CNS QP Sessional Answers

1.a) Explain the model for Network Security.

Ans.1.a)

Model For Network Security

A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.

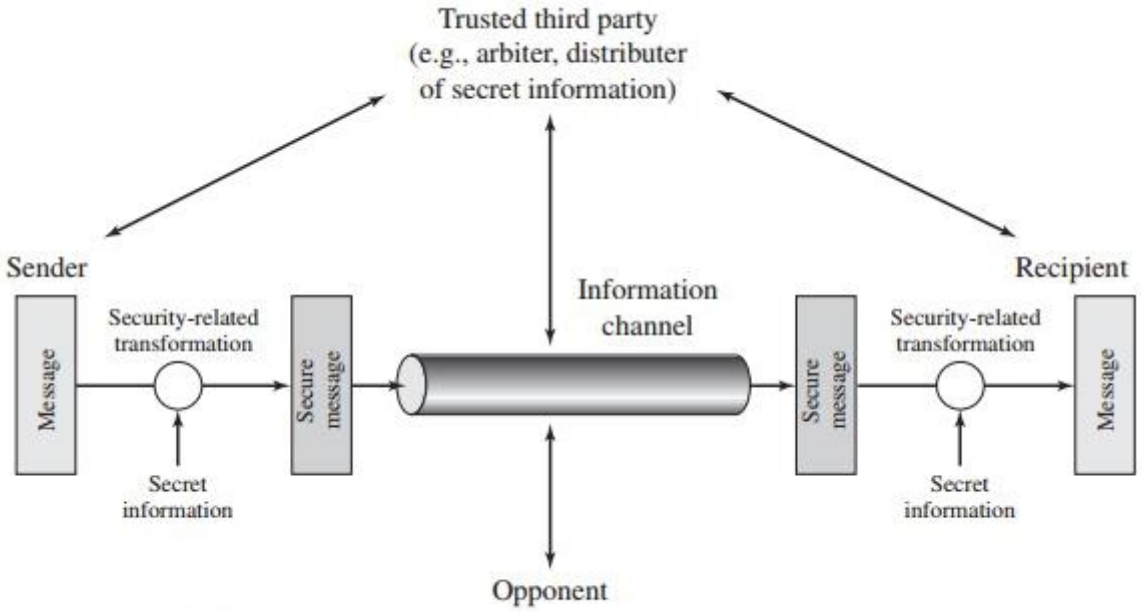


Figure 1.4 Model for Network Security

Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent. Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.

This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

1.b) Illustrate the encryption and decryption process using Hill Cipher for:

Plain Text : ATTACK

Keyword : BCCF

Ans.1.b)

2.a) Apply Extended Euclid algorithm to compute GCD (99,78).
Show: all the computations.

Ans.2.a)

GCD (99 , 78) using Extended Euclid's Algorithm

Q	A	B	R
1	99	78	21
3	78	21	15
1	21	15	6
2	15	6	3
1	6	3	0
	3	0	

GCD (99 , 78) = 3

Computations

- **a = b * q + r**
- **99 = 78 * 1 + 21**
- **78 = 21 * 3 + 15**
- **21 = 15 * 1 + 6**
- **15 = 6 * 2 + 3**
- **6 = 3 * 2 + 0**

2.b) State the different substitution encryption techniques.

Encrypt the following plaintext using Playfair cipher:

Plain Text : CHANDRAYAAN

Keyword : MONARCHY

Ans.2.b)

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

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

- **Monoalphabetic Cipher – In monoalphabetic substitution cipher, a character in a plaintext is always restored or changed to the similar character in the ciphertext indifferent of its position in the text.**
- **Polyalphabetic cipher – In polyalphabetic substitution, each appearance of a character in the plaintext can have a different substitution character in the ciphertext.**
- **One-Time Pad – The one-time pad cipher recommend that the key length must be as long as the plain text to avoid the repetition of key.**
- **Caesar Cipher – In this substitution technique, it can encrypt the plain text, each alphabet of the plain text is restored by the alphabet three places further it and it can decrypt the cipher text each alphabet of cipher text is restored by the alphabet three places before it.**
- **Playfair Cipher – The playfair cipher is also known as Playfair Square. It is a cryptographic technique used for manual encryption of information.**

The Playfair Cipher

Encryption:

Plain Text : CHANDRAYAAN

Key: MONARCHY

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

CH	AN	DR	AY	AX	AN
HY	RA	KD	NB	BA	RA

Cipher Text : " HYRAKDNBBARA "

3.a) Differentiate between block cipher and stream cipher.

Ans.3.a)

S.NO	Block Cipher	Stream Cipher
1.	Block Cipher Converts the plain text into cipher text by taking plain text's block at a time.	Stream Cipher Converts the plain text into cipher text by taking 1 byte of plain text at a time.
2.	Block cipher uses either 64 bits or more than 64 bits.	While stream cipher uses 8 bits.
3.	The complexity of block cipher is simple.	While stream cipher is more complex.
4.	Block cipher Uses confusion as well as diffusion.	While stream cipher uses only confusion.
5.	In block cipher, reverse encrypted text is hard.	While in-stream cipher, reverse encrypted text is easy.
6.	The algorithm modes which are used in block cipher are ECB (Electronic Code Book) and CBC (Cipher Block Chaining).	The algorithm modes which are used in stream cipher are CFB (Cipher Feedback) and OFB (Output Feedback).
7.	Block cipher works on transposition techniques like rail-fence technique, columnar transposition technique, etc.	While stream cipher works on substitution techniques like Caesar cipher, polygram substitution cipher, etc.
8.	Block cipher is slow as compared to a stream cipher.	While stream cipher is fast in comparison to block cipher.
9.	Suitable for applications that require strong encryption, such as file storage and internet communications	Suitable for applications that require strong encryption, such as file storage and internet communications
10.	More secure than stream ciphers when the same key is used multiple times	Less secure than block ciphers when the same key is used multiple times
11.	key length is Typically 128 or 256 bits	key length is Typically 128 or 256 bits
12.	Operates on fixed-length blocks of data	Encrypts data one bit or byte at a time

3.b) Explain Key Calculation Procedure in Simplified DES algorithm.
Illustrate your answer by considering user input key as 00011 00111.

Ans.3.b)

The Simplified Data Encryption Standard (S-DES) is a simplified version of the original Data Encryption Standard (DES) algorithm. It uses a shorter key length and fewer rounds for simplicity.

The key calculation procedure in S-DES involves generating two subkeys from aninitial 10-bit key. Here's an explanation of the key calculation procedure in S- DES:

Initial 10-Bit Key (K): The S-DES algorithm starts with an initial 10-bit key, represented as K. This key is provided as input to the encryption and decryptionprocesses.

Permutation P10: The first step in key calculation is to permute the 10-bit key using a fixed permutation called P10. P10 rearranges the bits in the following way:

P10: 3 5 2 7 4 10 1 9 8 6

The bits of the initial key are rearranged according to this permutation. The resulting 10-bit value is divided into two 5-bit halves, often denoted as left and right halves (L0 and R0).

Key Generation Rounds:

Round 1:

Left Circular Shift (LS-1): Both L0 and R0 are separately subjected to a left circularshift by one bit. This means that the leftmost bit is moved to the rightmost position, and the other bits are shifted one position to the left.

L0: 3 5 2 7 4 10 1 9 8 6
R0: 5 2 7 4 10 1 9 8 6 3

Permutation P8: After the left circular shift, both L0 and R0 are subjected to another fixed permutation called P8. P8 selects and permutes specific bits fromthe 10-bit halves to generate the first subkey, often denoted as K1.

P8: 6 3 7 4 8 5 10 9

The bits selected by P8 from both L0 and R0 are combined to form K1, which is a 8-bit subkey.

Round 2:

Left Circular Shift (LS-2): Both L0 and R0 (after the first round) are separately subjected to a left circular shift by two bits this time.

L1: 2 7 4 10 1 9 8 6 3 5
R1: 7 4 10 1 9 8 6 3 5 2

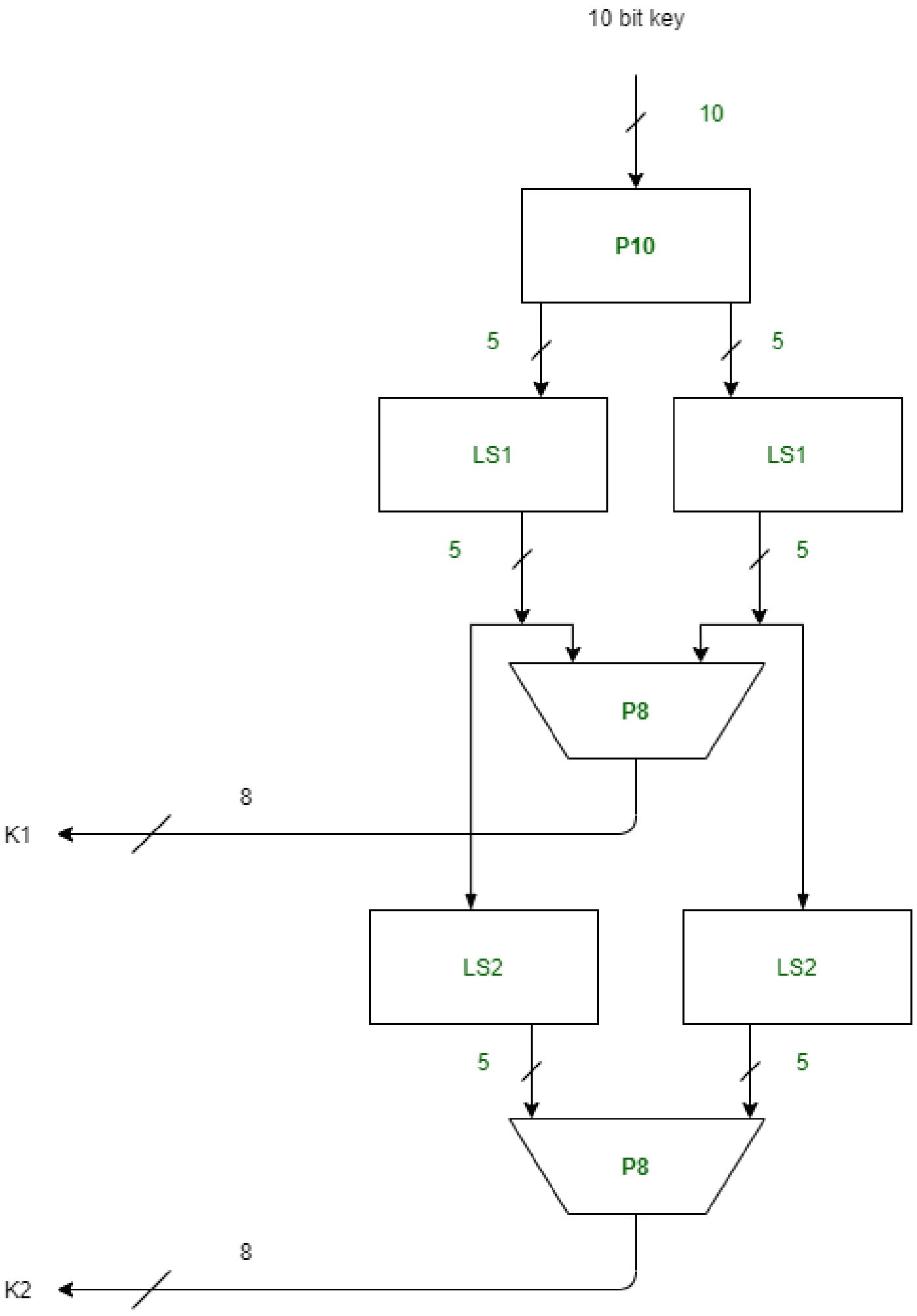
Permutation P8: After the left circular shift, both L1 and R1 are subjected to theP8 permutation again to generate the second subkey, often denoted as K2.

P8: 6 3 7 4 8 5 10 9

The bits selected by P8 from both L1 and R1 are combined to form K2, which is another 8-bit subkey.

At the end of the key calculation procedure, you have generated two 8-bit subkeys, K1 and K2, from the original 10-bit key K. These subkeys are used in theS-DES encryption and decryption processes.

In S-DES, these subkeys are used in a Feistel network structure to perform the initial and final permutations, as well as the rounds of substitution and permutation. This process helps encrypt and decrypt the plaintext.



Key Calculation Procedure in Simplified DES algorithm

4.a) What are the block cipher modes of operation of DES? Explain in detail.

Ans.4.a)

Encryption algorithms are divided into two categories based on the input type, as a block cipher and stream cipher.

Block cipher is an encryption algorithm that takes a fixed size of input say b bits and produces a ciphertext of b bits again. If the input is larger than b bits it can be divided further.

For different applications and uses, there are several modes of operations for a block cipher.

i. **Electronic Code Book (ECB) –**

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

ii. **Cipher Block Chaining –**

Cipher block chaining or CBC is an advancement made on ECB since ECB compromises some security requirements. In CBC, the previous cipher block is given as input to the next encryption algorithm after XOR with the original plaintext block. In a nutshell here, a cipher block is produced by encrypting an XOR output of the previous cipher block and present plaintext block.

iii. **Cipher Feedback Mode (CFB) –**

In this mode the cipher is given as feedback to the next block of encryption with some new specifications: first, an initial vector IV is used for first encryption and output bits are divided as a set of *s* and *b-s* bits. The left-hand side *s* bits are selected along with plaintext bits to which an XOR operation is applied. The result is given as input to a shift register having b-s bits to lhs,s bits to rhs and the process continues. Both of them use encryption algorithms.

iv. **Output Feedback Mode –**

The output feedback mode follows nearly the same process as the Cipher Feedback mode except that it sends the encrypted output as feedback instead of the actual cipher which is XOR output. In this output feedback mode, all bits of the block are sent instead of sending selected *s* bits. The Output Feedback mode of block cipher holds great resistance towards bit transmission errors. It also decreases the dependency or relationship of the cipher on the plaintext.

v. **Counter Mode –**

The Counter Mode or CTR is a simple counter-based block cipher implementation. Every time a counter-initiated value is encrypted and given as input to XOR with plaintext which results in ciphertext block. The CTR mode is independent of feedback use and thus can be implemented in parallel.

4.b) Explain in detail about DES encryption and decryption algorithm.

Ans.4.b)

The Data Encryption Standard (DES) is a symmetric-key block cipher that was widely used for secure data transmission and storage. It operates on fixed-size blocks of data (64 bits) using a key size of 56 bits. DES consists of two main processes: encryption and decryption.

- **Key Size: 56 bits (64 bits with 8 parity bits, but effectively 56 bits used for encryption).**
- **Block Size: 64 bits.**
- **Rounds: 16.**
- **Key Expansion: Permutation and shifting.**
- **Substitution: S-Boxes.**
- **Confusion and Diffusion: Achieved through permutations and substitutions.**

DES was widely used, but due to its small key size, it became vulnerable to brute-force attacks. Consequently, it has been replaced by more secure algorithms like AES (Advanced Encryption Standard).

DES Encryption Algorithm:

1. Initial Permutation (IP):

- **The 64-bit plaintext block undergoes an initial permutation.**
- **The bits are rearranged according to a fixed permutation table.**

2. Key Generation:

- **The 56-bit key is permuted using the PC-1 permutation table.**
- **The 56-bit key is split into two 28-bit halves (C0 and D0).**
- **16 subkeys (K1 to K16) are generated through 16 rounds of key permutation and shifting.**

3. Rounds (16 Rounds):

- **The 64-bit plaintext block is divided into two 32-bit halves (L0 and R0).**
- **For each round, the right half (Ri-1) is expanded to 48 bits using the E-Box.**
- **The expanded R is XORed with the round key (Ki).**
- **The result is passed through the S-Boxes, which substitute 48 bits with 32 bits.**
- **The output is then permuted using the P-Box.**
- **The permuted output is XORed with the left half (Li-1).**
- **The left and right halves are swapped, and the process repeats for 16 rounds.**

4. Final Permutation (IP^(-1)):

- **After the 16 rounds, the left and right halves are concatenated.**
- **The resulting 64-bit block undergoes a final permutation (inverse of the initial permutation).**

DES Decryption Algorithm:

The decryption process in DES is essentially the reverse of the encryption process:

1. Initial Permutation (IP):

- **The ciphertext block undergoes the same initial permutation used in encryption.**

2. Key Generation:

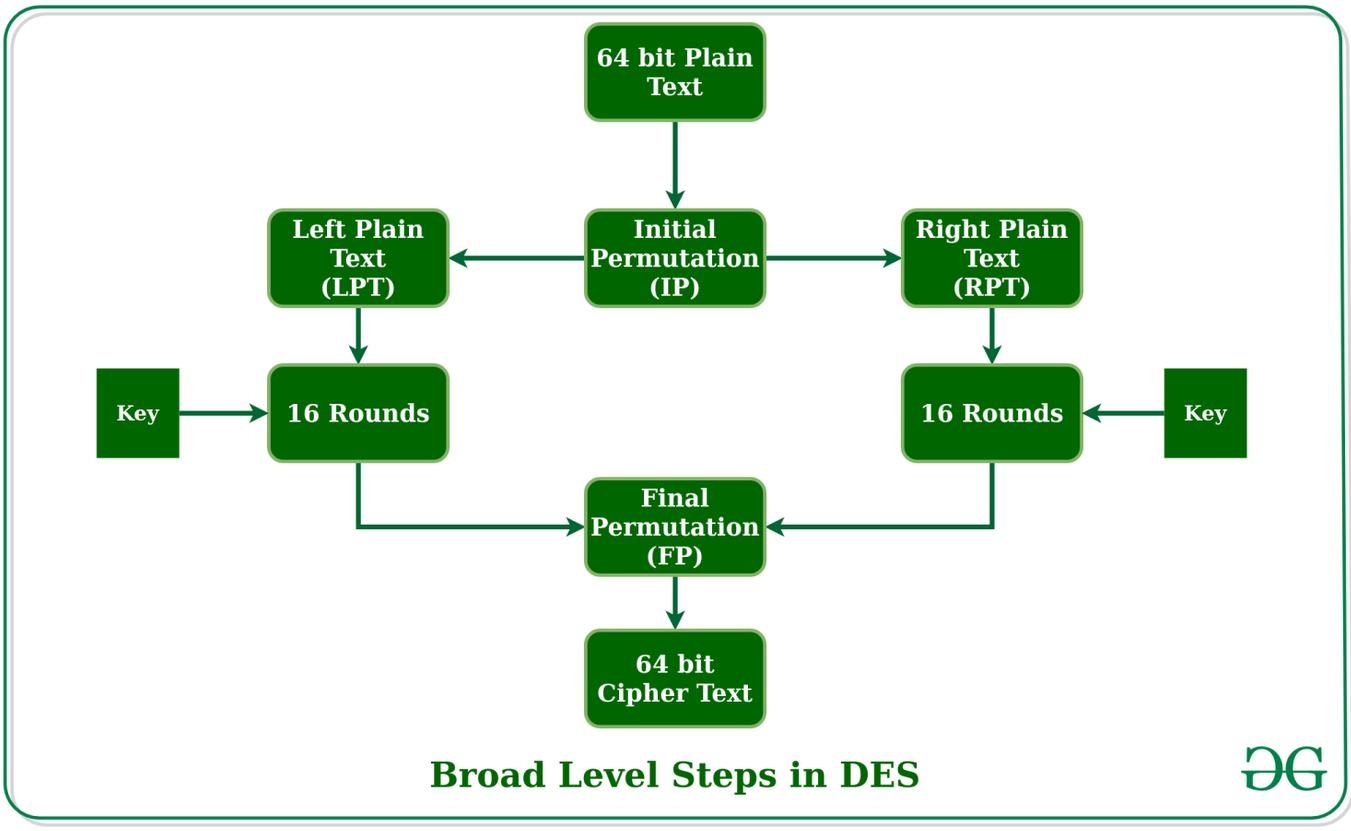
- **The key generation process is the same as in encryption.**

3. Rounds (16 Rounds):

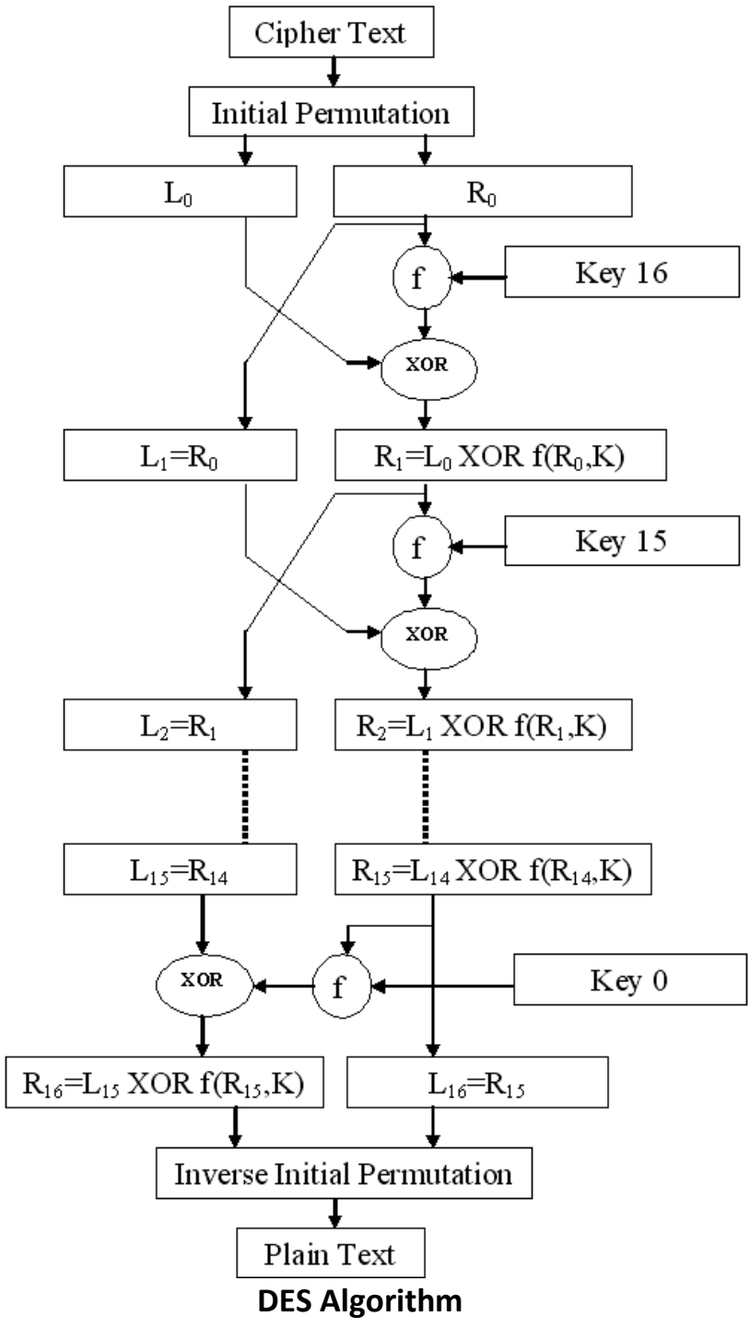
- **The only difference is that the subkeys are used in the reverse order (K16 to K1) during decryption.**

4. Final Permutation (IP^{-1}):

- **After the 16 rounds, the left and right halves are concatenated.**
- **The resulting 64-bit block undergoes the final permutation (inverse of the initial permutation).**



Broad Level Steps in DES



DES Algorithm

5.) Give decryption the stepwise Illustration of RSA algorithm to perform encryption and procedure for following data:

Plain Text 10 : 10
Prime No. P : 11
Prime No. Q : 17
Parameter e : 7

Ans.5)

RSA encryption and decryption involve the use of public and private keys, based on the mathematical properties of large prime numbers. Here's a stepwise illustration of the RSA algorithm for the given data:

1. Key Generation:

Select two large prime numbers, P = 11 and Q = 17 .
Calculate N = P * Q = 11 * 17 = 187 .
Calculate $\phi(N) = (P-1) * (Q-1) = 10 * 16 = 160$.
Choose a public exponent e such that $1 < e < \phi(N)$ and e is coprime to $\phi(N)$.
Here, e = 7 is given.

Public Key: (e, N) = (7, 187)

Calculate the private exponent d such that $d \equiv e^{-1} \bmod \phi(N)$.
In this case, $d \equiv 23 \bmod 160$.

Private Key: (d, N) = (23, 187)

2. Encryption:

Convert the plaintext message M to a number. Here, M = 10 .
Use the recipient's public key (e, N) to compute the ciphertext C: $C \equiv M^e \bmod N$.
For M = 10 and e = 7 : $C \equiv 10^7 \bmod 187 = 175$.
Calculate C using modular exponentiation.

3. Decryption:

Use the recipient's private key (d, N) to compute the original message M: $M \equiv C^d \bmod N$.
For C calculated in the encryption step and d = 23 : $M \equiv 175^{23} \bmod 187 = 10$.
Calculate M using modular exponentiation.

In summary, the steps involve key generation, encryption using the recipient's public key, and decryption using the recipient's private key to recover the original message. Note that the actual calculations involve modular arithmetic to ensure efficiency and security.

6.a) Explain in detail about the working of Diffie-Hellman key exchange algorithm.

Ans.6.a)

The Diffie-Hellman key exchange algorithm is a method for two parties to securely agree on a shared secret key over an insecure communication channel. The security of the algorithm relies on the difficulty of the discrete logarithm problem.

Here's a simplified example of the Diffie-Hellman key exchange algorithm:

Steps:

1. **Initialization:**
   - **Choose a large prime number *p* and a primitive root modulo *p*, denoted as *g*. These values are public and agreed upon by both parties.**

Let's choose *p*=23 and *g*=5 for this example.

2. **Public Key Exchange:**

- **Alice and Bob publicly share their choices of *p* and *g*.**
- **Alice chooses a private key *a* (a random number), and Bob chooses a private key *b*.**

Alice's private key: *a*=6

Bob's private key: *b*=15

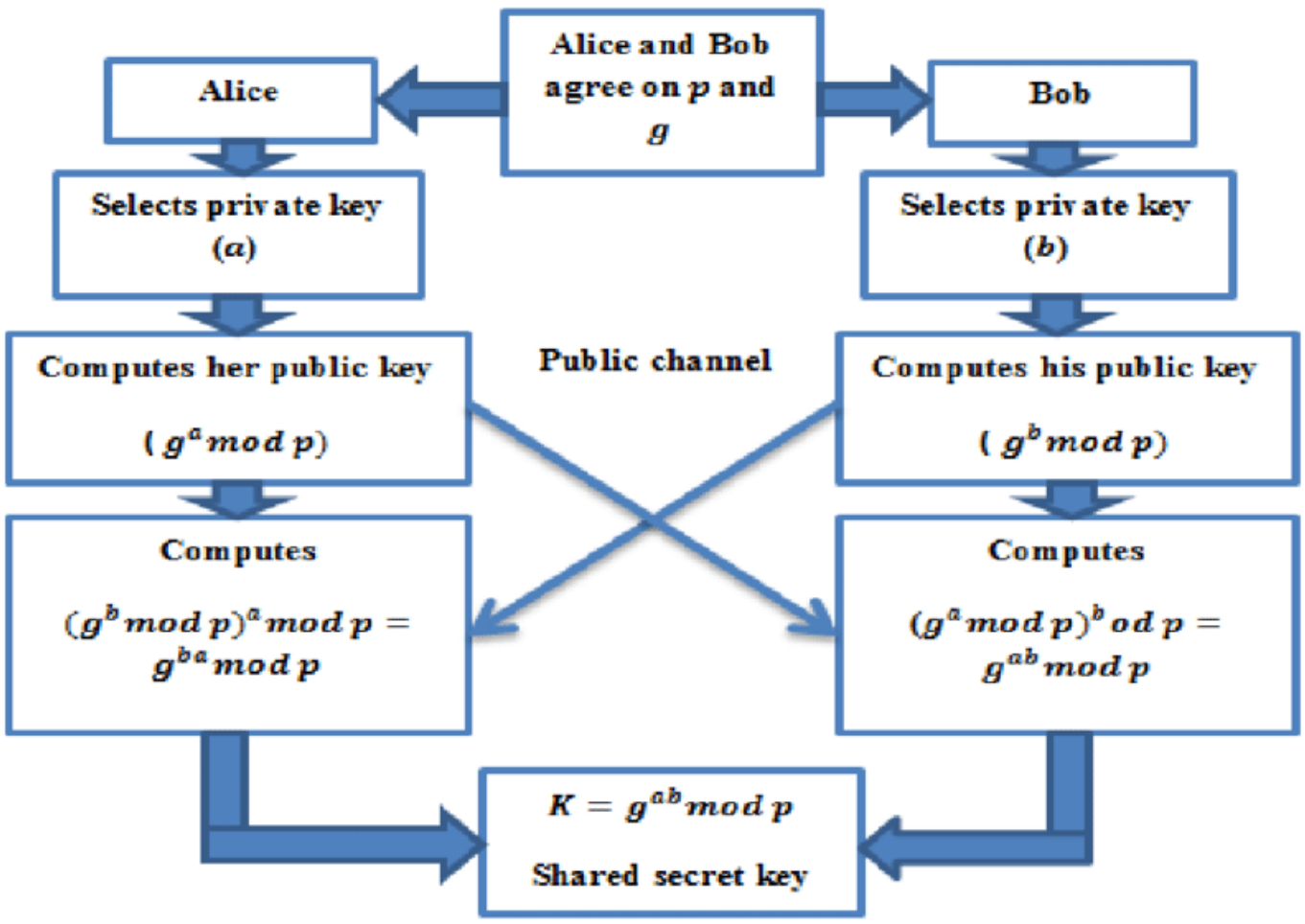
3. **Compute Partial Keys:**

- **Both Alice and Bob independently compute their partial keys using the public values *p* and *g* and their private keys *a* and *b*.**

Alice's partial key: $A = g^a \bmod p = 5^6 \bmod 23 = 8$

Bob's partial key: $B = g^b \bmod p = 5^{15} \bmod 23 = 19$

Now, both Alice and Bob have computed the same shared secret key (*s*=2) without explicitly exchanging it over the insecure channel. This shared secret can be used as a symmetric key for encryption and decryption in subsequent communication.



6.b) Apply the Chinese Remainder Theorem to solve following congruent equations.

$X \equiv 2 \pmod 3$
$X \equiv 3 \pmod 5$
$X \equiv 2 \pmod 7$

Ans.6.b)

$a_1 = 2$ $\quad m_1 = 3$
$a_2 = 3$ $\quad m_2 = 5$
$a_3 = 2$ $\quad m_3 = 7$

- **Calculate Common Modulus**

$M = m_1 * m_2 * m_3 * m_n$

$M = 3 * 5 * 7 = 105$

- **Calculate Partial Products**

$M_n = \frac{M}{m_n}$

$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$

$M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$

$M_3 = \frac{M}{m_3} = \frac{105}{7} = 15$

- **Calculate Modulus Inverse**

***Rule**

$M_n^{-1} = M_n * x \bmod m_n = 1$

$M_n^{-1} = x$

$M_1^{-1} = M_1 * x \bmod m_1$
$= 35 * 1 \bmod 3$
$= 35 \bmod 3 = 2$ ❌

$= 35 * 2 \bmod 3$
$= 70 \bmod 3 = 1$ ✅
$M_1^{-1} = 2$

$M_2^{-1} = M_2 * x \bmod m_2$
$= 21 * 1 \bmod 5$
$= 21 \bmod 5 = 1$ ✅
$M_2^{-1} = 1$

$M_3^{-1} = M_3 * x \bmod m_3$
$= 15 * 1 \bmod 7$
$= 15 \bmod 7 = 1$ ✅
$M_3^{-1} = 1$

- **Calculate X**

$X = [(a_1 * M_1 * M_1^{-1}) + (a_2 * M_2 * M_2^{-1}) + (a_3 * M_3 * M_3^{-1})] \bmod M$
$X = [(2 * 35 * 2) + (3 * 21 * 1) + (2 * 15 * 1)] \bmod 105$
$X = [140 + 63 + 30] \bmod 105$
$X = [(140) + (63) + (30)] \bmod 105$
$X = 233 \bmod 105$
$X = 23$

Verification:

$23 \bmod 3 = 2$ ✅
$23 \bmod 5 = 3$ ✅
$23 \bmod 7 = 2$ ✅

7.a) Explain in detail about X.509 directory authentication service.

Ans.7.a)

X.509 is a digital certificate that is built on top of a widely trusted standard known as ITU or International Telecommunication Union X.509 standard, in which the format of PKI certificates is defined. X.509 digital certificate is a certificate-based authentication security framework that can be used for providing secure transaction processing and private information. These are primarily used for handling the security and identity in computer networking and internet-based communications.

Working of X.509 Authentication Service Certificate:

The core of the X.509 authentication service is the public key certificate connected to each user. These user certificates are assumed to be produced by some trusted certification authority and positioned in the directory by the user or the certified authority. These directory servers are only used for providing an effortless reachable location for all users so that they can acquire certificates. X.509 standard is built on an IDL known as ASN.1. With the help of Abstract Syntax Notation, the X.509 certificate format uses an associated public and private key pair for encrypting and decrypting a message.

Once an X.509 certificate is provided to a user by the certified authority, that certificate is attached to it like an identity card. The chances of someone stealing it or losing it are less, unlike other unsecured passwords. With the help of this analogy, it is easier to imagine how this authentication works: the certificate is basically presented like an identity at the resource that requires authentication.

Generally, the certificate includes the elements given below:

- **Version number: It defines the X.509 version that concerns the certificate.**
- **Serial number: It is the unique number that the certified authority issues.**
- **Signature Algorithm Identifier: This is the algorithm that is used for signing the certificate.**
- **Issuer name: Tells about the X.500 name of the certified authority which signed and created the certificate.**
- **Period of Validity: It defines the period for which the certificate is valid.**
- **Subject Name: Tells about the name of the user to whom this certificate has been issued.**
- **Subject's public key information: It defines the subject's public key along with an identifier of the algorithm for which this key is supposed to be used.**
- **Extension block: This field contains additional standard information.**
- **Signature: This field contains the hash code of all other fields which is encrypted by the certified authority private key.**
-

Applications of X.509 Authentication Service Certificate:

Many protocols depend on X.509 and it has many applications, some of them are given below:

- **Document signing and Digital signature**
- **Web server security with the help of Transport Layer Security (TLS)/Secure Sockets Layer (SSL) certificates**
- **Email certificates**
- **Code signing**
- **Secure Shell Protocol (SSH) keys**
- **Digital Identities**

7.b) Explain MD5 message digest algorithm with example.

Ans.7.b)

MD5 is a cryptographic hash function algorithm that takes the message as input of any length and changes it into a fixed-length message of 16 bytes. MD5 algorithm stands for the message-digest algorithm. MD5 was developed as an improvement of MD4, with advanced security purposes. The output of MD5 (Digest size) is always 128 bits. MD5 was developed in 1991 by Ronald Rivest.

Use Of MD5 Algorithm:

- **It is used for file authentication.**
- **In a web application, it is used for security purposes. e.g. Secure password of users etc.**
- **Using this algorithm, we can store our password in 128 bits format.**

Application Of MD5 Algorithm:

- **We use message digest to verify the integrity of files/ authenticates files.**
- **MD5 was used for data security and encryption.**
- **It is used to Digest the message of any size and also used for Password verification.**
- **For Game Boards and Graphics.**

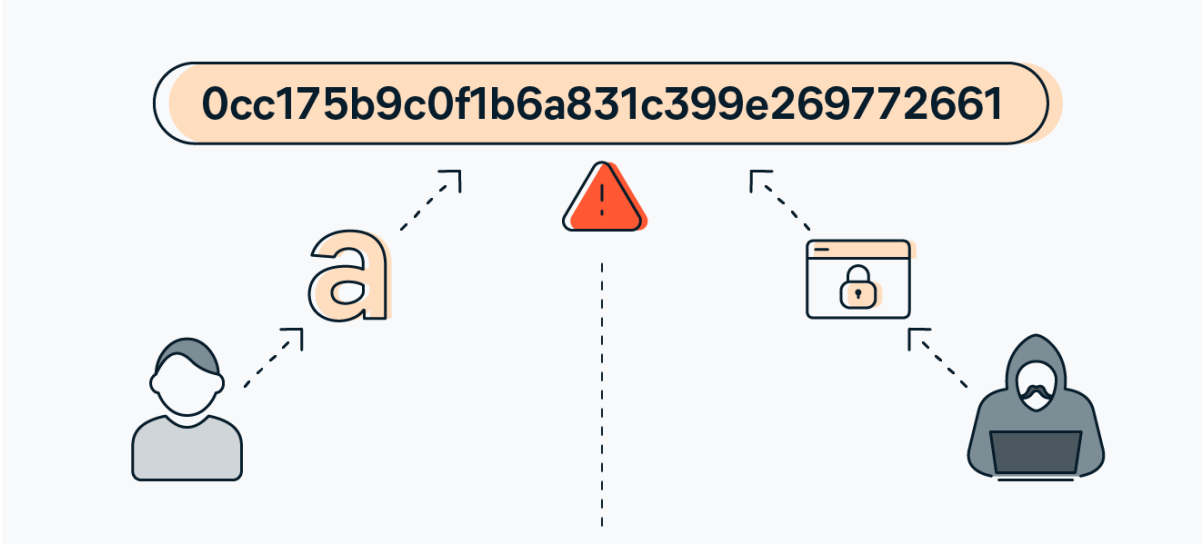
Advantages of MD5 Algorithm:

- **MD5 is faster and simple to understand.**
- **MD5 algorithm generates a strong password in 16 bytes format. All developers like web developers etc use the MD5 algorithm to secure the password of users.**
- **To integrate the MD5 algorithm, relatively low memory is necessary.**
- **It is very easy and faster to generate a digest message of the original message.**

Disadvantages of MD5 Algorithm:

- **MD5 generates the same hash function for different inputs.**
- **MD5 provides poor security over SHA1.**
- **MD5 has been considered an insecure algorithm. So now we are using SHA256 instead of MD5**
- **MD5 is neither a symmetric nor asymmetric algorithm.**

An MD5 hash example looks like this: 0cc175b9c0f1b6a831c399e269772661. That's the hash for the letter "a."



8.a) Explain in detail about the hash functions and their security.

Ans.8.a)

A hash function is a mathematical function that takes an input (or 'message') and produces a fixed-size string of characters, which is typically a hash value or hash code. The output, often a 'digest,' is unique to the specific input, and even a small change in the input should produce a substantially different hash.

Properties of Hash Functions:

1. **Deterministic:**
   - **For the same input, the hash function will always produce the same output.**
2. **Fixed Output Length:**
   - **The output of the hash function is of a fixed size, regardless of the input size.**
3. **Efficient to Compute:**
   - **It should be computationally efficient to calculate the hash value for any given input.**
4. **Pre-image Resistance:**
   - **Given a hash value, it should be computationally infeasible to reverse the process and find an input that produces that hash.**
5. **Collision Resistance:**
   - **It should be unlikely that two different inputs produce the same hash value.**

Security of Hash Functions:

1. **Data Integrity:**
   - **Hash functions are widely used to ensure data integrity. By comparing hash values before and after transmission or storage, one can verify if the data has been altered.**
2. **Password Hashing:**
   - **Hash functions are used to store passwords securely. Rather than storing plaintext passwords, systems store the hash of the password. This way, even if the hash is compromised, the original password is not easily obtainable.**
3. **Digital Signatures:**
   - **In digital signatures, hash functions are used to generate a fixed-size representation of a message, which is then signed. The recipient can use the sender's public key to verify the signature.**
4. **Cryptographic Applications:**
   - **Hash functions are essential in various cryptographic protocols, including HMAC (Hash-based Message Authentication Code), digital certificates, and blockchain.**
5. **Blockchain Technology:**
   - **Hash functions play a crucial role in creating a chain of blocks in blockchain. The hash of a block is included in the subsequent block, ensuring the integrity of the entire chain.**

Security Concerns:

1. **Collision Attacks:**
   - **A collision occurs when two different inputs produce the same hash output. While hash functions aim to minimize the likelihood of collisions, the existence of collision-resistant hash functions is a topic of ongoing research.**
2. **Length Extension Attacks:**
   - **Some hash functions are vulnerable to length extension attacks, where an attacker can extend the hash value without knowing the original input.**
3. **Algorithmic Vulnerabilities:**
   - **Cryptographic hash functions need to resist various attacks, such as birthday attacks and differential cryptanalysis.**

Common Hash Functions:

1. **MD5 (Message Digest Algorithm 5):**
   - **Previously widely used but now considered insecure due to vulnerabilities.**
2. **SHA-1 (Secure Hash Algorithm 1):**
   - **Also deprecated due to vulnerabilities; SHA-256 and SHA-3 are more secure alternatives.**
3. **SHA-256 (Secure Hash Algorithm 256-bit):**
   - **Part of the SHA-2 family, commonly used in blockchain and other security protocols.**
4. **SHA-3 (Secure Hash Algorithm 3):**
   - **The latest member of the Secure Hash Algorithm family, designed to provide the same security as SHA-2.**

8.b) What is Kerberos? Explain briefly about it.

Ans.8.b)

Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users. In Kerberos Authentication server and database is used for client authentication. Kerberos runs as a third-party trusted server known as the Key Distribution Center (KDC). Each user and service on the network is a principal.

The main components of Kerberos are:

- **Authentication Server (AS):**
  The Authentication Server performs the initial authentication and ticket for Ticket Granting Service.
- **Database:**
  The Authentication Server verifies the access rights of users in the database.
- **Ticket Granting Server (TGS):**
  The Ticket Granting Server issues the ticket for the Server.

Kerberos Limitations

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

Applications of Kerberos

i. **User Authentication**
ii. **Single Sign-On (SSO)**
iii. **Mutual Authentication**
iv. **Authorization**
v. **Network Security**

9.a) What is firewall? What are its type? Explain in brief.

Ans.9.a)

Network Firewalls are the devices that are used to prevent private networks from unauthorized access. A Firewall is a security solution for the computers or devices that are connected to a network, they can be either in form of hardware as well as in form of software. It monitors and controls the incoming and outgoing traffic (the amount of data moving across a computer network at any given time).

The major purpose of the network firewall is to protect an inner network by separating it from the outer network. Inner Network can be simply called a network created inside an organization and a network that is not in the range of inner network can be considered as Outer Network.

Types of Network Firewall :

1. **Packet Filters –**
   It is a technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols, and ports. This firewall is also known as a static firewall.

2. **Stateful Inspection Firewalls –**
   It is also a type of packet filtering which is used to control how data packets move through a firewall. It is also called dynamic packet filtering. These firewalls can inspect that if the packet belongs to a particular session or not. It only permits communication if and only if, the session is perfectly established between two endpoints else it will block the communication.

3. **Application Layer Firewalls –**
   These firewalls can examine application layer (of OSI model) information like an HTTP request. If finds some suspicious application that can be responsible for harming our network or that is not safe for our network then it gets blocked right away.

4. **Next-generation Firewalls –**
   These firewalls are called intelligent firewalls. These firewalls can perform all the tasks that are performed by the other types of firewalls that we learned previously but on top of that, it includes additional features like application awareness and control, integrated intrusion prevention, and cloud-delivered threat intelligence.

5. **Circuit-level gateways –**
   A circuit-level gateway is a firewall that provides User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) connection security and works between an Open Systems Interconnection (OSI) network model's transport and application layers such as the session layer.

6. **Software Firewall –**
   The software firewall is a type of computer software that runs on our computers. It protects our system from any external attacks such as unauthorized access, malicious attacks, etc. by notifying us about the danger that can occur if we open a particular mail or if we try to open a website that is not secure.

7. **Hardware Firewall –**
   A hardware firewall is a physical appliance that is deployed to enforce a network boundary. All network links crossing this boundary pass-through this firewall, which enables it to perform an inspection of both inbound and outbound network traffic and enforce access controls and other security policies.

8. **Cloud Firewall –**
   These are software-based, cloud-deployed network devices. This cloud-based firewall protects a private network from any unwanted access. Unlike traditional firewalls, a cloud firewall filters data at the cloud level.

9.b) Explain in detail about SQL injection?

Ans.9.b)

SQL injection is a type of cyberattack that occurs when an attacker is able to insert or manipulate malicious SQL code into a query, typically through user inputs in web applications or other software that interacts with a database. The goal of SQL injection attacks is to manipulate the SQL queries executed by the application's database, often leading to unauthorized access, data manipulation, or other malicious activities.

How SQL Injection Works:

1. **User Input Vulnerability:**
   - **SQL injection usually occurs when a web application doesn't properly validate or sanitize user inputs before including them in SQL queries.**
2. **Malicious Input:**
   - **An attacker submits specially crafted input, often in the form of SQL code, into input fields or parameters expected by the application.**
3. **Injection Points:**
   - **The attacker aims to exploit injection points where user input is directly concatenated into SQL queries.**
4. **Manipulating SQL Queries:**
   - **The injected SQL code becomes part of the query executed by the database server, leading to unintended and potentially harmful consequences.**

Types of SQL Injection:

1. **Classic SQL Injection:**
   - **Occurs when attackers inject malicious SQL code into user input fields, such as login forms or search boxes.**
2. **Blind SQL Injection:**
   - **Attackers infer information from the database by injecting queries that result in true or false conditions. The application's response helps them deduce the structure or content of the database.**
3. **Time-Based Blind SQL Injection:**
   - **Similar to blind SQL injection, but the attacker induces the server to wait for a specified time before responding, revealing information based on the delay.**
4. **Union-Based SQL Injection:**
   - **Involves injecting a SQL UNION statement to combine the results of the original query with results from another query, allowing attackers to extract data.**
5. **Error-Based SQL Injection:**
   - **Exploits SQL errors generated by the application to extract information about the database structure or content.**

Preventing SQL Injection:

1. **Parameterized Queries:**
   - **Use parameterized queries or prepared statements that separate SQL code from user input.**
2. **Input Validation and Sanitization:**
   - **Validate and sanitize user inputs to ensure they conform to expected formats and don't include malicious code.**
3. **Least Privilege Principle:**
   - **Limit database user permissions to the minimum necessary for the application to function, reducing the potential impact of an SQL injection attack.**
4. **Use ORM (Object-Relational Mapping) Libraries:**
   - **ORM libraries often provide abstraction layers that help prevent direct SQL injection by handling SQL queries behind the scenes.**
5. **Stored Procedures:**
   - **Use stored procedures with parameterized inputs to encapsulate SQL logic and minimize the risk of injection.**
6. **Web Application Firewalls (WAF):**
   - **Implement a WAF to filter and monitor HTTP traffic, blocking known SQL injection patterns.**
7. **Regular Security Audits:**
   - **Regularly audit and test web applications for security vulnerabilities, including SQL injection, to identify and address potential risks.**

10.a) Discuss in detail about application gateway firewall.

Ans.10.a)

An application gateway is a network device or service that provides application-layer functions, such as protocol translation, content filtering, and load balancing. It operates at the application layer (Layer 7) of the OSI model and can handle various protocols and applications.

Key functions of an application gateway may include:

1. **Protocol Conversion:**
   - **Translating between different network protocols to enable communication between systems that use different protocols.**
2. **Load Balancing:**
   - **Distributing incoming network traffic across multiple servers to ensure no single server is overwhelmed, improving reliability and performance.**
3. **SSL Termination:**
   - **Handling the encryption and decryption of SSL/TLS traffic, offloading this process from backend servers.**
4. **Caching:**
   - **Storing frequently accessed data in a cache to reduce latency and improve response times.**
5. **Content Filtering:**
   - **Inspecting and filtering content based on predefined rules or policies.**

Firewall in Computer Networks:

A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules. The primary goal of a firewall is to establish a barrier between a trusted internal network and untrusted external networks, such as the internet.

Key functions of a firewall may include:

1. **Packet Filtering:**
   - **Examining packets of data and allowing or blocking them based on predefined rules. This is often done at the network layer (Layer 3) using rules based on source and destination IP addresses and ports.**
2. **Stateful Inspection:**
   - **Keeping track of the state of active connections and making decisions based on the context of the traffic. Stateful firewalls operate at both the network and transport layers (Layers 3 and 4).**
3. **Proxy Services:**
   - **Acting as an intermediary between clients and servers, forwarding requests and responses to enhance security and privacy.**
4. **Network Address Translation (NAT):**
   - **Modifying network address information in packet headers to allow multiple devices in a private network to share a single public IP address.**

10.b) Explain in detail about PGP.

Ans.10.b)

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

The following are the services offered by PGP:

1. **Authentication:**
2. **Confidentiality**
3. **Compression**
4. **Email Compatibility**
5. **Segmentation**