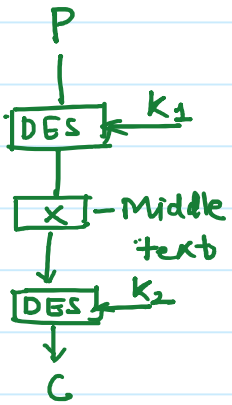
Multiple DES:

2-DES:

Encryption $C = DES_{k_2}(DES_{k_1}(P))$ ✓

Decryption $P = DES^{-1}_{k_1}(DES^{-1}_{k_2}(C))$



DES doesn't form a group under composition operation.

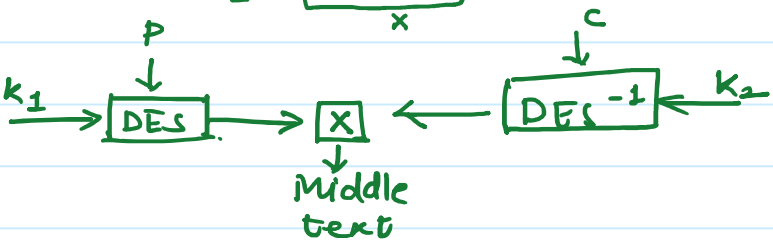
⇒ It seems that applying DES twice with two different key provides additional security.

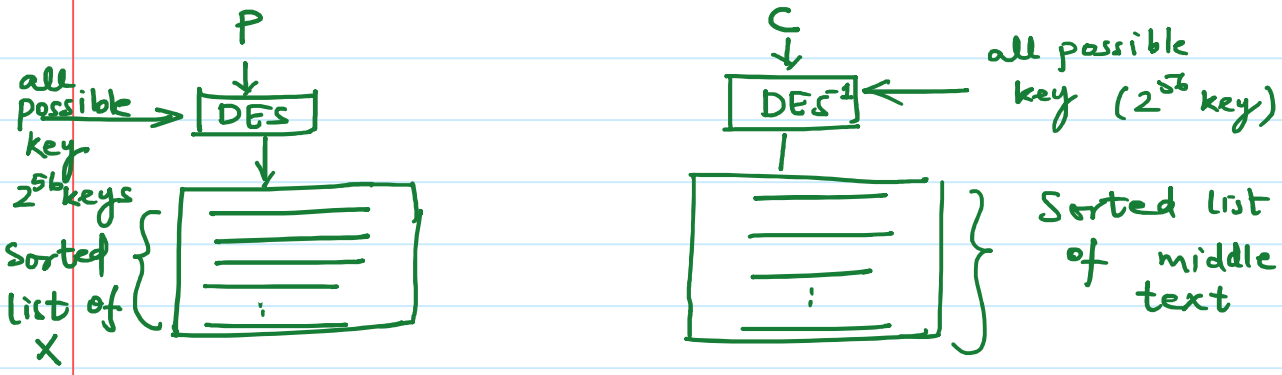
2-DES is expected to provide security equivalent to 112 (56 × 2) bits.

Meet-in-the-middle Attack:

Let (P, C) be a known plaintext-ciphertext pair.
and let (k_1, k_2) be the key.

$C = DES_{k_2}(\underbrace{DES_{k_1}(P)}_{X})$





We check the result of these two tables for a match.

If a match occur. the corresponding values of K_1 & K_2 may be the key.

For a plaintext block of 64 bits there are 2^{64} possible ciphertext values.

There are 2^{112} possible keys.

for a given plaintext P & the corresponding ciphertext C the average no. of keys that will produce the ciphertext C is $\frac{2^{112}}{2^{64}} = 2^{48}$

Therefore, there may be 2^{48} false alarms on the first (P, C) pair.

If we have another plaintext-ciphertext pair (P', C') then the above avg. becomes

$$2^{48-64} = 2^{-16}$$

If MITM attack is performed with two blocks of known plaintext-ciphertext pair

The prob that the correct key. is determined is $\underline{1-2^{-16}}$

3-DES: To avoid MIM attack we can use 3-DES (DES with 3 times) with 3 different keys or 2 different keys.

First: $C = DES_{k_3}(DES_{k_2}(DES_{k_1}(P)))$

second $C = DES_{k_1}(DES_{k_2}(DES_{k_1}(P)))$

⇒ 3 DES with 2 different keys is a relatively popular alternative to DES & it has been adopted for use in the key management std ANSI X9.17 & ISO 8732.

⇒ Currently, there is no practical cryptographic attack on 3-DES.

International Data Encryption Algorithm (IDEA)

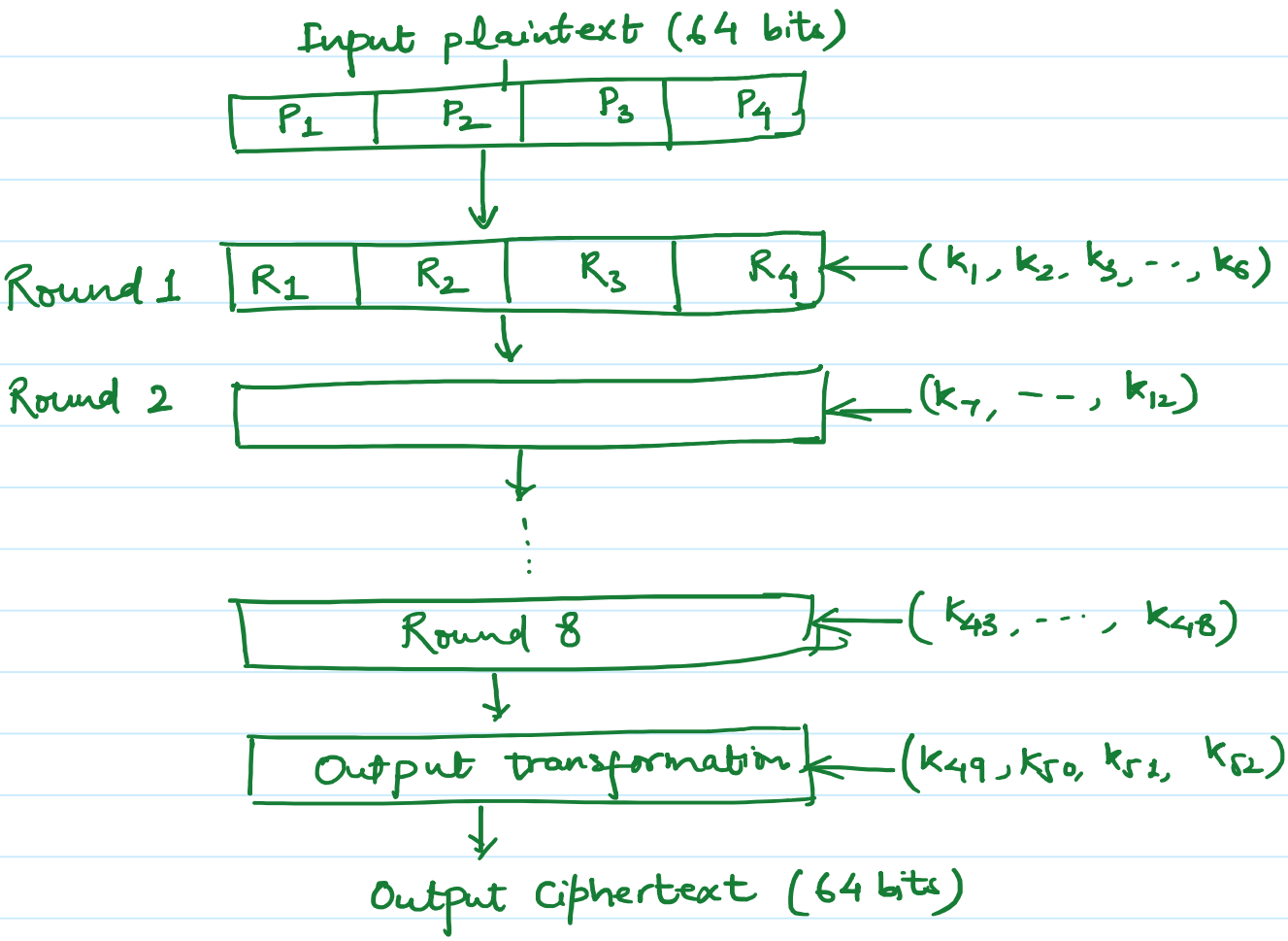
IDEA is one of the strongest cryptographic algorithm.

In 1990 : Proposed Encryption Std (PES) ✓
1991 : Improved PES (IPES)
1992 : IDEA

IDEA is also a block cipher.
There is no S-boxes in IDEA.

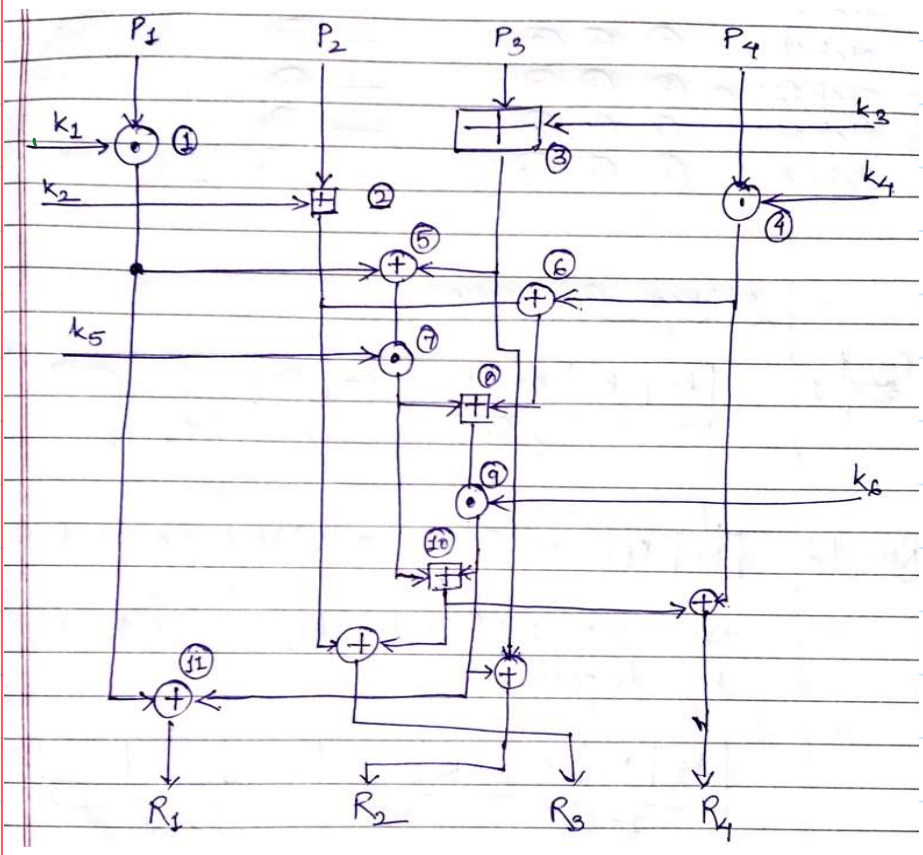
PGP is based on IDEA.

Basic Structure of IDEA



Operations in IDEA: ⊕ – XOR
⊞ – Addition Modulo 2^{16} (65536)
⊙ – Multiplication modulo $2^{16}+1$.

One Round of IDEA

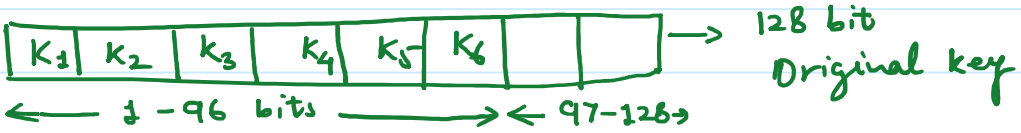


(1)	$P_1 \odot k_1$
(2)	$P_2 \boxplus k_2$
(3)	$P_3 \boxplus k_3$
(4)	$P_4 \odot k_4$
(5)	(1) ⊕ (3)
(6)	(2) ⊕ (4)
(7)	(5) ⊙ k_5
(8)	(6) ⊞ (7)
(9)	(8) ⊙ k_6
(10)	(7) ⊞ (9)
(11)	(1) ⊕ (9)
(12)	(3) ⊕ (9)
(13)	(2) ⊕ (10)
(14)	(4) ⊕ (10)

Steps in one round of IDEA.

Subkey Generation:

Round 1



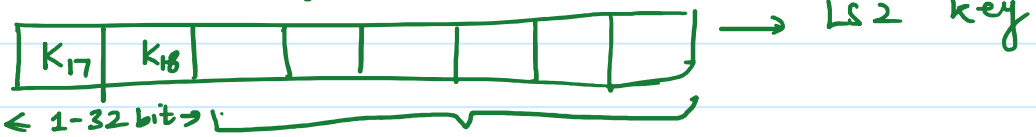
Round 2:

— First two subkeys for round 2 of the original key

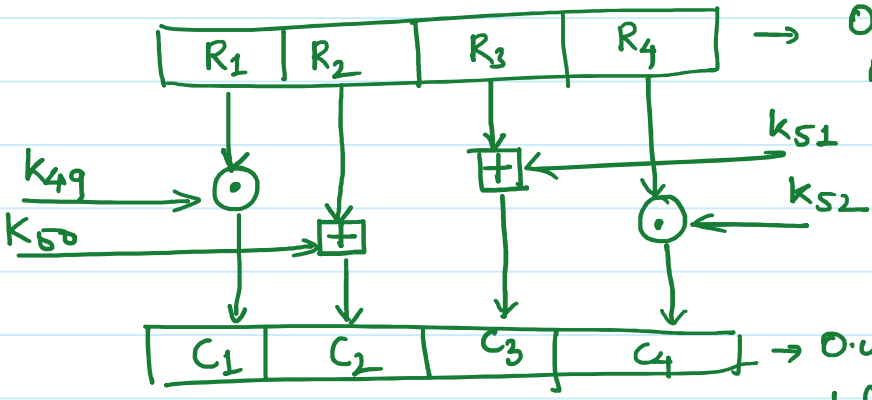
Now, a 25-bit circular left shift on the original key happens

Round 3

Now, a 25-bit circular left shift happens on LS 1 key



Output Transformation:



→ Output of the 8th round of IDEA.

→ Output Ciphertext block (64-bits)

⇒ Decryption Algorithm is same as the encryption algo.

⇒ Decryption subkeys are the inverse of encryption subkeys

Strength:

1. It uses 128-bit key, double than the key size of DES.
2. Size of the key space (2^{128}) is very large.
3. Examing half of the possible keys using a single computer takes more than 5.4×10^{23} years.