What is cryptography?
Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.
cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email.

Cryptographic algorithms
Cryptosystems use a set of procedures known as cryptographic algorithms, or ciphers, to encrypt and decrypt messages to secure communications among computer systems, devices and applications.
A cipher suite uses one algorithm for encryption, another algorithm for message authentication and another for key exchange. This process, embedded in protocols and written in software that runs on operating systems (OSes) and networked computer systems, involves:
public and private key generation for data encryption/decryption
digital signing and verification for message authentication
key exchange

Types Of Cryptography:
Symmetric/Private/Secret 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 is Data Encryption System(DES).
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.
Asymmetric Key/Public Cryptography:
Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a 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 knows the private key.

Difference Between Symmetric and Asymmetric Key Encryption
Symmetric-It only requires a single key for both encryption and decryption.,The size of cipher text is same or smaller than the original plain text.,The encryption process

is very fast.,It is used when a large amount of data is required to transfer.,It only provides confidentiality,Examples: 3DES, AES, DES and RC4

Asymmetric:-It requires two key one to encrypt and the other one to decrypt.,The size of cipher text is same or larger than the original plain text.,The encryption process is slow.,It is used to transfer small amount of data.,It provides confidentiality, authenticity and non-repudiation.,Examples: Diffie-Hellman, ECC, El Gamal, DSA and RSA.

Hash functions

Hash functions are extremely useful and appear in almost all information security applications.

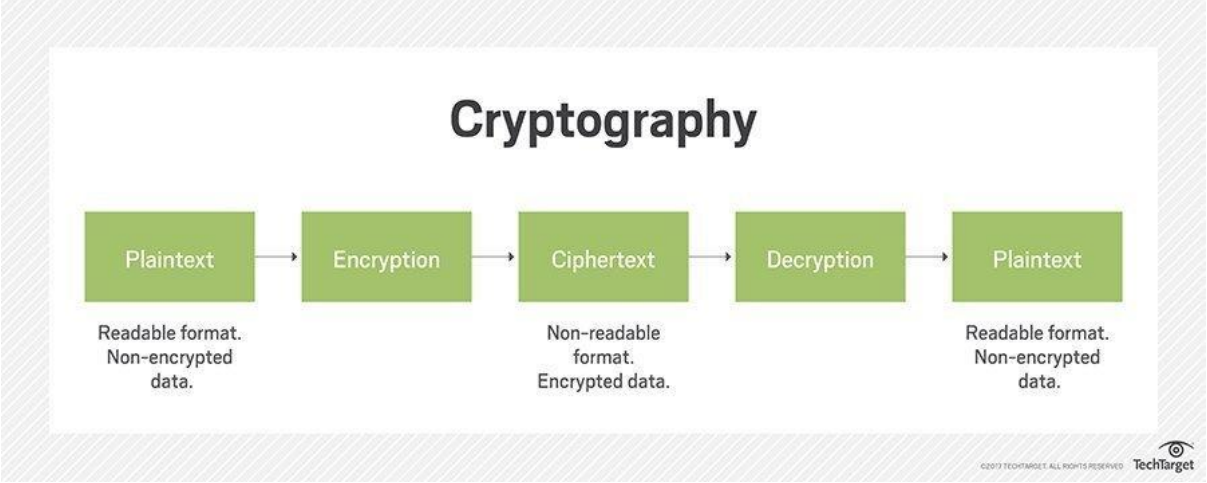
A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.

Values returned by a hash function are called message digest or simply hash values.

Conventional encryption

Conventional encryption is a cryptographic system that uses the same key used by the sender to encrypt the message and by the receiver to decrypt the message. It was the only type of encryption in use prior to the development of public-key encryption.

It is still much preferred of the two types of encryption systems due to its simplicity. It is a relatively fast process since it uses a single key for both encryption and decryption In this encryption model, the sender encrypts plaintext using the receiver's secret key, which can be later used by the receiver to decrypt the ciphertext. Below is a figure that illustrates this concept.



Suppose A wants to send a message to B, that message is called plaintext. Now, to avoid hackers reading plaintext, the plaintext is encrypted using an algorithm and a secret key (at 1). This encrypted plaintext is called ciphertext. Using the same secret key and encryption algorithm run in reverse(at 2), B can get plaintext of A, and thus the message is read and security is maintained.

The idea that uses in this technique is very old and that's why this model is called conventional encryption.

Conventional encryption has mainly 5 ingredients :

Plain text –

It is the original data that is given to the algorithm as an input.

Encryption algorithm –

This encryption algorithm performs various transformations on plain text to convert it into ciphertext.

Secret key –

The secret key is also an input to the algorithm. The encryption algorithm will produce different outputs based on the keys used at that time.

Ciphertext –

It contains encrypted information because it contains a form of original plaintext that is unreadable by a human or computer without proper cipher to decrypt it. It is output from the algorithm.

Decryption algorithm –

This is used to run encryption algorithms in reverse. Ciphertext and Secret key is input here and it produces plain text as output.

Requirements for secure use of conventional encryption :

We need a strong encryption algorithm.

The sender and Receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.

Advantages of Conventional Encryption :

Simple –

This type of encryption is easy to carry out.

Uses fewer computer resources –

Conventional encryption does not require a lot of computer resources when compared to public-key encryption.

Fast –

Conventional encryption is much faster than asymmetric key encryption.

Disadvantages of Conventional Encryption Model:

Origin and authenticity of the message cannot be guaranteed, since both sender and receiver use the same key, messages cannot be verified to have come from a particular user.

It isn't much secured when compared to public-key encryption.

If the receiver lost the key, he/she cant decrypt the message and thus making the whole process useless.

This scheme does not scale well to a large number of users because both the sender and the receiver have to agree on a secret key before transmission.

Cryptography and Network Security Principles

In the present day scenario security of the system is the sole priority of any organisation. The main aim of any organisation is to protect their data from attackers. In cryptography, attacks are of two types such as Passive attacks and Active attacks. Passive attacks are those that retrieve information from the system without affecting the system resources while active attacks are those that retrieve system information and make changes to the system resources and their operations.

The Principles of Security can be classified as follows:

Confidentiality:

The degree of confidentiality determines the secrecy of the information. The principle specifies that only the sender and receiver will be able to access the information shared between them. Confidentiality compromises if an unauthorized person is able to access a message.

For example, let us consider sender A wants to share some confidential information with receiver B and the information gets intercepted by the attacker C. Now the confidential information is in the hands of an intruder C.

Authentication:

Authentication is the mechanism to identify the user or system or the entity. It ensures the identity of the person trying to access the information. The authentication is mostly secured by using username and password. The authorized person whose identity is preregistered can prove his/her identity and can access the sensitive information.

Integrity:

Integrity gives the assurance that the information received is exact and accurate. If the content of the message is changed after the sender sends it but before reaching the intended receiver, then it is said that the integrity of the message is lost.

Non-Repudiation:

Non-repudiation is a mechanism that prevents the denial of the message content sent through a network. In some cases the sender sends the message and later denies it. But the non-repudiation does not allow the sender to refuse the receiver.

Access control:

The principle of access control is determined by role management and rule management. Role management determines who should access the data while rule management determines up to what extent one can access the data. The information displayed is dependent on the person who is accessing it.

Availability:

The principle of availability states that the resources will be available to authorize party at all times. Information will not be useful if it is not available to be accessed. Systems should have sufficient availability of information to satisfy the user request.

Security services and mechanisms

Failed to connect to MySQL: Access denied for user 'u688631385_eezytut'@'localhost' (using password: YES)

ITU-T provides some security services and some mechanisms to implement those services.
Security services and mechanisms are closely related because a mechanism or combination of mechanisms are used to provide a service..

Types of Security Mechanism
Network Security is a field in computer technology that deals with ensuring security of computer network infrastructure. As the network is very necessary for sharing of information whether it is at hardware level such as printer, scanner, or at software level. Therefore security mechanism can also be termed as is set of processes that deal with recovery from security attack. Various mechanisms are designed to recover from these specific attacks at various protocol layers.
Types of Security Mechanism are :

1. Encipherment :
   This security mechanism deals with hiding and covering of data which helps data to become confidential. It is achieved by applying mathematical calculations or algorithms which reconstruct information into not readable form. It is achieved by two famous techniques named Cryptography and Encipherment. Level of data encryption is dependent on the algorithm used for encipherment.
2. Access Control :
   This mechanism is used to stop unattended access to data which you are sending. It can be achieved by various techniques such as applying passwords, using firewall, or just by adding PIN to data.
3. Notarization :
   This security mechanism involves use of trusted third party in communication. It acts as mediator between sender and receiver so that if any chance of conflict is reduced. This mediator keeps record of requests made by sender to receiver for later denied.
4. Data Integrity :
   This security mechanism is used by appending value to data to which is created by data itself. It is similar to sending packet of information known to both sending and receiving parties and checked before and after data is received. When this packet or data which is appended is checked and is the same while sending and receiving data integrity is maintained.
5. Authentication exchange :
   This security mechanism deals with identity to be known in communication. This is achieved at the TCP/IP layer where two-way handshaking mechanism is used to ensure data is sent or not
6. Bit stuffing :
   This security mechanism is used to add some extra bits into data which is being transmitted. It helps data to be checked at the receiving end and is achieved by Even parity or Odd Parity.

7. Digital Signature :
   This security mechanism is achieved by adding digital data that is not visible to eyes. It is form of electronic signature which is added by sender which is checked by receiver electronically. This mechanism is used to preserve data which is not more confidential but sender's identity is to be notified.

Active Attacks:

Active attacks are the type of attacks in which, The attacker efforts to change or modify the content of messages. Active Attack is danger for Integrity as well as availability. Due to active attack system is always damaged and System resources can be changed. The most important thing is that, In active attack, Victim gets informed about the attack

1.Masquerade –

A masquerade attack takes place when one entity pretends to be a different entity. A Masquerade attack involves one of the other forms of active attacks. If an authorization procedure isn't always absolutely protected, it is able to grow to be extraordinarily liable to a masquerade assault. Masquerade assaults may be performed using the stolen passwords and logins, with the aid of using finding gaps in programs, or with the aid of using locating a manner across the authentication process.

2.Modification of messages –

It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorized effect. Modification is an attack on the integrity of the original data. It basically means that unauthorized parties not only gain access to data but also spoof the data by triggering denial-of-service attacks, such as altering transmitted data packets or flooding the network with fake data. Manufacturing is an attack on authentication. For example, a message meaning "Allow JOHN to read confidential file X" is modified as "Allow Smith to read confidential file X".

3.Repudiation –

This attack occurs when the network is not completely secured or the login control has been tampered with. With this attack, the author's information can be changed by actions of a malicious user in order to save false data in log files, up to the general manipulation of data on behalf of others, similar to the spoofing of e-mail messages.

4.Replay –

It involves the passive capture of a message and its subsequent transmission to produce an authorized effect. In this attack, the basic aim of the attacker is to save a copy of the data originally present on that particular network and later on use this data for personal uses. Once the data is corrupted or leaked it is insecure and unsafe for the users.

5.Denial of Service –
It prevents the normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network either by disabling the network or by overloading it with messages so as to degrade performance.

Passive Attacks:
Passive Attacks are the type of attacks in which, The attacker observes the content of messages or copy the content of messages. Passive Attack is danger for Confidentiality. Due to passive attack, there is no any harm to the system. The most important thing is that In passive attack, Victim does not get informed about the attack.
1.The release of message content
2.Traffic analysis

The release of message content –
Telephonic conversation, an electronic mail message, or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

Traffic analysis –
Suppose that we had a way of masking (encryption) information, so that the attacker even if captured the message could not extract any information from the message. The opponent could determine the location and identity of communicating host 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.
The most useful protection against traffic analysis is encryption of SIP traffic. To do this, an attacker would have to access the SIP proxy (or its call log) to determine who made the call.

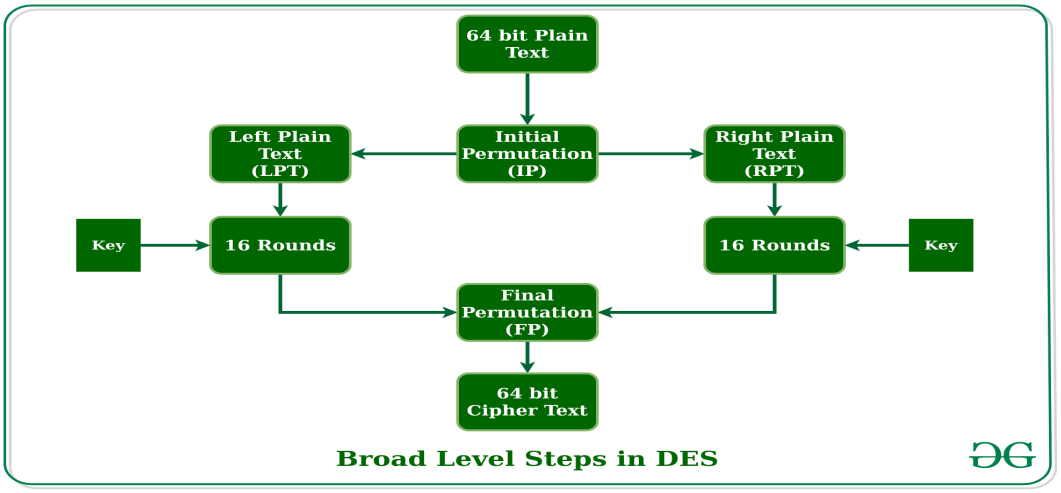
Difference between Active attack and Passive attack

On the basis of	Active attack	Passive attack
Definition	In active attacks, the attacker intercepts the connection and efforts to modify the message's content.	In passive attacks, the attacker observes the messages, then copy and save them and can use it for malicious purposes.

Modification	In an active attack, the attacker modifies the actual information.	In passive attacks, information remains unchanged.
Victim	In active attacks, the victim gets notified about the attack.	Unlike active attacks, in passive attacks, victims do not get informed about the attack.
System's impact	The damage done with active attacks can be harmful to the system and its resources.	The passive attacks do not harm the system.
System resources	In active attacks, the system resources can be changed.	In passive attacks, the system resources remain unchanged.
Dangerous for	They are dangerous for the integrity and availability of the message.	They can be dangerous for confidentiality of the message.
Emphasis on	In active attacks, attention is on detection.	In active attacks, attention is on prevention.
Types	Active attacks involve Masquerade, Modification of message, Repudiation, Replay, and Denial of service.	It involves traffic analysis, the release of a message.
Prevention	Active attacks are tough to restrict from entering systems or networks.	Unlike active attacks, passive attacks are easy to prohibit.

Data encryption standard (DES)

Data encryption standard (DES) has been found vulnerable to very powerful attacks and therefore, the popularity of DES has been found slightly on the decline. DES is a block cipher and encrypts data in blocks of size of 64 bits each, which means 64 bits of plain text go as the input to DES, which produces 64 bits of ciphertext. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits. The basic idea is shown in the figure.



DES is based on the two fundamental attributes of cryptography: substitution (also called confusion) and transposition (also called diffusion). DES consists of 16 steps, each of which is called a round. Each round performs the steps of substitution and transposition. Let us now discuss the broad-level steps in DES.

1. In the first step, the 64-bit plain text block is handed over to an initial Permutation (IP) function.
2. The initial permutation is performed on plain text.
3. Next, the initial permutation (IP) produces two halves of the permuted block; saying Left Plain Text (LPT) and Right Plain Text (RPT).
4. Now each LPT and RPT go through 16 rounds of the encryption process.
5. In the end, LPT and RPT are rejoined and a Final Permutation (FP) is performed on the combined block
6. The result of this process produces 64-bit ciphertext.

Initial Permutation (IP): As we have noted, the initial permutation (IP) happens only once and it happens before the first round. It suggests how the transposition in IP should proceed, as shown in the figure. For example, it says that the IP replaces the first bit of the original plain text block with the 58th bit of the original plain text, the second bit with the 50th bit of the original plain text block, and so on.

Step-1: Key transformation: We have noted initial 64-bit key is transformed into a 56-bit key by discarding every 8th bit of the initial key. Thus, for each a 56-bit key is available. From this 56-bit key, a different 48-bit Sub Key is generated during each round using a process called key transformation. For this, the 56-bit key is divided into two halves, each of 28 bits. These halves are circularly shifted left by one or two positions, depending on the round.

Step-2: Expansion Permutation: Recall that after the initial permutation, we had two 32-bit plain text areas called Left Plain Text(LPT) and Right Plain Text(RPT). During the expansion permutation, the RPT is expanded from 32 bits to 48 bits. Bits are permuted as well hence called expansion permutation. This happens as the 32-bit RPT is divided into 8 blocks, with each block consisting of 4 bits. Then, each

4-bit block of the previous step is then expanded to a corresponding 6-bit block, i.e., per 4-bit block, 2 more bits are added.

Difference between AES and DES ciphers

AES	DES
AES stands for Advanced Encryption Standard	DES stands for Data Encryption Standard.
AES allows the data length (plain text size) of 128, 192, and 256 bits.	Data encryption standard takes 64-bit plaintext as input and creates 64-bit Ciphertext i.e. it encrypts data in a block of size 64-bits per block.
AES divide plaintext into 16 bytes (128-bit) blocks and treats each block as a 4×4 State array and supporting three different key lengths, 128, 192. and 256 bits.	In DES plaintext message is divided into size 64-bit block each and encrypted using the 56-bit key at the initial level.
The number of rounds is 10, which is for the case when the encryption key is 128 bit long. (As mentioned earlier, the number of rounds is 12 when the key is 192 bits and 14 when the key is 256.)	The left plaintext and right plaintext goes through 16 rounds of encryption process along with 16 different keys for each round.
AES was designed by Vincent Rijmen and Joan Daemen.	DES was designed by IBM.
AES is faster.	DES is comparatively slower.
AES has a large secret key comparatively hence, more secure.	DES has a smaller key which is less secure.
Subbytes, Shiftrows, Mix columns, Addroundkeys.	Expansion Permutation, Xor, S-box, P-box, Xor, and Swap.

10 rounds for 128-bit algo 12 rounds for 192-bit algo 14 rounds for 256-bit algo	16 rounds

Key Distribution
Process of efficiently distributing cryptographic keys to the nodes that belong to a network. These keys could either be pairwise keys (for two party communications), group keys (for cluster-wide communication), or network keys (for secure broadcast communication).

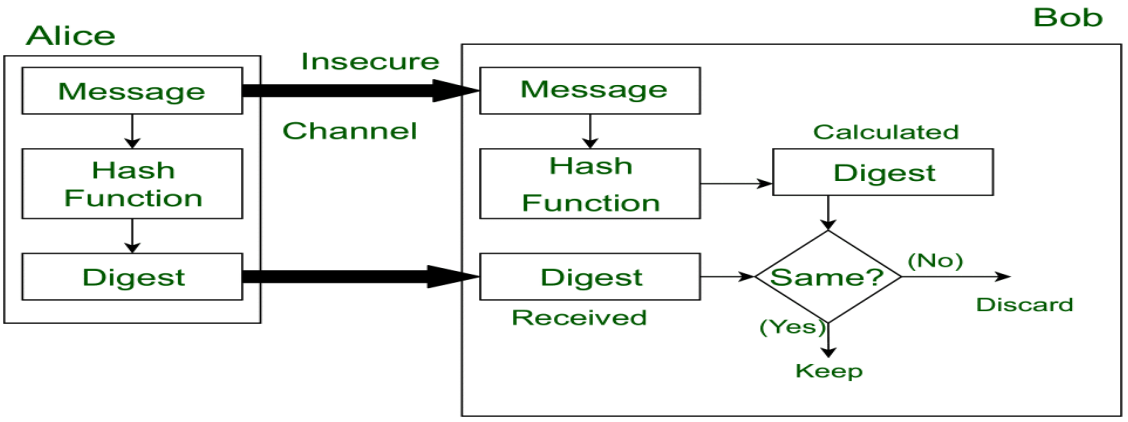
Message authentication code:
There are two methods for producing the message authentication code:
1.Data encryption standard (DES) product that requires a cryptographic product to be active. Using this method, both cryptography and message authentication can be performed concurrently. Although the keyword is DES, if the session is setup to use triple-DES encryption, TDES24 will be used. The use of the term DES here does not mean only DES encryption can be used.
2.Cyclic redundancy check (CRC), which creates a message authentication code using an internal VTAM algorithm. Using this method does not require a cryptography product to be active.

SHA-1
SHA-1 or Secure Hash Algorithm 1 is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value. This hash value is known as a message digest. This message digest is usually then rendered as a hexadecimal number which is 40 digits long. It is a U.S. Federal Information Processing Standard and was designed by the United States National Security Agency.
SHA-1 works by feeding a message as a bit string of length less than 2^64 bits, and producing a 160-bit hash value known as a message digest. Note that the message below is represented in hexadecimal notation for compactness.
There are two methods to encrypt messages using SHA-1. Although one of the methods saves the processing of sixty-four 32-bit words, it is more complex and time-consuming to execute, so the simple method is shown in the example below. At the end of the execution, the algorithm outputs blocks of 16 words, where each word is made up of 16 bits, for a total of 256 bits.

MD5
MD5 (Message Digest Method 5) is a cryptographic hash algorithm used to generate a 128-bit digest from a string of any length. It represents the digests as 32 digit hexadecimal numbers. Message Digest is used to ensure the integrity of a message transmitted

over an insecure channel (where the content of the message can be changed). The message is passed through a Cryptographic hash function. This function creates a compressed image of the message called Digest.

Lets assume, Alice sent a message and digest pair to Bob. To check the integrity of the message Bob runs the cryptographic hash function on the received message and gets a new digest. Now, Bob will compare the new digest and the digest sent by Alice. If, both are same then Bob is sure that the original message is not changed.



This message and digest pair is equivalent to a physical document and fingerprint of a person on that document. Unlike the physical document and the fingerprint, the message and the digest can be sent separately.

- Most importantly, the digest should be unchanged during the transmission.
- The cryptographic hash function is a one way function, that is, a function which is practically infeasible to invert. This cryptographic hash function takes a message of variable length as input and creates a digest / hash / fingerprint of fixed length, which is used to verify the integrity of the message.
- Message digest ensures the integrity of the document. To provide authenticity of the message, digest is encrypted with sender's private key. Now this digest is called digital signature, which can be only decrypted by the receiver who has sender's public key. Now the receiver can authenticate the sender and also verify the integrity of the sent message.

RSA algorithm

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and Private key is kept private. An example of asymmetric cryptography :

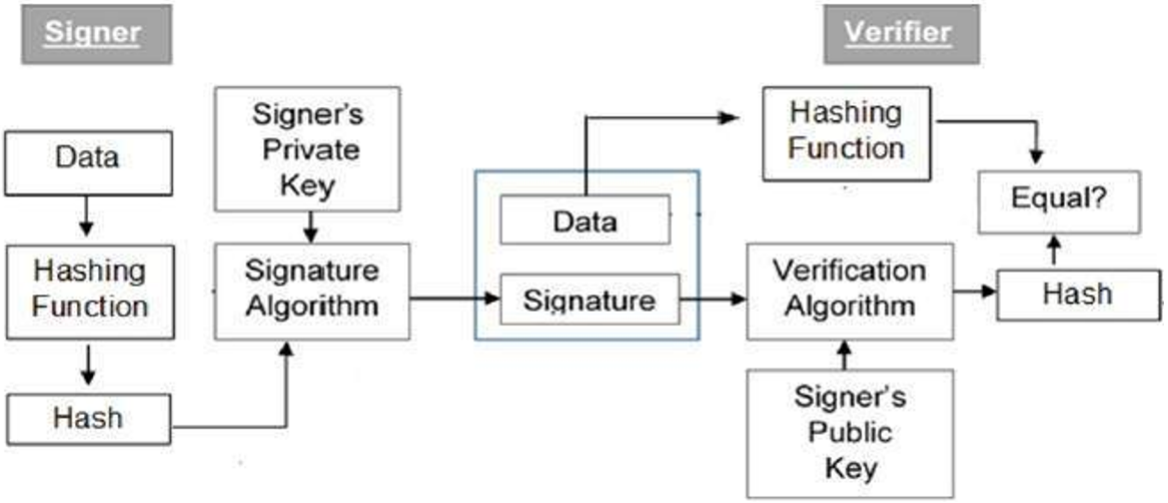
1. A client (for example browser) sends its public key to the server and requests for some data.
2. The server encrypts the data using client's public key and sends the encrypted data.

3. Client receives this data and decrypts it.

Since this is asymmetric, nobody else except browser can decrypt the data even if a third party has public key of browser.
The idea! The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024 bit keys could be broken in the near future. But till now it seems to be an infeasible task.

Digital Signature Algorithm (DSA)

Digital Signature Algorithm (DSA) is one of the Federal Information Processing Standard for making digital signatures depends on the mathematical concept or we can say the formulas of modular exponentiation and the discrete logarithm problem to cryptograph the signature digitally in this algorithm.
It is Digital signatures are the public-key primitives of message authentication in cryptography. In fact, in the physical world, it is common to use handwritten signatures on handwritten or typed messages at this time. Mainly, they are used to bind signatory to the message to secure the message.
Therefore, a digital signature is a technique that binds a person or entity to the digital data of the signature. Now, this will binding can be independently verified by the receiver as well as any third party to access that data.
Here, Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer or the person whose signature is that.



Explanation of the block diagram

- Firstly, each person adopting this scheme has a public-private key pair in cryptography.

- The key pairs used for encryption or decryption and signing or verifying are different for every signature. Here, the private key used for signing is referred to as the signature key and the public key as the verification key in this algorithm.
- Then, people take the signer feeds data to the hash function and generates a hash of data of that message.
- Now, the Hash value and signature key are then fed to the signature algorithm which produces the digital signature on a given hash of that message. This signature is appended to the data and then both are sent to the verifier to secure that message.
- Then, the verifier feeds the digital signature and the verification key into the verification algorithm in this DSA. Thus, the verification algorithm gives some value as output as a ciphertext.
- Thus, the verifier also runs the same hash function on received data to generate hash value in this algorithm.
- Now, for verification, the signature, this hash value, and output of verification algorithm are compared with each variable. Based on the comparison result, the verifier decides whether the digital signature is valid for this or invalid.
- Therefore, the digital signature is generated by the 'private' key of the signer and no one else can have this key to secure the data, the signer cannot repudiate signing the data in the future to secure that data by the cryptography.

Key Distribution

In cryptography, it is a very tedious task to distribute the public and private keys between sender and receiver. If the key is known to the third party (forger/eavesdropper) then the whole security mechanism becomes worthless. So, there comes the need to secure the exchange of keys.

There are two aspects for Key Management:

1. Distribution of public keys.
2. Use of public-key encryption to distribute secrets.

Distribution of Public Key:

The public key can be distributed in four ways:

1. Public announcement
2. Publicly available directory
3. Public-key authority
4. Public-key certificates.

These are explained as following below:

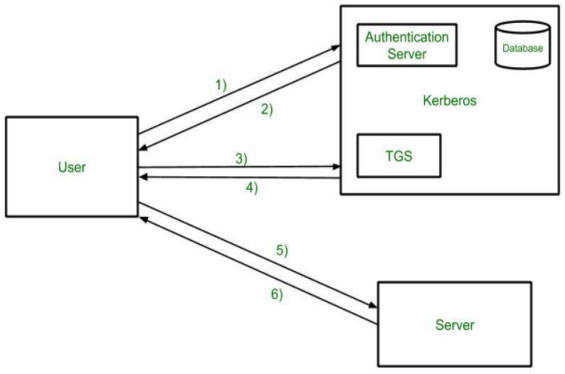
1. Public Announcement: Here the public key is broadcasted to everyone. The major weakness of this method is a forgery. Anyone can create a key claiming to be someone else and broadcast it. Until forgery is discovered can masquerade as claimed user.

2. Publicly Available Directory: In this type, the public key is stored in a public directory. Directories are trusted here, with properties like Participant Registration, access and allow to modify values at any time, contains entries like {name, public-key}. Directories can be accessed electronically still vulnerable to forgery or tampering.
3. Public Key Authority: It is similar to the directory but, improves security by tightening control over the distribution of keys from the directory. It requires users to know the public key for the directory. Whenever the keys are needed, real-time access to the directory is made by the user to obtain any desired public key securely.
4. Public Certification: This time authority provides a certificate (which binds an identity to the public key) to allow key exchange without real-time access to the public authority each time. The certificate is accompanied by some other info such as period of validity, rights of use, etc. All of this content is signed by the private key of the certificate authority and it can be verified by anyone possessing the authority's public key.

Kerberos

Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users. In Kerberos Authentication server and database is used for client authentication. Kerberos runs as a third-party trusted server known as the Key Distribution Center (KDC). Each user and service on the network is a principal.
The main components of Kerberos are:
1.Authentication Server (AS):
The Authentication Server performs the initial authentication and ticket for Ticket Granting Service.
2.Database:
The Authentication Server verifies the access rights of users in the database.
3.Ticket Granting Server (TGS):
The Ticket Granting Server issues the ticket for the Server

Kerberos Overview:



Step:-
1.User login and request services on the host. Thus user requests for ticket-granting service.
2.Authentication Server verifies user's access right using database and then gives ticket-granting-ticket and session key. Results are encrypted using the Password of the user.
3.The decryption of the message is done using the password then send the ticket to Ticket Granting Server. The Ticket contains authenticators like user names and network addresses.
4.Ticket Granting Server decrypts the ticket sent by User and authenticator verifies the request then creates the ticket for requesting services from the Server.
5.The user sends the Ticket and Authenticator to the Server.
6.The server verifies the Ticket and authenticators then generate access to the service. After this User can access the services.

Kerberos Limitations
Each network service must be modified individually for use with Kerberos, It doesn't work well in a timeshare environment, Secured Kerberos Server, Requires an always-on Kerberos server, Stores all passwords are encrypted with a single key, Assumes workstations are secure, May result in cascading loss of trust., Scalability

Is Kerberos Infallible?
No security measure is 100% impregnable, and Kerberos is no exception. Because it's been around for so long, hackers have had the ability over the years to find ways around it, typically through forging tickets, repeated attempts at password guessing (brute force/credential stuffing), and the use of malware, to downgrade the encryption.
Despite this, Kerberos remains the best access security protocol available today. The protocol is flexible enough to employ stronger encryption algorithms to combat new threats, and if users employ good password-choice guidelines, you shouldn't have a problem!

What is Kerberos Used For?
Although Kerberos can be found everywhere in the digital world, it is commonly used in secure systems that rely on robust authentication and auditing capabilities. Kerberos is used for Posix, Active Directory, NFS, and Samba authentication. It is also an alternative authentication system to SSH, POP, and SMTP.

Kerberos Version 4 :
Kerberos version 4 is an update of the Kerberos software that is a computer-network authentication system. Kerberos version 4 is a web-based authentication software which is used for authentication of users information while logging into the system by DES technique for encryption. It was launched in late 1980s.

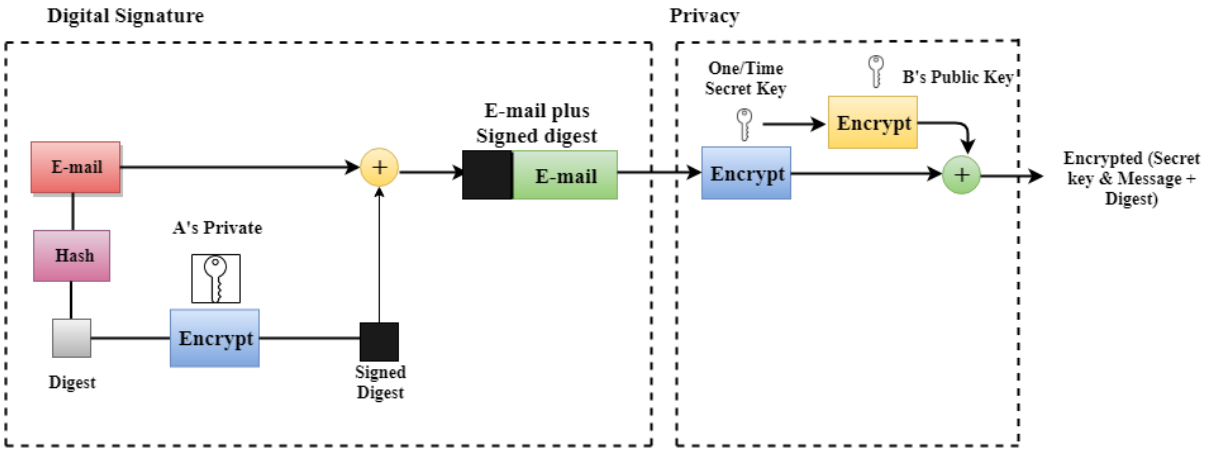
Difference between Karberos version 4 and Karberos version 5

Kerberos Version 4	Kerberos Version 5
Kerberos version 4 was released prior to version 5 in the late 1980s	Version 5 was published in 1993, years after the appearance of version 5.
Ticket support is Satisfactory in this version.	Ticket support is well extended. Facilitates forwarding, renewing, and postdating tickets.
It uses the “receiver-makes-right” encoding system.	It uses the ASN. I coding system.
Since the same key is used repeatedly to gain a service from particular server, there is a risk that an attacker can replay messages from an old session to the client or server.	In V5 this is avoided by requiring a sub-session key which is used only for one connection.
Kerberos V4 uses DES encryption techniques.	In Kerberos V5 the ciphertext is tagged with an encryption type identifier hence any type of encryption can be used.
Kerberos uses IP addressing.	Kerberos V5 can use any address since the address is now tagged with type and length.
In V4 the ticket lifetime has to be specified in units of 5 minutes.	In V5 ticket lifetime, one can specify explicit start and finish times allowing arbitrary lifetimes.
It contains only a few IP addresses and other addresses for types of network protocols.	It contains only multiple IP addresses and other addresses for types of network protocols.

PGP

- PGP stands for Pretty Good Privacy (PGP) which is invented by Phil Zimmermann.
- PGP was designed to provide all four aspects of security, i.e., privacy, integrity, authentication, and non-repudiation in the sending of email.
- PGP uses a digital signature (a combination of hashing and public key encryption) to provide integrity, authentication, and non-repudiation. **PGP uses a combination of secret key encryption and public key encryption to provide privacy. Therefore, we can say that the digital signature uses one hash function, one secret key, and two private-public key pairs.**
- **PGP is an open source and freely available software package for email security.**
- PGP provides authentication through the use of Digital Signature.
- It provides confidentiality through the use of symmetric block encryption.
- It provides compression by using the ZIP algorithm, and EMAIL compatibility using the radix-64 encoding scheme.

PGP at the Sender site (A)

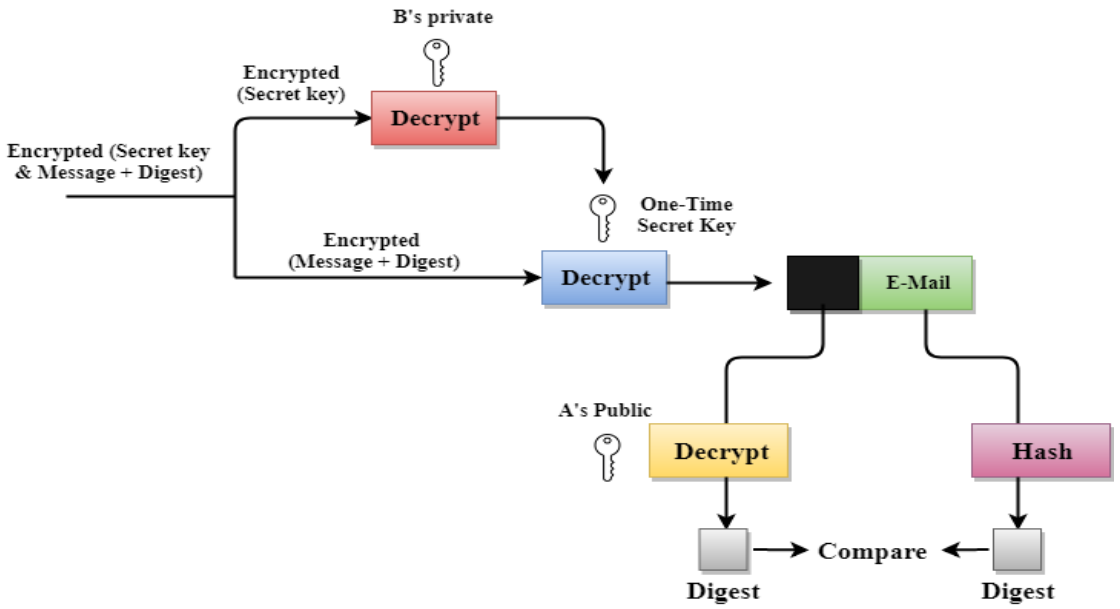


Following are the steps taken to show how PGP uses hashing and a combination of three keys to generate the original message:

- The receiver receives the combination of encrypted secret key and message digest is received.

- The encrypted secret key is decrypted by using the receiver's private key to get the one-time secret key.
- The secret key is then used to decrypt the combination of message and digest.
- The digest is decrypted by using the sender's public key, and the original message is hashed by using a hash function to create a digest.
- Both the digests are compared if both of them are equal means that all the aspects of security are preserved.

PGP at the Receiver site (B)



Disadvantages of PGP Encryption

- The Administration is difficult: The different versions of PGP complicate the administration.
- Compatibility issues: Both the sender and the receiver must have compatible versions of PGP. For example, if you encrypt an email by using PGP with one of the encryption technique, the receiver has a different version of PGP which cannot read the data.
- Complexity: PGP is a complex technique. Other security schemes use symmetric encryption that uses one key or asymmetric encryption that uses two different keys. PGP uses a hybrid approach that implements symmetric encryption with two keys. PGP is more complex, and it is less familiar than the traditional symmetric or asymmetric methods.

- No Recovery: Computer administrators face the problems of losing their passwords. In such situations, an administrator should use a special program to retrieve passwords. For example, a technician has physical access to a PC which can be used to retrieve a password. However, PGP does not offer such a special program for recovery; encryption methods are very strong so, it does not retrieve the forgotten passwords results in lost messages or lost files.

IP security (IPSec)

The IP security (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

Uses of IP Security –

IPsec can be used to do the following things:

1.To encrypt application layer data.

2.To provide security for routers sending routing data across the public internet.

3.To provide authentication without encryption, like to authenticate that the data originates from a known sender.

4.To protect network data by setting up circuits using IPsec tunneling in which all data is being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection.

Components of IP Security –

It has the following components:

1. Encapsulating Security Payload (ESP) –
   It provides data integrity, encryption, authentication and anti replay. It also provides authentication for payload.
2. Authentication Header (AH) –
   It also provides data integrity, authentication and anti replay and it does not provide encryption. The anti replay protection, protects against unauthorized transmission of packets. It does not protect data's confidentiality.
3. Internet Key Exchange (IKE) –
   It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. The Key Management Protocol (ISAKMP) and Internet Security Association which provides a framework for authentication and key exchange. ISAKMP tells how the set up of the Security Associations (SAs) and how direct connections between two hosts that are using IPsec.
   Internet Key Exchange (IKE) provides message content protection and also an open frame for implementing standard algorithms such as SHA and MD5.

The algorithm's IP sec users produces a unique identifier for each packet. This identifier then allows a device to determine whether a packet has been correct or not. Packets which are not authorized are discarded and not given to receiver.

Working of IP Security –

1. The host checks if the packet should be transmitted using IPsec or not. These packet traffic triggers the security policy for themselves. This is done when the system sending the packet apply an appropriate encryption. The incoming packets are also checked by the host that they are encrypted properly or not.
2. Then the IKE Phase 1 starts in which the 2 hosts(using IPsec) authenticate themselves to each other to start a secure channel. It has 2 modes. The Main mode which provides the greater security and the Aggressive mode which enables the host to establish an IPsec circuit more quickly.
3. The channel created in the last step is then used to securely negotiate the way the IP circuit will encrypt data across the IP circuit.
4. Now, the IKE Phase 2 is conducted over the secure channel in which the two hosts negotiate the type of cryptographic algorithms to use on the session and agreeing on secret keying material to be used with those algorithms.
5. Then the data is exchanged across the newly created IPsec encrypted tunnel. These packets are encrypted and decrypted by the hosts using IPsec SAs.
6. When the communication between the hosts is completed or the session times out then the IPsec tunnel is terminated by discarding the keys by both the hosts.

IPSec Architecture

IPSec (IP Security) architecture uses two protocols to secure the traffic or data flow. These protocols are ESP (Encapsulation Security Payload) and AH (Authentication Header). IPSec Architecture include protocols, algorithms, DOI, and Key Management. All these components are very important in order to provide the three main services:

1.Confidentiality 2.Authentication 3.Integrity

IP Security Architecture:

1. Architecture:

Architecture or IP Security Architecture covers the general concepts, definitions, protocols, algorithms and security requirements of IP Security technology.

2. ESP Protocol:

ESP(Encapsulation Security Payload) provide the confidentiality service.

Encapsulation Security Payload is implemented in either two ways:

ESP with optional Authentication.,ESP with Authentication.

Packet Format:

Security Parameter Index(SPI):

This parameter is used in Security Association. It is used to give a unique number to the connection build between Client and Server.

Sequence Number:
Unique Sequence number are allotted to every packet so that at the receiver side packets can be arranged properly.

Payload Data:
Payload data means the actual data or the actual message. The Payload data is in encrypted format to achieve confidentiality.

Padding:
Extra bits or space added to the original message in order to ensure confidentiality. Padding length is the size of the added bits or space in the original message.

Next Header:
Next header means the next payload or next actual data.

Authentication Data
This field is optional in ESP protocol packet format.

3. Encryption algorithm:
Encryption algorithm is the document that describes various encryption algorithm used for Encapsulation Security Payload.
4. AH Protocol:
AH (Authentication Header) Protocol provides both Authentication and Integrity service. Authentication Header is implemented in one way only: Authentication along with Integrity.
Authentication Header covers the packet format and general issue related to the use of AH for packet authentication and integrity.
5. Authentication Algorithm:
Authentication Algorithm contains the set of the documents that describe authentication algorithm used for AH and for the authentication option of ESP.
6. DOI (Domain of Interpretation):
DOI is the identifier which support both AH and ESP protocols. It contains values needed for documentation related to each other.
7. Key Management:
Key Management contains the document that describes how the keys are exchanged between sender and receiver.

Web Security

Web security refers to protecting networks and computer systems from damage to or the theft of software, hardware, or data. It includes protecting computer systems from misdirecting or disrupting the services they are designed to provide.

Web security is synonymous with cybersecurity and also covers website security, which involves protecting websites from attacks. It includes cloud security and web application security, which defend cloud services and web-based applications, respectively. Protection of a virtual private network (VPN) also falls under the web security umbrella.

Web security is crucial to the smooth operation of any business that uses computers. If a website is hacked or hackers are able to manipulate your systems or software, your website—and even your entire network—can be brought down, halting business operations.

Factors That Go Into Web Security and Web Protection

To comply with internal policies, government-imposed criteria, or Open Web Application Security Project (OWASP) standards, security professionals consider a variety of factors. Keeping abreast with OWASP standards helps security staff stay up to date with industry-standard web safety expectations.

In addition, encryption must be kept up to date, the latest threats in the Web Hacking Incident Database (WHID) monitored, and user authentications properly managed. When vulnerabilities emerge, security personnel must install the most recent patches to address them. To secure data, software development teams have to implement protocols that shield code from being stolen during or after writing it.

Various technologies are available to help companies achieve web security, including web application firewalls (WAFs), security or vulnerability scanners, password-cracking tools, fuzzing tools, black box testing tools, and white box testing tools.

Web Application Firewalls (WAFs)

A web application firewall (WAF) protects web applications by monitoring and filtering internet traffic that flows between an application and the internet. In this way, a WAF works as a secure web gateway (SWG). It provides protection for web applications against attacks, including cross-site scripting, file inclusion, cross-site forgery, Structured Query Language (SQL) injection, and other threats.

In the Open Systems Interconnection (OSI) model, a WAF works within Layer 7. Even though it works against many internet threats, it is not intended to defend against all kinds of threats. A WAF often works within a suite of protective tools meant to defend a network, computer, or application.

Threats to Web Security

SQL Injection

SQL injection is a technique an attacker uses to exploit vulnerabilities in a database's search process. With SQL injection, an attacker can obtain access to privileged information, create user permissions, modify permissions, or execute plans to change, manipulate, or destroy data. In this way, a hacker can capture

sensitive information or alter it to interrupt or control the functioning of a crucial system.

Cross-site Scripting

Cross-site scripting (XSS) refers to a vulnerability that gives hackers an opening to insert client-side scripts inside a page. This is then used to gain access to critical data directly. XSS can also be used by a hacker to pretend to be another user or to fool a user into disclosing crucial information.

Remote File Inclusion

With remote file inclusion, an attacker references external scripts using vulnerabilities in a web application. The attacker can then attempt to use the referencing function within an application to upload malware. These types of malware are also referred to as backdoor shells. All this is done from a different Uniform Resource Locator (URL) within a separate domain.

Password Breach

Breaching a user's password is a common technique to gain access to web resources. In many cases, the hacker will use a password that the user or administrator had used to log in to another site for which the hacker has a list of login credentials.

In other cases, hackers use a technique called password spraying, in which they use common passwords like "12345678" or "password123," and try them out one after the other until they gain access. There are several other techniques like keyloggers or simply finding your password written down and using it.

Data Breach

A data breach refers to when confidential or sensitive information gets exposed. Data breaches can sometimes happen by accident, but they are often perpetrated by hackers with the intention of using or selling the data.

Code Injection

Code injection involves an attacker using an input validation vulnerability in a computer's software system to introduce and run malicious code. This code then proceeds to make changes to how the software and computer work.

Secure Sockets Layer

Secure Sockets Layer (SSL) is a standard technique for transmitting documents securely across a network. SSL technology, created by Netscape, establishes a secure connection between a Web server and a browser, ensuring private and secure data transmission. SSL communicates using the Transport Control Protocol (TCP).

The term "socket" in SSL refers to the method of sending data via a network between a client and a server.

A Web server requires an SSL certificate to establish a secure SSL connection while using SSL for safe Internet transactions. SSL encrypts network connection segments atop the transport layer, a network connection component above the program layer. SSL is based on an asymmetric cryptographic process in which a Web browser generates both a public and a private (secret) key. A certificate signing request is a

data file that contains the public key (CSR). Only the recipient receives the private key.

How Does SSL Work?

SSL encrypts data communicated across the web to guarantee a high level of privacy. Anyone attempting to intercept this data will meet a jumbled mess of characters nearly hard to decrypt.

SSL begins an authentication process known as a handshake between two communicating devices to confirm that both devices are who they say they are.

SSL also digitally certifies data to ensure data integrity, ensuring that it has not been tampered with before reaching its intended receiver.

SSL has gone through multiple incarnations, each one more secure than the last. TLS (Transport Layer Security) was introduced in 1999, replacing SSL.

Objectives of SSL

The goals of SSL are as follows −

- Data integrity − Information is safe from tampering. The SSL Record Protocol, SSL Handshake Protocol, SSL Change CipherSpec Protocol, and SSL Alert Protocol maintain data privacy.
- Client-server authentication − The SSL protocol authenticates the client and server using standard cryptographic procedures.
- SSL is the forerunner of Transport Layer Security (TLS), a cryptographic technology for secure data transfer over the Internet.

Transport layer security

Transport layer security protocol is one of the security protocols which are designed to facilitate privacy and data security for communications over the Internet. The main use of TLS is to encrypt the communication between web applications and servers, like web browsers loading a website.

TLS is used to encrypt other communications like email, messaging, and voice over IP (VoIP). TLS was proposed by the Internet Engineering Task Force (IETF), which is an international standards organization.

Components

The three main components that TLS accomplishes are as follows −

- Encryption − It is used to hide the data being transferred from third parties.
- Authentication − It always ensures that the parties exchanging information are who they claim to be.
- Integrity − Integrity verifies that the data has not been tampered with.

Advantages

The advantages of TLS are as follows−

Encryption, Interoperability, Flexibility, Easy of deployment, Easy to use.

TLS handshake Protocol

The working condition of the TLS Handshake protocol is shown below −

Here,

- A client sends a synchronous message “client hello” requesting a connection and presents a list of supported cipher suites and a random string of bytes.
- The server responds with a “server hello” message containing a server certificate.
- The server is sending its SSL certificate to the client for the purpose of authentication. The client then authenticates the server by verifying the server's SSL certificate, and also sends a certificate for authentication if requested by the server.
- The client sends the client key exchange, change Cipher specification finished message to the server.
- The server decrypts the message sent by client secret with the private key.
- Both client and server generate session keys from the client random, the server random, and the secret message.
- The client sends a “finished” message that has been encrypted with a session key.
- The server responds with a finished message which was encrypted with a session key.
- The client and server have successfully achieved secure symmetric encryption, meaning the handshake is complete and communication can continue with the established session keys.
- Finally transfer the application data.

Following are the important differences between SSL and TLS.

Sr. No.	Key	SSL	TLS
1	Full Form	SSL stands for Secure Socket Layer	TLS stands for Transport Layer Security.
2	Fortezza Algorithm	Fortezza algorithm is supported in SSL.	Fortezza algorithm is not supported in TLS.
3	Version	Presently SSL is in 3.0.	Presently TLS is in 1.0
4	Master Secret Code	SSL uses Message Digest to create a master secret code.	TLS uses a pseudo-random function to create a master secret code.
5	Authentication	SSL uses Message Authentication Code protocol.	TLS uses Hashed Message Authentication Code protocol.

6	Complexity	SSL is complex than TLS.	TLS is simple to implement.

Secure Electronic Transaction

Secure Electronic Transaction or SET is a system that ensures the security and integrity of electronic transactions done using credit cards in a scenario. SET is not some system that enables payment but it is a security protocol applied to those payments. It uses different encryption and hashing techniques to secure payments over the internet done through credit cards. The SET protocol was supported in development by major organizations like Visa, Mastercard, Microsoft which provided its Secure Transaction Technology (STT), and Netscape which provided the technology of Secure Socket Layer (SSL).

SET protocol restricts the revealing of credit card details to merchants thus keeping hackers and thieves at bay. The SET protocol includes Certification Authorities for making use of standard Digital Certificates like X.509 Certificate.

Before discussing SET further, let's see a general scenario of electronic transactions, which includes client, payment gateway, client financial institution, merchant, and merchant financial institution.

Requirements in SET :

The SET protocol has some requirements to meet, some of the important requirements are :

1.It has to provide mutual authentication i.e., customer (or cardholder) authentication by confirming if the customer is an intended user or not, and merchant authentication.

2.It has to keep the PI (Payment Information) and OI (Order Information) confidential by appropriate encryptions.

3.It has to be resistive against message modifications i.e., no changes should be allowed in the content being transmitted.

4.SET also needs to provide interoperability and make use of the best security mechanisms.

Intruders

The most common threat to security is the attack by the intruder. Intruders are often referred to as hackers and are the most harmful factors contributing to the vulnerability of security. They have immense knowledge and an in-depth understanding of technology and security. Intruders breach the privacy of users and aim at stealing the confidential information of the users. The stolen information is then sold to third-party, which aim at misusing the information for their own personal or professional gains.

Intruders are divided into three categories:

- Masquerader: The category of individuals that are not authorized to use the system but still exploit user's privacy and confidential information by possessing techniques that give them control over the system, such category of intruders is referred to as Masquerader. A Masquerader is people that are outsiders and they don't have direct access to the system, which aims to attack unethically by stealing data/ information.
- Misfeasor: The category of individuals that are authorized to use the system, but misuse the granted access and privilege. These are individuals that take undue advantage of the permissions and access given to them, such category of intruders is referred to as Misfeasor. Masqueraders are people that are insiders and they have direct access to the system, which they aim to attack unethically by stealing data/ information.
- Clandestine User: The category of individuals that have supervision control over the system and misuse the authoritative power given to them. The misconduct of power is done often done by superlative authorities for financial gains, such a category of intruders is referred to as Clandestine User. A Clandestine User is people that can be any of the two, insiders or outsiders, and accordingly, they can have direct/ indirect access to the system, which they aim to attack unethically by stealing data/ information.

Intrusion Technique

1.Asymmetric Routing
In this method, the attacker attempts to utilize more than one route to the targeted network device. The idea is to have the overall attack evade detection by having a significant portion of the offending packets bypass certain network segments and their network intrusion sensors. Networks that are not set up for asymmetric routing are impervious to this attack methodology.
2.Buffer Overflow Attacks
This approach attempts to overwrite specific sections of computer memory within a network, replacing normal data in those memory locations with a set of commands that will later be executed as part of the attack. In most cases, the goal is to initiate a denial of service (DoS) situation, or to set up a channel through which the attacker can gain remote access to the network. Accomplishing such attacks is more difficult when network designers keep buffer sizes relatively small, and/or install boundary-checking logic that identifies executable code or lengthy URL strings before it can be written to the buffer.
3.Common Gateway Interface Scripts
The Common Gateway Interface (CGI) is routinely used in networks to support interaction between servers and clients on the Web. But it also provides easy openings—such as "backtracking"—through which attackers can access supposedly secure network system files. When systems fail to include input verification or check for backtrack characters, a covert CGI script can easily add the directory label ".." or

the pipe "|" character to any file path name and thereby access files that should not be available via the Web.

4.Protocol-Specific Attacks

When performing network activities, devices obey specific rules and procedures. These protocols—such as ARP, IP, TCP, UDP, ICMP, and various application protocols—may inadvertently leave openings for network intrusions via protocol impersonation ("spoofing") or malformed protocol messages. For example, Address Resolution Protocol (ARP) does not perform authentication on messages, allowing attackers to execute "man-in-the-middle" attacks. Protocol-specific attacks can easily compromise or even crash targeted devices on a network.

5.Traffic Flooding

An ingenious method of network intrusion simply targets network intrusion detection systems by creating traffic loads too heavy for the system to adequately screen. In the resulting congested and chaotic network environment, attackers can sometimes execute an undetected attack and even trigger an undetected "fail-open" condition.

Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for the harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.

Intrusion prevention systems also monitor network packets inbound the system to check the malicious activities involved in it and at once send the warning notifications.

Classification of Intrusion Detection System:

IDS are classified into 5 types:

1. Network Intrusion Detection System (NIDS):
   Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of a NIDS is installing it on the subnet

where firewalls are located in order to see if someone is trying to crack the firewall.

2. Host Intrusion Detection System (HIDS):
   Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.
3. Protocol-based Intrusion Detection System (PIDS):
   Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol. As HTTPS is un-encrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.
4. Application Protocol-based Intrusion Detection System (APIDS):
   Application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols. For example, this would monitor the SQL protocol explicit to the middleware as it transacts with the database in the web server.
5. Hybrid Intrusion Detection System :
   Hybrid intrusion detection system is made by the combination of two or more approaches of the intrusion detection system. In the hybrid intrusion detection system, host agent or system data is combined with network information to develop a complete view of the network system. Hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

Detection Method of IDS:

1. Signature-based Method:
   Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1’s or number of 0’s in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures.
   Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.

2. Anomaly-based Method:
   Anomaly-based IDS was introduced to detect unknown malware attacks as new malware are developed rapidly. In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model. Machine learning-based method has a better-generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

Password Protection

1. Use longer passwords

The longer the password, the harder it is to crack. Try using a phrase or sentence, rather than a single word. The more characters you add, the harder it is for an automated program to guess it.

2. Block common passwords

There are certain passwords that are so common that hackers use them as their first attempts. These passwords should be blacklisted, so your employees cannot use them to protect their accounts. You may also consider limiting the number of failed login attempts to block other brute-force attacks.

3. Use two-factor authentication

Passwords aren't your only method of protection. By adding two-factor (or multi-factor) authentication, you can add an extra layer of security. After entering a password, the user is sent a one-time code or USB token. Using two-factor authentication makes it much harder for hackers to gain access to the account.

4. Encrypt passwords

When you encrypt passwords or data before transmission, it enhances your security. If a hacker intercepts the transmission, they will be unable to decrypt it, thus rendering it useless.

5. Train your employees

The weakest link in network security is often the human element. People tend to write down passwords, share passwords, or use unsecured passwords without realizing the security risks. By taking the time to train your employees, you are helping to impress upon them their part in keeping your data secure. Getting your employees on board can make a big difference in your security.

It's important to protect your network with passwords, but in a way that will stop hackers in their tracks. Long passwords and encrypted passwords, two-factor authentication, and employee training can all help increase the strength of your security. Your network is only as strong as its weakest password.

Malwares – Malicious Software

Malware is a software that gets into the system without user consent with an intention to steal private and confidential data of the user that includes bank details and password. They also generates annoying pop up ads and makes changes in system settings

They get into the system through various means:

1. Along with free downloads.
2. Clicking on suspicious link.
3. Opening mails from malicious source.
4. Visiting malicious websites.
5. Not installing an updated version of antivirus in the system.

Types:

Virus, Worm, Logic Bomb, Trojan/Backdoor, Rootkit, Advanced Persistent Threat, Spyware and Adware

What is computer virus:

Computer virus refers to a program which damages computer systems and/or destroys or erases data files. A computer virus is a malicious program that self-replicates by copying itself to another program. In other words, the computer virus spreads by itself into other executable code or documents. The purpose of creating a computer virus is to infect vulnerable systems, gain admin control and steal user sensitive data. Hackers design computer viruses with malicious intent and prey on online users by tricking them.

Symptoms:

Letter looks like they are falling to the bottom of the screen.,The computer system becomes slow.,The size of available free memory reduces.,The hard disk runs out of space.,The computer does not boot.

Types of Computer Virus:

These are explained as following below.

1. Parasitic –
   These are the executable (.COM or .EXE execution starts at first instruction). Propagated by attaching itself to particular file or program. Generally resides at the start (prepending) or at the end (appending) of a file, e.g. Jerusalem.
2. Boot Sector –
   Spread with infected floppy or pen drives used to boot the computers. During system boot, boot sector virus is loaded into main memory and destroys data stored in hard disk, e.g. Polyboot, Disk killer, Stone, AntiEXE.
3. Polymorphic –
   Changes itself with each infection and creates multiple copies. Multipartite: use more than one propagation method. >Difficult for antivirus to detect, e.g. Involutionary, Cascade, Evil, Virus 101., Stimulate.
   Three major parts: Encrypted virus body, Decryption routine varies from infection to infection, and Mutation engine.
4. Memory Resident –
   Installs code in the computer memory. Gets activated for OS run and damages all files opened at that time, e.g. Randex, CMJ, Meve.

5. Stealth –
   Hides its path after infection. It modifies itself hence difficult to detect and masks the size of infected file, e.g. Frodo, Joshi, Whale.
6. Macro –
   Associated with application software like word and excel. When opening the infected document, macro virus is loaded into main memory and destroys the data stored in hard disk. As attached with documents; spreads with those infected documents only, e.g. DMV, Melissa, A, Relax, Nuclear, Word Concept.
7. Hybrids –
   Features of various viruses are combined, e.g. Happy99 (Email virus).

Worm:

A worm is a destructive program that fills a computer system with self-replicating information, clogging the system so that its operations are slowed down or stopped.
Types of Worm:

1. Email worm – Attaching to fake email messages.
2. Instant messaging worm – Via instant messaging applications using loopholes in network.
3. Internet worm – Scans systems using OS services.
4. Internet Relay Chat (IRC) worm – Transfers infected files to web sites.
5. Payloads – Delete or encrypt file, install backdoor, creating zombie etc.
6. Worms with good intent – Downloads application patches.

Logical Bomb:

A logical bomb is a destructive program that performs an activity when a certain action has occurred. These are hidden in programming code. Executes only when a specific condition is met, e.g. Jerusalem.
Script Virus:
Commonly found script viruses are written using the Visual Basic Scripting Edition (VBS) and the JavaScript programming language.

Trojan / Backdoor:

Trojan Horse is a destructive program. It usually pretends as computer games or application software. If executed, the computer system will be damaged. Trojan Horse usually comes with monitoring tools and key loggers. These are active only when specific events are alive. These are hidden with packers, crypters and wrappers.< Hence, difficult to detect through antivirus. These can use manual removal or firewall precaution.

RootKits:

Collection of tools that allow an attacker to take control of a system.

- Can be used to hide evidence of an attacker's presence and give them backdoor access.
- Can contain log cleaners to remove traces of attacker.

- Can be divided as:
  – Application or file rootkits: replaces binaries in Linux system
  – Kernel: targets kernel of OS and is known as a loadable kernel module (LKM)
- Gains control of infected m/c by:
  – DLL injection: by injecting malicious DLL (dynamic link library)
  – Direct kernel object manipulation: modify kernel structures and directly target trusted part of OS
  – Hooking: changing applicant's execution flow

Advanced Persistent Threat:
Created by well funded, organized groups, nation-state actors, etc. Desire to compromise government and commercial entities, e.g. Flame: used for reconnaissance and information gathering of system.
Spyware and Adware:
Normally gets installed along with free software downloads. Spies on the end-user, attempts to redirect the user to specific sites. Main tasks: Behavioral surveillance and advertising with pop up ads Slows down the system.

How The Antivirus Detects Virus?
Signature detection is a method by which antivirus keenly scans files that are brought into a system to analyze more likely hazardous files.
In essence, antivirus applications come with a directory of already checked-viruses and match the codes and patterns in files and web pages to unique bits and patterns that make up the code of a virus. If they match, the file is quarantined, means that it is moved to a new and safe location so that it does not infect any other files on the system.
Antivirus programs also checks for any malicious behavior on a system such as suspicious registry entries or executing an unknown program automatically upon system startup thus protecting our computer against encrypted viruses or viruses that are still unidentified.
Following is a list of the different virus detection methods an antivirus can use to protect our computer.

1. Virus Definitions :This is essentially the first method conventional antivirus software utilize to identify virus.
   The programs look for signatures to detect new malware. The antivirus companies analyze and extract an exact signature of the file and keep them in a database to which threats are compared and devices are then protected in case the signatures match.
2. Heuristic-based detection : This is the most common form of detection that uses an algorithm to compare the signature of known viruses against a potential threat. An antivirus packed with this type of detection can also detect viruses that have not yet been discovered and released as a new virus but it

can also generate false positive matches which means an antivirus scanner may report an uninfected file as an infected one.

3. Behavior-based detection :If a virus passes the above detection methods, the antivirus then observes the behavior of programs running on the computer. The antivirus triggers a warning if a program begins to perform strange actions listed below:
    - Settings of other programs are changed
    - Dozens of files are modified or deleted
    - Remotely connecting to computers
4. This is a useful method for finding viruses or any other type of malware that attempt to steal or log information.
5. Sandbox Detection : This is a type of detection method in which antivirus software run programs in a virtual environment and record the actions it performs to identify whether the programs are malicious or not. If the program is found safe, it is then executed in the real environment.
   This technique is rarely used in consumer antivirus solutions as it is both heavy and slow but antivirus solutions designed for corporate and network use offer this.
6. Data Mining : Data Mining is the recent development in malware detection that security companies now provide with their antivirus products to detect and eliminate forms of malware that has just been released. First, a series of features of files are extracted from files and then data mining and machine learning algorithms are used to determine the behavior of a file to detect whether the file is malicious or not.

What is a Firewall?

A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules. It acts as a barrier between internal private networks and external sources (such as the public Internet).

The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks. A firewall is a cybersecurity tool that filters network traffic and helps users block malicious software from accessing the Internet in infected computers.

How does a firewall work?

A firewall system analyzes network traffic based on pre-defined rules. It then filters the traffic and prevents any such traffic coming from unreliable or suspicious sources. It only allows incoming traffic that is configured to accept.

Typically, firewalls intercept network traffic at a computer's entry point, known as a port. Firewalls perform this task by allowing or blocking specific data packets (units of communication transferred over a digital network) based on pre-defined security rules. Incoming traffic is allowed only through trusted IP addresses, or sources.

Types of Firewall

Packet-filtering Firewalls

A packet filtering firewall is the most basic type of firewall. It acts like a management program that monitors network traffic and filters incoming packets based on configured security rules. These firewalls are designed to block network traffic IP

Circuit-level Gateways

Circuit-level gateways are another simplified type of firewall that can be easily configured to allow or block traffic without consuming significant computing resources. These types of firewalls typically operate at the session-level of the OSI model by verifying TCP (Transmission Control Protocol)

Application-level Gateways (Proxy Firewalls)

Proxy firewalls operate at the application layer as an intermediate device to filter incoming traffic between two end systems (e.g., network and traffic systems). That is why these firewalls are called 'Application-level Gateways'.

Stateful Multi-layer Inspection (SMLI) Firewalls

Stateful multi-layer inspection firewalls include both packet inspection technology and TCP

handshake verification, making SMLI firewalls superior to packet-filtering firewalls or circuit-level gateways. Additionally, these types of firewalls keep track of the status of established connections.

Next-generation Firewalls (NGFW)

Many of the latest released firewalls are usually defined as 'next-generation firewalls'. However, there is no specific definition for next-generation firewalls. This type of firewall is usually defined as a security device combining the features and functionalities of other firewalls. These firewalls include deep-packet inspection (DPI), surface-level packet inspection, and TCP handshake testing, etc.

Threat-focused NGFW

Threat-focused NGFW includes all the features of a traditional NGFW. Additionally, they also provide advanced threat detection and remediation. These types of firewalls are capable of reacting against attacks quickly. With intelligent security automation, threat-focused NGFW set security rules and policies, further increasing the security of the overall defense system.

Network Address Translation (NAT) Firewalls

Network address translation or NAT firewalls are primarily designed to access Internet traffic and block all unwanted connections. These types of firewalls usually hide the IP addresses of our devices, making it safe from attackers.