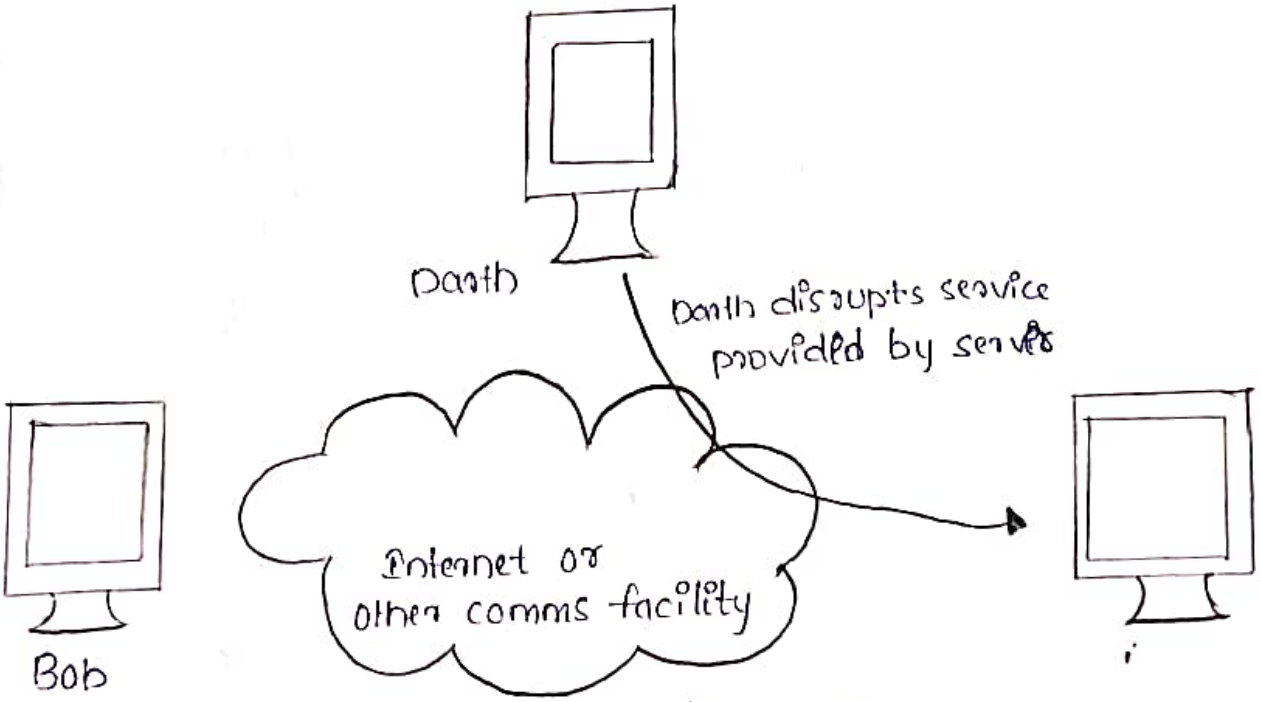
(a) Masquerade



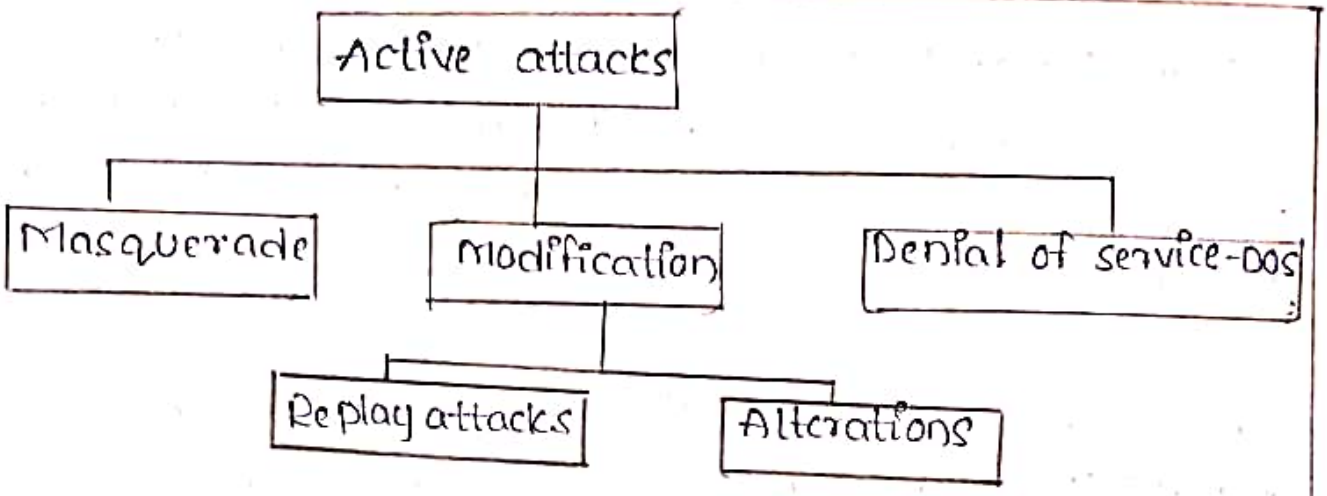
(b) Replay



(c) Modification of message



(d) Denial of service



⇒ Masquerade is caused when an unauthorized entity pretends to be another entity.

⇒ DoS (Denial of service) attacks make an attempt to prevent legitimate users from accessing some services, which they are eligible for.

⇒ In Reply attack, a user captures a sequence of events (or) some data units and resends them.

⇒ Alteration of messages involves some changes to the original message.

The Practical view of attacks:

⇒ As per the practical view attacks can be classified into two broad categories

(1) Application-level attacks

(2) Network-level attacks

1. Application-level attacks:

⇒ These attacks happen at an application level in the sense that the attacker attempts to access, modify or prevent access to information of a particular application or the application itself.

=> Examples of this are trying to obtain someone's credit card information on the internet, or changing the contents of a message to change the amount in a transaction, etc.

2. Network-level attacks:

=> These attacks generally aim at reducing the capabilities of a network by a number of ~~(provid)~~ possible means.

=> These attacks generally make an attempt to either slow down, or completely bring to halt, a computer network. This automatically can lead to application-level attacks.

Security services

=> A security service is defined as a communication service that is provided by a system to give a specific kind of protection to system resources.

=> The various categories of security services are

1. Authentication:

=> The authentication service is concerned with assuring that a communication is authentic.

=> In case of a single message, it assures the recipient that the message is from the source that it claims to be from.

=> In case of an ongoing interaction two aspects are involved.

=> first, at the time of connection initiation, the service assures that the two entities are authentic

=) Second, the service must assure that the connection is not interfered.
=) Two specific authentication services are.
(a) Peer entity authentication:
=) It provides corroboration of the identity of a peer entity in an association.
=) Two entities are considered peers if they implement same protocol in different systems.
(b) Data origin authentication:
=) It provides corroboration of the source of a data unit.
=) This type of service supports applications like electronic mail, where there are no prior interactions between the communicating entities.
2. Access control:
=) It limits and control the access to host syster and applications via communication links
=) It supports the avoidance of unauthorized use of a resource.
3. Data confidentiality:
=) This service defines that only the sender and the intended recipient should be capable to create the element of the message.
=) It protects the transmitted data from passive attack.
=) following are the types of Data confidentiality

* Connection confidentiality :

=) The protection of all user information on a connection.

* connectionless confidentiality :

=) The security of all user data in an individual data block.

* selective - field confidentiality :

=) The security of selected - fields within the user data.

* Traffic - flow confidentiality :

=) The protection of the information that can be derived from observation of traffic flows.

4. Data Integrity :

=) The assurance that data recieved are exactly as sent by an authorized entity.

=) The various type of data Integrity services are

* Connection Integrity with Recovery :

=) It provides the Integrity of all user data on a connection and detects any modification, Insertion, deletion or replay of any data, with recovery.

* connection Integrity without Recovery :

=) It provides any detection without recovery.

* selective - field connection Integrity :

=) provides for the integrity of selected fields within the user data and determines whether the selected fields have been modified, inserted, deleted or replayed.

* Connectionless Integrity :

⇒ provides for the integrity of a single connectionless data blocks.

* Selective - field connectionless Integrity :

⇒ Provides for the integrity of selected fields within a single connectionless data blocks.

5. Non - Repudiation :

⇒ Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

⇒ Non - Repudiation can be

* Nonrepudiation, Origin

⇒ proof that the message was sent by the specified party.

* Non repudiation, Destination

⇒ proof that the message was received by the specified party.

6. Availability service :

⇒ An availability service is one that protects a system to ensure its availability.

⇒ It is the property of a system or a system resource being accessible and usable upon demand by an authorized system entity.

Security Mechanism:

=) Security Mechanism is any process that is designed to detect, prevent, or recover from a security attack.

=) The mechanisms are divided into those that are implemented in a specific protocol layer and those that are not specific to any particular protocol layer.

Specific Security Mechanisms

=) These mechanisms can be incorporated into the appropriate protocol layer. The mechanisms are

1. Encipherment:

=) Encipherment is hiding or covering data and can provide confidentiality.

=) It makes use of mathematical algorithms to transform data into a form that is not readily intelligible.

=) The transformation and subsequent recovery of the data depends on an algorithm and zero or more encryption keys.

2. Data integrity:

=) The data integrity mechanism appends a short check value to the data.

=) The receiver receives the data and check value.

=) The receiver then creates a new check value from the received data and compares it with the received check value.

=) If the two check values match, the integrity of data is being preserved.

3. Digital Signature :

⇒ A digital signature is a way by which the sender can electronically sign the data and the receiver can electronically verify it.

⇒ It protect against forgery.

4. Authentication Exchange :

⇒ A mechanism intended to ensure the identity of an entity by means of information exchange.

5. Traffic padding :

⇒ The insertion of bits into gaps in data stream to frustrate traffic analysis attempts.

6. Routing control :

⇒ Enables selection of particular physically secure routes for certain data and allows routing changes especially when a breach of security is suspected.

7. Notarization :

⇒ The use of a trusted third party to assure certain properties of a data exchange.

8. Access control :

⇒ A variety of mechanisms are used to enforce access rights to resource/data owned by a system.

⇒ for example passwords and PINS.

Pervasive Security Mechanisms

=) Mechanisms that are not specific to any particular protocol layer. The Machanisms are:

1. Trusted Functionality:

=) Functionalities which are perceived to be correct with respect to some criteria.

eg: functionlities established by a security policy.

2. Security label:

=) The marking bound to a recource that names or designates the security attributes of that resource.

3. Event Detection:

=) Detection of security relevent events

=) for ex, a user clicking on a link in a spam email.

=) This incident doesn't directly cause any damage, but it could install malware that causes a ransomware attack.

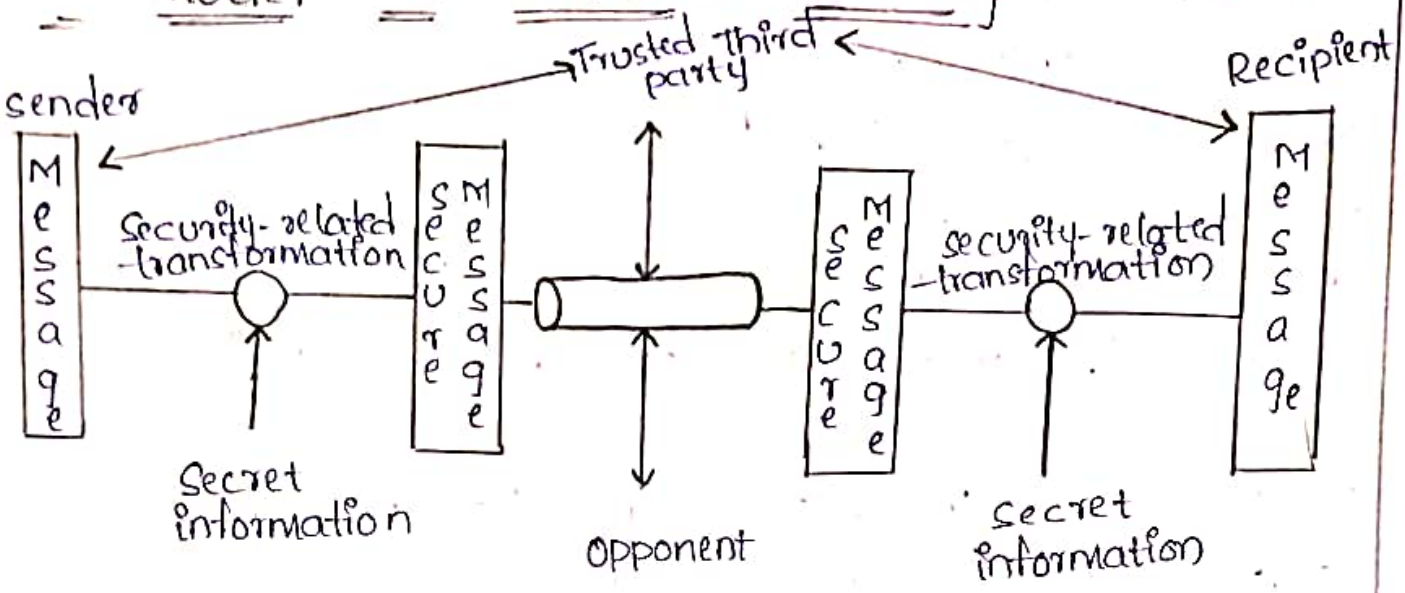
4. Security Audit Trail:

=) Data collected and potentially used to facilitate a security audit, which can be reviews, and examination of system records and activities.

5. Security Recovery:

=) Deals with requests from mechanisms, such as event handling and management functions and takes recovery actions.

A model for Network Security



⇒ A model for Network security is shown above, it consists of the following general terms.

1. A message to be transferred from one party to another across some sort of Internet service.
2. The two parties, who are the principals in this transaction. The two parties must cooperate for the exchange to take place.
3. A logical information channel is established by defining a route through the Internet from source to destination and by the cooperative use of communication protocols (e.g. TCP/IP) by the two parties.
4. Security aspects come into play when it is necessary to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity and so on.

⇒ All the techniques for providing security have two components.

(1) A security-related transformation on the information to be sent.

(2) Some secret information is shared by the two principals and it is hoped, unknown to the opponent.

5. A trusted third party may be needed to achieve secure transmission.
for Ex, a third party may be responsible for distributing the secret information to the two principals.

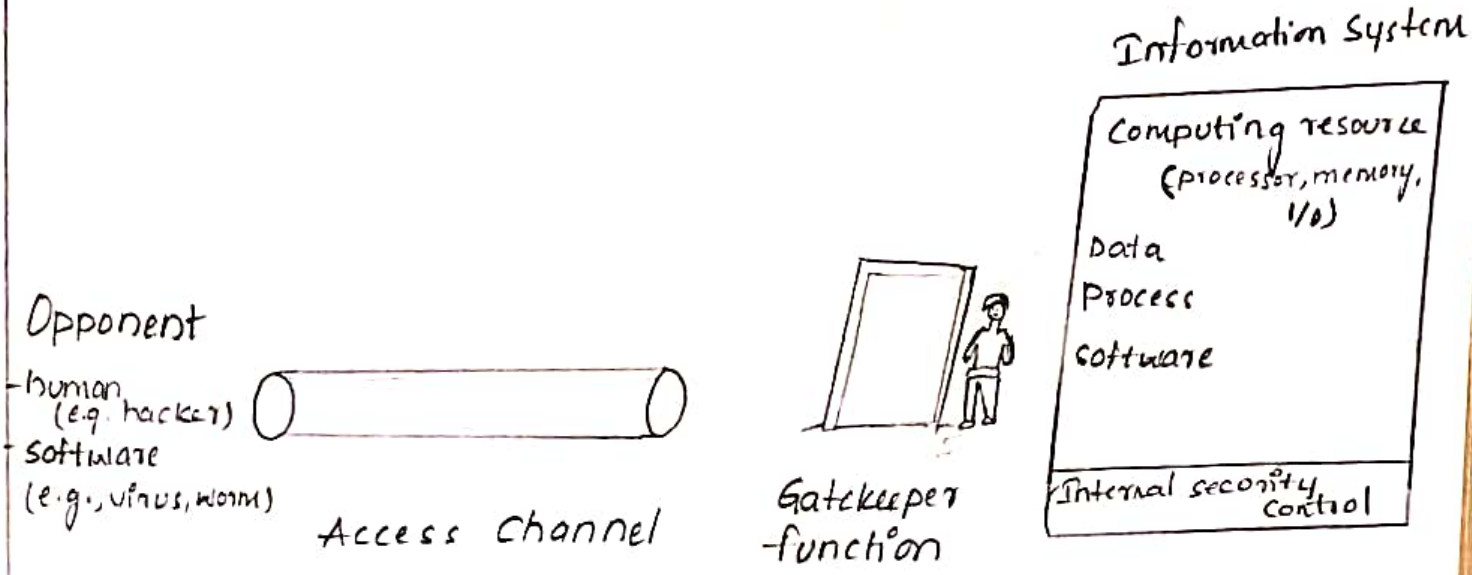
⇒ This General model shows that there are four basic tasks in designing a particular security service.

1. Design 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 secret information.
4. Specify a protocol to be used by the two principals that make use of the security algorithm and the secret information to achieve a particular security service.

⇒ In addition to the above security-related situation the network access security model should be designed which secure the information system from attackers.

UNIT - II

* Symmetric Key Ciphers :-



=) These attackers fall into two categories:

1. Hacker :

=) Hacker is one who is only interested in penetrating into your system.

=) They do not cause any harm to the system they only get satisfied by getting access to the system.

2. Intruders :

=) These attackers intend to do damage to the system (or) try to obtain the information from the system which can be used to attain financial gain.

=) The attackers can place a logical program on the system through the network, which leads to two kinds of risks.

(1) Information threat :

=) This kind of threat modifies data.

(2) Service threat :

=) This kind of threat disables the user from accessing data on the system.

=) This

=) These kinds of threats can be introduced by them launching worms and viruses.

=) There are two ways to secure the system from attacker of which the first is to introduce the gatekeeper functions.

=) Introducing gatekeeper function means introducing login-id and password which would keep away the unwanted access.

=) The second way to secure the system is introducing internal control which would detect the unwanted user trying to access the system.

=) These internal control's are the antivirus which are installed to prevent the unwarted users from accessing the computer system through the internet.

Encayption Techniques

⇒ plain text can be transformed into ciphen text Using substitution (or) transposition techniques.

Substitution techniques:

⇒ In substitution cipher, the character's of plain text are replaced by other characters (or) symbols.

⇒ The well known substitution ciphers are:

1. Caesar cipher:

⇒ Caxesar cipher is a substitution cipher and simplest cipher technique was introduced by Julius caesar.

⇒ which involver replacing each letter of alphabet replacing each letter of alphabet with the letter standing 3 places further down the alphabet i.e each letter in the plain text is shifted certain number of places down or up the alphabet.

1. Key: A number of that specifies how many positions each letter in the plain text will be shifted

Ex:- K = 3

2. Encayption:- Replace each letter in the plain text with letter that is a fixed no of positions away in the alphabet.

Ex:

P.T = Pay more money

C.T = SDB PRUH PRQHB

formula: $C = (P+K) \bmod 26$ where P → plain text and K - key

3. Decryption: Reverse the process by shifting the letters in the opposite decryption.

Ex:- C.T : SDB PRUH PRQHB
P.T = Pay more money
$P = (C - K) \bmod 26$

⇒ The Advantage of caesar cipher is easy to implement and understand.
⇒ The drawbacks of caesar cipher is that it is a very weak scheme. All that is required to break the caesar cipher is to do the reverse of the caesar cipher process.

2. Modified version of caesar cipher:

⇒ In this scheme the original plain text alphabets may not necessarily be three places down the order, but instead can be any places down the order.
⇒ Thus an alphabet 'A' in plain text would not necessarily be replaced by 'D'. It can be replaced by any valid alphabet i.e by 'E' or by 'F' or by 'G' and so on.
⇒ Once the replacement scheme is decided, it would be constant and will be used for all other alphabets in the message.
⇒ Ex:
plain Text : COME HERE
cipher Text : KIWOM PM2M

=) Here 'c' in is replaced by 'k' which is 8 places down to 'c'. similarly all other alphabets are replaced in the same fashion.

=) The major weakness of the caesar cipher is its predictability.

=) Once we decide to replace an alphabet in a plain-text message with an alphabet that is k positions up or down the order, we replace all other alphabets in the plain-text message with the same technique.

3. Mono-alphabetic cipher:

=) In Mono-alphabetic cipher we use random substitution.

=) This means that in a given plain-text message, each 'A' can be replaced by any other alphabet (B through Z) each 'B' can also be replace by any other random alphabet and so on.

=) The crucial difference being there is no relation between the replacement of 'B' and replacement of 'A'.

=) That is, if we have decided to replace each 'A' with 'D', we need not necessarily replace each 'B' with 'E', we can replace each 'B' with any other character.

Ex:

Plain Text : hello

Cipher Text : IFMMP

⇒ Mono-alphabetic cipher pose a difficult problem for a cryptanalyst because it can be very difficult to crack.

⇒ One hitch with this scheme is that if the message is short (or) if their are repeated patterns the cryptanalysft can try different attacks to crack the cipher text.

4. Homophonic substitution cipher:

⇒ Homophonic substitution cipher also involves substitution of one plain text character with a cipher text character at a time, however the cipher text character can be any one of a choosen set.

⇒ For instance A can be replaced by {D, H, P, R}, B can be replaced by {E, I, Q, S} and so on.

5. Polygram substitution cipher:

⇒ In the polygram substitution cipher ~~technique~~ technique, rather than replacing one-plain text alphabet with one cipher text alphabet at a time, a block of alphabets is replaced with another block.

⇒ For instance, HELLO could be replaced by YUQQW, and HELL could be replaced by a totally different cipher text TEUI.

6. Polyalphabetic Substitution cipher:

⇒ In polyalphabetic substitution, each appearance of a character in the plaintext can have a different substitution character in the ciphertext.

⇒ The relation among a character in plaintext and a character in ciphertext is one-to many.

⇒ For instance, letter 'A' can be restored by the letter 'C' and the similar letter 'A' can be restored by 'N' letter in the cipher text.

⇒ The main feature of polyalphabetic substitution are:

* It needs a set of associated monoalphabetic substitution rules.
* It needs a key that decides which rule is used for which transformation.

7. Playfair Cipher (or) Playfair square:

⇒ It is also known as square (or) wheat stone playfair cipher.

⇒ It is a manual symmetric encryption technique.

⇒ It is first literal diagram substitution cipher invented in 1854 by charles wheatstone.

⇒ playfair cipher is multiple letter encryption cipher which is 5×5 matrix constructed using a keyword (MONARCHY (or) CHARLES)

⇒ first removing any repeating letters as follows.

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

Rules for encryption using playfair cipher:

1. Write it
1. Create a 5x5 matrix and place the key in that matrix row-wise from left to right.
- Then put the remaining alphabet in the blank space.

2. Now, we have to break the plain text into a pair of alphabets.

Ex: plain Text : meet me tomorrow

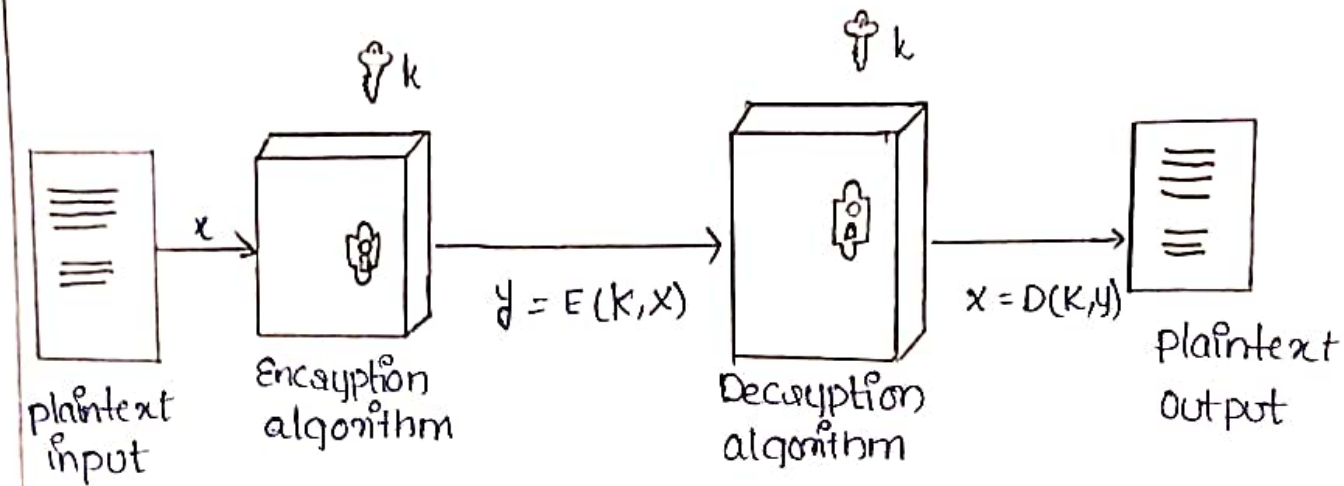
pair : me et me to mo rx ro wz

- Pair of alphabets must not contain the same letter. In case, pair has the same letter then break it and add 'x' to the previous letter.
- In case while making pair, the last pair has only one alphabet left then we add 'z' to it to form a pair.

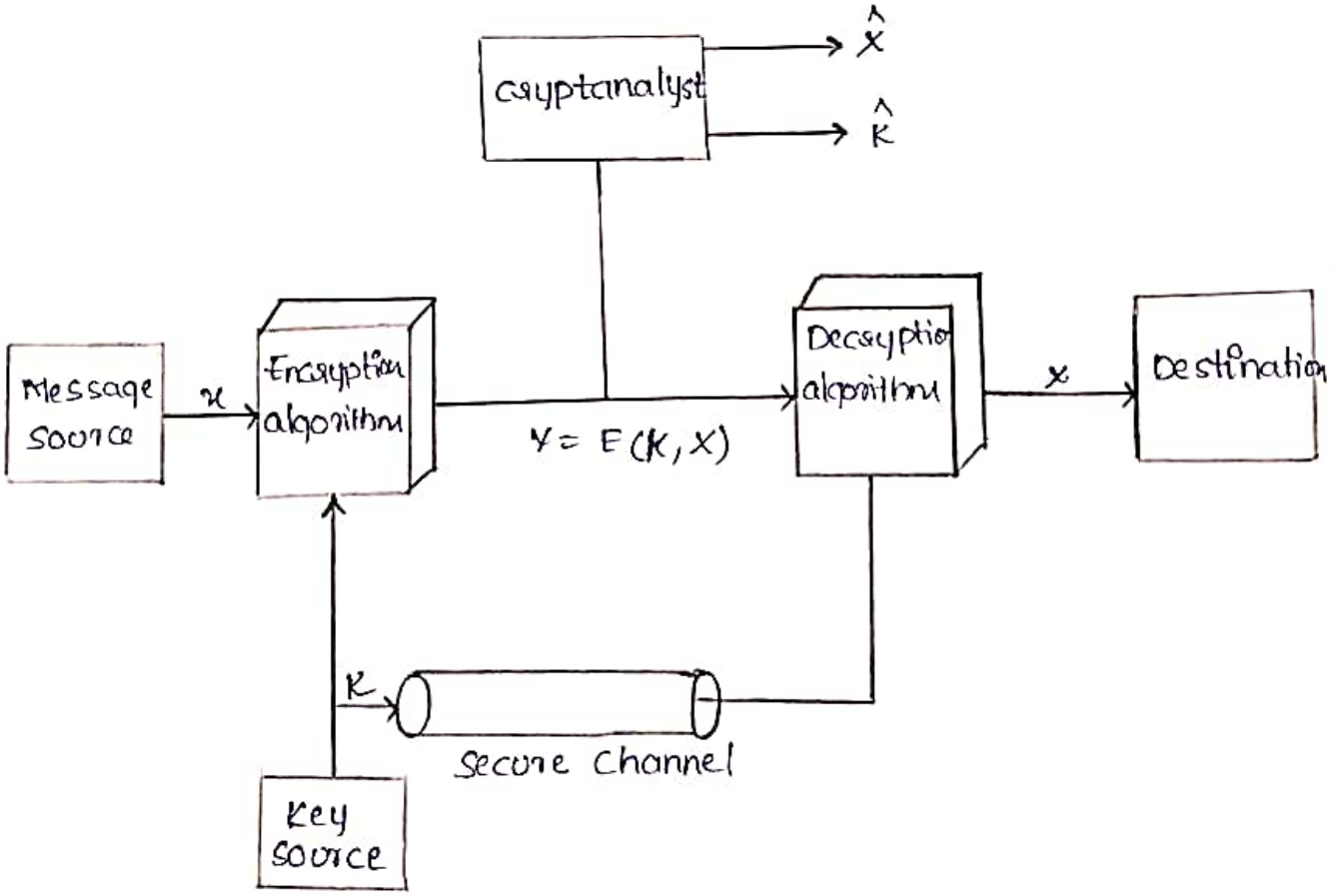
3. In this step, we will convert plain text into cipher text. for that, take the first pair of plain text and check for cipher alphabets for the corresponding in that matrix.

- To find cipher alphabets follow the rules below.

(i) If both the alphabets of the pair occur in the same row replace them with the alphabet to their immediate right. If an alphabet of the pair occurs at extreme right then replace it with the first element of that row, i.e the last element of the row in the matrix circularly



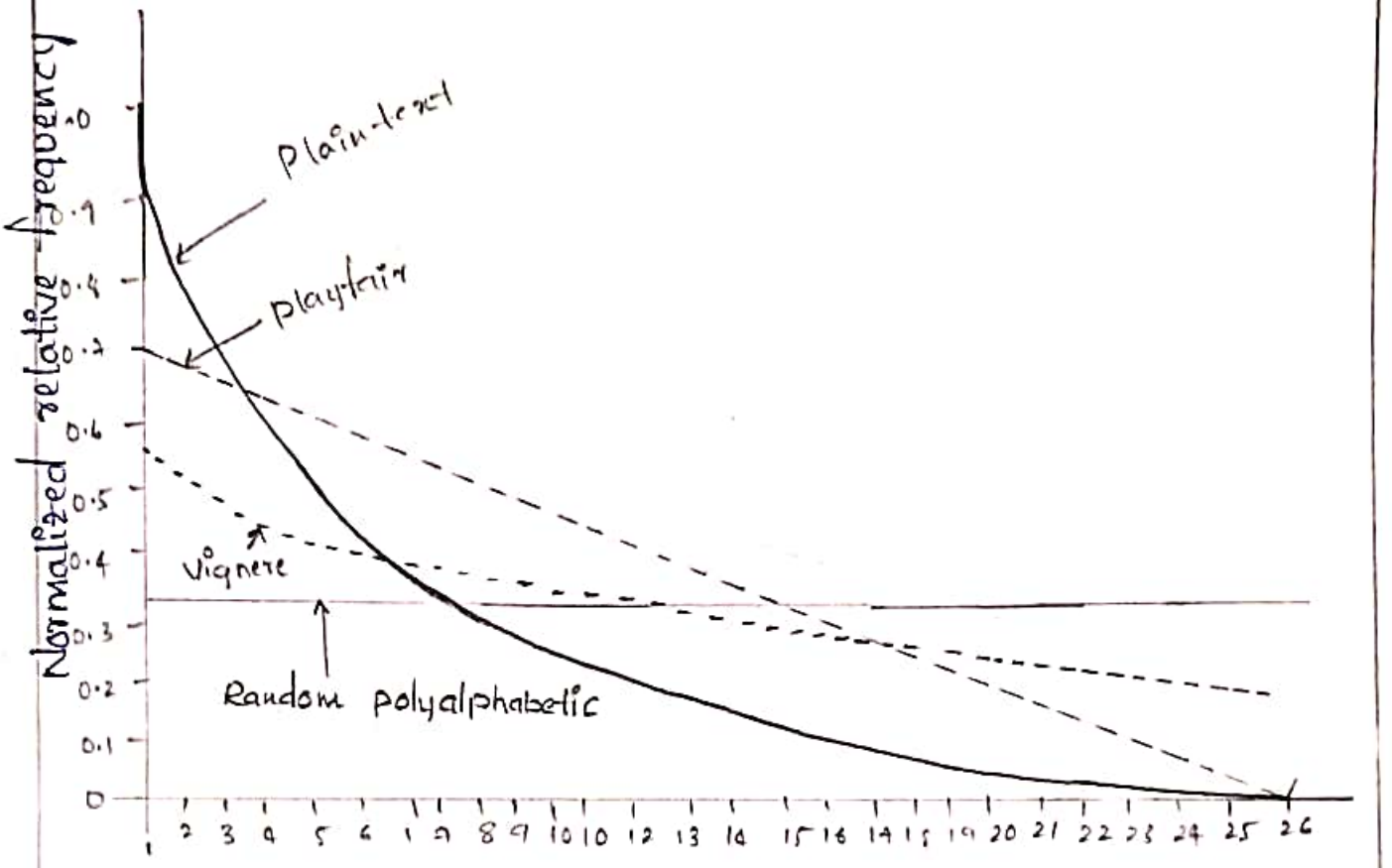
Simplified Model of Symmetric Encryption



Model of Symmetric cryptosystem

playfair

Relative Frequency of Occurrence of letters



Frequency ranked letters (decreasing Frequency)

follows the first element of the same row.

(ii) If the alphabets in the pair occur in the same column, the replace them with the alphabet immediate below them. Here also, the last element of the column circularly follows the first element of the same column.

⇒ If the alphabets in the pair are neither in the same column and nor in the same row then the alphabet is replaced by the element in its own row and the corresponding column of the other alphabet of the pair.

Ex: key = MONARCHY

plain Text = ME|ET | ME| AT | THE CO|LL|GE

Cipher Text = CL|KL| CL| SR| PD| LG | MP|UL| I/J F

8. Hill cipher:

⇒ Hill cipher is a type of polygraphic substitution cipher.

⇒ It works on multiple letters at the same time.

⇒ The way the Hill cipher works as shown below.

1. Treat every letter in the plain-text message as a number, so that A=0, B=1, ... Z = 25.

⇒ It encrypts a group of letters called polygraph.

i.e In like in playfair cipher, as it was encrypting a pair of letters which was called as digraph.

Ex: HE|LL|O2

→ formula - to encrypt a message $C = KP \bmod 26$

where K = key, P = plaintext

Steps - to encrypt a message by Hill cipher :-

1. Choose a key (A key matrix must be a square matrix)
   i.e $A = 0, B = 1, C = 2 \ldots Z = 25$.

Here we can take any key.

Ex: $VIEW = \begin{bmatrix} V & I \\ E & W \end{bmatrix}_{2\times2} = \begin{bmatrix} 21 & 8 \\ 4 & 22 \end{bmatrix}_{2\times2}$

$QUICKNESS = \begin{bmatrix} Q & U & I \\ C & K & N \\ E & S & S \end{bmatrix}_{3\times3} = \begin{bmatrix} 16 & 20 & 8 \\ 2 & 10 & 13 \\ 4 & 18 & 18 \end{bmatrix}$

for Example :- plaintext = ATTACK let key = $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$

Since the key is a 2x2 matrix, plain-text should be converted into vector of length '2'.

So, $\begin{bmatrix} A \\ T \end{bmatrix}_{2\times1} \begin{bmatrix} T \\ A \end{bmatrix}_{2\times1} \begin{bmatrix} C \\ K \end{bmatrix}_{2\times1}$

1. first vector → $\begin{bmatrix} A \\ T \end{bmatrix} = \begin{bmatrix} 0 \\ 19 \end{bmatrix}$

$\therefore C = KP \bmod 26$ (According to formula)

$= \begin{bmatrix} 2 & 3 \\ 2 & 6 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2\times0 + 3\times19 \\ 2\times0 + 6\times19 \end{bmatrix} \bmod 26$

$\Rightarrow \begin{bmatrix} 57 \\ 114 \end{bmatrix} \bmod 26 = \begin{bmatrix} 5 \\ 10 \end{bmatrix} = \begin{bmatrix} F \\ K \end{bmatrix}$

$\therefore \begin{bmatrix} A \\ T \end{bmatrix} = \begin{bmatrix} F \\ K \end{bmatrix} \Rightarrow AT \rightarrow FK.$

(ii) Now, 2nd vector $\begin{bmatrix} T \\ A \end{bmatrix} = \begin{bmatrix} 19 \\ 0 \end{bmatrix}$

$C = KP \bmod 26$

$\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}\begin{bmatrix} 19 \\ 0 \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 2\times19+3\times0 \\ 3\times19+6\times0 \end{bmatrix} \bmod 26$

$\Rightarrow \begin{bmatrix} 38 \\ 57 \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 12 \\ 5 \end{bmatrix} \Rightarrow \begin{bmatrix} M \\ F \end{bmatrix}$

$\therefore \begin{bmatrix} T \\ A \end{bmatrix} = \begin{bmatrix} M \\ F \end{bmatrix}$ ⇒ TA → MF

(iii) 3rd vector $\begin{bmatrix} C \\ K \end{bmatrix} = \begin{bmatrix} 2 \\ 10 \end{bmatrix}$

$C = KP \bmod 26$

$\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}\begin{bmatrix} 2 \\ 10 \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 2\times2+3\times10 \\ 3\times2+6\times10 \end{bmatrix} \bmod 26$

$\Rightarrow \begin{bmatrix} 34 \\ 66 \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 8 \\ 14 \end{bmatrix} = \begin{bmatrix} I \\ O \end{bmatrix}$

$\therefore \begin{bmatrix} C \\ K \end{bmatrix} = \begin{bmatrix} I \\ O \end{bmatrix}$.

∴ plainText = AT/TA/CK
Cipher-text = FK MF IO.

Decription in Hill cipher :

⇒ In Decryption first we have find the inverse of key matrix K^{-1}

⇒ for Decryption $P = K^{-1}C \bmod 26$

Ex :- cipher-text for the plaintext is ATTACK, key $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$

plaintext = ATTACT.

cipher-text = FK MF IO

Steps :-

1. To Decrypt find the Inverse of key matrix K^{-1}

$K^{-1} = \frac{1}{|d|} adj(K)$

Determinent of matrix $d = \begin{vmatrix} a & b \\ c & d \end{vmatrix}$

$d = \begin{vmatrix} 2 & 3 \\ 3 & 6 \end{vmatrix} = |12 - 9| = 3 \quad \therefore |d| = 3.$

Now find the multiplicative inverse of $|d|$

$dd^{-1} = 1 \bmod 26.$

$3 * d^{-1} = 1 \bmod 26$

$d^{-1} = 9.$

By using Hit & Trail method,

$1 \bmod 26 = 1 \Rightarrow 3 * d^{-1} \bmod 26 = 1$

$\Rightarrow 3 \times 9 \bmod 26 = 1$

$\Rightarrow 27 \bmod 26 = 1$

Now find Adjacent of the matrix

let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \Rightarrow Adj(A) = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

$\therefore adj(K) = \begin{bmatrix} 6 & -3 \\ -3 & 2 \end{bmatrix}$ // Add +26 to the Negative Numbers.

$\Rightarrow Adj(K) = \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix}$ and $d^{-1} = 9.$

$K^{-1} = \frac{1}{|d|} adj(K)$

$K^{-1} = 9 \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix} = \begin{bmatrix} 54 & 207 \\ 207 & 18 \end{bmatrix} \bmod 26.$

$K^{-1} = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}$

$\therefore$ Cipher Text = FKMFIO

formula for decryption

$P = K^{-1} C \bmod 26.$

(i) First vector $\begin{bmatrix} F \\ K \end{bmatrix} \cdot \begin{bmatrix} 5 \\ 10 \end{bmatrix}$

$P = K^{-1}C \mod 26$.

$\begin{bmatrix} F \\ K \end{bmatrix} = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 5 \\ 10 \end{bmatrix} \mod 26 \Rightarrow \begin{bmatrix} 260 \\ 305 \end{bmatrix} \mod 26$

$\begin{bmatrix} F \\ K \end{bmatrix} = \begin{bmatrix} 0 \\ 19 \end{bmatrix} \Rightarrow \begin{bmatrix} F \\ K \end{bmatrix} = \begin{bmatrix} A \\ T \end{bmatrix}$

$\therefore FK \rightarrow AT$

(ii) Second vector $\begin{bmatrix} M \\ F \end{bmatrix} = \begin{bmatrix} 12 \\ 5 \end{bmatrix}$

$P = K^{-1}C \mod 26$

$\begin{bmatrix} M \\ F \end{bmatrix} = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 12 \\ 5 \end{bmatrix} \mod 26 \Rightarrow \begin{bmatrix} 149 \\ 390 \end{bmatrix} \mod 26$

$\begin{bmatrix} M \\ F \end{bmatrix} = \begin{bmatrix} 19 \\ 0 \end{bmatrix} = \begin{bmatrix} T \\ A \end{bmatrix}$

$\Rightarrow \therefore MF \rightarrow TA$

(iii) Third vector $\begin{bmatrix} I \\ 0 \end{bmatrix} = \begin{bmatrix} 8 \\ 14 \end{bmatrix}$

$P = K^{-1}C \mod 26$

$$\begin{bmatrix} F \\ 0 \end{bmatrix} = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 8 \\ 14 \end{bmatrix} \text{ mod } 26$$

$$\begin{bmatrix} F \\ 0 \end{bmatrix} = \begin{bmatrix} 366 \\ 459 \end{bmatrix} \text{ mod } 26$$

$$\begin{bmatrix} F \\ 0 \end{bmatrix} \Rightarrow \begin{bmatrix} 2 \\ 10 \end{bmatrix} = \begin{bmatrix} C \\ K \end{bmatrix}$$

$\therefore$ FO $\longrightarrow$ CK.

Cipher Text : FKMFIO

plain Text : ATTACK.

Transpotition Techniques:

* Transposition technique is an encryption method which is achieved by performing permutations over the plain text.

* The various Transposition techniques are.

1. Rail-fence Technique:

* The rail fence technique is the simplest transposition cipher.

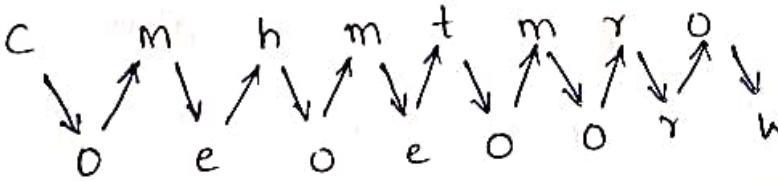
* The steps to obtain cipher text using their technique are as follows.

1. Write down the plain-text message as a sequence of diagonals.
2. Read the plain text written in step 1 as a sequence of rows.

- Example:

plain text : Come home tomorrow.

- Write the plain text sequence wise in a diagonal form.



* Now read the text row by row and write it sequentially.

* Thus we have Cmhmtmroeoeoorw as the cipher text.

- Rail-fence technique is quite simple for a Cryptanalyst to break into.

2. Simple Columnar Transposition Technique:

* The steps involved in Simpler Columnar Transposition Techniques are.

1. Write the plain-text message row by row in a rectangle of a pre-defined size.
2. Read the message column by column. However it need not be in the order of columns 1, 2, 3 etc. It can be any random order such as 2, 3, 1. etc.
3. The message thus obtained is the Cipher-text Message.

- Example:

Plain Text: Come home tomorow.

* Let us consider a rectangle with six Columns.
* Therefore, When we write the Message in the rectangle row by row, it would look as follows.

Column1	Column2	Column3	Column4	Column5	Column6
C	o	m	e	h	o
m	e	t	o	m	o
r	r	o	w		

* Now let us decide the order of columns as some random order say 4, 6, 1, 2, 5 and 3.
* Then read the text in the order of these colaumns.
* The cipher text thus obtained woold be eowoo cmroeihmm -ts.
* The simple columnar transposition technique is also quite simple to break into.

3. Simple Columnar Transposition technique with Multiple rounds.

- The basic algorithm used in this technique is.

1* Write the plain text message row by row in a rectangle of a pre-defined size.

2* Read the message column by column. It can be in any random order.

3* The message thus obtained is the cipher text message of round 1.

4* Repeat steps 1 to 3 as many times as desired.

- Example:

Plain Text : Come home tomorrow.

- Let us consider a rectangle with six columns. Write the message in the rectangle row by row.

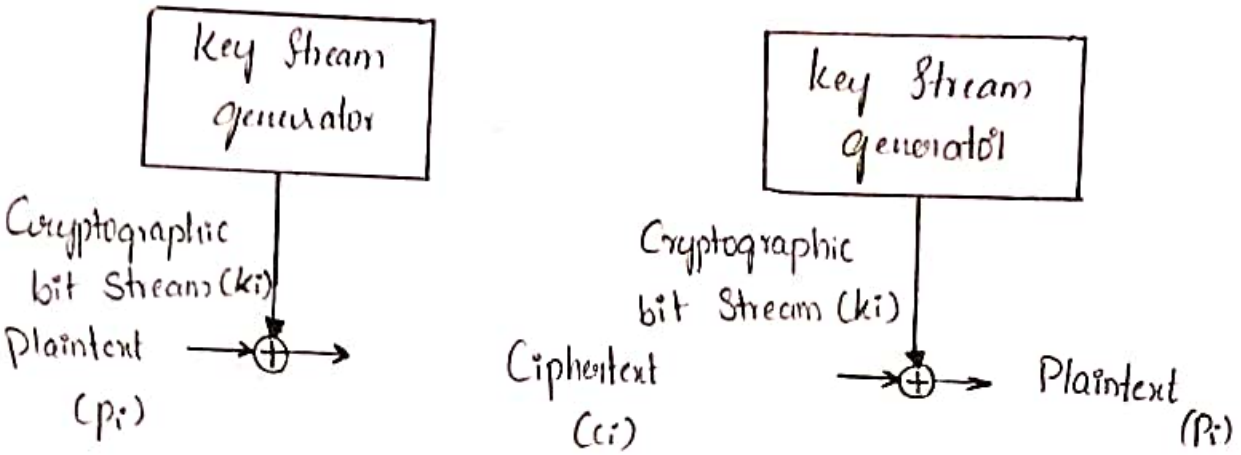
Column 1	Column 2	Column 3	Column 4	Column 5	Column 6
e	o	m	e	h	o
m	e	t	o	m	o
r	r	o	w		

* Now read the text in some random order say 4,6,12,5,3
* The cipher text obtained in round '1' is 'eowoocmroerhmmto'.
* Now steps 1 to 3 are repeated. The tabular representation of cipher text after round 1 is.

Column 1	Column 2	Column 3	Column 4	Column 5	Column 6
e	o	w	o	o	c
m	r	o	e	r	h
m	m	t	o		

* The cipher text thus obtained would be 'oeochemmormorwot'
* Continue like this if more number of iterations is desired, otherwise stop.

4. Vernam Cipher (One-Time Pad) :-
* The vernam cipher is implemented using a random set of non-repeating characters as the input cipher text (key).
* Once an input cipher text four transposition is used, it is never used again for any other message.


Key Stream generator
Cryptographic bit Stream (ki)
Plaintext (pi)
Key Stream generator
Cryptographic bit Stream (ki)
Ciphertext (ci)
Plaintext (Pi)

* The algorithm for vernam cipher is;

1. Treat each plain-text alphabet as a number in an increasing sequence i.e A=0, B=1, ... Z=25.
2. Do the same for each character of the input cipher text.
3. Add each number corresponding to the plain-text alphabet to the corresponding input cipher text alphabet number.
4. If the sum thus obtained is greater than 26, subtract 26 from it.
5. Translate each number of the sum back to the corresponding alphabet. This gives the output cipher text.

Example;

Plain Text : HOW ARE YOU

One time pad : NCB TZQ ARX.

Plain Text :	H	O	W	A	R	E	Y	O	U
	7	14	22	0	17	4	24	14	20
+									
Onetime Pad :	13	2	1	19	25	16	0	17	23
	N	C	B	T	Z	Q	A	R	X
Initial total :	20	16	23	19	42	20	24	31	43
Subtract 26, if > 26 :	20	16	23	19	16	20	24	5	17
Cipher text :	U	Q	X	T	Q	U	Y	F	R

- Note the length of input cipher text is equal to the length of the original plain text.

5. Book Cipher / Running-key Cipher:

- Book Cipher is quite simple, and is similar in principle to the Vernam Cipher.
- For producing cipher text, some portion of text from a book is used, which serves the purpose of a one-time pad.
- Thus the characters from a book are used as one-time pad and they are added to the input plain-text message similar to the way a one-time pad works.

Note:

- A Cryptanalyst is a person who attempts to break a Cipher-text message to obtain the original plain-text message. The process itself is called Cryptanalysis.
- Brute-force attack:

  A Cryptanalyst attempting a brute-force attack tries all possibilites to derive the original plain-text message from a given Cipher-text Message.

Key Range and Key Size :-

- The concept of key range and key size are related to each other.
- Key Range is total number of keys from Smallest to largest available key.
- An attacker usually is armed with the knowledge of the cryptographic algorithm and the encrypted message. So only the actual key value remains the challenge for the attacker.
- If the key is found, the attacker can get original plaintext message.
- In the brute force attack, every possible key in the key-range is tried, until we get the right key.
- In the best case, the right key is found in the first attempt, in the worst case, the key is found in the last attempt.
- On an average, the right key is found after trying half of the possible-keys in the key-range.
- Therefore by expanding the key range to a large extent, longer it will taken for an attacker to find the key using brute-force attack.
- The concept of key range leads to the principle of key size.
- The strength of a cryptographic key is measured with the key size.

- key size is measured in bits and is represented using binary number system.
- Thus if the key range from '0' to '8', then the key size is 3 bits.
- key size may be varying, depending upon the applications and the cryptographic algorithm being used, it can be 40bits, 56 bits, 128 bits & so on.
- In order to protect the cipher-text against the brute-force attack, the-size should be such that the attacker can not crack it within a specified amount of time.
- from a practical viewpoint, a 40-bit key takes about 3 hours to crack, however a 41-bit key would take 6 hours and 42-bit key would take 12 hours & so on.
- This means every additional bit doubles the amount of time required to crack the key.
- We can assume that 128 bit key is quite safe, considering the capabilities of today's computers.
- However as the computing power and techniques improve, thes numbers, will change in future. We would need to rely on keys of size atleast 256 bits or 512 bits.
- Today 56-bit keys are not safe, tomorrow 128-bit keys may not be sufficient, another day 256-bit keys can be cracked and so on.

- In the future we may not have to look beyond 512-bit key at any point i.e 512-bit keys will always be safe.

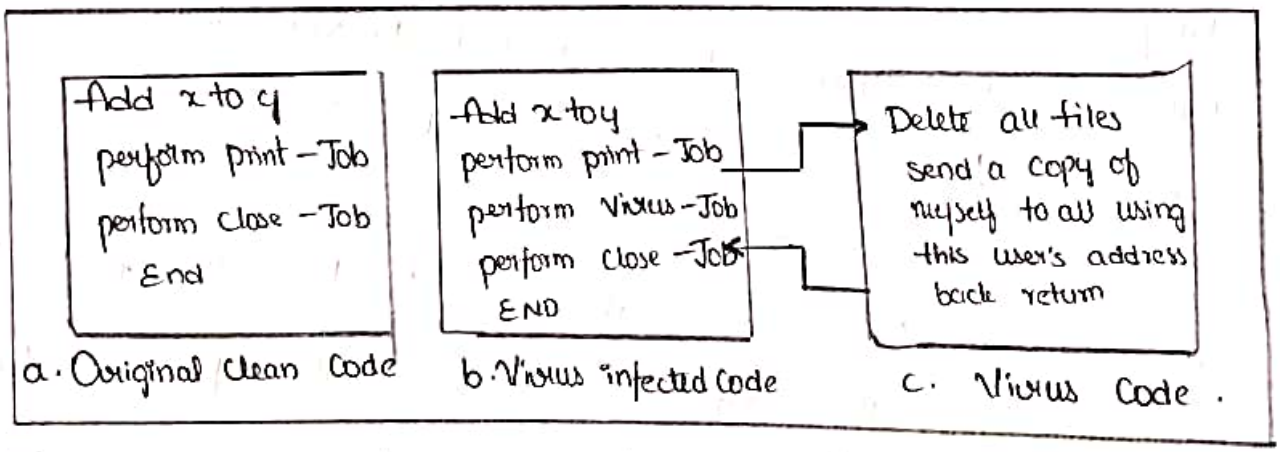
Program that Attack :-

- Program that attack Computer Systems to cause damage can be categorized as.

1. Virus
2. Worm
3. Trojan Horse

1. Virus :-

- "A Virus is a Computer program that attaches itself to another legitimate program and causes damage to the Computer system or to the network."
- Example :



- The Virus can Self-propagate or get triggered by specific events e.g. a Virus could automatically execute at 12Pm every day.
- During its lifetime, a Virus goes through four phases.

a) Dormant Phase :-

* Here the Virus is idle.
* It gets activated based on a Cutain action or event.

b) Propagation Phase :

- In this phase, a virus copies itself and each copy start creating more copies of itself.

c) Triggering phase :

- A dormant virus moves into this phase when the action/event for which it was waiting is initiated.

d) Execution Phase :

- This is the actual work of the virus, which could be harmless (display some message on the screen) or destructive (delete a file on the disk).

- Virus can be classified into following categories.

(a) Parasitic Virus :-

* Such a virus attaches itself to executable files and keeps replicating.
* Whenever the infected file is executed the virus looks for other executable files to attach itself and spread.

(b) Memory-resident Virus :-

* This type of virus first attaches itself to an area of the main memory and then infects every executable program that is executed.

(c) Boot Sector Virus :

* This type of virus infects the master boot record of the disk and spreads on the disk when the operating system starts booting the computer.

(d) Stealth Virus:
- This virus has intelligente built-in, which prevents anti-virus software from detecting it.

(e) Polymorphic Virus:
- A virus that keeps changing its signature (i.e identity) on every execution, making it every difficult to detect.

(f) Metamorphic Virus:
- In addition to changing its signature this type of virus keeps rewriting itself every time, making its detection even harder.

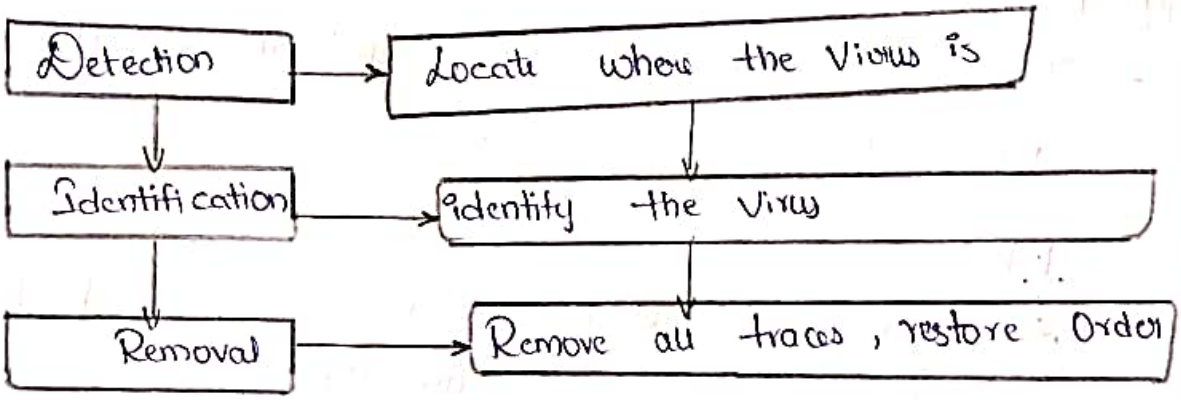
(g) Macro Virus:
- This virus affects specific application software, such as Microsoft Word & Excel.

(2) Worm:-
- Unlike virus, a Worm does not modify a program. Instead it replicates itself again and again.
- The replication grows so much that ultimately the Computer & the network becomes very slow, ultimately coming to a halt.
- The basic purpose of worm attack is to make the Computer & the network under attack unusable by eating all its resources.

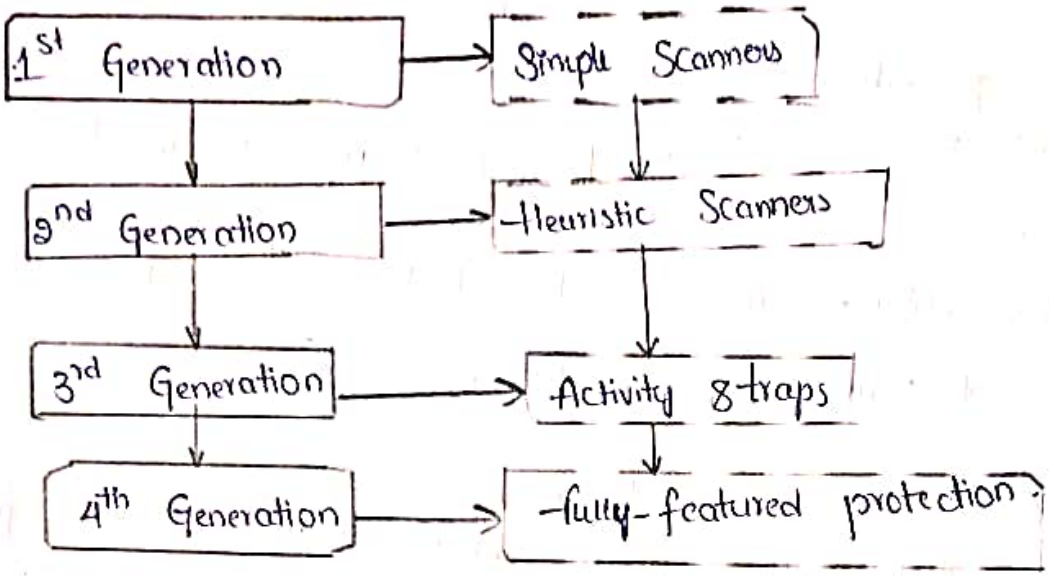
(3) Trojan Horse:
- A Trojan horse is a hidden piece of code that attacks a Computer & network to reveal confidential information to an attacker.

- for e.g. a Trojan horse could silently sit in the code for a login screen by attaching itself to it.
- When the user enters the user id and password, the Trojan horse could capture these details and send this information to the attacker.
- The attacker can then misuse the user id and password to gain access to the system.

- **Dealing With Viruses :-**
- following steps can be implemented to eliminate Virus.



- Detection of Viruses involves locating the virus.
- Then we need to identify the specific virus that has attacked.
- finally we need to remove it. for this we need to remove all traces of the virus and restore the affected program/file to their original states. This is done by anti-Virus Software.
- Anti-Virus Software is classified into four generations, as shown below.



1. First Generation :-

- These anti-Virus Software were called simple Scanner.
- They needed a virus Signature to identify a virus.
- A Variation of such program kept a watch on the length of programs and looked for changes so as to possibly identify a virus attack.

2. Second Generation :-

- These anti-Virus Software used heuristic rules to look for possible virus attacks.
- The idea was to look for code blocks that were commonly associated with viruses.
- for examples such a program could look for an encryption key used by a virus, find it, decrypt and remove the virus.

3. Third Generation :-

- These anti-Virus Software programs were memory resident
- They watched for viruses based on actions rather than their Structure.
- Thus, it is not necessary to maintain a large database of virus Signatures, Instead, the focus is to keep watch on a small

number of Suspect actions.

4. Fourth Generation :-

- These anti-Virus Software package many anti-Virus techniques together.
- They also Contains access control features, thess preventing the attempts of Viruses to infect files.

* Behaviour - blocking Software :-

- It is a Category of software which integrates with the Operating System of the Computer and keeps a watch on virus-like an action is detected, this Software blocks, it preventing damages.
- The actions Under watch can be :
  * Opening, Viewing, modifying, deleting files.
  * Network Communications.
  * Modification of settings Such as Start-up Script.
  * Attempts to formal disk.
  * Modification of Executable files.
  * Scripting of email and instant Messaging to send executable Content to others.

Specific Attacks:-

(1) Sniffing and Spoofing:-

- On the Internet, Computer exchange messages in the form of packets.
- Attackers target these packets, as they travel from a source Computer to destination computer over the Internet.
- These attacks take two main forms:-
  - (a) Packet Sniffing (or) IP Sniffing (or) Snooping
  - (b) Pack Spoofing (or) IP Spoofing

a) Packet Sniffing:-

- Packet Sniffing is a passive attack on an ongoing Conversation.
- An attacker need not hijack a conversation, but instead, can simple observe packets as they pass by.
- To prevent an attacker from Sniffing packets, the information that is passing an attack needs to be protected in some ways.
- This can be done at two levels.
  - (1) The data that is travelling can be encoded in some ways.
  - (2) The transmission link itself can be encoded.

b) Packet Spoofing:-

- In this technique, an attacker sends packets with an incorrect source address.
- When this happens, the receiver would send replies back to the forged address.
- This can lead to three possible cases.

(1) The attacker can intercept the reply.

- The attacker can intercept see the reply and use that information for hijacking attacks.

(2) The attacker need not see the reply.

- If the attacker's intention was a Denial of Service he need to not bother about the rely.

(3) The attacker does not want the rely:

- The attacker does not want a reply from the destination as it wants the host with the forged address to receive it and get confused.

2. Phishing:

- Phishing is a type of network security. attack that attempts to obtain data that are sensitive like username, password or PIN.
- It attacks the user through mail, text or direct messages.
- A real-life example of this kind of attack is a fake email sent by an attacker to an authorized paypal user.
- Here the attacker is trying to fool the paypal customer to verify his/her credit-card details.
- Once the user provides these details, the attacker misuse it.
- He simply uses these credit-card details to make purchases on behalf of the cheated card holder.

(3) Pharming (DNS Spoofing):

- Pharming is the process of poisoning entries on a DNS server to redirect a targeted user to a malicious website under attacker control.
- Suppose that there is a merchant (Bob) whose site's domain name is www.bob.com and IP address is 100.10.10.20.
- Therefore, the DNS entry for Bob in all the DNS servers in maintained as follows.

  WWW.bob.com 100.10.10.20

- The attacker say Trudy Manages to hack and replace the IP address of Bob with her own IP say 100.20.20.20 in the DSN server maintained by the ISP of a user, say Alice.
- When Alice wants to communicate with Bob site, her web (Address (Alice is 100.20.20.) browser queries the DNS server. Alice gets replaced IP address which is 100.20.20.20.
- Now, Alice starts communicating with Trudy, believing that she is communicating with Bob.
- A protocol called DNSSec (Secure DNS) is being used to prevent such attacks.