→ also called as IPES (Improved proposed Encryption standard)

PAGE NO.:
DATE

(VIII) IDEA Algorithm :-

(1) IDEA Algorithm " International Data Encryption Algorithm "

(2) Symmetric key block cipher.

(3) It was intended as a replacement for the DES (Data Encryption standard)

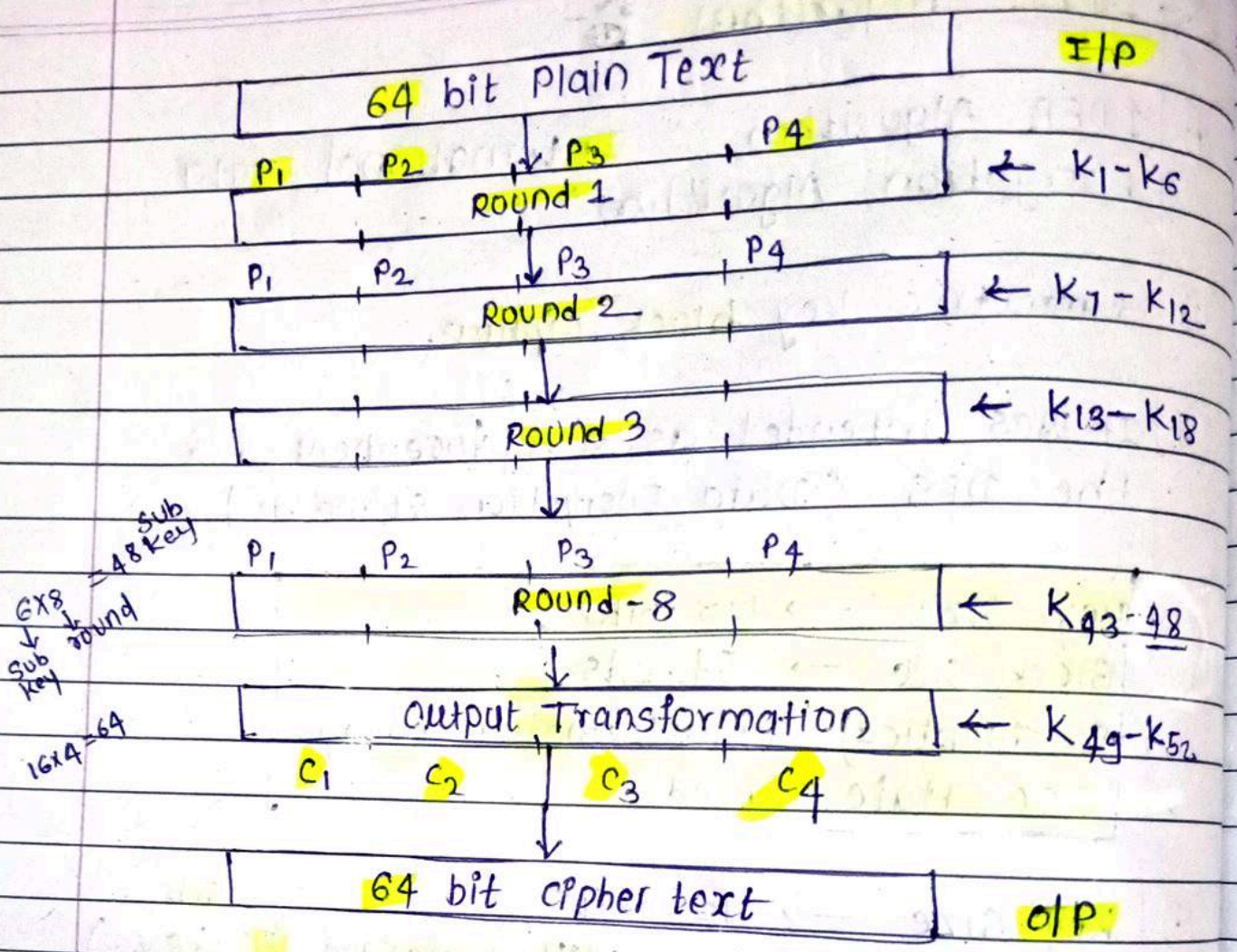
key Size → 128 bits
Block Size → 64 bits
8 identical Transformation Rounds
One Hafe round.

(1) key Size → 128 bits
(from Which We Will generate 52 sub key)

(2) Block Size → 64 bits.
(In each round, block divided into 4 parts 16 bit each)

(3) 8 identical Transformation Rounds →
(In each round, 6 sub keys are used)
(16 bit each)

(4) One Hafe Round i.e., the
(It uses 4 subkeys (16 bit each))
o/p after this round gives ciphertext (64 bits)



IDEA Algorithm

PAGE NO.:
DATE

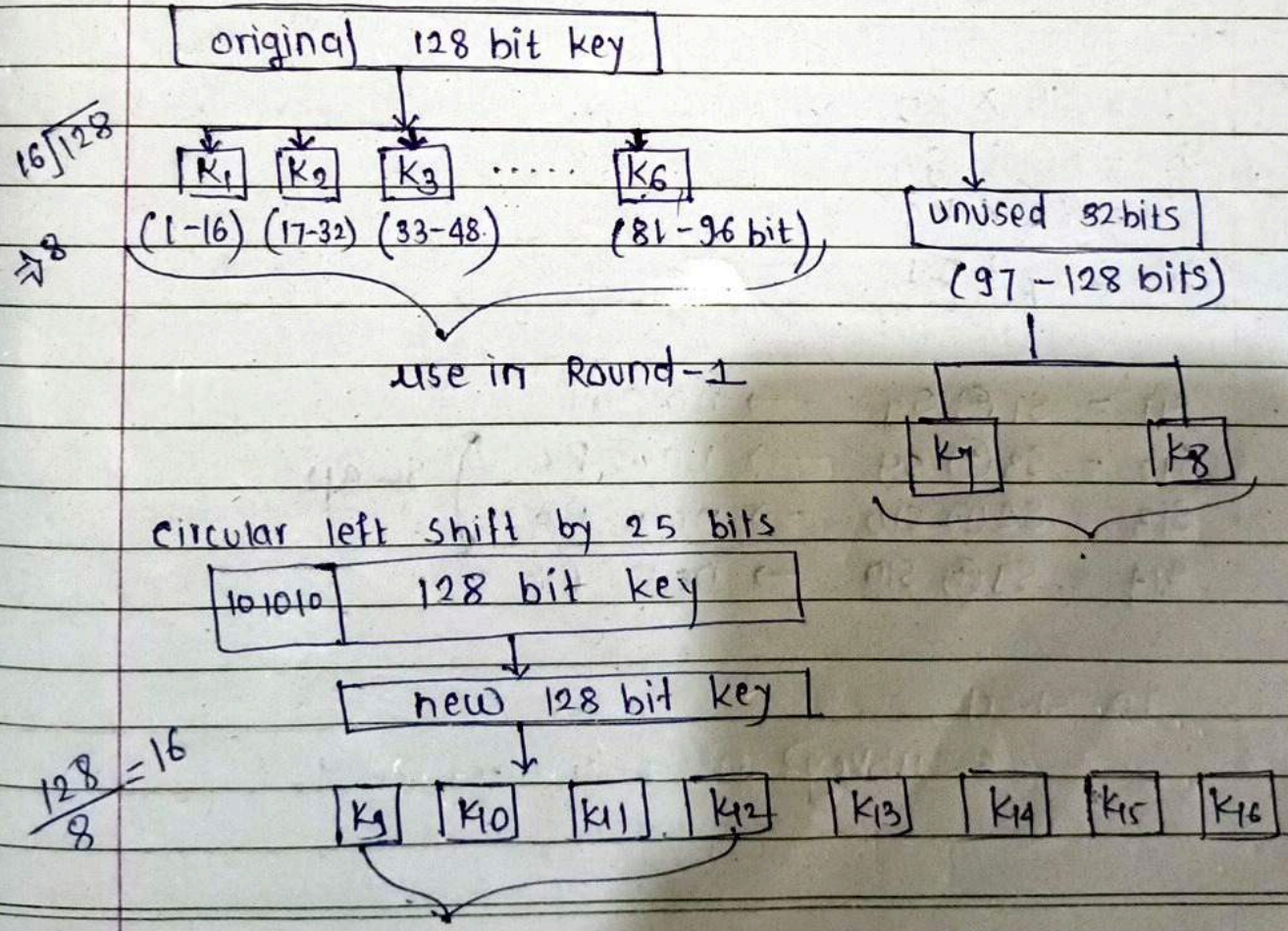
① I/P divided into 4 portions P1 to P4 (16 bit each)

② There are 8 Similar Rounds

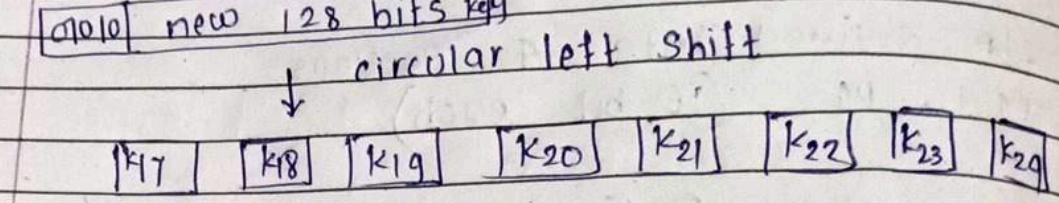
③ each round uses 6 subkeys (16 bit each)

④ Last Round i.e., the output Transformation produces the ciphertext uses 4 subkey (16 bit each).

52 Subkey Generation :-



circular left shift by 25 bits.



(iii) Single Round Details :-

$S1 = P1 \times K_1$
$S2 = P_2 + k_2$
$S3 = P3 + k_3$
$S4 = P4 \times K4$

$S5 = S1 \oplus S3$
$S6 = S2 \oplus S4$

$S7 = S5 \times K5$
$S8 = S6 + S7$
$S9 = S8 \times K6$
$S10 = S_7 + S9$

$S11 = S_1 \oplus S_9$ → new P1
$S12 = S3 \oplus S9$ → new P2
$S13 = S2 \oplus S10$ → new P3
$S14 = S9 \oplus S10$ → new P4

swap

In short,
6 subkey used in round 1

PAGE NO.:
DATE

(II) output Transformation :-

i.e., one halfe round

$R_1 \times K_{49} = C_1$ (16 bit)
$R_2 + K_{50} = C_2$
$R_3 + K_{51} = C_3$
$R_4 \times K_{52} = C_4$

} 64 bit o/p.

→ It takes place at the end of 8th round
→ I/p to this block is a 64 bit value divided into 4-sub blocks (say R_1, R_2, R_3 and R_4)

no swapping in 8th round.

—x—

IDEA :-

① It encrypts 64-bit block of plaintext into 64-bit block of cipher text using a 128 bit key

② It was designed to provide secure encryption for digital data and is used in a variety of appl^n. Such as
① secure communications,
② financial transactions
③ electronic voting systems.