DES (Data Encryption Standard)

```
┌──────────────┐                              ┌──────────────────┐
│ Plain text   │                              │ Initial Key      │
└──────────────┘                              └──────────────────┘
      │                                              │ 64bit
      │ 64bit                              ┌────────────────────────────┐
      ▼                                    │ PC1 (Permutted Choice1)    │
┌──────────────┐                           └────────────────────────────┘
│ Initial      │                    8bit Parity    │ 64 − 8 = 56bit
│ Permutation  │                        ┌───────────┴──────────────┐
└──────────────┘                    ┌──────┐ 28bit        ┌──────┐ 28bit
      │                             │ C₀   │              │ D₀   │
      │ 64bit                       └──────┘              └──────┘
      ▼                                │                      │
┌──────────────┐                    ┌──────┐              ┌──────┐
│ ROUND 1      │   48bit            │ LS   │              │ LS   │
└──────────────┘ ◄──────  ┌──────┐  └──────┘              └──────┘
      │                   │ PC1  │     │                     │
      │                   └──────┘  ┌──────┐              ┌──────┐
      ▼                             │ C1   │              │ D1   │
┌──────────────┐                    └──────┘              └──────┘
│ ROUND 2      │ ◄──┐                  │                     │
└──────────────┘    │               ┌──────┐              ┌──────┐
      ⋮          ┌──────┐  48bit    │ LS   │              │ LS   │
              │ PC2  │              └──────┘              └──────┘
              └──────┘                 │                     │
                                    ┌──────┐              ┌──────┐
                                    │ C2   │ ◄────────────│ D2   │
                                    └──────┘              └──────┘
      ⋮                                ⋮                     ⋮

┌──────────────┐   48bit   ┌──────┐  ┌──────┐           ┌──────┐
│ ROUND 16     │ ◄──────── │ PC16 │  │ C16  │           │ D16  │
└──────────────┘           └──────┘  └──────┘           └──────┘
      │  SWAP 32 bit
      ▼
┌──────────────────┐
│ FINAL Permutation│
└──────────────────┘
      │ 64 bit
      ▼
┌──────────────┐                         ┌──────────────────┐
│ Cypher text  │                         │ 1, 2, 9, 16      │
└──────────────┘                         └──────────────────┘
                                                 ▼
                                         One bit shift

                                         ┌────────┐
                                         │ Other  │
                                         └────────┘
                                         two bit shift
```
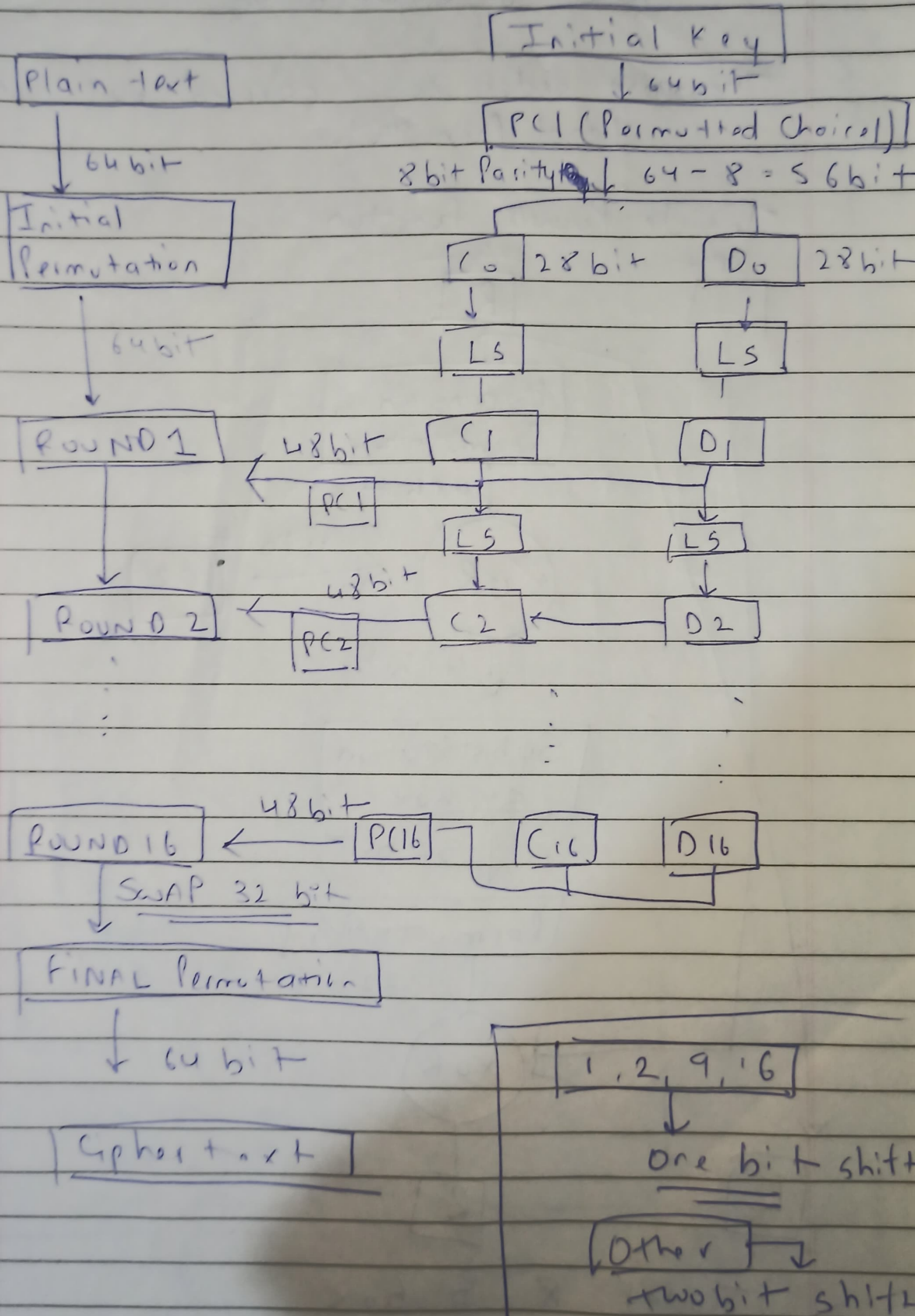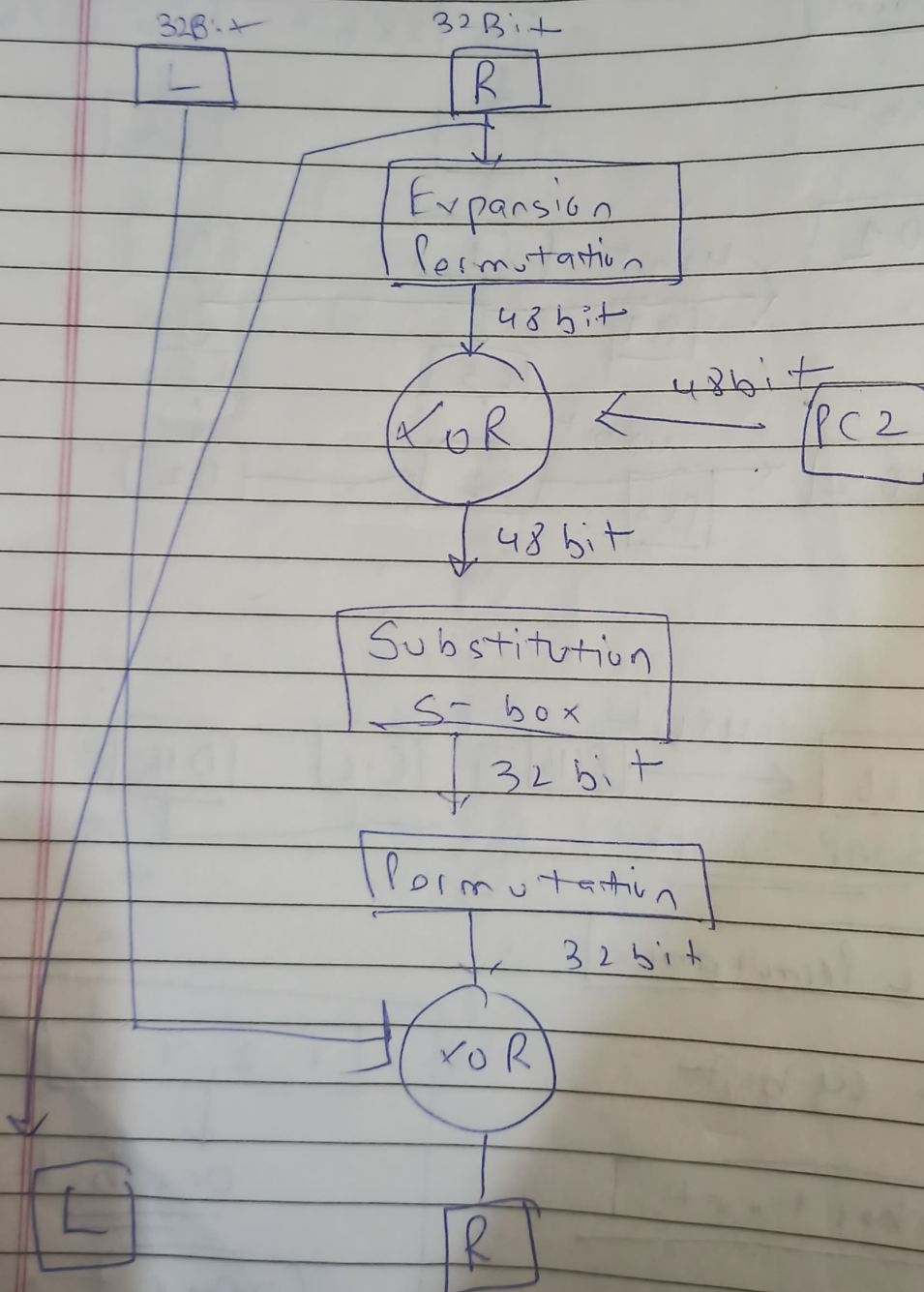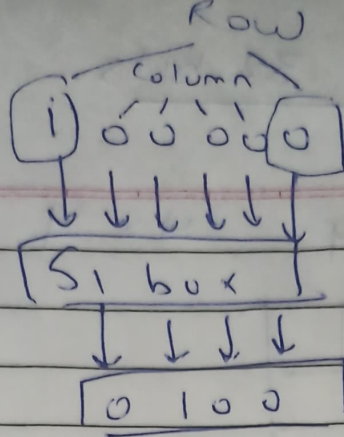
Initial and final Permutation cre inverse of each other

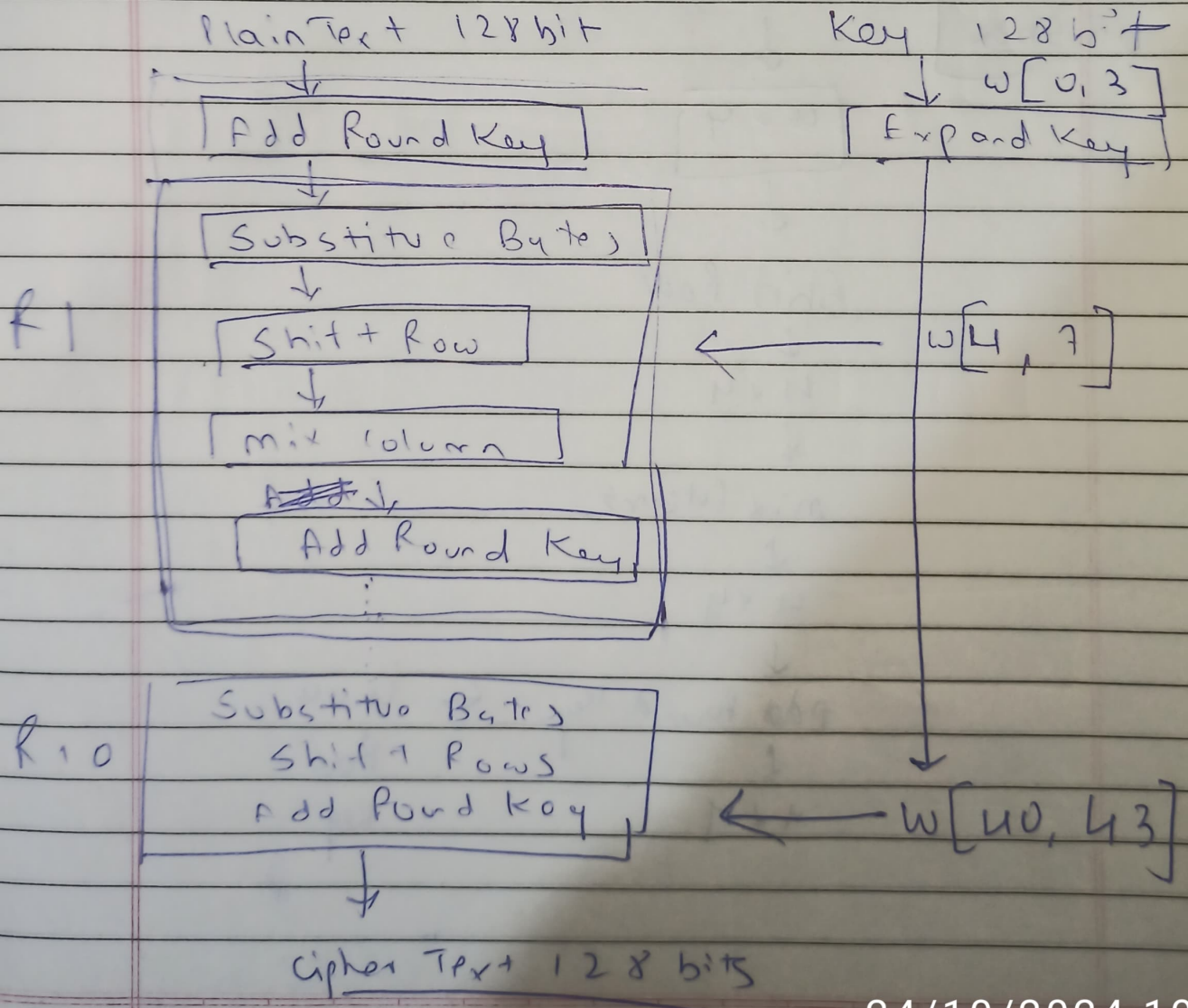Transpose order is carried out in final Permutation.

Inside Round function

32Bit   32 Bit

L   R

Expansion Permutation

48 bit

XOR ← 48 bit PC 2

48 bit

Substitution S-box

32 bit

Permutation

32 bit

XOR

L   R

Total 8 S box

Row

Column

[i] [0 0 0 0 0] [0]

↓ ↓ ↓ ↓ ↓ ↓

S₁ box

↓ ↓ ↓ ↓

[0 1 0 0]

R: 10 → 2
C: 0 000 → 0

01 23 ... 15

	0	1	2	3	...	15
0						
1						
2	4					
3						

4 → 0100

AES (Advanced Encryption Algo)

Plain Text 128 bit   Key 128 bit

↓   ↓ w[0,3]

| Add Round Key | | Expand Key |

↓

| Substitue Bytes |

↓

R1 | Shift Row | ← ─── w[4, 7]

↓

| mix column |

↓

| Add Round Key |

⋮

R10 | Substitue Bytes
     Shift Rows
     Add Round Key | ← ─ w[40, 43]

↓

Cipher Text 128 bits

24/10/2024 10:5

1 word = 32 bits

Input Array   4 × 4   16 byte
                                   4 word

At 5 in a Round.

$$4 \times 4$$

↓

6×16 →   Substitute Bytes
Sbox

↓

$$4 \times 4$$

↓

Shift Row

↓

4×4

↓

Mix Coluns

↓

4×4

↓

Add Round key   ← 4×4

↓   Round

4×4 Key