→ IPES (Improved proposed encryption Standard)

IDEA (International Data encryption Algo)

- Symmetric key block cipher
- James Massey and Xuijai Lai

— 1991

- intended as a replacement for the DES

Key size : 128 bit

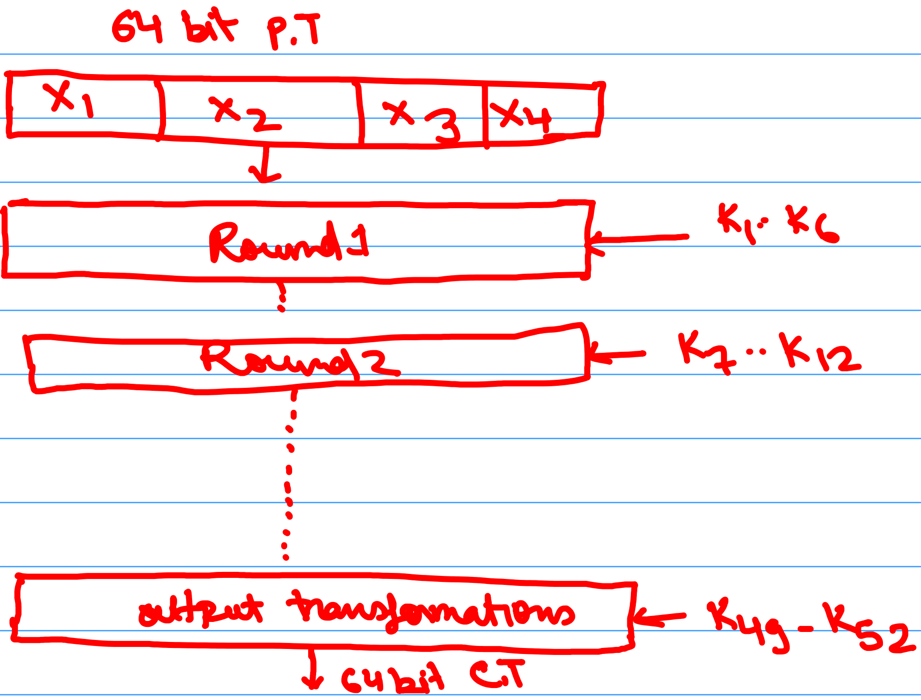
Block size = 64 bit

Round = 8

no. of subkey = 52

In each round, 6 subkeys are used.

Sub key size = 16 bits



Round Transformations

1. Multiply X1 and the first SubKey. $S1 = P1 \times K1$

2. Add X2 and the 2nd subKey $S2 = P2 + K2$

3. Add X3 and 3rd subKey $S3 = P3 + K3$

4. Multiply X4 and 4th subKey $S4 = X4 \times K4$

5. XOR Step 1 and Step3 $S5 = S1 \oplus S3$

6. XOR step 2 and step4 $S6 = S2 \oplus S4$

7. Multiply S5 with K5

8. Add the result of step S6 and S7

9. Multiply the results of Step 8 with K6

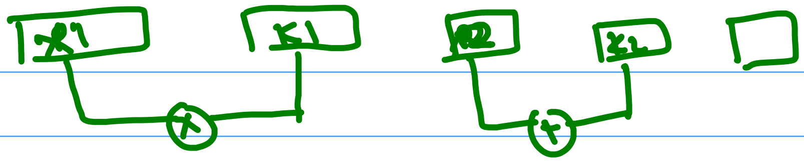
10.. Add the result of Step 7 and S9

11. XOR the result of S1 and S9 ⇒ Y1

12. XOR the result of S3 and S9 ⇒ Y2

13. XOR the result of ~~Ste~~ S2 and $\overset{S}{10}$ ⇒ Y3

14. XOR the result of S4 and S10 ⇒ Y4



output transformation

① Multiply Y1 and the first subkey $Y1 = Y1 \times K1$

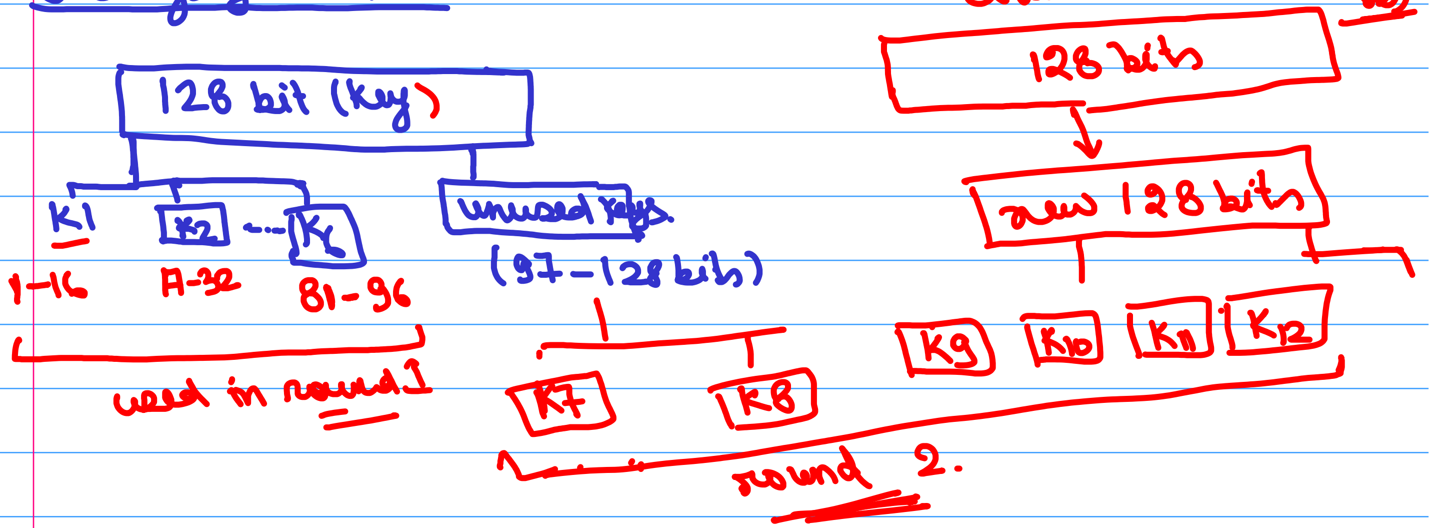
Ⓜ Add Y2 and the second subky. $Y2 = Y2 + K2$

Ⓜ Add Y3 and the third subkey $Y3 = Y3 + K3$

Ⓓ Multiply Y4 and the fourth subkey - $Y4 = Y4 + K4$

$$\underline{CT} = \underbrace{Y1 | Y2 | Y3 | Y4}_{\text{consatenation operation}}$$

Subkeys generation



Simplified Idea (S-IDEA)

P.T : 1001 1100 1010
1100

· key size = 32 bit

PT = 16 bit

K1 K2 K3 K4 K5 K6 K9 K8

Key : 1101 1100 0110 1111 0011 1111 0101 1001

K1 = 11

$x_1 = 1001$

$x2 = 1100$

$x3 = 1010$

$x4 = 1100$