Q1. Short answers :

1) **What is mono alphabetic substitution cipher ?**
   Ans :-
   A monoalphabetic substitution is a cipher in which each occurrence of a plaintext symbol is replaced by a corresponding ciphertext symbol to generate ciphertext. The key for such a cipher is a table of the correspondence or a function from which the correspondence is computed. Example: An affine cipher E(x) = (ax + b) MOD 26 is an example of a monoalphabetic substitution. There are other ways to "generate" a monoalphabetic substitution. Alphabet Mixing via a Keyword A keyword or key phrase can be used to mix the letters to generate the cipher alphabet. Example: If the keyword is ANDREW DICKSON WHITE,
   then the cipher alphabet is given by
   plain A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
   cipher A N D R E W I C K S O H T B F G J L M P Q U V X Y Z

2) **List out different types of components available in Feistel cipher.**
   Ans :-

   - **Feistel cipher named after block cipher pioneer Horst Feistel, is a general cipher design principle.**
   - **A Feistel cipher can have three types of components: self-invertible, invertible and non-invertible. This cipher combines all non-invertible elements in a unit and uses the same unit in the encryption and decryption algorithm.**
   - **In a Feistel cipher, the plaintext block P is split into left and right halves, P=(L0,R0)**
   - **For each round i = 1,2,... ,n new left and right halves are computed according to the rules**

3) **List out any two advantages of AES over DES.**
   Ans :-
   Advantages of AES : 1. As it is implemented in both hardware and software, it is the most robust security protocol.
   2. It uses higher length key sizes such as 128, 192 and 256 bits for encryption.
4) **What is worm ?**
   Ans :-
   A Worm is a form of malware that replicates itself and can spread to different computers via Network.
5) **What is MAC ?**
   Ans :-
   Short for media access control, or MAC address. Known as a physical address and hardware address whose number is uniquely formatted

in hexadecimal **format and given to each computer or network device on a computer network.**

6) **What is a transposition cipher ?**

Ans :-

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.

7) **What is the purpose of S-Box ?**

Ans :-

The substitution bytes (S-Box) in AES algorithm plays an important role as it provides confusion in the cipher text . The basic function of S-Box is to transforms the 8 bits input data into 8 bits secret data using a precomputed look-up-table (LUT).

8) **List out any two drawbacks of DES.**

Ans :-

- Hardware implementations of DES are very quick.
- DES was not designed for application and therefore it runs relatively slowly.

9) **What is steganography?**

Ans :-

Steganography is the practice of concealing information within another message or physical object to avoid detection. Steganography can be used to hide virtually any type of digital content, including text, image, video, or audio content. That hidden data is then extracted at its destination.

10) **What is an intruder ?**

Ans :-

Intruder is a unauthorized person or entity that tries to access the system without the permission.

11) **Define block cipher ?**

Ans :-

A block cipher is a method of encrypting data in blocks to produce ciphertext using a cryptographic key and algorithm. The block cipher processes fixed-size blocks simultaneously, as opposed to a stream cipher, which encrypts data one bit at a time. Most modern block ciphers are designed to encrypt data in fixed-size blocks of either 64 or 128 bits.

12) **What is Feistel cipher ?**

Ans :-

The Feistel cipher proposed the structure that implements substitution and permutation alternately. Substitution replaces plain text elements with

ciphertext. Permutation changes the order of the plain text elements rather than being replaced by another element as done with substitution.

13) List out any two virus countermeasures.

Ans :-

- Detection: Once the infection has occurred, determine that it has occurred and locate the virus.
- Identification: Once detection has been achieved, identify the specific virus that has infected a program.
- Removal: Once the specific virus has been identified, remove all traces of the virus from the infected program and restore it to its original state. Remove the virus from all infected systems so that the disease cannot spread further.

14) List out the functions used for rounds of AES?

Ans :-

Each round comprises of 4 steps :

- SubBytes.
- ShiftRows.
- MixColumns.
- Add Round Key.

15) Define Honeypot.

Ans :-

A honeypot is a security mechanism that creates a virtual trap to lure attackers. An intentionally compromised computer system allows attackers to exploit vulnerabilities so you can study them to improve your security policies. You can apply a honeypot to any computing resource from software and networks to file servers and routers.

Q2. Attempt the following :

1) List and explain different categories of security services.

Ans :-

Message Confidentiality – The principle of confidentiality defines that only the sender and the intended recipient should be capable to create the element of the message. It protects the transmitted data from passive attack.

Confidentiality can be used at several levels on the basis of content of an information to be transmitted.

Authentication − The authentication service is concerned with likely that a connection is authentic. In the case of a single message, including a warning or alarm signal, the function of the authentication service is to persuade the recipient that the message is from the source that it declare to be from.

Non-repudiation − Nonrepudiation avoids either sender or receiver from adverse a transmitted message. Therefore, when a message is sent, the receiver can validate that the asserted sender actually sent the message.

Likewise, when a message is received, the sender can validate that the asserted receiver actually received the message.

Access Control − The principle of access control decides who should be capable to access information or system through communication link. It supports the avoidance of unauthorized use of a resource.

Data Integrity − Data integrity is designed to secure information from modification, insertion, deletion and rehashing by any entity. Data integrity can be used to a flow of message, an individual message or a selected portion inside a message. Data integrity can be used to support total stream protection.

2) Define security attack. Explain its different types ?
Ans :-

security attacks are generally classified into two groups, namely active attacks and passive attacks. Passive attacks are used to obtain information from targeted computer networks and systems without affecting the systems. Main properties of passive attacks are as follows:

- The goal is to obtain transmitted information from communicated networks.
- Most of the time encryption of communications is used to prevent passive attacks.

Active attacks may modify communication contents or may create false contents in computer networks and systems. The main properties of active attacks are as follows:

- The goal is to alter computer networks and systems resources or alter their operations.
- Active attacks are easier to detect than passive attacks.
- It is difficult to prevent active attack. Most of the time, prevention against active attacks requires physical protection of computer networks and systems.

3) List and explain different categories of security mechanisms.

Ans :-

Types of Security Mechanism are :

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

4) Explain Passive Attacks and its type ?

Ans :-

Passive attacks: 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 eavesdropping on or monitoring transmission. The goal of the opponent is to obtain information that is being transmitted. Passive attacks involve an attacker passively monitoring or collecting data without altering or destroying it. Examples of passive

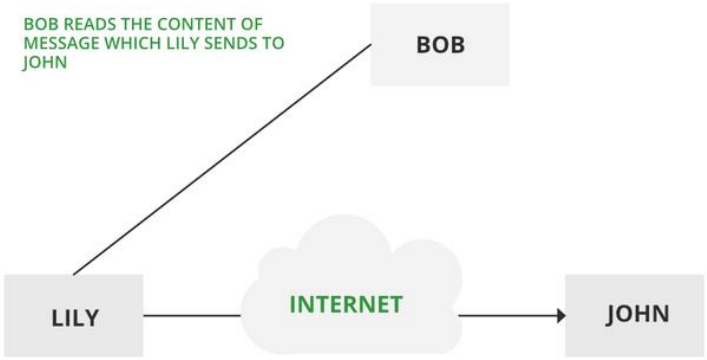
attacks include eavesdropping, where an attacker listens in on network traffic to collect sensitive information, and sniffing, where an attacker captures and analyzes data packets to steal sensitive information.

Types of Passive attacks are as follows:

- The release of message content
- Traffic analysis

The release of message content –

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

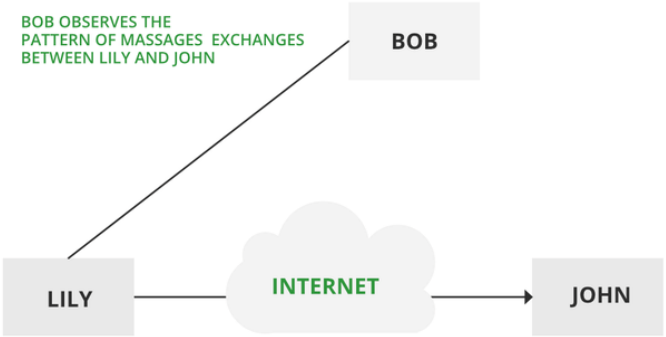


Passive attack

Traffic analysis –

Suppose that we had a way of masking (encryption) information, so that the attacker even if captured the message could not extract any information from the message. The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

The most useful protection against traffic analysis is encryption of SIP traffic. To do this, an attacker would have to access the SIP proxy (or its call log) to determine who made the call.



5) **Explain Active Attacks and its type ?**
Ans :-

Active attacks are a type of cybersecurity attack in which an attacker attempts to alter, destroy, or disrupt the normal operation of a system or network. Active attacks involve the attacker taking direct action against the target system or network, and can be more dangerous than passive attacks, which involve simply monitoring or eavesdropping on a system or network.

Types of active attacks are as follows:

- Masquerade
- Modification of messages
- Repudiation
- Replay
- Denial of Service

Masquerade –
Masquerade is a type of cybersecurity attack in which an attacker pretends to be someone else in order to gain access to systems or data.

Modification of messages –
It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorized effect. Modification is an attack on the integrity of the original data.

Repudiation –
Repudiation attacks are a type of cybersecurity attack in which an attacker attempts to deny or repudiate actions that they have taken, such as making a transaction or sending a message.

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

Denial of Service –
Denial of Service (DoS) is a type of cybersecurity attack that is designed to make a system or network unavailable to its intended users by overwhelming it with traffic or requests.

6) **What is substitution cipher ? Explain any one substitution technique in detail.**
Ans :-

Substitution technique is a classical encryption approach where the characters present in the initial message are restored by the other characters or numbers or by symbols. If the **plain text** (original message) is treated as the string of bits, thus the substitution technique would restore bit pattern of plain text with the bit pattern of cipher text.

There are various types of substitution ciphers which are as follows −

- **Monoalphabetic Cipher** − In monoalphabetic substitution cipher, a character in a plaintext is always restored or changed to the similar character in the ciphertext indifferent of its position in the text.
  For instance, if a letter A in the plaintext is changed to G then each appearance of A in the plaintext will be restored by G.
  Plaintext : hello
  Ciphertext : IFMMP

7) Write a short note on DES.
Ans :-

Data Encryption Standard (DES) is a block cipher with a 56-bit key length that has played a significant role in data security**.** Data encryption standard (DES) has been found vulnerable to very powerful attacks therefore, the popularity of DES has been found slightly on the decline. DES is a block cipher and encrypts data in blocks of size of **64 bits** each, which means 64 bits of plain text go as the input to DES, which produces 64 bits of ciphertext. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is **56 bits**.
Let us now discuss the broad-level steps in DES.

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

8) What are the different modes of operation to apply a block cipher ? Explain any one in detail.
Ans :-

Block cipher is an encryption algorithm that takes a fixed size of input say *b* bits and produces a ciphertext of *b* bits again. If the input is larger than *b* bits it can be divided further. For different applications and uses, there are several modes of operations for a block cipher.
Electronic Code Book (ECB) –
Electronic code book is the easiest block cipher mode of functioning. It is easier because of direct encryption of each block of input plaintext and output is in form of blocks of encrypted ciphertext. Generally, if a message is larger than *b* bits in size, it can be broken down into a bunch of blocks and the procedure is repeated.
Advantages of using ECB –

- Parallel encryption of blocks of bits is possible, thus it is a faster way of encryption.
- Simple way of the block cipher.

Disadvantages of using ECB –

- Prone to cryptanalysis since there is a direct relationship between plaintext and ciphertext.

9) Discuss asymmetric key cryptosystem. List out the differences between symmetric and asymmetric cryptography.

Ans :-

Asymmetric Key Encryption: Asymmetric Key Encryption is based on public and private key encryption techniques. It uses two different key to encrypt and decrypt the message. It is more secure than the symmetric key encryption technique but is much slower.

Symmetric Key Encryption	Asymmetric Key Encryption
It only requires a single key for both encryption and decryption.	It requires two keys, a public key and a private key, one to encrypt and the other one to decrypt.
The size of cipher text is the same or smaller than the original plain text.	The size of cipher text is the same or larger than the original plain text.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data is required to transfer.	It is used to transfer small amounts of data.
It only provides confidentiality.	It provides confidentiality, authenticity, and non-repudiation.
The length of key used is 128 or 256 bits	The length of key used is 2048 or higher
Examples: 3DES, AES, DES and RC4	Examples: Diffie-Hellman, ECC, El Gamal, DSA and RSA

10) Explain Playfair cipher giving proper example.

Ans :-

The Playfair Cipher encryption technique can be used to encrypt or encode a message. It operates exactly like typical encryption. The only difference is that it encrypts a digraph, or a pair of two letters, instead of a single letter.

An initial 5×5 matrix key table is created. The plaintext encryption key is made out of the matrix's alphabetic characters. Be mindful that you shouldn't repeat the letters. There are 26 alphabets however, there are only 25 spaces in which we can place a letter. The matrix will delete the extra letter because there is an excess of one letter (typically J). Despite this, J is there in the plaintext before being changed to I.

Find the example later

11) Write an overview of AES algorithm.

Ans :-

Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.

Points to remember

- AES is a block cipher.
- The key size can be 128/192/256 bits.
- Encrypts data in blocks of 128 bits each.

That means it takes 128 bits as input and outputs 128 bits of encrypted cipher text as output. AES relies on substitution-permutation network principle which means it is performed using a series of linked operations which involves replacing and shuffling of the input data.

12) Explain RSA algorithm.

Ans :-

RSA algorithm uses the following procedure to generate public and private keys:

- Select two large prime numbers, p and **q**.
- Multiply these numbers to find **n = p x q,** where **n** is called the modulus for encryption and decryption.
- Choose a number **e** less than **n**, such that n is relatively prime to **(p - 1) x (q -1).** It means that **e** and **(p - 1) x (q - 1)** have no common factor except 1. Choose "e" such that 1<e < ϕ (n), e is prime to ϕ (n), **gcd (e,d(n)) =1**

- If **n = p x q,** then the public key is <e, n>. A plaintext message **m** is encrypted using public key <e, n>. To find ciphertext from the plain text following formula is used to get ciphertext C.
  $C = m^e \bmod n$
  Here**, m** must be less than **n**. A larger message (>n) is treated as a concatenation of messages, each of which is encrypted separately.
- To determine the private key, we use the following formula to calculate the d such that:
  $D_e \bmod \{(p - 1) x (q - 1)\} = 1$
  Or
  $D_e \bmod \phi (n) = 1$
- The private key is <d, n>. A ciphertext message **c** is decrypted using private key <d, n>. To calculate plain text **m** from the ciphertext c following formula is used to get plain text m.
  $m = c^d \bmod n$

13) Explain public key cryptography. Explain its application.

Ans :-

Public key cryptography involves a pair of keys known as a public key and a private key (a *public key pair*), which are associated with an entity that needs to authenticate its identity electronically or to sign or encrypt data. Each public key is published and the corresponding private key is kept secret. Data that is encrypted with the public key can be decrypted only with the corresponding private key.

There are various application of Public key cryptography which are as follows:

Digital signatures − It is a message produced by user's private key used as authenticity of a user.

Encryption − It can transform the plaintext into unreadable format, and it can be used to connect message securely to receiver.

Authentication − It can certify that the message or user is legal or not. Authentication represent that users are who they request to be.

Non-repudiation − Non-repudiation defines that a person who sends a message cannot decline that sent it and, conversely, that a person who has received a message cannot decline that received it.

Signing − Each user can implement signing operation using its private key.

Verification − The signed signature is verified by the public key of concerned user.

14) Explain Vigenere cipher giving proper example.

Ans :-

Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using the *Vigenère square or Vigenère table*.

- The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.
- At different points in the encryption process, the cipher uses a different alphabet from one of the rows.
- The alphabet used at each point depends on a repeating keyword.

Examples are hard

15) Explain ECB mode of operation of block cipher.

Ans :-

Electronic Code Book (ECB) –

Electronic code book is the easiest block cipher mode of functioning. It is easier because of direct encryption of each block of input plaintext and output is in form of blocks of encrypted ciphertext. Generally, if a message is larger than *b* bits in size, it can be broken down into a bunch of blocks and the procedure is repeated.

Advantages of using ECB –

- Parallel encryption of blocks of bits is possible, thus it is a faster way of encryption.
- Simple way of the block cipher.

Disadvantages of using ECB –

- Prone to cryptanalysis since there is a direct relationship between plaintext and ciphertext.

16) Explain Asymmetric cryptography with its application.

Ans :-

Asymmetric encryption, also known as public-key cryptography, is a type of encryption that uses a pair of keys to encrypt and decrypt data. The pair of keys includes a public key, which can be shared with anyone, and a private key, which is kept secret by the owner. In asymmetric encryption, the sender uses the recipient's public key to encrypt the data. The recipient then uses their

private key to decrypt the data. This approach allows for secure communication between two parties without the need for both parties to have the same secret key.

1. Confidentiality

The most common application of Asymmetric Encryption is confidentiality.

2. Authenticity using Digital Signatures

A sender attaches his private key to the message as a digital signature and exchanges it with the receiver.

3. Integrity of Information Exchange

One way the hash of the data to be exchanged is created and encrypted using the sender's private key.

4. Non-repudiation

With the digital signature encryption tool in place, the owner of a document or information who exchanged it with others cannot disown the content, and a transaction done online cannot be disowned by its originator.

Q3. Attempt the following :

1) **Explain Diffie-Hellman key exchange algorithm.**
   Ans :-

To implement Diffie-Hellman, two end users, Alice and Bob, mutually agree on positive whole numbers *p* and *q*, such that *p* is a prime number and *q* is a generator of *p*. The generator *q* is a number that, when raised to positive whole-number powers less than *p*, never produces the same result for any two such whole numbers. The value of *p* may be large, but the value of *q* is usually small.

Once Alice and Bob have agreed on *p* and *q* in private, they choose positive whole-number personal keys *a* and *b*. Both are less than the prime number modulus *p*. Neither user divulges their personal key to anyone; ideally, they memorize these numbers and don't write them down or store them anywhere. Next, Alice and Bob compute public keys *a** and *b** based on their personal keys according to the following formulas:

$a^* = q_a \bmod p$

$b^* = q_b \bmod p$

The two users can share their public keys *a** and *b** over a communications medium assumed to be insecure, such as the internet or a corporate wide area network. From these public keys, a number *x* can be generated by either user on the basis of their own personal keys. Alice computes *x* using the following formula:

$x = (b^*) \bmod p$

Bob computes *x* using the following formula:

$x = (a^*) \bmod p$

The value of *x* turns out to be the same according to either of the above two formulas. However, the personal keys *a* and *b*, which are critical in the calculation of *x*, haven't been transmitted over a public medium. Because it's a large and apparently random number, a potential hacker has almost no chance of correctly guessing *x*, even with the help of a powerful computer to conduct millions of trials. The two users can, therefore, in theory,

communicate privately over a public medium with an encryption method of their choice using the decryption key *x*.

2) **Write a short note on HMAC.**

Ans :-

HMAC (Hash-based Message Authentication Code) is a type of a message authentication code (MAC) that is acquired by executing a cryptographic hash function on the data (that is) to be authenticated and a secret shared key. Like any of the MAC, it is used for both data integrity and authentication. Checking data integrity is necessary for the parties involved in communication. HTTPS, SFTP, FTPS, and other transfer protocols use HMAC. The cryptographic hash function may be MD-5, SHA-1, or SHA-256. Digital signatures are nearly similar to HMACs i.e they both employ a hash function and a shared key. The difference lies in the keys i.e HMACs use symmetric key(same copy) while Signatures use asymmetric (two different keys).

Applications

- Verification of e-mail address during activation or creation of an account.
- HMACs can be used for Internet of things (IoT) due to less cost.

3) **What is hash function? Discuss its characteristics.**

Ans :-

A **Hash Function** is a function that converts a given numeric or alphanumeric key to a small practical integer value. The mapped integer value is used as an index in the hash table. In simple terms, a hash function **maps** a significant number or string to a small integer that can be used as the **index** in the hash table.

Characteristics of good hash function

1. Minimum collision
2. High gain factor (distributes keys evenly). Like say we have 10 locations in the hash table, then almost 9 locations should have keys. It should not be the case that 4-5 locations have keys only where the keys collided.
3. Have a high load factor. Load factor means the number of keys stored/hash table size
4. Easy to compute

4) **What is digital signature? List out its desired properties.**

Ans :-

A digital signature is a mathematical technique used to validate the authenticity and integrity of a digital document, message or software. It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more

inherent security. A digital signature is intended to solve the problem of tampering and impersonation in digital communications.
The desired Properties of a digital signature
- Authenticity: a valid signature implies that the signer deliberately signed the associated message - Unforgeability: only the signer can give a valid signature for the associated message - Non-re-usability: the signature of a document can not be used on another document - Non-repudiation: the signer can not deny having signed a document that has valid signature - Integrity: ensure the contents have not been modified

5) **Discuss Kerberos in detail.**
Ans :-
Kerberos is a protocol for authenticating service requests between trusted hosts across an untrusted network, such as the internet. Kerberos support is built in to all major computer operating systems, including Microsoft Windows, Apple macOS, FreeBSD and Linux.

The three heads of the Kerberos protocol represent the following:

1. the client or principal;
2. the network resource, which is the application server that provides access to the network resource; and
3. a key distribution center (KDC), which acts as Kerberos' trusted third-party authentication service.

6) **Write a short note on X509 standard.**
Ans :-
An X.509 certificate is a digital certificate based on the widely accepted International Telecommunications Union (ITU) X.509 standard, which defines the format of public key infrastructure (PKI) certificates. They are used to manage identity and security in internet communications and computer networking. They are unobtrusive and ubiquitous, and we encounter them every day when using websites, mobile apps, online documents, and connected devices.

7) **Discuss the requirements of message authentication.**
Ans :-

Authentication Requirements:

- **Revelation:** It means releasing the content of the message to someone who does not have an appropriate cryptographic key.
- **Analysis of Traffic:** Determination of the pattern of traffic through the duration of connection and frequency of connections between different parties.
- **Deception:** Adding out of context messages from a fraudulent source into a communication network. This will lead to mistrust between the parties communicating and may also cause loss of critical data.
- **Modification in the Content:** Changing the content of a message. This includes inserting new information or deleting/changing the existing one.
- **Modification in the sequence:** Changing the order of messages between parties. This includes insertion, deletion, and reordering of messages.
- **Modification in the Timings:** This includes replay and delay of messages sent between different parties. This way session tracking is also disrupted.
- **Source Refusal:** When the source denies being the originator of a message.
- **Destination refusal:** When the receiver of the message denies the reception.

8) Explain SHA-512 algorithm.
Ans :-

SHA-512 does its work in a few stages. These stages go as follows:

1. Input formatting
2. Hash buffer initialization
3. Message Processing
4. Output

Let's look at these one-by-one.

1. **Input Formatting:**

SHA-512 can't actually hash a message input of any size, i.e. it has an input size limit. This limit is imposed by its very structure as you may see further on. The entire formatted mesage has basically three parts: the original message, padding bits, size of original message.

2. Hash buffer initialization:

The algorithm works in a way where it processes each block of 1024 bits from the message using the result from the previous block. Now, this poses a problem for the first 1024 bit block which can't use the result from any previous processing.

3. Message Processing:

Message processing is done upon the formatted input by taking one block of 1024 bits at a time. The actual processing takes place by using two things: The 1024 bit block, and the result from the previous processing.

4. Output:

After every block of 1024 bits goes through the message processing phase, i.e. the last iteration of the phase, we get the final 512 bit Hash value of our original message.

9) Write a short note on digital signature.
Ans :-

A digital signature is a mathematical technique used to validate the authenticity and integrity of a digital document, message or software. It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security. A digital signature is intended to solve the problem of tampering and impersonation in digital communications.

Digital signatures can provide evidence of origin, identity and status of electronic documents, transactions or digital messages. Signers can also use them to acknowledge informed consent. In many countries, including the U.S., digital signatures are considered legally binding in the same way as traditional handwritten document signatures.

10) Explain public key infrastructure. Explain its key elements.

Ans :-

Public Key Infrastructure:

Public key infrastructure affirms the usage of a public key. PKI identifies a public key along with its purpose. It usually consists of the following components:

- A digital certificate also called a public key certificate
- Private Key tokens
- Registration authority
- Certification authority
- CMS or Certification management system

- **Private and Public Keys**

  PKI uses these asymmetric keys to establish and secure an encrypted connection over the network using **asymmetric encryption**.

- **Public Key Certificates**

  These are issued by **Certificate Authorities** which prove the ownership of a public key. They state the authenticity of the keyholder.

- **Certificate Authority**

  Certificate Authorities, or CAs, are trusted entities which verify the organization and generate digital certificates which contain information about the organization, as well as the public key of that organization.

- **Certificate Repository**

  A location where all certificates are stored as well as their public keys, validity details, revocation lists, and root certificates. These locations are accessible through LDAP, FTP or web servers.

- **Automating PKI Operations**

  These help in issuing, revoking, and renewing certifications. They are done through certificate management software.

11) Write a short note on Kerberos.

Ans :- refer to the 5th question

12) Explain the format of X.509 certificate.

Ans :-

Standard information in an X.509 certificate includes the following:

- **Version.** Which X.509 version applies to the certificate, indicating what data the certificate must include.
- **Serial number.** The CA creating the certificate must assign it a serial number that distinguishes the CA certificate from other certificates.
- **Algorithm information.** The signature algorithm the issuer uses to sign the certificate.
- **Issuer distinguished name.** The name of the entity issuing the certificate -- usually, the CA.
- **Validity period of the certificate.** The start and end date, as well as the time the certificate is valid and can be trusted.
- **Subject distinguished name.** The name to which the certificate is issued.
- **Subject public key information.** The public key associated with the identity.
- **Extensions (optional).** Extensions have their own unique IDs, expressed as a set of values called an *object identifier*. An extension can be rejected if it is not recognized or if the extension has information that can't be processed.

13) Differentiate between stream cipher and block cipher.

Ans :-

S.NO	Stream Cipher	Block Cipher
1.	Stream Cipher Converts the plain text into cipher text by taking 1 byte of plain text at a time.	Block Cipher Converts the plain text into cipher text by taking plain text's block at a time.
2.	While stream cipher uses 8 bits.	Block cipher uses either 64 bits or more than 64 bits.
3.	While stream cipher is more complex.	The complexity of block cipher is simple.

S.NO	Stream Cipher	Block Cipher
4.	While stream cipher uses only confusion.	Block cipher Uses confusion as well as diffusion.
5.	While in-stream cipher, reverse encrypted text is easy.	In block cipher, reverse encrypted text is hard.
6.	Encrypts data one bit or byte at a time	Operates on fixed-length blocks of data

14) Discuss MAC in detail.

Ans :-

MAC stands for Message Authentication Code. Here in MAC, sender and receiver share same key where sender generates a fixed size output called Cryptographic checksum or Message Authentication code and appends it to the original message. On receiver's side, receiver also generates the code and compares it with what he/she received thus ensuring the originality of the message. These are components:

- Message
- Key
- MAC algorithm
- MAC value

15) Explain digital signature process.

Ans :-

The steps of the digital signature process are as follows:

1. The sender computes a message digest (with an algorithm such as RSA or SHA1) and then encrypts the digest with their private key, which forms the digital signature. Multiple signatures and signature formats can be attached to a message, each referencing different (or even overlapping) parts of the message.
2. The sender transmits the digital signature with the message.
3. The receiver decrypts the digital signature with the public key of the sender, thus regenerating the message digest.
4. The receiver computes a message digest from the message data that was received, and verifies that the two digests are the same. If these digests match, the message is both intact and authentic.

16) Discuss Diffie Hellman key exchange process.

Ans :-
Pending

17) Explain the concept of Digital Certificate in detail.
Ans :-

Digital certificate is issued by a trusted third party which proves sender's identity to the receiver and receiver's identity to the sender.
A digital certificate is a certificate issued by a Certificate Authority (CA) to verify the identity of the certificate holder. The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. Digital certificate is used to attach public key with a particular individual or an entity.

Digital certificate contains:- The authenticity.

1. Name of certificate holder.
2. Serial number which is used to uniquely identify a certificate, the individual or the entity identified by the certificate
3. Expiration dates.
4. Copy of certificate holder's public key.(used for decrypting messages and digital signatures)
5. Digital Signature of the certificate issuing authority.

Q4. Attempt the following :

1) Write a short note on PGP.
Ans :-

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

2) **What is SSL? Discuss its architecture.**
Ans :-

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

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

A Web server requires an SSL certificate to establish a secure SSL connection while using SSL for safe Internet transactions. SSL encrypts network connection segments atop the transport layer, a network connection component above the program layer.

SSL is based on an asymmetric cryptographic process in which a Web browser generates both a public and a private (secret) key. A certificate signing request is a data file that contains the public key (CSR). Only the recipient receives the private key.

3) **Define intruder. Explain different types of intruders.**
Ans :-
Definition : An intruder is an unauthorized person or entity that tries to access a system or network without authorization with the intent of doing harm, stealing data, or interfering with regular operations.

Types of Intruders
Intruders are divided into three categories:

- **Masquerader:** The category of individuals that are not authorized to use the system but still exploit users' privacy and confidential information by possessing techniques that give them control over the system, such category of intruders is referred to as Masquerader. Masqueraders are outsiders and hence they don't have direct access to the system, their aim is to attack unethically to steal data/ information.
- **Misfeasor:** The category of individuals that are authorized to use the system, but misuse the granted access and privilege. These are individuals that take undue advantage of the permissions and access given to them, such category of intruders is referred to as Misfeasor. Misfeasors are insiders and they have direct access to the system, which they aim to attack unethically for stealing data/ information.
- **Clandestine User:** The category of individuals who have supervision/administrative control over the system and misuse the authoritative power given to them. The misconduct of power is often done by

superlative authorities for financial gains, such a category of intruders is referred to as Clandestine Users. A Clandestine User can be any of the two, insiders or outsiders, and accordingly, they can have direct/ indirect access to the system, which they aim to attack unethically by stealing data/ information.

4) **Discuss different approaches of intrusion detection.**
   Ans :-

Signature-Based Detection

Signature-based detection is one of the most widely used approaches to intrusion detection and prevention. This method uses a database of known attack patterns or "signatures" to detect and prevent intrusions. The system compares incoming network traffic or system activity against the signatures in the database.

Anomaly-Based Detection

Anomaly-based detection is another approach to intrusion detection and prevention. This method uses machine learning algorithms to detect anomalies in network traffic or system activity. The system compares the current activity to a baseline of normal activity and flags any activity that deviates from the norm as potentially malicious.

Behavior-Based Detection

Behavior-based detection is a newer approach to intrusion detection and prevention. This method uses machine learning algorithms to detect abnormal behavior in network traffic or system activity. The system observes the behavior of the network or system and compares it to a baseline of normal behavior. If the system detects abnormal behavior, it flags it as potentially malicious.

5) **What is firewall ? Explain its limitations.**
   Ans :-
   Firewall is a network security device that observes and filters incoming and outgoing network traffic, adhering to the security policies defined by an organization. Essentially, it acts as a protective wall between a private internal network and the public Internet.

There are many limitations of firewall some of them are-

- Firewalls cannot stop users from accessing malicious websites, making it vulnerable to internal threats or attacks.
- Firewalls cannot protect against the transfer of virus-infected files or software.

- Firewalls cannot prevent misuse of passwords.
- Firewalls cannot protect if security rules are misconfigured.
- Firewalls cannot protect against non-technical security risks, such as social engineering.
- Firewalls cannot stop or prevent attackers with modems from dialing in to or out of the internal network.
- Firewalls cannot secure the system which is already infected.

6) What is virus ? Explain its counter measures.

Ans :-

A computer virus is malicious code that replicates by copying itself to another program, computer boot sector or document and changes how a computer works. A virus spreads between systems after some type of human intervention

The following measures can help you prevent a virus infection:

- Install current antivirus and antispyware software, and keep it up to date.
- Run daily scans of antivirus software.
- Disable autorun to prevent viruses from propagating to any media connected to the system.
- Regularly patch the OS and applications installed on the computer.
- Don't click on web links sent via email from unknown senders.
- Don't download files from the internet or email from unknown senders.
- Install a hardware-based firewall.

7) Explain S/MIME with its different functionalities.

Ans :-

S/MIME provides the following functions:

• **Enveloped data:** This consists of encrypted content of any type and encrypted-content encryption keys for one or more recipients.

• **Signed data:** A digital signature is formed by taking the message digest of the content to be signed and then encrypting that with the private key of the signer. The content plus signature are then encoded using base64 encoding. A signed data message can only be viewed by a recipient with S/MIME capability.

• **Clear-signed data:** As with signed data, a digital signature of the content is formed. However, in this case, only the digital signature is encoded using base64.

As a result, recipients without S/MIME capability can view the message content, although they cannot verify the signature.

• **Signed and enveloped data:** Signed-only and encrypted-only entities may be nested, so that encrypted data may be signed and signed data or clear-signed data may be encrypted.

8) **Discuss SSL record protocol in detail.**

Ans :-

The SSL Record Protocol provides two services for SSL connections:

• Confidentiality: The Handshake Protocol defines a shared secret key that is used for conventional encryption of SSL payloads.

• Message Integrity: The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC).

The overall operation of the SSL Record Protocol. The Record Protocol takes an application message to be transmitted, fragments the data into manageable blocks, optionally compresses the data, applies a MAC, encrypts, adds a header, and transmits the resulting unit in a TCP segment. Received data are decrypted, verified, decompressed, and reassembled and then delivered to higher-level users.

9) **Discuss different intrusion techniques. What precautions can be taken to prevent intrusion.**

Ans :-

Refer above answers.

10) **Write a short note on Honeypots.**

Ans :-

Honeypot is a network-attached system used as **a trap for cyber-attackers** to detect and study the tricks and types of attacks used by hackers. It acts as a potential target on the internet and informs the defenders about any unauthorized attempt to the information system.

Honeypots are mostly used by large companies and organizations involved in cybersecurity. It helps cybersecurity researchers to learn about the different type of attacks used by attackers. It is suspected that even the cybercriminals use these honeypots to decoy researchers and spread wrong information.

11) **Explain firewall with its types.**

Ans :-

There are multiple types of firewalls based on their traffic filtering methods, structure, and functionality. A few of the types of firewalls are:

- Packet Filtering

A packet filtering firewall controls data flow to and from a network. It allows or blocks the data transfer based on the packet's source address, the destination address of the packet, the application protocols to transfer the data, and so on.

- Proxy Service Firewall

This type of firewall protects the network by filtering messages at the application layer. For a specific application, a proxy firewall serves as the gateway from one network to another.

- Stateful Inspection

Such a firewall permits or blocks network traffic based on state, port, and protocol. Here, it decides filtering based on administrator-defined rules and context.

- Next-Generation Firewall

According to Gartner, Inc.'s definition, the next-generation firewall is a deep-packet inspection firewall that adds application-level inspection, intrusion prevention, and information from outside the firewall to go beyond port/protocol inspection and blocking.

- Unified Threat Management (UTM) Firewall

A UTM device generally integrates the capabilities of a stateful inspection firewall, intrusion prevention, and antivirus in a loosely linked manner. It may include additional services and, in many cases, cloud management. UTMs are designed to be simple and easy to use.

- Threat-Focused NGFW

These firewalls provide advanced threat detection and mitigation. With network and endpoint event correlation, they may detect evasive or suspicious behavior.

12) Explain DDOS.

Ans :-

Distributed Denial of Service (DDoS) is a type of DOS attack where multiple systems, which are trojan infected, target a particular system which causes a DoS attack.

A DDoS attack uses multiple servers and Internet connections to flood the targeted resource. A DDoS attack is one of the most powerful weapons on the cyber platform. When you come to know about a website being brought down, it generally means it has become a victim of a DDoS attack. This means that the hackers have attacked your website or PC by imposing heavy traffic. Thus, crashing the website or computer due to overloading.
Example: In 2000, Michael Calce, a 15-year-old boy who used the online name "Mafiaboy", was behind one of the first DDoS attacks. He hacked into the computer networks of various different universities. He used their servers to operate a DDoS attack that brought down several websites such as eBay and Yahoo.

13) Explain PGP with different services offered by it.

Ans :-

Following are the services offered by PGP :-

1. **Confidentiality and Authentication** − The both services can be used for the same message. First, a signature is produced for the plaintext message and prepended to the message. Therefore the plaintext message plus signature is encrypted using CAST-128 (or IDEA or 3DES), and the session key is encrypted using RSA.

2. **Compression** − As a default, PGP restrict the message after using the signature but before encryption. This has the advantage of storing space both for e-mail transmission and for file storage.
3. **E-mail compatibility** − Some electronic mail systems only allows the use of blocks including ASCII text. When PGP is used, minimum part of the block to be transmitted is encrypted.
4. **Segmentation** − E-mail facilities are restricted to a maximum message length. For instance, some facilities accessible throughout the internet set a maximum length of 50,000 octets. Some message higher than that should be broken up into smaller segments, each of which is mailed independently.

14) Discuss SSL handshaking protocol in detail.

Ans :-

SSL Handshake Protocol: The part of SSL which handles the preservation of authenticity. There is a distinct process that follows the authentication of web servers and clients, which you will look into later in this lesson.

- **Phase-1:** In Phase-1 both Client and Server send hello-packets to each other. In this IP session, cipher suite and protocol version are exchanged for security purposes.
- **Phase-2:** Server sends his certificate and Server-key-exchange. The server end phase-2 by sending the Server-hello-end packet.
- **Phase-3:** In this phase, Client replies to the server by sending his certificate and Client-exchange-key.
- **Phase-4:** In Phase-4 Change-cipher suite occurs and after this the Handshake Protocol ends.

15) Define Intrusion. Explain different approaches of Intrusion detection.

Ans :-

An illegal entrance into your network or an address in your assigned domain is referred to as a *network intrusion*. An intrusion can be passive (in which access is achieved quietly and undetected) or *aggressive* (in which access is gained overtly and without detection) (in which changes to network resources are effected).

Intrusion detection systems employ two detection methods −

- *Signature-based detection* matches data activity to a signature or pattern in a signatures database. A new harmful behavior that is not in the database, for example, is overlooked when using signature-based detection.
- Unlike signature-based detection, *behavior-based detection* recognizes any abnormality and issues alarms, making it capable of identifying new sorts of threats. It's referred to as an expert system since it learns what regular behavior looks like in your system.

16) Define malicious software. Explain different types of viruses.

Ans :-

Malicious Software refers to any malicious program that causes harm to a computer system or network. Malicious Malware Software attacks a computer or network in the form of viruses, worms, trojans, spyware, adware, or rootkits.

Various types of viruses:

- **File Virus:**
  This type of virus infects the system by appending itself to the end of a file. It changes the start of a program so that the control jumps to its code. After the execution of its code, the control returns back to the main program. Its execution is not even noticed. It is also called a **Parasitic virus** because it leaves no file intact but also leaves the host functional.

- **Boot sector Virus:**
  It infects the boot sector of the system, executing every time system is booted and before the operating system is loaded. It infects other bootable media like

floppy disks. These are also known as **memory viruses** as they do not infect the file systems.

- **Macro Virus:**
  Unlike most viruses which are written in a low-level language(like C or assembly language), these are written in a high-level language like Visual Basic. These viruses are triggered when a program capable of executing a macro is run. For example, the macro viruses can be contained in spreadsheet files.

- **Source code Virus:**
  It looks for source code and modifies it to include virus and to help spread it.

17) Explain capabilities and limitations of firewall.

Ans :-

Firewall Capabilities

- Block incoming and outgoing traffic based on a defined set of rules
- Scan packets of data for keywords or patterns and block any that match specific predefined rules
- Can be used with other security measures, like antivirus software, to protect computers against viruses and malware
- Specify the types of traffic they protect against (e.g., malicious websites) and how much bandwidth is allocated for each user
- Block certain websites from being accessed on a network

Firewall Limitations

- Don't provide complete protection against malicious websites and other online threats
- Can be bypassed by hackers using techniques like port redirection or IP spoofing
- Can create compatibility issues when switching vendors

18) Explain Secure Electronic Transaction.

Ans :-

Secure Electronic Transaction or SET is a system that ensures the security and integrity of electronic transactions done using credit cards in a scenario. SET is not some system that enables payment but it is a security protocol applied to those payments. It uses different encryption and hashing techniques to secure payments over the internet done through credit cards. The SET protocol was supported in development by major organizations like Visa, Mastercard, and Microsoft which provided its Secure Transaction Technology (STT), and Netscape which provided the technology of Secure Socket Layer (SSL).
SET protocol restricts the revealing of credit card details to merchants thus keeping hackers and thieves at bay. The SET protocol includes Certification Authorities for making use of standard Digital Certificates like X.509 Certificate.

Q5. Attempt the following :

1) **Discuss how public key cryptography complements private key cryptography rather being a replacement of it.**
   Ans :-

2) **Discuss Man in middle attack.**
   Ans :-

A MITM attack is a form of cyber-attack where a user is introduced with some kind of meeting between the two parties by a malicious individual, manipulates both parties and achieves access to the data that the two people were trying to deliver to each other. A man-in-the-middle attack also helps a malicious attacker, without any kind of participant recognizing till it's too late, to hack the transmission of data intended for someone else and not supposed to be sent at all. In certain aspects, like MITM, MitM, MiM or MIM, MITM attacks can be referred.

If an attacker puts himself between a client and a webpage, a Man-in-the-Middle (MITM) attack occurs. This form of assault comes in many different ways.

For example, In order to intercept financial login credentials, a fraudulent banking website can be used. Between the user and the real bank webpage, the fake site lies "in the middle."

3) **Write short note on :**
   i)Trapdoor ii)Logic bomb
   Ans :-
   i)Trapdoor :-

- A trap door is kind of a secret entry point into a program that allows anyone to gain access to any system without going through the usual security access procedures.
- Trap Doors are quite difficult to detect and also in order to find them the programmers or the developers have to go through the components of the system.

ii)Logic bomb :-

A logic bomb is a type of malware that contains malicious code that is discreetly installed into software, a computer network, or an operating system with the goal of causing harm to a network when certain conditions are met. It is triggered at a specific event and used to devastate a system by clearing hard drives, deleting files, or corrupting data. An event can be a specific date or time leading up to the launch of an infected software application or the deletion of a specific record from a system.

4) **Explain additive cipher with proper example.**
   Ans :-

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

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

5) **Explain two general approaches of attacking a cipher.**
   Ans :-

The general two approaches for attacking a cipher

1. **Cryptanalysis:** Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some samples plaintext-cipher text pairs. This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used. If the attack succeeds in deducing the key, the effect is catastrophic: All future and past messages encrypted with the key are compromised.
2. **Brute-force attack:** The attacker tries every possible key on a piece of cipher text until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

6) **Explain symmetric key cryptography. Discuss different techniques used in traditional ciphers.**
   Ans :-
   Symmetric Key Encryption: Encryption is a process to change the form of any message in order to protect it from reading by anyone. In Symmetric-key encryption the message is encrypted by using a key and the same key is used to decrypt the message which makes it easy to use but less secure. It also requires a safe method to transfer the key from one party to another.

7) **Explain IPSec in detail.**
   Ans :-

IPSec encryption is a software function that scrambles data to protect its content from unauthorized parties. Data is encrypted by an encryption key, and a decryption key is needed to unscramble the information. IPSec supports various types of encryptions, including AES, Blowfish, Triple DES, ChaCha, and DES-CBC.

IPSec uses asymmetric and symmetric encryption to provide speed and security during data transfer. In asymmetric encryption, the encryption key is made public while the decryption key is kept private. Symmetric encryption uses the same public key for encrypting and

decrypting data. IPSec establishes a secure connection with asymmetric encryption and switches to symmetric encryption to speed up data transfer.

8) **Explain different types of viruses.**
Ans :-

Various types of viruses:

- **File Virus:**
  This type of virus infects the system by appending itself to the end of a file. It changes the start of a program so that the control jumps to its code. After the execution of its code, the control returns back to the main program. Its execution is not even noticed. It is also called a **Parasitic virus** because it leaves no file intact but also leaves the host functional.

- **Boot sector Virus:**
  It infects the boot sector of the system, executing every time system is booted and before the operating system is loaded. It infects other bootable media like floppy disks. These are also known as **memory viruses** as they do not infect the file systems.

- **Macro Virus:**
  Unlike most viruses which are written in a low-level language(like C or assembly language), these are written in a high-level language like Visual Basic. These viruses are triggered when a program capable of executing a macro is run. For example, the macro viruses can be contained in spreadsheet files.

- **Source code Virus:**
  It looks for source code and modifies it to include virus and to help spread it.

9) **What is the role of audit record in intrusion detection?**
Ans :-
The audit records provide input to the intrusion detection function in two ways. First, the designer must decide on a number of quantitative metrics that can be us ed to measure user behavior. An analysis of audit records over a period of time can be used to determine the activity profile of the average user. Thus, the audit records serve to define typical behaviour. Second, current audit records are the input used to detect
intrusion. That is, the intrusion detection model analyzes incoming audit records t o determine deviation from average behaviour.

10) **Encode message 'CEASE FIRE' using additive cipher with key. Also explain decoding process.**
Ans :-

11) **Explain different aspects of Network security.**
Ans :-

1. **Confidentiality:** This component is often associated with secrecy and the use of encryption. Confidentiality in this context means that the data is only available to authorized parties. When information has been kept confidential it means that it has not been compromised by other parties; confidential data are not disclosed to people who do not require them or who should not have access to them.
2. **Integrity:** Data integrity refers to the certainty that the data is not tampered with or degraded during or after submission. It is the certainty that the data has not been subject to unauthorized modification, either intentional or unintentional.
3. **Availability:** This means that the information is available to authorized users when it is needed. For a system to demonstrate availability, it must have properly functioning computing systems, security controls and communication channels.

12) Explain different modes of operations of IPSec protocol.

Ans :-

The IPsec standards define two distinct modes of IPsec operation, **transport mode** and **tunnel mode**. The modes do not affect the encoding of packets. The packets are protected by AH, ESP, or both in each mode. The modes differ in policy application when the inner packet is an IP packet, as follows:

- In transport mode, the outer header determines the IPsec policy that protects the inner IP packet.
- In tunnel mode, the inner IP packet determines the IPsec policy that protects its contents.

In transport mode, the outer header, the next header, and any ports that the next header supports, can be used to determine IPsec policy. In effect, IPsec can enforce different transport mode policies between two IP addresses to the granularity of a single port. For example, if the next header is TCP, which supports ports, then IPsec policy can be set for a TCP port of the outer IP address. Similarly, if the next header is an IP header, the outer header and the inner IP header can be used to determine IPsec policy.

Tunnel mode works only for IP-in-IP datagrams. Tunneling in tunnel mode can be useful when computer workers at home are connecting to a central computer location. In tunnel mode, IPsec policy is enforced on the contents of the inner IP datagram. Different IPsec policies can be enforced for different inner IP addresses. That is, the inner IP header, its next header, and the ports that the next header supports, can enforce a policy. Unlike transport mode, in tunnel mode the outer IP header does not dictate the policy of its inner IP datagram.

13) Explain lifecycle of virus.

Ans :-

The life cycle of a computer virus can be divided into four phases:

Dormant phase

The virus is idle in the dormant phase. It has accessed the target device but does not take any action.

Note: Not all viruses have the dormant phase.

Propagation phase

In the propagation phase, the virus starts propagating by replicating itself. The virus places a copy of itself into other programs or accomplishes certain system areas on the disk. Each infected program will contain a clone of the virus, which will enter its own propagation phase as well.

Triggering phase

The triggering phase starts when the dormant virus is activated. It will perform the actions it is supposed to accomplish. This phase can be caused by various system events like the count of the times the virus has cloned or after a set time interval has elapsed.

Execution phase

In the execution phase, the payload will be released. It can harm deleting files, crashing the system, and so on. It can be harmless too and pop some humorous messages on screen.

14) Encrypt NOTHING IS AS IT SEEMS and decrypt MKHSE LWYAE ATSOL using Rail Fence cipher.

Ans :-

Rail Fence Cipher Example: We encipher NOTHING IS AS IT SEEMS by first writing it on two lines in a zig-zag pattern (or rail fence). The ciphertext is produced by transcribing the first row followed by the second row.

N T I G S S T E M
O H N I A I S E S

Ciphertext: NTIGS STEMO HNIAI SES.

To decrypt, we write half the letters on one line, half on the second.

Decipher MKHSE LWYAE ATSOL. Solution: Since there are 15 letters, we write 8 on the top line and 7 on the bottom line so that

M K H S E L W Y
A E A T S O L

Plaintext: MAKE HASTE SLOWLY.