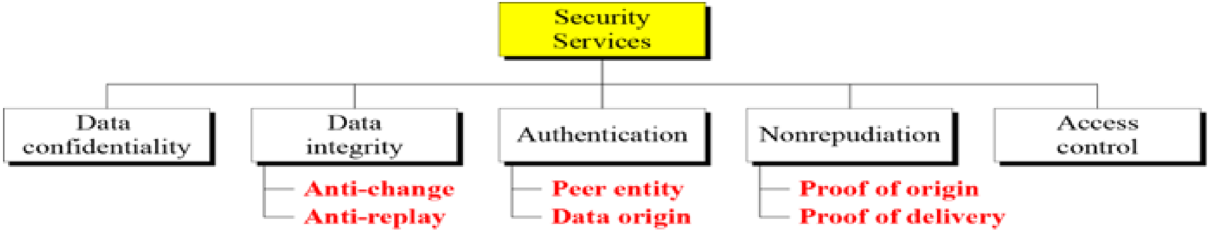
CNS important questions

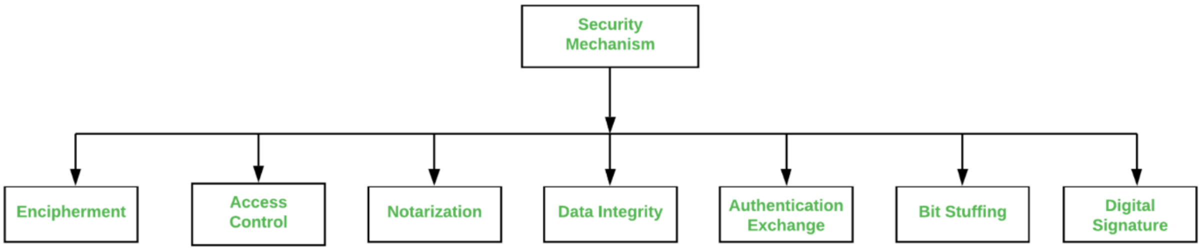
1.security services and mechanisms

Security services



- **Authentication:** assures recipient that the **message is from the source** that it **claims to** be from.
- **Access Control:** controls who can have **access to resource** under what **condition**
- **Availability:** available to authorized entities for 24/7.
- **Confidentiality:** information is not made available to unauthorized individual
- **Integrity:** assurance that the message is unaltered
- **Non-Repudiation:** protection against denial of sending or receiving in the communication

Security Mechanisms



Encipherment :

This security mechanism deals with hiding and covering of data which helps data to become confidential

Access Control :

This mechanism is used to stop unattended access to data which you are sending.

Notarization :

This security mechanism involves use of trusted third party in communication. It acts as mediator between sender and receiver so that if any chance of conflict is reduced.

Data Integrity :

This security mechanism is used by appending value to data to which is created by data itself. It is similar to sending packet of information known to both sending and receiving parties and checked before and after data is received.

Authentication exchange :

This security mechanism deals with identity to be known in communication. This is achieved at the TCP/IP layer where two-way handshaking mechanism is used to ensure data is sent or not

Bit stuffing :

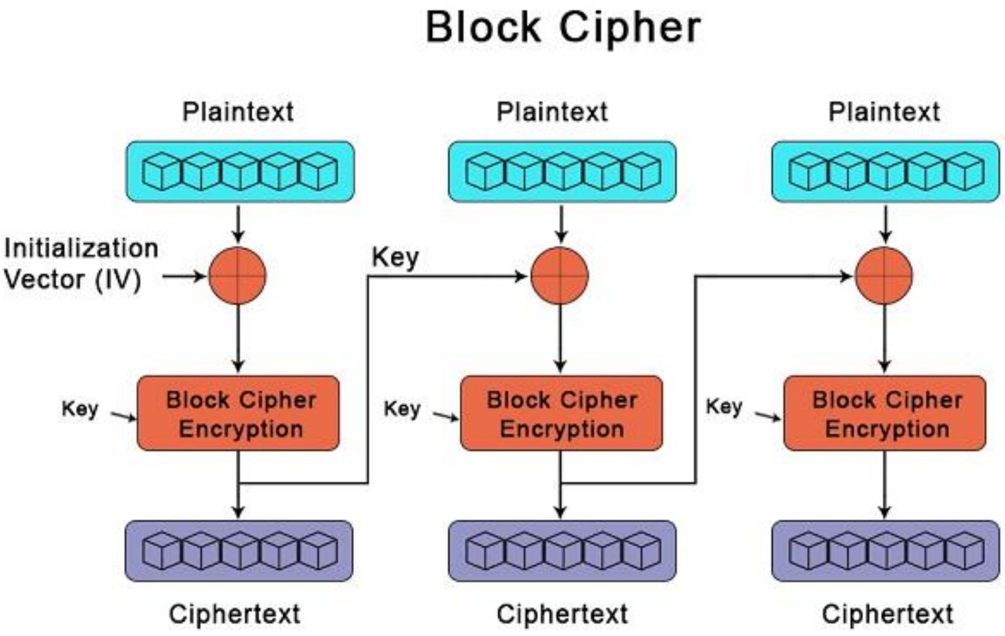
This security mechanism is used to add some extra bits into data which is being transmitted. It helps data to be checked at the receiving end and is achieved by Even parity or Odd Parity.

Digital Signature :

This security mechanism is achieved by adding digital data that is not visible to eyes. It is form of electronic signature which is added by sender which is checked by receiver electronically.

2.explain about stream cipher and block cipher

Block cipher and **stream cipher** are members of the family of **symmetric key ciphers,** essentially encryption techniques used for directly transforming the **plaintext** into **ciphertext**.

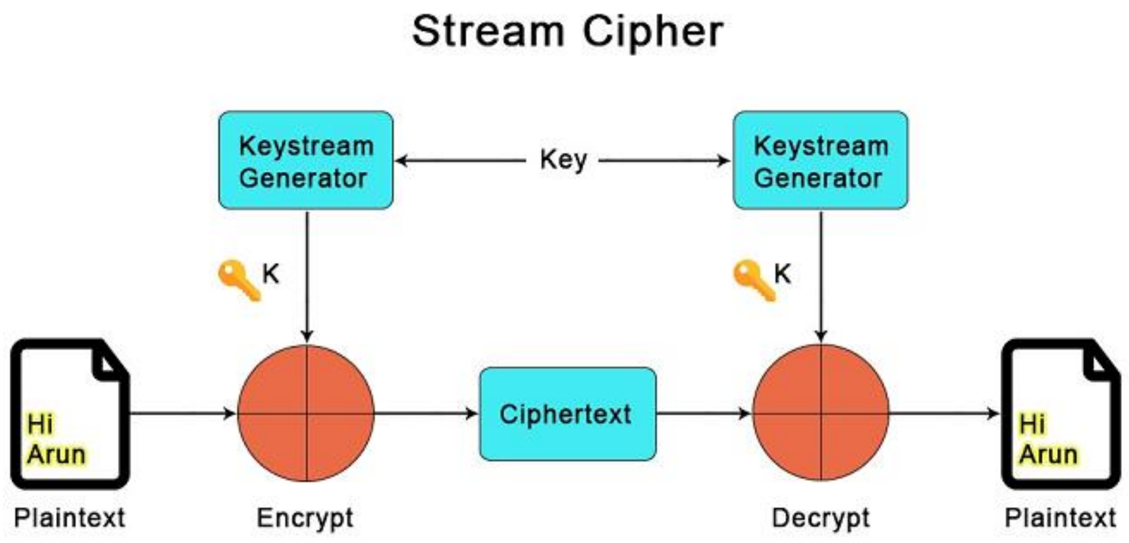


A **block cipher** is a ***symmetric cryptographic technique*** which we used to ***encrypt a fixed-size data block using a shared, secret key.*** During **encryption,** we used ***plaintext*** and **ciphertext** is the resultant encrypted text. It uses the same key to encrypt both the ***plaintext,*** and the ***ciphertext.***

A **block cipher** processes the data blocks of fixed size. Typically, a message's size exceeds a block's size. As a result, the lengthy message is broken up into a number of sequential message blocks, and the cipher operates on these blocks one at a time.

There are various modes of operation of a block cipher:

- Electronic Code Book (ECB) Mode
- Cipher Block Chaining (CBC) Mode
- Cipher Feedback (CFB) Mode
- Output Feedback (OCB) Mode
- Counter (CTR) Mode



stream cipher is a type of encryption that uses plain text numbers and a stream of pseudorandom cipher digits. Each binary digit receives one bit at a time of this pseudorandom encryption digit stream. This encryption technique uses an infinite number of pseudorandom cipher digits for each key.
State cipher is another name for a stream cipher. The term "state cipher" refers to a system where the encryption of each number is dependent on the cipher's current state.

There are two types of Stream Ciphers:

1. **Synchronous Stream Ciphers**

   In a **synchronous stream cipher,** the **keystream block** is created independently of the previous ciphertext and plaintext messages

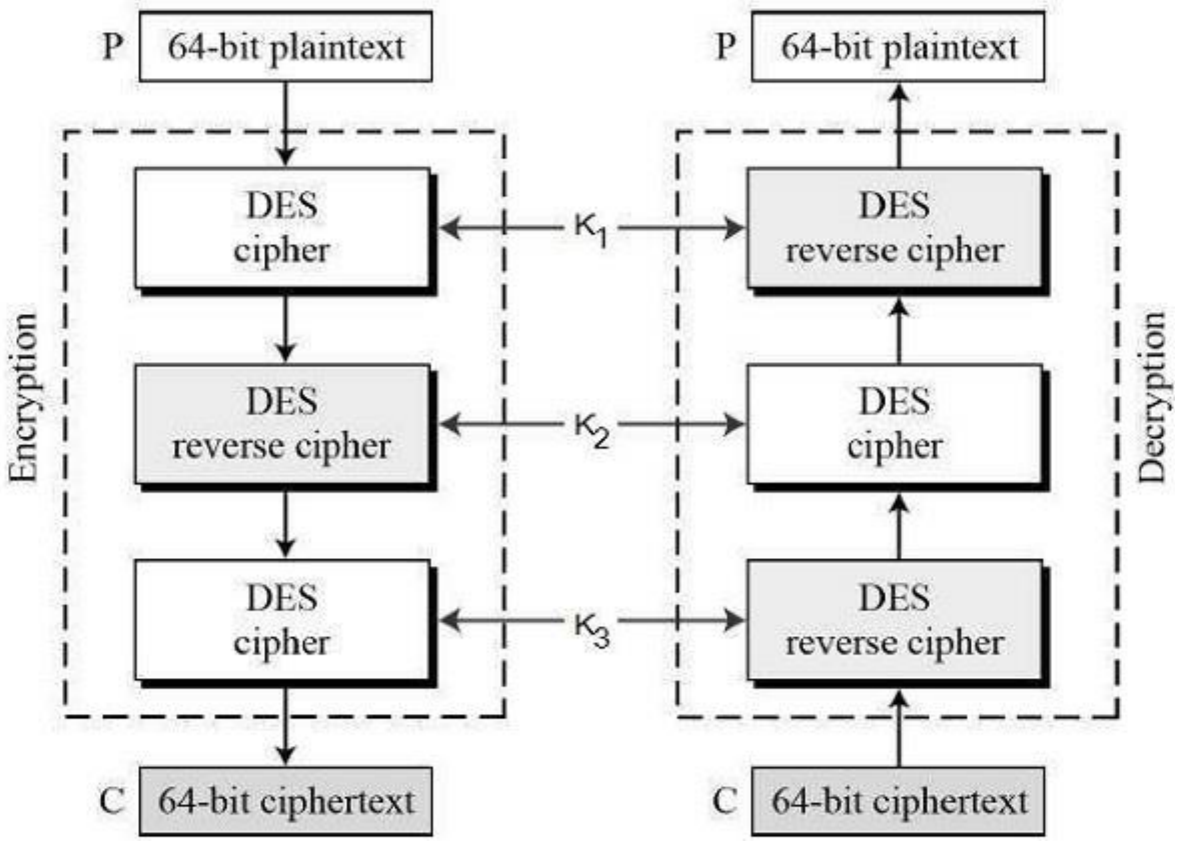
2. **Self-Synchronizing/Asynchronous stream Ciphers**
   Asynchronous stream cipher can recognize active attacks by altering the ciphertext, which changes the information in the subsequent keystream

3.DES algorithm

In the field of cryptography, Triple DES (3-DES) is a symmetric-key block cypher that encrypts each data block three times using the Data Encryption Standard (DES) encryption algorithm.

3-KEY Triple DES

Before using 3TDES, user first generate and distribute a 3TDES key K, which consists of three different DES keys K_1, K_2 and K_3. This means that the actual 3TDES key has length 3×56 = 168 bits. The encryption scheme is illustrated as follows –



The encryption-decryption process is as follows –

- Encrypt the plaintext blocks using single DES with key K_1.
- Now decrypt the output of step 1 using single DES with key K_2.
- Finally, encrypt the output of step 2 using single DES with key K_3.
- The output of step 3 is the ciphertext.
- Decryption of a ciphertext is a reverse process. User first decrypt using $K_{3,}$ then encrypt with $K_{2,}$ and finally decrypt with K_1.

Due to this design of Triple DES as an encrypt–decrypt–encrypt process, it is possible to use a 3TDES (hardware) implementation for single DES by setting $K_{1,}$ $K_{2,}$ and K_3 to be the same value. This provides backwards compatibility with DES.

Second variant of Triple DES (2TDES) is identical to 3TDES except that $K_3$is replaced by K_1. In other words, user encrypt plaintext blocks with key $K_{1,}$ then decrypt with key $K_{2,}$ and finally encrypt with K_1 again. Therefore, 2TDES has a key length of 112 bits.

Triple DES systems are significantly more secure than single DES, but these are clearly a much slower process than encryption using single DES.

4.Eulers algorithm with example

Euler's Theorem

Euler's theorem is a generalization of Fermat's little theorem. Euler's theorem extends Fermat's little theorem by removing the imposed condition where n must be a prime number. This allows Euler's theorem to be used on a wide range of positive integers. It states that if a random positive integer a and n are co-prime, then a raised to the power Euler's totient function $\varphi(n)$ is congruent to 1 $(mod\, n)$. The mathematical form is as follows:

$$a^{\varphi(n)} \cong 1\,(mod\, n)$$

However, if n is a prime number, Euler's theorem is simplified to Fermat's little theorem as follows:

$$a^{\varphi(n)} \cong 1\,(mod\, n)$$

As $\varphi(n) = n - 1$, where n is a prime number, we can plug the value of the totient function into the equation above resulting in the equation as follows:

$$a^{n-1} \cong 1\,(mod\, n)$$

Let $a = 4$ and $n = 7$, a and n are co-prime as their greatest common divisor is 1. Now plug the values into Euler's equation above resulting in the equation as follows:

$$4^{\varphi(7)} \cong 1\,(mod\, 7)$$

As $\varphi(7) = 6$, we plug this value into the equation above resulting in the equation as follows:

$$4^{6} \cong 1\,(mod\, 7)$$

We then simplify it as follows:

$$4096 \cong 1\,(mod\, 7)$$

This equation suggests if we divide 4096 by 7, we will get a reminder of 1. This proves that Euler's theorem is valid on the given values.

5.chinese remainder theorem

- One of the most useful results of number theory is the Chinese Remainder Theorem (CRT).
- The CRT says it is possible to reconstruct integers in a certain range from their residues modulo a set of pairwise relatively prime moduli.
- The CRT can be stated in several ways. We present here a formulation that is most useful. An alternative formulation is explored. Let

  M = $\prod_{i=1}^{k} mi$

Where the m_i are pairwise relatively prime;

that is gcd (m_i,m_j) = 1 for $1 \leq i, j \leq k$, and $i \neq j$.

- We can represent any integer in Z_m by a k- tuple whose elements are in Z_{mi} using the following correspondence:

  A <-> (a_1, a_2, … , a_k),

where A € Z_m, a_i € Z_{mi}, and ai = A mod m_i for $1 \leq i \leq k$.

- **The CRT makes two assertions:**
- Let us demonstrate the **first assertion**. The transformation from A to (a_1, a_2, … , a_k), is obviously unique; just take $a_i = A$ mod $m_{i.}$
- Computing A from (a_1, a_2, … , a_k) can be done as follows:
- Let M_i = M/m_i for $1 \leq i \leq k$. Note that $M_i = m_1$ X m_2 X … X m_{i-1} X m_{i+1} X … X m_k, so that $M_i \equiv 0$ (mod m_j) for all $j \neq i$. Then let

  $c_i = M_i$ X (M_i^{-1} mod m_i *)* for $1 \leq i \leq k$.

- By the definition of M_i, it is relatively prime to m_i and therefore has a unique multiplicative inverse mod m_i. So Equation c_i is well defined and produces a unique value C_i. We can now compute

A ≡ ($\sum_{i=1}^{k} aici$) (mod m)

- To show that the value of A produced by equation is correct, we must show that a_i = A mod mi for $1 \leq i \leq k$. Note that $C_j \equiv M_j \equiv 0$ (mod m_i) if $j \neq i$ and that $c_i \equiv 1$ (mod m_i). It follows that a_i = A mod $m_{i.}$

- The **second assertion** of the CRT, concerning arithmetic operations, follows from the rules for modular arithmetic. That is, the second assertion can be stated as follows: If

  $A <-> (a_1, a_2, \ldots , a_k)$

  $B <-> (b_1, b_2, \ldots , b_k)$

Then

$(A + B) \bmod M <-> ((a_1 + b_1) \bmod m_1, \ldots , (a_k + b_k) \bmod m_k)$

$(A - B) \bmod M <-> ((a_1 - b_1) \bmod m_1, \ldots , (a_k - b_k) \bmod m_k)$

$(A X B) \bmod M <-> ((a_1 X b_1) \bmod m_1, \ldots , (a_k X b_k) \bmod m_k)$

6.general solution for 40x+16y=88

Given an equation `ax + by = n`

1. Use the Euclidean algorithm to compute `gcd(a, b) = d`.
2. Determine whether `d | n`. If not, then there are no solutions.
3. Reformat the equations from the Euclidean algorithm.
4. Using substitution, go through the steps of the Euclidean algorithm to find a solution to the equation $ax_i + by_i = d$.
5. The initial solution to the equation `ax + by = n` is the ordered pair $(x_i . n/d, y_i . n/d)$.

```
40x + 16y = 88
GCD(40, 16) = 8
The given equation has Infinite solutions.
Reduced Equation: 5s + 2t = 1
General solution:
x = 11 + 2k for any integer m
y = -22 – 5k for any integer m
```

7.Attacks on security goals

The security attacks aim to compromise the five major security goals for network security (extended from CIA requirements): *Confidentiality*, *Availability*, *Authentication*, *Integrity* and *Nonrepudiation*.

Types of attacks are as follows:

- **Masquerade-**
  A masquerade attack takes place when one entity pretends to be a different entity. A Masquerade attack involves one of the other forms

of active attacks.Masquerade assaults may be performed using the stolen passwords and logins.

- **Modification of messages-**
  It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorized effect. Modification is an attack on the integrity of the original data.
- **Repudiation-**
  This attack occurs when the network is not completely secured or the login control has been tampered with. With this attack, the author's information can be changed by actions of a malicious user in order to save false data in log files, up to the general manipulation of data on behalf of others, similar to the spoofing of e-mail messages.
- **Replay-**
  It involves the passive capture of a message and its subsequent transmission to produce an authorized effect
- **Denial of Service-**
  It prevents the normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination.

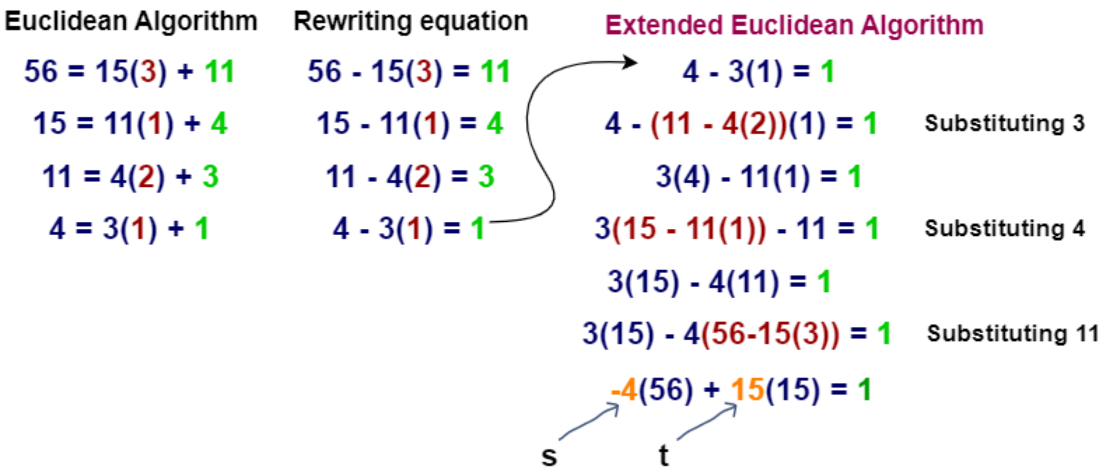
8.Explain extended Euclidean algorithm.find GCD ???

Extended Euclidean Algorithm is an extension of the *Euclidean Algorithm* that computes the greatest common divisor (GCD) of integers *a* and *b.*

In addition to computing GCD, Extended Euclidean Algorithm also finds integers s and t such that $as + bt = gcd(a, b)$.

Bézout's Identity guarantees the existence of s and t.

Extended Euclidean Algorithm finds s and t by using back substitutions to recursively rewrite the division algorithm equation until we end up with the equation that is a linear combination of our initial numbers. Below is an example of how to use the Extended Euclidean Algorithm to find the GCD of 56 and 15 to find s and t such that $56s + 15t = gcd(56, 15)$



Euclidean Algorithm	Rewriting equation
56 = 15(3) + 11	56 - 15(3) = 11
15 = 11(1) + 4	15 - 11(1) = 4
11 = 4(2) + 3	11 - 4(2) = 3
4 = 3(1) + 1	4 - 3(1) = 1

Extended Euclidean Algorithm

4 - 3(1) = 1

4 - (11 - 4(2))(1) = 1 Substituting 3

3(4) - 11(1) = 1

3(15 - 11(1)) - 11 = 1 Substituting 4

3(15) - 4(11) = 1

3(15) - 4(56-15(3)) = 1 Substituting 11

-4(56) + 15(15) = 1

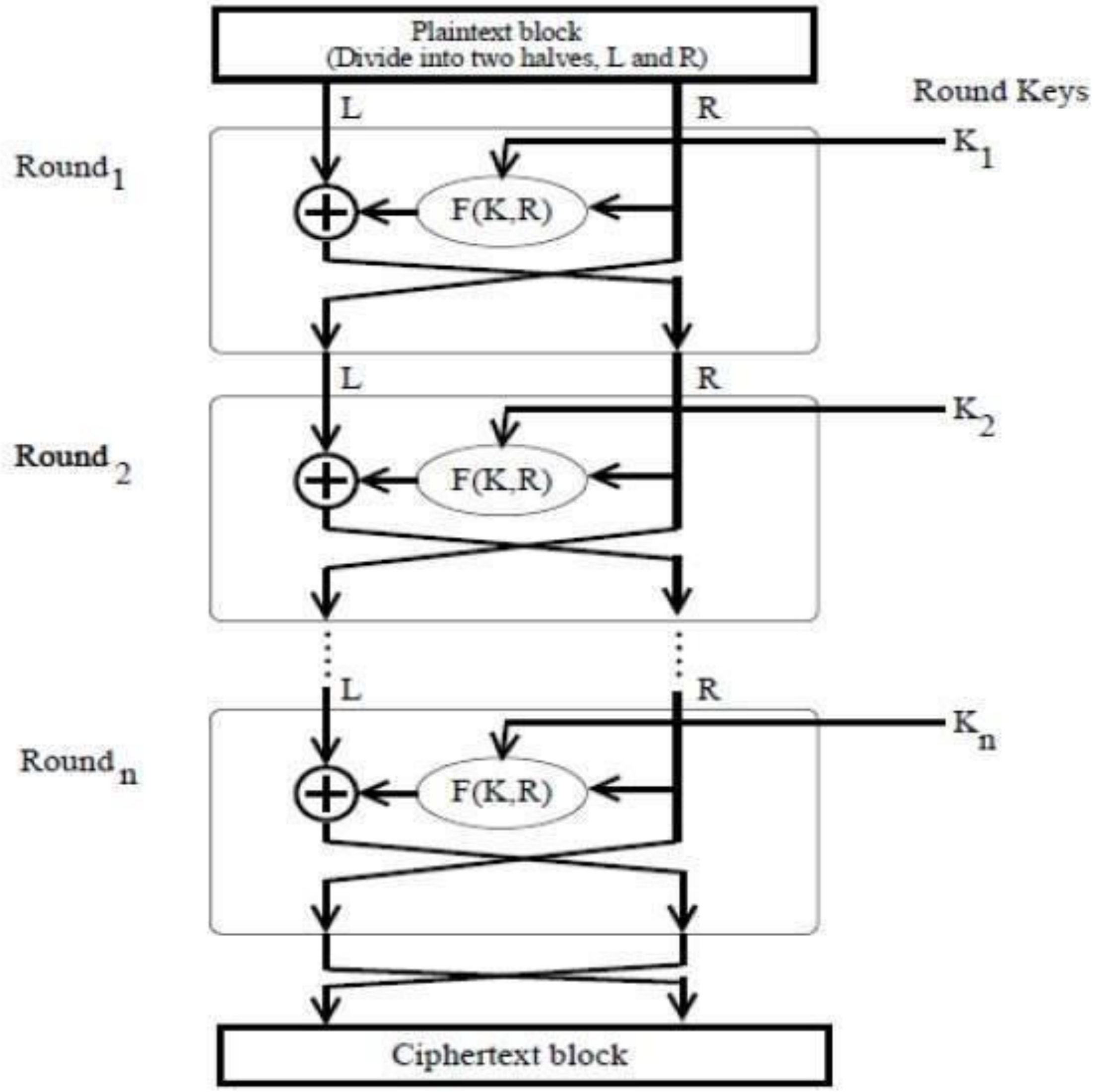
9.Fiestal structure with diagram

Feistel Cipher is a design model from which many different block ciphers are derived. DES is just one example of a Feistel Cipher. A cryptographic system based on Feistel cipher structure uses the same algorithm for both encryption and decryption.

Encryption Process

The encryption process uses the Feistel structure consisting multiple rounds of processing of the plaintext, each round consisting of a "substitution" step followed by a permutation step.

Feistel Structure is shown in the following illustration –



- The input block to each round is divided into two halves that can be denoted as L and R for the left half and the right half.
- In each round, the right half of the block, R, goes through unchanged. But the left half, L, goes through an operation that depends on R and the encryption key. First, we apply an encrypting function ‘f’ that takes two input – the key K and R. The function produces the output f(R,K). Then, we XOR the output of the mathematical function with L.
- In real implementation of the Feistel Cipher, such as DES, instead of using the whole encryption key during each round, a round-dependent key (a subkey) is derived from the encryption key. This means that each round uses a different key, although all these subkeys are related to the original key.
- The permutation step at the end of each round swaps the modified L and unmodified R. Therefore, the L for the next round would be R of the current round. And R for the next round be the output L of the current round.

- Above substitution and permutation steps form a ‘round’. The number of rounds are specified by the algorithm design.
- Once the last round is completed then the two sub blocks, ‘R’ and ‘L’ are concatenated in this order to form the ciphertext block.

Decryption Process

The process is said to be almost similar and not exactly same. In the case of decryption, the only difference is that the subkeys used in encryption are used in the reverse order.

The final swapping of ‘L’ and ‘R’ in last step of the Feistel Cipher is essential. If these are not swapped then the resulting ciphertext could not be decrypted using the same algorithm.

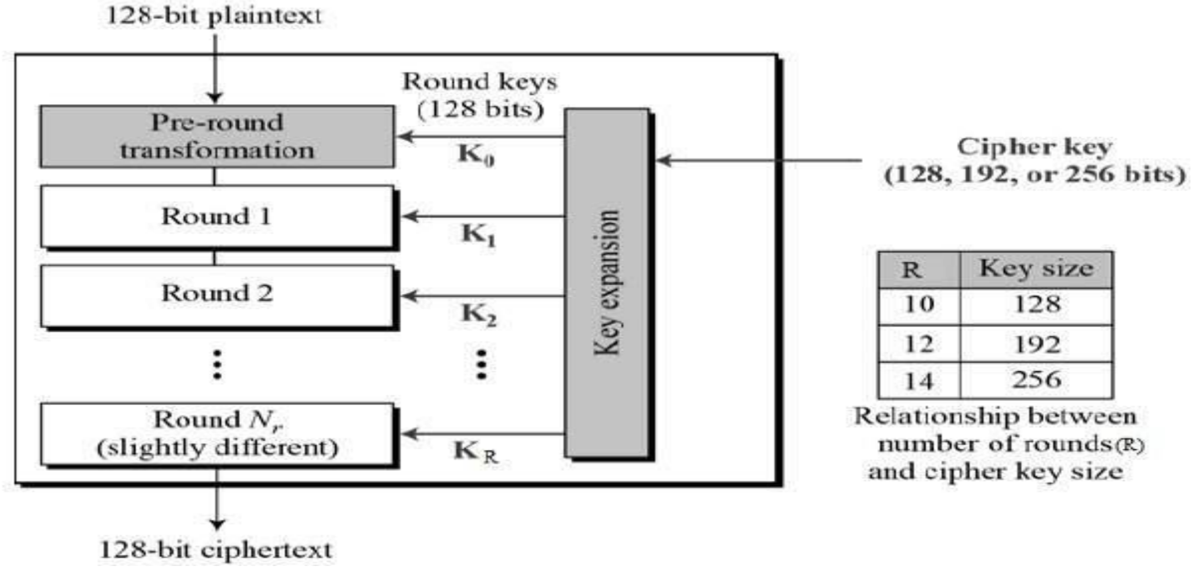
10.AES ALGORITHM

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.

The features of AES are as follows –

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

The schematic of AES structure is given in the following illustratio



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

4 steps of algorithm:

Byte Substitution (SubBytes)

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

Shiftrows

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row.

MixColumns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column.

The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

Addroundkey

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

11.Compare symmetric and asymmetric key

Symmetric Key Encryption	Asymmetric Key Encryption
It only requires a single key for both encryption and decryption.	It requires two keys, a public key and a private key, one to encrypt and the other one to decrypt.
The size of cipher text is the same or smaller than the original plain text.	The size of cipher text is the same or larger than the original plain text.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data is required to transfer.	It is used to transfer small amounts of data.

Symmetric Key Encryption	Asymmetric Key Encryption
It only provides confidentiality.	It provides confidentiality, authenticity, and non-repudiation.
The length of key used is 128 or 256 bits	The length of key used is 2048 or higher
In symmetric key encryption, resource utilization is low as compared to asymmetric key encryption.	In asymmetric key encryption, resource utilization is high.
It is efficient as it is used for handling large amount of data.	It is comparatively less efficient as it can handle a small amount of data.
Security is less as only one key is used for both encryption and decryption purpose.	It is more secure as two keys are used here- one for encryption and the other for decryption.
The Mathematical Representation is as follows- $P = D (K, E(P))$ where K –> encryption and decryption key P –> plain text D –> Decryption E(P) –> Encryption of plain text	The Mathematical Representation is as follows- $P = D(Kd, E (Ke,P))$ where Ke –> encryption key Kd –> decryption key D –> Decryption E(Ke, P) –> Encryption of plain text using encryption key Ke . P –> plain text

12.Diffie hellman key exchange

The Diffie-Hellman algorithm is being used to establish a shared secret that can be used for secret communications while exchanging data over a public network using the elliptic curve to generate points and get the secret key using the parameters.

- For the sake of simplicity and practical implementation of the algorithm, we will consider only 4 variables, one prime P and G (a primitive root of P) and two private values a and b.
- P and G are both publicly available numbers. Users (say Alice and Bob) pick private values a and b and they generate a key and exchange it publicly. The opposite person receives the key and that generates a secret key, after which they have the same secret key to encrypt.

Step by Step Explanation

Alice	Bob
Public Keys available = P, G	Public Keys available = P, G
Private Key Selected = a	Private Key Selected = b
Key generated = $k_a = y^a modP$	Key generated = $k_b = x^b modP$
Exchange of generated keys takes place	
Key received = y	key received = x
Generated Secret Key =	Generated Secret Key =
Algebraically, it can be shown that $k_a = k_b$	
Users now have a symmetric secret key to encrypt	

Example:

```
Step 1: Alice and Bob get public numbers P = 23, G = 9


Step 2: Alice selected a private key a = 4 and
        Bob selected a private key b = 3


Step 3: Alice and Bob compute public values
Alice:    x =(9^4 mod 23) = (6561 mod 23) = 6
        Bob:    y = (9^3 mod 23) = (729 mod 23)  = 16
```

```
Step 4: Alice and Bob exchange public numbers


Step 5: Alice receives public key y =16 and
        Bob receives public key x = 6


Step 6: Alice and Bob compute symmetric keys
        Alice:  ka = y^a mod p = 65536 mod 23 = 9
        Bob:    kb = x^b mod p = 216 mod 23 = 9


Step 7: 9 is the shared secret.
```

13.elgomal cryptography

ElGamal encryption is a public-key cryptosystem. It uses asymmetric key encryption for communicating between two parties and encrypting the message.

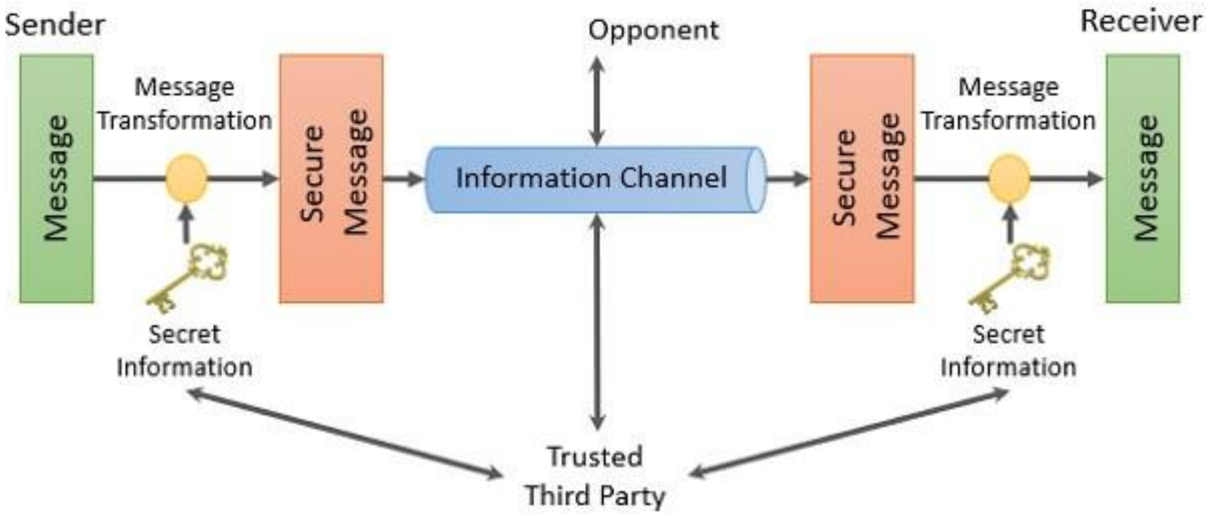
This cryptosystem is based on the difficulty of finding **discrete logarithm** in a cyclic group that is even if we know g^a and g^k, it is extremely difficult to compute g^{ak}.

Idea of ElGamal cryptosystem

Suppose Alice wants to communicate with Bob.

1. Bob generates public and private keys:
   - Bob chooses a very large number **q** and a cyclic group $\mathbf{F}_q$.
   - From the cyclic group $\mathbf{F}_q$, he choose any element **g** and an element **a** such that gcd(a, q) = 1.
   - Then he computes $h = g^a$.
   - Bob publishes **F**, $\mathbf{h = g^a}$, **q**, and **g** as his public key and retains **a** as private key.
2. Alice encrypts data using Bob’s public key :
   - Alice selects an element **k** from cyclic group **F** such that gcd(k, q) = 1.
   - Then she computes $p = g^k$ and $s = h^k = g^{ak.}$
   - She multiples s with M.
   - Then she sends $(p, M*s) = (g^k, M*s)$.
3. Bob decrypts the message :
   - Bob calculates $s' = p^a = g^{ak}$.
   - He divides M*s by s' to obtain M as $s = s'$.

14.block diagram of network security



Network Security Model