Information Security

1) State and explain principals of security.

Ans i) Confidentiality: Information is not disclosed to unauthorized individuals, entities and process. Ex: Gmail password

(ii) Integrity: Maintaining accuracy and completeness of data. Data cannot be edited in an unauthorized way. Ex: If person leaves the job.

(iii) Availability: Information must be available when needed. Ex: To access information of a particular employee.

(iv) Non-repudiation: One party cannot deny receiving a message or a transaction nor can the other party deny sending a message or a transaction.

- **Ex: In cryptography it is sufficient to show that message matches the digital signature signed with sender's private key and that sender could have a sent a message and nobody else could have altered it in transit.**

(v) Authenticity: Verifying that users are who they say they are and that each input arriving at destination is from a trusted source.

Ex: If sender sends the message along with digital signature which was generated using the hash value of message and private key. Now at the receiver side this digital signature is decrypted using the public key generating a hash value and message is again hashed to generate the hash value. If the 2 value matches then it is known as valid transmission with the authentic or we say genuine message received at the recipient side.

(vi) Accountability: It should be possible to trace actions of an entity uniquely to that entity. Ex: Not every employee should be allowed to do changes in other employees data. For this there is a separate department in an organization that is responsible for making such changes. Approval from higher authority.

2) What is non-repudiation?

Ans) Non-repudiation: One party cannot deny receiving a message or a transaction nor can the other party deny sending a message or a transaction.

• Ex: In cryptography it is sufficient to show that message matches the digital signature signed with sender's private key and that sender could have a sent a message and nobody else could have altered it in transit.

3) State some advantages and disadvantages of Information Security.

Ans) Advantages:

(i) Improved security: By identifying and classifying sensitive information, organizations can better protect their most critical assets from unauthorized access or disclosure.

(ii) Compliance: Many regulatory and industry standards require organizations to implement information classification and data protection measures.

(iii) Improved efficiency: By clearly identifying and labelling information, employees can quickly and easily determine the appropriate handling and access requirements for different types of data.

(iv) Better risk management: By understanding the potential impact of a data breach or unauthorized disclosure, organizations can prioritize resources and develop more incident response plans.

Disadvantages:

(i) Complexity: Developing and maintaining an information classification system can be complex and time-consuming, especially for large organizations with a diverse range of data types.

(ii) Cost: Implementing and maintaining an information classification system can be costly, especially if it requires new hardware or software.

(iii) Resistance to change: Some employees may resist the implementation of an information classification system, especially if it requires them to change their usual work habits.

(iv) Lack of flexibility: Information classification systems can be rigid and inflexible, making it difficult to adapt to changing business needs or new types of data.

4) What are different types of criminal attacks?

Ans) TYPES OF CRIMINAL ATTACKS:

(i) FRAUD: Credit cards, ATMs, stock certificates, etc.

(ii) SCAMS: Nigeria Scam.

(iii) DESTRUCTION: Unhappy employees.

(iv) IDENTITY THEFT: Stealing password.

(v) INTELLECTUAL PROPERTY THEFT: Digital videos, music, software, sounds, etc.

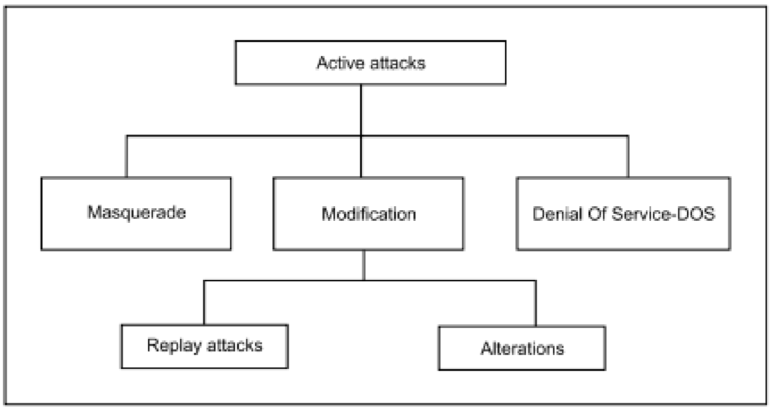
(vi) BRAND THEFT: Setting up fake website.

5) State and explain active attacks.

OR

Write a short note on active attacks.

Ans) Active attacks: Based on the modification of the original message in some manner, or in the creation of false message.



- **Masquerade Attack: When an unauthorized entity pretends to be another entity. The attack may involve capturing the user's authentication sequence (e.g. user ID and password). Later, those details can be replayed to gain illegal access to the computer system.**

- **Modification:**
  - ➢ **Replay Attack: A user captures a sequence of events, or some data units, and re-sends them.**

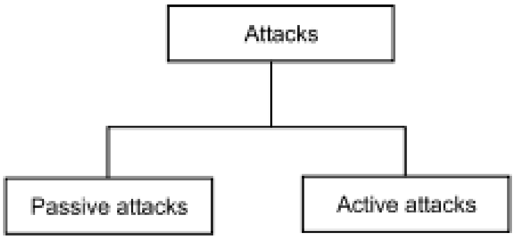
- **Alteration of messages: Involves some change to the original message.**

• Denial Of Service (DOS): Attacks make an attempt to prevent legitimate users from accessing some services, which they are eligible for.

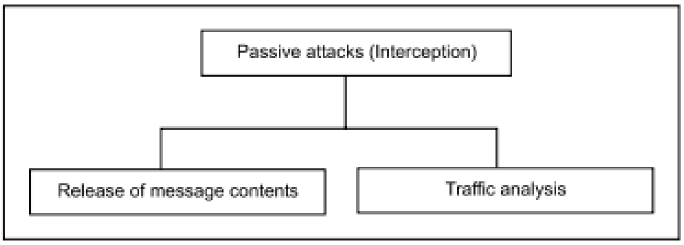
- **For instance, an unauthorized user might send too many login requests to a server using random user ids in quick succession, so as to flood the network and deny other legitimate users to use the network facilities.**

6) Differentiate between active attacks and passive attacks.

Ans)



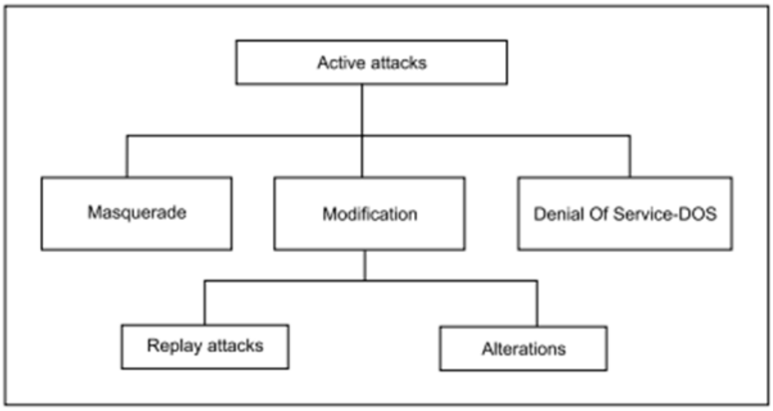
(i) Passive Attacks: Passive attacks are those wherein the attacker indulges in monitoring of data transmission. Passive attacks do not involve any modifications to the contents of an original message.



• Release of message contents: When the contents of the message is confidential, only the sender and the receiver should have an access. Release of message to someone else refers to Release of message contents. We can encode messages to prevent such problem.

• Traffic-analysis attack attempts of analysing (encoded) messages. A passive attacker could try to come up with some sort of pattern that provides some clues regarding the communication that is taking place.

(ii) Active attacks: Based on the modification of the original message in some manner, or in the creation of false message.



• Masquerade Attack: When an unauthorized entity pretends to be another entity. The attack may involve capturing the user's authentication sequence (e.g. user ID and password). Later, those details can be replayed to gain illegal access to the computer system.

• Modification:

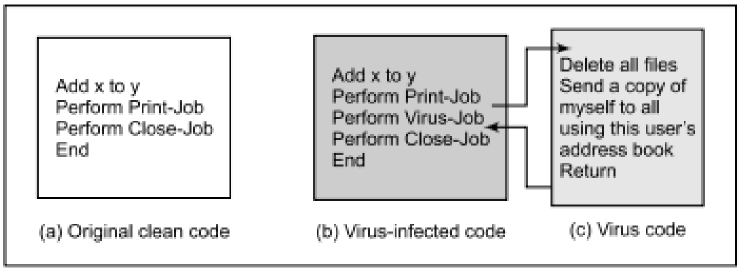
- **Replay Attack: A user captures a sequence of events, or some data units, and re-sends them.**
- **Alteration of messages: Involves some change to the original message.**

• Denial Of Service (DOS): Attacks make an attempt to prevent legitimate users from accessing some services, which they are eligible for.

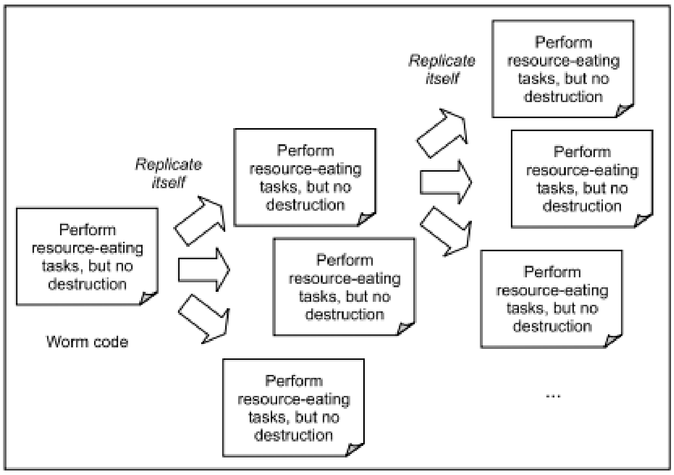
- **For instance, an unauthorized user might send too many login requests to a server using random user ids in quick succession, so as to flood the network and deny other legitimate users to use the network facilities.**

7) Explain different types of programs that attacks.

Ans i) 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.

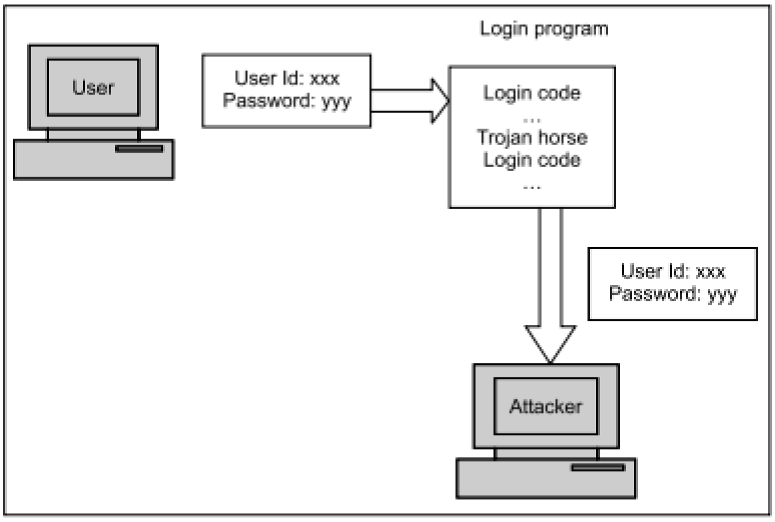


(ii) Worm: A worm does not perform any destructive actions, and instead, only consumes system resources to bring it down.


Worm code
Perform resource-eating tasks, but no destruction
Replicate itself
Perform resource-eating tasks, but no destruction
Perform resource-eating tasks, but no destruction
Perform resource-eating tasks, but no destruction
Replicate itself
Perform resource-eating tasks, but no destruction
Perform resource-eating tasks, but no destruction
Perform resource-eating tasks, but no destruction
...

Worm

(iii) Trojan Horse: A Trojan horse is a hidden piece of code. a trojan horse attempts to reveal confidential information to an attacker.



Trojan horse

8) What do you mean by sniffing and spoofing?

Ans i) Sniffing and Spoofing: On the Internet, computers exchange messages with each other in the form of small groups of data, called packets.

A packet, like a postal envelope contains the actual data to be sent, and the addressing information.

Attackers target these packets, as they travel from the source computer to the destination computer over the Internet.

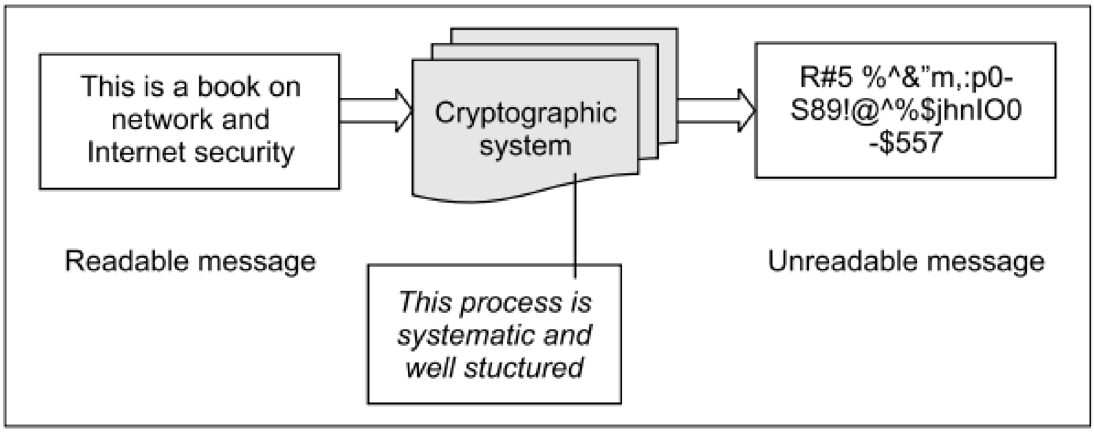
(ii) Packet Sniffing: Packet sniffing is a passive attack on an ongoing conversation.

An attacker need not hijack a conversation, but instead, can simply observe (i.e. sniff) packets as they pass by.

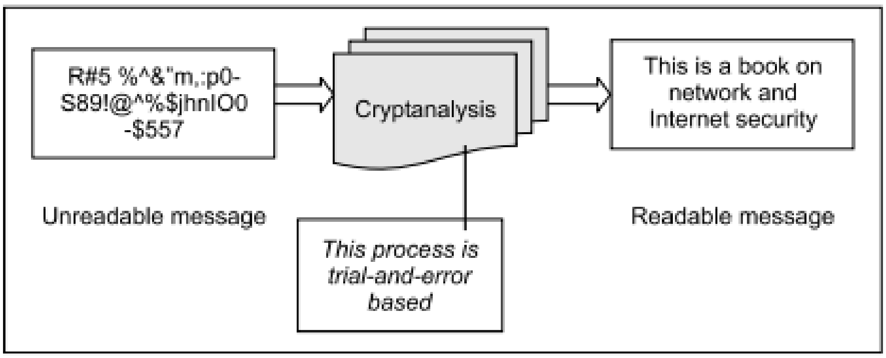
(iii) Packet Spoofing: In this technique, an attacker sends packets with an incorrect source address.

9) Define cryptography and crypt-analysis with the help of a neat diagram.

Ans) Cryptography is the art of achieving security by encoding messages to make them non-readable.


This is a book on network and Internet security
Cryptographic system
R#5 %^&"m,:p0-S89!@^%$jhnIO0 -$557
Readable message
Unreadable message
This process is systematic and well stuctured

Cryptanalysis is the technique of decoding messages from a non-readable format back to a readable format without knowing how they were initially converted from readable format to non-readable format.


R#5 %^&"m,:p0-S89!@^%$jhnIO0 -$557
Cryptanalysis
This is a book on network and Internet security
Unreadable message
Readable message
This process is trial-and-error based

Cryptology is a combination of cryptography and cryptanalysis.

Cryptography + Cryptanalysis = Cryptology.

10) Define encryption and decryption with the help of a neat diagram.

Ans i) ENCRYPTION: The process of encoding plaintext messages into cipher text messages.

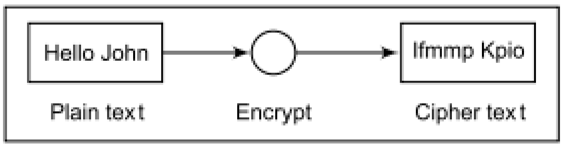


Fig. 2.43 Encryption

(ii) DECRYPTION: The reverse process of transforming cipher-text messages back to plain text messages.

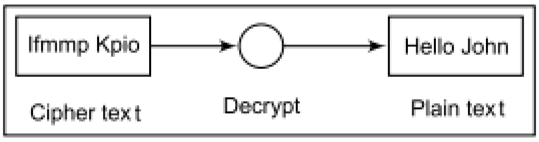
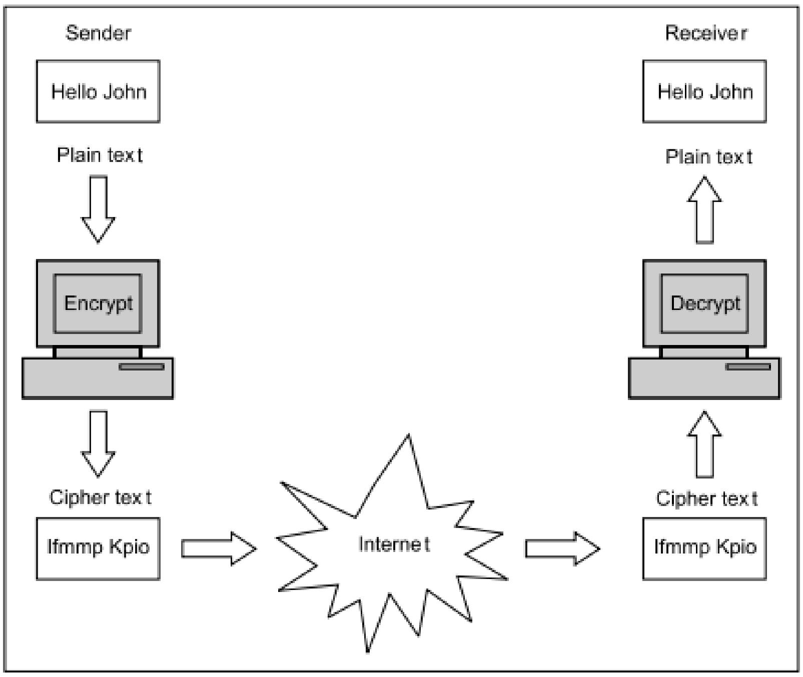


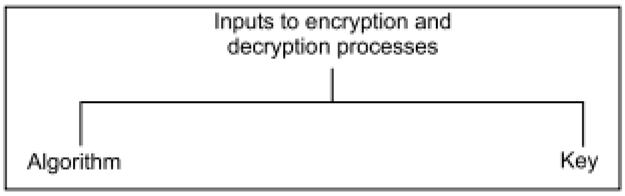
Fig. 2.44 Decryption



ɟ. **2.45** Encryption and decryption in the real world

11) What do you mean by a algorithm and a key?

Ans) Algorithm and Key are the aspects of Encryption and Decryption.



(i) How to open the lock is an algorithm (pieces of public knowledge).

(ii) However, the actual value of the key required for opening a specific lock is the key.

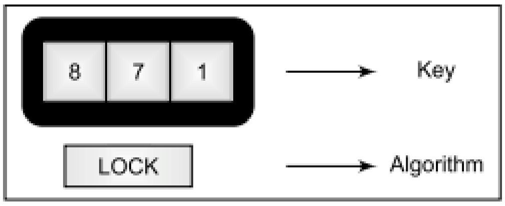
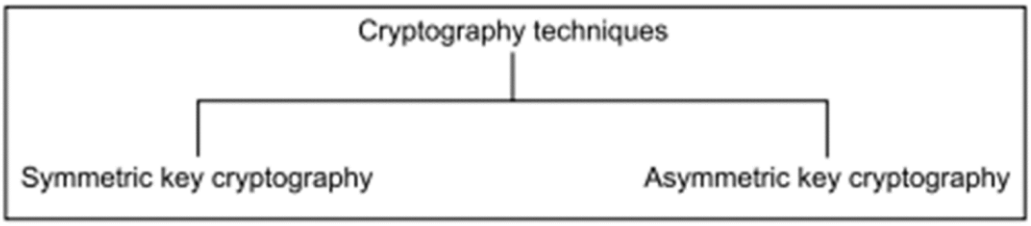


Fig. 2.47 Combination lock

12) Define symmetric and asymmetric key cryptography.

Ans)



(i) Symmetric key cryptography: If the same key is used for encryption and decryption. It is also called as Private key.

(ii) Asymmetric key cryptography: If two different keys are used in a cryptographic mechanism, wherein one key is used for encryption, and another, different key is used for decryption. It is also called as Public key.

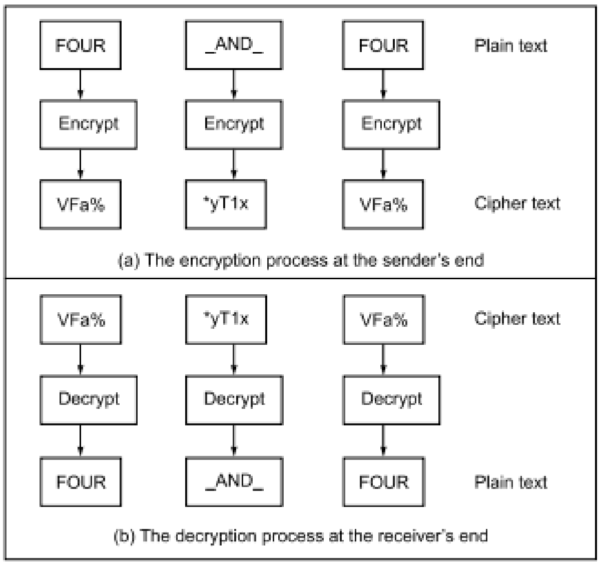
13) Differentiate between private and public key.

Ans)

Private Key	**Public Key**
(i) In this, the same key (secret key) and algorithm are used to encrypt and decrypt the message.	(i) In public-key cryptography, two keys are used, one key is used for encryption, and the other is used for decryption.
(ii) In private key cryptography, the key is kept a secret.	(ii) In public-key cryptography, one of the two keys is kept a secret.
(iii) It is Symmetrical because there is only one key that is called a secret key.	(iii) It is Asymmetrical because there are two types of keys: private and public keys.
(iv) In this cryptography, the sender and receiver need to share the same key.	(iv) In this cryptography, the sender and receiver do not need to share the same key.
(v) It is an efficient technology.	(v) It is an inefficient technology.

14) Explain block cryptography with the help of a neat diagram.

Ans) BLOCK ENCRYPTION (BLOCK CIPHER): The block-cipher technique involves encryption of one block of text at a time. Decryption also takes one block of encrypted text at a time.



(a) The encryption process at the sender's end

(b) The decryption process at the receiver's end