## ****Private Key:****

In the Private key, the same key (secret key) is used for encryption and decryption. In this key is symmetric because the only key is copied or shared by another party to decrypt the cipher text. It is faster than public-key cryptography.

## ****Public Key:****

In a [Public key](https://www.geeksforgeeks.org/public-key-encryption/), two keys are used one key is used for encryption and another key is used for decryption. One key (public key) is used to encrypt the plain text to convert it into cipher text and another key (private key) is used by the receiver to decrypt the cipher text to read the message.

## Caesar Cipher Technique

The Caesar cipher is the simplest and oldest method of cryptography. The Caesar cipher method is based on a mono-alphabetic cipher and is also called a shift cipher or additive cipher. Julius Caesar used the shift cipher (additive cipher) technique to communicate with his officers. For this reason, the shift cipher technique is called the Caesar cipher. The Caesar cipher is a kind of replacement (substitution) cipher, where all letter of plain text is replaced by another letter.

Let's take an example to understand the Caesar cipher, suppose we are shifting with 1, then A will be replaced by B, B will be replaced by C, C will be replaced by D, D will be replaced by C, and this process continues until the entire plain text is finished.

Caesar ciphers is a weak method of cryptography. It can be easily hacked. It means the message encrypted by this method can be easily decrypted.

Plaintext: It is a simple message written by the user.

Ciphertext: It is an encrypted message after applying some technique.

The formula of encryption is:

En (x) = (x + n) mod 26

The formula of decryption is:

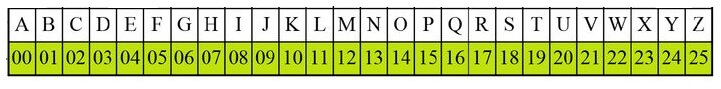
Dn (x) = (xi - n) mod 26

If any case (Dn) value becomes negative (-ve), in this case, we will add 26 in the negative value.

Where,

E denotes the encryption  
D denotes the decryption  
x denotes the letters value  
n denotes the key value (shift value)

Note: "i" denotes the offset of the ith number of the letters, as shown in the table below.



Example: 1 Use the Caesar cipher to encrypt and decrypt the message "JAVATPOINT," and the key (shift) value of this message is 3.

Encryption

We apply encryption formulas by character, based on alphabetical order.

The formula of encryption is:

En (x) = (x + n) mod 26

|  |  |  |
| --- | --- | --- |
| Plaintext: J → 09 | En: (09 + 3) mod 26 | Ciphertext: 12 → M |
| Plaintext: A → 00 | En: (00 + 3) mod 26 | Ciphertext: 3 → D |
| Plaintext: V → 21 | En: (21 + 3) mod 26 | Ciphertext: 24 → Y |
| Plaintext: A → 00 | En: (00 + 3) mod 26 | Ciphertext: 3 → D |
| Plaintext: T → 19 | En: (19 + 3) mod 26 | Ciphertext: 22 → W |
| Plaintext: P → 15 | En: (15 + 3) mod 26 | Ciphertext: 18 → S |
| Plaintext: O → 14 | En: (14 + 3) mod 26 | Ciphertext: 17 → R |
| Plaintext: I → 08 | En: (08 + 3) mod 26 | Ciphertext: 11 → L |
| Plaintext: N → 13 | En: (13 + 3) mod 26 | Ciphertext: 16 → Q |
| Plaintext: T → 19 | En: (19 + 3) mod 26 | Ciphertext: 22 → W |

The encrypted message is "MDYDWSRLQW". Note that the Caesar cipher is monoalphabetic, so the same plaintext letters are encrypted as the same letters. For example, "JAVATPOINT" has "A", encrypted by "D".

Decryption

We apply decryption formulas by character, based on alphabetical order.

The formula of decryption is:

Dn (x) = (xi - n) mod 26

If any case (Dn) value becomes negative (-ve), in this case, we will add 26 in the negative value.

|  |  |  |
| --- | --- | --- |
| Ciphertext: M → 12 | Dn: (12 - 3) mod 26 | Plaintext: 09 → J |
| Ciphertext: D → 03 | Dn: (03 - 3) mod 26 | Plaintext: 0 → A |
| Ciphertext: Y → 24 | Dn: (24 - 3) mod 26 | Plaintext: 21 → V |
| Plaintext: A → 00 | En: (00 + 3) mod 26 | Ciphertext: 3 → D |
| Plaintext: T → 19 | En: (19 + 3) mod 26 | Ciphertext: 22 → W |
| Plaintext: P → 15 | En: (15 + 3) mod 26 | Ciphertext: 18 → S |
| Plaintext: O → 14 | En: (14 + 3) mod 26 | Ciphertext: 17 → R |
| Plaintext: I → 08 | En: (08 + 3) mod 26 | Ciphertext: 11 → L |
| Plaintext: N → 13 | En: (13 + 3) mod 26 | Ciphertext: 16 → Q |
| Plaintext: T → 19 | En: (19 + 3) mod 26 | Ciphertext: 22 → W |

The decrypted message is "JAVATPOINT".

Example: 2 Use the Caesar cipher to encrypt and decrypt the message "HELLO," and the key (shift) value of this message is 15.

### Encryption

We apply encryption formulas by character, based on alphabetical order.

The formula of encryption is:

En (x) = (x + n) mod 26

|  |  |  |
| --- | --- | --- |
| Plaintext: H → 07 | En: (07 + 15) mod 26 | Ciphertext: 22 → W |
| Plaintext: E → 04 | En: (04 + 15) mod 26 | Ciphertext: 19 → T |
| Plaintext: L → 11 | En: (11 + 15) mod 26 | Ciphertext: 00 → A |
| Plaintext: L → 11 | En: (11 + 15) mod 26 | Ciphertext: 00 → A |
| Plaintext: O → 14 | En: (14 + 15) mod 26 | Ciphertext: 03 → D |

Note that the Caesar cipher is monoalphabetic, so the same plaintext letters are encrypted as the same letters. Like, "HELLO" has "L", encrypted by "A".

The encrypted message of this plain text is "WTAAD".

### Decryption

We apply decryption formulas by character, based on alphabetical order.

The formula of decryption is:

Dn (x) = (xi - n) mod 26

|  |  |  |
| --- | --- | --- |
| Ciphertext: W → 22 | Dn: (22 - 15) mod 26 | Plaintext: 07 → H |
| Ciphertext: T → 19 | Dn: (19 - 15) mod 26 | Plaintext: 04 → E |
| Ciphertext: A → 00 | Dn: (00 - 15) mod 26 | Plaintext: 11 → L |
| Ciphertext: A → 00 | Dn: (00 - 15) mod 26 | Plaintext: 11 → L |
| Ciphertext: D → 03 | Dn: (03 - 15) mod 26 | Plaintext: 14 → O |

The decrypted message is "HELLO".

Note: If any case (Dn) value becomes negative (-ve), in this case, we will add 26 in the negative value. Like, the third letter of the ciphertext.

Dn = (00 - 15) mod 26  
= -15

The value of dn is negative, so 26 will be added to it.

= -15 + 26  
= 11

Advantages of Caesar cipher

Its benefits are as follows: -

It is very easy to implement.

This method is the simplest method of cryptography.

Only one short key is used in its entire process.

If a system does not use complex coding techniques, it is the best method for it.

It requires only a few computing resources.

Disadvantages of Caesar cipher

Its disadvantages are as follows: -

It can be easily hacked. It means the message encrypted by this method can be easily decrypted.

It provides very little security.

By looking at the pattern of letters in it, the entire message can be decrypted.

## Greatest Common Factor (GCD) :

The greatest common divisor (also known as greatest common factor, highest common divisor or highest common factor) of a set of numbers is the largest positive integer number that devides all the numbers in the set without remainder. It is the biggest multiple of all numbers in the set.

The GCD is most often calculated for two numbers, when it is used to [reduce fractions to their lowest terms](http://www.alcula.com/calculators/math/simplify-fractions/). When the greatest common divisor of two numbers is 1, the two numbers are said to be coprime or relatively prime.

How is the greatest common divisor calculated?

This calculator uses Euclid's algorithm. To find out more about the Euclid's algorithm or the GCD, see this [Wikipedia article](http://en.wikipedia.org/wiki/Greatest_common_divisor).

The GCD may also be calculated using the [least common multiple](http://www.alcula.com/calculators/math/lcm/) using this formula:

$ GCD(a,b) = \frac{\left| a \cdot b \right|}{LCM(a,b)} $

In mathematics, the **greatest common factor** or **greatest common divisor** of two or more integers is the largest positive integer that divides each of the integers completely.

In this section, we will learn about **factors, common factors,** and **greatest common factor**. Before moving to the greatest common factor, first, we will understand **factor** and **common factor**.

**Factors:** Factors are whole numbers that multiplied together to get another number. A number may have more than two factors. For example, **5×3=15, 1×15=15** where 5, 3, 1 and 15 are the factors of 15. Similarly, the factors of 24 are: **1×24=24, 2×12=24, 3×8=24, 4×6=24**. Hence, the factors of 24 are **1, 2, 3, 4, 6, 8, 12, 24**.

2.1 Try Catch

**Common Factors:** The factor(s) that are common in two or more numbers is called the common factor(s). In other words, common factor(s) are numbers that you can multiply together to produce another number. The numbers should divide exactly into two or more numbers. It is necessary to have at least two numbers to find the common factor(s). For example, we have to find the factor of 12 and 16.

**Factors of 12:** 1, 2, 3, 4, 6, 12

**Factors of 16:** 1, 2, 4, 8, 16

We see that **1, 2,** and **4** is common in both. So, these are the common factors of the integer 12 and 16.

In the above examples, we have observed that 1 and the number itself appears in both the factors. So, we can conclude that **1** and the **number itself** are the two factors of ever number.

**Greatest Common Factor:** It is the highest number that completely divides two or more numbers. It is abbreviated for **GCF**. It is also known as the **Greatest Common Divisor** (GCD) and the **Highest Common Factor** (HCF). It is used to simplify the fractions.

How to Find Greatest Common Factor

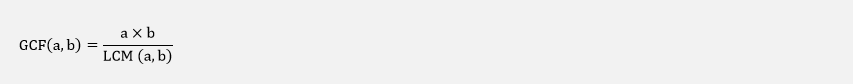
Follow the steps given below to find the greatest common factor.

Write all the factors of each number.

Select the common factors.

Select the greatest number, as GCF.

We can also use the following formula:



Note: Use the above formula only for two numbers.

Let's understand it through examples.

**Example 1: Find the GCF of 12 and 8.**

**Solution:**

Factors of 12: 1, 2, 3, 4, 6, 12

Factors of 8: 1, 2, 4, 8

Common Factors: 1, 2, 4

Greatest Common Factor: 4

**Hence, the GCF of 12 and 8 is 4.**

**Example 2: Find the GCF of 24 and 36.**

**Solution:**

Factors of 24: 1, 2, 3, 4, 6, 8, 12, 24

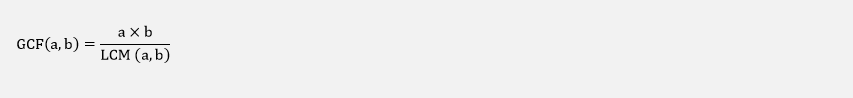
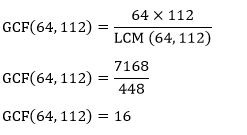
Factors of 36: 1, 2, 3, 4, 6, 9, 12, 18, 36

Common Factors: 1, 2, 3, 4, 6, 12

Greatest Common Factor: 12

**Hence, the GCF of 24 and 36 is 12.**

**Using GCF Formula**

**Hence, the GCF of 64 and 112 is 16.**

**Example 6: Find the GCF of 33 and 56.**

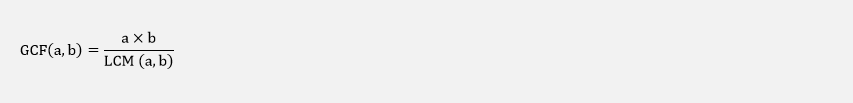
**Solution:**

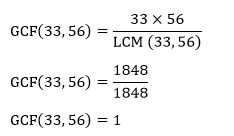
Factors of 33: 1, 3, 11, 33

Factors of 56: 1, 2, 4, 7, 8, 14, 28, 56

Common Factors: 1

Greatest Common Factor: 1

**Using GCF Formula**



**Hence, the GCF of 33 and 56 is 1.**

## What is the RSA algorithm (Rivest-Shamir-Adleman)?

The RSA algorithm (Rivest-Shamir-Adleman) is the basis of a cryptosystem -- a suite of cryptographic algorithms that are used for specific security services or purposes -- which enables public key encryption and is widely used to secure sensitive data, particularly when it is being sent over an insecure network such as the internet

### How does the RSA algorithm work?

Alice generates her RSA keys by selecting two primes: p=11 and q=13. The modulus is n=p×q=143. The totient is n ϕ(n)=(p−1)x(q−1)=120. She chooses 7 for her RSA public key e and calculates her RSA private key using the Extended Euclidean algorithm, which gives her 103.

Bob wants to send Alice an encrypted message, M, so he obtains her RSA public key (n, e) which, in this example, is (143, 7). His [plaintext](https://www.techtarget.com/searchsecurity/definition/plaintext) message is just the number 9 and is encrypted into [ciphertext](https://www.techtarget.com/whatis/definition/ciphertext), C, as follows:

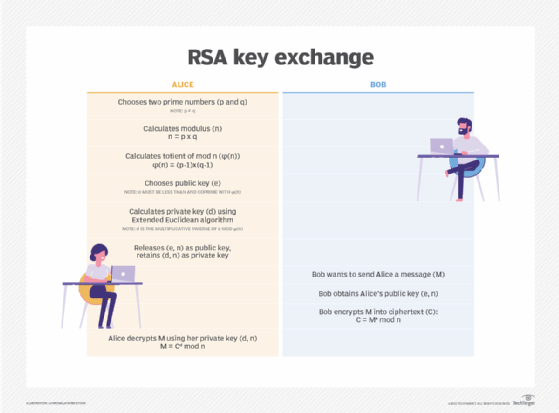
Me mod n = 97 mod 143 = 48 = C

When Alice receives Bob's message, she decrypts it by using her RSA private key (d, n) as follows:

Cd mod n = 48103 mod 143 = 9 = M

To use RSA keys to [digitally sign a message](https://www.techtarget.com/searchsecurity/answer/Which-private-keys-and-public-keys-can-create-a-digital-signature), Alice would need to create a [hash](https://searchsqlserver.techtarget.com/definition/hashing) -- a message digest of her message to Bob -- encrypt the hash value with her RSA private key, and add the key to the message. Bob can then verify that the message has been sent by Alice and has not been altered by decrypting the hash value with her public key. If this value matches the hash of the original message, then only Alice could have sent it -- authentication and non-repudiation -- and the message is exactly as she wrote it -- integrity.

Alice could, of course, encrypt her message with Bob's RSA public key -- confidentiality -- before sending it to Bob. A [digital certificate](https://www.techtarget.com/searchsecurity/definition/digital-certificate) contains information that identifies the certificate's owner and also contains the owner's public key. Certificates are signed by the [certificate authority](https://www.techtarget.com/searchsecurity/definition/certificate-authority) that issues them, and they can simplify the process of obtaining public keys and verifying the owner.



## Cryptography and its Types

[Cryptography](https://www.geeksforgeeks.org/cryptography-introduction-to-crypto-terminologies/) is technique of securing information and communications through use of codes so that only those person 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 use 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.

### ****Features Of Cryptography are as follows:****

1. **Confidentiality:** Information can only be accessed by the person for whom it is intended and no other person except him can access it.
2. **Integrity:** Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
3. **Non-repudiation:** The creator/sender of information cannot deny his intention to send information at later stage.
4. **Authentication:** The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

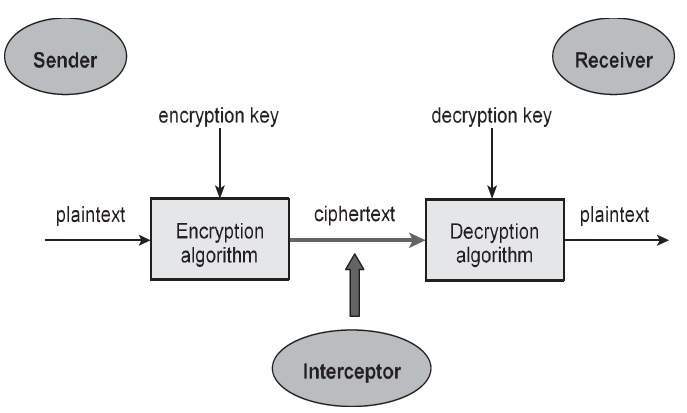
Types Of Cryptography: In general there are three types Of cryptography:

1. **Symmetric Key Cryptography:** It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system are Data Encryption System(DES) and Advanced Encryption System(AES).
2. **Hash Functions:** There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.
3. **Asymmetric Key Cryptography:** Under this system a pair of keys is used to encrypt and decrypt information. A receiver’s public key is used for encryption and a receiver’s private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone know his private key. The most popular asymmetric key cryptography algorithm is RSA algorithm.

## Cryptosystems

A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a **cipher system**.

Let us discuss a simple model of a cryptosystem that provides confidentiality to the information being transmitted. This basic model is depicted in the illustration below −



The illustration shows a sender who wants to transfer some sensitive data to a receiver in such a way that any party intercepting or eavesdropping on the communication channel cannot extract the data.

The objective of this simple cryptosystem is that at the end of the process, only the sender and the receiver will know the plaintext.

### Components of a Cryptosystem

The various components of a basic cryptosystem are as follows −

* **Plaintext.** It is the data to be protected during transmission.
* **Encryption Algorithm.** It is a mathematical process that produces a ciphertext for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a ciphertext.
* **Ciphertext.** It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key. The ciphertext is not guarded. It flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel.
* **Decryption Algorithm,** It is a mathematical process, that produces a unique plaintext for any given ciphertext and decryption key. It is a cryptographic algorithm that takes a ciphertext and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.
* **Encryption Key.** It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the ciphertext.
* **Decryption Key.** It is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the ciphertext in order to compute the plaintext.

For a given cryptosystem, a collection of all possible decryption keys is called a **key space**.

An **interceptor** (an attacker) is an unauthorized entity who attempts to determine the plaintext. He can see the ciphertext and may know the decryption algorithm. He, however, must never know the decryption key.

### Types of Cryptosystems :

Fundamentally, there are two types of cryptosystems based on the manner in which encryption-decryption is carried out in the system −

* Symmetric Key Encryption
* Asymmetric Key Encryption

The main difference between these cryptosystems is the relationship between the encryption and the decryption key. Logically, in any cryptosystem, both the keys are closely associated. It is practically impossible to decrypt the ciphertext with the key that is unrelated to the encryption key.

## Cryptography Digital signatures

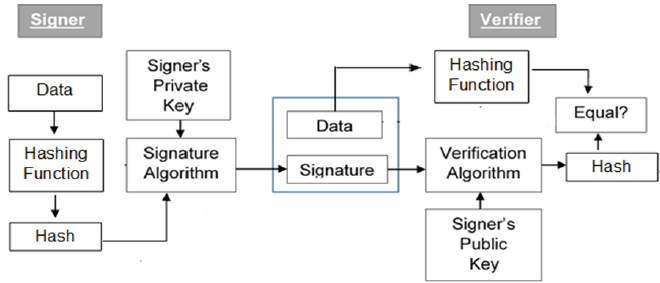
Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message.

Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party.

Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

### Model of Digital Signature

As mentioned earlier, the digital signature scheme is based on public key cryptography. The model of digital signature scheme is depicted in the following illustration −



The following points explain the entire process in detail −

* Each person adopting this scheme has a public-private key pair.
* Generally, the key pairs used for encryption/decryption and signing/verifying are different. The private key used for signing is referred to as the signature key and the public key as the verification key.
* Signer feeds data to the hash function and generates hash of data.
* Hash value and signature key are then fed to the signature algorithm which produces the digital signature on given hash. Signature is appended to the data and then both are sent to the verifier.
* Verifier feeds the digital signature and the verification key into the verification algorithm. The verification algorithm gives some value as output.
* Verifier also runs same hash function on received data to generate hash value.
* For verification, this hash value and output of verification algorithm are compared. Based on the comparison result, verifier decides whether the digital signature is valid.
* Since digital signature is created by ‘private’ key of signer and no one else can have this key; the signer cannot repudiate signing the data in future.

It should be noticed that instead of signing data directly by signing algorithm, usually a hash of data is created. Since the hash of data is a unique representation of data, it is sufficient to sign the hash in place of data. The most important reason of using hash instead of data directly for signing is efficiency of the scheme.

Let us assume RSA is used as the signing algorithm. As discussed in public key encryption chapter, the encryption/signing process using RSA involves modular exponentiation.

Signing large data through modular exponentiation is computationally expensive and time consuming. The hash of the data is a relatively small digest of the data, hence **signing a hash is more efficient than signing the entire data**.

### Importance of Digital Signature

Out of all cryptographic primitives, the digital signature using public key cryptography is considered as very important and useful tool to achieve information security.

Apart from ability to provide non-repudiation of message, the digital signature also provides message authentication and data integrity. Let us briefly see how this is achieved by the digital signature −

* **Message authentication** − When the verifier validates the digital signature using public key of a sender, he is assured that signature has been created only by sender who possess the corresponding secret private key and no one else.
* **Data Integrity** − In case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and the output provided by the verification algorithm will not match. Hence, receiver can safely deny the message assuming that data integrity has been breached.
* **Non-repudiation** − Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signature on a given data. Thus the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future.

By adding public-key encryption to digital signature scheme, we can create a cryptosystem that can provide the four essential elements of security namely − Privacy, Authentication, Integrity, and Non-repudiation.

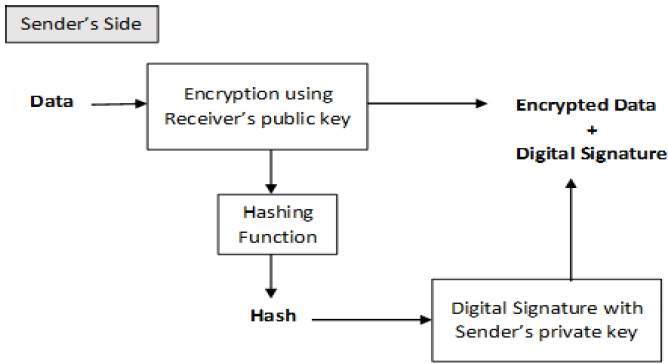
### Encryption with Digital Signature

In many digital communications, it is desirable to exchange an encrypted messages than plaintext to achieve confidentiality. In public key encryption scheme, a public (encryption) key of sender is available in open domain, and hence anyone can spoof his identity and send any encrypted message to the receiver.

This makes it essential for users employing PKC for encryption to seek digital signatures along with encrypted data to be assured of message authentication and non-repudiation.

This can archived by combining digital signatures with encryption scheme. Let us briefly discuss how to achieve this requirement. There are **two possibilities, sign-then-encrypt** and **encrypt-then-sign**.

However, the crypto system based on sign-then-encrypt can be exploited by receiver to spoof identity of sender and sent that data to third party. Hence, this method is not preferred. The process of encrypt-then-sign is more reliable and widely adopted. This is depicted in the following illustration −



The receiver after receiving the encrypted data and signature on it, first verifies the signature using sender’s public key. After ensuring the validity of the signature, he then retrieves the data through decryption using his private key.

## what are the types of attacks

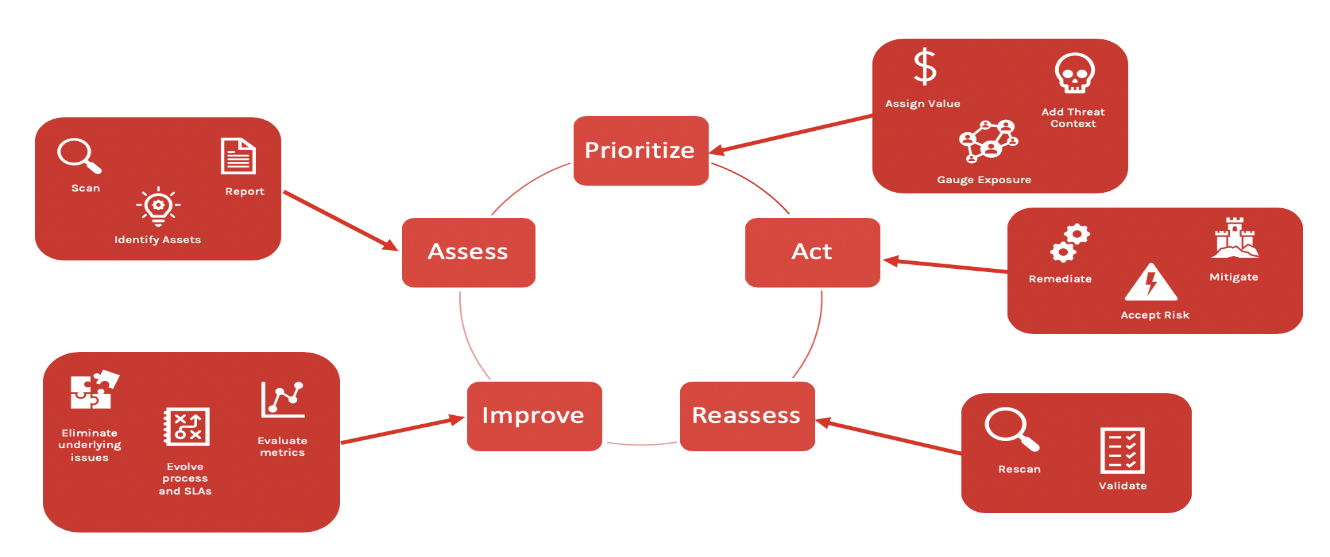
There are many types of cyberattacks that can target different aspects of a computer system, network, or application. Some of the most common types of cyberattacks are:

* **Malware**: Malware is any malicious software or code that is designed to harm or compromise a computer, network, or server. [Malware can include ransomware, trojans, spyware, viruses, worms, keyloggers, bots, and more](about:blank)[1](https://www.javatpoint.com/types-of-cyber-attacks)[2](https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/).
* **Phishing**: Phishing is a type of social engineering attack that attempts to trick users into revealing sensitive information or clicking on malicious links or attachments. [Phishing emails often impersonate legitimate entities or individuals and use deceptive techniques to lure users into falling for the scam](about:blank)[1](https://www.javatpoint.com/types-of-cyber-attacks)[2](https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/).
* **Man-in-the-middle (MITM)**: MITM is a type of attack that intercepts the communication between two parties and alters or steals the data being exchanged. [MITM attacks can be used to eavesdrop on confidential information, modify transactions, or redirect users to malicious websites](about:blank)[1](https://www.javatpoint.com/types-of-cyber-attacks)[2](https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/).
* **Denial-of-service (DoS) or distributed denial-of-service (DDoS)**: DoS and DDoS are types of attacks that aim to disrupt the availability or performance of a system, network, or service by overwhelming it
* with illegitimate requests or traffic. [DoS and DDoS attacks can cause slowdowns, crashes, or outages for the targeted system](about:blank)[1](https://www.javatpoint.com/types-of-cyber-attacks)[2](https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/).
* **SQL injection**: SQL injection is a type of attack that exploits a vulnerability in a web application that uses a SQL database. [SQL injection allows an attacker to execute malicious SQL commands on the database and access, modify, or delete data](about:blank)[1](https://www.javatpoint.com/types-of-cyber-attacks)[2](https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/).
* **Zero-day exploit**: A zero-day exploit is a type of attack that takes advantage of a previously unknown vulnerability in a software or hardware system. [A zero-day exploit gives an attacker an opportunity to compromise the system before the vendor or developer can release a patch or fix](about:blank)[1](https://www.javatpoint.com/types-of-cyber-attacks)[2](https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/).
* **Password attack**: A password attack is a type of attack that tries to guess or crack the passwords of users or systems. [Password attacks can use brute force methods, dictionary methods, or phishing methods to obtain passwords](about:blank).

## what is the vulnerability life cycle management system.

The vulnerability life cycle management system is a cybersecurity process that aims to identify, assess, prioritize, and act on the vulnerabilities that exist in an IT system, network, or application. Vulnerabilities are the weaknesses or flaws that can be exploited by cyberattackers to compromise the security or functionality of a system. [The vulnerability life cycle management system helps to prevent or mitigate the impact of cyberattacks by finding and fixing the vulnerabilities before they can be exploited](about:blank)[1](https://www.crowdstrike.com/cybersecurity-101/vulnerability-management/vulnerability-management-lifecycle/)[2](https://heimdalsecurity.com/blog/vulnerability-management-lifecycle/).

### The vulnerability life cycle management system consists of five main stages:



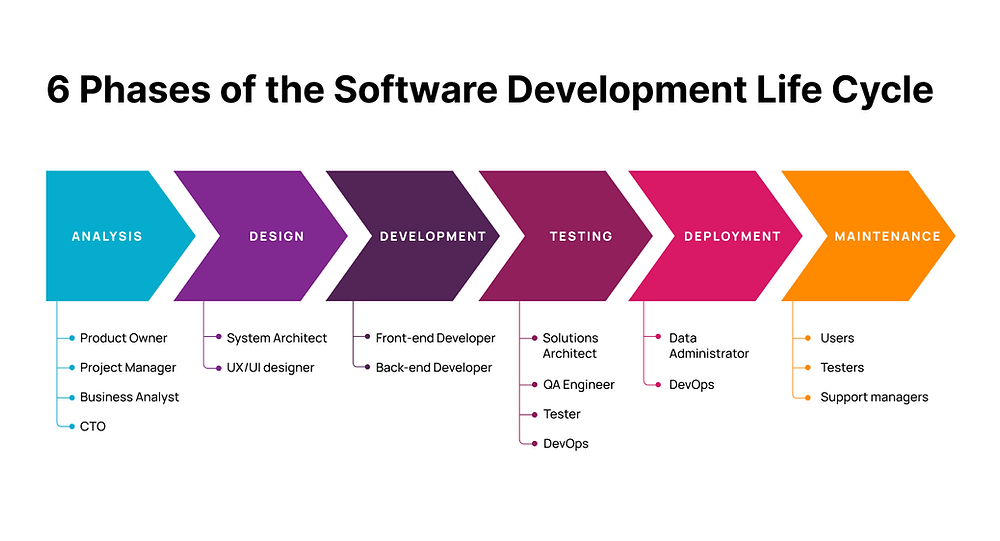
* **Assessment**: This stage involves scanning and testing the system for vulnerabilities using various tools and methods. [The assessment stage produces a report that lists the vulnerabilities and their severity levels](about:blank)[1](https://www.crowdstrike.com/cybersecurity-101/vulnerability-management/vulnerability-management-lifecycle/)[2](https://heimdalsecurity.com/blog/vulnerability-management-lifecycle/).
* **Prioritization**: This stage involves ranking the vulnerabilities based on their risk and impact. [The prioritization stage helps to allocate the resources and time for the remediation process](about:blank)[1](https://www.crowdstrike.com/cybersecurity-101/vulnerability-management/vulnerability-management-lifecycle/)[2](https://heimdalsecurity.com/blog/vulnerability-management-lifecycle/).
* **Act**: This stage involves applying the appropriate solutions to fix or mitigate the vulnerabilities. [The act stage can involve patching, updating, configuring, or replacing the vulnerable components](about:blank)[1](https://www.crowdstrike.com/cybersecurity-101/vulnerability-management/vulnerability-management-lifecycle/)[2](https://heimdalsecurity.com/blog/vulnerability-management-lifecycle/).
* **Reassessment**: This stage involves verifying that the solutions have been implemented correctly and effectively. [The reassessment stage can involve rescanning, retesting, or auditing the system for any remaining or new vulnerabilities](about:blank)[1](https://www.crowdstrike.com/cybersecurity-101/vulnerability-management/vulnerability-management-lifecycle/)[2](https://heimdalsecurity.com/blog/vulnerability-management-lifecycle/).
* **Improvement**: This stage involves analyzing the results and feedback from the previous stages and improving the vulnerability management process. [The improvement stage can involve updating the policies, procedures, tools, or best practices for vulnerability management](about:blank)[1](https://www.crowdstrike.com/cybersecurity-101/vulnerability-management/vulnerability-management-lifecycle/)[2](https://heimdalsecurity.com/blog/vulnerability-management-lifecycle/).

## SDLC

SDLC stands for Software Development Life Cycle, which is a process that defines the stages and tasks involved in creating, testing, and deploying software applications. [SDLC aims to ensure that the software meets the quality, cost, and time requirements of the clients and stakeholders1](https://www.javatpoint.com/software-engineering-software-development-life-cycle)[2](https://stackify.com/what-is-sdlc/).

There are different models or methodologies of SDLC, such as waterfall, agile, spiral, and iterative. [Each model has its own advantages and disadvantages, depending on the nature and scope of the software project3](https://www.tutorialspoint.com/sdlc/sdlc_overview.htm)[4](https://en.wikipedia.org/wiki/Systems_development_life_cycle).

The common stages of SDLC are:



* **Requirement analysis**: This stage involves gathering and analyzing the needs and expectations of the
* clients and users. [It also involves defining the scope, objectives, and feasibility of the software project1](https://www.javatpoint.com/software-engineering-software-development-life-cycle)[2](https://stackify.com/what-is-sdlc/).
* **Planning**: This stage involves estimating the cost, time, and resources required for the software project. [It also involves identifying the risks and challenges and developing strategies to mitigate them](about:blank)[1](https://www.javatpoint.com/software-engineering-software-development-life-cycle)[2](https://stackify.com/what-is-sdlc/).
* **Design**: This stage involves creating the architecture and design of the software system. [It also involves selecting the appropriate tools, technologies, and frameworks for the software development](about:blank)[1](https://www.javatpoint.com/software-engineering-software-development-life-cycle)[2](https://stackify.com/what-is-sdlc/).
* **Development**: This stage involves writing and coding the software according to the design specifications. [It also involves following the coding standards and best practices for software development](about:blank)[1](https://www.javatpoint.com/software-engineering-software-development-life-cycle)[2](https://stackify.com/what-is-sdlc/).
* **Testing**: This stage involves verifying and validating the functionality, performance, and quality of the software. [It also involves finding and fixing any errors or bugs in the software](about:blank)[1](https://www.javatpoint.com/software-engineering-software-development-life-cycle)[2](https://stackify.com/what-is-sdlc/).
* **Deployment**: This stage involves releasing and delivering the software to the clients or users. [It also involves installing and configuring the software on the target platforms or environments1](https://www.javatpoint.com/software-engineering-software-development-life-cycle)[2](https://stackify.com/what-is-sdlc/).
* **Maintenance**: This stage involves providing ongoing support and updates for the software. [It also involves resolving any issues or problems that may arise in the software1](https://www.javatpoint.com/software-engineering-software-development-life-cycle)[2](https://stackify.com/what-is-sdlc/).

# What is the hub?

A hub is a common connection point, also known as a network hub, which is used for connection of devices in a network. It works as a central connection for all the devices that are connected through a hub. The hub has numerous ports. If a packet reaches at one port, it is able to see by all the segments of the network due to a packet is copied to the other ports. A network hub has no routing tables or intelligence (unlike a network switch or router), which is used to send information and broadcast all network data across each and every connection.

Although most of the hubs can recognize network troubles or errors like collisions, broadcasting all information to the several ports can be a security risk and cause bottlenecks. The network hubs were popular in the past time as they were cheaper as compared to a switch or router. Nowadays, switches are much cheaper than a hub and provide a better solution for any network. Furthermore, a hub is no [IP](https://www.javatpoint.com/ip) address, as it is a dumb device.

### Types of Hub

There are three types of the hub that are given below:

1. Passive Hub
2. Active Hub
3. Intelligent Hub

**Passive Hub:** The passive hubs are the connection point for wires that helps to make the physical network. It is capable of determining the bugs and faulty hardware. Simply, it accepts the packet over a port and circulates it to all ports. It includes connectors (10base-2 port and RJ-45) that can be applied as a standard in your network. This connector is connected to all [local area network (LAN)](https://www.javatpoint.com/wireless-lan-introduction) devices. Additionally, the advanced passive hubs have AUI ports, which are connected as the transceiver according to the network design.

**Active Hub:** As compared to a passive hub, it includes some additional features. It is able to monitor the data sent to the connected devices. It plays an important role between the connected devices with the help of store technology, where it checks the data to be sent and decides which packet to send first.

It has the ability to fix the damaged packets when packets are sending, and also able to hold the direction of the rest of the packets and distribute them. If a port receives a weak signal, but still it is readable, then the active hub reconstructs the weak signal into a stronger signal before its sending to other ports. It can boost the signal if any connecting device is not working in the network. Therefore, it helps to make the continuity of services in LAN.

**Intelligent Hub:** It is a little smarter than passive and active hubs. These hubs have some kinds of management software that help to analyze the problem in the network and resolve them. It is beneficial to expend the business in networking; the management can assign users that help to work more quickly and share a common pool efficiently by using intelligent hubs. However, it offers better performance for the local area network. Furthermore, with any physical device, if any problem is detected, it is able to detect this problem easily.

### Features of Hub

* It acts with shared bandwidth and broadcasting.
* It includes only one collision domain and broadcast domain.
* It works at the physical layer of the OSI model and also offers support for half-duplex transmission mode.
* It cannot create a virtual LAN and does not support spanning tree protocol.
* Furthermore, mainly packet collisions occur inside the hub.
* It also has a feature of flexibility, which means it includes a high transmission rate to different devices.

### Applications of Hub

The important applications of a hub are given below:

* Hub is used to create small home networks.
* It is used for network monitoring.
* They are also used in organizations to provide connectivity.
* It can be used to create a device that is available thought out of the network.

### What hubs do?

Hubs work as a central connection between all network equipment and handle a data type, which is called frames. If a frame is received, it is transmitted to the port of the destination computer after amplifying it. A frame is passed to each of its ports in the hub, whether it is destined only for one port. It does not include the way of deciding a frame to which port it should be sent. Therefore, a frame has to transmit to every port, which ensures that it will reach its intended destination that generates a lot of traffic on the network and can be caused to damage the network. The hub is slower as compared to standard switch as it is not able to send or receive information at the same time, but a switch is more costly than a hub.

### Advantages of Hub

* It provides support for different types of Network Media.
* It can be used by anyone as it is very cheap.
* It can easily connect many different media types.
* The use of a hub does not impact on the network performance.
* Additionally, it can expand the total distance of the network.

### Disadvantages of Hub

* It has no ability to choose the best path of the network.
* It does not include mechanisms such as collision detection.
* It does not operate in full-duplex mode and cannot be divided into the Segment.
* It cannot reduce the network traffic as it has no mechanism.
* It is not able to filter the information as it transmits packets to all the connected segments.
* Furthermore, it is not capable of connecting various network architectures like a ring, token, and ethernet, and more.

### Difference between hub and switch

A table below contains the major difference between hub and switch:

|  |  |
| --- | --- |
| **Hub** | **Switch** |
| A hub works at the physical layer of the OSI model. | A switch works at the data link layer of the OSI model. |
| A hub contains a single domain of collision. | In switch, several ports include separate collision domains. |
| It performs frame flooding, which can be broadcast, unicast, or multicast. | It mainly performs broadcast, and also performs unicast and multicast when required. |
| In the hub, the transmission mode is Half-duplex | In switch, the transmission mode is full-duplex. |
| It uses electrical signal orbits. | It uses frame & packet. |
| It does not support the Spanning-Tree protocol. | It supports Multiple Spanning-Tree. |
| In the hub, mostly collisions occur in setup. | In full-duplex switch does not occur collisions. |
| It is a passive device. | It is an active device. |
| A hub is not capable of storing MAC addresses. | It uses accessible content memory, which can be accessed by application-specific integrated chips (ASIC). |
| It is not an intelligent device. | A switch is an intelligent device. |
| The speed of the hub network is up to 10 Mb per second. | The speed of switch is 10/100 Mbps, 1 Gbps, and 10 Gbps. |

# What is a Router?

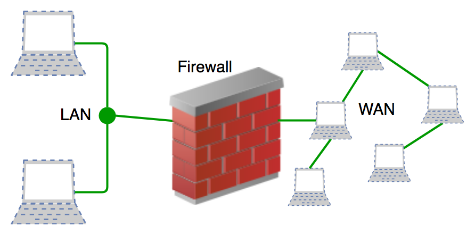
The router is a physical or virtual internetworking device that is designed to receive, analyze, and forward data packets between computer networks. A router examines a destination IP address of a given data packet, and it uses the headers and forwarding tables to decide the best way to transfer the packets. There are some popular companies that develop routers; such are **Cisco**, **3Com**, **HP**, **Juniper**, **D-Link**, **Nortel**, etc. Some important points of routers are given below:

* A router is used in **LAN** (Local Area Network) and **WAN** (Wide Area Network) environments. For example, it is used in **offices** for connectivity, and you can also establish the connection between distant networks such as from **Bhopal** to
* It shares information with other routers in networking.
* It uses the routing protocol to transfer the data across a network.
* Furthermore, it is more **expensive** than other networking devices like switches and hubs.

A router works on the **third layer**of the OSI model, and it is based on the IP address of a computer. It uses protocols such as ICMP to communicate between two or more networks. It is also known as an ***intelligent device*** as it can calculate the best route to pass the network packets from source to the destination automatically.

# Network security concepts of firewall?

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic. **Accept :** allow the traffic **Reject :** block the traffic but reply with an “unreachable error” **Drop :**block the traffic with no reply A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet..



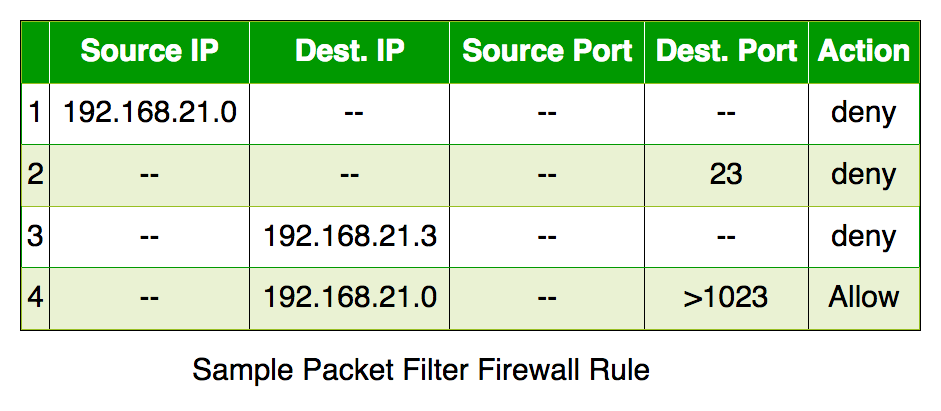
**History and Need for Firewall**

Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers. ACLs are rules that determine whether network access should be granted or denied to specific IP address. But ACLs cannot determine the nature of the packet it is blocking. Also, ACL alone does not have the capacity to keep threats out of the network. Hence, the Firewall was introduced. Connectivity to the Internet is no longer optional for organizations. However, accessing the Internet provides benefits to the organization; it also enables the outside world to interact with the internal network of the organization. This creates a threat to the organization. In order to secure the internal network from unauthorized traffic, we need a Firewall.

## Generation of Firewall?

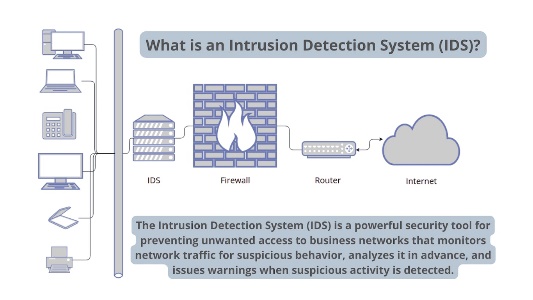
Firewalls can be categorized based on their generation.

1. **First Generation- Packet Filtering Firewall:**Packet filtering firewall is used to control network access by monitoring outgoing and incoming packets and allowing them to pass or stop based on source and destination IP address, protocols, and ports. It analyses traffic at the transport protocol layer (but mainly uses first 3 layers). Packet firewalls treat each packet in isolation. They have no ability to tell whether a packet is part of an existing stream of traffic. Only It can allow or deny the packets based on unique packet headers. Packet filtering firewall maintains a filtering table that decides whether the packet will be forwarded or discarded. From the given filtering table, the packets will be filtered according to the following rules:



1. Incoming packets from network 192.168.21.0 are blocked.
2. Incoming packets destined for the internal TELNET server (port 23) are blocked.
3. Incoming packets destined for host 192.168.21.3 are blocked.
4. All well-known services to the network 192.168.21.0 are allowed.
5. **Second Generation- Stateful Inspection Firewall:**Stateful firewalls (performs Stateful Packet Inspection) are able to determine the connection state of packet, unlike Packet filtering firewall, which makes it more efficient. It keeps track of the state of networks connection travelling across it, such as TCP streams. So the filtering decisions would not only be based on defined rules, but also on packet’s history in the state table.
6. **Third Generation- Application Layer Firewall :**Application layer firewall can inspect and filter the packets on any OSI layer, up to the application layer. It has the ability to block specific content, also recognize when certain application and protocols (like HTTP, FTP) are being misused. In other words, Application layer firewalls are hosts that run proxy servers. A proxy firewall prevents the direct connection between either side of the firewall, each packet has to pass through the proxy. It can allow or block the traffic based on predefined rules. *Note: Application layer firewalls can also be used as Network Address Translator(NAT).*
7. **Next Generation Firewalls (NGFW):**Next Generation Firewalls are being deployed these days to stop modern security breaches like advance malware attacks and application-layer attacks. NGFW consists of Deep Packet Inspection, Application Inspection, SSL/SSH inspection and many functionalities to protect the network from these modern threats.

## Network security concepts of IDS



An Intrusion Detection System (IDS) is a network security technology originally built for detecting vulnerability exploits against a target application or computer.

The IDS is also a listen-only device. The IDS monitors traffic and reports results to an administrator. It cannot automatically take action to prevent a detected exploit from taking over the system.

**Types of IDS Detection**

There are five types of IDS: network-based, host-based, protocol-based, application protocol-based and hybrid.

The two most common types of IDS are:

1. **Network-based intrusion detection system (NIDS)**  
   A network IDS monitors a complete protected network. It is deployed across the infrastructure at strategic points, such as the most vulnerable subnets. The NIDS monitors all traffic flowing to and from devices on the network, making determinations based on packet contents and metadata.
2. **Host-based intrusion detection system (HIDS)**  
   A host-based IDS monitors the computer infrastructure on which it is installed. In other words, it is deployed on a specific endpoint to protect it against internal and external threats. The IDS accomplishes this by analyzing traffic, logging malicious activity and notifying designated authorities.

The remaining three types can be described as such:

1. **Protocol-based (PIDS)**  
   A protocol-based intrusion detection system is usually installed on a web server. It monitors and analyzes the protocol between a user/device and the server. A PIDS normally sits at the front end of a server and monitors the behavior and state of the protocol.
2. **Application protocol-based (APIDS)**  
   An APIDS is a system or agent that usually sits inside the server party. It tracks and interprets correspondence on application-specific protocols. For example, this would monitor the SQL protocol to the middleware while transacting with the web server.
3. **Hybrid intrusion detection system**  
   A hybrid intrusion detection system combines two or more intrusion detection approaches. Using this system, system or host agent data combined with network information for a comprehensive view of the system. The hybrid intrusion detection system is more powerful compared to other systems. One example of Hybrid IDS is Prelude.

There is also a subgroup of IDS detection methods, the two most common variants being:

1. **Signature-based**  
   A signature-based IDS monitors inbound network traffic, looking for specific patterns and sequences that match known attack signatures. While it is effective for this purpose, it is incapable of detecting unidentified attacks with no known patterns.
2. **Anomaly-based**  
   The anomaly-based IDS is a relatively newer technology designed to detect unknown attacks, going beyond the identification of attack signatures. This type of detection instead uses machine learning to analyze large amounts of network data and traffic.  
     
   Anomaly-based IDS creates a defined model of normal activity and uses it to identify anomalous behavior. However, it is prone to false positives. For example, if a machine demonstrates rare, but healthy behavior, it is identified as an anomaly. This results in a false alarm.

## Network traffic analysis in cybersecurity

Network traffic analysis is a method of monitoring and analyzing the communication patterns of network traffic to detect and respond to security threats. It can help you gain visibility into your network activity, optimize performance, troubleshoot issues, and comply with legal obligations.

## Network security concepts of IPS

Intrusion Prevention System is also known as Intrusion Detection and Prevention System. It is a network security application that monitors network or system activities for malicious activity. Major functions of intrusion prevention systems are to identify malicious activity, collect information about this activity, report it and attempt to block or stop it.

Intrusion prevention systems are contemplated as augmentation of [Intrusion Detection Systems (IDS)](https://www.geeksforgeeks.org/intrusion-detection-system-ids/) because both IPS and IDS operate network traffic and system activities for malicious activity.

* **Types of IPS:**

There are two main types of IPS:

1. **Network-Based IPS:** A Network-Based IPS is installed at the network perimeter and monitors all traffic that enters and exits the network.
2. **Host-Based IPS:** A Host-Based IPS is installed on individual hosts and monitors the traffic that goes in and out of that host.

* **Classification of Intrusion Prevention System (IPS):**   
  Intrusion Prevention System (IPS) is classified into 4 types:

1. Network-based intrusion prevention system (NIPS):   
   It monitors the entire network for suspicious traffic by analyzing protocol activity.
2. Wireless intrusion prevention system (WIPS):   
   It monitors a wireless network for suspicious traffic by analyzing wireless networking protocols.
3. Network behavior analysis (NBA):   
   It examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service attacks, specific forms of malware and policy violations.
4. Host-based intrusion prevention system (HIPS):   
   It is an inbuilt software package which operates a single host for doubtful activity by scanning events that occur within that host.

## Network security concepts of VPN?

A Virtual Private Network (VPN) is a connection between a VPN server and a VPN client. It is a secure tunnel-like connection across the internet.

As seen in the figure above, the VPN client connects to the internet by interacting with the VPN server through an encrypted tunnel. Since the communication between the client and the server happens through this tunnel, attackers cannot hack the information.