UNIT-1

INTRODUCTION TO SECURITY MECHANISMS

1.1 VARIOUS SECURITY TERMS

Computer data often travels from one computer to another, leaving the safety of its protected physical surroundings. Once the data is out of hand, people with bad intentions could modify or forge your data, either for amusement or for their own benefit.

In many cases information is sensitive so we need to take care that only authorized party can get that data.

For its maintenance we require some mechanism or physical device which ensures that it is safe. Such mechanism is known as **Security System.**

Computer Security: The generic name for the collection of tools designed to protect data and to thwart hackers is computer security.

Network Security: Network Security refers to the measures taken by any enterprise or organization to secure its computer network and data using both hardware and software systems. Network security measures are needed to protect data during their transmission.

Internet Security: Internet security refers to security designed to protect systems and the activities of employees and other users while connected to the internet, web browsers, web apps, websites, and networks. Internet security solutions protect users and corporate assets from cybersecurity attacks and threats.

1.1.1 Virus

The Virus is a type of code that enters the system along with any file or programs and carries out malfunctions in the system. The virus-affected program will be a replica of the existing program. They enter the system through any file and when the file runs, parallelly the virus also runs in the background.

There are many ways in which the virus gets into the system. Some of them are through mail attachments, by clicking inappropriate advertisements, and by downloading any software, or files from unauthorized websites. The main objective of viruses is to spread them along different hosts. They steal the personal data and other credentials of the system. The various types of viruses are depicted in this article.

Types of Virus

1) **Parasitic Virus:** The traditional and still most common form of virus. A parasitic virus attaches itself to executable files and replicates, when the infected program is executed, by finding other executable files to infect.
2) **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.
3) **Boot Sector Virus:** Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus.
4) **Stealth Virus:** A form of virus explicitly designed to hide itself from detection by antivirus software.

5) **Polymorphic Virus:** A virus that mutates with every infection, making detection by the "signature" of the virus impossible.
6) **Metamorphic Virus:** As with a polymorphic virus, a metamorphic virus mutates with every infection. The difference is that a metamorphic virus rewrites itself completely at each iteration, increasing the difficulty of detection. Metamorphic viruses my change their behaviour as well as their appearance.

Intruder

An intruder (also called hacker) is an individual who performs security attacks on others domain in a networked computing environment. The intruder may attempt to read privileged data (like password cracking), perform unauthorized modification of data or disrupt normal functioning of data. There are three types of intruders:

1) **Masquerader:** An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account. The masquerader is likely to be an outsider
2) **Misfeasor:** A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges. Misfeasor is an insider.
3) **Clandestine User:** An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection. Clandestine user can be either insider or an outsider.

Insiders

The inside people may be current or former employees, business partners, contractors, or security admins who had access to the confidential information previously. They carry out insider attacks as they are familiar with the computer network system and hold authorised access to all the information. This may involve fraud, theft of confidential or commercially valuable information, theft of intellectual property etc. This form of cyber-attack is extremely dangerous as the attack is led by the system employees, which makes the entire process extremely vulnerable.

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 a vulnerability.

Attack: An attack is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission.

Hacker: A hacker is a person who makes use of computer system to gain unauthorized access to another system for data or who makes another system unavailable.

1.2 SECURITY BASICS

1.2.1 Pillars of Information Security

It is necessary to protect information from being stolen, compromised or attacked. The CIA triad is one of the most important models which is designed to guide policies for information security within an organization. **CIA** stands for: **Confidentiality, Integrity, Availability.** These are considered as three pillars of information security.

1) Confidentiality:

Confidentiality means that only authorized individuals/systems can view sensitive or classified information. The data being sent over the network should not be accessed by unauthorized individuals. The attacker may try to capture the data using different tools available on the Internet and gain access to your information.

For Example: User A sends message to User B. Another User C gets access to this message which is not desired and therefore defeats purpose of confidentiality. This type of attack is called interception.

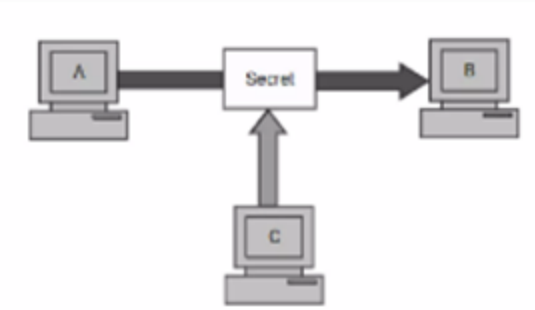


Figure: Loss of Confidentiality

2) Integrity:

The message that is sent from sender to receiver is not modified or altered before it reaches to the receiver. If the message is modified before it reaches to the receiver then integrity is lost.

For Example: User A wants to send message to User B. User C somehow manages to access data of user A, changes its contents and sends changed message to user B. Users A and B have no idea that the contents of message were changed. This type of attack is called modification and we can say that integrity of the message is lost.

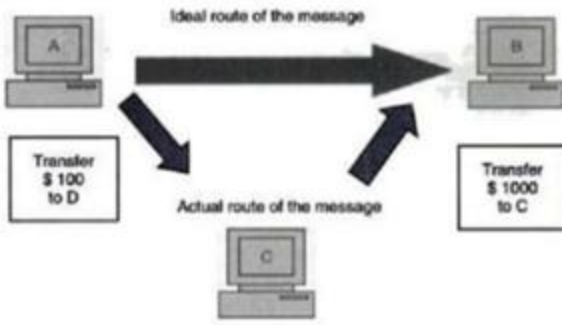


Figure: Loss of Integrity

3) Availability:

It assures that systems work promptly and service is not denied to authorize users. Availability means that information should be available to authorized parties at all times.

For Example: due to the intentional actions of unauthorized User C, an authorised User A may not be able to contact a server computer B. This type of attack is called interruption. Thus, proper measures should be taken to prevent such attacks.

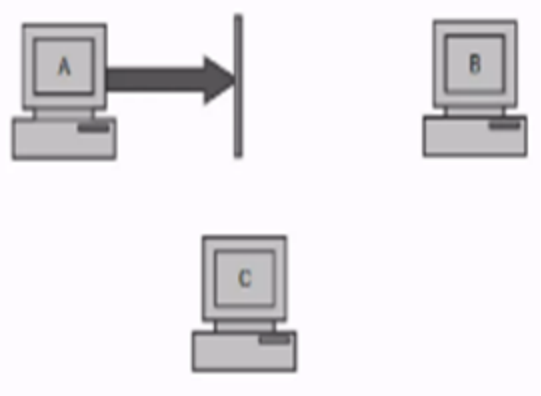


Figure: Loss of Availability

1.2.2 The OSI Security Architecture

The OSI (Open Systems Interconnection) security architecture provides a systematic framework for defining security attacks, mechanisms, and services. This architecture was developed as an international standard, so various vendors have developed security features for their products and services that relate to this structured definition of services and mechanisms.

Security Attacks: Any action that compromises the security of information owned by an organization.

Security Mechanisms: A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

Security Services: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

➢ **Security Services:**

Various security services are explained as follows:

1) Confidentiality: It ensures the protection of data from unauthorized disclosure.

2) Authentication: It is the assurance that the communicating entity is the one that it claims to be.

3) Integrity: The is the assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

4) Non – Repudiation: It provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

5) Access Control: The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

6) Availability: It states that resources/information should be available to authorized parties at all time.

➢ **Security Mechanisms:**

Security mechanisms are classified into two types:

1) Specific Security Mechanism
2) Pervasive Security Mechanism

- **Specific Security Mechanism**

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

b) Digital Signature: A digital signature is an authentication mechanism that enables the creator of a message to attach a code that act as a signature.

c) Access Control: A variety of mechanisms that enforce access rights to resources.

d) Data Integrity: A variety of mechanisms used to assure 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) Routing Control: Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

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

- **Pervasive Security Mechanism**

Pervasive Security Mechanisms 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 (e.g., as established by a security policy).

b) Security Label: The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

c) Event Detection: Detection of security-relevant events.

d) Security Audit Trail: Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.

e) Security Recovery: Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

1.3 TYPES OF COMPUTER AND NETWORK ATTACKS

1.3.1 Security Attacks:

Security Attacks are of two types:

1) Passive Attack
2) Active Attack

- **Passive Attack:**

In passive attack, attacker attempts to learn or make use of information from the system but does not affect system resources. The goal of the opponent/attacker is to obtain information that is transmitted. Passive attacks are of two types:

a) Release of message contents

b) Traffic analysis

a) **Release of Message Contents:**

A Telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information.

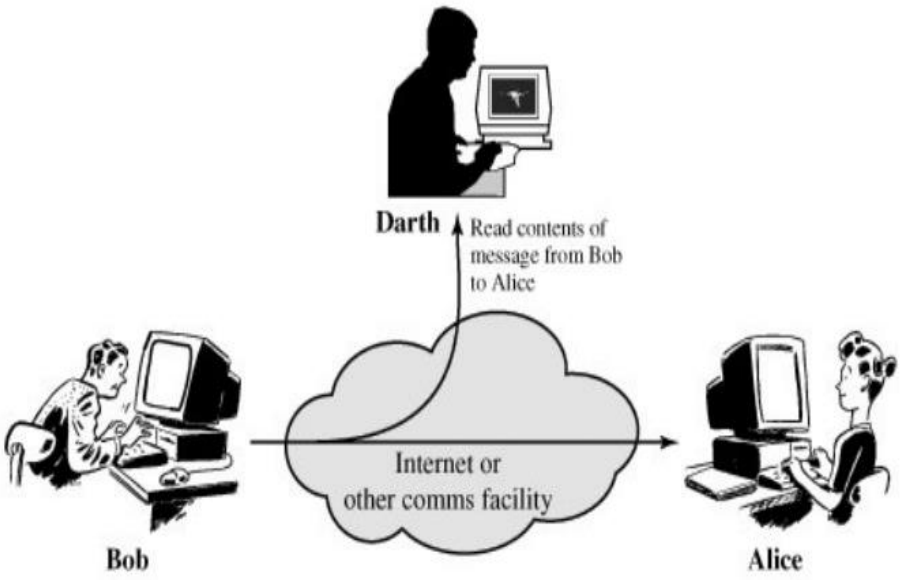


Figure: Release of Message Contents

We would like to prevent an opponent from learning the contents of these transmissions.

b) Traffic Analysis:

Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message.

The common technique for masking contents is encryption. If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages.

The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged.

This information might be useful in guessing the nature of the communication that was taking place.

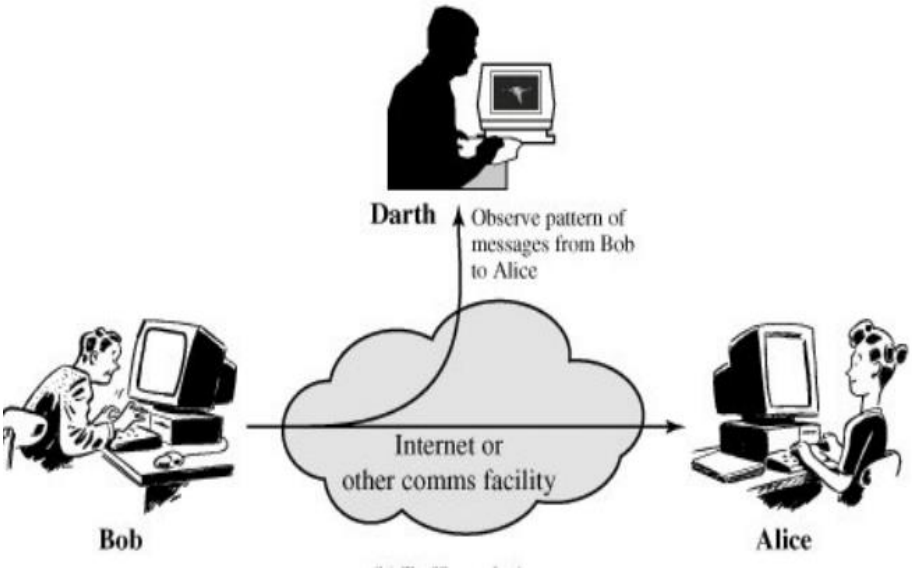


Figure: Traffic Analysis

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

- **Active Attack:**

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

a)Masquerade:

A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification.

If an authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack. Masquerade attacks can be perpetrated using stolen passwords and logons, by locating gaps in programs, or by finding a way around the authentication process.

If they've gained the highest access authority to a business organization. Personal attacks, although less common, can also be harmful.

The attack can be triggered either by someone within the organization or by an outsider if the organization is connected to a public network.

The amount of access masquerade attackers get depends on the level of authorization they've managed to attain. As such, masquerade attackers can have a full smorgasbord of cybercrime opportunities

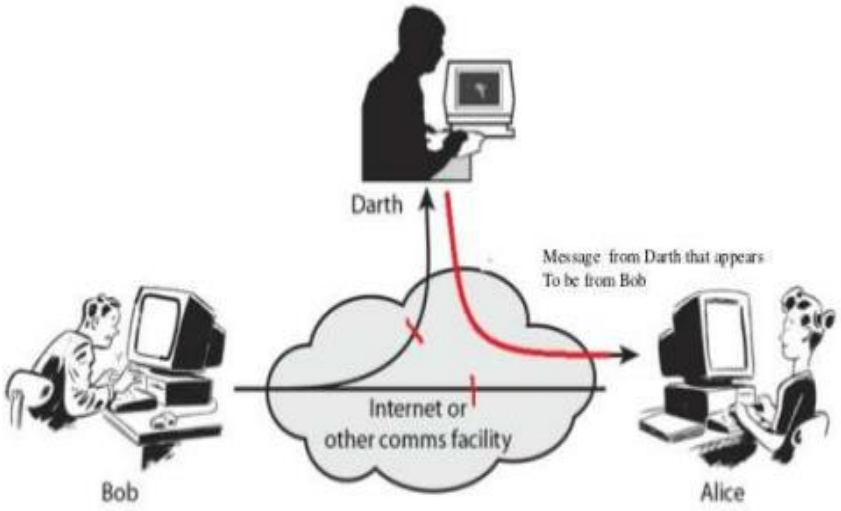
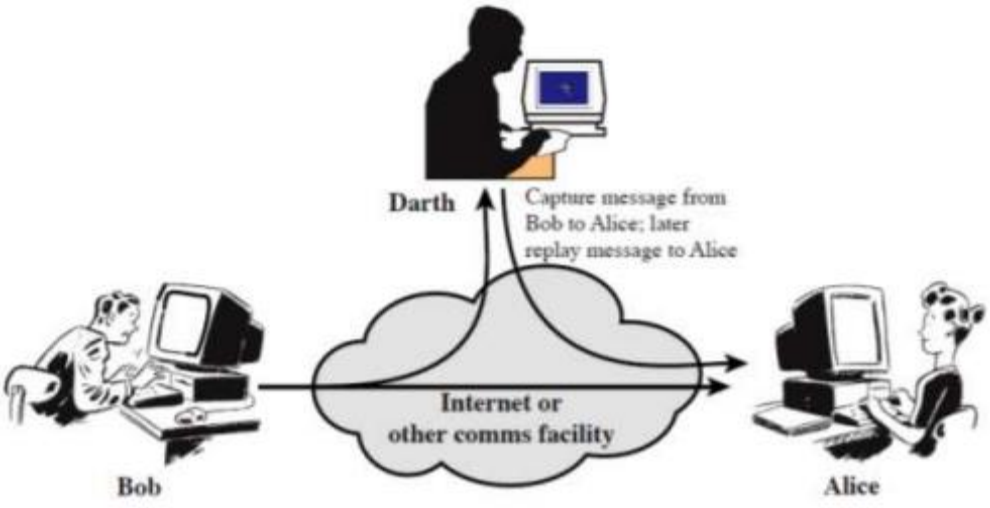


Figure: Release of Message Contents

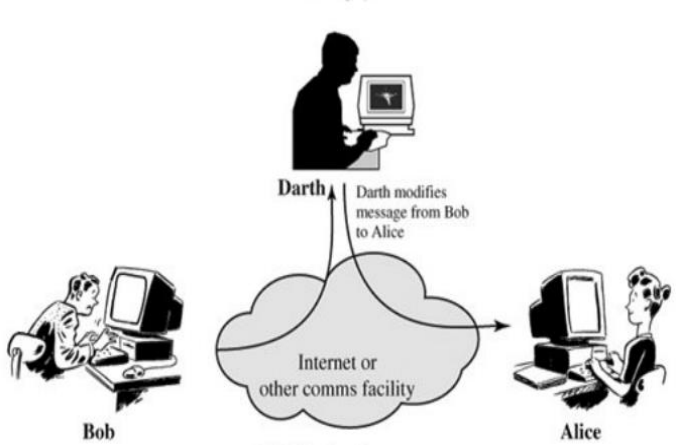
b) Replay:

A replay attack occurs when an attacker eavesdrops on a secure network communication, intercepts it, and then fraudulently delays or resends it to misdirect the receiver into doing what the hacker wants. Consider this real-world example of an attack. A staff member at a company asks for a financial transfer by sending an encrypted message to the company's financial administrator. An attacker eavesdrops on this message, captures it, and is now in a position to resend it. Because it's an authentic message that has simply been resent, the message is already correctly encrypted and looks legitimate to the financial administrator. In this scenario, the financial administrator is likely to respond to this new request unless he or she has a good reason to be suspicious.



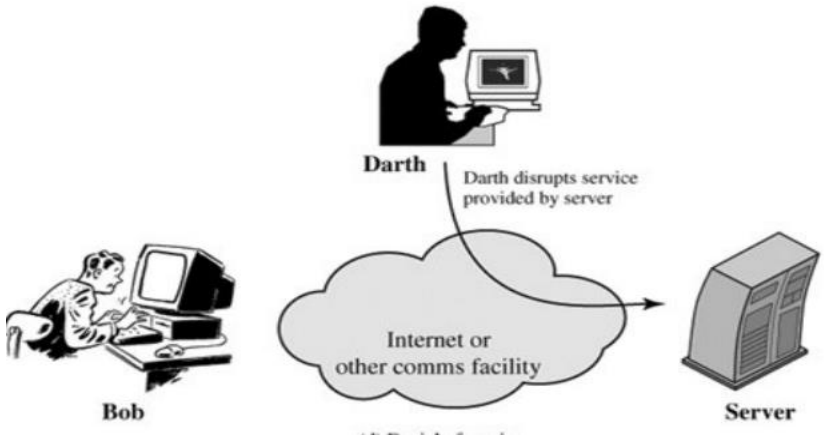
c) Modification of Message:

Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect (Figure 1.4c). For example, a message meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file accounts."



d) Denial of Service:

A denial-of-service (DoS) attack is a security threat that occurs when an attacker makes it impossible for legitimate users to access computer systems, networks, services, or other information technology (IT) resources. Attackers in these types of attacks typically flood web servers, systems or networks with traffic that overwhelms the victim's resources and makes it difficult or impossible for anyone else to access them. DoS and DDoS attacks often take advantage of vulnerabilities in networking protocols and how they handle network traffic. For example, an attacker might overwhelm the service by transmitting many packets to a vulnerable network service from different Internet Protocol (IP) addresses. DoS and DDoS attacks target one or more of the seven layers of the Open Systems Interconnection (OSI) model. The most common OSI targets include Layer 3 (network), Layer 4 (transport), Layer 6 (presentation), and Layer 7 (application). An enterprise that suspects a DoS attack is underway should contact its internet service provider (ISP) to determine whether slow performance or other indications are from an attack or some other factor. The ISP can reroute the malicious traffic to counter the attack. It can also use load balancers to mitigate the severity of the attack.

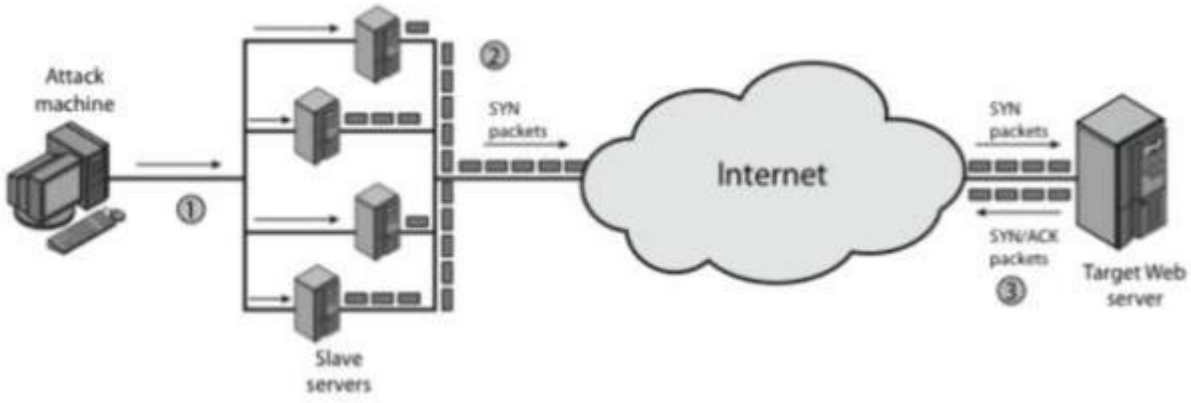


1.3.2 Computer and Network Attack

1) Distributed Denial-of-Service

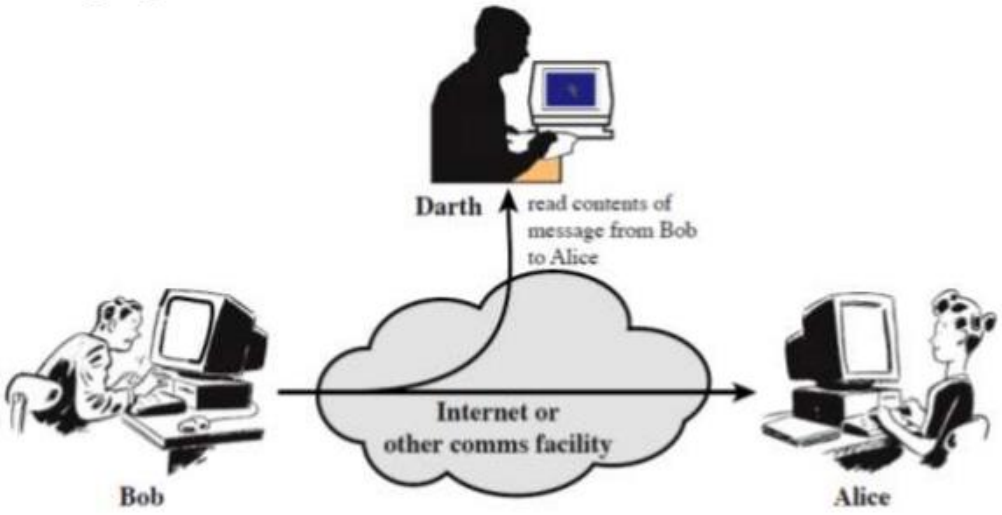
A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT

devices. From a high level, a DDoS attack is like an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination.



2) Eavesdropping

An eavesdropping attack occurs when a hacker intercepts, deletes, or modifies data that is transmitted between two devices. Eavesdropping, also known as sniffing or snooping, relies on unsecured network communications to access data in transit between devices. To further explain the definition of "attacked with eavesdropping", it typically occurs when a user connects to a network in which traffic is not secured or encrypted and sends sensitive business data to a colleague.



The data is transmitted across an open network, which gives an attacker the opportunity to exploit a vulnerability and intercept it via various methods. Eavesdropping attacks can often be difficult to spot. Unlike other forms of cyber-attacks, the presence of a bug or listening device may not adversely affect the performance of devices and networks.

3) Malware

It is short form for malicious software which is specifically designed to disrupt, damage, or gain authorized access to a computer system. Much of the malware out there today is self-replicating: once it infects one host, from that host it seeks entry into other hosts over the Internet, and from the newly infected hosts, it seeks entry into yet more hosts. In this manner, self-replicating malware can spread exponentially fast. Several different

types of malicious software's can be used such as viruses, trojan horses, logic bombs, spyware and worms. All these differs in the way they are installed and their purpose.

4) Man in Middle Attack

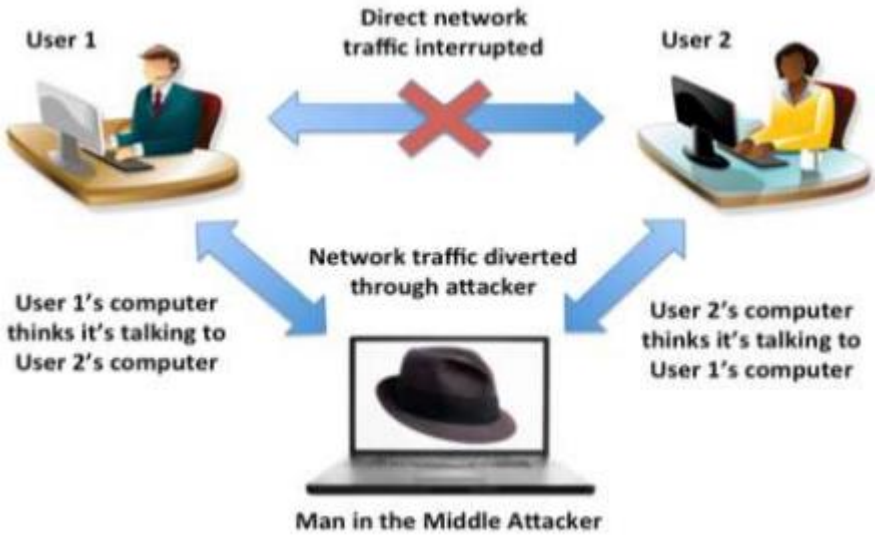
A man in the middle (MITM) attack is a general term for when an attacker positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway. The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers.

A man-in-the-middle (MiTM) attack is a type of attack in which the attacker secretly intercepts and relays messages between two parties who believe they are communicating directly with each other.

The attack is a type of eavesdropping in which the attacker intercepts and then controls the entire conversation. During MiTM attacks, attackers insert themselves in the middle of data transactions or online communication. Through the distribution of malware, the attacker gains easy access to the user's web browser and the data it sends and receives during transactions.

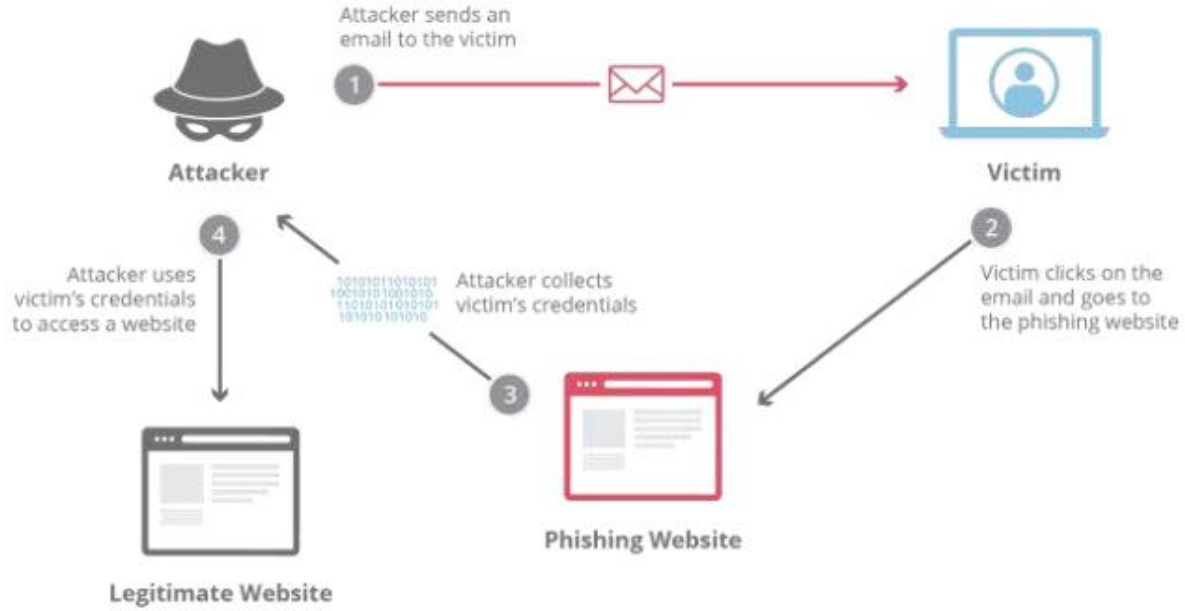
Online banking and e-commerce sites, which require secure authentication with a public key and a private key, are the prime targets of MiTM attacks as they enable attackers to capture login credentials and other confidential information.

Typically, these attacks are carried out through a two-step process known as data interception and decryption. Data interception consists of an attacker intercepting a data transfer between a client and a server. The attacker tricks the client and the server into believing that they are exchanging information with each other, while the attacker intercepts the data, creates a connection to the real site and acts as a proxy to read and insert false information into the communication. The decryption phase is where the intercepted data is unencrypted. This essential step enables the attacker to finally decipher and use the data to their advantage; for example, they can carry out identity theft or cause disruptions to business operations.



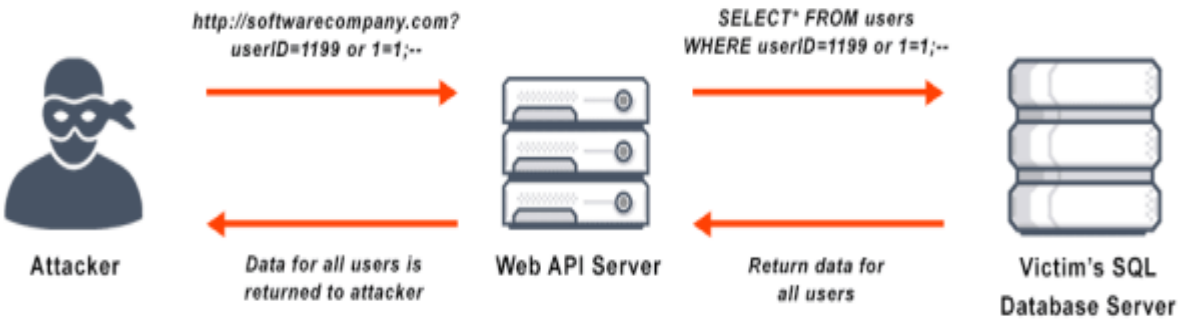
5) Phishing

Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine. Phishing is a common type of cyber-attack that everyone should learn about in order to protect themselves. Phishing starts with a fraudulent email or other communication that is designed to lure a victim. The message is made to look as though it comes from a trusted sender. If it fools the victim, he or she is coaxed into providing confidential information, often on a scam website. Sometimes malware is also downloaded onto the target's computer.



6) SQL Injection:

SQL injection is a technique used to extract user data by injecting web page inputs as statements through SQL commands. Basically, malicious users can use these instructions to manipulate the application's web server. SQL injection is a code injection technique that can compromise your database. SQL injection is one of the most common web hacking techniques. SQL injection is the injection of malicious code into SQL statements via web page input.



SQL injection is a set of SQL commands that are placed in a URL string or in data structures in order to retrieve a response that we want from the databases that are connected with the web applications. This type of attacks generally takes place on webpages developed using PHP or ASP.NET.

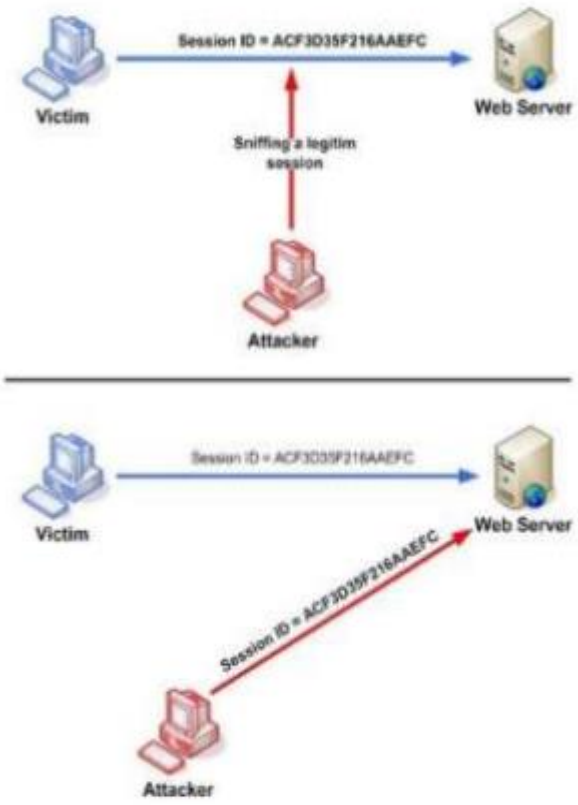
An SQL injection attack can be done with the following intentions −

- To dump the whole database of a system,
- To modify the content of the databases, or
- To perform different queries that are not allowed by the application.

This type of attack works when the applications don't validate the inputs properly, before passing them to an SQL statement. Injections are normally placed put in address bars, search fields, or data fields. The easiest way to detect if a web application is vulnerable to an SQL injection attack is to use the " ' " character in a string and see if you get any error.

7) TCP/IP Hacking

TCP/IP Hijacking is when an authorized user gains access to a genuine network connection of another user. It is done in order to bypass the password authentication which is normally the start of a session. An attacker monitors the data transmission over a network and discovers the IP's of two devices that participate in a connection. When the hacker discovers the IP of one of the users, he can put down the connection of the other user by DoS attack and then resume communication by spoofing the IP of the disconnected user.



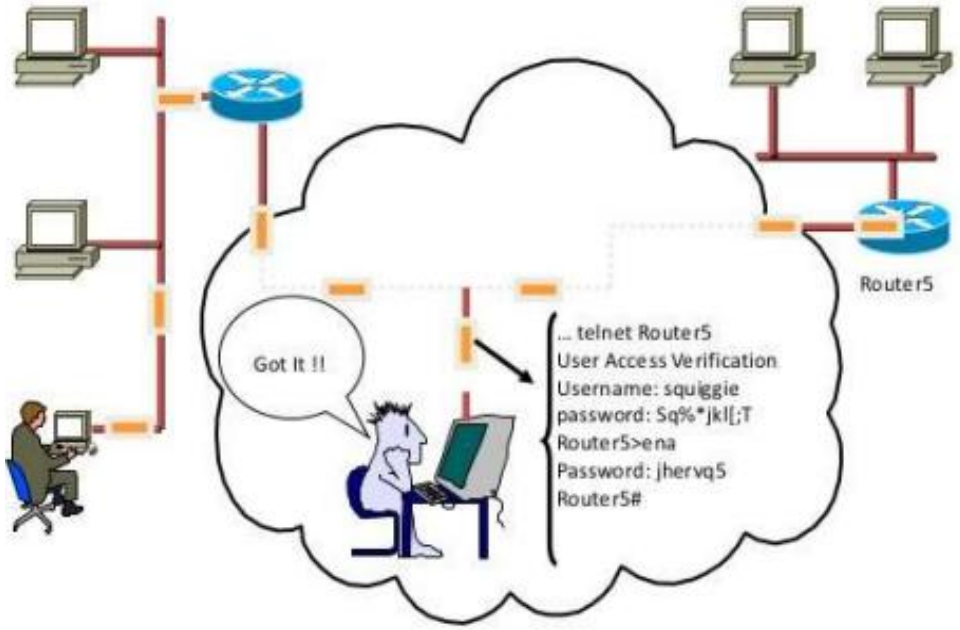
8) Backdoors and Trapdoors

A **Backdoor** Attack is an attempt to infiltrate a system or a network by maliciously taking advantage of software's weak point. Backdoors allow the attackers to quietly get into the system by deceiving the security

protocols and gain administrative access. It is similar to the real-life robbery in which burglars take advantage of the loopholes in a house and get a 'backdoor' entry for conducting the theft. After gaining high-level administrative privilege, the cyber attackers could perform various tasks like injecting spyware, gaining remote access, hack the device, steal sensitive information, encrypt the system through ransomware, and many more. Backdoors are originally meant for helping software developers and testers, so they are not always bad. A **trap door** is kind of a secret entry point into a program that allows anyone to gain access to any system without going through the usual security access procedures. Another definition of a trap door is it is a method of bypassing normal authentication methods. Therefore, it is also known as a back door. Trap Doors are quite difficult to detect and also in order to find them the programmers or the developers have to go through the components of the system. Programmers use Trap door legally to debug and test programs. Trap doors turn to threats when any dishonest programmers gain illegal access. Program development and software update activities should be the first focus of security measures. The operating system that controls the trap doors is difficult to implement.

9) Sniffing

Sniffing attack in context of network security, corresponds to theft or interception of data by capturing the network traffic using a packet sniffer (an application aimed at capturing network packets). When data is transmitted across networks, if the data packets are not encrypted, the data within the network packet can be read using a sniffer. Using a sniffer application, an attacker can analyse the network and gain information to eventually cause the network to crash or to become corrupted, or read the communications happening across the network.



10) Spoofing

Spoofing, is when someone or something pretends to be something else in an attempt to gain our confidence, get access to our systems, steal data, steal money, or spread malware. For example, a spoofed email from PayPal or Amazon might inquire about purchases you never made. Concerned about your account, you might be motivated to click the included link.

From that malicious link, scammers will send you to a web page with a malware download or a faked login page—complete with a familiar logo and spoofed URL— for the purpose of harvesting your username and password.

Difference of Active Attack and Passive Attack

Active Attack	Passive Attack
In an active attack, modification in information takes place.	In a passive attack, modification in the information does not take place.
Active Attack is a danger to integrity as well as availability.	Passive Attack is a danger to confidentiality.
In an active attack, attention is on prevention.	In passive attack attention is on detection.
Due to active attacks, the execution system is always damaged.	Due to passive attack, there is no harm to the system.
In an active attack, victim gets informed about the attack.	In a passive attack, victim does not get informed about the attack.
Active attack is tough to restrict from entering systems or networks.	Passive attack is easy to prohibit in comparison to active attack.
The prevention possibility of active attack is high.	The prevention possibility of passive attack is low.
The duration of an active attack is short.	The duration of passive attack is long.
The purpose of an active attack is to harm the system.	The purpose of passive attack is to learn the system.

Difference of DoS and DDoS

Parameters	DoS	DDoS
Full form	Denial of Service	Distributed Denial of Service
Source of attack	DoS attack typically uses one computer and one internet connection to flood a targeted system or resource	DDoS attack uses multiple computers and internet connections to flood the targeted resource
Protection	System can be stopped/protected easily	Difficult to protect system against DDoS.
Threat Level	Low	Medium to High
Malware involvement	No malware involved	A botnet is usually made up of thousands of infected PC's
Cost and management	Easier to operate and manage	Not easy to manage and operate

1.4 TYPES OF CRYPTOGRAPHY

1.4.1 Introduction to Cryptography

Cryptography is technique of securing information and communications through use of codes so that only those people for whom the information is intended can understand it and process it. Thus, preventing unauthorized access to information. The prefix "crypt" means "hidden" and suffix "graphy" means "writing". In Cryptography the techniques which are used to protect information are obtained from mathematical concepts and a set of rule-based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

Cryptographic systems are characterized along three independent dimensions:

1) The type of operations used for transforming plaintext to ciphertext.

2) The number of keys used.

3) The way in which the plaintext is processed.

Features of Cryptography:

1) Confidentiality

2) Integrity

3) Non-repudiation

4) Authentication

1.4.2 Basic terms used in Cryptography:

1) **Plain Text:** The original message, before being transformed, is called plaintext.
2) **Cipher Text:** The original message after being transformed into non-readable message is called ciphertext.
3) **Encryption:** The process of transforming the plaintext into ciphertext is known as enciphering or encryption. It takes plain text and key value as an input to produce cipher text.
4) **Decryption:** The process of transforming the cipher text back into plain text is known as deciphering or decryption. It takes cipher text and key value as an input to produce plain text back.
5) **Key:** A key is a value or set of values used with plain text and cipher text to perform encryption and decryption.

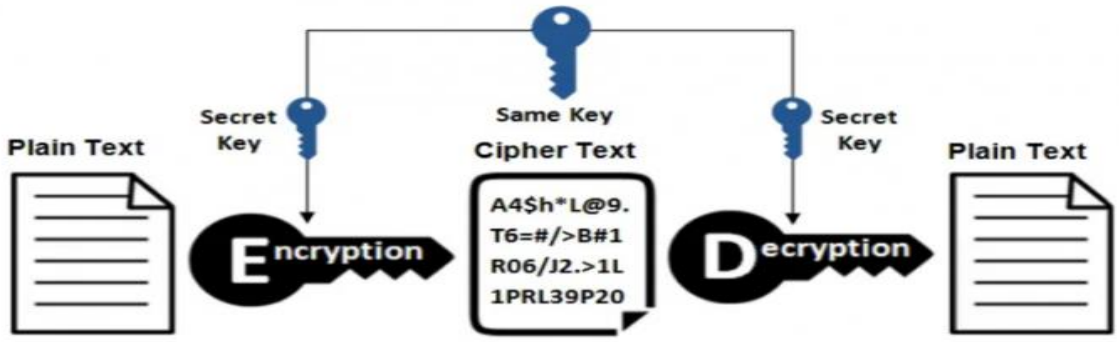
1.4.3 Types of Cryptography

There are three types of cryptography:

1) Symmetric key cryptography
2) Asymmetric key cryptography
3) Hash Function

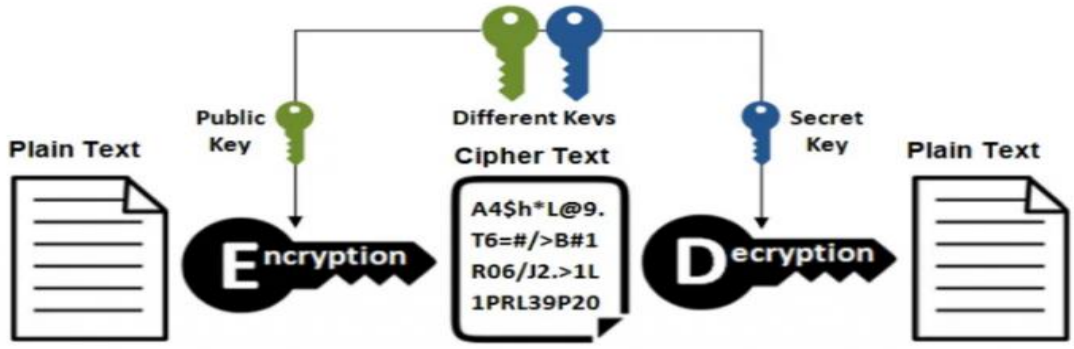
- **Symmetric Key Cryptography:**

Symmetric key cryptography is also known as secret-key cryptography, and in this type of cryptography, you can use only a single key. The sender and the receiver can use that single key to encrypt and decrypt a message. Because there is only one key for encryption and decryption, the symmetric key system has one major disadvantage: the two parties must exchange the key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System (DES) and Advanced Encryption System (AES), Blowfish.



- **Asymmetric Key Cryptography:**

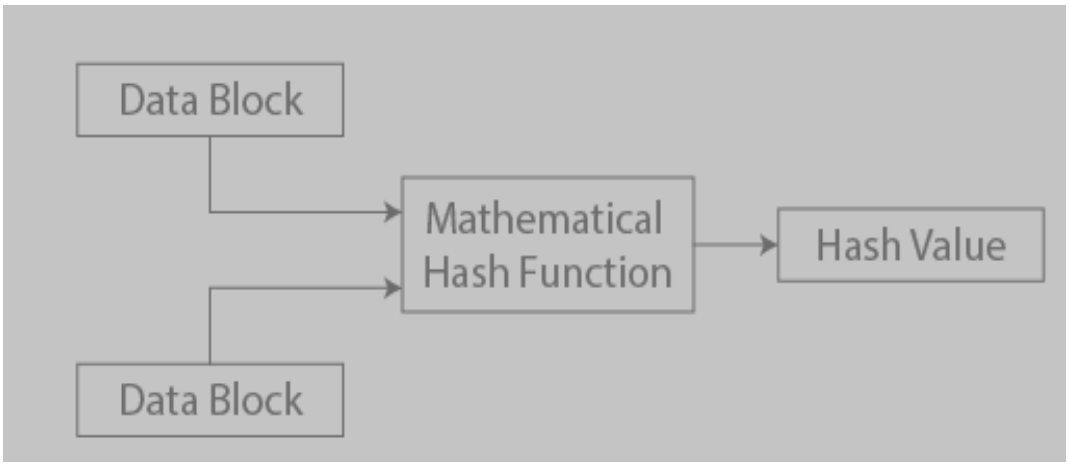
Asymmetric key cryptography is also known as public key cryptography and it employs the use of two keys. This cryptography differs from and is more secure than symmetric key cryptography. In this system, each user encrypts and decrypts using two keys or a pair of keys (private key and public key). Each user keeps the private key secret and the public key is distributed across the network so that anyone can use those public keys to send a message to any other user. You can use any of those keys to encrypt the message and can use the remaining key for decryption. The most popular symmetric key cryptography system is DSA and RSA.



- **Hash Function:**

There is no usage of any key in this algorithm. It is a type of cryptography in which an algorithm followed by a hash function take an arbitrary length of the message as input and returns a fixed length of the output. It is also referred to as a mathematical equation because it uses numerical values as input to generate the hash message. This method does not require a key because it operates in a one-way scenario. Each round of hashing operations considers input as an array of the most recent block and generates the last round of activity as output. Commonly used hash algorithms include:

Message Digest 5 (MD5), SHA (Secure hash Algorithm)



1.4.4 Advantages

1) **Access Control:** Cryptography can be used for access control to ensure that only parties with the proper permissions have access to a resource. Only those with the correct decryption key can access the resource thanks to encryption.
2) **Secure Communication:** For secure online communication, cryptography is crucial. It offers secure mechanisms for transmitting private information like passwords, bank account numbers, and other sensitive data over the internet.
3) **Protection against attacks:** Cryptography aids in the defence against various types of assaults, including replay and man-in-the-middle attacks. It offers strategies for spotting and stopping these assaults.
4) **Compliance with legal requirements:** Cryptography can assist firms in meeting a variety of legal requirements, including data protection and privacy legislation.

1.4.5 Cryptanalysis and Cryptanalytic Attacks

Cryptanalysis which is the study of the cryptographic algorithm and the breaking of those secret codes. The person practicing Cryptanalysis is called a Cryptanalyst. It helps us to better understand the cryptosystems and also helps us improve the system by finding any weak point and thus work on the algorithm to create a more secure secret code.

To determine the weak points of a cryptographic system, it is important to attack the system. This attacks are called Cryptanalytic attacks. The attacks rely on nature of the algorithm and also knowledge of the general characteristics of the plaintext, i.e., plaintext can be a regular document written in English or it can be a code written in Java. Therefore, nature of the plaintext should be known before trying to use the attacks.

Types of Cryptanalytic Attacks:

1) **Known-Plaintext Analysis (KPA):** In this type of attack, some plaintext-ciphertext pairs are already known. Attacker maps them in order to find the encryption key. This attack is easier to use as a lot of information is already available.
2) **Chosen-Plaintext Analysis (CPA):** In this type of attack, the attacker chooses random plaintexts and obtains the corresponding ciphertexts and tries to find the encryption key. It's very simple to implement like KPA but the success rate is quite low.
3) **Ciphertext-Only Analysis (COA):** In this type of attack, only some cipher-text is known and the attacker tries to find the corresponding encryption key and plaintext. Its the hardest to implement but is the most probable attack as only ciphertext is required.
4) **Man-In-The-Middle (MITM) attack:** In this type of attack, attacker intercepts the message/key between two communicating parties through a secured channel.
5) **Adaptive Chosen-Plaintext Analysis (ACPA):** This attack is similar CPA. Here, the attacker requests the cipher texts of additional plaintexts after they have ciphertexts for some texts.
6) **Birthday attack:** This attack exploits the probability of two or more individuals sharing the same birthday in a group of people. In cryptography, this attack is used to find collisions in a hash function.
7) **Side-channel attack:** This type of attack is based on information obtained from the physical implementation of the cryptographic system, rather than on weaknesses in the algorithm itself. Side-channel attacks include timing attacks, power analysis attacks, electromagnetic attacks, and others.
8) **Brute-force attack:** This attack involves trying every possible key until the correct one is found. While this attack is simple to implement, it can be time-consuming and computationally expensive, especially for longer keys.
9) **Differential cryptanalysis:** This type of attack involves comparing pairs of plaintexts and their corresponding ciphertexts to find patterns in the encryption algorithm. It can be effective against block ciphers with certain properties.