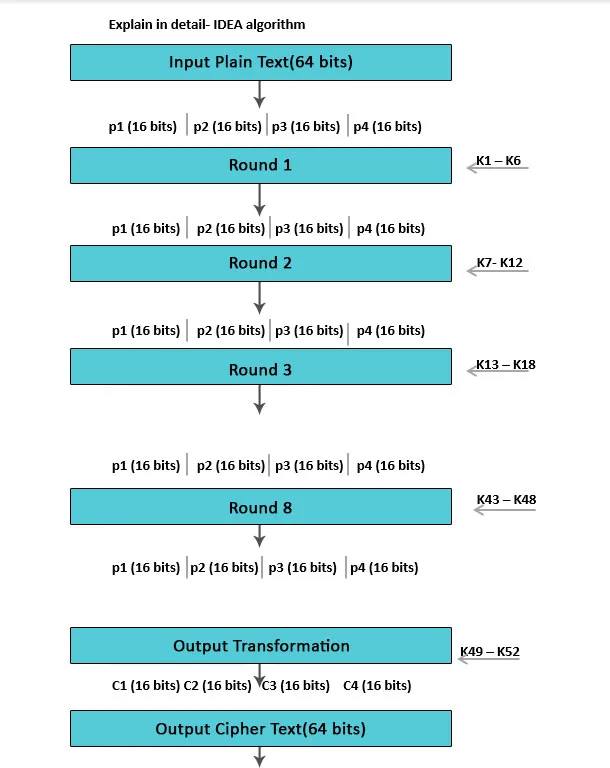
**IDEA (International Data Encryption Algorithm)**

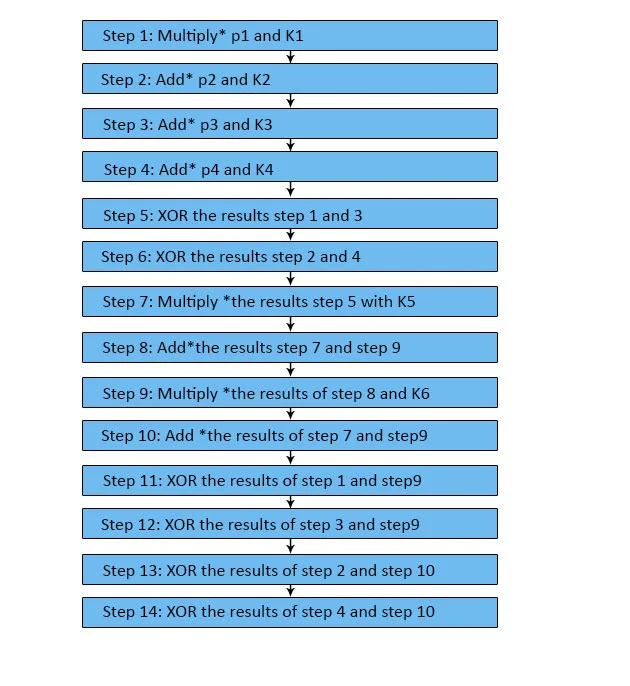
Algorithm— (First Round---total steps 14)

P.T is divided into 4 blocks (B1, B2, B3 and B4)

* IDEA (International Data Encryption Algorithm) is an encryption algorithm.
* Plain Text=64 bits
* Key Size=128 bits
* No. of Rounds=8
* No. of Keys in one Round=6
* Total Keys=52
* In Each round 6 different subkeys are used, and four keys are used for output transformation.
* It entirely avoids the use of any lookup tables or S-boxes.



**Process-**

****

Step 1- B1 \* K1

Step 2- B2 + K2

Step 3- B3 + K3

Step 4- B4 \* K4

Step 5- Step 1 **⊕ Step 3**

**Step 6- Step 2 ⊕ Step 4**

**Step 7- Step 5 \* K5**

**Step 8- Step 6 + Step 7**

**Step 9- Step 8 \* K6**

**Step 10- Step 7 + Step 9**

**Step 11- Step 1 ⊕Step 9---------- R1**

**Step 12- Step 3 ⊕ Step 9----------R2**

**Step 13- Step 2 ⊕ Step 10---------R3**

**Step 14- Step 4 ⊕ Step 10…………R4**

**Now, Output of first round is R1, R2, R3 and R4.**

**Swap R2 and R3, We get ----**

**R1, R3, R2, R4 (again, we have 4 blocks. Each having 16 bits).**

**R1, R3, R2, R4 will act as input for the second round. We will repeat this process till 7 rounds.**

**After 8th Round, We get – R1, R2, R3, R4.**

**Now, use the remaining 4 keys-**

**R1 \* K49 ----- CT1**

**R2 \* K50 ------ CT2**

**R3 \* K51 ----- CT3**

**R4 \* K52------- CT4**

**Final Cipher Text= CT1 + CT2 + CT3 + CT4**

**Key Generation-**

**Diagram, timeline

Description automatically generated**

Difference between DES & IDEA Algorithm-

|  |  |  |
| --- | --- | --- |
|  | DES | IDEA |
| Key Size (bits) | 56 | 128 |
| No. of Rounds | 16 | 8 |
| No. of Sub-Keys | 16 | 52 |
| Key Generation | Shift operation | Shift operation |
| Mathematical Operations | X-OR, S-Boxes | X-OR, Addition, Multiplication |
| Attack | Broken, Brute Force, 1998 | NO Known Attack |

**Q. 1-** define the followings-

* S-Box
* Circular shift
* X-OR operation

OR

Discuss the different encryption techniques used in DES algorithm.

Q. 2- how do we generate keys for different rounds in the IDEA algorithm?