Bachelor of Science in Computer Science

Information & Network Security

Sem 5 (NOV-2022) Subject Code: 82904

Ql. Attempt All (10 Marks)

(a) Multiple Choice Questions:

i) Which of the following is not an example of a substitution cipher?
a) Caesar cipher
b) Playfair cipher
c) Rail Fence cipher
d) Hill cipher

ii) A deliberate attempt to evade security services is called_____.
a) threat
b) attack
c) masquerade
d) repudiation

iii) Which security protocol is used at the transport Layer?
a) IPSec
b) PGP
c) SMIME
d) SSL

Iv) A digital signature needs a(n)_____system.
a) symmetric-key
b) asymmetric-key
c) private key

d) session key

v) which or the following is a means to access a Computer program or entire computer system bypassing all security mechanisms?
a) Backdoor
c) Phishing
b) Masquerading
d) Trojan Horse.

vi) Passive attacks do not include
a) modification of data stream
b) obtaining the information that is being Transmitted
c) eavesdropping on transmission
d) the possibility of replay attack in future.

vii) Public key encryption is also known as _____.
a) asymmetric encryption
b) symmetric Encryption
c) single encryption
d) Super encryption

viii) PKI stands for _____.
a) Parent Key Interface
b) Public Key Infrastructure
c) Protocol Key Infrastructure
d) Private Key Infrastructure

ix) AES has _____different configurations.
a) one
b) three
c) four
d) five

x) One commonly used public-key cryptography is the_____ algorithm.
a) RSS
b) RAS
c) RSA

d) RAA

(b) Fill in the blanks

(hashing, 64,128, shared secret, steganography, cryptanalysis, transposition)

i) **transposition** ciphers hide the message by rearranging the letter order without altering the actual letter used.

ii) SHA is a **hashing** algorithm.

iii) **steganography** is an alternative to encryption which hides the very existence of a message by some means.

iv) DES is a non-Feistel cipher that encrypts a data block of **64** bits.

v)Private key cryptography uses a **shared secret**.

Q.2 Attempt the following (Any THREE)(Each of 5Marks) (15M)

a) What is the CIA triad? Explain in detail. (5M)

Answer]

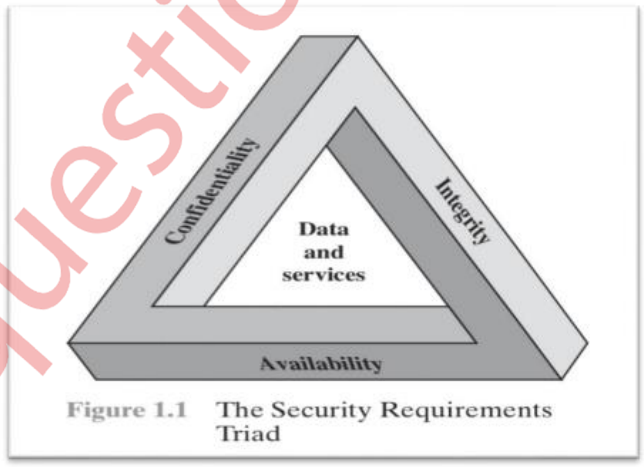


Figure 1.1 The Security Requirements Triad

- The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/ data, and telecommunications). These three concepts form what is often referred to as the CIA triad.

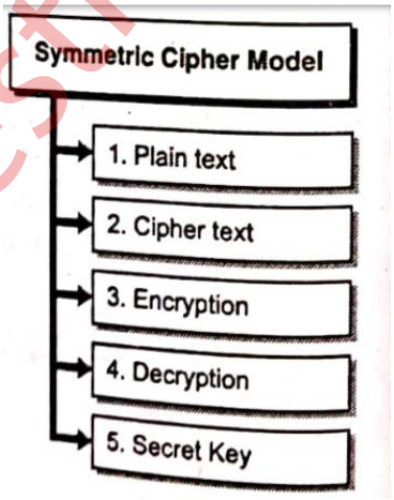
- **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
- **Integrity:** Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.
- **Availability:** Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

---

b) Explain symmetric cipher model. Discuss different techniques used in traditional ciphers. (5M)

Answer]

A symmetric encryption scheme has five ingredients :



- **Plaintext:** This is the original intelligible message or data that is fed into the algorithm as 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 and of the algorithm. 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.
- **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.
- **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

Examples of different techniques used in traditional symmetric ciphers:

1. **Caesar Cipher:** One of the earliest known ciphers, it involves shifting each letter of the plaintext by a fixed number of positions down the alphabet.
2. **Playfair Cipher:** It uses a 5x5 matrix of letters (excluding 'J') to encrypt messages in pairs of letters from the plaintext.
3. **Vigenère Cipher:** A polyalphabetic substitution cipher that uses a keyword to apply different Caesar ciphers to the plaintext.
4. **Hill Cipher:** A matrix-based cipher that operates on groups of letters using matrix multiplication.
5. **Rail Fence Cipher**: A transposition cipher that rearranges the letters of the plaintext in a zigzag pattern.

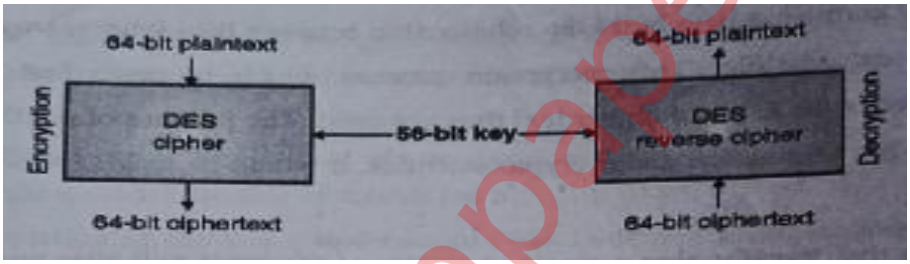
---

c) Explain DES cipher in detail. (5M)

Answer]

- In the year 1971, IBM developed an algorithm called LUCIFER that operated on a block of 64 bits using a 128-bit key.
- Later on, Walter Tuchman, an IBM researcher refined the LUCIFER algorithm and reduced the key size to 56-bit so as to fit on a chip.

- And, then in 1977 as a result of progress in Tuchman's research, his project was adopted as the Data Encryption Standard by IBM.
- DES is the most popular private key encryption technique adopted by industries to have secure communication. For example, DES is used to encrypt personal identification numbers (PINs) and account transactions in ATMs, used by Clearing House Interbank Payments System (CHIPS) to authenticate the transactions involving over $1.5x per week.
- DES is the combination of substitution and transposition (permutation) techniques developed to obtain a more secured encryption algorithm.
- DES encrypts and decrypts 64-bit data blocks through many stages of transposition and substitution using a 56-bit encryption key. It takes a 64-bit block of plaintext as input and outputs a 64-bit block of ciphertext.

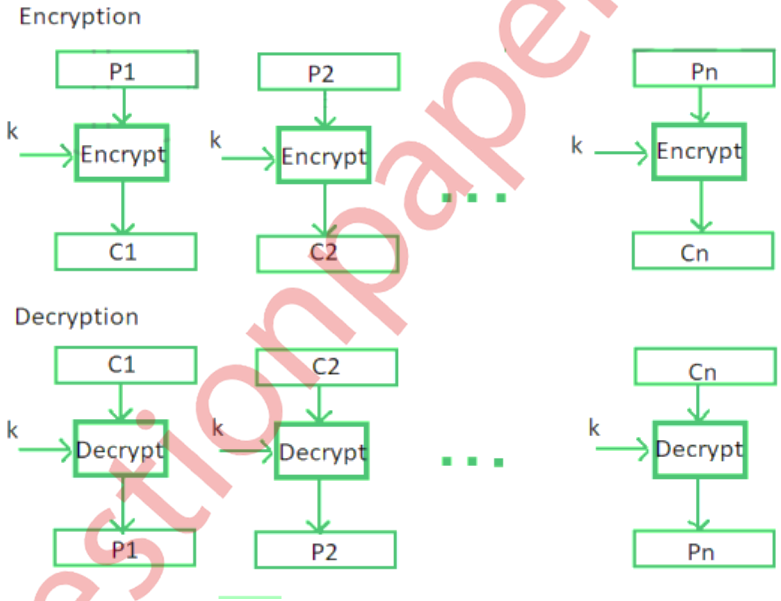


- With Private Key Encryption technique. the key is known both to sender and receiver even if it is a This is known as Secret key cryptography or Symmetric Key cryptography and it is usually categorized either stream ciphers or block ciphers.
- **Stream Cipher :** These operate On a single bit (or byte) at a tin-r and the mechanism changes the key constantly. As the key is changed constantly, the plain text is encrypted to different cipher-text each time.
- **Block Cipher :** As the name implies, these on one block Of data at a time using same key on each block. Here, a message is broken into a block of 64 bits for processing. If the last block is not 64 bits long, dummy bits (padding bits) are added to make it a 64- bit block. As the same key is used, the plain text block is always encrypted to same cipher-text.
- DES has 16 rounds i.e. the main algorithm is repeated 16 times before producing the ciphertext- It is found that the number of rounds is exponentially proportional to the amount Of time required to find a key using a brute-force attack. Therefore, as the number of rounds increases, the security the algorithm also increases exponentially.

d) Explain ECB block cipher mode of operation with its advantages and limitation. (5M)

Answer]

- 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 bunch of blocks and the procedure is repeated.
- Procedure of ECB is illustrated below:



Advantages of using ECB –

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

Limitation of using ECB –

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

e) Explain the differences between symmetric and asymmetric cryptograph

(5M)

Answer]

Symmetric Key Cryptography (Secret-Key Cryptography)	Asymmetric Key Cryptography (Public-Key Cryptography)
1) It only requires a single key for both encryption and decryption.	1) It requires two keys, a public key and a private key, one to encrypt and the other one to decrypt.
2) The size of cipher text is the same or smaller than the original plain text.	2) The size of cipher text is the same or larger than the original plain text.
3) The encryption process is very fast.	3) The encryption process is slow.
4) It only provides confidentiality.	4) It provides confidentiality, authenticity, and non-repudiation.
5) The length of key used is 128 or 256 bits.	5) The length of key used is 2048 or higher.
6) It can not be used in digital signature.	6) It can be used in digital signature.
7) Examples: 3DES, AES, DES and RC4.	7) Examples: Diffie-Hellman, ECC, El Gamal, DSA and RSA.

---

f) Discuss different categories of security services as per X-800 recommendations. (5M)

Answer]

- Security mechanisms are used to implement security services.
- They include X-800

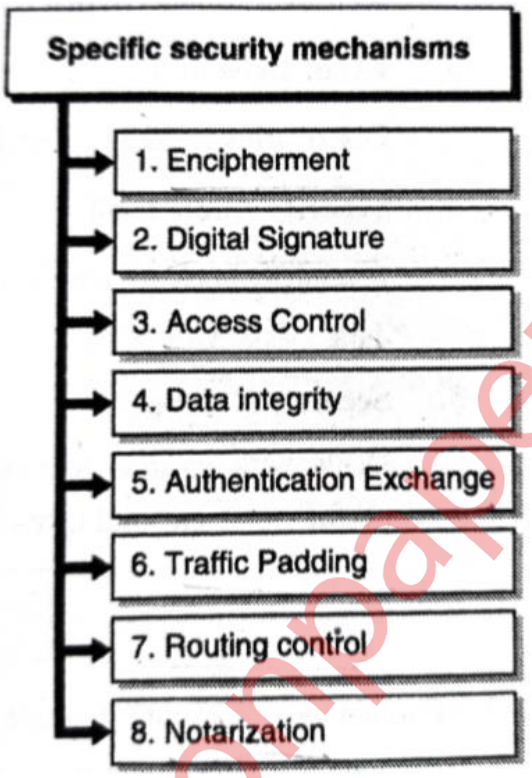
Specific Security Mechanisms :

- May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

Pervasive Security Mechanisms

- Mechanisms that are not specific to any particular OSI security service or protocol layer

➢ Specific security mechanisms are as follows



1. Encipherment
   - Algorithms based on mathematics are used to convert data into a form that is not easily comprehensible.
   - The conversion and recovery of data depends on these algorithms and also on encryption keys.

2.Digital Signature
   - Cryptographic alteration of data allows receiver of the message to prove the source and integrity Of message and guard against counterfeit attacks.

3.Access Control
   - Kinds of mechanisms which determines who should be able to access what resources.

4.Data integrity
   - Kinds of mechanisms used to maintain the originality of data or to keep-data intact till it reaches destination.

5.Authentication Exchange

- Kinds of mechanisms used to ensure originality of user by means of information exchange.

6.Traffic Padding

- Appending of data bits into gaps of a data flow to prevent traffic analysis attempts.

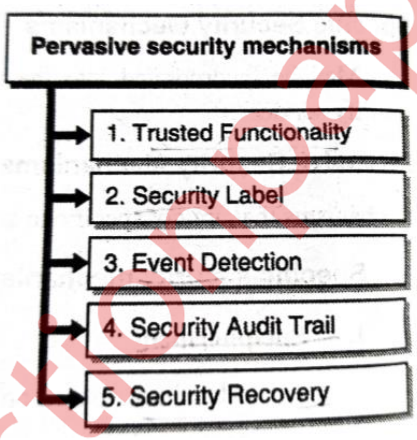
7.Routing control

- Allows selecting secure route for confident data and also enables routing modifications when violation to security

8.Notarization

- To guarantee particular features of data exchange, trusted third party is used

➢ Pervasive security mechanisms are as follows :



1.Trusted Functionality

- It is appeared to be correct regarding some criteria.

2.Label

- The indicator to a resource which specifies security attributes of that resource.

3.Event Detection

- Discovering security related events.

4.Audit Trail

- A security audit to review and observe system activities and records is performed on collected data

5.Security

- Deals with various requests sent by other mechanisms like function management, event performance etc. and takes necessary recovery actions.

Q.3. Attempt the following (Any THREE) (Each Of 5Marks) (15M)
a) Explain key generation process in Diffie-Hellman key exchange algorithm. (5M)

Answer]

- The Diffie-Hellman key exchange algorithm is produces a session key.
- This algorithm solves problem of key agreement between sender and receiver or exchange of keys between communication parties.
- In this cryptographic keys are securely exchanged over a public channel.
- This method is used for two parties who are unknown to each other, jointly create a secret key over an insecure medium.
- Symmetric key is generated which is agreed by both the parties taking part in communication.
- generated key is used for encryption and decryption mechanism.

Advantages of Diffie-Hellman Key

- Parties involved in communication do know each other.
- Communication can be possible in an insecure channel.
- Secret key sharing is a safe process.

Disadvantage of Diffie-Hellman Key

- Asymmetric key exchange not supported
- Signing of digital signature is not possible.
- Suffers from Man in the middle attacks as it never authenticates the parties involved in communication.
- To implement Diffie-Hellman, the two end users Alice and Bob. who are unknown to each other while communicating over a channel, jointly agree on positive prime numbers n and g.
- When Alice and Bob have agreed on n and g in private, they select positive random number keys x and y, both less than the prime number.

The steps are as follows

- S and R jointly agree on two large prime numbers n and g.

- S chooses one more large random number x, and calculate A such that
- A = gx mod n
- S forwards number A to R.
- R also chooses one more large random number y, and calculate B such that
- B = gy mod n
- R forwards B to S.
- S computes secret kl as kl = Bx mod n
- R computes secret key k2 as k2 = Ay mod n

---

b) Discuss different approaches of distribution of public key in public key cryptography. (5M)

Answer]

1. Public Key Infrastructure (PKI): PKI is a system that manages the generation, distribution, storage, and revocation of digital certificates. It provides a trusted framework for verifying the authenticity of public keys. In PKI, a Certificate Authority (CA) digitally signs the public key of an entity, binding it to that entity's identity. Users can verify the authenticity of the public key by checking the digital signature against the CA's root certificate.
2. Key Exchange Protocols: Key exchange protocols enable parties to securely exchange public keys during communication setup. Some common key exchange protocols include: a) Diffie-Hellman Key Exchange: Allows two parties to establish a shared secret key over an insecure channel without directly transmitting the key. b) Elliptic Curve Diffie-Hellman (ECDH): A variant of Diffie-Hellman that uses elliptic curve cryptography for key exchange.
3. Self-Signed Certificates: In small-scale or closed systems, self-signed certificates can be used to distribute public keys. In this approach, the entity generates its own certificate, containing the public key, and signs it with its private key. While this doesn't offer the same level of trust as PKI, it can be sufficient for certain scenarios.
4. Direct Exchange: In some cases, users can exchange public keys directly with each other through secure means like in-person meetings, phone calls, or secure messaging platforms. While effective for small-scale scenarios, this approach becomes challenging for large-scale or distributed systems.

5. Directory Services: Organizations or communities can maintain centralized directories where public keys are stored and can be looked up by other users. LDAP (Lightweight Directory Access Protocol) is commonly used for this purpose.
6. Key Escrow: In certain applications, key escrow services can be used. Trusted third parties hold a copy of users' private keys, allowing recovery in case of key loss or other emergencies. However, this approach raises concerns about data privacy and security.

---

c) What is Message authentication? Discuss different approaches that can be used to achieve message authentication. (5M)
Answer]

Message authentication is a fundamental aspect of information and network security that ensures the integrity and authenticity of a message or data transmitted between parties. It verifies that the message has not been altered, corrupted, or tampered with during transmission and confirms the identity of the sender. Achieving message authentication is crucial to prevent unauthorized access, data manipulation, and impersonation in communication.

Different approaches that can be used to achieve message authentication include:

1. **Message Authentication Codes (MAC):** A Message Authentication Code is a cryptographic tag generated using a secret key and the contents of the message. The MAC is appended to the message and sent along with it. Upon receipt, the recipient recalculates the MAC using the same secret key and verifies it against the received MAC. If they match, it indicates that the message has not been altered and is authentic. HMAC (Hash-based Message Authentication Code) is a widely used MAC construction that combines a cryptographic hash function with a secret key.
2. **Digital Signatures:** Digital signatures use public-key cryptography to provide message authentication and non-repudiation. The sender creates a digital signature by encrypting a hash of the message using their private key. The recipient can verify the signature using the sender's public key. If the

signature is valid, it confirms the message's authenticity and integrity and prevents the sender from denying their involvement in the message.

3. **Secure Hash Functions**: Secure hash functions, such as SHA-256 or SHA-3, are used to generate a fixed-size hash value (digest) from the message. The hash serves as a unique fingerprint of the message's content. By comparing the received hash with a recalculated hash of the received message, the recipient can ensure that the message has not been tampered with.
4. **Message Authentication using Block Ciphers**: Block ciphers, such as AES (Advanced Encryption Standard), can be used for message authentication. Techniques like Cipher Block Chaining Message Authentication Code (CBC-MAC) or Cipher-Based Message Authentication Code (CMAC) leverage block ciphers to generate authentication tags for the message.
5. **Public Key Infrastructure (PKI):** In PKI, digital certificates and public keys are used to authenticate messages. The sender signs the message using their private key, and the recipient verifies the signature using the sender's public key obtained from a trusted Certificate Authority (CA)

---

d) Explain various characteristics of Hash function. (5M)

Answer]

- Storing data in an array with the aim Of performing operations like sorting searching speedily is called as hashing.
- Unique key is needed to perform such operations with hashing.
- It finds correct location of a record by comparing the records also searching for the location of the element in array.
- **'Hash function'** is function that returns the position of the record in array and **'hash table'** is the array used to store records.
- It is very difficult to find out an appropriate hash function and its execution algorithm though it is essential for better table performance.
- A basic requirement is that the function must provide an equal distribution of hash values.
- Unequal distribution rises the number of collisions and efforts for undertaking them

Uses of Hash Tables

- Compilers use hash tables for symbol storage.
- Hash tables are used in disk based data indexing in Databases.
- Hash tables are used in high speed routing.
- Hash tables are used in many algorithms for speedily processing of data
- The Linux Kernel uses hash tables to manage memory pages and buffers.

Advantages of Hash Tables

- Synchronization
- More efficient than arrays. search trees or table lookup structure.
- Speedily access the data.

Need of Hashing

- Many application like search engines. web pages, social networking web sites deals with large amount of data.
- To search for a particular value from this massive amount of data we can use countless look ups. But they are time consuming.
- Data structures like arrays, linked list may not be efficient enough to handle sufficient searches.
- so efficient search techniques like hashing is used to minimize such comparisons and make the process fast.
- In hashing the searching depends upon the location of the record and not the location with respect to other keys.

---

e) Explain SHA algorithm. (5M)

Answer]

- Secure Hashing Algorithm known as SHA. is a group of cryptographic functions intended maintain data security.
- It functions by converting the data using a hash function which uses an algorithm that modular additions, compression functions and bitwise operations.
- Then the hash functions generated a fixed size string which is similar to original string.
- These algorithms are proposed to be one way functions i.e. it is virtually impractical to convert

- them into original form once they are altered into their corresponding hash values.
- Algorithms like SHA — l, SHA — 2, SHA — 5 are mainly developed with gradually stronger encryption with respect to hacker attacks.
- A basic application of SHA is encrypting passwords because rather than keeping track of actual password, the server side only has to maintain specific user's value.
- It is useful in case an attacker attacks on the database. as they will only get hashed function and not the real passwords, thus if the input is considered to be the hashed value as a password, it will be transformed into different string by the hash function and then it Also. SHA reveals the effect. where alteration Of Very limited encrypted letters affects a big change in output; or extremely dissimilar strings produce identical hash values.
- This result affects on hash values for not sharing any information about the input string like its original length.
- Moreover SHAS are also used to expose the altering of data by attackers. in car. if text file is altered to some extent and it is hardly noticed, updated file's hash and original file's hash value will be dissimilar. and thus tampering Of message will be perceptible.

Working of SHA

Step 1:Padding

- End of the original message is appended with padding in such a way that the message length is 64 bits smaller than the multiple of 512

Step 2: Append Length

- Calculation of message length eliminating padding length is appended as 64 bit block to end of padding.

Step 3 : Split the input into 512 bit blocks

- input is spilt into blocks of length 512 bits each.

Step 4 : Initialize chaining variables

- Initialization of A to E. chaining variables and their hexadecimal values are
- A:01 23 45 67
- B:89 ab cd ef
- C:fe dc ba 98
- D:76 54 32 10
- E:C3 D2 e1 f0

Step 5: process block

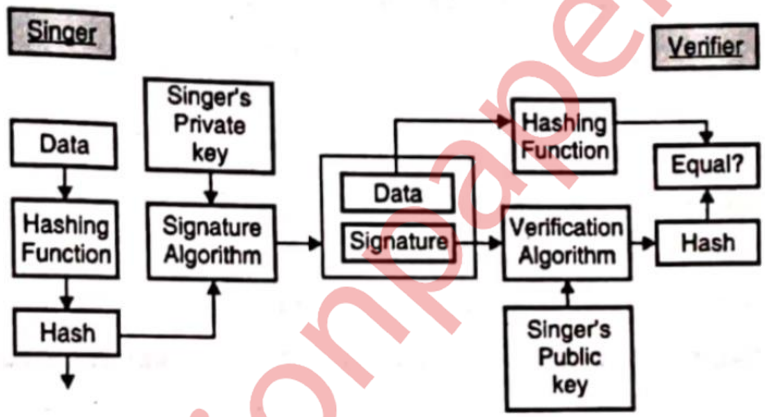
- To process blocks following steps are considered :

1. 1.five chaining variables copied into five variables a. b, c. d, e. Single register is considered for keeping temporary. intermediary and final result.
2. Separating current 512 bit block into 16 sub block each Of size 32 bit.
3. SHA supports 4 with 20 iterations so each 80 iterations and in each round processing Of an 16 sub blocks takes place.

---

f) Explain basic digital signature Model.What security requirements do you feel can be achieved in digital communication by using digital signature? (5M)

Answer]



- Every party involved in the process should have a public and private key pair.
- Basically, Different key pairs are used for the process of verifying /signing and encryption /decryption.
- Signature key is that is private key is used for signing and the verification key is the public key.
- Hash function data is provided to the signer and produces hash of data.
- The signature algorithm is then fed by the signature key and value.
- it generates digital signature on that particular hash.
- Data is appended by the signature.
- Both Signature and data are sent to the verifier.
- Verification algorithm is fed by the digital signature and the verification key by the verifier.
- Output is generated by the verification algorithm.

- To produce hash value, verifier executes same hash function on the data which is received.
- Output of verification algorithm and this hash value are compared for verification.
- The validity of digital signature is verified by the verifier which is based on comparison result.
- As signer generates digital signature by its own private key, he cannot in future deny about the document in future.

By using digital signatures in digital communication, the following security requirements can be achieved:

1. **Data Integrity:** Ensuring that the message remains unchanged and unaltered during transmission.
2. **Authentication:** Verifying the sender's identity, confirming the message's origin.
3. **Non-Repudiation:** Preventing the sender from denying sending the message.
4. **Secure Communication**: Enabling secure transmission over insecure channels.
5. **Tamper Detection:** Detecting any unauthorized modifications to the message.
6. **Public Key Infrastructure (PKI**): Providing a trusted framework for verifying public keys.

Q.4. Attempt the following (Any THREE) (Each Of 5Marks) (15M)

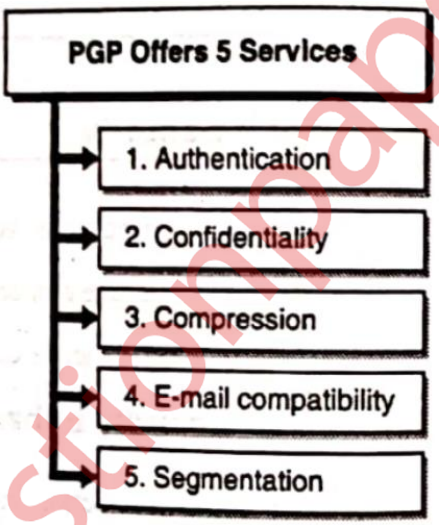
a) Discuss any one protocol which is used to add security email applications. (5M)

Answer]

- PGP stands for Pretty Good Privacy.
- Developed by Phil Zimmermann in 1991.
- Open-source, freely available software package for secure e-mail.
- It is the de facto standard for secure email.

- Runs on a variety of platforms like Unix, PC, Macintosh, and other systems, originally free (now also have commercial versions available).
- Documentation and source code are freely available.
- The package does not depend on any operating system and its processor
- Security for e-mail communication is achieved by combining the best cryptographic algorithms with PGP.
- Public-key cryptography is used by the users, and they generate a public key and private key pair.
- RSA with digital signatures or ElGamal with DSA algorithms are used.
- Symmetric key methods like Rijndael or Triple DES are used by all users

PGP offers following services:



1. **Authentication:** PGP offers authentication through digital signatures. Users can sign their outgoing emails using their private key, generating a digital signature that provides proof of the sender's identity. Recipients can verify the signature using the sender's public key, ensuring the message's authenticity and origin. Authentication helps prevent email spoofing and ensures that messages come from trusted sources.
2. **Confidentiality:** PGP achieves confidentiality through encryption. When sending an email, the sender can encrypt the message content using the recipient's public key. Only the recipient, who possesses the corresponding private key, can decrypt and read the message. Encryption ensures that the

message remains confidential and secure, protecting it from unauthorized access during transmission.

3. **Compression:** PGP includes compression as a service to optimize the transmission of encrypted messages. Before encrypting the email content, PGP can compress the data to reduce its size. Compression reduces the overhead of encryption and speeds up email transmission, especially for large attachments or lengthy messages.
4. **Email Compatibility:** PGP is compatible with various email clients and platforms. It can be seamlessly integrated into popular email programs, such as Microsoft Outlook, Mozilla Thunderbird, and Apple Mail, making it widely accessible to users across different systems. This compatibility ensures that PGP can be used efficiently and effectively by a broad user base.
5. **Segmentation:** PGP supports the segmentation of large files or messages into smaller chunks, known as "packets" or "radix-64 encoding." This segmentation ensures that large attachments or messages can be efficiently transmitted over email without running into size limitations imposed by email servers

---

b) What is SSL? Discuss its protocol stack. (5M)
Answer]

- SSL stands for Secure Socket Layer.
- An increasingly popular general-purpose solution is to implement security as a protocol that sits between the underlying transport protocol (TCP) and the application.
- The foremost example of this approach is the Secure Sockets Layer (SSL) and the follow-on Internet standard of SSL known as Transport Layer Security (TLS).
- Transport Layer Security (TLS) and its ancestor, Secure Sockets Layer (SSL), are cryptographic protocols.
- TLS and SSL provide communication security over the internet.
- It is Netscape-developed SSL.

SSL protocol stack:

1. Application Layer: The application layer represents the actual application that needs to communicate securely over the network. It could be a web browser, email client, or any other software that requires data security. The application initiates the SSL/TLS handshake process to establish a secure connection.
2. TLS Handshake Protocol: The TLS handshake protocol is responsible for negotiating the security parameters and setting up a secure connection between the client and the server. The handshake process involves several steps:
    - Client Hello: The client sends a Client Hello message to the server, indicating the TLS version and a list of supported cryptographic algorithms.
    - Server Hello: The server responds with a Server Hello message, selecting the TLS version and cryptographic algorithms from the client's list.
    - Key Exchange: The client and server exchange cryptographic keys and agree on a shared secret for encryption and decryption.
    - Authentication: The server presents its digital certificate to the client for authentication. The client validates the certificate, ensuring the server's identity.
    - Session Establishment: Both client and server exchange messages to establish a secure session using the agreed-upon parameters.
3. Record Protocol: The record protocol operates on top of the TLS handshake protocol and handles the encryption and decryption of data exchanged between the client and server. It takes the data from the application layer, divides it into smaller fragments, and adds a header that includes the necessary information for decryption. The record protocol then encrypts these fragments using the negotiated cryptographic keys before sending them over the network. On the receiving end, the record protocol decrypts the data and delivers it to the application layer.
4. Transport Layer: Below the record protocol, the secure data is transmitted over the network using standard transport layer protocols such as TCP (Transmission Control Protocol). The transport layer ensures the reliable and ordered delivery of data between the client and server.

c) What is a honeypot? How does it facilitate intrusion detection? (5M)

Answer]

1. Honeypots are traps set to detect attempts at any unauthorized use of information systems, with a view to learning from the attacks to further improve computer security.
2. Considering the classical field of computer security, a computer needs to be secure, but in the domain of Honeypots, the security holes are set to open on purpose.
3. Honeypots essentially turn the tables for hackers and computer security experts.
4. The main purpose of a Honeypot is to detect and learn from the attacks and further use the information to improve security.
5. Honeypots have long been used to track attackers' activity and defend against coming threats.
6. Monitoring the data that enters and leaves a honeypot lets the user gather information that is not otherwise available.
7. Honeypots are generally based on a real server, real operating system, along with data that looks like real

Intrusion detection by honey pots :

- These are trapped systems designed to trap an attacker away from critical systems.
- It distracts an intruder from accessing critical systems.
- Even it gathers information of attacker's activity.
- These systems are occupied with faked information appeared to be valuable but authorized user couldn't access. So any access to these systems is suspected.
- The systems are designed with event loggers and sensitive monitors who notice these accesses and gathers information regarding attacker's activities.

d) What do you understand about malware? Explain any two types of malicious program. (5M)

Answer]

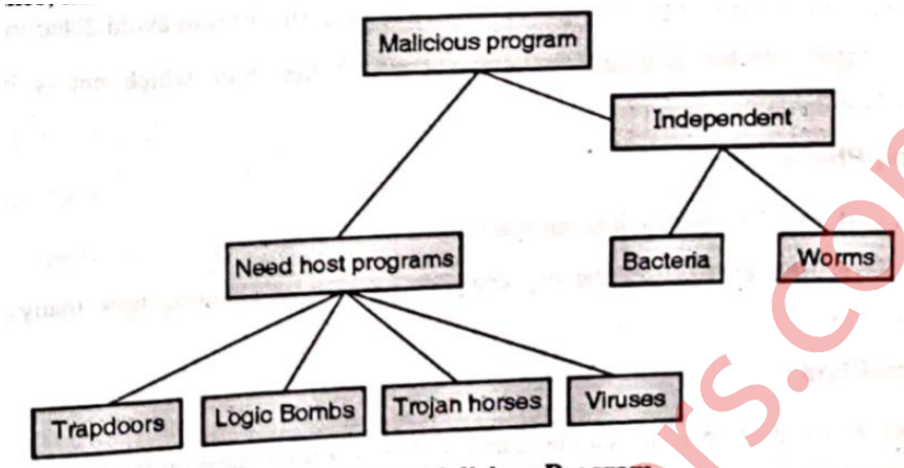


Fig. 12.1.1 : Malicious Program

- Malware means malicious software.
- These software help hackers to gather sensitive information, interrupt user's computer operations, and gain unauthorized access to the computer.
- It can be in the form of an annoying script or code or software.
- Viruses, spyware, Trojan Horses, Worms, and other malicious programs are examples of malware.
- Sometimes, malware can be genuine software which can be created by the company's official website.

Two types of malicious programs:

Viruses:

- Viruses are one of the most common types of malicious software. They are designed to replicate themselves and infect other files or programs on a computer.
- Once a virus infects a host file or program, it can spread to other files when the infected file is executed or shared. Viruses can propagate through email attachments, infected software downloads, or removable storage devices like USB drives.
- Viruses can cause various harmful effects, such as corrupting or deleting files, slowing down system performance, displaying unwanted messages, and even rendering the computer inoperable.

Spyware:

- Spyware is a type of malicious program that secretly gathers information about a user's online activities without their knowledge or consent.
- It can monitor web browsing habits, record keystrokes, capture login credentials, and collect personal information like passwords, credit card details, and browsing history.
- Spyware is often used for malicious purposes, such as identity theft, unauthorized access to sensitive data, and targeted advertising. It can also compromise user privacy by transmitting collected information to remote servers without the user's awareness.

---

e) Discuss the significance and limitations of firewalls. (5M)

Answer]

1. A firewall acts like a guard between your computer and the internet.
2. It checks if the traffic should continue on the network or stop towards sending to the destination.
3. It keeps unwanted access out and allows only designated traffic to enter or leave the computer.
4. Firewalls see each packet which enters into the network and leaves it.
5. It also determines packets based on their origin and destination point and also contents on it.

Limitations of Firewall are as follows:

1. The attacks which bypass the firewall are not protected by it.
2. No protection for internal threats or attacks.
3. Virus-infected programs cannot be protected.
4. Protection against authorized resources is not possible.
5. Social engineering attacks cannot be stopped.
6. Unauthorized users deliberately using access for unnecessary purposes cannot be stopped.

7. Attacks cannot be prevented if traffic does not pass through it.
8. They are only effective for the rules which they are designed to impose.

---

f) What is the SET protocol? What business requirement does it fulfil? (5M)

Answer]

- SET protocol is a standard protocol developed by Master card and Visa for protecting transaction over unprotected networks.
- SET is not a payment systems it is a set of security which allows users to use credit card payment framework securely in an open network.
- SET basically provides security for financial transaction over internet.
- In SET process, an electronic wallet is given to the user and then he conducts the transaction which then authenticated using digital signature and digital certificates among a merchant, the purchaser and its bank in such a way that it ensures confidentiality and privacy. SET uses SSL.

SET provides 3 services that are:

- Provides a communications channel among all parties involved in a e-commerce transaction.
- Provides trust by use of X.509v3 digital certificates .
- Ensures confidentiality. because information is only available to parties in a transaction when And where necessary.

Business requirement SET fulfil:

- Provides confidentiality of payment and ordering information.
- Ensure integrity of all transmitted data.
- Provides authentication that a cardholder is a legitimate user of a credit card account.
- Provides authentication that a merchant can accept credit card transactions through its relationship with a financial institution.
- Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction.
- Create a protocol that neither depends on transport security mechanism nor prevents their use.

- Facilitate and encourage interoperability among software and network providers.

Q.5. Attempt the following (Any FIVE) (Each Of 3Marks) (15M)

a) What is asymmetric key cryptography? Discuss its various applications.(3M)

Answer]

- Asymmetric key systems use 'two keys' - a public key known to everyone is used to encrypt the data, and a private key used for decryption is known only by the authorized recipient of the message.
- Because a pair of keys is required, this approach is also called asymmetric cryptography.
- These two keys are associated with an entity whose identity needs to be authenticated electronically, i.e. it needs to be signed or encrypted.
- In this type of cryptography, the public key is published to all the users, but the corresponding private key is kept secret.
- Here, the data is encrypted using the public key but decrypted only with the private key.

Application of Public Key Cryptography:

- Public key cryptography provides encryption and authentication for e-mail and file storage applications.
- It also provides data compression, encryption, digital signature, and email compatibility.
- It is also used in the timestamping technique where an encryption model is used to certify an electronic document or communication and delivered within a specific amount of time.
- Encryption is used in electronic money patterns to secure transactional data like transaction amounts, account numbers, passwords, digital signatures, etc.
- Secure Socket Layer (SSL) uses the RSA public key cryptosystem for authentication. Kerberos uses an authentication scheme which uses secret key ciphers for authentication and encryption.

b) Explain rail fence cipher with proper example.(3M)

Answer]

- The rail fence technique, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows. For example, to encipher the message “meet me after the toga party” with a rail fence of depth 2, we write the following:
  m e m a t r h t g p r y
  e t e f e t e o a a
- The encrypted message isThis sort of thing would be trivial to cryptanalyze. A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns. The order of the columns then becomes the key to the algorithm. For example
  ,
  Key: 4 3 1 2 5 6 7
  Plaintext: a t t a c k p
  o s t p o n e
  d u n t i l t
  w o a m x y z

- Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ
- Thus, in this example, the key is 4312567. To encrypt, start with the column that is labeled 1, in this case column 3.Write down all the letters in that column. Proceed to column 4, which is labeled 2, then column 2, then column 1, then columns 5, 6, and 7.
- A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext. For the type of columnar transposition just shown, cryptanalysis is fairly straightforward and involves laying out the ciphertext in a matrix and playing around with column positions. Digram and trigram frequency tables can be useful.
- The transposition cipher can be made significantly more secure by performing more than one stage of transposition.The result is a more complex permutation thatis not easily reconstructed. Thus, if the foregoing message is reencrypted using the same algorithm,

Key: 4 3 1 2 5 6 7
Input: t t n a a p t
m t s u o a o
d w c o i x k
n l y p e t z

- Output: NSCYAUOPTTWLTMDNAOIEPAXTTOKZ

- To visualize the result of this double transposition, designate the letters in the original plaintext message by the numbers designating their position. Thus,with 28 letters in the message, the original sequence of letters is
  01 02 03 04 05 06 07 08 09 10 11 12 13 14
  15 16 17 18 19 20 21 22 23 24 25 26 27 28

- After the first transposition, we have

  03 10 17 24 04 11 18 25 02 09 16 23 01 08
  15 22 05 12 19 26 06 13 20 27 07 14 21 28
- which has a somewhat regular structure. But after the second transposition, we have
  17 09 05 27 24 16 12 07 10 02 22 20 03 25
  15 13 04 23 19 14 11 01 26 21 18 08 06 28
- This is a much less structured permutation and is much more difficult to cryptanalyze.

---

c) Briefly explain Man in middle attack. (3M)

Answer]

- A Man-in-The-Middle (MiTM) attack is a type of cyberattack in which the attacker secretly intercepts and relays messages between two parties who believe they are communicating directly with each other.
- The main objective behind these attacks is to steal financial information by intercepting a user's traffic to a banking or financial website.
- Man-in-the-middle attack is also called a Brute-force attack. It involves tricking individuals into surrendering their keys.

- The cryptanalyst/attacker places himself in the communication channel in the middle of the two parties who wish to exchange their keys for secure communication.
- The cryptanalyst then performs a key exchange with each party, and the original parties believe that they are exchanging keys with each other's partner.
- Finally, the cryptanalyst comes to know about the keys.
- The attack is a type of eavesdropping in which the attacker intercepts and then controls the entire conversation.
- MiTM attacks are also sometimes referred to as monster-in-the-middle, machine-in-the-middle, monkey-in-the-middle, and man-in-the-browser attacks.
- MiTM cyberattacks pose a serious threat to online security because they give the attacker the ability to capture and manipulate sensitive personal information - such as login credentials, account details, or credit card numbers - in real-time.
- Man-in-the-browser is the most common type of MiTM attack in which the attackers focus on browser infection and inject malicious proxy malware into the victim's device.

---

d) What is kerberos? Explain its different components. (3M)

Answer]

- Kerberos is a Network Authentication Protocol.
- It ensures strong authentication for all client-server applications.
- To provide strong authentication, it uses secret key cryptography.
- It is an authentication service.
- It provides very high security for physically insecure networks.
- It also provides a centralized authentication server, which authenticates users to servers and servers to users.
- Rather than using public key encryption, it depends on conventional encryption.

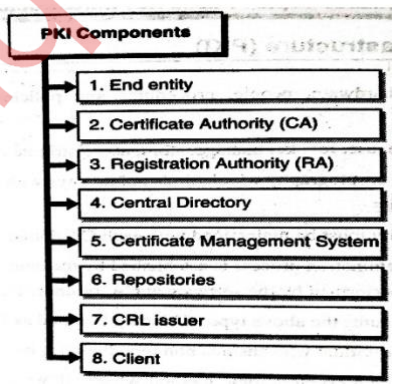
Components of Kerberos:

- Principal: any users, computers, and services provided by servers need to be defined as Kerberos Principals.
- Instances: are used for service principals and special administrative principals.
- Realms: the unique realm of control provided by the Kerberos installation. Think of it as the domain or group your hosts and users belong to. Convention dictates the realm should be in uppercase. By default, ubuntu will use the DNS domain converted to uppercase (EXAMPLE.COM) as the realm.
- Key Distribution Center: (KDC) consist of three parts, a database of all principals, the authentication server, and the ticket granting server. For each realm there must be at least one KDC.
- Ticket Granting Ticket(TGT): issued by the Authentication Server (AS), the Ticket Granting Ticket (TGT) is encrypted in the user's password which is known only to the user and the KDC.
- Ticket Granting Server: (TGS) issues service tickets to clients upon request.
- Tickets: confirm the identity of the two principals. One principal being a user and the other a service requested by the user. Tickets establish an encryption key used for secure communication during the authenticated session.
- Keytab Files: are files extracted from the KDC principal database and contain the encryption key for a service or host.

---

e) Explain the key elements of public key infrastructure. (3M)

Answer]



1. **End entity:** Consumes and supports PKI services. The end entity represents users, resources, or any entity specified in the subject of a digital certificate.
2. **Certificate Authority (CA):** Issues and verifies digital certificates. It supports various administrative functions related to managing certificates, such as issuing, renewing, and revoking certificates.
3. **Registration Authority (RA):** Verifies the identity of users requesting information from the CA and assists in the process of certificate enrollment.
4. **Central Directory**: A secure location to store and index keys and certificates within the PKI infrastructure.
5. **Certificate Management System:** Sign and encrypt digital documents, manage certificates, and handle various PKI-related operations.
6. **Repositories:** Store and make available certificates and Certificate Revocation Lists (CRLs). CRLs are lists of revoked certificates issued by CAs.
7. **CRL (Certificate Revocation List) Issuer:** An optional component that a CA can delegate to publish CRLs.
8. **Client:** Validates the digital signatures and their certification path using a known public key of a trusted CA

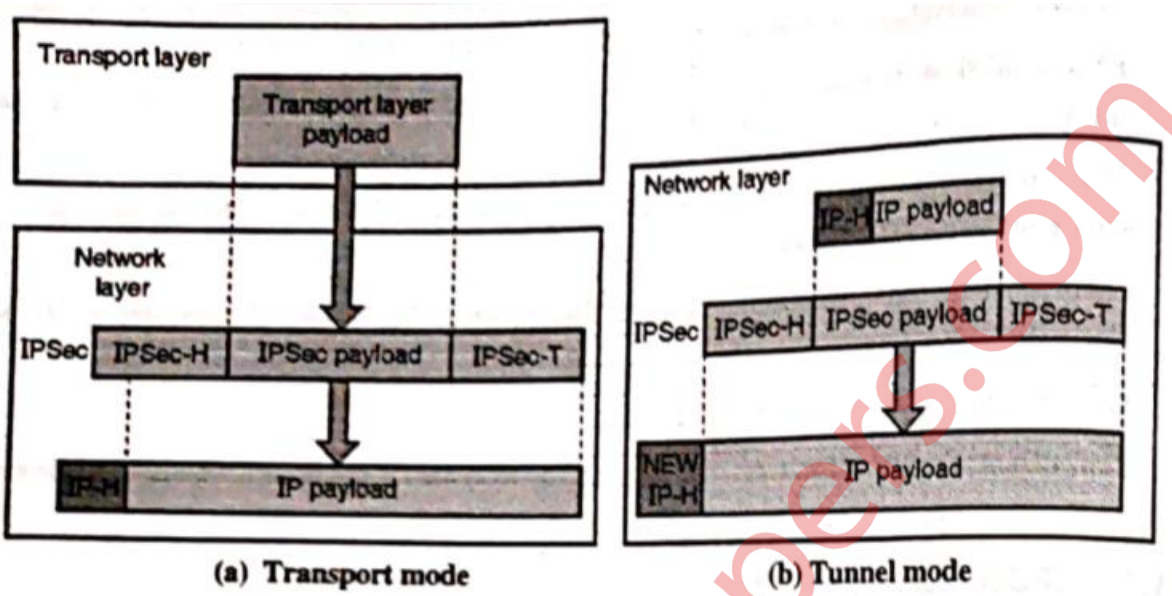
---

f) Discuss IPSec protocol with its different modes of operation. (3M)

Answer]

- IPSec stands for Internet Protocol Security.
- IPSec is a set of protocols and services that provide a comprehensive security solution and multiple protection types for IP networks.
- IPSec enables secure communication across a Local Area Network (LAN), private and public Wide Area Networks (WANs), and the Internet. It ensures the confidentiality, integrity, and authentication of data transmitted over IP-based networks, making it an essential technology for securing sensitive information and ensuring secure communication between network nodes.

Modes of operations :



(a) Transport mode (b) Tunnel mode

Transport Mode :

- In IPSec the data that is transferred from transport layer to network layer therefore. Protecting the payload that is to be encapsulated within the network layer.
- In this mode. IPSec reader and trailer are added to the information coming from the transport layer. IP header is added later on.

Tunnel Mode:

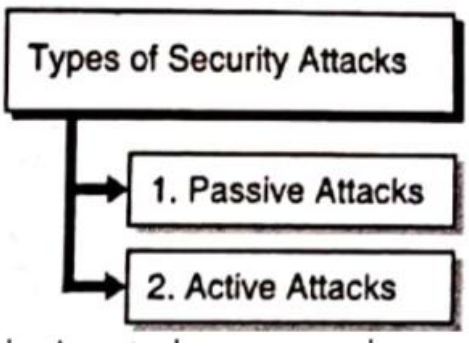
- The entire IP is protected by IPSec.
- It obtains an IP packet containing the header and applies IPSec security methods on it. It updates it With a new IP .
- The updated IP header contains different information than original one.
- This mode is basically used between two routers, between a router and a host ,between a host and a router.
- Tunnel mode is used for a host who are neither sender nor receiver.
- Between sender and receiver the whole original packet is protected from invasion.
- It seems like entire packer transmits through an imaginary tunnel.

g) What do you understand attacks? Discuss different types of attacks. (3M)

Answer]

- An attempt to gain unauthorized access to information resources or services or to cause harm or damage to information systems.
- Any form of malicious actions taken to harm the security of information system components.

Types of Attack :



Active Attacks:

- Active attacks are aggressive and involve direct interaction with the target system or network to modify, disrupt, or gain unauthorized access to data or services.
- These attacks are more intrusive and can cause significant damage to the target. They may be easier to detect because they leave traces of their presence.
- Examples of active attacks include:
- Malware attacks that infect the target system, such as viruses, worms, Trojans, and ransomware.
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks that overwhelm a target's resources, making services unavailable to legitimate users.
- Man-in-the-Middle (MitM) attacks, where an attacker intercepts and alters communication between two parties.
- Data modification attacks, where an attacker modifies or deletes data on the target system.

Passive Attacks:

- Passive attacks are more covert and involve monitoring, eavesdropping, or analyzing data without directly modifying or disrupting the target system or network.
- These attacks are often difficult to detect as they leave little to no trace of their presence.
- Passive attacks are primarily focused on gathering information, such as sensitive data or confidential communications, without the target's knowledge.
- Examples of passive attacks include:
- Eavesdropping on network traffic to intercept and capture data, such as passwords, credit card numbers, or confidential messages.
- Packet sniffing, where an attacker captures and analyzes data packets transmitted over a network to gain insights into the network's structure or vulnerabilities.
- Traffic analysis, where an attacker analyzes patterns in network traffic to infer sensitive information, such as user behavior or the structure of a communication network.

---

h) Explain the process of encryption and decryption using caesar cipher for plaintext "attack at dawn".(3M)

Answer]

Plain Text (p)	(p + 3) mod 26	Cipher Text
A	(0 + 3) mod 26	D
T	(19 + 3) mod 26	W
T	(19 + 3) mod 26	W
A	(0 + 3) mod 26	D
C	(2 + 3) mod 26	F
K	(10 + 3) mod 26	N

A	**(0 + 3) mod 26**	**D**
T	**(19 + 3) mod 26**	**W**
D	**(3 + 3) mod 26**	**G**
A	**(0 + 3) mod 26**	**D**
W	**(22 + 3) mod 26**	**Z**
N	**(13 + 3) mod 26**	**Q**

Encryption:

1. The plaintext "attack at dawn" is converted to uppercase: "ATTACKATDAWN."
2. Each letter in the plaintext is replaced by the corresponding letter in the "Cipher Text" column.
3. Plain Text: A T T A C K A T D A W N Cipher Text: D W W D F N D W G D Z Q
4. The encrypted ciphertext using Caesar cipher with a shift of 3 positions is "DWWDFNDWGZQ."

Decryption:

1. To decrypt the ciphertext "DWWDFNDWGZQ" back to the original plaintext "attack at dawn," we need to reverse the Caesar cipher process. We need to find the plaintext letters that correspond to the ciphertext letters in the "Cipher Text" column of the box.
2. Ciphertext: D W W D F N D W G D Z Q Plain Text: A T T A C K A T D A W N
3. The decrypted plaintext using Caesar cipher with a shift of 3 positions is "attack at dawn."