International Data Encryption Algorithm(IDEA) for IT 7th Sem Students

Developed and Presented By:

Dileep Kumar Yadav
Assistant professor
Dept. of CSE
V.B.S PU,Jaunpur
Mb. No.8726943272
Email-dileep1482@gmail.com

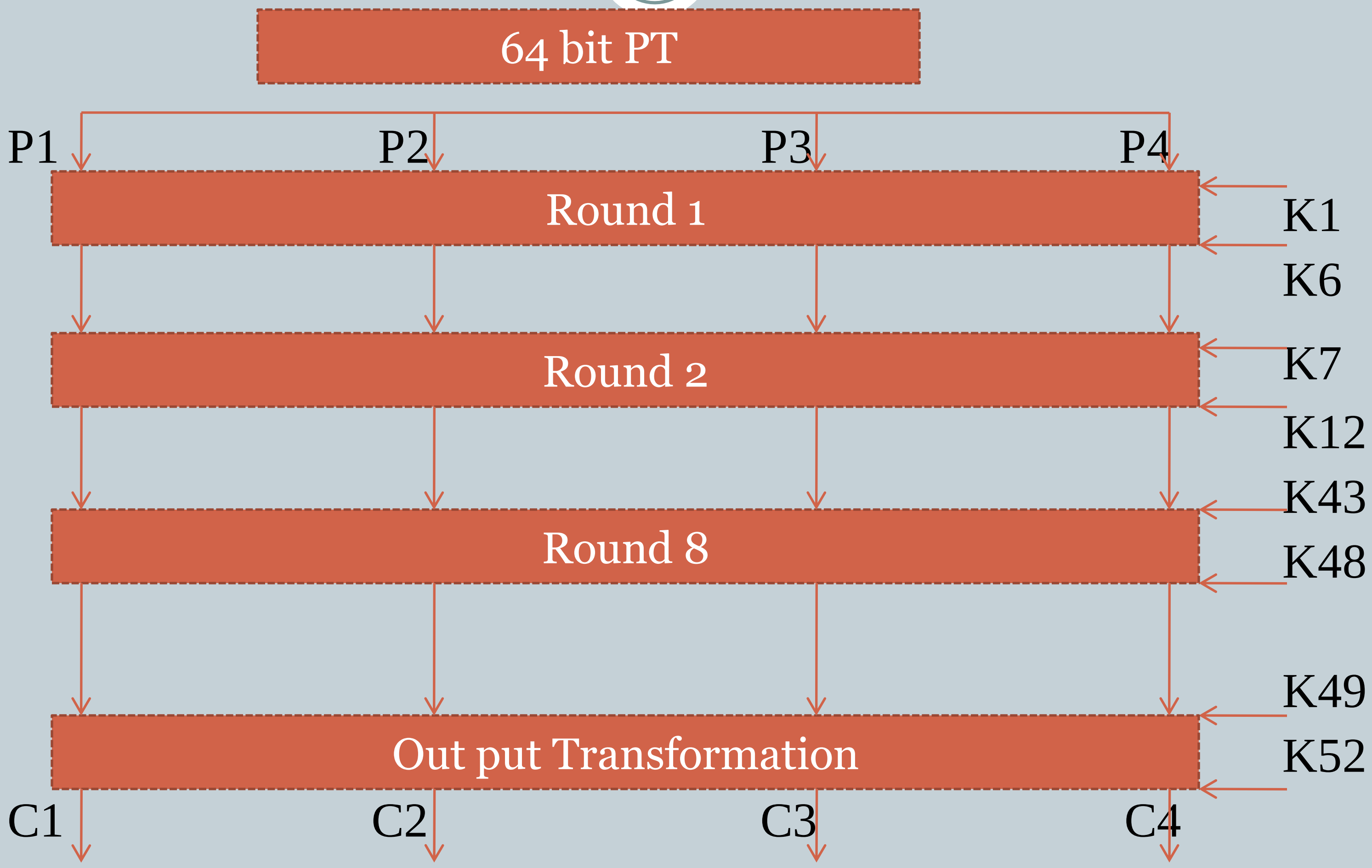
International Data Encryption Algorithm(IDEA)

- IDEA is strongest cryptographic algorithm.
- It was launched in 1990 and finally named IDEA in 1992.
- It is also block cipher.
- It is patent algorithm.
- One popular email privacy technology i.e. PGP is based on IDEA.

How IDEA Works

- It also works on 64 bit plain text blocks.
- The key is longer however and consists of 128 bits.
- It is reversible like DES that is the same algorithm is used for encryption and decryption process.

Cont…



64 bit PT

P1 P2 P3 P4

Round 1

K1

K6

Round 2

K7

K12

Round 8

K43

K48

Out put Transformation

K49

K52

C1 C2 C3 C4

Rounds

- We have mentioned above diagram there are 8 rounds in IDEA.
- Each rounds involves a series of operations on the four data blocks using 6 keys.
- After 8 rounds there is output transformation which produces 64 bits cipher text.
- Round are performed on some mathematical operation like multiplication, addition, and XOR operations.

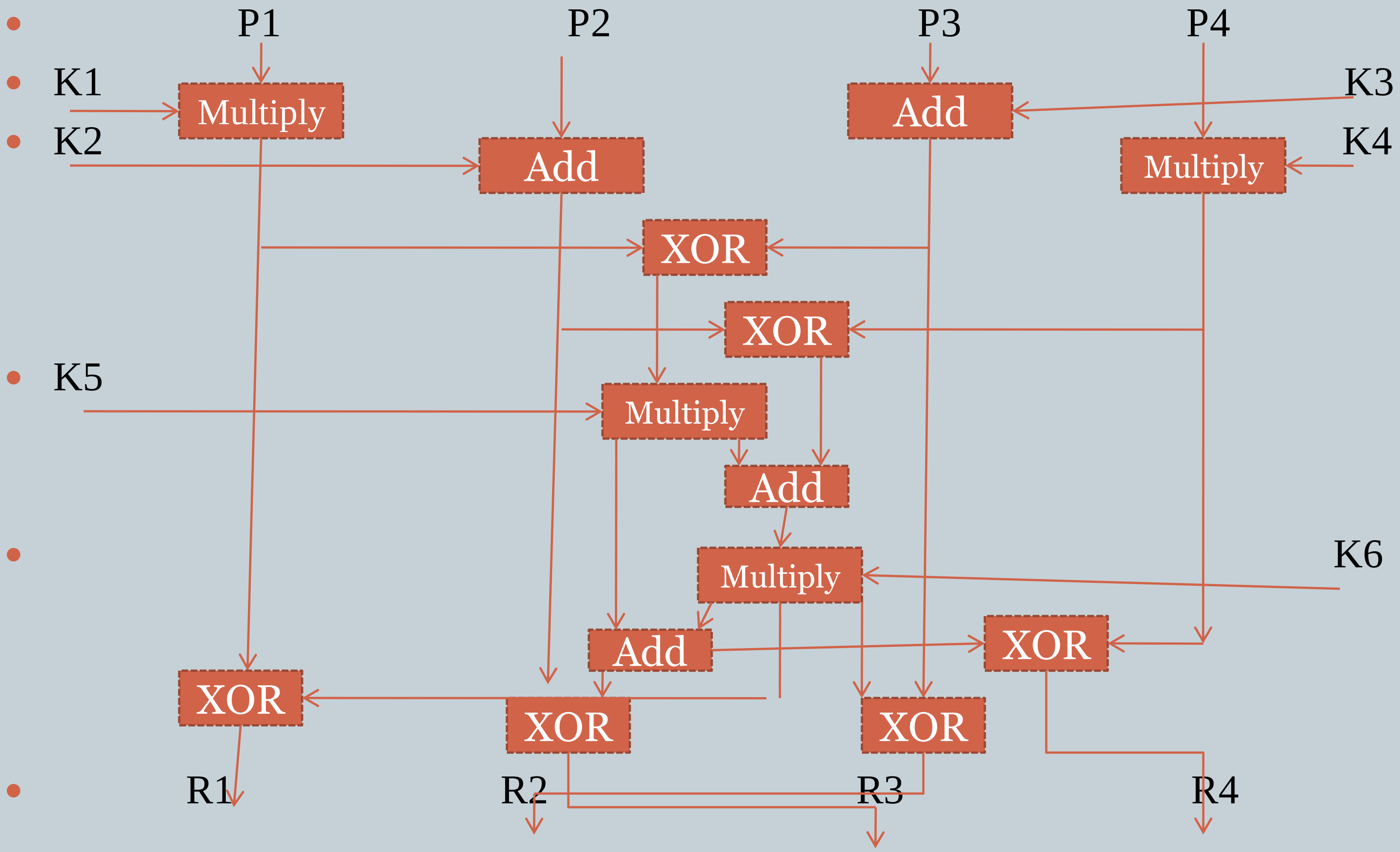
Cont…

- Step1-multiply P1 and K1
- Step2- Add P2 and K2
- Step3-Add P3 and K3
- Step4-Multiply P4 and K4
- Step5-XOR the results of step1 and step3
- Step6-XOR the results of step2 and step4
- Step7-Multiply the results of step5 with K5
- Step8-Add the results of step6 and step7
- Step9- Multiply the results of step8 with K6

Cont…

- Step10-Add the results of step7 and step9
- Step11-XOR the results of step1 and step9
- Step12-XOR the results of step3 and step9
- Step13-XOR the results of step2 and step10
- Step14-XOR the results of step4 and step10

Circuit Diagram of IDEA in One Round



P1 P2 P3 P4

- K1 Multiply
- K2 Add
Add K3
Multiply K4

XOR

XOR

- K5 Multiply

Add

- Multiply K6

Add XOR

XOR XOR XOR

- R1 R2 R3 R4

Sub key Generation for a Round

- We mentioned here each of the eight rounds make use of six sub keys so 8*6=48 sub keys are required for the rounds.
- The final output transformation uses four sub keys making a total sub keys i.e. 48+4=52 sub keys are generated.
- Form an input key of 128 bits how are these 52 sub keys are generated.
- Let us understands this with the explanation for the first rounds.

First Rounds

- We know that the initial key consists of 128 bits, from which 6 sub keys k1 to k6 are generated for the first round.
- Since k1 to k6 consist of 16 bits each, out of the original 128 bits, the first 96 bits i.e. 6 sub keys*16bits per key are used for the first rounds.
- At the end of first rounds 97 to 128 bits of the original keys are unused.

Second Round

- In the second round firstly the 32 unused bits(i.e.97 to 128) of the first round are used. We know that each round requires 6 sub keys k1 to k6 each of 16 bits making a total of 96 bits.
- Thus for the second round we still require 96-32=64 more bits. However we have already exhausted all the 128 bits of the original key. How do we now get the remaining 64 bits?
- For this IDEA employs the technique of key shifting. At this stage the original key is shifted left circularly by 25 bits.

Cont…

- That is the 26th bit of the original key moves to the first position and becomes the first bit after the shift and the 25th bit of the original key moves to the last position and becomes the 128th bit after the shift.
- So in this way this process works at 8 rounds and finally total 128 bits are used properly.

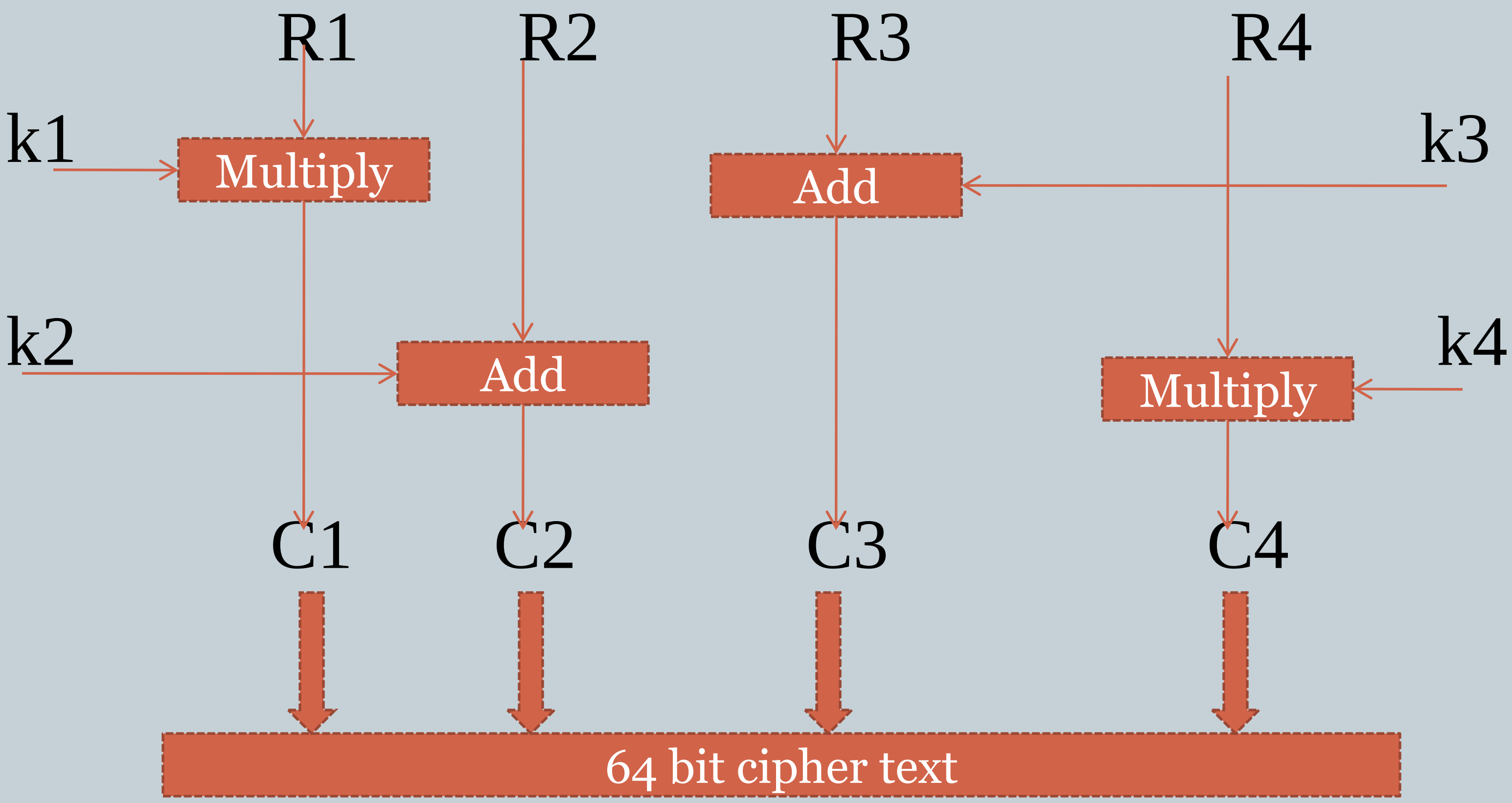
Output Transformation

- The output transformation is one time operation. It takes place at the end of the 8th round.
- The input to the output transformation is of course the output of the 8th round.
- This is as usual a 64 bit value divided into four sub block i.e.R1 to R4 each consisting of 16 bits.
- In output transformation four sub keys are used like k49 to k52.

Details of the Output Transformation

- Step1- Multiply R1 and K1
- Step2- Add R2 and K2
- Step3- Add R3 and K3
- Step4- Multiply R4 and K4

Output Transformation Process



R1 R2 R3 R4

k1 Multiply Add k3

k2 Add Multiply k4

C1 C2 C3 C4

64 bit cipher text

Reference

- Cryptography and network security “Atul Kahate” 3e,Mc Graw hill education.