IV - B.TECH - I Semester End Exam (Reg) - Dec-2025

PART-A INFORMATION SECURITY (R22IT702PC)

1) a) Information security is the Practice of Protecting Information and Information systems from unauthorized access, use, disclosure, disruption, modification or destruction. it aims to ensure the confidentiality, Integrity and availability of data by using technical, physical and administrative controls to mitigate risks. This Includes safeguarding information in both digital and physical forms from threats like cyberattacks and data breaches.

1) b) In Information Security, random number generation is the Process of creating sequences of numbers that are unpredictable and cannot be reasonably guessed by an attacker. These numbers are crucial for cryptographic Operations; such as generating keys, session tokens and which are essential for securing Communications, data encryption and authentication systems.

There are two main types:

① True random number generators

② Pseudo-random number generators.

:) c) The key management system outlines the stages through which cryptographic keys are generated, used and eventually retired or destroyed. Proper management of these keys is critical to ensuring the security of cryptographic systems.

1. Key Generation:

. Creation: Keys are created using secure algorithms to ensure randomness and strength.

. Initialization: Keys are initialized with specific parameters required for their intended and use.

2. Key Distribution:

. Sharing: For symmetric keys, secure methods must be used to share the key b/w parties.

. Publication: For asymmetric keys, the public key is shared openly, while the private key remains confidential.

3. Key storage:

. protection: Keys must be stored securely, typically in hardware security modules (HSMs) or encrypted key stores, to prevent unauthorized access.

. Access control: only authorized users or systems should be able to access keys.

4. Key Usage:

. Application: keys are used for their intended cryptographic functions, such as encryption / decrypting data or

. Monitoring: Usage is monitored to detect any unusual or unauthorized activities.

1) d) Authentication Protocols are sets of rules and procedures used to verify the identity of a user, device or system to ensure it is who it claims to be. They are crucial for secure communication by establishing that the entities communicating are legitimate, which is a prerequisite for access control.
Examples include Kerberos which uses a ticket system for secure authentication in a n/w and SAML, which is an XML-based framework used for single sign-on (SSO) in web applications.

1) e) Digital signature:
A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, s/w or digital document. These are some of the key features of it.
- key generation Algorithms:
- signing Algorithms
- signature Verification Algorithms.

Digital signatures and certificates are two key technologies that play an important role in ensuring the security and authenticity of online activities.

1) f) PGP - Authentication and confidentiality

Pretty Good Privacy (PGP) is an encryption software designed to ensure the confidentiality, Integrity and authenticity of virtual communications and Information. It is considered as one of the best methods for securing digital facts.

The following are the services offered by PGP.

1. Authentication
2. Confidentiality
3. Email Compatibility
4. Segmentation

1) g) Define IP security

IP Security refers to a collection of communication rules or Protocols used to establish secure network connections. Internet Protocol (IP) is the common standard that controls how data is transmitted across the Internet. IPsec enhances the Protocol security by introducing encryption and authentication. IPsec encrypts data at the source and then decrypts it at the destination. It also verifies the sources of the data.

1) h) Secure Electronic Transaction is a Security Protocol designed to ensure the security and integrity of electronic transactions conducted using credit cards. It uses different encryption and hashing techniques to secure payments over the Internet done through credit cards. SET Protocol restricts the revealing of credit card details to merchants thus keeping hackers and thieves at bay. The SET Protocol includes Certification Authorities by making use of standard Digital certificates like X509 certificate.

1) i) A computer virus is a type of malicious software program that, when executed, replicates itself by modifying other computer programs and inserting its code, when this replication succeeds, the affected areas are then said to be "infected". Viruses can spread to other computers and files when the sw or documents they are attached to are transferred from one computer to another using a network.

1) j) A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. it acts as a barrier between a trusted internal network and untrusted external networks, such as the internet, to protect against unauthorized access and cyber threats. Firewalls can be h/w, s/w or both and they function by inspecting data packets and they function by inspecting data packets and allowing

2) The OSI (open systems interconnection) security architecture provides a systematic framework for defing security attacks and services.

- Security attacks are classified as either Passive attacks which include unauthorized reading of a message of file and traffic analysis and active attacks such as modification of messages or files and denial of service.

Security Attacks

A useful means of classifying security attacks, used both in X.800 and RFC 2828, is in terms of passive attacks and active attacks. A Passive attack attempts to learn or make use of information from the system but does not affect system resources. An active attack attempts to alter system resources

Passive Attacks

Passive attacks are in the nature of eavesdropping on or monitoring of transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of Passive attacks are release of message contents and traffic analyses.

The release of message contents is easily understood. A telephone conversation, an electronic mail message and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

A second type of Passive attack, traffic analysis, is subtler. Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent might still be able to observe the Pattern of these messages. The opponent could determine the location and identity of communicating hosts 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. Passive attacks are very difficult to detect because they do not involve any alteration of the data. Typically, the message traffic is sent and received in an apparently normal fashion and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic Pattern. However, it is feasible to prevent the success of these attacks, usually by means of encryption. Thus, the emphasis in dealing with Passive attacks is on Prevention rather than detection

Active Attacks

Active Attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

A masquerade takes place when one entity Pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack.

Authentication sequences can be captured and replayed after a valid authentication sequence has taken place; thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges. Modification of messages simply means that some portion of a legitimate message is altered or that messages simply means ~~that some portion of~~ of are delayed or reordered, to produce an unauthorized effect. For example, a meaning for message "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred brown to read confidential file accounts.". The denial of service prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target, for example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire n/w, either by disabling the n/w or by overloading it with messages so as to degrade performance.

Active attacks present the opposite characteristics of passive attacks. whereas passive attacks are difficult to detect, measures are available to prevent active attacks obsolutely, because of the wide variety of potential physical, s/w and n/w either by disabling the n/w or by overloading it with messages so as to degrade performance.

Active attacks present the opposite characteristics of passive attacks. whereas passive attacks are difficult to detect, measures are available to prevent their success. on the other hand, it is

Security Services:-

X.800 defines a security Service as a service Provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers. Perhaps a clearer definition is found in RFC 2828, which Provides the following definition; a processing or communication service that is provided by a system to give a specific kind of Protection to system resources; security services implement security Policies and are implemented by security mechanism.

Security Services (X.800)

AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be. Peer entity Authentication used in association with logical connection to Provide Confidence in the identity of entities connected.

Data origin Authentication in a Connectionless transfer, Provides assurance that the source of received data is as claimed.

ACCESS CONTROL.

The Prevention of unauthorized use of a resource. (i.e Service controls who can have access to a resource, under what conditions access can occur and what those accessing the resource are allowed to do).

DATA CONFIDENTIALITY:-

The Protection of data from unauthorized disclosure.

Connectionless Confidentiality

The Protection of all user data in a single data block.

Selective-Field Confidentiality

The Confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-Flow Confidentiallity:

The Protection of the information that might be derived from observation of traffic flows.

DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e, contain no modification, insertion, deletion or replay)

Connection integrity with Recovery:

Provides for the integrity of all user data on a connection and detects any modification, Insertion, deletion or replay of any data within an entire data sequence, with recovery attempted.

Connection integrity without Recovery..

As above but Provides only detection without recovery.

Selective-Field Connection integrity

Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selective fields have been modified, inserted, deleted or replayed

Connectionless integrity

Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless integrity

Provides for the integrity of selected fields within a single connectionless data block. takes the form of determination of whether the selected fields have been modified.

NON REPUDIATION:

Provides Protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. Nonrepudiation, origin proof that the message was received by the specified party.

Availability service

Both X-800 and RFC 2828 define availability to be the property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system. A variety of attacks can result in the loss of reduction in availability Some of these attacks are amenable to automated countermeasures, such as authentication and encryption, whereas other require some sort of physical action to prevent or recover from loss of availability of elements of a distributed system.

X.800 treats availability as a property to be associated with various security services. However, it makes sense to call out specifically an availability. This service addresses the Security concerns raised by denial-of-service attacks. It depends on proper management and control of system resources and thus depends on access control service and other security services.

3) DES is a symmetric key block cipher that operates on 64-bit blocks of plaintext using a 56-bit key (derived from a 64-bit key where 8 bits are Parity bits). It is based on the Feistal structure which leverages both substitution and Permutation for encryption

Detailed Principles of DES:

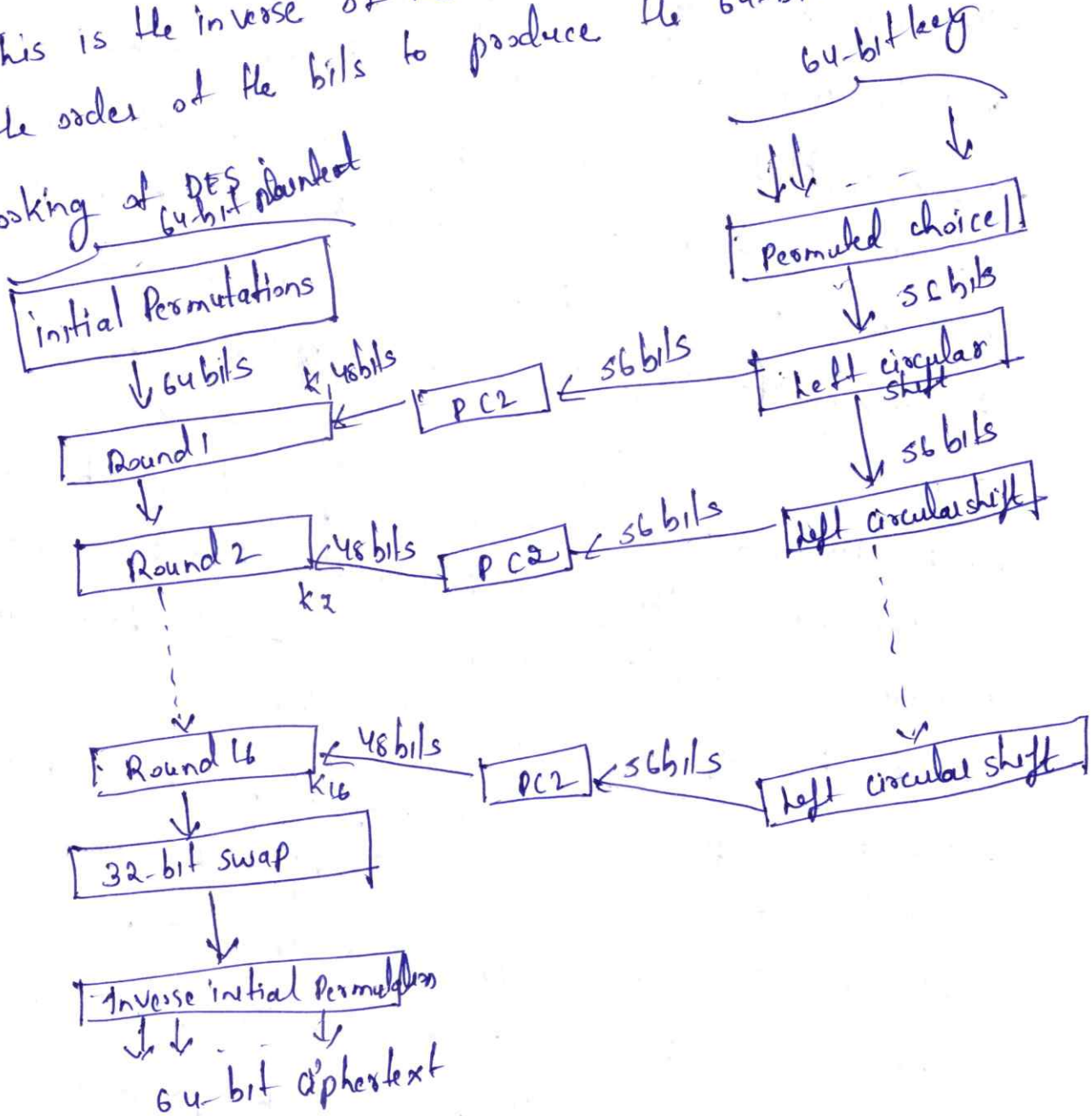
- initial Permutation (IP): The 64-bit plaintext block undergoes an initial Permutation, rearranging the bits according to a fixed table. This step has no cryptographic significance but Prepares the data for Feistal rounds.
- Feistal Rounds (16 Rounds): The core of DES consists of 16 identical rounds of Processing. Each round takes the output of the Previous round and a 48-bit subkey (derived from the main 56-bit key) as input.
  - splitting: The 64-bit block is split into two 32-bit halves: left plaintext (LPT) and Right plaintext (RPT)

- Expansion Permutation: The 32-bit RPT is expanded to 48 bits using an expansion Permutable table. this expansion allows it to be XoRed with the 48-bit Round key.
- XoR with Round key: The expanded 48-bit RPT is XoRed with the 48-bit subkey generated for the specific round.
- S-Box Substitution: The 48-bit result is then divided into eight 6-bit blocks, each of which is fed into a substitution Box(s-box). Each s-box Performs a non-linear substitution, transforming the 6-bit input into a 4 bit output. This is a crucial step for achieving confusion.
- P-Box Permutation: The 32-bit output from the s-boxes is then Passed through a Permutation Box (P-box), which rearranges the bits according to a fixed Permutation table. This step contributes to diffusion.
- XoR and swap: The 32-bit output of the P-box is XoRed with the 32-bit LPT. Finally, the roles of the LPT and RPT are swapped for the next round - meaning the new LPT becomes the Previous RPT, and the new RPT becomes the result of the XoR operation.
- key schedule: A key schedule algorithm generates 16 different 48-bit subkeys from the main 56-bit key one for each of the 16 rounds. This involves

Permutations and left circular shifts of the key bits

- Final Permutation (FP): After the 16 rounds, the two 32-bit halves are rejoined and a final Permutation is applied. This is the inverse of the initial Permutation, restoring the order of the bits to produce the 64-bit ciphertext.

Working of DES algorithm



Example:

Consider a plaintext block "11010110" and a key "10101010". The DES algorithm would perform the initial Permutation, followed by 16 rounds of Processing (each with its own subkey derived from the main key) and finally the final Permutations to Produce the ciphertext.

4. Elliptic curve Cryptography

Cryptography is the study of techniques for secure communication in the Presence of adversarial behaviours. Encryption uses an algorithm to encrypt data and a secret key to decrypt it.

1 Symmetric-key encryption (secret key encryption):
Symmetric-key algorithms are cryptographic algorithms that empby the same cryptographic keys both for plaintext encryption and ciphertext decoding. The keys could be identical or there could be a simple transition b/w them.

2. Asymmetric-key encryption (Public-key encryption):-
Asymmetric-key algorithms encrypts and decrypt a message using a pair of related keys (one public key and one Private key) and

safeguard it from unauthorized access or usage.

ECC, as the name implies, is an asymmetric encryption algorithm that employs the algebraic architecture of elliptic curves with finite fields.

- Elliptic Curve Cryptography (ECC) is an encryption technology comparable to RSA that enables public-key encryption.
- while RSA's security is dependent on huge prime numbers. ECC leverages the mathematical theory of elliptic curves to achieve the same level of security with considerably smaller keys.
- ~~vector~~

Components of Elliptic curve cryptography

1. ECC keys:

→ Private key: ECC cryptography's Private key creation is as simple as safely producing a random integer in a specific range, making it highly quick. Any integer in the field represents a valid ECC Private key.

→ Public key: Public keys within ECC are EC Points, which are pairs of integer coordinates x and y that lie on a curve Because of its unique features, EC Points can be compressed to a single coordinate + 1bit. As a result, the compressed Public key corresponds to a 256-bit ECC

2. Generator Point:

- ECC cryptosystems establish a special predefined EC Point called generator Point G (base Point) for elliptic curves over finite fields, which can generate any other Position in its subgroup over the elliptic curve by multiplying G from some integer in the range [0 ... r).
- The number r is referred to as the "ordering" of the cyclic subgroup.
- Elliptic curve subgroups typically contain numerous generator Points, but cryptologists carefully select one of them to generate the entire group and is excellent for Performance optimizations in calculations.

Elliptic curve Cryptography Algorithms

→ Digital signature algorithms:

- Elliptic curve Digital signature Algorithm: It is a more highly complicated Public-key cryptography encryption algorithm. Elliptic curve cryptography is a type of public key cryptography that uses the algebraic structure of elliptic curves with finite fields as the foundation.

Elliptic curve cryptography is primarily used to generate Pseudo-random numbers, digital signatures and other data.

- Edwards-curve Digital signature Algorithm:

The Edwards-curve Digital signature Algorithm (EdDSA) was proposed as a replacement for the Elliptic curve Digital signature Algorithm for performing fast Public-key digital digital signatures (ECDSA). Its primary benefits for embedded devices are higher performance and simple, secure implementations. During a signature, no branch or lookup operations based on the secret values are performed.

Benefits of Elliptic Curve cryptography:

1: High Efficiency: ECC provides stronger security than traditional encryption algorithms like RSA with much smaller key sizes. For instance, a 256-bit ECC key offers a security level equivalent to a 3072-bit RSA key. This results in faster computations and lower power consumption, which is particularly beneficial for mobile devices and IoT devices.

2 Resource Efficiency: Due to the smaller key sizes, ECC requires less storage and bandwidth. This is crucial for applications where resources are limited. Such as in mobile apps or embedded systems.

→ strong Security: ECC is based on the mathematical difficulty of solving the elliptic curve discrete logarithm problem.

* Scalability: ECC can be easily scaled to accommodate growing security needs without a proportional increase in computational requirements.

→ Scalability: ECC can be easily scaled to accommodate growing security needs without a proportional increase in Computational requirements.

5) The SHA-512 algorithm generates a 512-bit hash value (message digest) from an input message of arbitary length.

. Pre Processing (Padding and length appending):-

⇒ the input message is Padded to ensure its length is congruent to 896 modulo 1024. This involves appending a '1' bit, followed by as many '0' bits as necessary.

. A 128-bit representation of the original message's length is then appended to the Padded message. This results in a total message length that is a multiple of 1024 bits

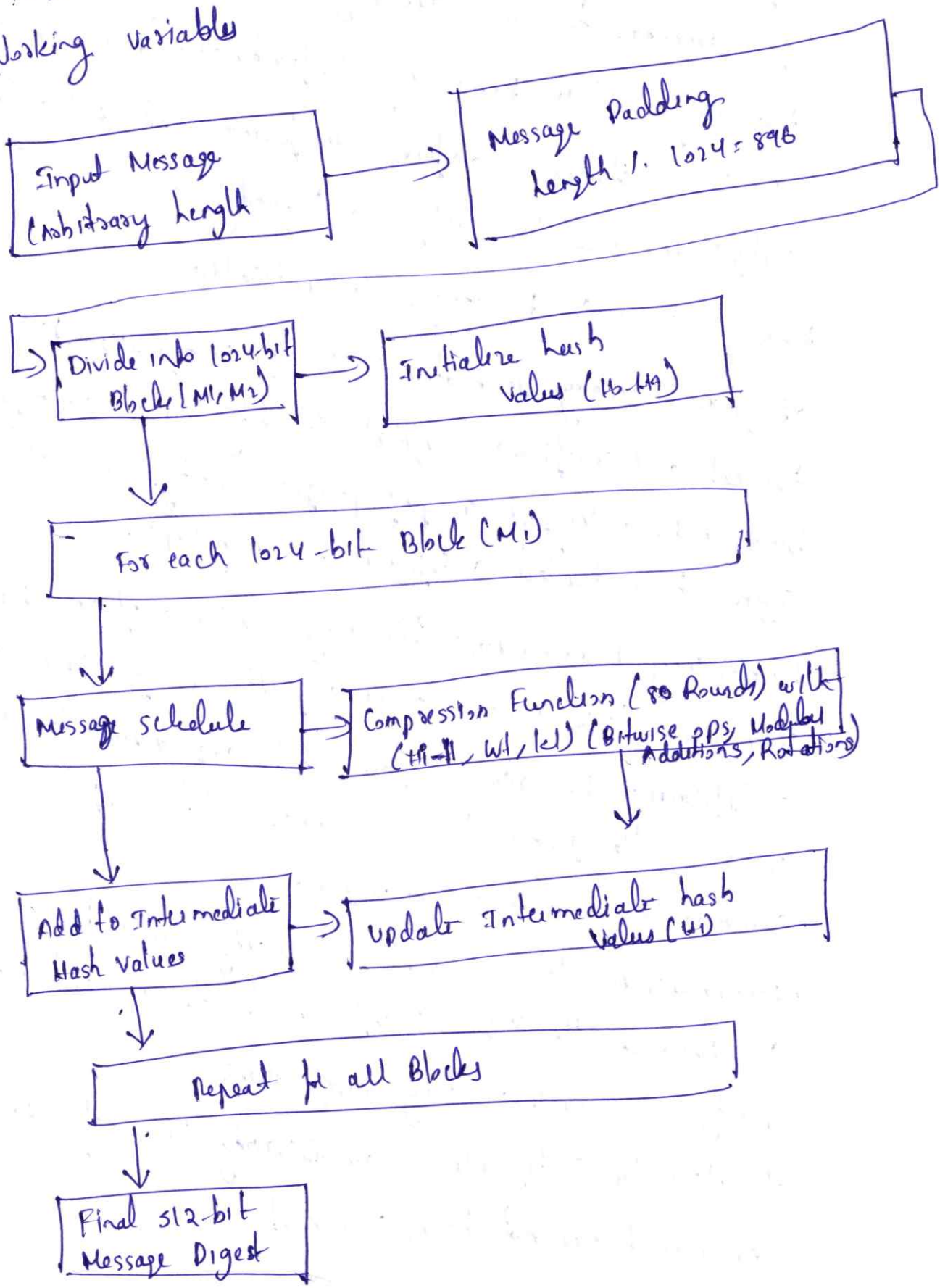
- Parsing into 1024-bit Blocks
  - The Preprocessed message is divided into a sequence of 1024-bit blocks.
- Initialization of Hash Values:
  - Eight 64-bit initial hash values (H_0 through H_7) are set. These values are derived from the fractional Parts of the square roots of the first eight prime numbers.

Main Loop (Message Processing):

- Each 1024-bit message block is Processed sequentially.
- For each block, a message schedule is created, extending the initial 16 64-bit words of the block into 80 64-bit Words. This involves specific bitwise operations and additions.
- The algorithm then iterates through 80 rounds.
- A complex series of bitwise operations, modular addition and bitwise rotations are applied to the current 512-bit intermediate hash value and the current 64-bit Word from the message schedule.
- An additive constant (K_t), derived from the fractional Parts of the cube roots of the first 80 prime numbers, is also incorporated.
- The Working variables are updated based on the results of these operations.

output:

→ After all 1024-bit message blocks have been processed through the main loop, the final values of the eight 64-bit working variables



6) X.509 Authentication Service

X.509 is a digital certificate that is built on top of a widely trusted standard known as ITU X.509 certificates are fundamental to secure directory authentication services, particularly within Public key Infrastructure (PKI) environments. The X.509 standard defines the format of Public-key certificates used to verify the identity of users, devices

Role of X.509 in Directory Authentication

- Digital Identity Verification: X.509 certificates provide a trusted and verifiable digital identity. Each certificate binds a Public key to a specific entity and is digitally signed by a trusted certificate Authority (CA).
- Public key Distribution: Directory services, often based on standards like X.500, act as repositories for these X.509 certificates. This allows users and applications to easily retrieve the public keys of other entities for secure communication and authentication.
- Authentication Process: When an entity needs to authenticate it presents its X.509 certificate to the authenticating party. The authenticating party then:
- Verifies the certificate's authenticity Validity Period and ensures it has not been revoked

-> Uses the Public key within the certificate to verify a digital signature so to establish a secure, encrypted communication channel.

Secure Communication :- X.509 certificates are integral to Protocols like TLS/SSL which are commonly used for secure communication b/w client and servers. In this context, server certificate authenticates the server to the client and in cases of mutual TLS, client certificate authenticates the client to the server.

key components :-

- X.509 Certificate : Contains information about the subject the Issuer (CA), Validity Period and a digital signature from the CA.
- Certificate Authority : A trusted third party responsible for issuing and managing digital certificates.
- Directory Server : Store and Provides access to X.509 Certificates, acting as a central location for Public key distribution.

1) S/MIME stand for Secure/Multipurpose Internet Mail Extensions through encryption, S/MIME offers protection for business emails.

S/MIME comes under the concept of cryptography. S/MIME is a protocol used for encrypting or decrypting ~~digitally~~ digitally signed E-mails. This means that users can digitally sign their emails as the owner of the e-mail.

How S/MIME Works

S/MIME enables non-ASCII data to be sent using Secure Mail Transfer Protocol. Moreover, many data files are sent, including music, video and image files. This data is securely sent using the encryption method. The data which is encrypted using a Public key is then decrypted using a Private key which is only present with the received of the E-mail. The receiver then decrypts the message and then the message is used. In this way, data is shared using e-mails Providing an end-to-end security source using the cryptography method.

Versions of S/MIME Versions

- 1st Version: 1995
- 2nd Version: 1998
- 3rd Version: 1999

How to get S/MIME Certificates:

The following are steps to have S/MIME certificate for Securing your emails

- Choose a Certificate Authority: you can select any trusted Certificate Authority, such as Sectigo, that has the functionality to provide you with S/MIME certificates. Most of these certificate Authorities provide both free and Paid versions according to one's needs.
- Get or Apply for a Certificate: log on to the website of the CA, and select the S/MIME certificate you would like to buy or apply for you might be asked for your name, email, address and organizational details.

S/MIME Services

->Authentication

->Confidentiality

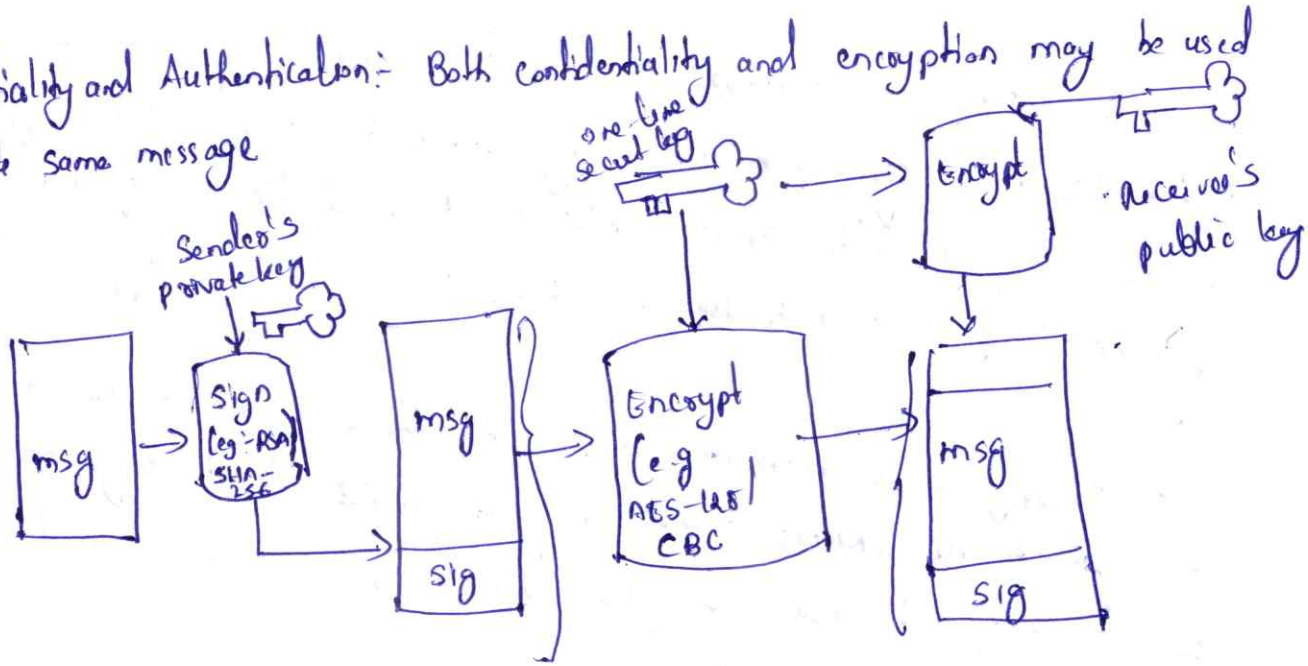
->Compression

->Email Compatibility

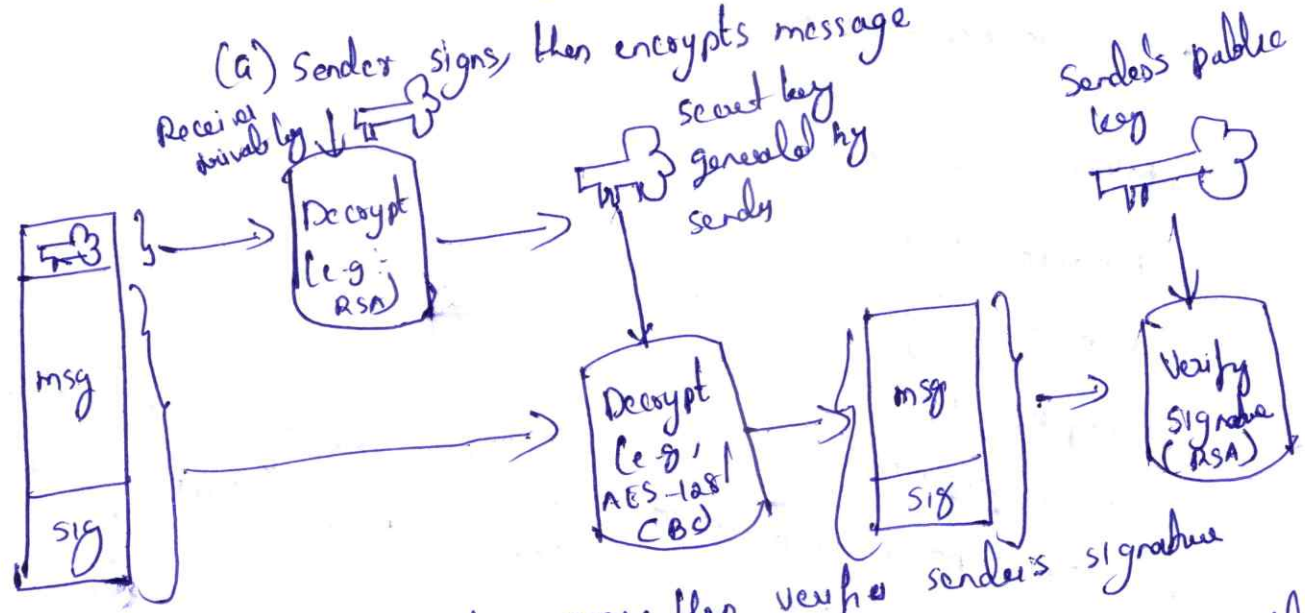
AUTHENTICATION: Authentication is provided by means of a digital signature, using the general scheme Most commonly RSA with SHA-256 is used.

1. The sender creates a message
2. SHA-256 is used to generate a 256-bit message digest of the message
3. The message digest is encrypted with RSA using the sender's Private key and the result is appended to the message. information for the signer, which will enable the receiver to retrieve the signer's Public key.
4. The receiver uses RSA with the sender's Public key to decrypt and recover the message digest.
5. The receiver generates a new message digest for the message and compares it with the decrypted hash code. If the two match the message is accepted as authentic

Confidentiality and Authentication:- Both confidentiality and encryption may be used for the same message



(a) Sender signs, then encrypts message



(b) Receiver decrypts message, then verifies sender's signature

The figure shows a sequence in which a signature is generated for the plaintext message and appended to the message. Then the plaintext message and signature are encrypted as a single block using symmetric encryption and the symmetric encryption key is encrypted using Public-key encryption.

EMAIL compatibility:- when S/MIME is used, at least part of the block to be transmitted is encrypted. If only the signature service is used, then the message digest is encrypted (with the sender's private key). If the confidentiality service is used, the message plus signature are encrypted. Thus, part or all of the resulting blocks consists of a stream of arbitary 8-bit octets

However, many electronic mail systems only permit the use of blocks consisting of ASCII text. To accomodate this restriction, S/MIME provides the service of converting the raw 8-bit binary stream to a stream of Printable ASCII characters, a process referred to as 7 bit encoding

The scheme typically used for this purpose is base64 conversion Each group of three octets of binary data is mapped into four ASCII characters. Base64 is described in RFC 4648.

One noteworthy aspect of the base64 algorithm is that it blindly converts the input stream to base64 format regardless of content, even if the input happens to be ASCII text. Thus if a message is signed but not encrypted and the conversion is applied to the entire block, the output will be unreadable to casual observer which provides a certain level of confidentiality

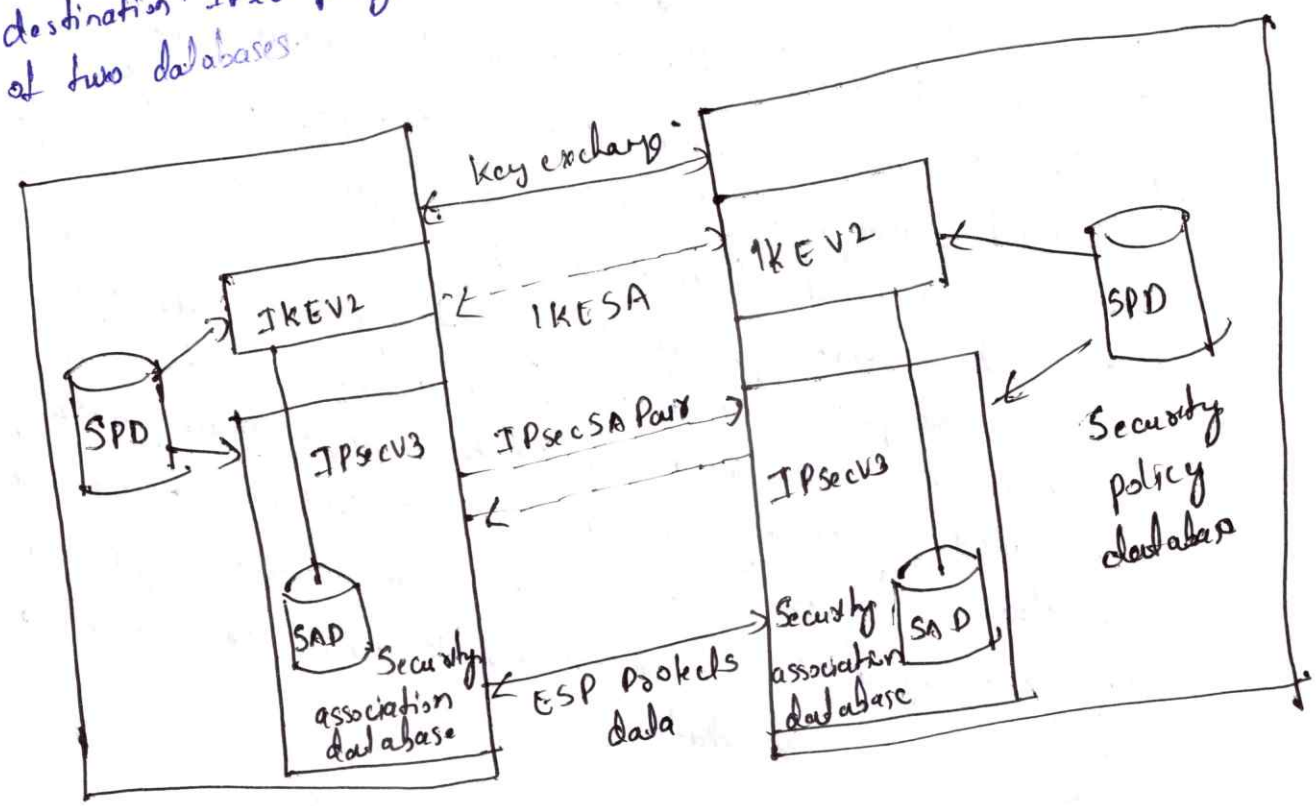
RFC 5751 also recommends that even if outer 7-bit encoding is not used, the original MIME content should be 7 bit encoded. The reason for this is that it allows the MIME entity to be handled in any environment without changing it. For example a trusted gateway might remove the encryption, but not the signature of a message and then forward the signed message on to the end recipient so that they can verify the signatures directly. if the transport internal to the site is not 8-bit clean such as on a wide area n/w with a single mail gateway, verifying the signatures directly. If the transport internal to the site is not 8-bit clean, such as on a wide area n/w with a single mail gateway verifying the signature will not be possible unless the original MIME entity was only 7 bit data.

COMPRESSION: S/MIME also offers the ability to compress a message. This has the benefit of saving space both for email transmission and for the storage. Compression can be applied in any order with respect to the signing and message encryption operations, RFC 5751 provides the following guidelines.

- Compression of binary encoded encrypted data is discouraged, since it will not yield significant compression. Base64 encrypted data could very well benefit, however.
- If a lossy compression algorithm is used with signing, you will need to compress first, then sign.

8) IP Security Policy:

Fundamental to the operation of IPsec is the concept of a security policy applied to each IP packet that transits from a source to a destination. IPsec policy is determined primarily by the interaction of two databases.



Security Associations

A key concept that appears in both the authentication and Confidentiality mechanisms for IP is the Security association (SA). An association is a one-way logical connection b/w a sender and a receiver that affords security services to the traffic carried on it. If a Peer relationship is needed for two-way secure exchange; then two security associations are required.

A security association is uniquely identified by three Parameters.

→ Security Parameters Index (SPI): A 32-bit unsigned integer assigned to the SA and having local significance only. The SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received Packet will be Processed.

→ IP Destination Address: This is the address of the destination endpoint of the SA, which may be an end-user system or a n/w system such as a firewall or router.

→ Security Protocol Identifier: This field from the outer IP header indicates whether the association is an AH or ESP security association.

Security Association Database:

In each IPsec implementation, there is a nominal Security Association Database that defines the Parameters associated with each SA. A security association is normally defined by the following parameters in an SAD entry.

→ Security Parameter Index:
→ Sequence Number Counter
→ Sequence Counter overflow
→ Anti-Replay window
→ AH information
→ ESP Information
→ Lifetime of this Security Association

→ IPsec Protocol Mode

→ Path MTU

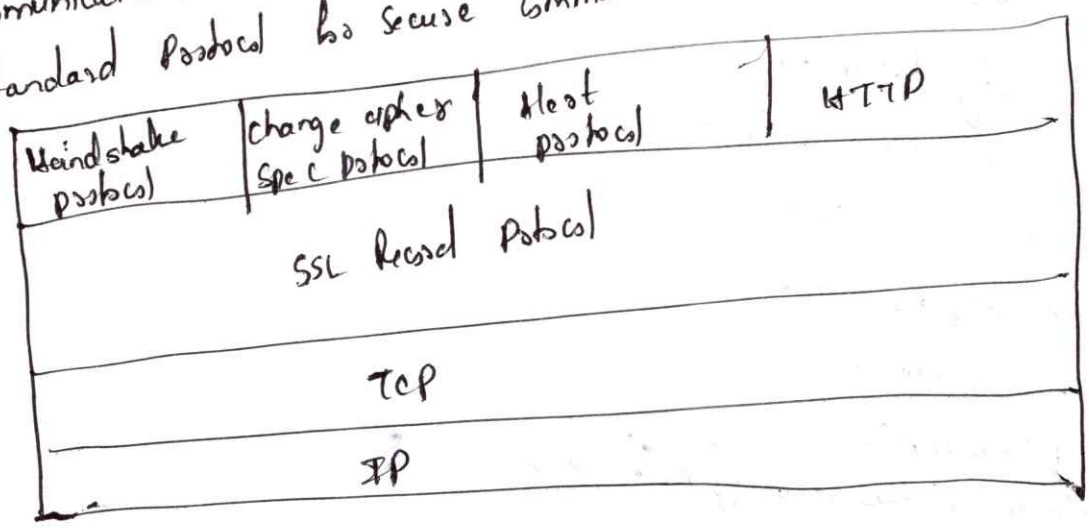
The key management mechanism that is used to distribute keys is coupled to the authentication and Privacy only by way of the security Parameters Index (SPI). Hence, authentication and Privacy have been specified independent of any specific key management mechanism

IPsec Provides the user with considerable flexibility in the way in which IPsec services are applied to IP traffic. SAs can be combined in a number of ways to yield the desired user configuration. Furthermore, IPsec Provides a high degree of granularity in discriminating between traffic that is affected. IPsec protection and traffic that is allowed to bypass IPsec, as in the former case relating IP traffic to specific SAs.

9) Secure Socket layer (SSL)

⇒ Secure Sockets layer (SSL) is an Internet security Protocol that encrypts data to ensure secure communication between devices over a network.

→ SSL Provides Privacy, authentication and data Integrity for online communications SSL is the predecessor of TLS, which is now the standard Protocol for secure communications on the Internet.



Working of SSL:

SSL ensures secure communication through three main mechanisms.

1. Encryption: Data transmitted over the n/w is encrypted, preventing unauthorised parties from reading it. if intercepted, encrypted data appears as an unreadable jumble of characters.
2. Authentication: SSL uses a handshake process to authenticate both the client and server, ensuring each party is legitimate and not an impostor.
3. Data Integrity: SSL digitally signs transmitted data to detect any tampering. ensuring that the data received is exactly what was sent.

SSL Protocols

→ SSL Record Protocol
→ Handshake Protocol
→ change-cipher spec Protocol
→ Alert Protocol

TLS:

Transport layer security (TLS) is a cryptographic Protocol designed to Provide security at the transport layer. it was derived from a security Protocol called secure socket layer. TLS ensures that no third Party can eavesdrop on or tamper with any message transmitted b/w a client and a server.

Benefits of TLS

1. Encryption: TLS/SSL helps secure transmitted data using encryption, ensuring that sensitive information remains confidential and protected from unauthorised access

-> Interoperability
-> Algorithm flexibility
-> Ease of deployment.
-> Ease of use

Working of TLS:

When a client connects to a server using TCP. it initiates a process called the SSL/TLS handshake. During this handshake the client sends several pieces of information to the server including.

-> The version of SSL/TLS it supports
-> A list of cipher suites (encryption algorithms) it can use.
-> The compression methods it supports.

This allows the server to select compatible settings and establish a secure connection.

The server checks the highest SSL/TLS version supported by both parties, selects a cipher suite from the client's options and optionally chooses a compression method. After this setup, the server provides its digital certificate. which must be trusted either directly by the client or by a trusted third party.

Both the server and client then compute the session key by symmetric encryption. once the handshake is complete the two hosts can communicate securely. if the TCP connection is closed improperly, both sides will know the connection was interrupted - but it cannot be compromised, only terminated

10 Virus

A computer virus is a type of malicious software (malware) designed to attach itself to a legitimate file or program in order to spread from one system to another. Much like a biological virus, it needs a host to survive and replicate.

key characteristics of a computer virus

- Requires Human Action: A virus cannot spread by itself. It needs the user to run the infected program or file (for example, opening a malicious email attachment or executing an infected application) for it to activate and start infecting the system.
- Attaches to Host Files: viruses embed themselves into other executable files, documents, or system files. When the infected file is run, the virus activates.
- Spreads Locally or Through Devices:

Viruses often spread through USB drives, shared files, infected downloads, or email attachments. They are less likely to spread rapidly over a network compared to worms.

- Can Cause Damage: Depending on its purpose, a virus can
  - → Delete or corrupt files
  - → Slow down system performance
  - → Display unwanted messages

Types of computer viruses

- File infector virus: Attaches to executable files.
- Macro virus: Infects documents like Word or Excel by exploiting macros.
- Boot Sector virus: Targets the boot sector of hard drives or USBs

- Polymorphic virus: Changes its code each time it spreads, making it hard to detect.
- Resident virus: Hides in the system memory and infects files as they are opened.

Worms

Worms are similar to a virus but it does not modify the program. A computer worm is a type of malware that can replicate itself and spread across computers and networks without needing a host file or any user interaction. It is self-contained meaning it doesn't need to attach to other programs or files to function. Worms can be controlled by remote. The main objective of worms is to eat the system's resources.

Types of Worms:

→ Code Red Worm: Exploited a vulnerability in Microsoft IIS web servers infecting over 350,000 systems in hours.

→ SQL slammer: Spread in minutes, bringing down banks, airlines and emergency services due to internet congestion.

→ Stuxnet: A highly sophisticated worm that ~~targeted~~ targeted.

11) Intrusion Detection system (IDS):

Intrusion is when an attacker gets unauthorized access to a device, n/w or system. Cyber criminals use advanced techniques to sneak into organizations without being detected.

Intrusion Detection System (IDS) observes n/w traffic for malicious Internet transactions and sends immediate alerts when it is observed. it is s/w that checks a n/w or system for malicious activities or Policy violations. Each illegal activity or violation is often recorded to an administration. IDS monitors a n/w or system for malicious activity or Policy violations.

An intrusion Detection System working:-

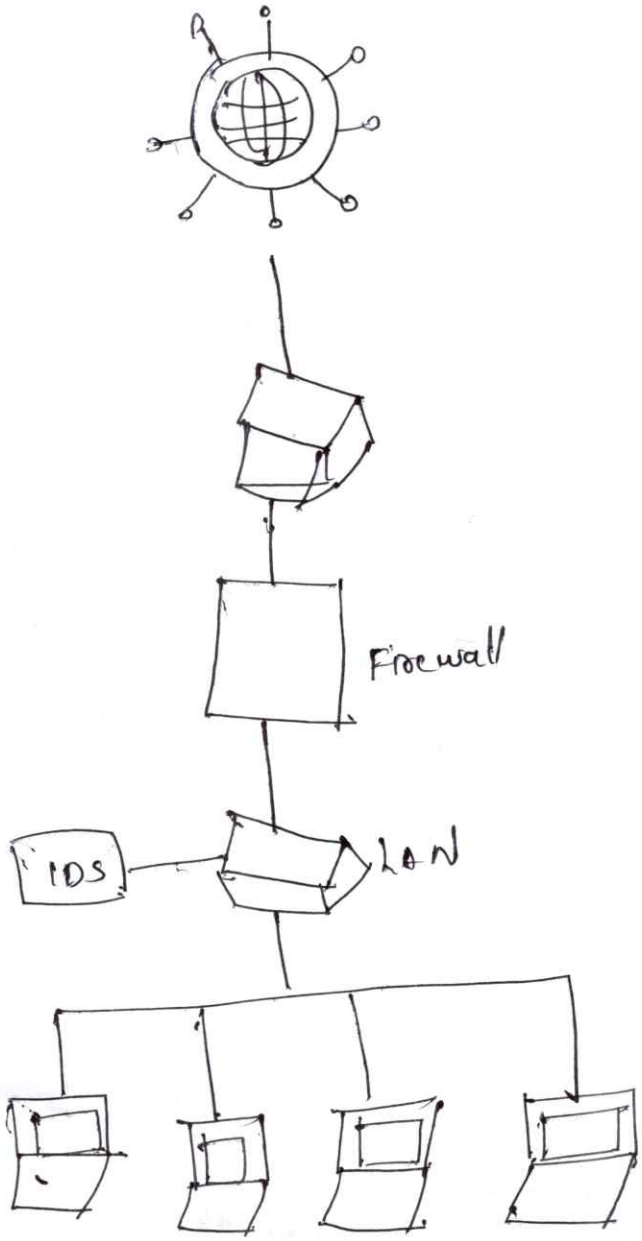
→ An IDS monitors the traffic on a Computer network to detect any suspicious activity

→ It analyzes the data flowing through the network to look for Patterns and signs of abnormal behaviour

→ The IDS compares the network activity to a set of Predefined rules and Patterns to identify any activity that might indicate an attack or Intrusion.

→ If the IDS detects something that matches one of these rules or Patterns, it sends an alert to the system administrator.

→ The system administrator can then investigate the alert and take action to Prevent any damage or further intrusion



Benefits of IDS :-

- Detects Malicious Activity : IDS can detect any suspicious activities and alert the system administrator before any significant damage is done.
- Improves Network Performance : IDS can identify any Performance issues on the n/w, which can be addressed to improve n/w Performance.
- Compliance Requirements : IDS can help in meeting compliance requirements by monitoring n/w activity and generating reports.
- Provides Insights : IDS generates valuable insights into n/w traffic which can be used to identify any weaknesses and improve n/w security.

PART - A

1) a) Information security explanation — 2M

b) Random number generation explanation — 2M

c) key management explanation — 2M

d) Authentication Protocol explanation — 2M

e) Digital signature explanation — 2M

f) Pretty good Privacy definition — 2M

g) IP security definition — 2M

h) Secure electronic transaction explanation — 2M

i) virus explanation — 2M

j) firewall explanation — 2M

PART B

2) Types of security attacks — 2-5M

Types of security services — 2-5M

3) DES Algorithm steps — 3M

principles of DES — 2M

4) Explain Eliptic curve cryptography — 3M

Advantages of cryptography — 2M

5) SHA-512 algorithm with steps — 3M
drawing a neat diagram — 2M
— 1M

6) X-509 explanation
Directory authentication service using X-509 — 4M

7) S/MIME Protocol explanation — 3M
S/MIME Services — 2M

8) Combining security association in IPSec — 3M
key management in IPSec — 2M

9) SSL explanation with operations — 2.5M
TLS protocols with operations — 2.5M

10) Types of viruses with definition — 2.5M
Types of worms with definition — 2.5M

11) Intrusion detection system explanation — 1M
Architecture of an IDS with diagram — 3M
Advantages of IDS — 1M