TRABALHO PRÁTICO 2 DE SISTEMAS EMBARCADOS

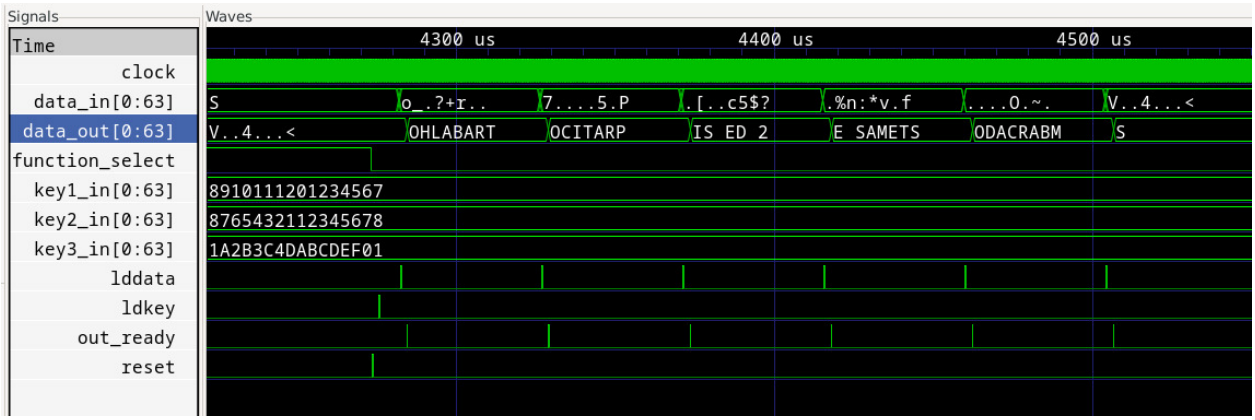
GUILHERME MARTINS SPECHT

O código implementa um driver que realiza a criptografia e descriptografia de uma mensagem (“TRABALHO PRATICO 2 DE SISTEMAS EMBARCADOS”) utilizando os três modos ECB, CBC e CTR através de um módulo 3DES, junto de um *wrapper* dentro do *testbench* do arquivo VHDL presente no trabalho. As imagens abaixo mostram a execução tanto no *debug.txt* quanto na *waveform* do GTKWave.

```
bootUCX/OS v0.97 boot on RV32E (HF-RISCV-E)
heap_init(), 17748 bytes free
task 0: 0x40000648, stack: 0x40003368, size 2048

====== Teste Completo do Driver 3DES ======
Mensagem Original: TRABALHO PRATICO 2 DE SISTEMAS EMBARCADOS

40003B30 54 52 41 42 41 4C 48 4F  20 50 52 41 54 49 43 4F  |TRABALHO PRA
TICO|
40003B40 20 32 20 44 45 20 53 49  53 54 45 4D 41 53 20 45  | 2 DE SISTEM
AS E|
40003B50 4D 42 41 52 43 41 44 4F  53 00 00 40 00 00 00 00  |MBARCADOS..@
....|

====== Testando Modo: ECB ======

Dados Criptografados (hexdump):

40003A30                                    19 EA 72 2B  |0...;.@...@
..r+|
40003A40 3F D6 5F 6F 50 9B 35 06  A3 15 06 37 3F 24 35 63  |?._oP.5....7
?$5c|
40003A50 FD 01 5B 13 66 1D 76 2A  3A 6E 25 F6 03 7E A1 4F  |..[.f.v*:n%.
.~.O|

Dados Descriptografados:

40003A30                                    54 52 41 42  |0...;.@...@
TRAB|
40003A40 41 4C 48 4F 20 50 52 41  54 49 43 4F 20 32 20 44  |ALHO PRATICO
 2 D|
40003A50 45 20 53 49 53 54 45 4D  41 53 20 45 4D 42 41 52  |E SISTEMAS E
MBAR|

Dados Descriptografados: "TRABALHO PRATICO 2 DE SISTEMAS EMBARCADOS"
Verificacao: SUCESSO!
```

```
====== Testando Modo: CBC ======

Dados Criptografados (hexdump):

40003A30                                        BE 97 44 E6  |0...,;.@...@
..D.|
40003A40 0C 80 46 14 A2 15 7D 60  6A BF 31 7A C0 84 22 B8  |..F...}`j.1z
.."."|
40003A50 64 A8 5B 1E 15 8F 99 48  20 78 CC 76 D2 96 6D EE  |d.[....H x.v
..m.|

Dados Descriptografados:

40003A30                                        54 52 41 42  |0...,;.@...@
TRAB|
40003A40 41 4C 48 4F 20 50 52 41  54 49 43 4F 20 32 20 44  |ALHO PRATICO
 2 D|
40003A50 45 20 53 49 53 54 45 4D  41 53 20 45 4D 42 41 52  |E SISTEMAS E
MBAR|

Dados Descriptografados: "TRABALHO PRATICO 2 DE SISTEMAS EMBARCADOS"
Verificacao: SUCESSO!
```

```
====== Testando Modo: CTR ======

Dados Criptografados (hexdump):

40003A80 69 66 BE D7 C5 9E 37 A8  CB 48 79 A1 21 22 F2 91  |if....7..Hy.
!"..|
40003A90 10 4D 17 8B 73 95 78 03  F8 3B 1A DA 7E 0A 2A AE  |.M..s.x..;..
~.*.|
40003AA0 5B 4F FA FB 5E 2A 26 57  09 51 48 4F 20 50 52 41  |[O..^*&W.QHO
 PRA|

Dados Descriptografados:

40003A80 54 52 41 42 41 4C 48 4F  20 50 52 41 54 49 43 4F  |TRABALHO PRA
TICO|
40003A90 20 32 20 44 45 20 53 49  53 54 45 4D 41 53 20 45  | 2 DE SISTEM
AS E|
40003AA0 4D 42 41 52 43 41 44 4F  53 00 48 4F 54 52 41 42  |MBARCADOS.HO
TRAB|

Dados Descriptografados: "TRABALHO PRATICO 2 DE SISTEMAS EMBARCADOS"
Verificacao: SUCESSO!

====== Todos os testes foram finalizados. ======

*** HALT (0) - no error
```


Signals
Waves
Time
clock
data_in[0:63]
data_out[0:63]
function_select
key1_in[0:63]
key2_in[0:63]
key3_in[0:63]
lddata
ldkey
out_ready
reset
4300 us
4400 us
4500 us
S
o_.?+r..
7....5.P
.[..c5$?
.%n:*v.f
....O.~.
V..4...<
V..4...<
OHLABART
OCITARP
IS ED 2
E SAMETS
ODACRABM
S
8910111201234567
8765432112345678
1A2B3C4DABCDEF01