EXAMPLE OF USING SIMPLIFIED DES*

Input:

1	0	1	0	0	1	0	1

Key:

0	0	1	0	0	1	0	1	1	1

Generating KEY1

Original key :

0	0	1	0	0	1	0	1	1	1

After applying (A):

1	0	0	0	0	1	0	1	1	1

After applying (B):

0	0	0	0	1	0	1	1	1	1

After applying (C):

KEY1

0	0	1	0	1	1	1	1

Generating KEY2

Original key :

0	0	1	0	0	1	0	1	1	1

After applying (A):

1	0	0	0	0	1	0	1	1	1

After applying (B):

0	0	0	0	1	0	1	1	1	1

After applying (D):

0	0	1	0	0	1	1	1	0	1

After applying (C):

KEY2

1	1	1	0	1	0	1	0

ENCRYPTION

Original input:

1	0	1	0	0	1	0	1

---

(1) Apply IP:

0	1	1	1	0	1	0	0

---

(2) Apply F_{Key1}:

F_{Key1}(0 1 1 1 0 1 0 0) = ((0 1 1 1) **XOR** f(0 1 0 0, Key1), (0 1 0 0))

To compute f(0 1 0 0 , Key1):

(A) Apply E/P:

0	0	1	0	1	0	0	0

(B) Add Key1:

0	0	0	0	0	1	1	1

(C) Pass left 4 bits through S0 and right four bits through S1:

0	1	1	1

(D) Apply P4:

1	1	1	0

F_{Key1}(0 1 1 1 0 1 0 0) = ((0 1 1 1) **XOR** (1 1 1 0) , (0 1 0 0)) =

1	0	0	1	0	1	0	0

---

(3) Apply SW:

0	1	0	0	1	0	0	1

---

(4) Apply F_{Key2}:

F_{Key2}(0 1 0 0 1 0 0 1) = ((0 1 0 0) **XOR** f(1 0 0 1 , Key2), (1 0 0 1))

To compute f(1 0 0 1 , Key2):

(A) Apply E/P:

1	1	0	0	0	0	1	1

(B) Add Key2:

0	0	1	0	1	0	0	1

(C) Pass left 4 bits through S0 and right four bits through S1:

0	0	1	0

(D) Apply P4:

0	0	1	0

F_{Key2}(0 1 0 0 1 0 0 1) = ((0 1 0 0) **XOR** (0 0 1 0) , (1 0 0 1)) =

0	1	1	0	1	0	0	1

---

(5) Apply IP^{-1}:

0	0	1	1	0	1	1	0

*Example by Laura Sanchis, Colgate University.
