DES - Data Encryption Standard Algo

* it is Block Cipher Algo

→ it is used to convert plain text (PT) to Cipher text (CT)

* DES has 16 No. of Rounds

* plain text size = 64 bits, we will get Cipher text also 64 bits

Text size = 64 bits

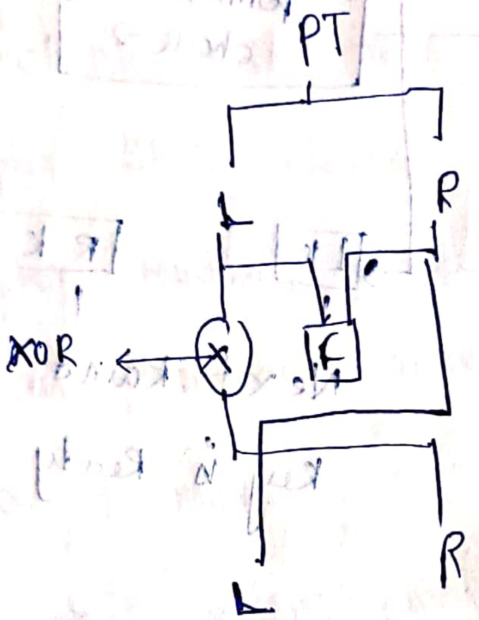
Key size = 48 bits

→ 8 bits for parity

→ 8 bits for rearrangement

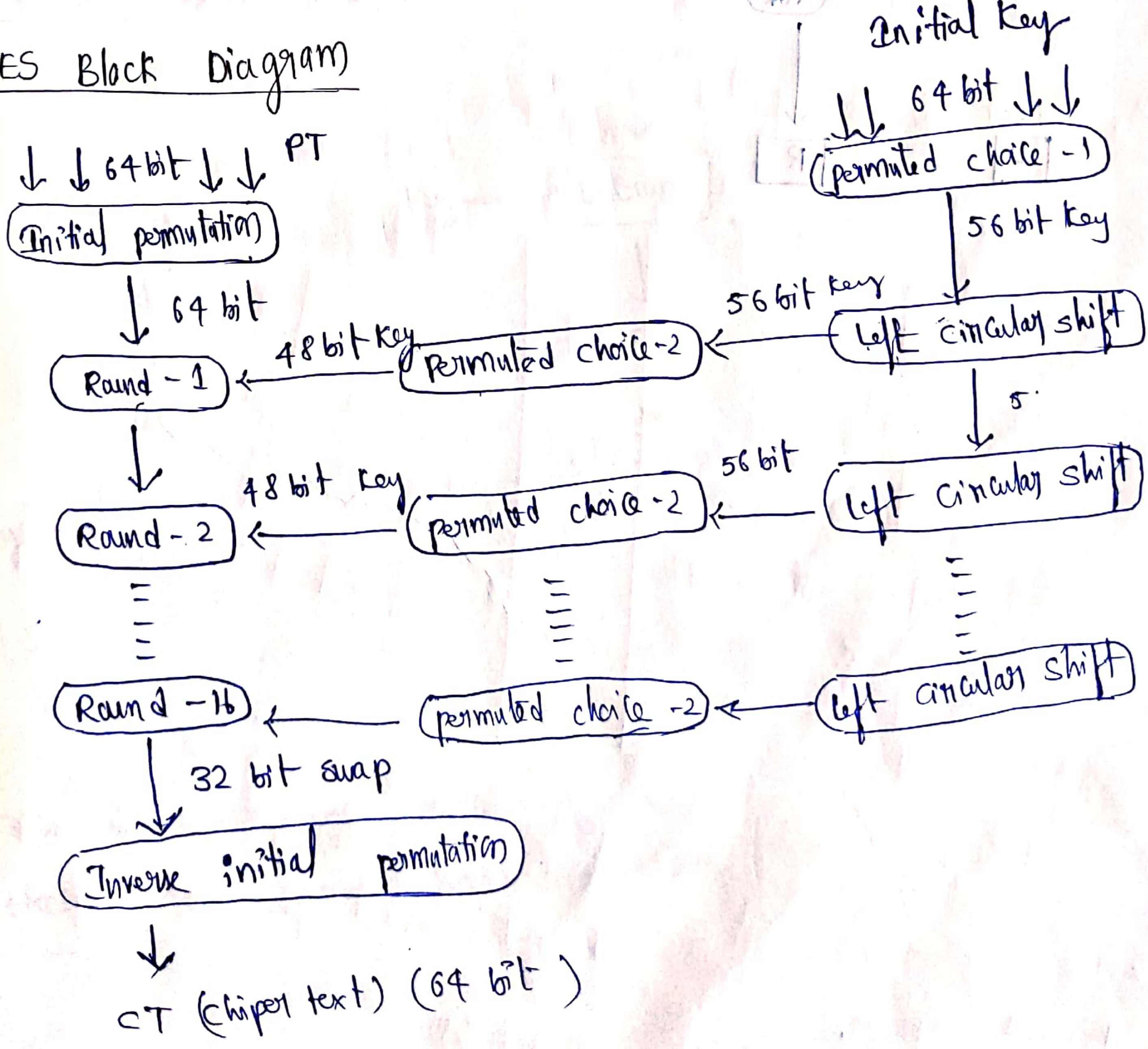
* Each and Every round, 4 steps are performed

1. Dividing bits into 2 parts (32 bits, 32 bits)
2. Bit shuffling
3. Non Linear substitution
4. Exclusive OR operations.



Based on sounds it becomes complex
↳ (Hacker can't Hack easily)

DES Block Diagram



→ In PC1, initially 64 bits, 8 parity bits are to be removed from every 8th position

64 has Eight 8th positions

$= 64 - 8$

$= 56$ bits

→ Then Apply left circular shift < 28 bits
28 bits

* move the bits based on Round number

* for Rounds 1, 2, 9, 16 – 1 bit shift

others – 2 bits shift

→ output is 56 bits (28 bits + 28 bits)
↳ rearranged

→ The output of Left circular shift (56 bits) is the input of PC2 (48 bits) → Key for round 1

* remaining 8 bits is removed for rearrangement

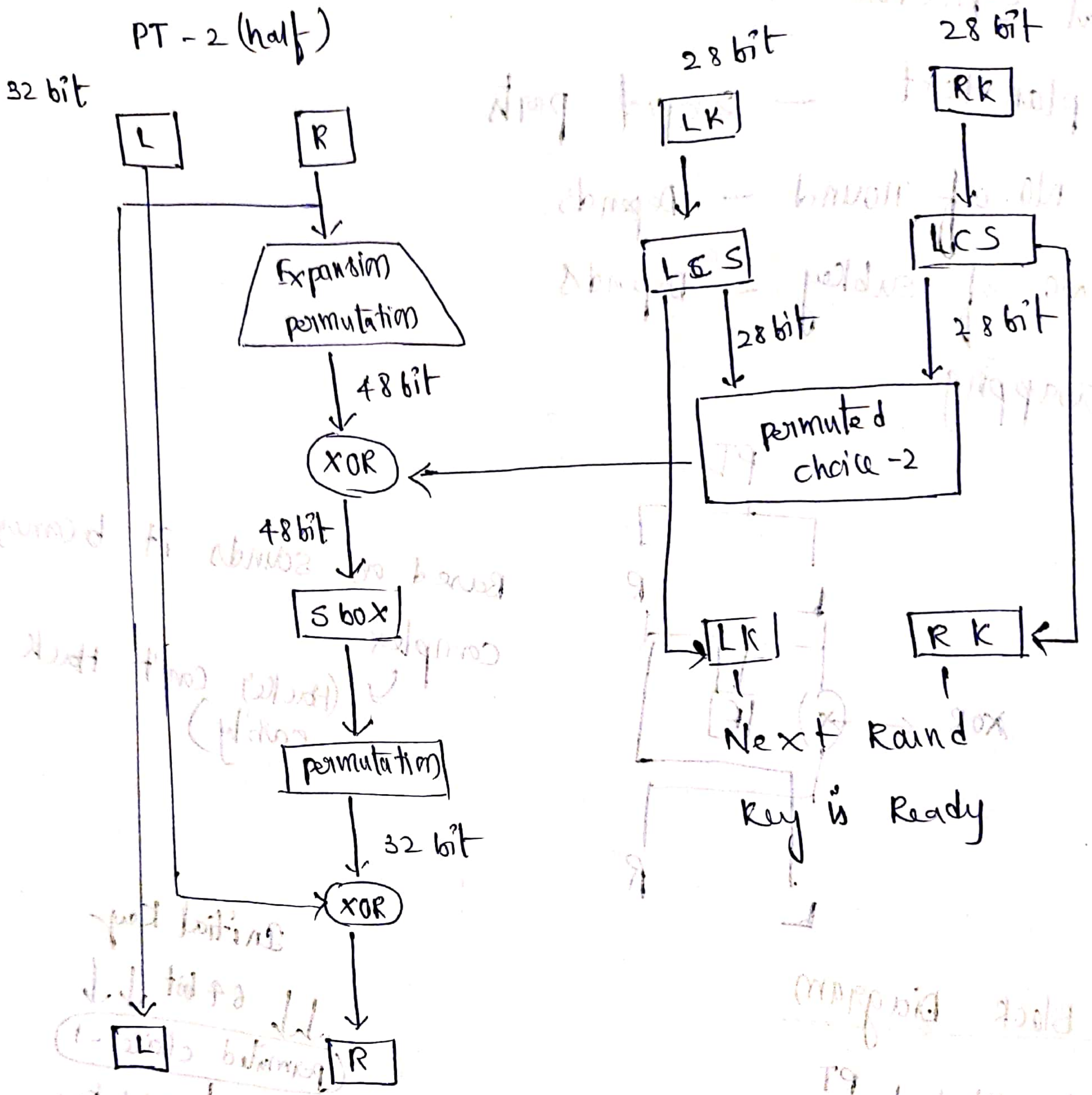
→ PC2 (48 bits) is Key for round 1

→ Input for round 1 is 64 bits + 48 bits, output is 64 bits

→ same process will Repeat upto 16 rounds

• After final / Inverse initial permutation we will get Cipher text (64 bits)

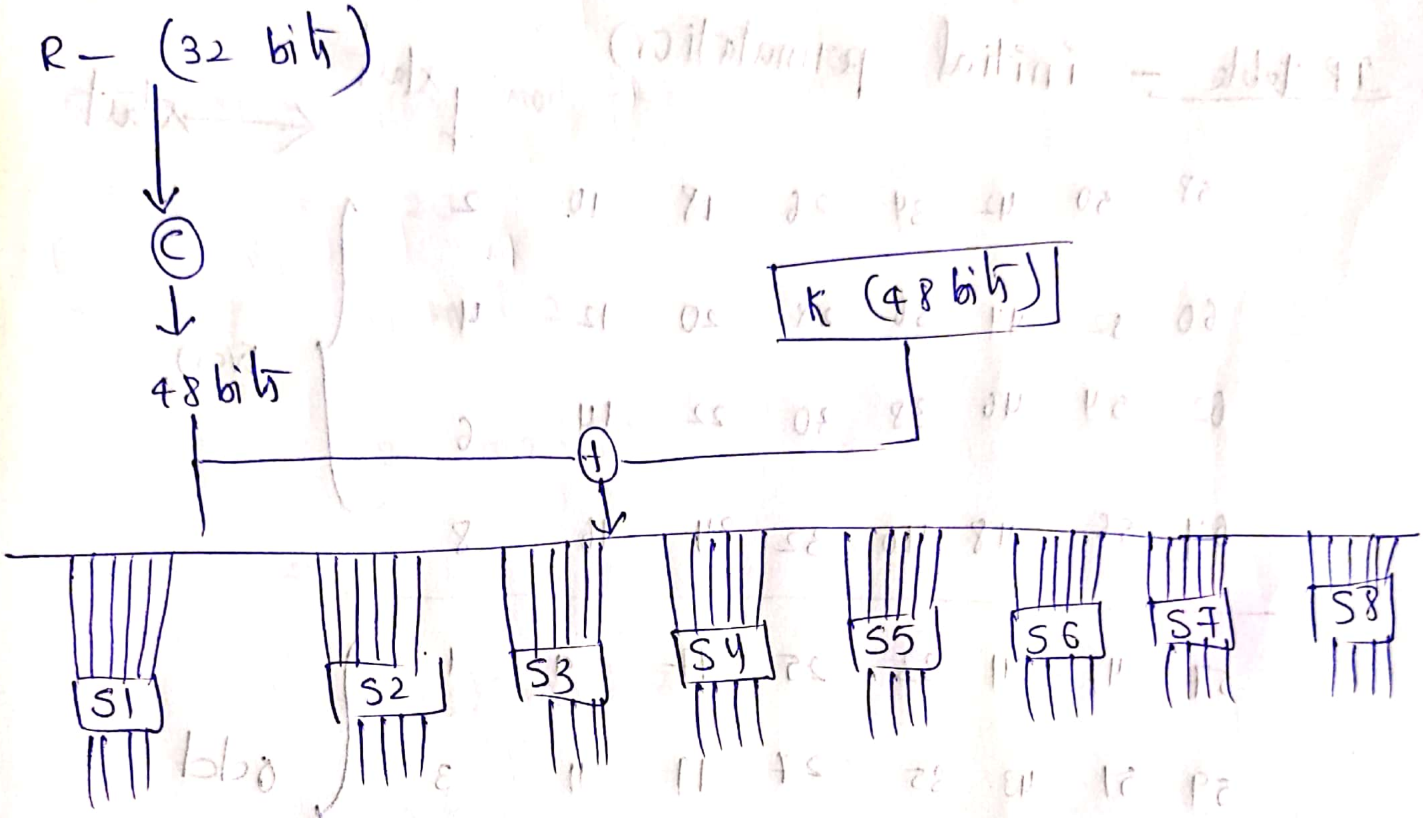
Round function of DES



S-BOX

- substitution box
- s box can have different no.of inputs and outputs
- s box is a basic component of symmetric key Algorithms which performs substitution.
- sbox is used as an intermediate stage of encryption or decryption.

DES S-box



I/p → 48 bits

O/p → 32 bits

6 → S1 → 4

6 → S2 → 4

6 → S3 → 4

6 → S4 → 4

6 → S5 → 4

6 → S6 → 4

6 → S7 → 4

6 → S8 → 4

Random Number Generators (PRNGS)

- used in encryption for network security Applications
- Generation of keys for R.S.A (Rivest Shamir Adleman) Algo
- Generation of symmetric key for temporary session key.

Requirements

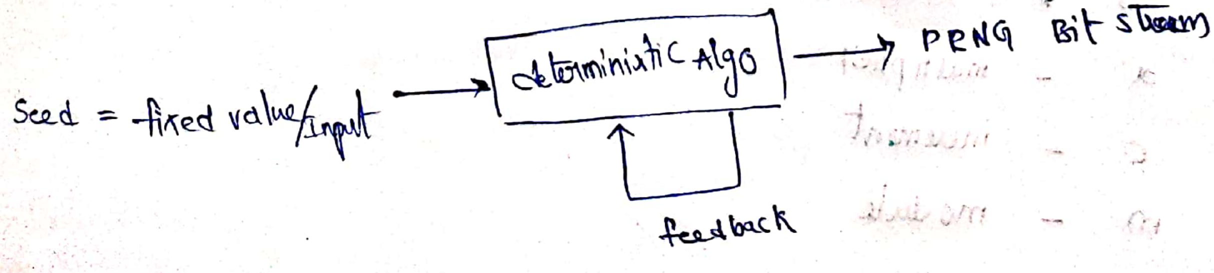
1. Randomness
   - uniform distribution [The no. of 0's and 1's in the key are approximately same]
   - independence [a subsequence is derived from a sequence should not derived from any other sequence

2. unpredictability [The next number not to be predictable]

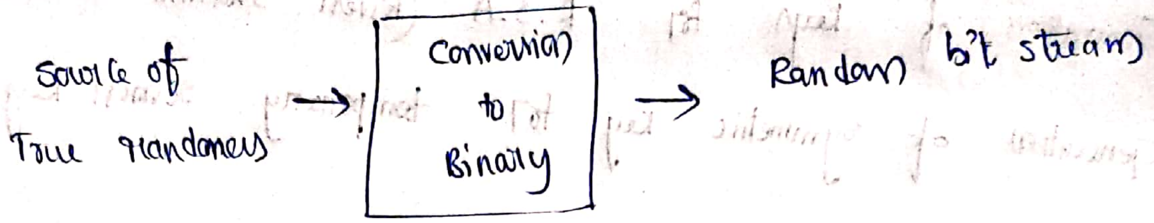
sequence: A, B, C
Subsequence: BC

1. PRNG

- Pseudo means fake
- A Pseudo random number generator is a computer algorithm that generates a sequence of numbers that appear to be random, but are actually generated using a deterministic process.
- The numbers generated by a PRNG are truly random, because they are determined by a fixed mathematical formula or algorithm. but they are unpredictable enough for many practical purposes.
- PRNGs are commonly used in games, Cryptography .. etc.



2. TRNG (True Random Number Generator)



→ Input as a source that is Randomness — entropy source (physical environment)

→ TRNG is a device that generates random numbers from a physical process that is inherently random, such as atmospheric noise, radioactive decay, or thermal noise.

→ TRNG Applications

- security levels
- scientific experiments

3. LCM (Linear Congriuential Method)

→ eariest method to generate random numbers

$$X_{i+1} = (aX_i + c) \bmod m$$

$$R_i = \frac{X_i}{m}$$

X_0 - seed element

a - multiplier

c - increment

m - module

if $c = 0$ → Multiplicatine LCM

$c \neq 0$ → Mixed LCM

Example

$X_0 = 27$, $a = 17$, $c = 43$, $m = 100$

① $X_1 = x_{i+1}$

$\boxed{x_i = x_0}$

$X_1 = (17 * 27 + 43) \bmod 100$

$= 502 \bmod 100$

$X_1 = 2$

② $X_2 = (17(X_1) + 43) \bmod 100$

$= (17(2) + 43) \bmod 100$

$= 77 \bmod 100 = 77$

③ $X_3 = (17(X_2) + 43) \bmod 100$

$= (17(77) + 43) \bmod 100$

$= 1352 \bmod 100$

$= 52$

④ $X_4 = (17(X_3) + 43) \bmod 100$

$= (17(52) + 43) \bmod 100$

$= 27$

⑤ $X_5 = (17(27) + 43) \bmod 100$

$= 2$ → [stop here Because in ① we already got 2]

$R_1 = \frac{X_1}{100} = \frac{2}{100} = 0.02$ $R_4 = \frac{27}{100} = 0.27$

$R_2 = \frac{X_2}{100} = \frac{77}{100} = 0.77$ $R_5 = \frac{2}{100} = 0.02$

$R_3 = \frac{52}{100} = 0.52$

→ Random Number values.

4. BBS (Blum Blum shub Generator)

- BBS is popular Algorithm for secured Number

steps

1. take two large prime numbers p, q

2. $n = p * q$

3. s - Generate a random number
   Neither p nor q is a factor of s

4. $x_0 = s^2 \bmod n$

5. for $i=1$ to k
   k - no. of random number

6. Calculate $x_1 = (x_{i-1})^2 \bmod n$

7. $B_i = x_i \bmod 2$