1- The generated subkey must have this relation to one another:

$$k_{i+1} = k_{16-i} \quad \text{for } i = \phi, 1, \ldots, 7$$

2- Rotating all ϕs or all 1s is the only way. Because they always produce the same subkey in each round:

1. $C_0 = (FFFFFFF)_{16}$ and $D_0 = (FFFFFFF)_{16}$
2. $C_0 = (FFFFFFF)_{16}$ and $D_0 = (0000000)_{16}$
3. $C_0 = (0000000)_{16}$ and $D_0 = (FFFFFF)_{16}$
4. $C_0 = (0000000)_{16}$ and $D_0 = (0000000)_{16}$

The weak keys after PC-1 are:

1. $(00000000000000)_{16}$
2. $(0000000FFFFFFF)_{16}$
3. $(FFFFFFF0000000)_{16}$
4. $(FFFFFFFFFFFFFF)_{16}$

3- The liklyhood of choosing one of these 4 at random:

$$\frac{4}{2^{56}} = \frac{2^2}{2^{56}} = \frac{1}{2^{54}}$$

4- We should not use weak keys in multiple DES algorithms. Because we will reach the plaintext again, after eg. 2 encryption with the same weak key. for example: By using the first weak key (shown in part 2), after two following encryption, the second cipher text will be just like the plaintext in the begining.

5- There are 6 key pairs that are called semi-weak.

pairs:

	first				second			
1.	01FE	01FE	01FE	01FE	FE01	FE01	FE01	FE01
2.	1FE0	1FE0	0EF1	0EF1	E01F	E01F	F10E	F10E
3.	01E0	01E0	01F1	01F1	E001	E001	F101	F101
4.	1FFE	1FFE	0EFE	0EFE	FE1F	FE1F	FE0E	FE0E
5.	011F	011F	010E	010E	1F01	1F01	0E01	0E01
6.	E0FE	E0FE	F1FE	F1FE	FEE0	FEE0	FEF1	FEF1

6- These keys only produce 2 different subkeys, each used 8 times in the algorithm.

7- total number of these keys: $4+12+48=64$

→ probability of choosing one of these keys:

$$\frac{64}{2^{56}} = \frac{2^6}{2^{56}} = \frac{1}{2^{50}} = 2^{-50} \cong \underbrace{8,8 \times 10^{-16}}$$

→ It is almost impossible

1- S-Box is nonlinear. So, it makes DES secure.

2- $x_1 = 101010$, $x_2 = 010101$, $x_1 \oplus x_2 = 111111$

x_1: row: 10 ⇒ 2, column: 0101 ⇒ 5

x_2: rows: 01 ⇒ 1, column: 1010 ⇒ 10

$x_1 \oplus x_2$: rows: 11 ⇒ 3, column: 1111 ⇒ 15

⇒ $i = 1$
- $S_1(x_1) \oplus S_1(x_2) = 06 \oplus 12 = (0110) \oplus (1100) = (1010)$
- $S_1(x_1 \oplus x_2) = S_1(111111) = 13 = (1101)$

⇒ ≠

⇒ $i = 2$
- $S_2(x_1) \oplus S_2(x_2) = 04 \oplus 01 = (0100) \oplus (0001) = 0101$
- $S_2(x_1 \oplus x_2) = S_2(111111) = 09 = (1001)$

⇒ ≠

⇒ $i = 3$
- $S_3(x_1) \oplus S_3(x_2) = 15 \oplus 05 = (1111) \oplus (0101) = (1010)$
- $S_3(x_1 \oplus x_2) = S_3(111111) = 12 = (1100)$

⇒ ≠

⇒ $i = 4$
- $S_4(x_1) \oplus S_4(x_2) = 11 \oplus 02 = (1011) \oplus (0010) = (1001)$
- $S_4(x_1 \oplus x_2) = S_4(111111) = 14 = (1110)$

⇒ ≠

⇒ $i = 5$
- $S_5(x_1) \oplus S_5(x_2) = 13 \oplus 15 = (1101) \oplus (1111) = (0010)$
- $S_5(x_1 \oplus x_2) = S_5(111111) = 03 = (0011)$

⇒ ≠

⇒ $i = 6$
- $S_6(x_1) \oplus S_6(x_2) = 08 \oplus 13 = (1000) \oplus (1101) = (0101)$
- $S_6(x_1 \oplus x_2) = S_6(111111) = 13 = (1101)$

⇒ ≠

⇒ $i = 7$
- $S_7(x_1) \oplus S_7(x_2) = 03 \oplus 05 = (0011) \oplus (0101) = (0110)$
- $S_7(x_1 \oplus x_2) = S_7(111111) = 12 = (1100)$

⇒ ≠

⇒ $i = 8$
- $S_8(x_1) \oplus S_8(x_2) = 12 \oplus 06 = (1100) \oplus (0110) = (1010)$
- $S_8(x_1 \oplus x_2) = S_8(111111) = 11 = (1011)$

⇒ ≠

3- input: 100011
- row: 11 ⇒ 3
- column: 0001 ⇒ 1

⇒ output: 12 ⇒ (1100)

[1]- x is the plain text. IP(x) maps bit 57 to bit 33. This means:

$L_0 = \emptyset$ and $R_0 = 2^{31}$

Now we should calculate $f(R_0)$. the 1 in R_0 is in position 1. E-Expansion box maps bit 1 to position 1 and 48. This means:

$S_1 = 010000$, $S_2 = S_3 = S_4 = S_5 = S_6 = S_7 = 000000$, $S_8 = 000001$

⟹ So 2 S-Boxes (S_1 & S_8) get a different input.

[2]-

SBox	input	row	Column	output
S_1	⟹ 010000	0	8	0011
S_2	⟹ 000000	0	0	1111
S_3	⟹ 000000	0	0	1010
S_4	⟹ 000000	0	0	0111
S_5	⟹ 000000	0	0	0010
S_6	⟹ 000000	0	0	1100
S_7	⟹ 000000	0	0	0100
S_8	⟹ 000001	1	0	0001

⟹ Then, This will be permuted by P:

11010000001011000010110111001110 (I)

⟹ Then, This will be XORed with $L_\emptyset$. As $L_\emptyset$ is $\emptyset$, R_1 will be just the same as up.

⟹ So:

$L_1 = R_0 = (08000000)_{16}$, $R_1 = (D0585B9E)_{16}$

[3]- The minimum number of output bits that will be changed per S-Box as a result of a 1bit change in input, is 2.

4_ The all-zero case : $S_1(0) = 1110$, $S_2(0) = 1111$, $S_3(0) = 1010$, $S_4(0) = 0111$

, $S_5(0) = 0010$, $S_6(0) = 1100$, $S_7(0) = 0100$, $S_8(0) = 1101$

↳ output of S-Boxes : 11101111101001110010110001001101

↳ after permutation: 11011000110110001101101110111100 (II)

↳ Now I should calculate the XOR of this code, with the one I calculated in part 2 :

(I) XOR (II) = 000010001000000001000000000100010 ⇒ 5 output bits of R_1 are different and L_1 is just like R_0. So it has 1 bit different. ↳ Total = 5+1 = 6

1- The K_0 and K_1 are: $K_0 = (w_0, w_1, w_2, w_3)$, $K_1 = (w_4, w_5, w_6, w_7)$

→ first step: initial K_0 addition with plaintext:

$$\begin{bmatrix} 2B & 28 & AB & 09 \\ 7E & AE & F7 & CF \\ 15 & D2 & 15 & 4F \\ 16 & A6 & 88 & 3C \end{bmatrix} \oplus \begin{bmatrix} 01 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{bmatrix} = \begin{bmatrix} 2A & 28 & AB & 09 \\ 7E & AE & F7 & CF \\ 15 & D2 & 15 & 4F \\ 16 & A6 & 88 & 3C \end{bmatrix}$$

K_0 — input — result of this step

→ Next; SubBytes:

E5	34	62	01
F3	E4	68	8A
59	B5	59	84
47	24	C4	EB

→ Next; ShiftRows:

E5	34	62	01
E4	68	8A	F3
59	84	59	B5
EB	47	24	C4

→ Next; MixColumns:

$$\begin{bmatrix} B_0 \\ B_1 \\ B_2 \\ B_3 \end{bmatrix} \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} = \begin{bmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{bmatrix}$$

each column of the matrix calculated in the former step. (input columns)

the outputted column

first Column:
$$\begin{bmatrix} 02 \times E5 + 03 \times E4 + 01 \times 59 + 01 \times EB \\ 01 \times E5 + 02 \times E4 + 03 \times 59 + 01 \times EB \\ 01 \times E5 + 01 \times E4 + 02 \times 59 + 03 \times EB \\ 03 \times E5 + 01 \times E4 + 01 \times 59 + 02 \times EB \end{bmatrix}$$

second Column:
$$\begin{bmatrix} 02 \times 34 + 03 \times 68 + 01 \times 84 + 01 \times 47 \\ 01 \times 34 + 02 \times 68 + 03 \times 84 + 01 \times 47 \\ 01 \times 34 + 01 \times 68 + 02 \times 84 + 03 \times 47 \\ 03 \times 34 + 01 \times 68 + 01 \times 84 + 02 \times 47 \end{bmatrix}$$

third Column:
$$\begin{bmatrix} 02 \times 62 + 03 \times 8A + 01 \times 59 + 01 \times 24 \\ 01 \times 62 + 02 \times 8A + 03 \times 59 + 01 \times 24 \\ 01 \times 62 + 01 \times 8A + 02 \times 59 + 03 \times 24 \\ 03 \times 62 + 01 \times 8A + 01 \times 59 + 02 \times 24 \end{bmatrix}$$

forth colum:
$$\begin{bmatrix} 02 \times 01 + 03 \times F3 + 01 \times B5 + 01 \times C4 \\ 01 \times 01 + 02 \times F3 + 03 \times B5 + 01 \times C4 \\ 01 \times 01 + 01 \times F3 + 02 \times B5 + 03 \times C4 \\ 03 \times 01 + 01 \times F3 + 01 \times B5 + 02 \times C4 \end{bmatrix}$$

$\Rightarrow$ the produced state:

54	13	3C	7D
36	34	A2	FC
95	86	36	D4
44	3E	3D	D6

$(P(x) = x^8 + x^4 + x^3 + x + 1)$

$\Rightarrow$ Next; AddRoundKey:

K_1

A0	88	23	2A
FA	54	A3	6C
FE	2C	39	76
17	B1	39	05

$\oplus$

input

54	13	3C	7D
36	34	A2	FC
95	86	36	D4
44	3E	3D	D6

=

result of this step

F4	9B	1F	57
CC	60	01	90
6B	AA	0F	A2
53	8F	04	D3

$\Rightarrow$ So, the output of first round is:

$(F4CC6B539B60AA8F1F010F045790A2D3)_{16}$

2- The k_0 and k_1 are the same as part.

→ first step: As the input is all-zero, the addition of plaintext with the K_0, will be just the K_0:

2B	28	AB	09
7E	AE	F7	CF
15	D2	15	4F
16	A6	88	3C

→ Next; SubBytes:

F1	34	62	01
F3	E4	68	8A
59	B5	59	84
47	24	C4	EB

→ Next; ShiftRows:

F1	34	62	01
E4	68	8A	F3
59	84	59	B5
EB	47	24	C4

→ Next; MixColumns: the formulation is just like the part 1:

- first Column:
$$\begin{bmatrix} 02 \times F1 + 03 \times E4 + 01 \times 59 + 01 \times EB \\ 01 \times F1 + 02 \times E4 + 03 \times 59 + 01 \times EB \\ 01 \times F1 + 01 \times E4 + 02 \times 59 + 03 \times EB \\ 03 \times F1 + 01 \times E4 + 01 \times 59 + 02 \times EB \end{bmatrix}$$

second, third and forth Columns are just like part 1.

→ the produced state:

7C	13	3C	7D
22	34	A2	FC
81	86	36	D4
78	3E	3D	D6

$(P(x) = x^8 + x^4 + x^3 + x + 1)$

⟹ Next; AddRoundkey: the formulation is like part 1.

DC	9B	1F	57
D8	60	01	90
7F	AA	0F	A2
6F	8F	04	D3

⟹ So, the output of first round is:

$(DCD87F6F9B60AA8F1F010F045790A2D3)_{16}$

3 - By XORing the two output values together, we can see how many output bits have been altered:

$$(\underbrace{2814143C}_{}000000000000000000000000)_{16}$$

↓

Just the first column is altered after first round:

$(2814143C)_{16} = (00101000000101000001010000111100)_b$

⇓

the 1s in this, correspond to output bits which have changed. There are Ten of them.

⟹ So, the number of output bits which have changed due to a 1 bit change in input, is 10 after the first round.

Scanned by CamScanner

all polynomials with degree $= 4$:

$x^4+x^3+x^2+x+1 \Rightarrow \begin{matrix} x=0 \to 1 \\ x=1 \to 1 \end{matrix} \Rightarrow \checkmark$

$x^4+x^3+x^2+x \Rightarrow \begin{matrix} x=0 \to 0 \\ x=1 \to 0 \end{matrix} \Rightarrow \times$

$x^4+x^3+x^2+1 \Rightarrow \begin{matrix} x=0 \to 1 \\ x=1 \to 0 \end{matrix} \Rightarrow \times$

$x^4+x^3+x+1 \Rightarrow \begin{matrix} x=0 \to 1 \\ x=1 \to 0 \end{matrix} \Rightarrow \times$

$x^4+x^2+x+1 \Rightarrow \begin{matrix} x=0 \to 1 \\ x=1 \to 0 \end{matrix} \Rightarrow \times$

$x^4+x^3+x^2 \Rightarrow \begin{matrix} x=0 \to 0 \\ x=1 \to 1 \end{matrix} \Rightarrow \times$

$x^4+x^3+x \Rightarrow \begin{matrix} x=0 \to 0 \\ x=1 \to 1 \end{matrix} \Rightarrow \times$

$x^4+x^3+1 \Rightarrow \begin{matrix} x=0 \to 1 \\ x=1 \to 1 \end{matrix} \Rightarrow \checkmark$

$x^4+x^2+x \Rightarrow \begin{matrix} x=0 \to 0 \\ x=1 \to 1 \end{matrix} \Rightarrow \times$

$x^4+x^2+1 \Rightarrow \begin{matrix} x=0 \to 1 \\ x=1 \to 1 \end{matrix}$ but $\equiv (x^2+x+1)^2 \Rightarrow \times$

$x^4+x+1 \Rightarrow \begin{matrix} x=0 \to 1 \\ x=1 \to 1 \end{matrix} \Rightarrow \checkmark$

$x^4+x^3 \Rightarrow \begin{matrix} x=0 \to 0 \\ x=1 \to 0 \end{matrix} \Rightarrow \times$

$x^4+x^2 \Rightarrow \begin{matrix} x=0 \to 0 \\ x=1 \to 0 \end{matrix} \Rightarrow \times$

$x^4+x \Rightarrow \begin{matrix} x=0 \to 0 \\ x=1 \to 0 \end{matrix} \Rightarrow \times$

$x^4+1 \Rightarrow \begin{matrix} x=0 \to 1 \\ x=1 \to 0 \end{matrix} \Rightarrow \times$

$\Rightarrow$ irreducable polynomials:

[1] $x^4+x^3+x^2+x+1$

[2] x^4+x^3+1

[3] x^4+x+1

*

Scanned by CamScanner

$P(x) = x^3 + x + 1$

	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$