Cryptography &

Network Security

Suggestion made by: **MriDul TaLha**

Solve prepared by: **RaiHaN ChowDhurY**

1. What do you mean by network security? What are the traditional methods for network security?

Network security: Network security entails protecting the usability, reliability, integrity, and safety of network and data.

Network security is any system, device, or action designed to protect the safety and reliability of a network and its data.

Or, Network security is the protection of the layers of security to data, files, and directories against unauthorized access that could lead to data theft or misuse.

Traditional methods for network security: Traditionally network security was about protecting the boundaries of the environment, later more ubiquitous methods started to be introduced.

1990's - Firewall with DMZ and Bastion Host, some VLAN infrastructure and towards the end of the decade QoS.

2000's - The extension of VM, VL and virtual network environments, multiple DMZ with VPN concentrators and multi-factor for remote access. IDS became important then IPS was introduced along with the beginnings of defense in depth and tools like 802.1x, comprehensive QoS and PoS across both LAN and WAN environments.

2010's - True defense in depth approaches including Network Segmentation (function and protocol based), Next generation firewalls operating distributed across the environment, Identity and Access management. Remote data centers (and ASP providers) become known as "Cloud" and the usual restrictions are removed adding complexity and impacting security.

2. Define cryptography. How can cryptography work as a security tool?

Cryptography: The word 'cryptography' is derived from Greek word 'Kryptos' that means "hidden writing".

Cryptography is a method of protecting information and communications through the use of codes.

Or, Cryptography is the science to encrypt and decrypt data that enables the users to store sensitive information or transmit it across insecure networks so that it can be read only by the intended recipient.

Cryptography can work as a security tool:

A cryptographic algorithm works in combination with a key (can be a word, number, or phrase) to encrypt the plaintext and the same plaintext encrypts to different cipher text with different keys.

Hence, the encrypted data is completely dependent couple of parameters such as the strength of the cryptographic algorithm and the secrecy of the key.

Cryptography Techniques:

- **Symmetric Encryption** − Conventional cryptography, also known as conventional encryption, is the technique in which only one key is used for both encryption and decryption. For example, DES, Triple DES algorithms, MARS by IBM, RC2, RC4, RC5, RC6.
- **Asymmetric Encryption** − It is Public key cryptography that uses a pair of keys for encryption: a public key to encrypt data and a private key for decryption. Public key is published to the people while keeping the private key secret. For example, RSA, Digital Signature Algorithm (DSA), Elgamal.
- **Hashing** − Hashing is ONE-WAY encryption, which creates a scrambled output that cannot be reversed or at least cannot be reversed easily. For example, MD5 algorithm. It is used to create Digital Certificates, Digital signatures, Storage of passwords, Verification of communications, etc.

3. What do you mean by symmetric and asymmetric encryption a technique? Differentiate between them.

Symmetric encryption technique: A symmetric encryption is a technique where the same key is used to both encrypt and decrypt the data. The Caesar Cipher is one of the simplest symmetric encryption techniques.

Asymmetric encryption technique: Asymmetric Encryption is a technique where keys come in pairs. What one key encrypts, only the other can decrypt. Asymmetric Encryption is also known as Public Key Cryptography, since users typically create a matching key pair, and make one public while keeping the other secret.

Differentiate between Symmetric and Asymmetric encryption: The differences between symmetric and asymmetric encryption are given below:

Symmetric encryption	Asymmetric encryption
Symmetric cryptography uses the same secret (private) key to encrypt and decrypt its data.	Asymmetric uses both public and private key.
Mathematically it is represented as P= D (K, E(P)). Where, K is encryption and decryption key. P= plain text D= Decryption E(P)= Encryption of plain text.	Mathematically it is represented as P= D (Kd, E(Ke,P)). Where, Ke and Kd are encryption and decryption key. E(Ke,P)= Encryption of plain text using private key Ke.
The most commonly used symmetric encryption algorithms include DES, 3DES, AES, and RC4. 3DES and AES are commonly used in IPsec and other types of VPNs.	The most common asymmetric encryption algorithm is RSA.
Symmetric encryption requires a single key that must be shared by the sender and receiver.	Asymmetric encryption solves the key, distribution problem by using two keys, one of which is perfectly fine to share.
Symmetric encryption schemes are less secure than the asymmetric encryption.	Asymmetric encryption schemes are more secure
Symmetric encryption faster than asymmetric encryption.	Asymmetric encryption slower than Symmetric encryption.
Encryption process is less complicated.	Encryption process is more complicated.

4. Briefly explain OSI Security Architecture.

OSI Security Architecture: The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as follows:

- **Security Attack:** Any action that compromises the security of information owned by an organization.

  - Active attack: attempts to alter system resources or affect their operation.
  - Passive attack: aims to learn or make use of information from the system but does not affect system resources.

- **Security Mechanism:** A mechanism that is designed to detect, prevent, or recover from a security attack.

  Security mechanisms are used to implement security services. They include:
  - Decipherment
  - Digital signature
  - Access Control mechanisms
  - Data Integrity mechanisms
  - Authentication Exchange
  - Traffic Padding
  - Routing Control
  - Notarization

- **Security service:** A service that enhances the security of the data processing systems and the information transfers of an organization. The services make use of one or more security mechanisms to provide the service.

  Security services as follows:

  - Authentication: Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.
  - Access control: Requires that access to information resources may be controlled by or the target system.
  - Data confidentiality: The protection of data from unauthorized disclosure.
  - Data integrity: Ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification

includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages.

- Nonrepudiation: Requires that neither the sender nor the receiver of a message be able to deny the transmission.
- Availability service: Requires that computer system assets be available to authorized parties when needed.

5. Briefly explain different types of security services.

Security service: Security service is a service which ensures adequate security of the systems or of data transfers. Security services have divided into some categories:

- **Authentication:** The authentication service is concerning with assuring that a communication is authentic:
  - The recipient of the message should be sure that the message came from the source that it claims to be
  - All communicating parties should be sure that the connection is not interfered with by unauthorized party.

- **Access control:** This service controls
  - who can have access to a resource;
  - under what conditions access can occur;
  - what those accessing are allowing to do.

- **Data confidentiality:** The protection of data from unauthorized disclosure (from passive attacks).
  - Connection confidentiality
  - Connectionless confidentiality
  - Selective field confidentiality
  - Traffic-Flow Confidentiality.

- **Data integrity:**
  - The assurance that data received are exactly as sent by an authorized entity, i.e. contain (no modification, no insertion, no deletion, no replay).
  - Protection from active attacks.

- **Non-repudiation:**
  - Protection against denial by one of the entities involved in a communication of having participated in the communication.
  - Nonrepudiation can be related to:
    - Origin: proof that the message was sent by the specified party
    - Destination: proof that the message was received by the specified party

- **Availability services:**
  - Protects a system to ensure its availability
  - Particularly, it addresses denial-of-service attacks
  - Depends on other security services: access control, authentication, etc.

6. How can a plaintext can be converted into cipher text? Give example.

There are two transformations in which a plain text can be converted to obtain cipher text: Substitution transformation and Transposition transformation.

- Substitution Transformation: Substitution is done either by replacing a character by another character a number of places away from it in the collating sequence or by table lookup.

  We will assume the 26 letters are arranged circularly and we replace a character by the fourth character following it in the collating sequence. In other words, A is replaced be E, B by F, …., Y by C and Z by D. Suppose a plain text is:

  AQUICKFOXJUMPST

  Applying this method, the transformed plain text is:

  EUYMGOJSBNYQTWX
- Transposition transformation: Transposition is usually done by permutation of characters by a specified permutation operator.

  We choose blocks of five characters. Replace the first character of this five-character block by the fourth character, the second character by the first, the third character by the second character, the fourth by the fifth and the fifth by the third. The transformed Cipher text is:

  EUYMG | OJSBN | YQTWX

  Transposition by permutation gives:

  MEUGY | BOJNS | WYQXT

Decryption of the cipher text is done by applying the inverse transformation. Now, we apply the inverse permutation to blocks of 5 characters.
This gives:

EUYMGOJSBNYQTWX

Replacing a letter by the fourth letter preceding it, we get:

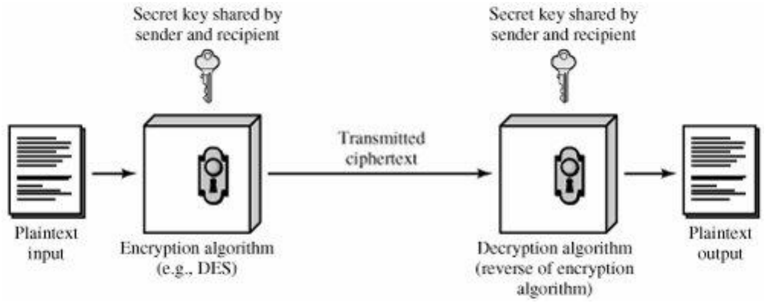
AQUICKFOXJUMPST

Which is the original plain text.

7. Explain the symmetric cipher model with its ingredients.

A Symmetric cipher model has five ingredients:

- **Plaintext:** This is the original intelligible data that is given to the algorithm as an input.
- **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.
- **Secret Key:** The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.
- **Cipher Text:** This is the scrambled message produced as output. It depends on the plain text and the secret key. For a given message, two different keys will produce two different cipher texts. The cipher text is an apparently random stream of data and, as it stands it is unintelligible.
- **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key and produces the original plaintext.


Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

8. Make a comparison/Differentiate between stream cipher and block ciphers with examples.

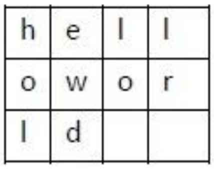
Both **Block Cipher** and **Stream Cipher** are belonging to the symmetric key cipher. These two block cipher and stream cipher are the methods used for converting the plain text into cipher text.

Block cipher	Stream cipher
Block Cipher Converts the plain text into cipher text by taking plain text's block at a time.	Stream Cipher Converts the plain text into cipher text by taking 1 byte of plain text at a time.
Block cipher uses either 64 bits or more than 64 bits.	While stream cipher uses 8 bits.
The complexity of block cipher is simple.	While stream cipher is more complex.
Block cipher Uses confusion as well as diffusion.	While stream cipher uses only confusion.
In block cipher, reverse encrypted text is hard.	While in stream cipher, reverse encrypted text is easy.
The algorithm modes which are used in block cipher are: ECB (Electronic Code Book) and CBC (Cipher Block Chaining).	The algorithm modes which are used in stream cipher are: CFB (Cipher Feedback) and OFB (Output Feedback).
Block cipher works on transposition techniques like Caesar cipher, Polygram substitution cipher, etc.	While stream cipher works on substitution techniques like rail-fence technique, columnar transposition technique, etc.
Block cipher is slow as compared to stream cipher.	While stream cipher is fast in comparison to block cipher.

9. Define transposition cipher. Why block cipher modes are convenient?

Transposition Cipher is a cryptographic algorithm where the order of alphabets in the plaintext is rearranged to form a cipher text. In this process, the actual plain text alphabets are not included.

Example: Consider the plain text hello world, and let us apply the simple columnar transposition technique as shown below:



h	e	l	l
o	w	o	r
l	d		

The plain text characters are placed horizontally and the cipher text is created with vertical format as: **holewdlo lr.** Now, the receiver has to use the same table to decrypt the cipher text to plain text.

Block cipher modes: A block cipher processes the data blocks of fixed size. Usually, the size of a message is larger than the block size. Hence, the long message is divided into a series of sequential message blocks, and the cipher operates on these blocks one at a time. Main block cipher modes of operation:

- Electronic codebook mode (ECB)
- Cipher block chaining (CBC)
- Cipher feedback (CFB)
- Output feedback (OFB)
- Counter mode (CTR)

Block cipher models are convenient because:

In ECB, it is easier because of direct encryption of each block of input plaintext and output is in form of blocks of encrypted cipher text.

In CBC, previous cipher block is given as input to next encryption algorithm after XOR with original plaintext block. In a nutshell here, a cipher block is produced by encrypting a XOR output of previous cipher block and present plaintext block.

In CFB, each cipher text block gets ‘fed back’ into the encryption process in order to encrypt the next plaintext block.

In OFB, these feedback blocks provide string of bits to feed the encryption algorithm which act as the key-stream generator as in case of CFB mode.

In CTR, both the sender and receiver need to access to a reliable counter, which computes a new shared value each time a cipher text block is exchanged.

10. Why do some block cipher modes of operation only use encryption while others use both encryption and decryption?

We know from the block cipher mode operations that, ECB and CBC use encryption function and decryption function because ECB and CBC generates output of Block Cipher type. And CFB, OFB and CTR use encryption function because CFB, OFB and CTR generates output of Stream Cipher type.

Some modes of operation (e.g. CTR) work in such a way that only known values are ever encrypted, forming a stream of pseudo-random data that is then combined with the plaintext by a keyless reversible operation (often XOR) to form the cipher text.

Other modes (e.g. CBC) directly encrypt secret (i.e. plaintext) values, meaning decryption is required to find out what the secret value was.

11. What is brute force attack? Give example of brute-force attack.

Or, briefly explain brute force attacks.

Brute force attack: The phrase "brute force" describes the simplistic manner in which the attack takes place. These attacks can be implemented by criminals to try to access data that is otherwise protected by credentials.

A **brute force** attack is a method used to obtain private user data.

Or, a brute force attack is a method used to obtain private user information such as usernames, passwords, passphrases, or Personal Identification Numbers (PINs).

These attacks are typically carried out using a script or bot to 'guess' the desired information until a correct entry is confirmed.

A brute force attack can also be a useful way for IT specialists to test the security of their networks. Indeed, one of the measures of a system's encryption strength is how long it would take for an attacker to be successful in a brute force attempt.

Example: Brute force attacks take place all the time and there are many high-profile examples to speak of. We likely don't even know about many bygone and ongoing attacks, but here are a few that have come to light in recent years:

- **Canadian Revenue Agency (CRA):** In August 2020, a credential stuffing attack resulted in the hacking of more than 11,000 accounts for the CRA and other government-related services.
- **Alibaba:** A massive 2016 brute force attack on the popular e-commerce site affected millions of accounts.
- **Northern Irish Parliament:** Also in March, 2018, the accounts of several members of the Northern Irish Parliament were accessed by brute force attackers.
- **Westminster Parliament:** An earlier attack hit Westminster Parliament in 2017 where up to 90 email accounts were compromised.
- **Firefox:** It was revealed early in 2018 that Firefox's 'master password' feature can be easily brute-force attacked. This means that over the past nine years, many users' credentials may have been exposed.

According to Kaspersky, RDP-related brute force attacks rose dramatically in 2020 due to the COVID-19 pandemic.

Types of brute force attack:

- **Dictionary attacks –** surmises usernames or passwords utilizing a dictionary of potential strings or phrases.
- **Rainbow table attacks –** a rainbow table is a precomputed table for turning around cryptographic hash capacities. It very well may be utilized to figure a capacity up to a specific length comprising of a constrained arrangement of characters.
- **Reverse brute force attack –** utilizes a typical password or assortment of passwords against numerous conceivable usernames. Focuses on a network of clients for which the attackers have recently acquired information.
- **Hybrid brute force attacks** – begins from outer rationale to figure out which password variety might be destined to succeed, and afterward proceeds with the simple way to deal with attempt numerous potential varieties.
- **Simple brute force attack** – utilizes an efficient way to deal with 'surmise' that doesn't depend on outside rationale.
- **Credential stuffing –** utilizes beforehand known password-username sets, attempting them against numerous sites. Adventures the way that numerous clients have the equivalent username and password across various frameworks.

The goal of a brute force attack:

Here is some goal of the brute force attack-

- Stealing or exposing users' personal information found inside online accounts
- Harvesting sets of credentials for sale to third parties
- Posing as account owners to spread fake content or phishing links
- Stealing system resources for use in other activities
- Defacement of a website through gaining access to admin credentials
- Spreading malware or spam content or redirecting domains to malicious content.

Brute force attacks can also be used to test for vulnerabilities in the system, so are not always malicious.

The prevention of brute force attack:

- Never use information that can be found online (like names of family members).
- Have as many characters as possible.
- Combine letters, numbers, and symbols.
- Avoid common patterns.
- Be different for each user account.
- Change your password periodically
- Use strong and long password
- Use multifactor authentication.
- Employing the use of CAPTCHAs.

What is Cryptanalysis? Explain various types of cryptanalysis attack with necessary diagram.

Or, briefly explain cryptanalysis attacks.

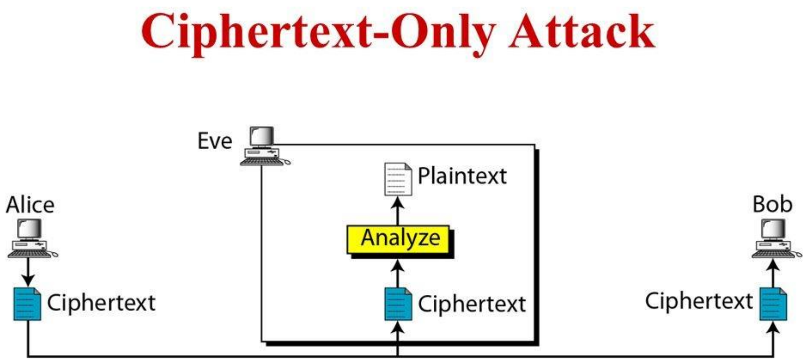
Cryptanalysis: Cryptanalysis is the process of breaking codes to decipher the information encoded.

Or, cryptanalysis is the art of trying to decrypt the encrypted messages without the use of the key that was used to encrypt the messages.

Or, cryptanalysis is the study of methods for obtaining the meaning of encrypted information, without access to the secret information that is typically required to do so. Typically, this involves knowing how the system works and finding a secret key. Cryptanalysis is also referred to as codebreaking or cracking the code.

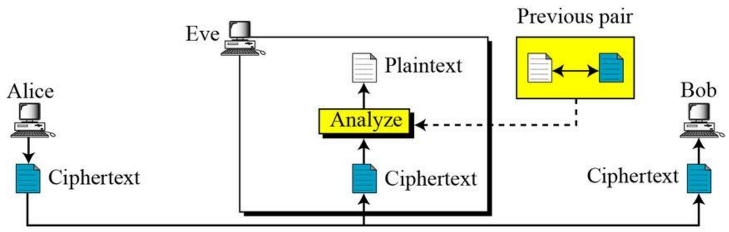
Various types of cryptanalysis attack: There are many different types of cryptanalysis attacks and techniques, which vary depending on how much information the analyst has about the cipher text being analyzed. Some cryptanalytic methods include:

- **Cipher text only attack (COA):** In this method, the attacker has access to a set of cipher text(s). He does not have access to corresponding plaintext. COA is said to be successful when the corresponding plaintext can be determined from a given set of cipher text. Occasionally, the encryption key can be determined from this attack. Modern cryptosystems are guarded against cipher text-only attacks.


Ciphertext-Only Attack

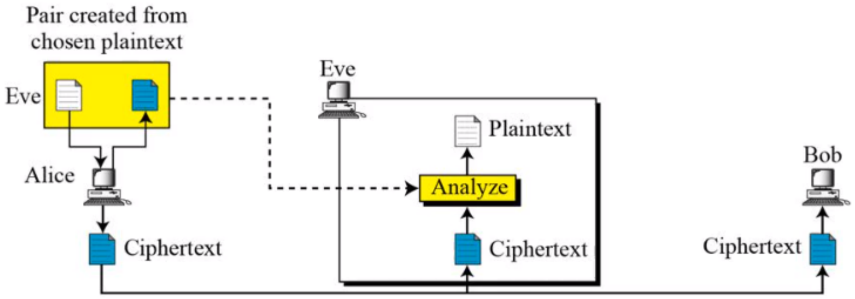
- **Known plain-text attack (KPA):** In this method, the attacker knows the plaintext for some parts of the cipher text. The task is to decrypt the rest of the cipher text using this information. This may be done by determining the key or via some other method. The best example of this attack is linear cryptanalysis against block ciphers.

Known-Plaintext Attack

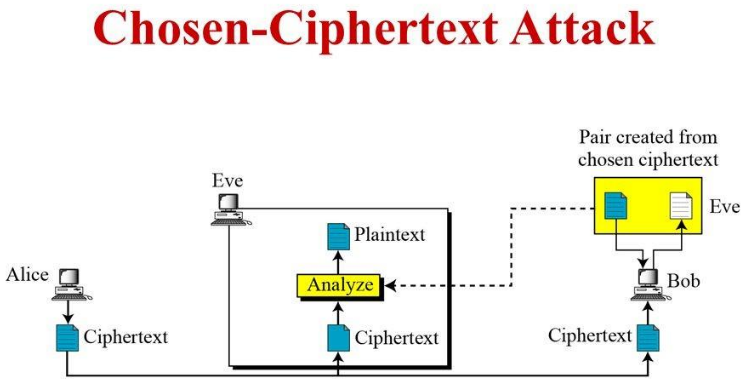


- **Chosen plain-text attack (CPA):** In this method, the attacker has the text of his choice encrypted. So he has the cipher text-plaintext pair of his choice. This simplifies his task of determining the encryption key. An example of this attack is differential cryptanalysis applied against block ciphers as well as hash functions. A popular public key cryptosystem, RSA is also vulnerable to chosen-plaintext attacks.

Chosen-Plaintext Attack



- **Chosen cipher-text attack (CCA):** In a chosen cipher text attack (CCA), the cryptanalyst can choose different cipher texts to be decrypted and has access to the decrypted plaintext. This type of attack is generally applicable to attacks against public key cryptosystems. An adaptive chosen cipher text attack involves the attacker selecting certain cipher texts to be decrypted, then using the results of these decryptions to select subsequent cipher texts.



- **Related-key attack:** In cryptography, a related-key attack is any form of cryptanalysis where the attacker can observe the operation of a cipher under several different keys whose values are initially unknown, but where some mathematical relationship connecting the keys is known to the attacker.
- **Brute force attack:** A brute force attack involves trying all possible keys until hitting on the one that results in plaintext. This can involve significant costs related to the amount of processing required to try quadrillions (in the case of DES) of keys. The time required is a factor of how many keys can be tried per unit of time, which is a factor of how many computers can be assigned to the task in parallel.
- **Birthday attack:** A birthday attack is a class of brute force attack used against hashing functions. It is based on the "birthday paradox." This states that in a group of 23 people, there is at least a 50% probability that at least two people will share the same birthday. In a group of 60 people, the probability is over 99%. A hash function gives a set value for a message. It can be easier for an attacker to find two messages with the same digest value than it is to match a specific value.

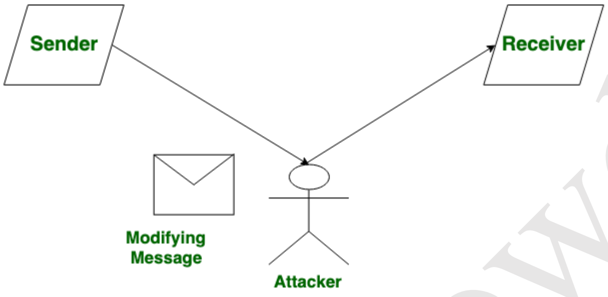
12. What is Security attack? List and briefly define categories of attack methodologies.

Or, briefly explain different types of security attacks.

Or, Discuss in a nutshell the different types of security attack with suitable figure.

Security attack: In computer network an attack is any attempt to destroy, expose alter, disable, steal or gain unauthorized access. There are two types of attack:

Active attack: An Active attack attempts to alter system resources or effect their operations. Active attack involves some modification of the data stream or creation of false statement.



Active Attack

Several types of active attacks in cryptography and network security:

- Brute-force attack:
  - A brute-force attack is a very simple attack.
  - Attacker uses a list of passwords and executes such operation.
  - Attacker tries every password from the list to login.
  - Attacker gain access to the victim’s account, if it recognizes the right password otherwise failed.

- Man-in-the-middle attack:
  - Probably, the attacker can change the communications between two parties.
  - The attacker makes an independent connection with the victim.
  - Attacker can see or broadcast the messages between sender & receiver.
  - Attacker can use the revealed information for some illegal activities.

- Replay attack:

  - The attacker captures each piece of traffic between two parties and re-transmits it constantly.
  - Attacker can easily fool the participants by replaying the transactions.
  - As a result, participants think that they have completed the operation.

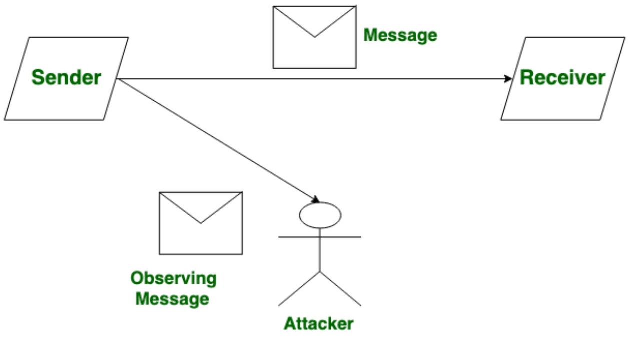
- Known plain text attack:
  - This attack is a standard attack for breaking ciphers.
  - Attacker is aware of the number of plain texts and also the cipher text.
  - This attack was effective against straightforward ciphers like the ‘substitution cipher’.

- Differential Crypt-Analysis:
  - This types of attacks are against block algorithms like DES, AES, etc.
  - The first aim of this attack is to find the ‘key’.
  - Attacker checks numerous messages of plain text into their converted cipher text.
  - The attacker chooses the plain text to look at the transformation.

- Dictionary attack:
  - Attacker makes a dictionary of cipher texts and their corresponding plain texts.
  - Attacker tries to find the corresponding plain text with the help of the dictionary.

- Side-channel attack:
  - This attack is occurred in the victim’s PC or Laptop.
  - Used to collect data through the plain-text, power consumption, sound, any secret key being processed, etc.
  - It is used to help the attacker to verify the secret key.

Passive attack: A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of overhearing on or monitoring of transmission.



Passive Attack

Several Types of Passive attacks are as following:

- Traffic analysis:
  - Attacker tries to predict the nature of communication by using information.
  - Information such as analyzing traffic, identify communication hosts, and frequency of messages.

- Release of Message content:
  - It is similar to hearing a telephone conversation between two users.
  - The attacker can monitor the content of the transmitted data such as email messages, etc.

13. Define encryption. State the applications of the public key crypto system.

Encryption: Encryption is the process of converting plaintext to cipher text.

Or, Encryption is the method by which information is converted into secret code that hides the information's true meaning.

Or, Encryption is a technique employed for keeping sensitive and private information safe, such as passwords, identity information, credit card details.

The applications of the public key crypto system: Public-key cryptosystem is one in which messages encrypted with one key can only be decrypted with a second key, and vice versa.

The applications for public-key cryptosystem can classified as follows:

- Encryption/Decryption: Content is encrypted using an individual’s public key and can only be decrypted with the individual’s private key.
- Digital signature: In this sender encrypt the plain text using his own private key. This step will make sure the authentication of the sender because receiver can decrypt the cipher text using senders pubic key only.
- Key exchange: If the sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received. The nature of the equipping they require depends on the encryption technique they might use.

14. State and explain the principles of public key cryptography.

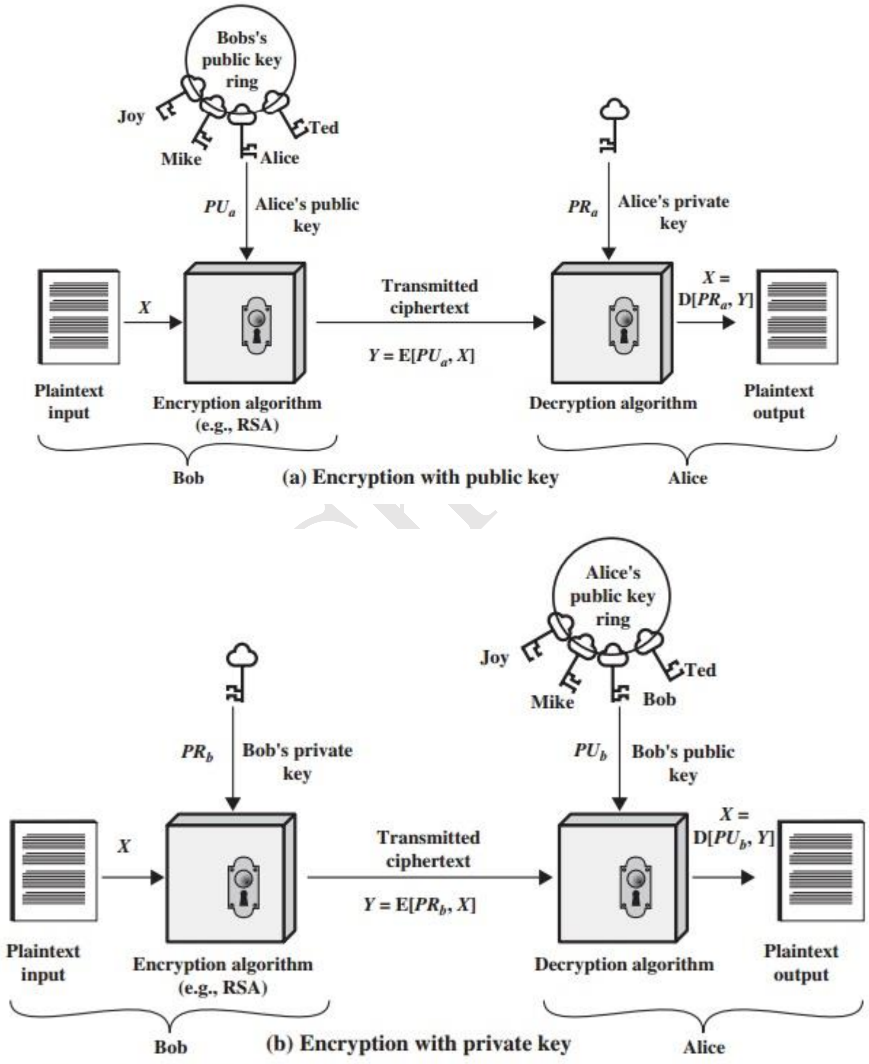
Public key: Public-key is a cryptographic system that uses pairs of keys. In Public key, two keys are used one key is used for encryption and another key is used for decryption.

Principles of public key cryptography:

- Asymmetric algorithms rely on one key for encryption and a different but related key for decryption. These algorithms have the following important characteristic.
    - It is computationally infeasible to determine the decryption key given only knowledge of the cryptographic algorithm and the encryption key.
- In addition, some algorithms, such as RSA, also exhibit the following characteristic:
    - Either of the two related keys can be used for encryption, with the other used for decryption.
- A public-key encryption scheme has six ingredients:
    - Plain text: This is the readable message or data that is fed into the algorithm as input.
    - Encryption algorithm: The encryption algorithm performs various transformations on the plaintext.
    - Public and private key: his is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the algorithm depend on the public or private key that is provided as input.

- Cipher text: This is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different cipher texts.
- Decryption algorithm: This algorithm accepts the cipher text and the matching key and produces the original plaintext.

Now, we will illustrate encryption and decryption in the below:



(a) Encryption with public key

(b) Encryption with private key

Figure 9.1 Public-Key Cryptography

The essential steps for following figure:

- Each user generates a pair of keys to be used for the encryption and decryption of messages.

- Each user places one of the two keys in a public register or other accessible file. This is the public key.
- The companion key is kept private. As shown in figure suggests, each user maintains a collection of public keys obtained from others.
- If Bob wishes to send a confidential message to Alice, Bob encrypts the message using Alice's public key.
- When Alice receives the message, she decrypts it using her private key. No other recipient can decrypt the message because only Alice knows Alice's private key.

15. Compare the security system on public key cryptography and private key cryptography.

Or, Difference between public key and private key.

Let's see that the difference between Public key and Private key:

Public key	Private key
Public key is slower than private key.	It is faster than public key.
In public key cryptography, two keys are used, one key is used for encryption and while the other is used for decryption.	In this, the same key (secret key) and algorithm is used to encrypt and decrypt the message.
In public key cryptography, one of the two keys is kept as a secret.	In private key cryptography, the key is kept as a secret.
Public key is Asymmetrical because there are two types of key: private and public key.	Private key is Symmetrical because there is only one key that is called secret key.
In this cryptography, sender and receiver does not need to share the same key.	In this cryptography, sender and receiver need to share the same key.
In this cryptography, public key can be public and private key is private.	In this cryptography, the key is private.

16. Differentiate public key and conventional encryption.

Public key encryption	Conventional encryption
It is a type of encryption scheme which instead of a single key, uses pair of keys to encrypt the message and decrypt it.	It is type of cryptographic system which uses a single key to both encrypt the message and decrypt it.
The public key can be shared freely to anyone while the private key is kept secret and is known only to the recipient.	The same secret key is shared by the sender and the recipient and must be kept secret all the times.
Public key encryption schemes are typically substantial slower than conventional encryption algorithms.	Conventional encryption algorithms are generally faster because they do not require as many CPU cycles as public key encryption.
It is more secure because the secret key is only known to the receiver and there are infinite numbers of possibilities for keys.	It is less secure because the same secret key is shared by both the sender and the recipient.

17. Distinguish between a session key and a master key.

Session key	Master key
A session key is a temporary encryption key used between two principals.	A master key is a long-lasting key that is used between a key distribution center and a principal for the purpose of encoding the transmission of session keys.
Communication between end system is encrypted using temporary key, often referred to as a session key.	Session keys are transmitted in encrypted form, using master key that is shared by the keys distribution center.
It has not a fixed size.	The master secret has a fixed size.

The TLS Protocol allows multiple connections within its sessions.	There would not be enough for all possible Connections.
The session key used for the duration of a logical connection, such as a frame relay connection or transport connection and then discarded.	For each end system or user, there is unique master key that it shares with the key distribution center.
It uses one way hashes.	It does not use one way hashes.

18. Perform encryption and decryption operation using RSA algorithm for a specific case.

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.

Generating public key:

- Select two prime no' s. Suppose $P = 53$ and $Q = 59$.
  Now First part of the Public key: $n = P*Q = 3127$.
- We also need a small exponent say e:
  But ‘e’ must be
  - An integer.
  - Not be a factor of n.
  - $1 < e < \Phi(n)$ [$\Phi(n)$ is discussed below],

  Let us now consider it to be equal to 3.
- Our Public Key is made of n and e.

Generating private key:

- We need to calculate $\Phi(n)$:
  Such that $\Phi(n) = (P-1)(Q-1)$
  so, $\Phi(n) = 3016$
- Now calculate Private Key, d:
  $d = (k*\Phi(n) + 1) / e$ for some integer k
  For $k = 2$, value of d is 2011.

Now we are ready with our – Public Key (n = 3127 and e = 3) and Private Key (d = 2011).

Now we will encrypt “HI”:

- Convert letters to numbers: H = 8 and I = 9

- Thus Encrypted Data c = 89e mod n.
  Thus our Encrypted Data comes out to be 1394.

Now we will decrypt 1394:

- Decrypted Data = cd mod n.
  Thus our Encrypted Data comes out to be 89.

8 = H and I = 9 i.e. "HI".

19. Explain Data Encryption Standard (DES) in detail.

Or, briefly explain general DES encryption algorithm.

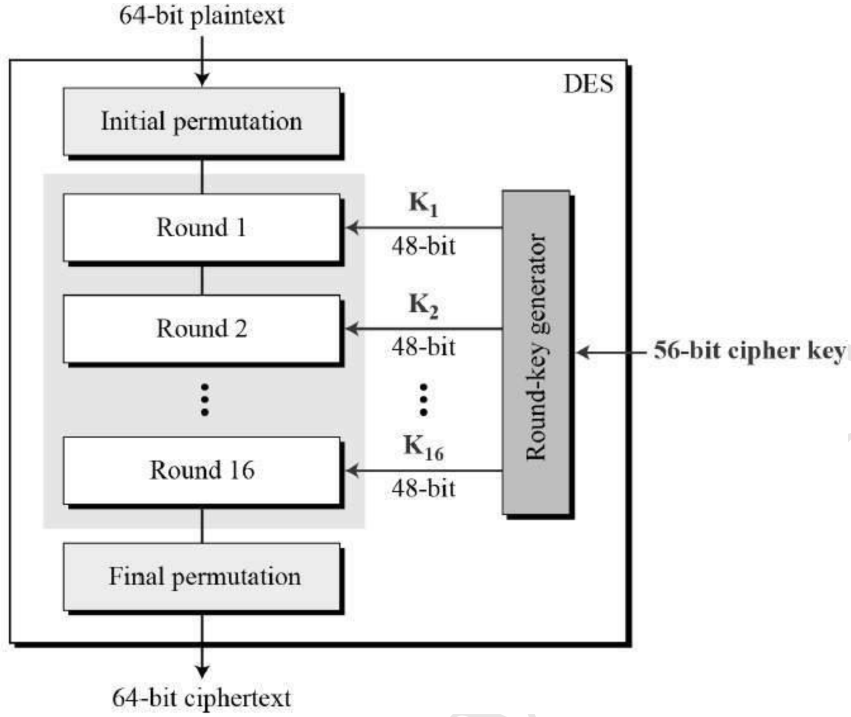
Or, state the DES process with diagram.

Or, describe symmetric-key cryptographic algorithm with example.

Data Encryption Standard: DES encryption method was first proposed by IBM in 1975 and standardized in 1977. DES works by using the same key to encrypt and decrypt a message, so both the sender and the receiver must know and use the same private key.

The Data Encryption Standard is a block cipher, meaning a cryptographic key and algorithm are applied to a block of data simultaneously rather than one bit at a time.

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. DES uses a 64-bit key, but eight of those bits are used for parity checks, effectively limiting the key to 56-bits. General structure of DES is depicted in the following illustration-



Since DES is based on the Feistel Cipher, all that is required to specify DES is:

- Round function
- Key schedule
- Any additional processing − Initial and final permutation.

DES transforms blocks of 64 bits corresponding to binary encoding of ASCII characters of message text. The algorithm uses exclusive OR operation defined by:

$A\oplus B = A\ .\ \overline{B} + B\ .\ \overline{A}$; where $\oplus$ is the exclusive OR operator.

With faster computers DES key can be broken by exhaustive search. It is not secure and has been replaced by Triple DES which uses DES algorithm thrice with three different 56-bit keys. 3 DES is quite secure.

DES algorithm step: DES takes 64-bit plain text and turns it into a 64-bit cipher text. The algorithm process breaks down into the following steps:

1) The process begins with the 64-bit plain text block getting handed over to an initial permutation (IP) function.
2) The initial permutation (IP) is then performed on the plain text.
3) Next, the initial permutation (IP) creates two halves of the permuted block, referred to as Left Plain Text (LPT) and Right Plain Text (RPT).
4) Each LPT and RPT goes through 16 rounds of the encryption process.
5) Finally, the LPT and RPT are rejoined, and a Final Permutation (FP) is performed on the newly combined block.

6) The result of this process produces the desired 64-bit cipher text.

The encryption process step (step 4) is further broken down into five stages:

1) Key transformation
2) Expansion permutation
3) S-Box permutation
4) P-Box permutation
5) XOR and swap.

For decryption, we use the same algorithm, and we reverse the order of the 16 round keys.

20. Why is the middle portion of 3 DES in a decryption rather than an encryption? Discuss the strength of DES algorithm.

Or, what is the strength of Data encryption standard (DES).

Triple DES/3 DES: Triple DES is an encryption technique which uses three instance of DES on same plain text. It uses their different types of key choosing technique in first all used keys are different and in second two keys are same and one is different and in third all keys are same.

The middle portion of 3 DES in a decryption rather than an encryption because:

- There is no cryptographic significance to the use of decryption for the second stage. Its only advantage is that it allows users of 3DES to decrypt data encrypted by users of the older single DES by repeating the key.
- The encryption algorithm is: cipher text = EK3(DK2(EK1(plaintext)))
  Decryption requires that the keys be applied in reverse order:
  P=Dk1[Ek1[P]]
  This results in a dramatic increase in cryptographic strength. The use of DES results in a mapping that is not equivalent to a single DES encryption.

The strength of DES algorithm:

There are mainly two categories of concerns about the strength of Data encryption standard. They are:

1) Concerns about the particular algorithm used: the algorithm used addresses the possibility of cryptanalysis by making use of the DES algorithm characteristics.
2) Concerns about the usage of key of size 56-bit: A more severe concern is about the length of secret key used. There can be 2^{56} possible keys with a key length of 56 bits. Thus, a brute force attack appears to be impractical.

21. Difference between Data Encryption Standard (DES) and Advanced Encryption Standard (AES).

AES and DES are both examples of symmetric block ciphers but have certain dissimilarities.

DES	AES
DES stands for Data Encryption Standard.	AES stands for Advanced Encryption Standard.
DES was designed by IBM in 1976.	AES was designed by Vincent Rijmen and Joan Daemen in 1999.
The design rational for AES is closed.	The design rational for AES is open.
The structure is based in feistal network.	The structure is based on substitution-permutation network.
The selection process for this is secret.	The selection process for this is secret but accepted open public comment.
DES can encrypt 64 bits of plaintext.	AES can encrypt 128 bits of plaintext.
Key length is 56 bits in DES.	Key length can be of 128-bits, 192-bits and 256-bits.
DES involves 16 rounds of identical operations.	Number of rounds depends on key length : 10(128-bits), 12(192-bits) or 14(256-bits).

The rounds in DES are : Expansion, XOR operation with round key, Substitution and Permutation.	The rounds in AES are : Byte Substitution, Shift Row, Mix Column and Key Addition.
DES cipher is derived from Lucifer cipher.	AES cipher is derived from square cipher.

22.What is the difference between the AES decryption algorithm and the equivalent inverse cipher?

The difference between the AES decryption algorithm and the equivalent inverse cipher given below:

AES decryption algorithm	Equivalent inverse cipher
The DES decryption cipher is not identical to the encryption cipher, so the sequence of transformation for decryption differs for encryption.	An equivalent version of the decryption algorithm that has the same structure as the encryption algorithm.
AES decryption algorithm use same round keys as the encryption algorithm, but applies transformation procedures in a different sequence.	Equivalent decryption algorithms have the same sequence of applying transformation procedures as the encryption algorithm, but uses modified round keys.
In AES decryption we use inverse shift rows, inverse sub bytes, inverse mix columns.	In equivalent cipher e interchange inverse shift rows and inverse sub bytes.

23. What was the final set of criteria used by NIST to evaluate candidate AES cipher?

The final set of criteria used by NIST to evaluate candidate AES cipher are:

- **General security:** to access general security, NIST replied on the public security analysis conducted by the cryptographic community.

- **Software implementations:** the principle concerns in this category are execution speed, performance across a variety of platforms and variation of speed with key size.
- **Hardware implementations:** like software, hardware implementation can be optimized for speed or size. However, in the case of h/w, size translate much more directly into cost than is usually the case for s/w implementations.
- **Attacks on implementations:** the criteria of general security, discuss in the first bullet is concerned with cryptanalytic attacks that exploit mathematical properties of the algorithm.
- **Encryption vs decryption:** this criterion deals with several issues related to considerations of both encryption and decryption.
- **Key agility:** refers to the ability to change key quickly with a minimum resource.
- Potential for instruction-level parallelism.
- Other versatility and flexibility.

24) What is feistel cipher? How it works in a cryptography algorithm?

Or, Describe the operation of Feistel cipher.

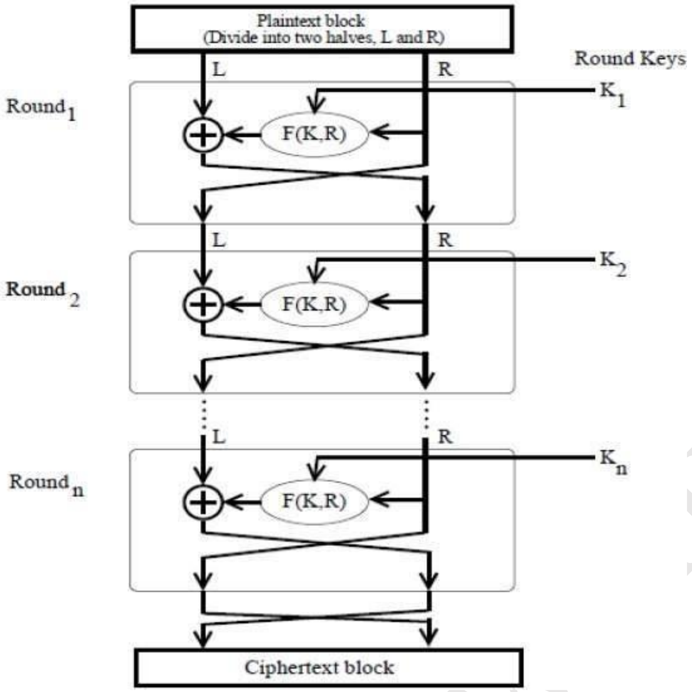
Or, a feistel cipher is used in the DES algorithm. Describe a feistel cipher.

Feistel cipher: The Feistel Cipher is a structure used to create block ciphers.

Or, in cryptography, a Feistel cipher is a symmetric structure used in the construction of block ciphers. It's also known as Luby–Rackoff block cipher. In a Feistel cipher, encryption and decryption are very similar operations, and both consist of iteratively running a function called a "round function" a fixed number of times. DES is just one example of a Feistel Cipher.

The operation of Feistel cipher: The complete process of feistel cipher is explained as follows:

Encryption process: The encryption process uses the Feistel structure consisting multiple rounds of processing of the plaintext, each round consisting of a "substitution" step followed by a permutation step. Feistel Structure is shown in the following illustration −



- The input block to each round is divided into two halves that can be denoted as L and R for the left half and the right half.
- In each round, the right half of the block, R, goes through unchanged. But the left half, L, goes through an operation that depends on R and the encryption key. First, we apply an encrypting function ‘f’ that takes two input − the key K and R. The function produces the output f (R, K). Then, we XOR the output of the mathematical function with L.
- In real implementation of the Feistel Cipher, such as DES, instead of using the whole encryption key during each round, a round-dependent key (a sub-key) is derived from the encryption key. This means that each round uses a different key, although all these sub-keys are related to the original key.
- The permutation step at the end of each round swaps the modified L and unmodified R. Therefore, the L for the next round would be R of the current round. And R for the next round be the output L of the current round.
- Above substitution and permutation steps form a ‘round’. The number of rounds are specified by the algorithm design.
- Once the last round is completed then the two sub blocks, ‘R’ and ‘L’ are concatenated in this order to form the cipher text block.

The difficult part of this algorithm is designing the round function because it must be applied in every round until the final cipher text is received. The more the number of rounds, the more secure the data becomes.

Decryption process: The decryption process of Feistel Cipher is almost the same as the encryption process. Just like we entered the plain text in the Feistel block, we have to do the same with the cipher text. The cipher text will be divided into two parts just like the plain text. The only difference is that the keys will be used in reverse order.

Number of rounds: The number of rounds depends upon how much security you want. Security is directly proportional to the number of rounds. But simultaneously it slows down the speed of encryption and decryption. The larger the number of rounds is, the creation of cipher text from plain text and plain text from cipher text will be slow.

25. What is message authentication? Define the classes of message authentication function.

Message authentication: Message authentication is a mechanism or service used to verify the integrity of a message.

Or, in information security, message authentication or data origin authentication is a property that a message has not been modified while in transit and that the receiving party can verify the source of the message.

Message authentication assures that data received is exactly same as sent by the transmitter (i.e. contains no modification, insertion, detection or replay).

Classes of message authentication function: This section is concerned with the types of functions that may be used to produce an authenticator. These may be grouped into three classes:

- Hash function: A function that maps a message of any length into a fixed-length hash value, which serves as the authenticator.
- Message encryption: The cipher text of the entire message serves as its authenticator.
- Message authentication code: A function of the message and a secret key that produces a fixed-length value that serves as the authenticator.

26. What do you mean by digital signature? What are properties a digital signature should have?

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

Or, a digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document.

Or, digital signature is a type of electronic signature that encrypts documents with digital codes that are particularly difficult to duplicate.

Properties a digital signature: To be valid, digital signatures require properties:

- Authenticity: a valid signature implies that the signer deliberately signed the associated message. The active participation of the signer in the transaction must be ensured. This active participation can rely on two elements:
    - The presence of the smart card owned by the signer
    - The validation of a secret code known only by the signer (PIN code or password).
- Unforgeability: only the signer can give a valid signature for the associated message.
- Non-re-usability: the signature of a document cannot be used on another document.
- Non-repudiation: the signer cannot deny having signed a document that has valid signature. This property relies on the security of the whole system: if there is any way to attack the system a signer can repudiate a signature arguing that the system is not secure.
- Integrity: ensure the contents have not been modified.

27. Briefly explain Diffie-Hellman key exchange.

Diffie-Hellman key exchange: There is another public key algorithm called Diffie-Hellman key exchange algorithm. It’s developed by the original proposers of the public key encryption idea.

Diffie-Hellman key exchange algorithm is a method for securely exchanging cryptographic keys over a public communications channel.

The main advantage of this method compared to RSA is that it uses a symmetric key employing public key exchanged between sender and receiver.

The steps of the algorithm are:

Step 1: Two numbers are selected. We will call them q and a. q is a prime number. a<q is a primitive root of q. a is a primitive root of q if the following is true:

a mod q, a^2 mod q, a^3 mod q, …., a^{q-1} mod q are distinct and are numbers 1 to q-1 in some permutation.

Step 2: The sender selects a random number XS<q which is private to him. The sender calculates his public key YS = a^{XS} mod q.

Step 3: The receiver selects a random number XR<q. XR is private to him. The receiver calculates his public key YR = a^{XR} mod q.

Step 4: The sender and receiver exchange their public keys.

Step 5: S generates secret key, K= $(YR)^{XS}$ mod q.

Step 6: R generates secret key, K= $(YS)^{XR}$ mod q.

It can be seen that, K= $(YR)^{XS}$ mod q= $(a^{XR})^{XS}$ mod q

= $(YS)^{XR}$ mod q= $(a^{XS})^{XR}$ mod q.

Example:

Step 1: Alice and Bob get public numbers q = 23, a = 9

Step 2: Alice selected a private key XS = 4 and

Bob selected a private key XR = 3

Step 3: Alice and Bob compute public values

Alice: YS = (9^4 mod 23) = (6561 mod 23) = 6

Bob: YR = (9^3 mod 23) = (729 mod 23) = 16

Step 4: Alice and Bob exchange public numbers

Step 5: Alice receives public key YR =16 and

Bob receives public key YS = 6

Step 6: Alice and Bob compute symmetric keys

Alice: $K = (YR)^{XS} \bmod 23 = 16^4 \bmod 23 = 9$

Bob: $K = (YS)^{XR} \bmod 23 = 6^3 \bmod 23 = 9$

The common secret key is 9.

28. What are the differences between weak and strong collision resistance?

The differences between weak and strong collision resistance given below:

Weak collision	Strong collision
Weak collision resistance means that the probability of failure in find collision is not negligible.	Strong collision resistance means that the probability of success in finding collision is negligible.
Weak collision resistance, or second preimage resistance, is the property that given x and h (x) (h a bash function) it's difficult to find x' ≠ x such that h (x') = h (x).	Strong collision resistance, or just collision resistance, is the property that it's difficult to find any two x, x' with the same hash value.
Weak collision resistance is bound to a particular input.	Strong collision resistance applies to any two arbitrary inputs.
It is less difficult to achieve weak collision resistance compared to strong collision resistance..	It is more difficult to achieve strong collision resistance than weak collision resistance.
Weak collision resistance does not imply collision resistance.	Strong collision resistance implies weak collision resistance.

29. What is MIME? List the limitations of SMTP/RFC 822.

MIME: MIME stands for Multipurpose Internet Mail Extension. MIME is a kind of add on or a supplementary protocol which allows non-ASCII data to be sent through SMTP. It allows the users to exchange different kinds of data files on the Internet: audio, video, images, application programs as well.

SMTP is a push protocol and is used to send the mail whereas POP (post office protocol) or IMAP (internet message access protocol) are used to retrieve those mails at the receiver’s side.

RFC 822 specification defines an electronic message format consisting of header fields and an optional message body. The header fields contain information about the message, such as the sender, the recipient, and the subject.

Limitations of SMTP/RFC 822 given below:

- Cannot transmit executable or binary files without conversion into text through non-standard programs.
- It cannot transmit text data containing national language characters.
- Cannot transmit diacritical marks.
- Transfers limited in size.
- Has a problem with lines longer than a certain length (72 to 254 Characters)
- Gateways do not always map properly between EBCDIC and ASCII.
- Cannot handle non-text data in X.400 message.
- Some SMTP implementations do not adhere completely to the SMTP network standards defined in RFC821.

30. Define PGP. Why E-mail compatibility function in PGP needed?

PGP: PGP stands for Pretty Good Privacy. PGP is a cryptographic method that lets people communicate privately online.

Or, PGP is an open source software package that is designed for the purpose of email security. It provides the basic or fundamental needs of cryptography.

E-mail compatibility function in PGP:

Electronic mail systems only permit the use of blocks consisting of ASCII text. To accommodate this restriction PGP provides the service converting the row 8-bit binary stream to a stream of printable ASCII characters. The scheme used for this purpose is Radix -64 conversion.

31. Define Kerberos. Briefly explain Kerberos v4.

Or, explain the authentication service provided by Kerberos.

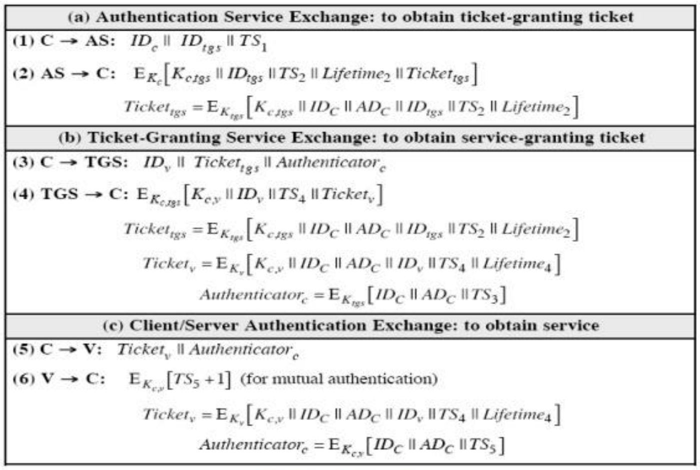
Kerberos: Kerberos is a network protocol that uses secret-key cryptography to authenticate client-server applications.

Or, Kerberos is a network authentication protocol that allows users to securely access services over a physically insecure network. It builds on symmetric key cryptography and require a trusted third party known as the Key Distribution Center (KDC). MIT developed Kerberos to protect network services provided by project Athena.

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 user’s information while logging into the system by DES technique for encryption. It was launched in late 1980s.

The actual Kerberos protocol version 4 is as follows:

- A basic third-party authentication scheme
- Have an Authentication Server (AS).
    - users initially negotiate with AS to identify self
    - AS provides a non-corruptible authentication credential (ticket granting ticket TGT).
- have a Ticket Granting server (TGS).
    - users subsequently request access to other services from TGS on basis of users TGT.



(a) Authentication Service Exchange: to obtain ticket-granting ticket

(1) C → AS: $ID_c \parallel ID_{tgs} \parallel TS_1$

(2) AS → C: $\mathrm{E}_{K_c}\left[K_{c,tgs} \parallel ID_{tgs} \parallel TS_2 \parallel Lifetime_2 \parallel Ticket_{tgs}\right]$

$$Ticket_{tgs} = \mathrm{E}_{K_{tgs}}\left[K_{c,tgs} \parallel ID_C \parallel AD_C \parallel ID_{tgs} \parallel TS_2 \parallel Lifetime_2\right]$$

(b) Ticket-Granting Service Exchange: to obtain service-granting ticket

(3) C → TGS: $ID_v \parallel Ticket_{tgs} \parallel Authenticator_c$

(4) TGS → C: $\mathrm{E}_{K_{c,tgs}}\left[K_{c,v} \parallel ID_v \parallel TS_4 \parallel Ticket_v\right]$

$$Ticket_{tgs} = \mathrm{E}_{K_{tgs}}\left[K_{c,tgs} \parallel ID_C \parallel AD_C \parallel ID_{tgs} \parallel TS_2 \parallel Lifetime_2\right]$$

$$Ticket_v = \mathrm{E}_{K_v}\left[K_{c,v} \parallel ID_C \parallel AD_C \parallel ID_v \parallel TS_4 \parallel Lifetime_4\right]$$

$$Authenticator_c = \mathrm{E}_{K_{tgs}}\left[ID_C \parallel AD_C \parallel TS_3\right]$$

(c) Client/Server Authentication Exchange: to obtain service

(5) C → V: $Ticket_v \parallel Authenticator_c$

(6) V → C: $\mathrm{E}_{K_{c,v}}\left[TS_5 + 1\right]$ (for mutual authentication)

$$Ticket_v = \mathrm{E}_{K_v}\left[K_{c,v} \parallel ID_C \parallel AD_C \parallel ID_v \parallel TS_4 \parallel Lifetime_4\right]$$

$$Authenticator_c = \mathrm{E}_{K_{c,v}}\left[ID_C \parallel AD_C \parallel TS_5\right]$$

Kerberos 4 Overview

Implementation of Kerberos Authentication with NFS:

- The /usr/sbin/kerbd daemon must be running on the NFS client and server.
    - This daemon is normally started when needed by inetd.
- The system administrator sets up the NFS server to use Kerberos authentication.
- The user mounts the shared file system.
- The user logs in to the Kerberos service, using the kinit command.
- The user accesses the mounted directory.
- The user destroys the tickets at the end of the session to prevent them from being compromised.
- If tickets have been destroyed before the session has finished, the user must request a new ticket with the kinit command.

32. Briefly discuss how attacks on password are broadly classified?

Password attack: A password attack is any means by which a hacker attempts to obtain a user’s login information. The approach doesn’t have to be sophisticated.

Attacks on password are broadly classified: Attacks on password are broadly classified in below:

- Brute force attack:
    - The most common forms of password attack methods, and the easiest for hackers to perform.
    - Inexperienced hackers favor this method precisely.

    - Hacker uses a computer program to login to a user’s account with all possible password combinations.
    - Don’t start at random; hacker start with the easiest-to-guess passwords.
- Dictionary attack:
    - Allows hackers to employ a program which cycles through common words.
    - Dictionary attacks rely on a few key factors of users’ psychology.
    - Brute force attack goes letter by letter, whereas a dictionary attack only tries possibilities most likely to succeed.
- Rainbow table attack:
    - Rainbow table compiles a list of pre-computed hashes.
    - Using compilations of hash values for known algorithms, hackers are able to systematically work.
    - This requires a significant amount of computing power and isn’t guaranteed to succeed in cracking hashed passwords.
- Credential stuffing:
    - Hackers use lists of stolen usernames and passwords in combination on various accounts.
    - Hackers share stolen passwords on the Dark Web or sell them.
    - Hackers may attempt to use previously stolen credentials to obtain access to users’ accounts on other platforms.
    - Proves incredibly effective because it uses known passwords.
- Social engineering:
    - Attacks use the social conventions of the workplace to fool users.
    - Allows hackers to learn information about users.
    - Hackers can always just guess with the information they find online.
    - Hackers may also try offline techniques, such as making phone calls and posing as someone from the IT department asking for password information to help fix a technical problem.
- Password spraying:
    - Password spraying attacks involve using common passwords to attempt logins across numerous accounts.
    - Allows hackers to work around the account lockouts normally triggered after repeated failed logins.
    - Hackers can obtain more widespread access to networks and compromise or steal a greater amount of data.
- Key-logger attack:
    - Install a program on users’ endpoints to track all of a users’ keystrokes.

- As the user types in their usernames and passwords, the hackers record them for use later.
- It must first infect the users’ endpoints.

33. What is firewall and what are its limitations? Why corporate house implement more than one firewall for security?

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.

Or, a firewall is a crucial component of securing your network and is designed to address the issues of data integrity or traffic authentication and confidentiality of your internal network.

Limitations of firewall: Firewalls do have the following limitations:

- A firewall cannot prevent users or attackers with modems from dialing in to or out of the internal network, thus bypassing the firewall and its protection completely.
- Firewalls cannot enforce our password policy or prevent misuse of passwords. Our password policy is crucial in this area because it outlines acceptable conduct and sets the ramifications of noncompliance.
- Firewalls are ineffective against non-technical security risks such as social engineering.
- Firewalls cannot stop internal users from accessing websites with malicious code, making user education critical.
- Firewalls cannot protect us from poor decisions.
- Firewalls cannot protect us when our security policy is too lax.

Corporate house implement more than one firewall for security because:

In a topology with a single firewall serving both internal and external users (LAN and WAN), it acts as a shared resource for these two zones. Due to limited computing power, a denial of service attack on the firewall from WAN can disrupt services on the LAN.

In a topology with two firewalls, you protect internal services on the LAN from denial of service attacks on the perimeter firewall.

And for this corporate houses implement more than one firewall for security.

Of course, having two firewalls will also increase administrative complexity - you need to maintain two different firewall policies + backup and patching.

34. Describe MD-5 algorithm in detail. Compare its performance with SHA-1.

MD-5/Message Digest algorithm-5: MD5 is uses to create a message digest for digital signatures.

Or, MD5 is a message authentication protocol to verify the content of the message.

Or, in cryptography, MD5 is a widely used cryptographic hash function with a 128-bit hash value.

MD5 algorithm works as: This encryption of input of any size into hash values undergoes 5 steps and each step has its a predefined task.

- Step1: Append Padding Bits
  - Padding means adding extra bits to the original message. So in MD5 original message is padded such that its length in bits is congruent to 448 modulo 512. Padding is done such that the total bits are 64 less being a multiple of 512 bits' length.
  - Padding is done even if the length of the original message is already congruent to 448 modulo 512. In padding bits, the only first bit is 1 and the rest of the bits are 0.
- Step 2: Append Length
  - After padding, 64 bits are inserted at the end which is used to record the length of the original input. Modulo 2^64. At this point, the resulting message has a length multiple of 512 bits.
- Step 3: Initialize MD buffer
  - A four-word buffer (A, B, C, D) is used to compute the values for the message digest. Here each of A, B, C, D is a 32-bit register. These registers are initialized to the following values in hexadecimal:

word A: 01 23 45 67
word B: 89 ab cd ef
word C: fe dc ba 98
word D: 76 54 32 10

- Step 4: Processing message in 16-word block
    - MD5 uses the auxiliary functions which take the input as three 32-bit number and produces a 32-bit output. These functions use logical operators like OR, XOR, NOR.

$$
\begin{aligned}
F(X,Y,Z) &= (X \wedge Y) \vee (\neg X \wedge Z) \\
G(X,Y,Z) &= (X \wedge Y) \vee (Y \wedge \neg Z) \\
H(X,Y,Z) &= X \oplus Y \oplus Z \\
I(X,Y,Z) &= Y \oplus (X \vee \neg Z)
\end{aligned}
$$

The content of four buffers are mixed with the input using this auxiliary buffer and 16 rounds are performed using 16 basic operations.

Performance:

- MD5 codes any stream of bytes into a 128-bit value while SHA1 codes any stream of bytes into a 160-bit value. Therefore, the SHA1 will provide more security compared to MD5.
- MD5 is broken, one can generate a collision, so MD5 should not be used for any security applications. SHA1 is not known to be broken and is believed to be secure, other than that. So, MD5 is faster but has 128-bit output, while SHA1 has 160-bit output.

35. Draw an analogy between MD5 and SHA algorithm.

Or, Compare between MD5 and SHA algorithm.

Both MD5 stands for Message Digest and SHA1 stands for Secure Hash Algorithm square measure the hashing algorithms wherever The speed of MD5 is fast in comparison of SHA1's speed.

Let's see the difference between MD5 and SHA1 which are given below:

MD5	SHA/SHA1
MD5 stands for Message Digest. It was presented in the year 1992.	SHA stands for Secure Hash Algorithm. It was presented in the year 1995.
MD5 can have 128 bits length of message digest.	SHA can have 160 bits length of message digest.

The speed of MD5 is fast in comparison of SHA's speed.	The speed of SHA is slow in comparison of MD5's speed.
To make out the initial message the aggressor would want 2^{128} operations whereas exploitation the MD5 algorithmic program.	In SHA it'll be 2^{160} that makes it quite troublesome to seek out.
MD5 is simple than SHA1.	SHA1 is more complex than MD5.
MD5 provides indigent or poor security.	it provides balanced or tolerable security.
In MD5, if the assailant needs to seek out the 2 messages having identical message digest then assailant would need to perform 2^{64} operations.	in SHA1, assailant would need to perform 2^{80} operations which is greater than MD5.

36. What is the purpose of X.509 standard? Explain the IPsec architecture.

X.509: An X.509 certificate is a digital certificate that uses the widely accepted international X.509 public key infrastructure.

Or, X.509 is a standard defining the format of public-key certificates. X.509 certificates are used in many Internet protocols, including TLS/SSL, which is the basis for HTTPS, the secure protocol for browsing the web.

Purpose of X.509 standard: The X.509 is part of the X.500 series that defines a directory service. The directory is in effect, a server or distributed set of servers that maintain a database of information about users. The X.509 defines the framework for the provision of authentication services by the X.500 directory to its users, and it may serve as a repository of public-key certificates. Additionally, the X.509 defines alternative authentication protocols based on the use of public-key certificates.

IPsec Architecture: The IP security architecture uses the concept of a security association as the basis for building security functions into IP.

IPsec 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:

- Confidentiality
- Authentication
- Integrity

IPsec architecture illustrate in below:

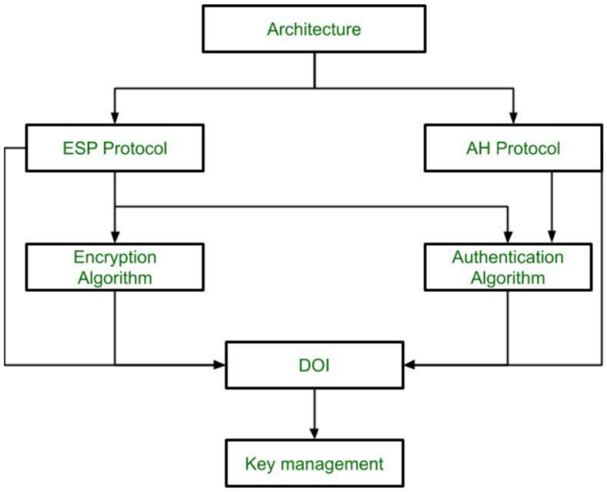


Fig: IPsec architecture

- **Architecture:**
  Architecture or IP Security Architecture covers the general concepts, definitions, protocols, algorithms and security requirements of IP Security technology.
- **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.
- **Encryption algorithm:**
  Encryption algorithm is the document that describes various encryption algorithm used for Encapsulation Security Payload.
- **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 algorithm:**
  Authentication Algorithm contains the set of the documents that describe authentication algorithm used for AH and for the authentication option of ESP.
- **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.
- **Key management:**
  Key Management contains the document that describes how the keys are exchanged between sender and receiver.

37. Give the applications & benefits of IP security.

IP security: The IP security is an Internet Engineering Task Force (IETF) standard suite of protocols between two communication points across the IP network that provide data authentication, integrity, and confidentiality.

Applications of IPsec: IPsec can be applied to do the following things:

- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.
- 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.
- To secure remote access over the internet.
- To establish extranet and intranet connectivity with partners.
- To enhance electronic commerce security.

Benefits of IPsec:

- Provides strong security whose application is to all traffic crossing this perimeter.
- There is no need to change software on a user or server system when IPsec is implemented in the firewall or router.
- No need to train users on security mechanisms, issue keying material on a per-user basis.

- Useful for offsite workers and also for setting up a secure virtual subnetwork.
- Reduced key negotiation overhead and simplified maintenance by supporting the IKE protocol.
- Can provide security for individual users if needed.
- Can be transparent to end users
- Good compatibility.

38. State and explain man-in-the middle attack.

Man-in-the middle attack: Man-in-the-middle cyberattacks allow attackers to secretly intercept communications or alter them.

In cryptography and computer security, a man-in-the-middle, monster-in-the-middle, or machine-in-the-middle, or monkey-in-the-middle (MITM) or person-in-the-middle (PITM) attack is a cyberattack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other.

MITM attack progression: Successful MITM execution has two distinct phases:

- **Interception:** The first step intercepts user traffic through the attacker's network before it reaches its intended destination. The most common way of doing this is a passive attack in which an attacker makes free, malicious Wi-Fi hotspots available to the public. Attackers wishing to take a more active approach to interception may launch one of the following attacks:
  - **IP spoofing** involves an attacker disguising himself as an application by altering packet headers in an IP address. As a result, users attempting to access a URL connected to the application are sent to the attacker's website.
  - **ARP spoofing** is the process of linking an attacker's MAC address with the IP address of a legitimate user on a local area network using fake ARP messages. As a result, data sent by the user to the host IP address is instead transmitted to the attacker.
  - **DNS spoofing** also known as DNS cache poisoning, involves infiltrating a DNS server and altering a website's address record. As a result, users attempting to access the site are sent by the altered DNS record to the attacker's site.

- **Decryption:** After interception, any two-way SSL traffic needs to be decrypted without alerting the user or application. A number of methods exist to achieve this:
    - **HTTPS spoofing** sends a phony certificate to the victim's browser once the initial connection request to a secure site is made. It holds a digital thumbprint associated with the compromised application, which the browser verifies according to an existing list of trusted sites. The attacker is then able to access any data entered by the victim before it's passed to the application.
    - **SSL BEAST** (browser exploit against SSL/TLS) targets a TLS version 1.0 vulnerability in SSL. Here, the victim's computer is infected with malicious JavaScript that intercepts encrypted cookies sent by a web application. Then the app's cipher block chaining (CBC) is compromised so as to decrypt its cookies and authentication tokens.
    - **SSL hijacking** occurs when an attacker passes forged authentication keys to both the user and application during a TCP handshake. This sets up what appears to be a secure connection when, in fact, the man in the middle controls the entire session.
    - **SSL stripping** downgrades a HTTPS connection to HTTP by intercepting the TLS authentication sent from the application to the user. The attacker sends an unencrypted version of the application's site to the user while maintaining the secured session with the application. Meanwhile, the user's entire session is visible to the attacker.

Man in the middle attack prevention: Blocking MITM attacks requires several practical steps on the part of users, as well as a combination of encryption and verification methods for applications.

- Avoiding Wi-Fi connections that aren't password protected.
- Paying attention to browser notifications reporting a website as being unsecured.
- Immediately logging out of a secure application when it's not in use.
- Not using public networks (e.g., coffee shops, hotels) when conducting sensitive transactions.

39. Define a worm? Diagrammatically illustrate a digital immune system.

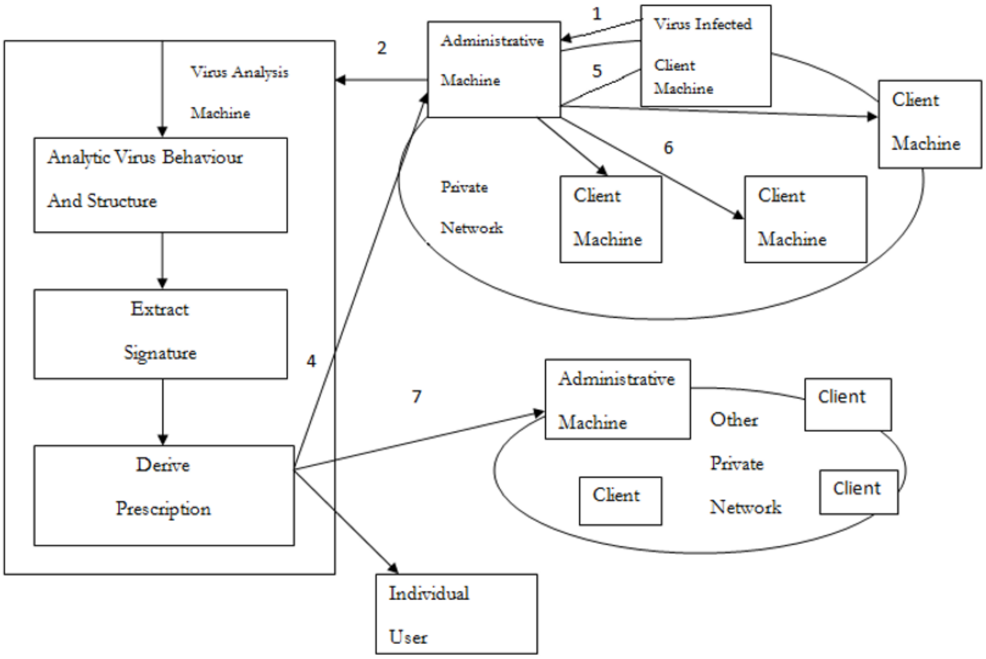
Worm: A computer worm is a type of virus that replicates itself, but does not alter any files on our machine.

If a worm consumes our memory, our computer will run very slowly and possibly even crash. If the worm affects our hard disk space, our computer will take a long time to access files and we will not be able to save or create new files until the worm has been eradicated. Worms are hard to detect because they are typically invisible files. They often go unnoticed until your computer begins to slow down or starts having other problems.

Digital immune system (DIS): The Digital Immune system is a comprehensive approach to virus protection developed by IBM. The Digital Immune System:

- Detects a high percentage of new or unknown threats at the desktop, server, and gateway.
- Makes the full system highly scalable.
- Provide high-speed analysis capabilities.
- Reduces instances of false positives.
- Provides real-time status updates on all submissions.

Illustrate digital immune system in below:



Simplification

40. User A & B exchanges the key using Diffie-Hellman algorithm. Assume a=5, q=11, X_A=2, X_B=3. Find the value of Y_A, Y_B, K.

Solution:

$Y_A = \alpha^{XA} \bmod q$

$= 5^2 \bmod 11$

$= 25 \bmod 11$

$= 3$

$Y_B = \alpha^{XB} \bmod q$

$= 5^3 \bmod 11$

$= 125 \bmod 11$

$= 4$

$K_A = (Y_A)^{XB} \bmod q$

$= 3^3 \bmod 11$

$= 27 \bmod 11$

$= 5$

$K_B = (Y_B)^{XA} \bmod q$

$= 4^2 \bmod 11$

$= 16 \bmod 11$

$=5$

41. Users A & B use the Diffie-Hellman key exchange technique with a common prime q=71 and a primitive root α =7

(i) If user A has private key X_A= 5, what is the A's public key Y_A?

(ii) If user B has private key X_B= 12 what is the B's public key Y_B?

(iii) What is the shared secret key?

Solution:

i) $Y_A = \alpha^{XA} \bmod q$

$= 7^5 \bmod 71$

$= 16807 \bmod 71$

$= 51$

ii) $Y_B = \alpha^{XB} \bmod q$

$= 7^{12} \bmod 71$

$= 4$

iii) $K_A = (Y_A)^{XB} \bmod q$

$= 51^{12} \bmod 71$

$= 30$

$K_B = (Y_B)^{XA} \bmod q$

$= 4^5 \bmod 71$

$= 1024 \bmod 71$

$= 30$

Short notes

i)

S/MIME: It stands for Secure/Multipurpose Internet Mail Extensions.

S/MIME is a protocol for the secure exchange of e-mail and attached documents originally developed by RSA Security.

In this, public key cryptography is used for digital sign, encrypt or decrypt the email. User acquires a public-private key pair with a trusted authority and then makes appropriate use of those keys with email applications. S/MIME provides the following cryptographic security services for electronic messaging applications:

- Authentication
- Message integrity
- Non-repudiation of origin (using digital signatures)
- Privacy
- Data security (using encryption).

Working principle:

- The body portion of an SMTP message is structured and formatted.
- Uses the RSA public key cryptography algorithm along with the DES encryption algorithm.
- The MIME body section consists of a message in PKCS #7 format that contains an encrypted form of the MIME body parts.
- The MIME content type for the encrypted data is application/pkcs7-mime.

S/MIME is gaining in popularity in the enterprise because its key management facilities are implemented as a hierarchical public key infrastructure (PKI) scheme.

ii)

E-mail security: Email security refers to the collective measures used to secure the access and content of an email account or service

Or, Email security is a term for describing different procedures and techniques for protecting email accounts, content, and communication against unauthorized access, loss or compromise. Email is often used to spread malware, spam and phishing attacks.

Email Security Features: Email security services provide various types of email security solutions. Some of the principal email security features are as follows:

- Spam Filters
- Anti-virus Protection
- Image & Content Control
- Data Encryption.

Email security services: Growing use of e-mail communication for important and crucial transactions demands provision of certain fundamental security services as the following –

- Confidentiality: E-mail message should not be read by anyone but the intended recipient.
- Authentication: E-mail recipient can be sure of the identity of the sender.
- Integrity: Assurance to the recipient that the e-mail message has not been altered since it was transmitted by the sender.
- Non-repudiation: E-mail recipient is able to prove to a third party that the sender really did send the message.
- Proof of submission: E-mail sender gets the confirmation that the message is handed to the mail delivery system.
- Proof of delivery: Sender gets a confirmation that the recipient received the message.

Prevention of email security: From an individual/end user standpoint, proactive email security measures include:

- Strong passwords
- Password rotations
- Spam filters
- Desktop-based anti-virus/anti-spam applications
- Anti-Phishing
- Data Loss Prevention
- Account Takeover Prevention.

iii)

Encapsulating Security Payload (ESP): ESP provides confidentiality, data integrity, encryption, authentication and anti-replay.

Or, An ESP is a protocol within the IPsec for providing authentication, integrity and confidentially of network packets data/payload in IPv4 and IPv6 networks.

ESP is implemented in either two ways:

- ESP with optional Authentication.
- ESP with Authentication.

Process of ESP: One can apply ESP in two ways-

- **Transport mode:**
  - The ESP header follows the IP header of the original IP datagram.
  - If the datagram has an IPsec header, then the ESP header goes before it.
  - ESP trailer and the optional authentication data follow the payload.
  - Hosts use ESP in transport mode.
- **Tunnel mode:**
  - Creates a new IP header and uses it as the outermost IP header of the datagram.
  - If use both encryption and authentication, ESP completely protects the original datagram.
  - ESP trailer and the optional authentication data are appended payload.
  - Gateway must use ESP in tunnel mode.

The **ESP Header** is designed to provide several different services including the following:

- Confidentiality of datagrams through encryption
- Authentication of data origin through the use of public key encryption
- Anti-replay services through the same sequence number mechanism as provided by the Authentication Header
- Limited traffic flow confidentiality through the use of security gateways.

iv)

Steganography: The word Steganography is derived from two Greek words- ‘stegos’ meaning ‘to cover’ and ‘grayfia’, meaning ‘writing’, thus translating to ‘covered writing’, or ‘hidden writing’.

Steganography is a method of hiding secret data, by embedding it into an audio, video, image or text file.

Or, Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data.

Cryptography and steganography are both methods used to hide or protect secret data. However, they have many difference:

- Cryptography makes the data unreadable, or hides the meaning of the data, while steganography hides the existence of the data.
- In cryptography, people can read it, but won’t understand what it means. While steganography would hide the letter inside a pair of socks that would be gifting the intended recipient of the letter.
- In cryptography, if someone either knows or figures out your secret language, then our message can easily be read. But in steganography, the intended recipient knows what to look for, and finds the message hidden in them.

Steganography techniques: Different technique are used in steganography.

- Character marking.
- Invisible ink
- Pin punctures.
- Typewriter correction ribbon.

Advantages over cryptography:

- The primary advantage of using steganography is to hide data over encryption.
- It helps obscure the fact that there is sensitive data hidden in the file or other content.
- Helps to obscure the presence of the secure channel.

Steganography software: Some online steganography software tools include:

- Xiao Steganography, used to hide secret files in BMP images or WAV files.
- Image Steganography, a Java-script tool that hides images inside other image files.
- Crypture, a command line tool that is used to perform steganography.

v)

Elliptic curve cryptography (ECC): Elliptic curve cryptography is used to implement public key cryptography.

In 1985, cryptographic algorithms were proposed based on elliptic curves. An elliptic curve is the set of points that satisfy a specific mathematical equation.

Elliptic Curve Cryptography (ECC) is an approach to public-key cryptography, based on the algebraic structure of elliptic curves over finite fields. ECC requires a smaller key as compared to non-ECC cryptography to provide equivalent security.

For a better understanding of Elliptic Curve Cryptography, it is very important to understand the basics of Elliptic Curve. An elliptic curve is a planar algebraic curve defined by an equation of the form:

$$y^2 = x^3 + ax + b$$

Where ‘a’ is the co-efficient of x and ‘b’ is the constant of the equation.

The curve is non-singular; that is its graph has no cusps or self-intersections (when the characteristic of the Co-efficient field is equal to 2 or 3). Elliptic curves could intersect almost 3 points when a straight line is drawn intersecting the curve. The elliptic curve is symmetric about the x-axis; this property plays a key role in the algorithm.

Use of ECC:

- Websites make extensive use of ECC to secure customers’ hypertext transfer protocol connections.
- It is used for encryption by combining the key agreement with a symmetric encryption scheme.
- It is also used in several integer factorization algorithms like Lenstra elliptic-curve factorization.
- Time stamping uses an encryption model called a blind signature scheme. It is possible using Elliptic Curve Cryptography.

vi)

Feistel cipher: The Feistel Cipher is a structure used to create block ciphers.

Or, in cryptography, a Feistel cipher is a symmetric structure used in the construction of block ciphers. It’s also known as Luby–Rackoff block cipher. In a Feistel cipher, encryption and decryption are very similar operations, and both consist of iteratively running a function called a "round function" a fixed number of times. DES is just one example of a Feistel Cipher.

Feistel cipher algorithm:

- Create a list of all the Plain Text characters.
- Convert the Plain Text to ASCII and then 8-bit binary format.
- Divide the binary Plain Text string into two halves: left half (L1) and right half (R1)
- Generate a random binary keys (K1 and K2) of length equal to the half the length of the Plain Text for the two rounds.
- First Round of Encryption:

    a) Generate function f1 using R1 and K1 as follows:

    f1= XOR (R1, K1)

    b) Now the new left half(L2) and right half(R2) after round 1 are as follows:

    R2= XOR (f1, L1)
    L2=R1

- Second Round of Encryption:

    a) Generate function f2 using R2 and K2 as follows:

    f2= XOR (R2, K2)

    b) Now the new left half(L2) and right half(R2) after round 1 are as follows:

    R3= XOR (f2, L2)

    L3=R2

- Concatenation of R3 to L3 is the Cipher Text
- Same algorithm is used for decryption to retrieve the Plain Text from the Cipher Text.

Design features:

- Feistel cipher was based on the structure proposed by Shannon.
- Shannon structure has an alternate implementation of diffusion and confusion to obtain cipher text block.
- Feistel cipher structure has alternate application substitution and permutation on plain text block to obtain cipher text block.
- Feistel block cipher operates on each block independently.
- The encryption and decryption algorithm in Feistel cipher is the same.
- The key used for encryption and decryption is the same but the sequence of application of sub-key is reversed.

- During encryption a plain text block undergoes multiple rounds. But the function performed in each round is same.
- Generally, 16 rounds are performed in Feistel cipher.
- Typical block size of Feistel cipher is 64-bit but modern block cipher uses 128-bit block.
- Typical key size of Feistel cipher is 64-bit but modern block cipher has 128-bit key size.

vii)

X.509 Authentication Format: X.509 is a standard defining the format of public-key certificates. X.509 certificates are used in many Internet protocols, including TLS/SSL, which is the basis for HTTPS, the secure protocol for browsing the web.

Structure of X.509:

- **Version number:** This field defines the version of X.509 of the certificates. The version number started from at 0.
- **Serial number:** This field defines a number assigned to each certificate. The value is unique for each certificate issuer.
- **Signature algorithm ID:** This field identifies the algorithm used to sign the certificate. Any parameter that is needed for the signature is also defined in this field.
- **Issuer name:** This field identifies the certification authority that issued the certificate.
- **Validity period:** This field defines the earliest time and the latest time the certificate is valued.
- **Subject period:** This field defines the entity to which the public key belongs. It is also a hierarchy of strings.
- **Subject public key:** This field defines owner's key, the heart of the certificate.
- **Issuer unique identifier:** This optional field allows two issuers to have the same issuer field value if the issuer unique identifiers are different.
- **Subject unique identifier:** This optional field allow two different subjects to have the same subject field value, if the subject unique identifiers are different.
- **Extension:** This optional field allows issuer to add more private information to the certificate.
- **Signature:** This made of their sections. The first section contains all other field is in the certificate. The second section contains the digest of first section

and the third section contains the algorithm identifier used to create the second section.

Applications of X.509: Common applications of X.509 certificates include:

- SSL/TLS and HTTPS for authenticated and encrypted web browsing
- Signed and encrypted email via the S/MIME protocol
- Code signing
- Document signing
- Client authentication
- Government-issued electronic ID.

viii)

Public key infrastructure: PKI is a framework that enables the encryption of public keys and includes their affiliated crypto-mechanisms.

A PKI supports the distribution and identification of public encryption keys, enabling users and computers to both securely exchange data over networks such as the Internet and verify the identity of the other party.

PKI used for:

- Establishing the identity of endpoints on a network
- Encrypting the flow of data via the network's communication channels.

PKI is applied:

- Secure Browsing (via SSL/TLS)
- Securing Email (signing and encrypting messages)
- Secure Code-signing
- Network Security
- File Security (via Encrypted File Systems).

The Components of an Ideal PKI:

- Public and Private Keys
- Public Key Certificates
- Certificate Repository
- Certificate Authority (CA)
- Registration Authority (RA)
- Key encryption and storage facilities
- Software to manage and automate PKI operations.

Working principle of PKI:

- When a browser wishes to establish a secure communication channel with a web server, it requests the server to present its public key.
- The server possesses an asymmetric public key; whose copy it presents to the browser.
- The browser generates a 'session key', a symmetric key that is encrypted using the public key that the server provided. This session key is then passed to the server.
- The web server, which has a unique copy of a private key, uses the private key to decrypt the session key. If it is able to do this, the browser takes it as proof that the server is safe to communicate with, and an encrypted channel is opened.

ix)

PGP: PGP stands for Pretty Good Privacy. PGP is a cryptographic method that lets people communicate privately online.

Or, PGP is an open source software package that is designed for the purpose of email security. It provides the basic or fundamental needs of cryptography.

It uses public key cryptography, symmetric key cryptography, hash function, and digital signature. The following are the services offered by PGP:

- Authentication
- Confidentiality
- Compression
- Email Compatibility
- Segmentation.

Working of PGP:

- Hash of the message is calculated. (MD5 algorithm)
- Resultant 128-bit hash is signed using the private key of the sender (RSA Algorithm).
- The digital signature is concatenated to message, and the result is compressed.
- A 128-bit symmetric key, KS is generated and used to encrypt the compressed message with IDEA.

- KS is encrypted using the public key of the recipient using RSA algorithm and the result is appended to the encrypted message.

Everyday more than 250 billion Emails are being exchanged over the Internet. A series of processing are involved for the transmission of an email from a sender to a recipient. the email service providers use Compression as a mechanism to reduce the amount of data to be transferred.

Compression is basically converting a message of n bits to m bits (n > m) using a compression algorithm. Compression helps the email service providers to increase their productivity as the storage overhead, processing and labor spent on the maintenance of their servers is reduced.

In PGP, message is compressed only after the application of Signature. The compressed data is decompressed at the receiver's end to obtain the original message and the signature. Then, we can extract the hash value from the signature and then we can directly determine the authenticity right away by simply calculating the message's hash value and comparing it with the value obtained from the signature.

X)

Hash function: 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

Features of Hash Functions:

- Fixed Length Output (Hash Value):
    - Hash function coverts data of arbitrary length to a fixed length. This process is often referred to as hashing the data.
    - In general, the hash is much smaller than the input data, hence hash functions are sometimes called compression functions.
    - Since a hash is a smaller representation of a larger data, it is also referred to as a digest.
- Efficiency of Operation:
    - Generally, for any hash function h with input x, computation of h(x) is a fast operation.
    - Computationally hash functions are much faster than a symmetric encryption.

Properties of Hash Functions: In order to be an effective cryptographic tool, the hash function is desired to possess following properties –

- Pre-Image Resistance: This property means that it should be computationally hard to reverse a hash function.
- Second Pre-Image Resistance: This property means given an input and its hash, it should be hard to find a different input with the same hash.
- Collision Resistance: This property means it should be hard to find two different inputs of any length that result in the same hash. This property is also referred to as collision free hash function.

Popular Hash Functions: Let us briefly see some popular hash functions –

- Message Digest (MD): The MD family comprises of hash functions MD2, MD4, MD5 and MD6. It was adopted as Internet Standard RFC 1321. It is a 128-bit hash function.
- Secure Hash Function (SHA): Family of SHA comprise of four SHA algorithms; SHA-0, SHA-1, SHA-2, and SHA-3. Though from same family, there are structurally different.
- RIPEMD: The RIPEMD is an acronym for RACE Integrity Primitives Evaluation Message Digest. The set includes RIPEMD, RIPEMD-128, and RIPEMD-160. There also exist 256, and 320-bit versions of this algorithm.
- Whirlpool: Three versions of Whirlpool have been released; namely WHIRLPOOL-0, WHIRLPOOL-T, and WHIRLPOOL.

Applications of Hash Functions: There are two direct applications of hash function based on its cryptographic properties.

- Password Storage:
    - Instead of storing password in clear, mostly all logon processes store the hash values of passwords in the file.
    - The Password file consists of a table of pairs which are in the form (user id, h(P)).
- Data Integrity Check:
    - It is used to generate the checksums on data files.
    - This application provides assurance to the user about correctness of the data.

Xi)

Product cipher: Product ciphers are ciphers that are built as a composition of several different functions.

Or, in cryptography, a product cipher is a popular type of stream ciphers that works by executing in sequence a number of simple transformations such as substitution, permutation, and modular arithmetic.

Or, in cryptography, a product cipher combines two or more transformations in a manner intending that the resulting cipher is more secure than the individual components to make it resistant to cryptanalysis.

In the days of manual cryptography, product ciphers were a useful device for cryptographers, and in fact double transposition or product ciphers on key word-based rectangular matrices were widely used.

There was also some use of a class of product ciphers known as fractionation systems, wherein a substitution was first made from symbols in the plaintext to multiple symbols in the cipher text, which was then encrypted by a final transposition, known as super-encryption.

One of the most famous field ciphers of all time was a fractionation system, the ADFGVX cipher employed by the German army during World War I. This system used a 6 × 6 matrix to substitution-encrypt the 26 letters and 10 digits into pairs of the symbols A, D, F, G, V, and X.

xii)

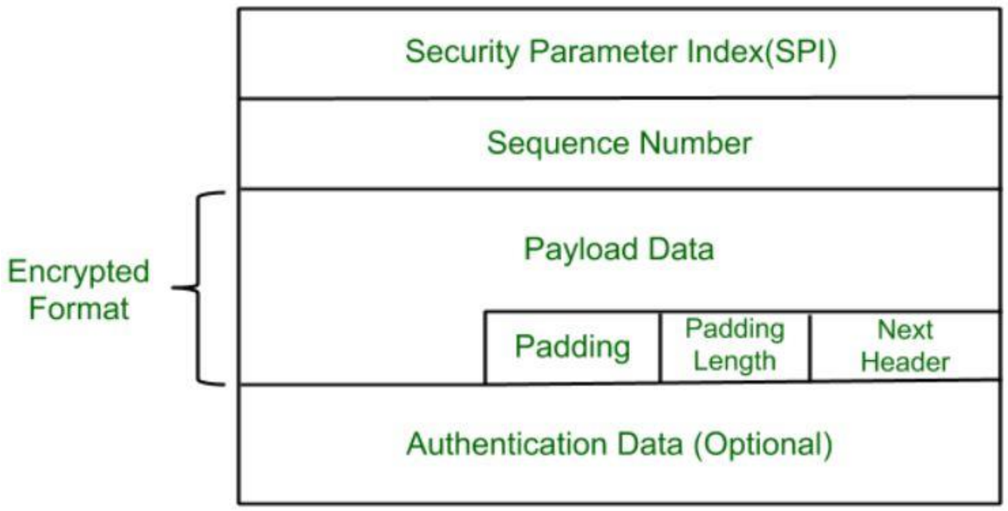
IPsec ESP format: Encapsulation Security Payload (ESP) provide the confidentiality service.

Or, ESP provides origin authenticity through source authentication, data integrity through hash functions and confidentiality through encryption protection for IP packets. ESP operates directly on top of IP, using IP protocol number 50.

ESP packet format: It contains the following field:

- 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.



Some extra question

1. Differentiate between active attacks and passive attacks.

Active Attack	Passive Attack
In active attack, Modification in information take place.	While in passive attack, Modification in the information does not take place.
Active Attack is danger for Integrity as well as availability.	Passive Attack is danger for Confidentiality.
In active attack attention is on detection.	While in passive attack attention is on prevention.
Due to active attack system is always damaged.	While due to passive attack, there is no any harm to the system.
In active attack, Victim gets informed about the attack.	While in passive attack, Victim does not get informed about the attack.
In active attack, System resources can be changed.	While in passive attack, System resources are not change.
Active attack influences the services of the system.	While in passive attack, information and messages in the system or network are acquired.
In active attack, information collected through passive attacks are used during executing.	While passive attack is performed by collecting the information such as passwords, messages by itself.
Active attack is tough to restrict from entering systems or networks.	Passive Attack is easy to prohibited in comparison to active attack.

2. What is threats and attacks? Distinguish network threats and attacks.

Threat: A Threat is a possible security violation that might exploit the vulnerability of a system or asset. The origin of threat may be accidental, environmental (natural disaster), human negligence or human failure. Difference types of security threats are interruption, interception, fabrication and modification.

Attack: Attack is a deliberate unauthorized action on a system or asset. Attack can be classified as active and passive attack. An attack will have a motive and will follow a method when opportunity arise.

The difference between threat and attack are:

Threat	Attack
Can be intentional or unintentional.	Is intentional.
May or may not be malicious.	Is malicious.
Circumstance that has ability to cause damage.	Objective is to cause damage.
Information may or may not be altered or damaged.	Chance for information alteration and damage is very high.
Comparatively hard to detect.	Comparatively easy to detect.
Can be blocked by control of vulnerabilities.	Cannot be blocked by just controlling the vulnerabilities.
Can be initiated by system itself as well as outsider.	Is always initiated by outsider (system or user).

3. What do you mean by confusion and diffusion?

A good cryptosystem should have to hinder statistical analysis: diffusion and confusion. Confusion and diffusion area unit the properties for creating a secure cipher.

Diffusion means that if we change a character of the plaintext, then several characters of the cipher text should change, and similarly, if we change a character of the cipher text, then several characters of the plaintext should change.

Confusion means that the key does not relate in a simple way to the cipher text. In particular, each character of the cipher text should depend on several parts of the key.

Let's see the difference between Confusion and Diffusion:

Confusion	**Diffusion**
Confusion is a cryptographic technique which is used to create faint cipher texts.	While diffusion is used to create cryptic plain texts.
This technique is possible through substitution algorithm.	While it is possible through transportation algorithm.
In confusion, if one bit within the secret's modified, most or all bits within the cipher text also will be modified.	While in diffusion, if one image within the plain text is modified, many or all image within the cipher text also will be modified.
In confusion, vagueness is increased in resultant.	While in diffusion, redundancy is increased in resultant.
Both stream cipher and block cipher uses confusion.	Only block cipher uses diffusion.
The relation between the cipher text and the key is masked by confusion.	While The relation between the cipher text and the plain text is masked by diffusion.

4. Explain the SHA-512 logic algorithm.

SHA-512: SHA-512 is a hashing algorithm that performs a hashing function on some data given to it.

The SHA-2 family of cryptographic hash functions consists of six hash functions. These are:

SHA-224, with 224-bit hash values

SHA-256, with 256-bit hash values

SHA-384, with 384-bit hash values

SHA-512, with 512 -bit hash values

SHA-512/224, with 512-bit hash values.

SHA-512/256, with 512-bit hash values.

Among these, **SHA-256 and SHA-512** are the most commonly accepted and used hash functions computed with 32-bit and 64-bit words.

Processing of SHA-512:

- Appending padding and fixed 128-bit length field.
- Dividing the augmented message into blocks.
- Using a 64-bit word derived from the current message block.
- Using 8 constants based on square root of first 8 prime numbers (2-19).
- Updating a 512-bit buffer.
- Using a round constant based on cube root of first 80 prime numbers (2-409.

Applications of SHA-512:

- Used as part of a system to authenticate archival video from the International Criminal Tribunal of the Rwandan genocide.
- Proposed for use in DNSSEC.
- Are moving to 512-bit SHA-2 for secure password hashing by Unix and Linux vendors.

5. Short notes:

RC4 algorithm: Rivest Cipher (RC4) is a stream cipher and variable length key algorithm. This algorithm encrypts one byte at a time.

It uses either 64 bit or 128-bit key sizes. It is generally used in applications such as Secure Socket Layer (SSL), Transport Layer Security (TSL), and also used in IEEE 802.11 wireless LAN std.

Applications of RC4:

RC4 is used in various applications such as WEP from 1997 and WPA from 2003. We also find applications of RC4 in SSL from 1995 and it is a successor of TLS from 1999. RC4 is used in varied applications because of its simplicity, speed, and simplified implementation in both software and hardware.

Types of RC4: There are various types of RC4 such as:

- Spritz
- RC4A
- VMPC
- RC4A.

Working of RC4:

- Encryption Procedure:
  - The user inputs a plain text file and a secret key.
  - The encryption engine then generates the keystream by using KSA and PRGA Algorithm.
  - This keystream is now XOR with the plain text, this XOR-ing is done byte by byte to produce the encrypted text.
  - The encrypted text is then sent to the intended receiver, the intended receiver will then decrypt the text and after decryption, the receiver will get the original plain text.
- Decryption Procedure: Decryption is achieved by doing the same byte-wise X-OR operation on the Cipher text.

Advantages:

- RC4 stream ciphers are simple to use.
- The speed of operation in RC4 is fast as compared to other ciphers.
- RC4 stream ciphers are strong in coding and easy to implement.
- RC4 stream ciphers do not require more memory.
- RC4 stream ciphers are implemented on large streams of data.

Disadvantages:

- If RC4 is not used with strong MAC, then encryption is vulnerable to a bit-flipping attack.
- RC4 stream ciphers do not provide authentication.
- RC4 algorithm requires additional analysis before including new systems.
- RC4 stream ciphers cannot be implemented on small streams of data.
- RC4 fails to discard the beginning of output keystream or fails to use non-random or related keys for the algorithm.