IDEA

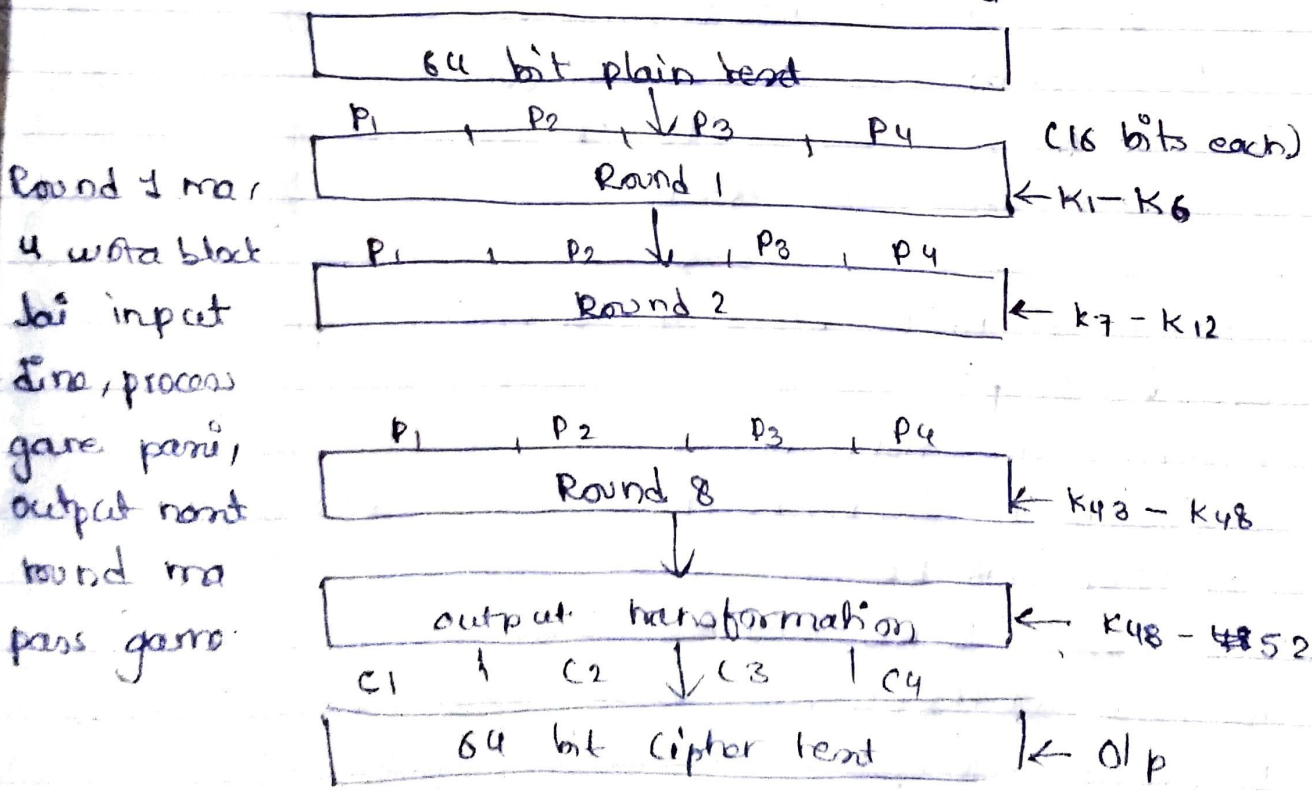
Block size - 64 bits (divided into 4 parts (16 bit each)

key size - 128 bits single key (52 sub keys generate garne) ?
52 " " will be 16 bit each

8 identical transformation Rounds [Each round, 6 subkeys use (6X8 = 48 subkey

One half Round i.e. [Uses 4 subkeys (16 bit each)

Output Transformation: O/p after this round gives ciphertext (64 bit)



Round 1 ma, 4 wota block lai input dine, process gare pani, output round ma pass garne

3 operations are used in IDEA to combine two 16 bit values to produce a 16 bit result, addition, XOR & multiplication.

Single Round

6 XOR
6 subkeys

S1
S2 $P_1 \times K_1$
S3 $P_2 + K_2$
S4 $P_3 + K_3$
$P_4 \times K_4$

S5
S6 $S_1 \oplus S_3$ step 1 ra step 3 ta result X-OR
$S_2 \oplus S_4$

S7 $S_5 \times K_5$
S8 $S_6 + S_7$
S9 $S_8 \times K_6$
S10 $S_7 + S_9$

S11 $S_1 \oplus S_9$ → new P_1
S12 $S_3 \oplus S_9$ → new P_2 ↕ swap
S13 $S_2 \oplus S_{10}$ → new P_3
S14 $S_4 \oplus S_{10}$ → new P_4

In 2nd Round, P_1 P_3 P_2 P_4

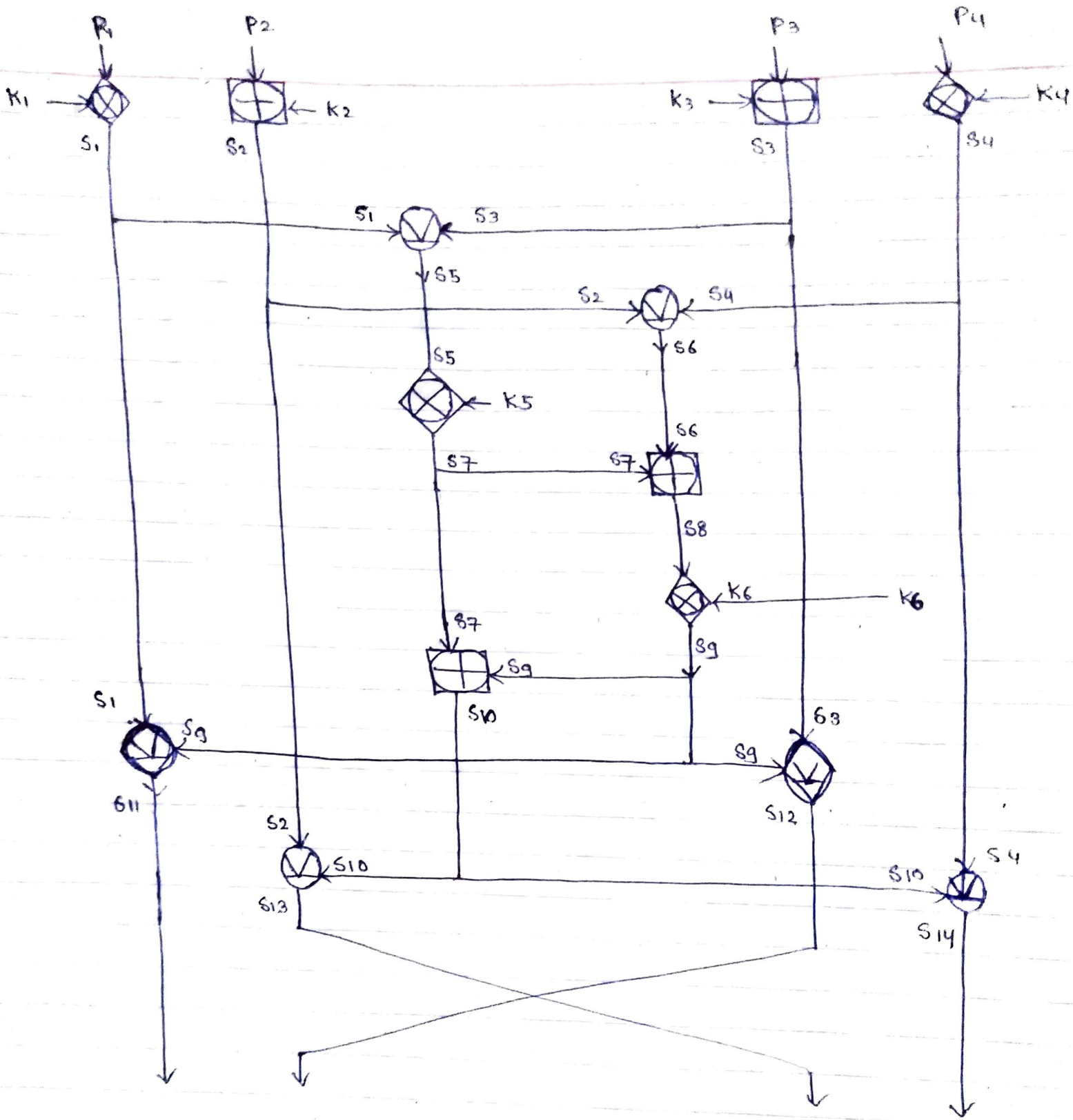
In 8th Round X swap.

Output transformation, One-half round

After 8th round, let output be R_1, R_2, R_3, R_4 (no swap)

$R_1 \times K_{49} \rightarrow C_1$ (16 bits
$R_2 + K_{50} \rightarrow C_2$ (16 bits } 64 bits
$R_3 + K_{51} \rightarrow C_3$ (16 bits
$R_4 \times K_{52} \rightarrow C_4$ (16 bits

lets say output of 8th R is P_1, P_2, P_3, P_4


P1
P2
P3
P4
K1
K2
K3
K4
S1
S2
S3
S4
S1
S3
S5
S2
S4
S6
S5
K5
S6
S7
S7
S8
K6
K6
S7
S9
S9
S10
S1
S9
S3
S9
S11
S12
S2
S10
S10
S4
S13
S14