EXAMPLE OF USING SIMPLIFIED DES*

Input:



Key:



Generating KEY1

Original key:



After applying (A):

After applying (B):

				н
1	1	1	1 1	l

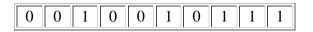
After applying (C):

KEY1



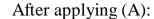
Generating KEY2

Original key:

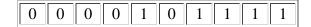


1 of 4 9/19/2010 12:07 PM

9/19/2010 12:07 PM



After applying (B):

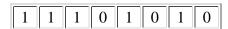


After applying (D):



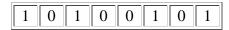
After applying (C):

KEY2



ENCRYPTION

Original input:



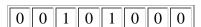
(1) Apply IP:

(2) Apply F_{Key1}:

$$F_{Key1}(0\ 1\ 1\ 1\ 0\ 1\ 0\ 0) = ((0\ 1\ 1\ 1)\ \textbf{XOR}\ \ f(0\ 1\ 0\ 0,\ Key1),\ (0\ 1\ 0\ 0))$$

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

(A) Apply E/P:



(B) Add Key1:

0 0 0 0 1 1 1

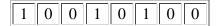
2 of 4

(C) Pass le	t 4	bits	through	S0	and	right	four	bits	through	ı S	1:
-------------	-----	------	---------	----	-----	-------	------	------	---------	-----	----

0 1 1 1

(D) Apply P4:

$$F_{\text{Key1}}(0\ 1\ 1\ 1\ 0\ 1\ 0\ 0) = ((0\ 1\ 1\ 1)\ \textbf{XOR}\ (1\ 1\ 1\ 0)\ , (0\ 1\ 0\ 0)) =$$



(3) Apply SW:



(4) Apply F_{Key2}:

$$F_{\text{Kev2}}(0\ 1\ 0\ 0\ 1\ 0\ 0\ 1) = ((0\ 1\ 0\ 0)\ \textbf{XOR}\ f(1\ 0\ 0\ 1\ ,\ \text{Key2}), (1\ 0\ 0\ 1))$$

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

(A) Apply E/P:

(B) Add Key2:

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

(D) Apply P4:

$$F_{\text{Kev2}}(0\ 1\ 0\ 0\ 1\ 0\ 0\ 1) = ((0\ 1\ 0\ 0)\ \textbf{XOR}\ (0\ 0\ 1\ 0)\ , (1\ 0\ 0\ 1)) =$$



(5) Apply IP^{-1} :



*Example by Laura Sanchis, Colgate University.

4 of 4