Cryptography and Network security

UNIT-1 :

PART-A : Basic principles.

1. Security goals
2. Cryptographic attacks
3. Services and Mechanism.
4. Mathematics of cryptography.
   a. Integer
   b. arthematic
   c. Extended Eucledian Algorithm.
   d. Modular Arithematic.
   e. Matrices.
   f. Linear Congruence.

PART-B : Symmetric Encryption.

1. Mathematics of symmetric key cryptography.
   a. Algebraic structures.
   b. Group
   c. Ring
   d. Field
   e. GF (2^n) Field.
2. Introduction to modren symmetric key ciphers.
   a. Modren Block ciphers for Encryption
   b. components of Modren Block ciphers.
   c. Two classes of product ciphers.
   d. Attacks designed for block ciphers.
   e. Stream ciphers.
3. DES (Data Encryption standard)

a. History of DES
b. DES structure
c. DES analysis
d. Security of DES
e. Multiple DES

4. Advanced Encryption standard (AES)
a. History of AES
b. Transformation used by AES
c. Key expansion
d. AES cipher
e. Analysis of AES

UNIT-I

PART-A: Basic principles

1. Security Goals.

The security goals in a Network are categorized into Three types. They are

1. Confidentiality
2. Integrity
3. Availability

1. Confidentiality:

→ It relates to protect the information by hiding The content from unauthourized users.

→ confidentiality is applied while storing The information and also applied during The Transmission of information.

2. Integrity:

→ When The changes in The information are to be done constantly, It should be done only by The authourized entity, This process leads to Integrity.

3. Availability:

→ The information which is created and stored by an organization must be made available to the authourized Entity.

2. Cryptographic attacks.

The cryptographic attacks are categorized into two types, They are

1. Crypt-Analytic attacks.
2. Non Crypt-Analytic attacks

1. Crypt-Analytic attacks:

→ These attacks uses statistical and algebraic techniques along with a secret key on the cipher text.

→ The objective of the cryptanalytics (crypt-analysis) is to find the properties of the cipher text.

→ The attacker looks for a distinguished property and guesses the key which is applied on the cipher Text.

→ Most of the cryptanalytic attacks uses divide and conquer policy, which reduces the complexity of guessing the key, which leads to Brute force attack.

2. Non-Cryptanalytic attacks:

→ The Non-cryptanalytic attacks mainly focus on the confidentiality, integrity and availability.

→ The confidentiality Threats are snooping and Traffic analysis.

→ The integrity Threats are modification, masque reading, replaying and repudiation.

→ The availability Threat is denial of service.

→ Snooping: It refers to unauthorized access or intersection of data.

→ Traffic Analysis: Here We obtain information by monitoring the online Traffic.

→ Modification: After Accessing the information the attacker modifies the information for his benefit.

→ Masque Reading: It is the process of impersinate someone else ie, the attacker steals the atm card number and pin from a person and pretend himself/herself as a customer.

→ Replaying : The attacker obtains a copy of a message used by a user and later tries to use that message.

→ Repudiation : It is performed by Two parties during communication These Two parties are sender and Receiver where They sometimes do not accept the Transaction.

→ Denial of service : The Denial of service is very common attack where user requests are not accepted by a server.

3. Services and Mechanism.

Security services and security mechanisms are provided by "ITU-T" (International Telecommunication Union for Telecommunication sector).

Security Services :

The security services are defined by ITU-T (X.800)

* The security services are categorized into 5 types. They are
  (1) Data confidentiality
  (2) Data Integrity
  (3) Authentication
  (4) Non-Repudiation
  (5) Access control.

(1) Data Confidentiality :

It is used to protect the data and prevent snooping. When preventing disclosure of information to unauthorized parties is needed, the property of confidentiality is required. To provide confidentiality, The cryptographic algorithm and mode of operation needs to be designed and implemented.

(2) Data Integrity :

It is designed to protect the data from modification, insertion or deletion etc.., Data Integrity provides assurance

The data has not been modified in an unauthorized manner after it was created, Transmitted or stored.

(3) Authentication:

It is used to give to provide access of data to n authorized users only. authentication services are

(1) Integrity authentication

(2) source Authentication.

(4) Non-Repudiation:

This service protects the data either by a sender or a receiver by verifying them with a valid proof. It requires digital Signature Key.

(5) Access control:

The service provide protection against the unautherized access to the data.

Security Mechanisms:

The security mechanisms are defined by ITU-T (X-800). The various security mechanisms are

(1) Encipherment:

It is the process of hiding or convering the data. It provides confidentiality. which can be done by using 2 Techniques. They are

(a) Cryptography

(b) Steganography

(2) Data Integrity:

In This mechanism a short check value is appended to the actual data by the sender which will be revalued only to the receiver. The receiver verifies the check values and processes the data.

(3) Digital signature:

In this mechanism, the sender sends a digital signature electronically to a receiver.

(4) Authentication exchange:

In Authentication exchange two entities exchange data or messages and must prove there identity to each other.

(5) Traffic padding:

It involves adding some relevant data into the actual data Traffic and tries to detect the Traffic analysis.

(6) Routing control:

To provide more security, various routing control strategies are to be used and frequently changed.

(7) Access control:

Various access control mechanisms or Techniques are to be used for better security which are provided in the form of Login name and password.

4. Mathematics of cryptography.

a. Integer Arthematic
b. Extended Euclidian Algorithm.
c. Modular Arthematic
d. Matrices.
e. Linear Congruence.

(a) Integer Arthematic:

→ In integer Arthematic, we use a set of integers and apply some operations.

→ A set of integers are denoted by 'Z' which contains all integer numbers ranging from Negative infinity to positive infinity. i.e., $Z = \{-\infty, \ldots -3, -2, -1, 0, 1, 2, 3 \ldots \ldots, \infty\}$.

→ In cryptography, We mostly use the arthematic operations like addition, subtraction, multiplication and division.

→ To perform a binary operation on any two inputs will lead

to four possible outputs.

ex: Let two inputs 5 and 9, by applying addition on these two inputs will provide four possible outputs.

Addition : Inputs : 5, 9

$(+5) + (+9) = 14$

$(-5) + (-9) = -14$

$(+5) + (-9) = -4$

$(-5) + (+9) = 4.$

Hence, The possible outputs ~~are~~ for 5 and 9 are (-14, -4, 4, 14)

Integer Division:

→ In Integer Arthematic, if we divide a number with another, we get a remainder, Quotient.

→ let The ~~te~~ number we divide is denoted by 'A' and devisor is denoted by "n", Quotient is denoted by 'Q' and remainder is denoted by 'R". Here the relationship between above four integers which are denoted by A, Q, n and R is denoted by $\boxed{A = Q \times n + R}$

ex: let $A = 255$ and $n = 11$. calculate the divisibility rule by using the above formula.

$255 \Leftrightarrow (23 \times 11) + 2$

$\Leftrightarrow 253 + 2$

$\Leftrightarrow 255.$

→ GCD (or) HCF → Highest common factor.

↓

GReatest Common Divisor

→ The GCD or HCF is calculated on two values, where the common multiples of each value are extracted and multiplied to produce GCD.

ex: calculate the GCD for 24 and 48

common factors are $2 \times 2 \times 2 \times 3 \times 1 = 24$

The GCD of 24 and 48 is 24

2 | 24	2 | 48
2 | 12	2 | 24
2 | 6	2 | 12
3 | 3	2 | 6
1	3 | 3
	1
$2 \times 2 \times 2 \times 3 \times 1$	$2 \times 2 \times 2 \times 2 \times 3 \times 1$

(b) Extended Eucledian Algorithm.

→ Eucledian Algorithm: An Eucledian Algorithm is used to find the gcd of two positive numbers based on the following facts.

Fact-1: $\boxed{gcd(a,0) = a}$

From the above fact, if the second integer is zero, then the GCD of the two numbers is the first integer. (Non-zero).

ex: $gcd(2346,0) = 2346$

Fact-2: $\boxed{gcd(a,b) = gcd(b,r)}$

From the above fact, a and b are positive integer values and 'r' is the remainder which is obtained by dividing a/b.

ex: $gcd(36,10)$

$= gcd(10,6)$

$= gcd(6,4)$

$= gcd(4,2)$

$= gcd(2,0)$

$= 2$ (By applying Fact-1)

10)36(3
30
6 → remainder

Fact-3: $\boxed{gcd(a,b) = 1}$ where a,b are prime numbers.

From the above fact, it will be valid when the two numbers are relatively prime.

ex: $gcd(11,37) = 1$

→ Extended Eucledian Algorithm:

→ The extended Eucledian Algorithm is used to calculate the gcd of a,b and also calculate the values of 's' and 't'.

→ Given two integers 'a' and 'b', we need to find 's' and 't' such that

$$\boxed{gcd(a,b) = (s \times a) + (t \times b)}$$

$$= s \cdot a + t \cdot b$$

Algorithm:

1. Initialization

$r_1 \leftarrow a$; $r_2 \leftarrow b$;
$s_1 \leftarrow 1$; $s_2 \leftarrow 0$;
$t_1 \leftarrow 0$; $t_2 \leftarrow 1$;

2. while $(r_2 > 0)$

$Q = r_1 / r_2$;
$r = r_1 - Q \times r_2$; $r_1 \leftarrow r_2$; $r_2 \leftarrow r$;
$S = s_1 - Q \times s_2$; $s_1 \leftarrow s_2$; $s_2 \leftarrow S$;
$t = t_1 - Q \times t_2$; $t_1 \leftarrow t_2$; $t_2 \leftarrow t$;

3. $gcd(a,b) \leftarrow r_1$; $s \leftarrow s_1$; $t \leftarrow t_1$;

Example: Given $a = 161$ and $b = 28$, Find the $gcd(a,b)$ and the values of s and t.

r_1	r_2	r	Q	s_1	s_2	s	t_1	t_2	t
161	28	21	5	1	0	1	0	1	-5
28	21	7	1	0	1	-1	1	-5	6
21	7	0	3	1	-1	4	-5	6	-23
7	0	×	×	-1	4	×	6	-23	×

Hence $s = s_1 = -1$
$t = t_1 = 6$

$gcd(7,0) = 7$

$gcd(a,b) = a \times s + t \times b$
$= 161 \times -1 + 6 \times 28$
$= -161 + 168$
$= 7$

Hence $7 \rightleftharpoons 7$

Hence proved.

From the above example, We infer $r_1 = 7$, $s = -1$, $t = 6$ at the final iteration where $r_2 = 0$.

Hence the assumption $s = -1$ and $t = 6$ for $a = 161$ and $b = 28$ is True.

ex-2 : Given $a = 17$ and $b = 0$, find the gcd (a, b) and the values of s and t.

r_1	r_2	r	Q	s_1	s_2	s	t_1	t_2	t
17	0	x	x	1	0	x	0	1	x

$r_1 = 17$ $\quad s = s_1 = 1$ $\quad t = t_1 = 0$.

$$\gcd(a,b) = s \times a + t \times b$$
$$\downarrow r_1 = (1 \times 17) + (0 \times 0)$$
$$\downarrow 17 = 17$$

LHS = RHS

Hence proved.

From the above example, We infer $r_1 = 17$, $s = 1$, $t = 0$ for $a = 17$ and $b = 0$

ex-3: Given $a = 0$ and $b = 45$, find the gcd (a, b) and the values of s and t.

r_1	r_2	r	Q	s_1	s_2	s	t_1	t_2	t
0	45	0	0	1	0	1	0	1	0
45	0	x	x	0	1	x	1	0	x

$r_1 = 45$ $\quad s = s_1 = 0$ $\quad t = t_1 = 1$

$$\gcd(a,b) = s \times a + t \times b$$
$$\downarrow r_1 = (0 \times 0) + (1 \times 45)$$
$$\downarrow 45 = 45$$

LHS = RHS

Hence proved.

From the above example, We infer $r_1 = 45$, $s = 0$ and $t = 1$ for $a = 0$ and $b = 45$.

(C) Modular Arthematic:

In modular Arthematic, after we divide one integer with another integer, we consider only the remainder value. We will not consider the quotient in the modular Arthematic.

Syntax: $\boxed{a \bmod n = r}$ where $a > n$

From the above syntax, we divide "a" value with "n" value and consider the remainder "r".

ex: 27 mod 5 = 2
36 mod 12 = 0
5 mod 27 = 5
12 mod 36 = 12
} when $a < n$ then a

From the above example, if the "a" value is greater than "n" we calculate the division for a remainder. if "a" value is less than "n", the remainder will be "a".

For Negative Values:

ex:1: $-18 \bmod 14 = 10$

From the above example, since "a" value is negative (-ve), we first calculate a mod n and then assign the negative sign to "r" and later add "n" to "r".

Step-1: Calculate $a \bmod n = r$
$18 \bmod 14 = 4 \quad (r)$

Step-2: Assign -ve sign to $r = -4 \ (r)$

Step-3: Add n to $r = 14 + (-4)$
$= 14 - 4$
$= 10$

ex-2: $-7 \bmod 10 = 3$

Step-1: calculate $a \bmod n = r$
$7 \bmod 10 = 7 \ (r)$

Step-2: Assign -ve sign to $r = -7 \ (r)$

Step-3: Add n to $r = 10 + (-7)$
$= 10 - 7 = 3$

(d) Matrices :

→ A matrix is collection of elements which are represented in the form of rows and columns. Rows are indicated by "r" and columns are indicated by "c".

ex: $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}_{2\times 2}$ (r = 2, c = 2)

Row matrix : A row matrix is matrix which has only one row ($r = 1$).

ex: $[1 \quad 2 \quad 3 \quad 4]$

column matrix : A column matrix is a matrix which has only one column ($c = 1$)

ex: $\begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \end{bmatrix}$

Square matrix : In a square matrix, the number of rows will be equal to the number of columns in a matrix ($r = c$).

ex: $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}_{3\times 3}$

Additive Identity matrix : It is a matrix which contains all zeroes and when added to a matrix will produce the same result.

ex: $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$

↓ Additive Identity matrix

Multiplicative Identity matrix : The multiplicative identity matrix contains all the diagonal values with 1's and the remaining values are 0's.

ex: $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \times \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$

↓ multiplicative Identity Matrix.

Addition and subtraction:

ex: $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} + \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 2 & 4 \\ 6 & 8 \end{bmatrix}$

ex: $\begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} - \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 4 & 5 \\ 6 & 7 \end{bmatrix}$

Scalar multiplication:

In scalar multiplication, we multiply a matrix with a scalar value.

ex: $3 \times \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 3 & 6 \\ 9 & 12 \end{bmatrix}$

(3 ↓ scalar, matrix ↓)

Determinant: $|M| = ad - bc$

if $M = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ Then $|m| = ad - bc$

$= (1 \times 4) - (2 \times 3)$

$= 4 - 6$

$= -2$

(e) Linear congruence:

Congruence: Two integers are said to be congruent if one integer maps multiple numbers of other integers.

→ Congruence is indicated by congruence operator ($\approx$).

→ To denote "a" and "b" are congruent, we represent it as $a \approx b$.

ex: $2 \mod 10 = 2$

$12 \mod 10 = 2$

$22 \mod 10 = 2$

$-8 \mod 10 = 2$

→ From the above example $-8, 2, 12, 22$ are congruent to each other since the above values are applied with modular Arithmatic and gives the same result.

→ The congruence for the above values are represented as

$-8 \approx 2 \approx 12 \approx 22 \mod 10$

Linear congruence:

(1) The linear congruence is used in cryptography for solving an Equation or a set of equations of one or more variables.

(2) The linear congruence can be solved for

(i) single-variable linear Equations.

(ii) set of linear Equations.

(i) single-variable linear equations:

We can solve the single variable linear equation which is in the form $\boxed{ax \approx b \pmod n}$.

ex: solve the Equation $14x \approx 12 \pmod{18}$

sol: calculate gcd of (14, 18)

gcd of (a, n)

$\Rightarrow \gcd(14,18) = 2$

since the gcd of (14, 18) is 2. Now check the 'x' value is divisible by "b" ($\frac{a}{d} = \frac{b}{d}$ 2 by 12).

since 2 divides 12, we have possible solutions.

Now $14x \approx 12 \pmod{18}$

$7x \approx 6 \pmod 9$

$x \approx \frac{6}{7} \pmod 9$

$x \approx 6 \cdot 7^{-1} \pmod 9 \Rightarrow 7^{-1} \bmod 9 \Rightarrow 7x \equiv 1 \pmod 9$

1 → ✗ $7 \times 1 \bmod 9 = 7$

2 → ✗ $7 \times 2 \bmod 9 = 5$

3 → ✗ $7 \times 3 \bmod 9 = 3$

4 → ✓ $7 \times 4 \bmod 9 = 1$

$x \approx 6 \cdot 4 \pmod 9$

$x \approx 24 \bmod 9$

$x \approx 6$

Assume x as x_0. to find another x (x_1). where

$x_1 = x_0 + k(n/d)$

By applying x_0, k, n and d in above equation, we get

$x_1 = x_0 + k(n/d)$ [$\because d = \gcd(14,18)$

$= 6 + 1(18/2)$

$x_1 = 6+9$

$x_1 = 15$.

Hence, after reducing the Equation, we have Two solutions. 6 and 15. which satisfy the congruence.

$14x \equiv 12 \pmod{18}$

$14 \times 6 \pmod{18} = 12$

$14 \times 15 \pmod{18} = 12$

PART-B: Symmetic Encryption.

1. Mathematics of symmetic key Cryptography

a. Algebraic structures
b. Group
c. Ring
d. Field
e. GF (2^n) Field.

(a) Algebraic Structures:

An Algebraic structure is a combination of the set and the operations that are applied to the Elements of the set. Algebraic structures are of three types. They are.

(1) Groups
(2) Rings
(3) Fields.

(b) Groups:

A Group (G) is a set of elements with a binary operation "." which satisfies four properties. They are

* closure
* Associative
* Identity
* Inverse

Abelian group:

→ An Abelian group is a group where it satisfies all the four group properties along with an additional property (commutative property).

→ An Abelian group can also be called as commutative group.

properties:

* closure property: If 'a' and 'b' are elements of 'G', Then $c = a \cdot b$ is also an element of 'G'.
* Associative property: If 'a', 'b' and 'c' are elements of 'G', then $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
* Identity property: For all 'a' in 'G', There exists an element 'e' which is called the identity element, where $e \cdot a = a \cdot e = a$.
* Inverse property: For each 'a' in 'G', There exists an element a^{-1} where $a \cdot a^{-1} = a^{-1} \cdot a = e$
* Commutative property: For all 'a' and 'b' in 'G', we have $a \cdot b = b \cdot a$

Finite Group:

→ A Group is called a finite group, if the group has finite number of elements in a set, else it is called infinite group.

Order of group: $(|G|)$:

→ It indicates the total number of elements in a group.

Sub group:

→ let 'H' be a subgroup of 'G', if $G = \langle S, \cdot \rangle$ (S: subset, $\cdot$: operation) and $H = \langle T, \cdot \rangle$, where 'T' is a non empty subset of 'S' then 'H' is a subgroup of 'G'.

Cyclic Group:

→ If a subgroup of a group is generated by using the power of an element Then that sub group is called a cyclic group.

(c) Ring:

A Ring is an algebraic structure which is denoted by 'R' where

$$R = \langle \{ \ldots \}, \overset{1^{st}}{\cdot}, \overset{2^{nd}}{[\ ]} \rangle$$

The Ring has Two operations, where The first operation must satisfy all the five properties of abelian group where as the second operation must satisfy only two properties (closure, associative).

→ In a Ring the second operation must be distributed over the first operation. Distributivity:

→ Distributivity means that for all a, b and c relevants of "R" we have Distributivity

$$a \square (b \cdot c) = (a \square b) \cdot (a \square c)$$

$$(a \cdot b) \square c = (a \square c) \cdot (b \square c)$$

Commutative Ring: A commutative Ring is also a ring in which the commutative property is also satisfied for the second operation

(d) Fields:

A Field is a commutative Ring which is denoted by "F" where

$$F = \langle \{ \ldots \}, \underset{\text{(abelian) 1st}}{\cdot}, \underset{2^{nd}}{\square} \rangle$$

(1) In a field, the second operation which also satisfies all the properties (5) like the first operation.

(2) In a field, the identity of first operation has no inverse.

* G.F:

(1) GF stands for Galois Fields.

(2) Galois fields are finite fields where the number of elements should be p^n where 'p' is a prime number and 'n' is a positive integer number.

(3) Hence Galois Fields are indicated by GF (p^n).

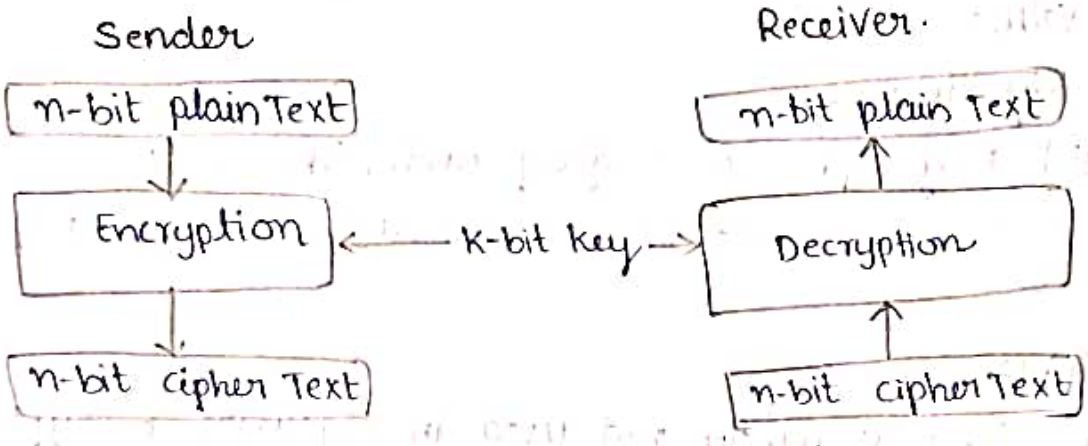
2. Introduction to Modren Symmetric Key ciphers.

a. Modren Block ciphers.

(1) A Symmetric-key modren Block cipher encrypts "n-bit" blocks of plain Text or decrypts "n-bit" blocks of cipher Text.

(2) An encryption or decryption Algorithm uses The Same "K-bit" key.

(3) Decryption Algorithm must be The inverse of Encryption Algorithm where both The Algorithms use The same key.



(4) The n-bit block Values can be 64, 128, 256 or 512 bits

(5) The modren block cipher uses Two types of mechanisms, They are (1) Substitution (or) Transposition.

(2) permutation.

(1) Substitution (or) Transposition:

→ This mechanism substitutes bits instead of characters.

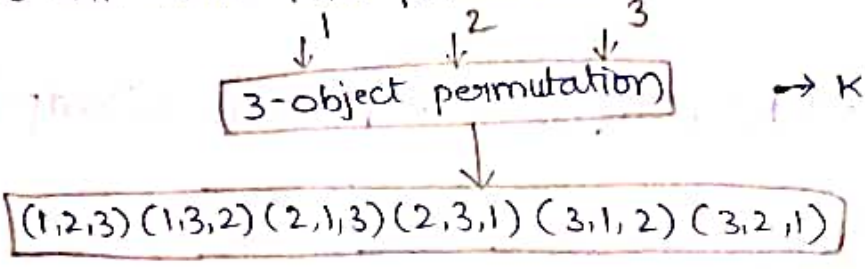
→ Here, 1-bit or 0-bit in The plain Text can be replaced either by 0 or 1.

(2) permutation:

→ In permutation cipher, The Text is permutated by factorial Times. That is if a block has 3 elements Then n=3.

→ calculate n!, which gives 3! ⇒ 3X2X1 = 6

→ We will have Total permutations of '6' if n=3.



→ The set of permutations for n=3 is 6 elements.
→ The permutation in modren Block cipher uses Three types of keys, They are (a) Full-size key
(b) partial-size key
(c) key-less cipher.

(a) Full-size key cipher:

A Full-size key Transposition cipher Transposes bits without changing Their values.

(b) Partial-size key cipher:

The partial key cipher is a group under The composition operation, if it is a subgroup of The corresponding fill-size key cipher

(c) Key-less cipher:

A key-less cipher is mostly not used in software Encryption or Decryption, Instead it can be used in Hardware Implementations.

5. Components of a Modren Block cipher.

The main components which are involved in a Modren Block cipher are (1) D-Box (Diffusion)
(2) S-Box (substitution)

(1) D-Box: (Diffusion).

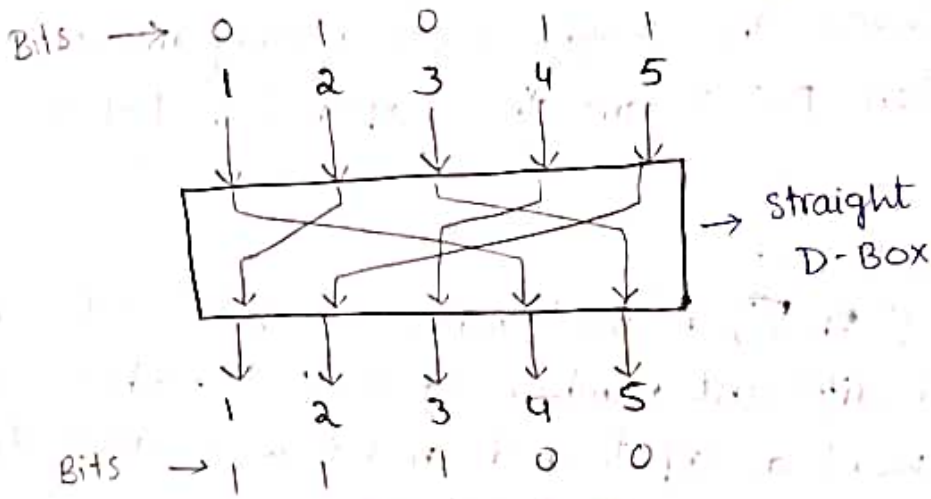
→ A D-Box is a Traditional mechanism which is used for Transposition cipher (characters). in the form of bits.

→ In modren Block cipher There are Three types of D-Box, They are
(a) Straight D-Box
(b) Compression D-Box
(c) Expansion D-Box

(a) Straight D-Box:

→ A straight D-Box takes 'n' inputs and produces 'n' outputs as a permutation.

→ Here we have n! possible mappings.

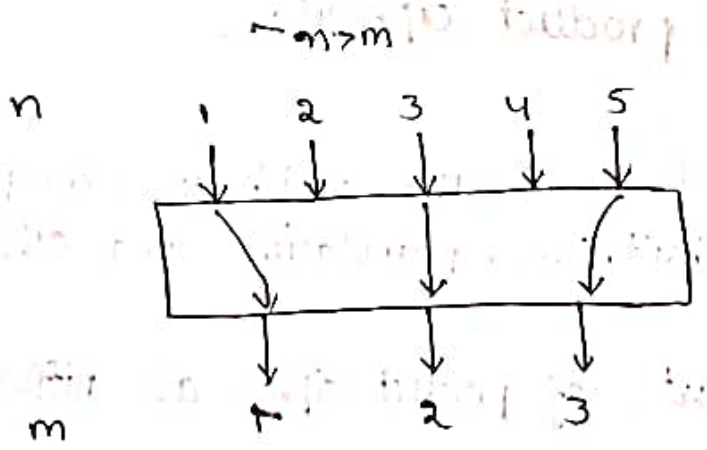


(b) Compression D-Box :

→ A compression D-Box is a D-Box with 'n' inputs and 'm' outputs where $m < n$.

→ Here some of the inputs are blocked and will not reach the output.

→ The compression D-BOX is mostly used with key-less Block cipher.

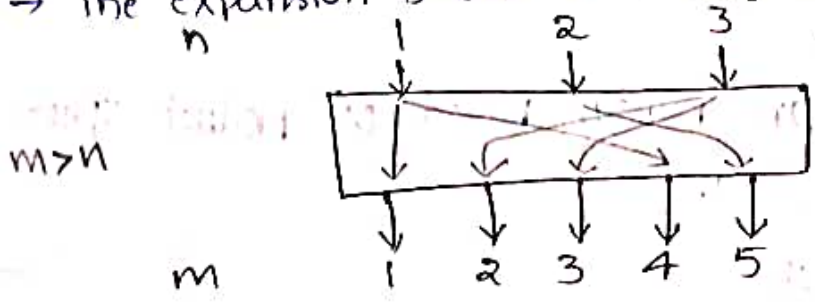


(c) Expansion D-Box :

→ An expansion D-Box is a D-Box with n inputs and m outputs where $m > n$.

→ Here some of the inputs are connected to more than one output.

→ The expansion D-Box is mostly used with key-less Block cipher.



NOTE:

From the above D-Boxes, the straight D-Box is only invertible, where as the compression D-Box and the expansion D-Box are not invertible.

(2) S-Box (substitution Box):

→ A substitution Box (S-Box) is used when we have different number of inputs and different number of outputs, which are represented as n-bit word as input and m-bit word as output, where 'n' and 'm' are not necessarily the same.

→ The various activities that are performed by S-Boxes are

(a) Invertibility
(b) Complement
(c) Inverse
(d) Circular shift (Exclusive OR)

c. Two classes of product ciphers.

Product cipher:

(1) Product cipher was developed by shannon which is a complex structure where it combines substitution, permutation and other components also.

(2) The Two important components of product cipher are Diffusion and confusion

Diffusion: It is used to hide the relationship between the cipher Text and the plain text.

Confusion: It is used to hide the relationship between the cipher Text and the key.

Two classes of product cipher:

(1) The modren block ciphers are mostly based on product ciphers.

(2) The classes of product ciphers are:

(a) Feistel cipher

(b) Non - Feistel cipher.

(a) Feistel cipher :

(1) Feistel cipher uses both invertible and non-invertible components for block cipher.

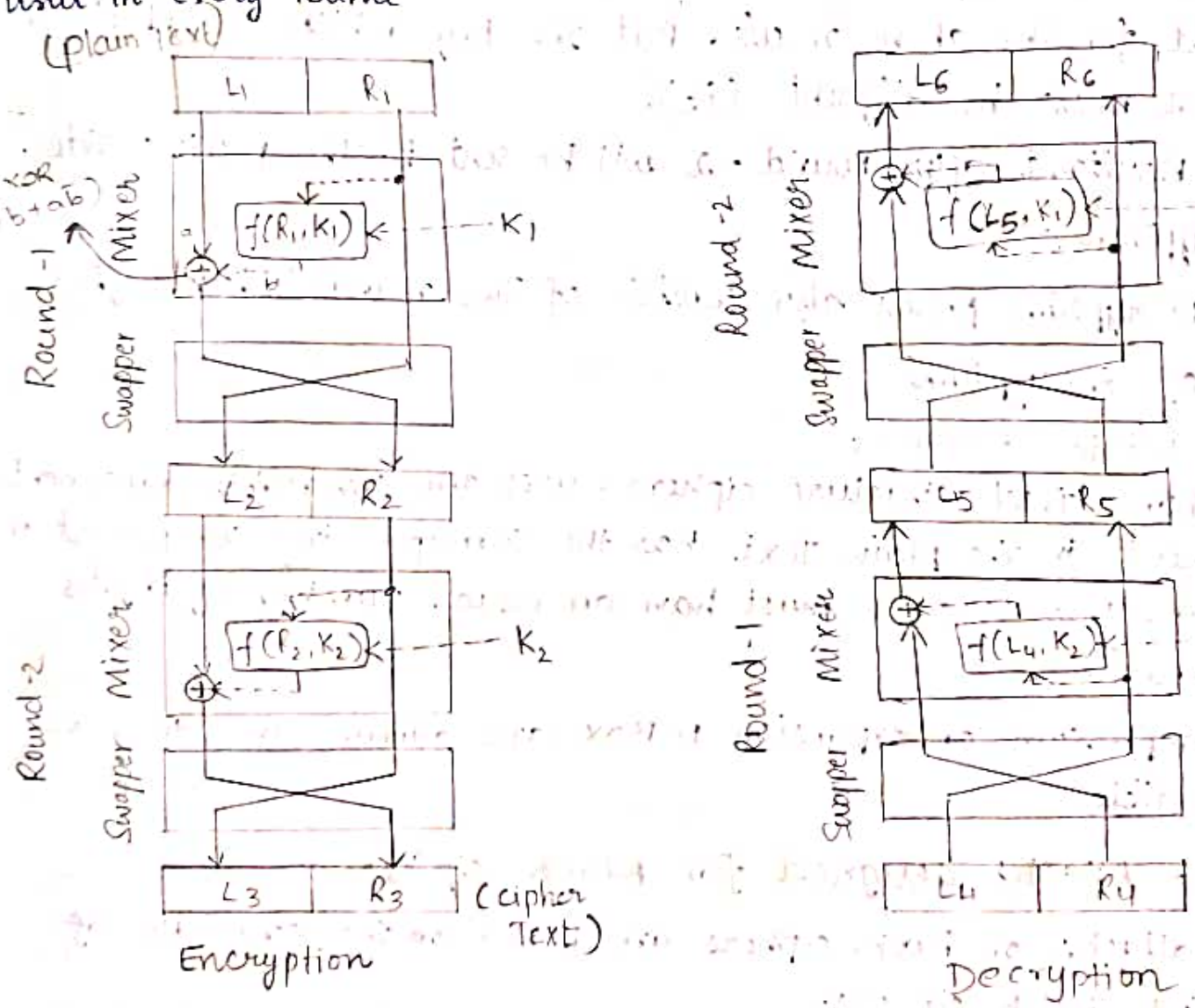
(2) It is used in DES (Data Encryption standard).

(3) It was designed by Feistel, Hence called Feistel cipher.

Feistel structure :

→ In Feistel structure, 'n' number of rounds are performed, where in each round a substitution is performed on half of the plain Text. followed by permutation.

→ In Feistel structure, the key is expanded, where a different key is used in every round



From the above figure ; the final design of a Feistel cipher with two rounds for Encryption and Decryption are Observed.

(1) In Encryption side of Feistel cipher, first the plain Text is divided into two parts (L_1, R_1).

(2) The R_1 (Right side of plain Text) is now applied with an Encryption function (f) along with a key (K_1) that is $f(R_1, K_1)$.

(3) The above result of $f(R_1, K_1)$ is XOR ($\oplus$) with Left part of plain Text (L_1).

(4) The resultant of XOR is swapped with the right part (R_1) of the plain Text.

(5) The result of above are Taken as input for the next round. Since the Feistel cipher consists of Two rounds, the same process is applied for the above result, But the key which is applied for Encryption must be different (K_2).

(6) The Resultant after Round-2 will be sent to the Receiver side for Decryption.

(7) The Decryption process also consists of Two rounds which is the inverse of Encryption.

(b) Non-Feistel structure:

A non-feistel structure ciphers. uses the invertable components. A component in the plain Text has the corresponding component in the cipher. This is S-Box must have an equal number of inputs and outputs.

→ No compression or expansion D-Box are allows. since they are not invertible.

d. Attacks designed for Block ciphers.

→ The attacks on block ciphers are based on the structure of The modren block ciphers.

→ The attacks for the block ciphers may use two different type of Techniques. They are

(1) Differential Crypt analysis

(2) Linear Crypt analysis.

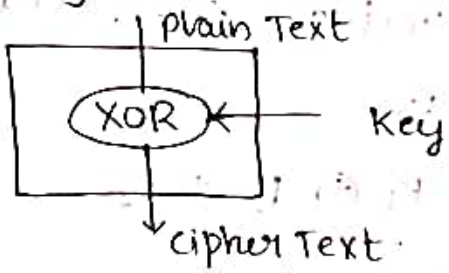
(1) Differential Crypt Analysis :

The differential crypt analysis attack is done on a choosen plain Text. The goal of the differential crypt analysis attack is to find the cipher key for the choosen plain Text.

→ Since, we do not know the cipher key we need to analyze the encryption algorithm in order to collect some information about the relationship between the plain text and cipher Text.

Procedure :

Consider, S-Box which is present in the cipher which has one XOR and one-key to convert the plainText into cipher Text.



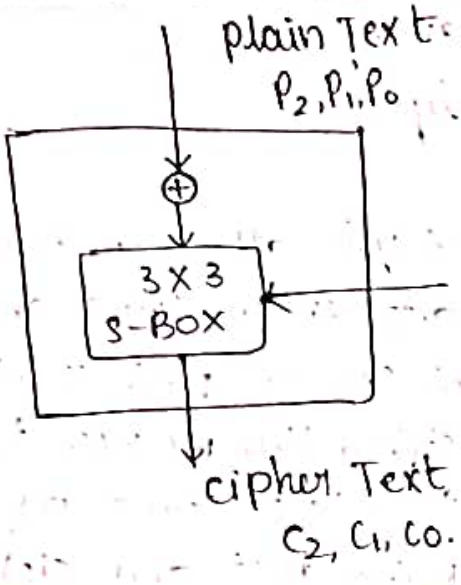
→ We can create the differential distribution table. For each S-Box and combine them to create the distribution for each round.

→ We can create a distribution Table for the complete cipher by multiplying the corresponding probabilities.

Conclusion : Hence the differential crypt analysis is based on non-uniform differential distribution table of the S-Boxes in a Block cipher.

(2) Linear Crypt Analysis :

The Linear Crypt analysis attacks is done on known plain Text. Here The cipher is made of a single round where the output is represented by 3 bits. (C_0, C_1, C_2) and the input of S-Box are also represented by 3-bits (x_0, x_1, x_2) and the plain Text is represented by P_0, P_1, P_2 and the key values (3-bit) are represented as



From the above figure, the linear Transformation takes place in a S-Box. where each input is applied with a linear function By applying the linear function We can create the 3 linear equations between plain Text and cipher Text, mentioned below

$$C_0 = P_0 \oplus K_0 \oplus P_1 \oplus K_1$$

$$C_1 = P_0 \oplus K_0 \oplus P_1 \oplus K_1 \oplus P_2 \oplus K_2$$

$$C_2 = P_1 \oplus K_1 \oplus P_2 \oplus K_2$$

e. Modren stream ciphers.

→ In a modren stream cipher, The encryption and decryption are done n bits at a time.

→ The plain Text bit stream is indicated by 'P' where

$$P = P_n, \ldots P_2, P_1$$

→ The cipher Text bit stream is indicated by 'C' where

$$C = C_n, \ldots C_2, C_1$$

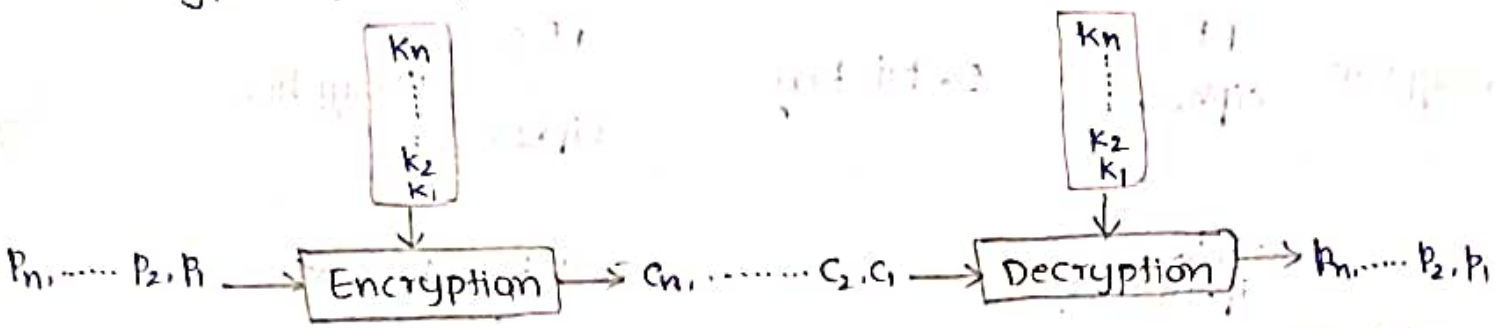
→ The key bit stream is indicated by 'K' where

$$K = k_n, \ldots k_2, k_1.$$

→ The n bits are used for i^{th} elements of plain Text (P_i), cipher Text (C_i) and key (k_i)

Encryption, $C_i = E(k_i, p_i)$

Decryption, $P_i = D(k_i, C_i)$



The modren stream cipher is categorized into two types, They are (1) Synchronous stream cipher.

(2) Non Synchronous stream cipher.

(1) Synchronous stream cipher:

→ In a synchronous stream cipher the key stream is independent of the plain text or the cipher Text.

→ The synchronous stream cipher uses

(a) one-time pad

(b) Feed-back shift Register (FSR)

(c) Linear Feed-back shift Register (LFSR)

(d) Non-Linear Feed-back shift Register (NLFSR)

(2) Non-Synchronous stream cipher:

→ In Non-synchronous stream cipher, the key depends on either the plain text or the cipher Text.

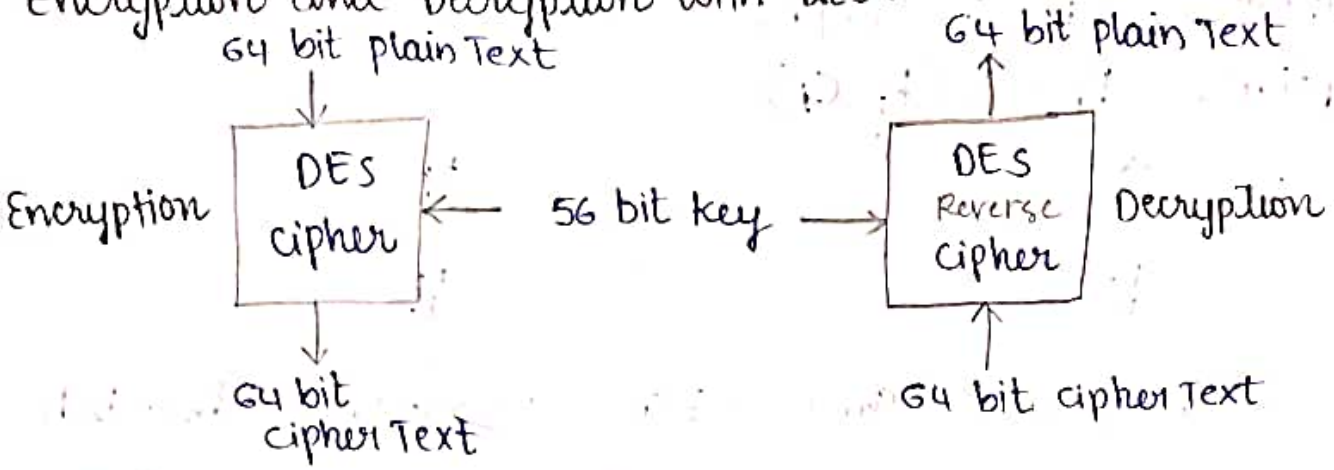
3. DES (Data Encryption Standard)

a. History of DES.

History: DES stands for Data Encryption Standard, which is a symmetric key block cipher that was developed by NIST (National Institute of standards and Technology).

→ DES was published by FIPS (Federal Information processing Standard) in 1975.

Encryption and Decryption with DES:

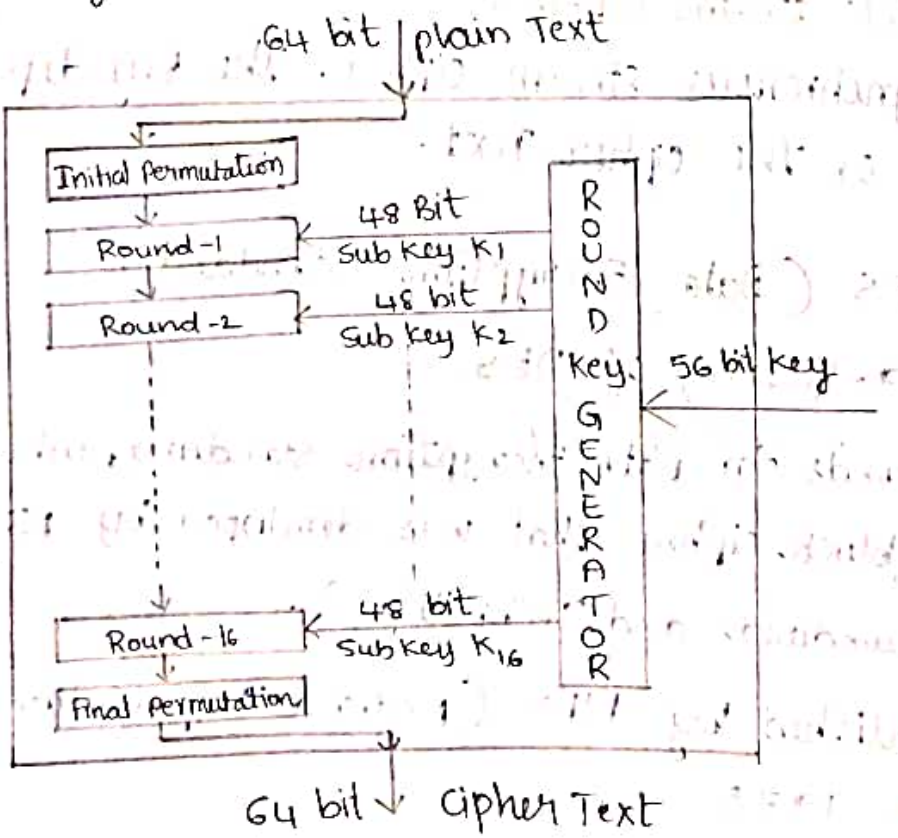


b. DES Structure:

(1) DES stands for Data Encryption **standard**.
(2) DES is based on Block cipher where the block size is 64 bit.
(3) DES Algorithm is symmetric, where it uses one super key.
(4) DES Algorithm is based on Feistel cipher.

Details:

(1) Block size of plain Text : 64 bit
(2) Block size of cipher Text : 64 bit
(3) Total number of Rounds : 16
(4) Number of permutations : 2 (Initial, Final)
(5) super key : 1 (64-bit)
(6) Sub Key : 16 (48 bit each).



From the above DES structure, the three main components are

(1) Initial and final permutations.

(2) 16 Rounds

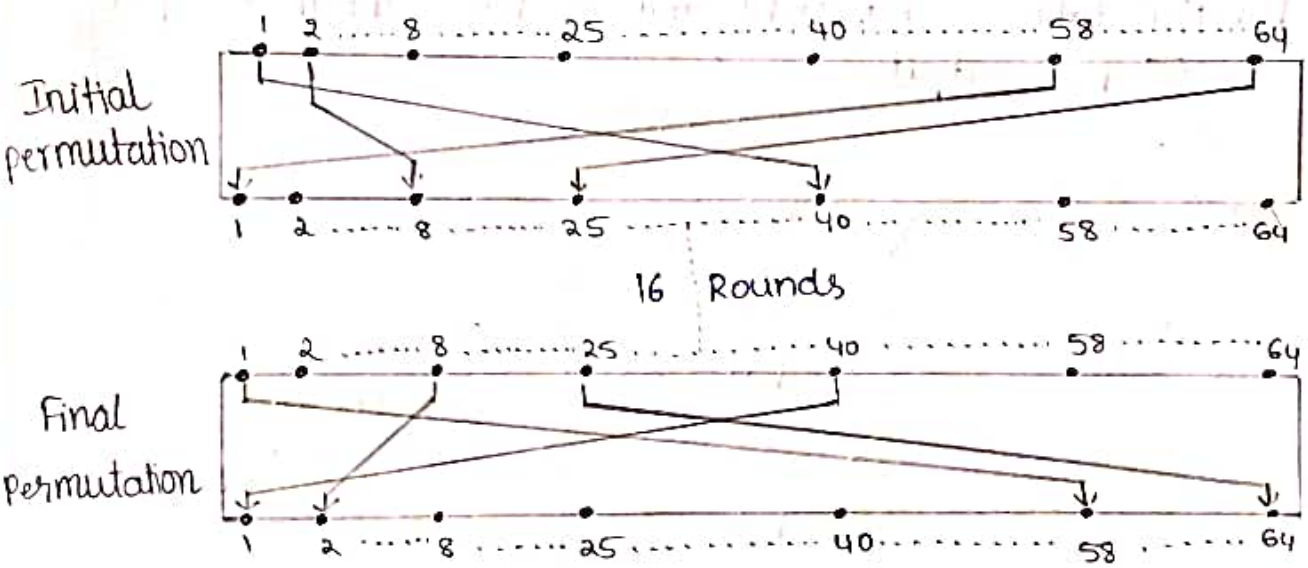
(3) Round Key Generator.

(1) Initial and Final permutations:

The DES Algorithm uses two permutation boxes, They are initial Permutation and final permutation.

→ The initial permutation takes 64 Bit plain Text as input and produces 64 bit output, where the output is forwarded to Round-1 function.

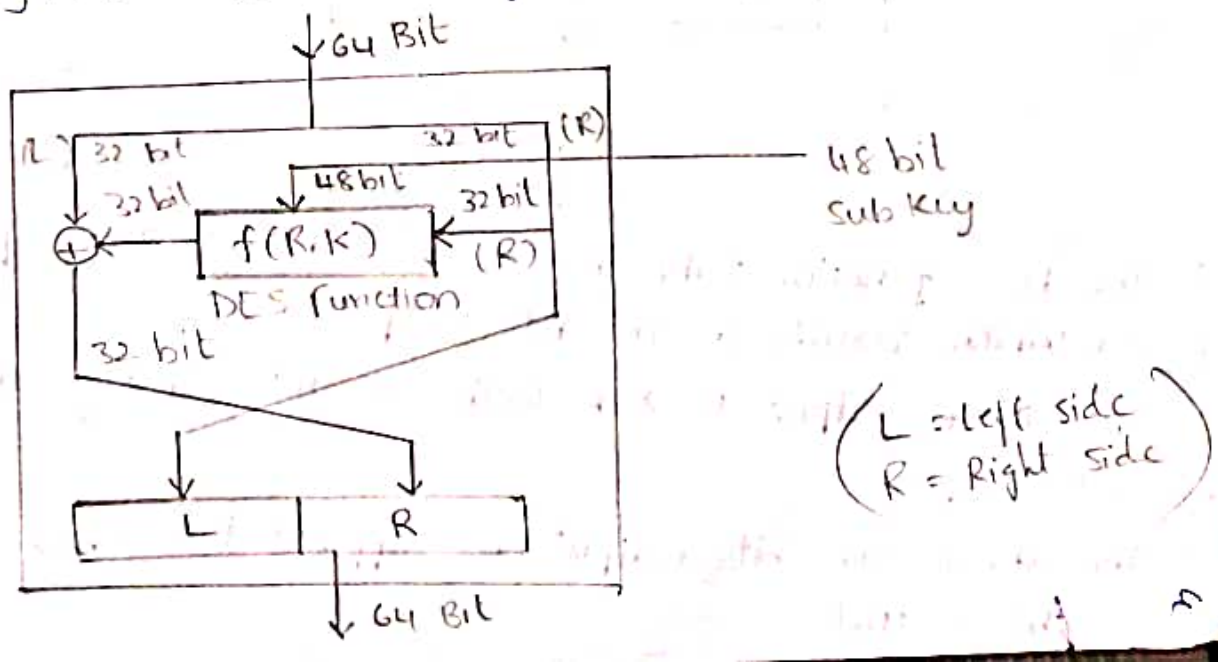
→ The final permutation takes 64 bit input from Round-16 and produces 64-bit cipher Text as output.



(2)

* Round Function:

(1) A DES structure has a total of 16 rounds, where each round takes 64 bit input along with a 48 bit subkey and produces a 64 bit output.



(2) The Round function takes the 64 bit input and divides it into two equal parts, where these parts are named as Left (L) and Right (R). These two parts are 32-bit each.

(3) Now the R-32 bit is forwarded to DES function along with a 48-bit subkey which produces a 32 bit output.

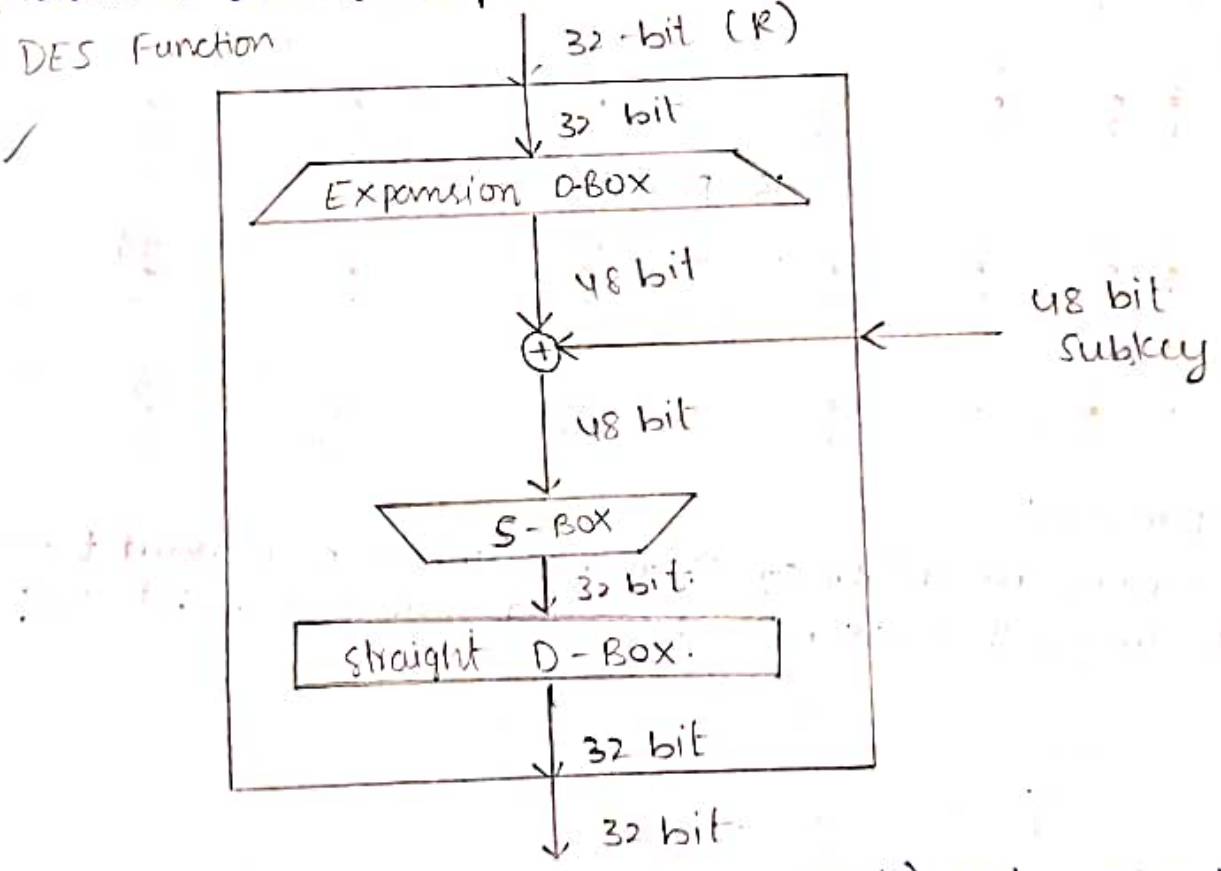
(4) The above 32 bit output is XOR with L-32 bit which results a 32-bit output.

(5) The above L-32 bit is swapped with R-32 bit and both the L-32 bit and R-32 bit are combined.

(6) This combined 64-bit data is the output of one round.

* DES Function:

(1) The DES Function takes 32-bit right and 48 bit subkey as input and produces a 32-bit output.



(2) The DES function takes the 32 bit (Right) and supplies to expansion D-Box which results a 48 bit output

(3) The above output is XOR with 48 bit sub key and results a 48 bit output.

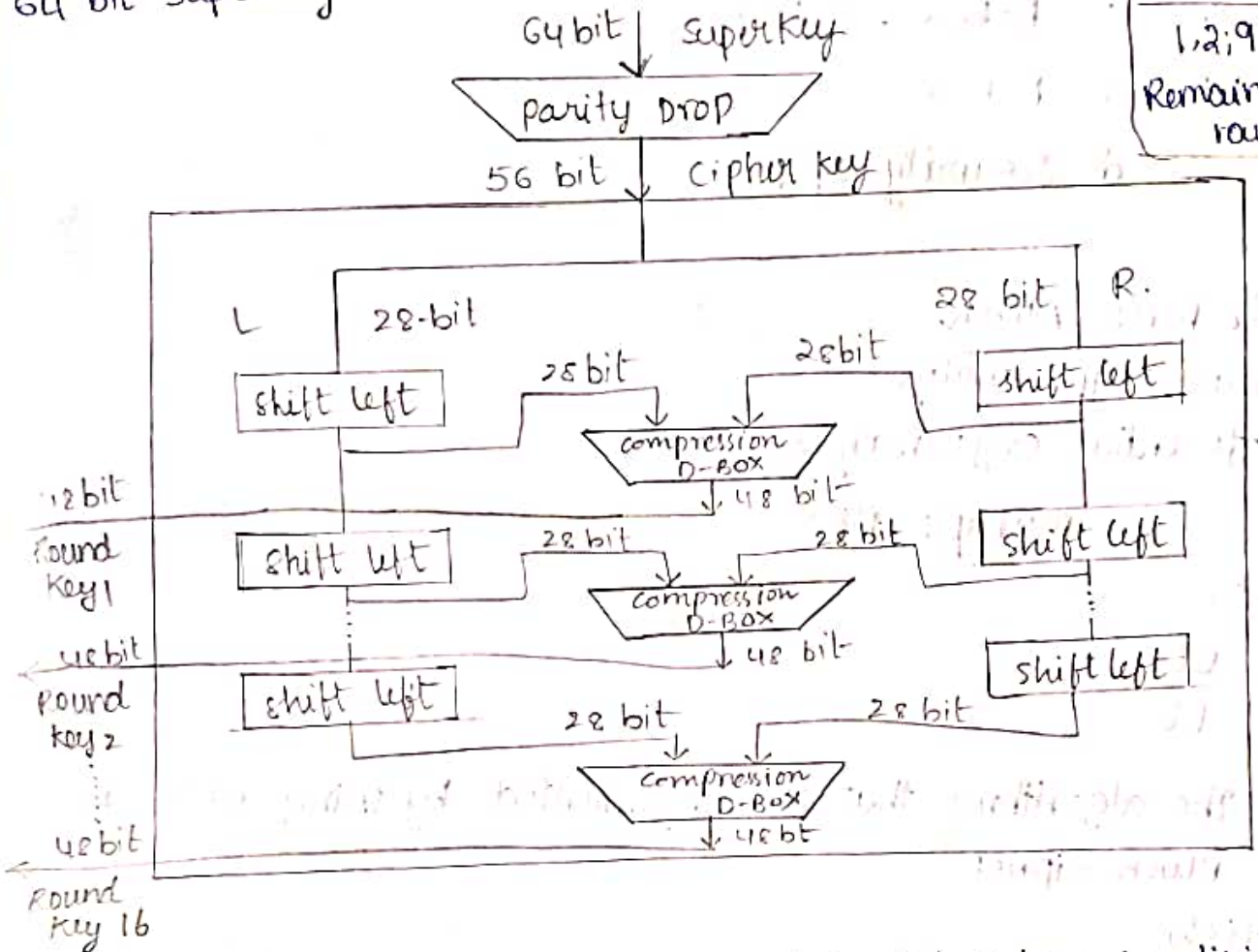
(4) The above 48-bit output is supplied to S-Box which results 32 bit output.

(5) The above 32 bit output is send to a straight D-Box which results a 32 bit output.

(3) Round Key Generator:

(1) A round key generator takes a 56 bit cipher key as input from the 64 bit superkey.

Raunds	Shift
1,2,9,16	1-bit
Remaining raunds	2-bit



(1) From the above figure, the 56 bit cipher key is divided into two halves (28 bit each).

(2) The 28-bits on left side and right side are applied with left circular shift.

(3) The output of left circular shifts on left side and right side are combined again and sent to the compression D-Box.

(4) The Compression D-Box will result a 48-bit output which is used as a round key.

(5) similarly, the same process is repeated another 15 times to produce a total of 16 Round keys (sub keys).

NOTE: The left circular shift is done with 1-bit for the rounds 1, 2, 9 and 16, whereas the left circular shift is

done with 2-bits for the remaining rounds.

C. DES Analysis.

DES Analysis

(1) properties : Avalance Effect
(2) Design : D-BOX , S-BOX
(3) Weakness : D-BOX , S-BOX

d. Security of DES.

Security :

(1) Brute Force Attack (2^{55} combinations)
(2) Linear crypt_analysis
(3) Differential cryptanalysis

e. Multiple DES.

Multiple DES.

(1) 2 DES
(2) 3 DES.

Examples : The algorithms that are implemented by using DES are

(1) CAST Block cipher
(2) Blowfish.
(3) IDEA (International Data Encryption Algorithm).

4. AES (Advanced Encryption standard).

→ AES stands for Advanced Encryption standard which is a specification for the encryption that was established by National institute of Standards and Technology (NIST) in 2001.

→ AES is much stronger than DES and triple DES despite being harder to implement.

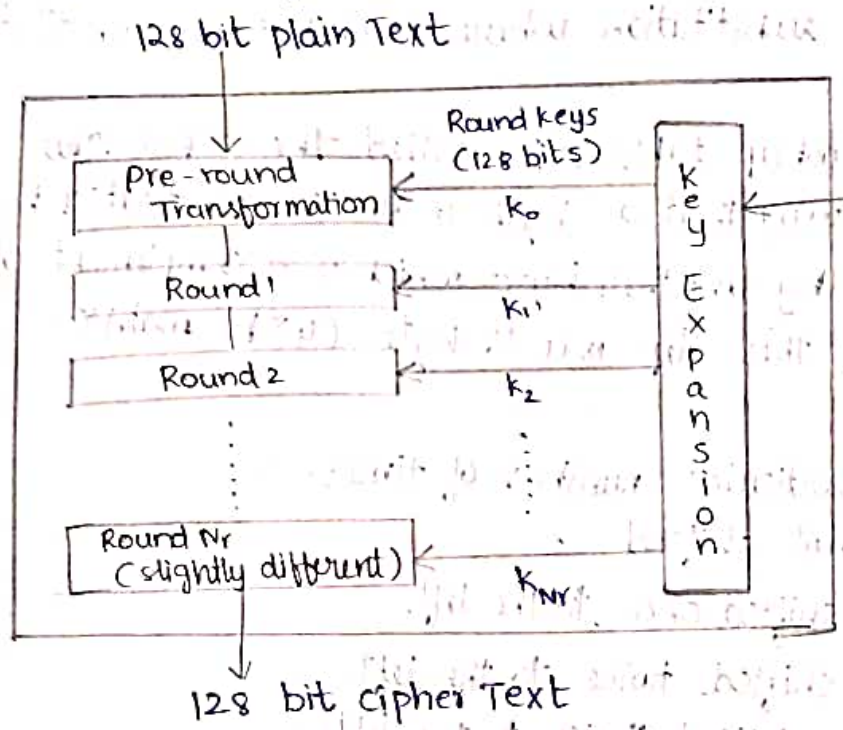
AES Details :

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

That means it takes 128 bits as input and outputs 128 bits of

encrypted cipher Text as output.

AES relies on substitution-permutation network principle which means it is performed using a series of linked operations which involves replacing and shuffling of the input data.



N_r	Key size
10	128
12	192
14	256

Relationship between Number of rounds and cipher key size.

Working of the cipher:

AES performs operations on bytes of data rather than in bits. Since the block size is 128 bits, the cipher processes 128 bits (or 16 bytes) of the input data at a time.

→ The number of rounds depends on the key length as follows.

- 128 bit key - 10 rounds
- 192 bit key - 12 rounds
- 256 bit key - 14 rounds.

Encryption:

AES considers each block as a 16 byte ((4 byte × 4 byte) = 128) grid in a column major arrangement.

Each round comprises of 4 steps.

→ subbytes
→ shift rows
→ mix columns
→ Add round key.

NOTE: The last round doesn't have the . Mix columns round.
→ The subbytes does the substitution and shift rows and mix columns performs the permutation in the algorithm.

• Subbytes:

→ This step implements the substitution where each byte is substituted by another byte.

→ Its performed using a lookup table also called the S-BOX. This substitution is done in a way that a byte is never substituted by itself and also not substituted by another byte which is a complement of the current byte. The result of this step is a 16 byte (4×4) matrix.

• Shift Rows:

→ Each row is shifted a particular number of times.

* The first row is not shifted.
* The second row is shifted once to the left.
* The Third row is shifted twice to the left.
* The fourth row is shifted thrice to the left.

• Mix Columns:

→ This step is basically a matrix multiplication. Each column is multiplied with a specific matrix and thus the position of each byte in the column is changed as a result.

• Add round keys:

→ Now the Resultant output of the previous stage is XOR with the corresponding round key. Here, the 16 bytes is not considered as a grid but just as 128 bits of data.

→ After all these rounds 128 bits of encrypted data is given back as output. This process is repeated until all the data to be encrypted undergoes this process.

Decryption:

The stages in the rounds can be easily undone as these stages have an opposite to it which when performed reverts the changes.

→ Each 128 blocks goes through the 10, 12 or 14 rounds depending

on the Key size.

→ The stages of each round in Decryption is as follows.

- Add round Key
- Inverse MixColumns
- shift rows
- Inverse subByte.

• Inverse mix columns:

→ This step is similar to the mix columns step in encryption, but differs in the matrix used to carry out the operation.

• Inverse subbytes:

→ Inverse S-Box is used as a look up table and using which the bytes are substituted during decryption.

Encryption and decryption of AES.