

# CPEN 311 Lab 4

Zihao Pu  
47060645

# Task 1: Filling memory

In-System Memory Content Editor - C:/Users/John/OneDrive/UBC/Year 3 Term 2/CPEN 311/Labs/Lab 4/template\_de1soc/rc4 - rc4

File Edit View Processing Tools Window Help

Search altera.com

Instance Manager: Ready to acquire

Index	Instance ID	Status	Width	Depth	Type
0	S	Not running	8	256	RAM/ROM

JTAG Chain Configuration: JTAG ready

Hardware: DE-SoC [USB-1] Setup...

Device: @2: 5CSE(BA5|MA5)/5CS Scan Chain

File: ...

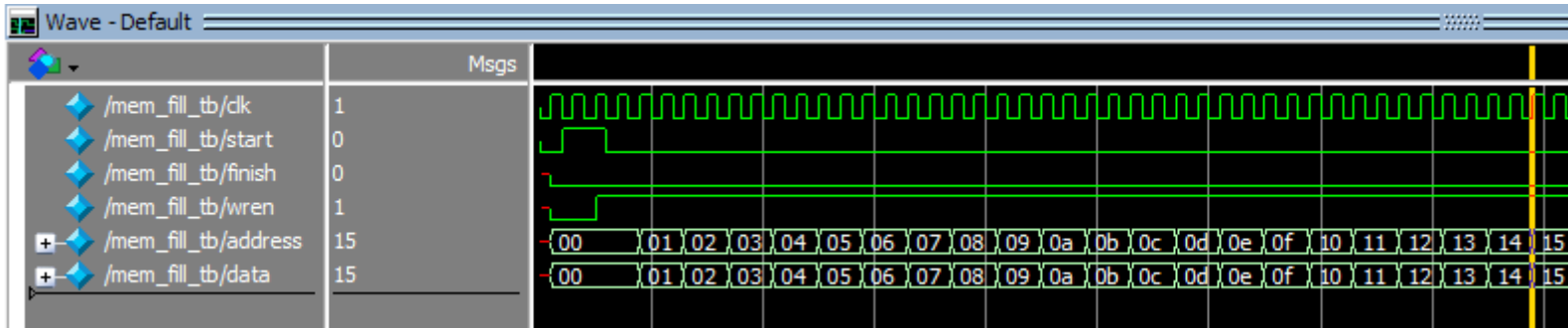
Instance 0: S

```
000000 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 .....
00001a 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 ..... !"#$%&'()*+,-./0123
000034 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 456789:;<=>?@ABCDEFGHIJKLM
00004e 4E 4F 50 51 52 53 54 55 56 57 58 59 5A 5B 5C 5D 5E 5F 60 61 62 63 64 65 66 67 NOPQRSTUVWXYZ[\]^_`abcdefg
000068 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79 7A 7B 7C 7D 7E 7F 80 81 hijklmnopqrstuvwxyz{|}~...
000082 82 83 84 85 86 87 88 89 8A 8B 8C 8D 8E 8F 90 91 92 93 94 95 96 97 98 99 9A 9B .....
00009c 9C 9D 9E 9F A0 A1 A2 A3 A4 A5 A6 A7 A8 A9 AA AB AC AD AE AF B0 B1 B2 B3 B4 B5 .....
0000b6 B6 B7 B8 B9 BA BB BC BD BE BF C0 C1 C2 C3 C4 C5 C6 C7 C8 C9 CA CB CC CD CE CF .....
0000d0 D0 D1 D2 D3 D4 D5 D6 D7 D8 D9 DA DB DC DD DE DF E0 E1 E2 E3 E4 E5 E6 E7 E8 E9 .....
0000ea EA EB EC ED EE EF F0 F1 F2 F3 F4 F5 F6 F7 F8 F9 FA FB FC FD FE FF .....
```

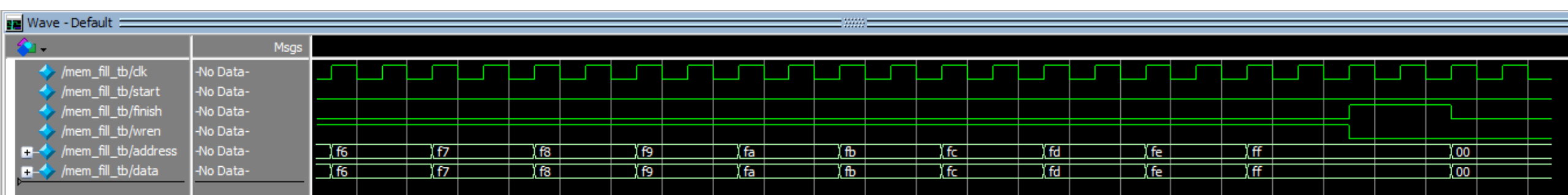
0% 00:00:00 Instance: Word: Bit

# Task 1 Simulation

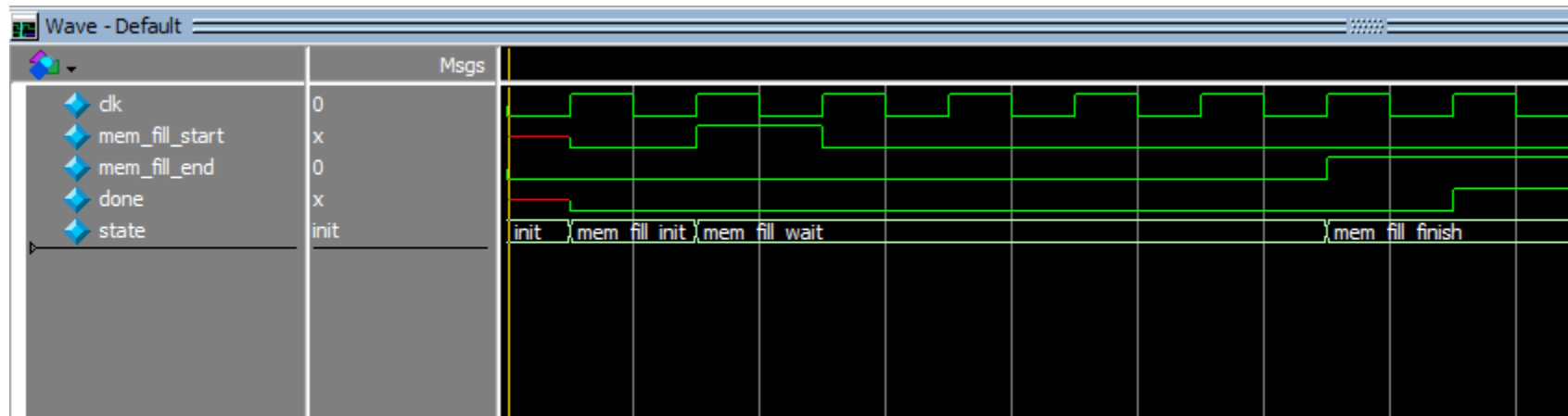
At start:



At end:



# Task 1 – Control FSM



The FSM is done, but the control logic does not work very well. The following tasks are done by 1 massive FSM.

# Task 2a

Same as expected

In-System Memory Content Editor - C:/Users/John/OneDrive/UBC/Year 3 Term 2/CPEN 311/Labs/Lab 4/lab4/rc...

File Edit View Processing Tools Window Help

Search altera.com

Instance Manager: Ready to acquire

Index	Instance ID	Status	Width	Depth	Type
0	S	Not runni...	8	256	RAM/ROM
1	D	Not runni...	8	32	RAM/ROM
2	E	Not runni...	8	32	RAM/ROM

JTAG Chain Configuration: JTAG ready

Hardware: DE-SoC [USB-1] Setup...

Device: @2: 5CSE(BA5|MA5)/5CS Scan Chain

File: ...

Instance 0: S

000000	3A A8 4E 08 55 A3 B8 40 93 0C 44 24 A6 89 26 EA 72 66 61 5A	:.N.U..@..D\$.&.rfaz
000014	DA EF B2 9E 1F 02 15 3D 01 8E AC CD 4A 57 7B 9B 2C 32 49 C8	.....=.....JW{.,2I.
000028	79 30 64 11 CC 7E 81 CE 9D 5C 46 FA 65 B1 52 2F 74 C4 AB 88	y0d..~... \F.e.R/t...
00003c	C0 FF 86 F4 16 91 3F 0B A5 0F CA 90 37 F3 E8 BE 8F 67 09 5F	.....?.....7....g._
000050	AD A4 EE BF A1 8A F2 EC A0 5E 1E 96 45 C2 3B 28 2B 68 ED 36	.....^..E.;(+h.6
000064	E5 92 9A B3 DB 77 6A D4 A2 56 27 1B EB 54 98 84 25 BC 34 FB	.....wj..V'..T.%.4.
000078	42 F0 17 D0 D2 13 51 4C 33 C3 1A 31 F6 60 82 10 E1 73 41 D8	B.....QL3..1. ....sA.
00008c	4B 3C DF AA 5D 9C 05 D6 0A 19 C9 0E FC 06 6D F5 99 58 29 B6	K<..].....m..X).
0000a0	4D C7 53 C1 C6 48 07 8D 59 7A B7 00 7D B5 CF 14 DD 3E DE D7	M.S..H..Yz..}.....>..
0000b4	BB 22 62 2D A9 03 39 50 21 20 76 7C E0 D9 95 AE BD 6E 1C 12	."b-...9P! v .....n..
0000c8	D3 70 38 AF F7 43 F9 6B D5 1D 71 8C 83 23 F8 7F 9F FD 2A DC	.p8..C.k..q..#....*.
0000dc	69 97 FE 8B B9 0D 2E E3 85 87 E2 B0 63 D1 B4 94 78 BA E9 E4	i.....c...x...
0000f0	E6 18 CB 04 C5 E7 A7 6C 4F 6F 47 80 35 5B 75 F1	.....lOoG.5[u.

Instance 1: D

000000	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
000014	00 00 00 00 00 00 00 00 00 00 00 00	.....

Instance 2: E

000000	C5 AF B0 4D 4E FD A5 58 2C 54 10 D6 4F D0 86 B8 05 57 42 10	...MN..X,T..O....WB.
000014	1C E9 27 36 35 04 C6 E7 A7 1D C4 E8	..'65.....

0% 00:00:00 Instance: Word: Bit:

# Task 2b

In-System Memory Content Editor - C:/Users/John/OneDrive/UBC/Year 3 Term 2/CPEN 311/Labs/Lab 4/lab4/rc4 - rc4

File Edit View Processing Tools Window Help

Search altera.com

Instance Manager: Ready to acquire

Index	Instance ID	Status	Width	Depth	Type	Mode
0	S	Not runni...	8	256	RAM/ROM	Read/Write
1	D	Not runni...	8	32	RAM/ROM	Read/Write
2	E	Not runni...	8	32	RAM/ROM	Read/Write

JTAG Chain Configuration: JTAG ready

Hardware: DE-SoC [USB-1] Setup...

Device: @2: 5CSE(BA5|MA5)/5CS Scan Chain

File: ...

Instance 0: S

```
000000 3A 02 A7 75 BF 4E CF E9 C3 3C 1D E7 66 2C E8 65 07 F5 56 12 C7 5D 15 B9 :..u.N...<..f,.e..V..]..
000018 F1 59 3F 55 A1 2E DF 96 48 57 7B 9B 89 32 49 C8 79 30 64 11 CC 7E 81 CE .Y?U....HW{...2I.y0d..~..
000030 9D 5C 46 FA EA B1 52 2F 74 C4 AB 88 C0 FF 86 F4 16 91 B2 0B A5 0F CA 90 .\F...R/t.....
000048 37 F3 26 BE 8F 67 09 5F AD A4 EE 3D 01 8A F2 EC A0 5E 1E CD 45 C2 3B 28 7.&..g._...=.....^..E.;(
000060 2B 68 ED 36 E5 92 9A B3 DB 77 6A D4 A2 61 27 1B EB 54 98 84 25 BC 34 FB +h.6.....wj..a'..T..%.4.
000078 42 F0 17 D0 D2 13 51 4C 33 93 1A 31 F6 60 82 10 E1 73 41 D8 4B 0C AC AA B.....QL3..1.`....sA.K...
000090 EF 9C 05 D6 0A 19 C9 0E FC 06 6D A6 99 58 29 B6 4D DA 53 C1 C6 4A 72 8D .....m..X).M.S..Jr.
0000a8 A8 7A B7 00 7D B5 B8 14 DD 3E DE D7 BB 22 62 2D A9 03 39 50 21 20 76 7C .z..)....>..."b--.9P! v|
0000c0 E0 D9 95 AE BD 6E 1C 5A D3 70 38 AF F7 43 F9 6B D5 44 71 8C 83 23 F8 7F .....n.Z.p8..C.k.Dq..#..
0000d8 9F FD 2A DC 69 97 FE 8B 9E 0D 8E E3 85 87 E2 B0 63 D1 B4 94 78 BA 40 E4 ..*.i.....c...x.@.
0000f0 E6 18 CB 04 C5 24 A3 6C 4F 6F 47 80 35 5B 08 1F .....$.10oG.5[...
```

Instance 1: D

```
000000 74 68 69 73 20 63 6F 75 72 73 65 20 69 73 20 6D 79 20 66 61 76 6F 75 72 this course is my favour
000018 69 74 65 20 20 20 20 20
```

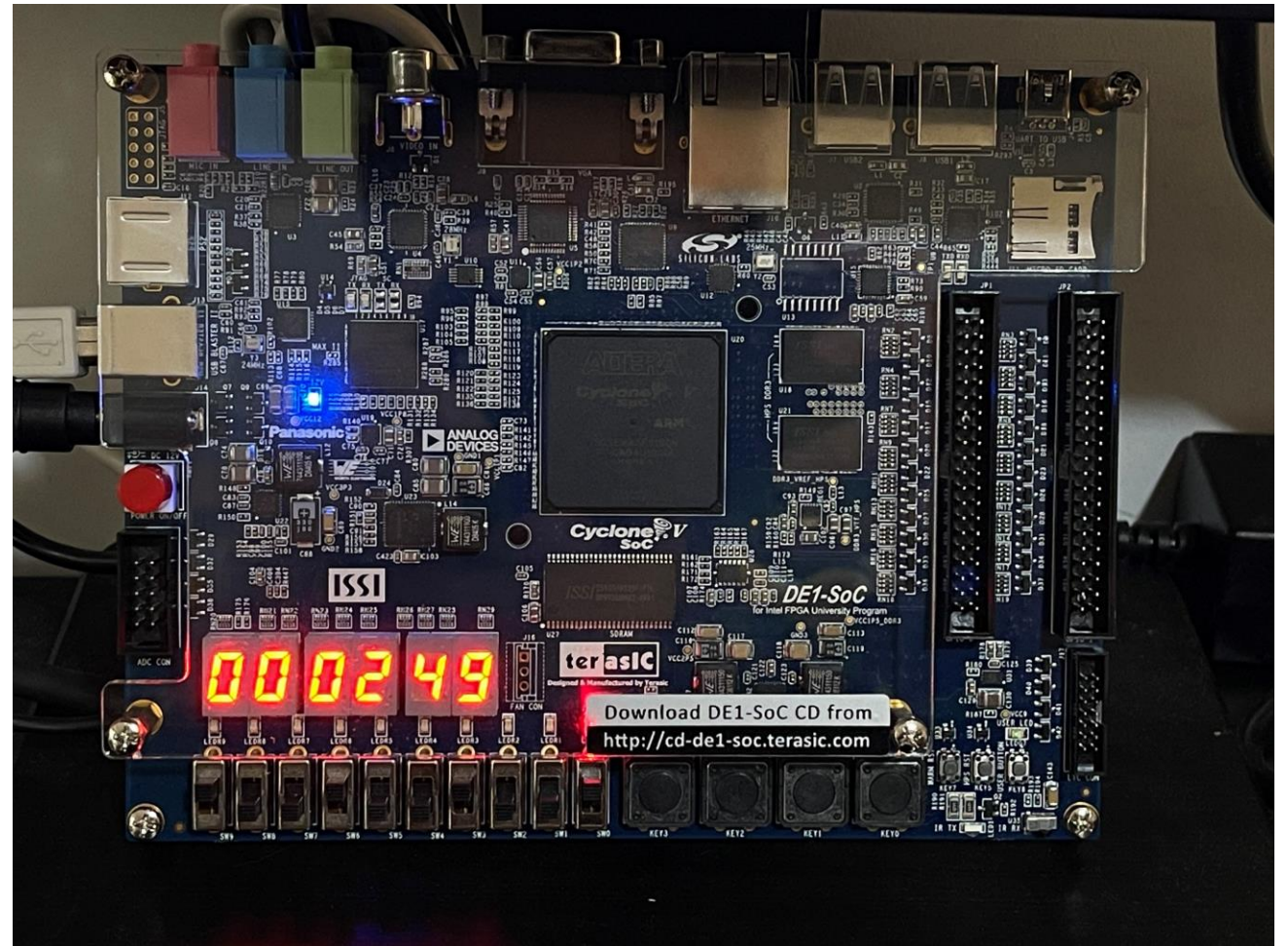
Instance 2: E

```
000000 2D 8F 7A A9 38 73 5F 87 45 1B 82 86 4B 9B 7F 9D EF 0D C4 BB F9 77 99 75 -.z.8s_.E...K.....w.u
000018 FF D5 60 73 01 F8 16 25 ..`s...%
```

0% 00:00:00 Instance: Word: Bit:

## Task 3

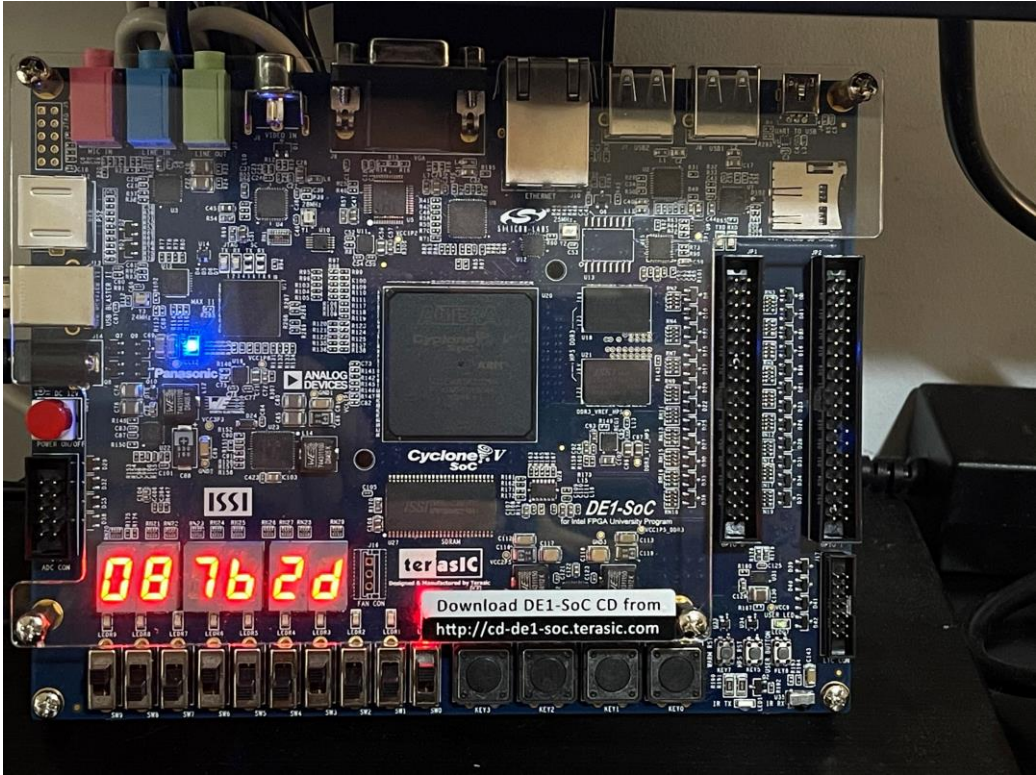
A test on message used for task 2a. The cracked code is exactly same as known one.





# Task 3

## Secret Key



## Result

In-System Memory Content Editor - C:/Users/John/OneDrive/UBC/Year 3 Term 2/CPEN 311/Labs/Lab 4/lab4/rc4 - rc4

File Edit View Processing Tools Window Help

Search altera.com

Instance Manager: Ready to acquire

Index	Instance ID	Status	Width	Depth	Type	Mode
0	S	Not runni...	8	256	RAM/ROM	Read/Write
1	D	Not runni...	8	32	RAM/ROM	Read/Write
2	E	Not runni...	8	32	RAM/ROM	Read/Write

JTAG Chain Configuration: JTAG ready

Hardware: DE-SoC [USB-1] Setup...

Device: @2: 5CSE(BA5)MA5/5CS Scan Chain

File: ...

Instance 0: S

000000	08 84 88 8F 2F FB EA BC 78 EF CB E8 58 B1 63 04 26 6E CD 95 5F CE 0D 4B	.../...x...X.c.&n...K
000018	B3 27 11 9E 52 C0 D1 9B 23 93 16 AC D8 2A C2 0B 6C F3 90 1E 66 2D D6 B6	'..R...#...*.l...E-..
000030	C8 46 13 AD 22 03 FC 74 B2 09 ED 44 15 54 7F 65 99 47 31 D4 4D 91 5C 20	.F..."...t...D.T.e.Gl.M.\
000048	D0 80 12 A7 19 67 4A 6D 76 81 DB 33 E6 9A A5 6B 9D 2E 57 87 05 43 73 BD	.....gJmv...3...k...W..Cs.
000060	83 A8 E2 8B 3A 8C 64 5B 1C F4 21 06 2B 02 3F B7 1D A0 69 AA 68 56 0E E7	.....d[...!...+?...i.hV..
000078	7A EC 3B 00 F9 C3 53 AF 14 F1 EE 6F 01 3E 92 CF 48 F6 E4 F5 35 1A BE CA	z...;...S...o...?..H...5...
000090	2C C7 37 BF 6A 7C 25 B5 9F 5E FF 18 30 F8 32 62 DD A3 E9 24 DE E5 B0 F7	..7..j %.^..0.2b...\$....
0000a8	40 A2 5D 71 29 97 C5 4F 0C 55 0A 34 FA 5A 86 59 D3 B9 60 D7 C4 61 E0 C1	@.jq)...O.U.4.Z.Y...'.a...
0000c0	C9 7E 3C 72 DF 41 77 10 D2 F0 A4 50 70 FE B8 07 0F 82 94 BA 36 E3 DA 79	..<r.Aw....Fp.....6...y
0000d8	AE 42 B4 E1 75 7B 4E BB A1 A9 3D 51 AB 38 96 D5 17 DC 89 EB 85 39 8E 49	..B...u{N...=Q.8.....9..I
0000f0	8A A6 1F 8D 98 D9 1B 4C 9C C6 45 CC 7D F2 28 FD	.....L..E..).(.)

Instance 1: D

000000	72 63 20 66 6F 75 72 20 69 73 20 6E 6F 74 20 76 65 72 79 20 73 65 63 75	rc four is not very secu
000018	72 65 20 20 20 20 20 20	re

Instance 2: E

000000	C5 AF B0 4D 4E FD A5 58 2C 54 10 D6 4F D0 86 B8 05 57 42 10 1C E9 27 36	...MN...X,T..O...WB...*6
000018	35 04 C6 E7 A7 1D C4 E8	5.....

0% 00:00:00 Instance: Word: Bit:



# Simulation

Full FSM Simulation

# Simulation: Construct of Memories

Since the M10K memory is not accessible from ModelSim, hand-written memories are implemented as system memories.

This code here shows the code of s\_memory

```
1.  module s_memory(address, clock, data, wren, q);
2.      input wire clock;
3.      input logic [7:0] address;
4.      input logic [7:0] data;
5.      input wire wren;
6.      output logic [7:0] q;
7.
8.      reg [7:0] mem [256];
9.
10.     always_ff @( posedge clock ) begin : smem
11.         if(wren) mem[address] <= data;
12.     end
13. endmodule
```

# Simulation: Construct of Memories

Since the M10K memory is not accessible from ModelSim, hand-written memories are implemented as system memories.

This code here shows the code of d\_memory

```
1. module d_memory(address, clock, data, wren, q);
2.     input wire clock;
3.     input logic [4:0] address;
4.     input logic [7:0] data;
5.     input wire wren;
6.     output logic [7:0] q;
7.     reg [7:0] mem [32];
8.     always_ff @( posedge clock ) begin : dmem
9.         if(wren) mem[address] <= data;
10.        q <= mem[address];
11.    end
12. endmodule
```

# Simulation: Construct of Memories

Since the M10K memory is not accessible from ModelSim, hand-written memories are implemented as system memories.

This code here shows the code of ROM for message

The message is hardcoded from MIF file.

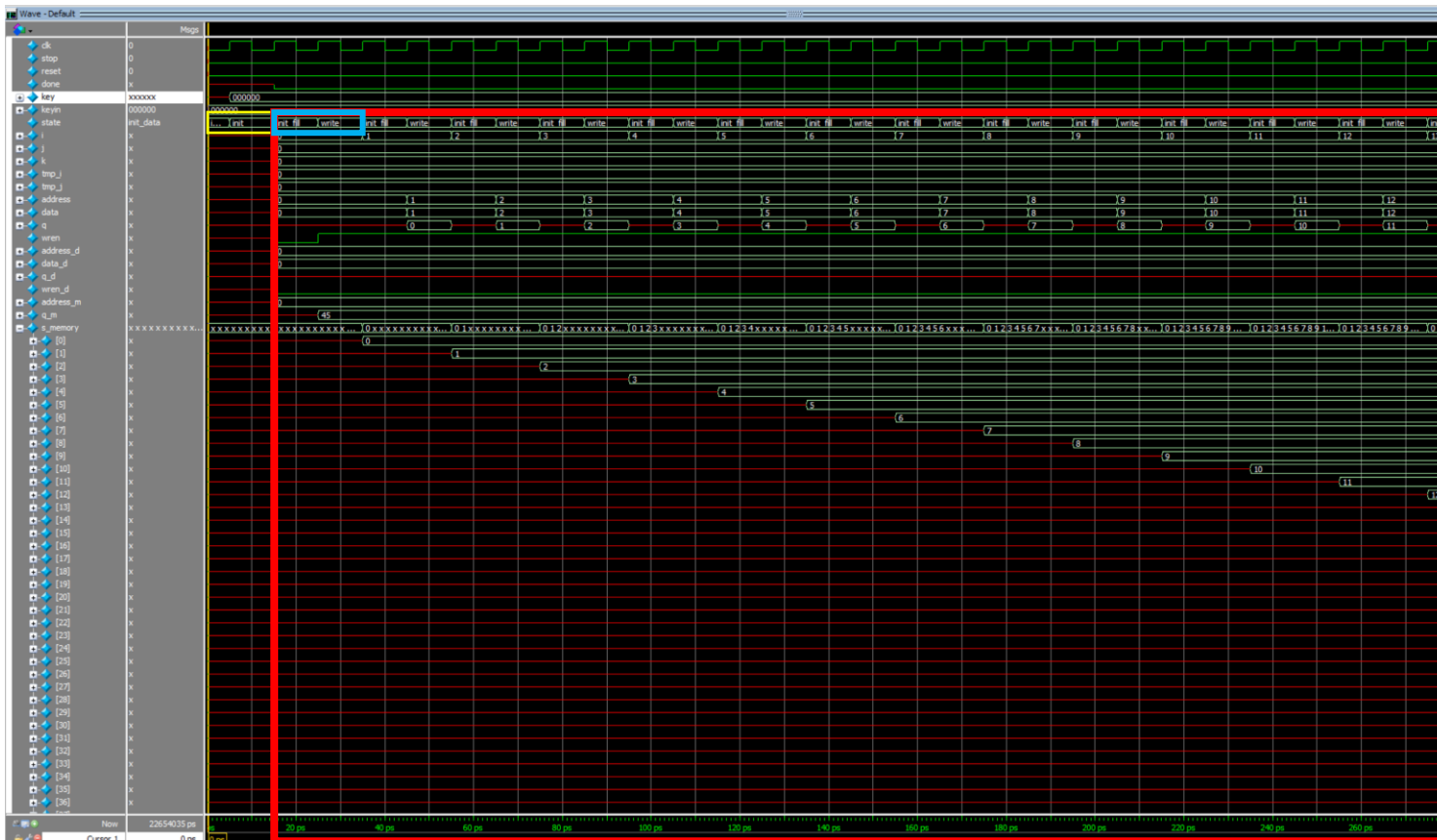
```
1.  module message(address, clock, q);
2.      input wire clock;
3.      input logic [4:0] address;
4.      output logic [7:0] q;
5.      //Message 1
6.      always_ff @( posedge clock ) begin : message
7.          case(address)
8.              0 : q<=45;
9.              1 : q<=143;
10.             2 : q<=122;
11.             3 : q<=169;
12.             4 : q<=56;
13.             5 : q<=115;
14.             6 : q<=95;
15.             7 : q<=135;
16.             8 : q<=69;
17.             9 : q<=27;
18.             10 : q<=130;
19.             11 : q<=134;
20.             12 : q<=75;
21.             13 : q<=155;
22.             14 : q<=127;
23.             15 : q<=157;
24.             16 : q<=239;
25.             17 : q<=13;
26.             18 : q<=196;
27.             19 : q<=187;
28.             20 : q<=249;
29.             21 : q<=119;
30.             22 : q<=153;
31.             23 : q<=117;
32.             24 : q<=255;
33.             25 : q<=213;
34.             26 : q<=96;
35.             27 : q<=115;
36.             28 : q<=1;
37.             29 : q<=248;
38.             30 : q<=22;
39.             31 : q<=37;
40.             default: q<=8'bx;
41.         endcase
42.     end
43. endmodule
```

# Simulation: The testbench

Since the IO of FSM is super easy, a simple implementation of testbench is written.

```
1.  module fsm_tb;
2.      logic clk, stop, reset, done;
3.      logic [23:0] key, keyin;
4.      fsm DUT(
5.          .clk(clk),
6.          .key(key),
7.          .keyin(keyin),
8.          .stop(stop),
9.          .reset(reset),
10.         .done(done)
11.     );
12.     always #5 clk = ~clk;
13.     always @(*) begin
14.         if(done) begin
15.             #100 $stop;
16.         end
17.     end
18.     initial begin
19.         #0 clk = 0; reset = 0; stop = 0; keyin <= 0;
20.     end
21. endmodule
```

# Simulation: Step1



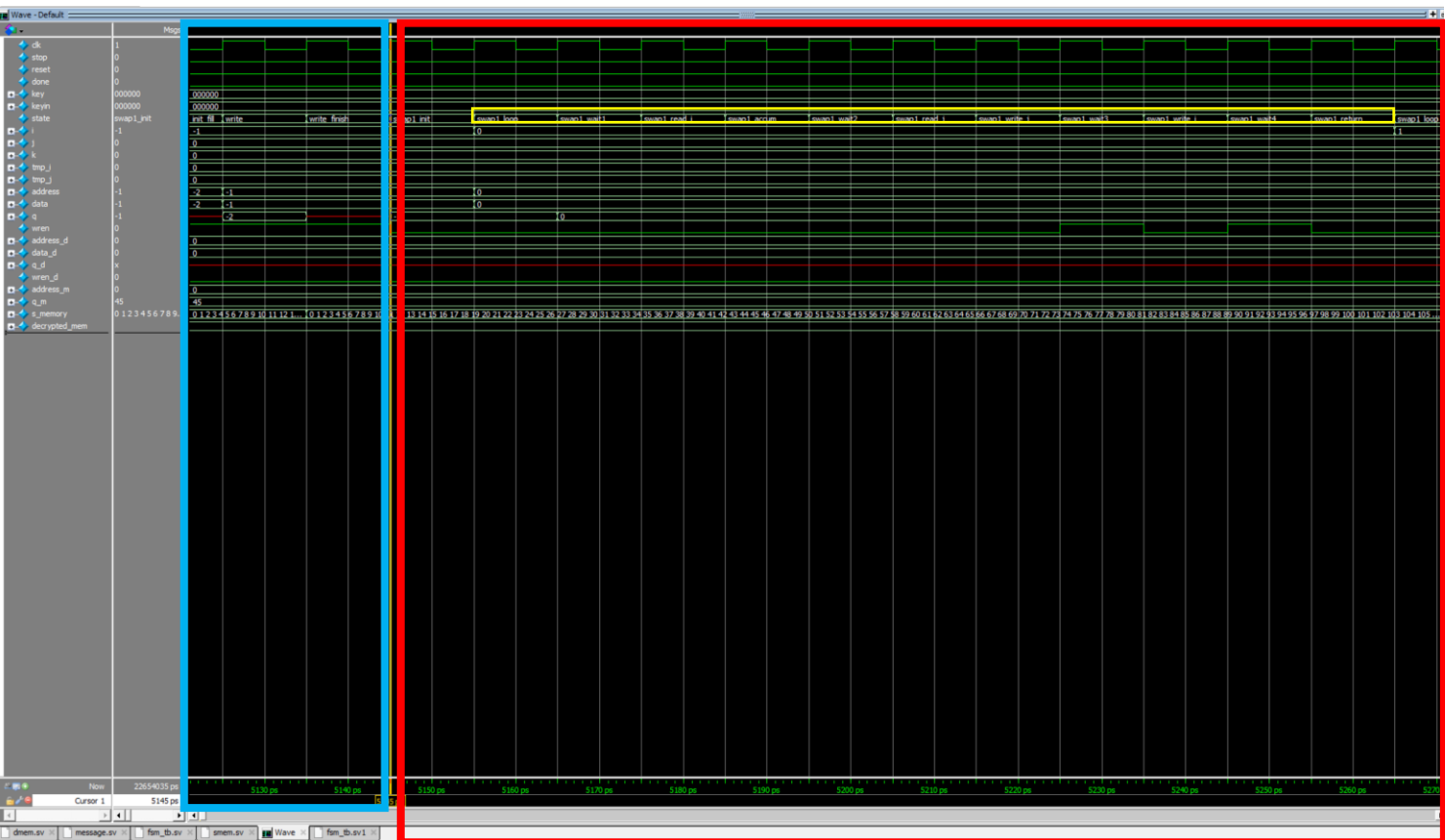
At step 1, the FSM will fill s\_memory from 0 to 255.

```
for i = 0 to 255{  
    s[i] = i;  
}
```

- Yellow box: initialization, to initialize variables
- Red box: filling mechanism
- Blue box: one filling cycle, 2 states
  - -init\_fill
  - -write



# Simulation: Step1&2

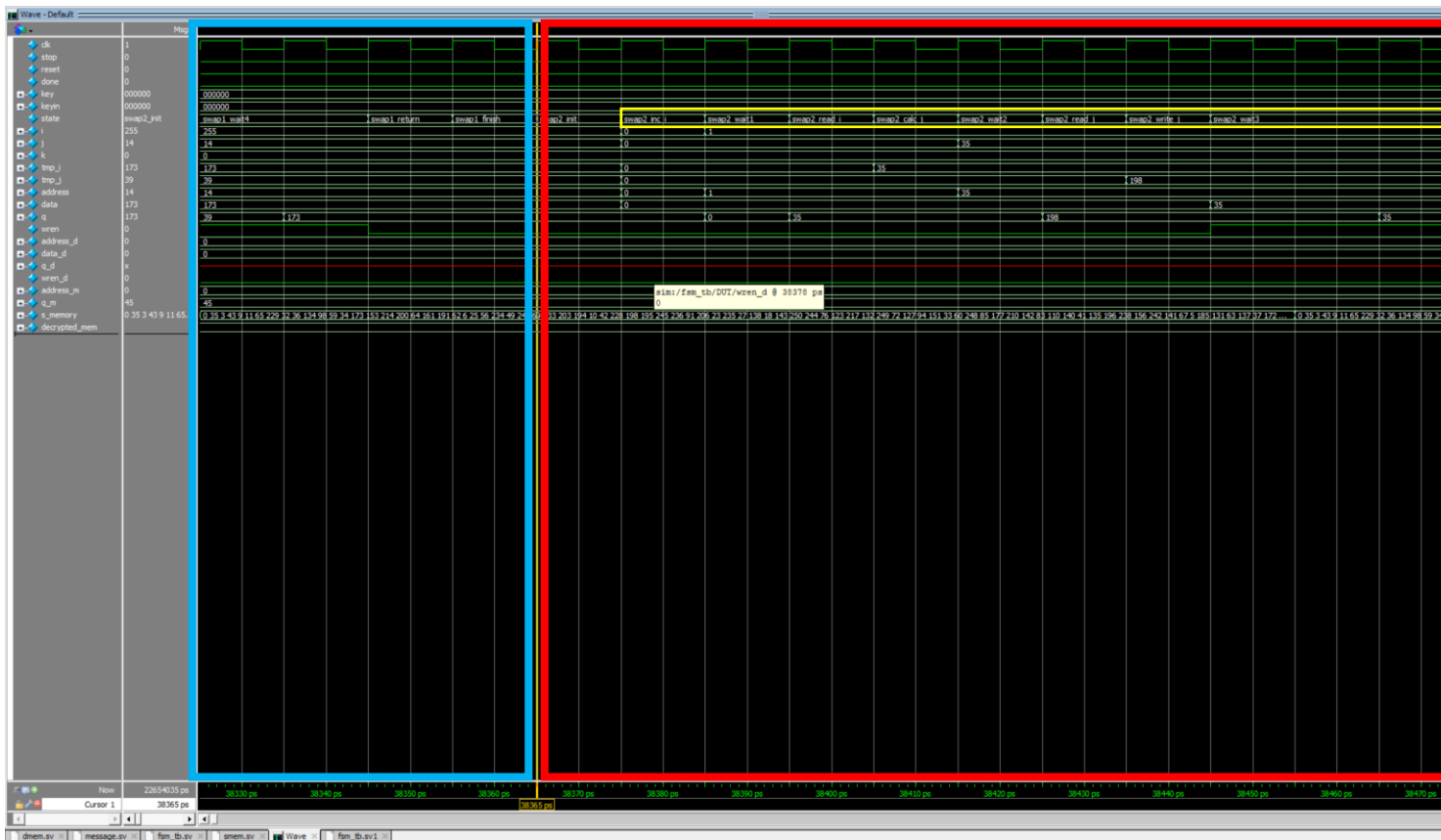


- At step 2, the FSM will swap s\_memory from 0 to 255.

```
j = 0
for i = 0 to 255{
    j = (j + s[i] + secretkey[i%3]) % 256
    swap s[i] and s[j]
}
```

- Blue box: Filling ends
- Red box: Step 2 FSM, start swapping
- Yellow box: one filling cycle, 11 states

# Simulation: Step2a&2b



- Step 2a ends at 38365ps.

$i = 0, j = 0$

```
for k = 0 to message_length-1 { //
message_length is 32 in our
implementation
```

$i = (i+1) \bmod 256$

$j = (j+s[i]) \bmod 256$

swap values of  $s[i]$  and  $s[j]$

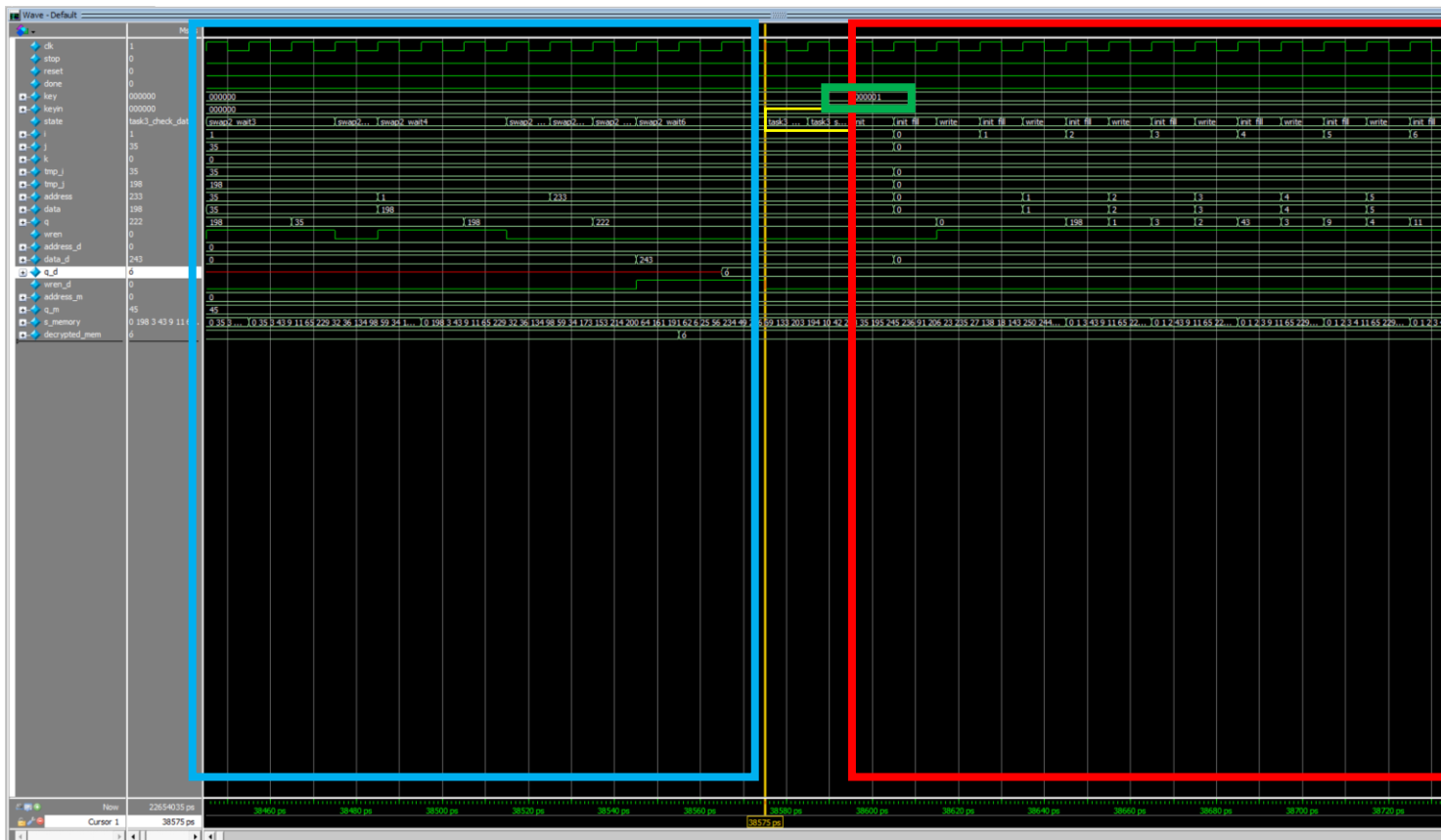
$f = s[(s[i]+s[j]) \bmod 256]$

```
decrypted_output[k] = f xor
encrypted_input[k] // 8 bit wide XOR
function
```

}

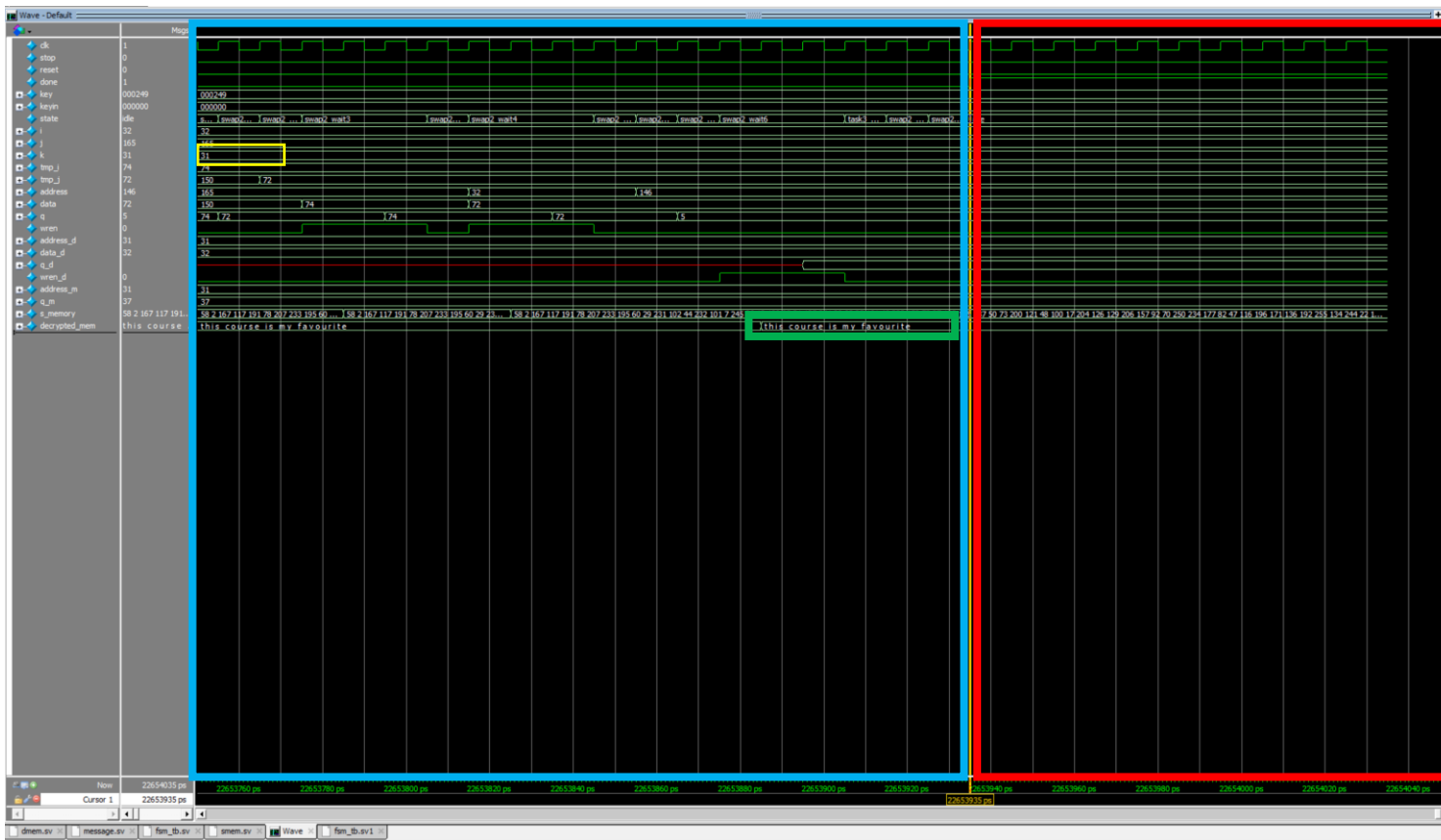
- Blue box: swap1
- Red box: swap 2 FSM, start decrypting
- Yellow box: step 2b states

# Simulation: Step2b & 3



- First Step 2b decryption ends at 38575ps. The decrypted data is not a letter.
- Blue box: swap2
- Yellow box: Step3 detect FSM
- Red box: Restart with new key
- Green box: New key in new cycle

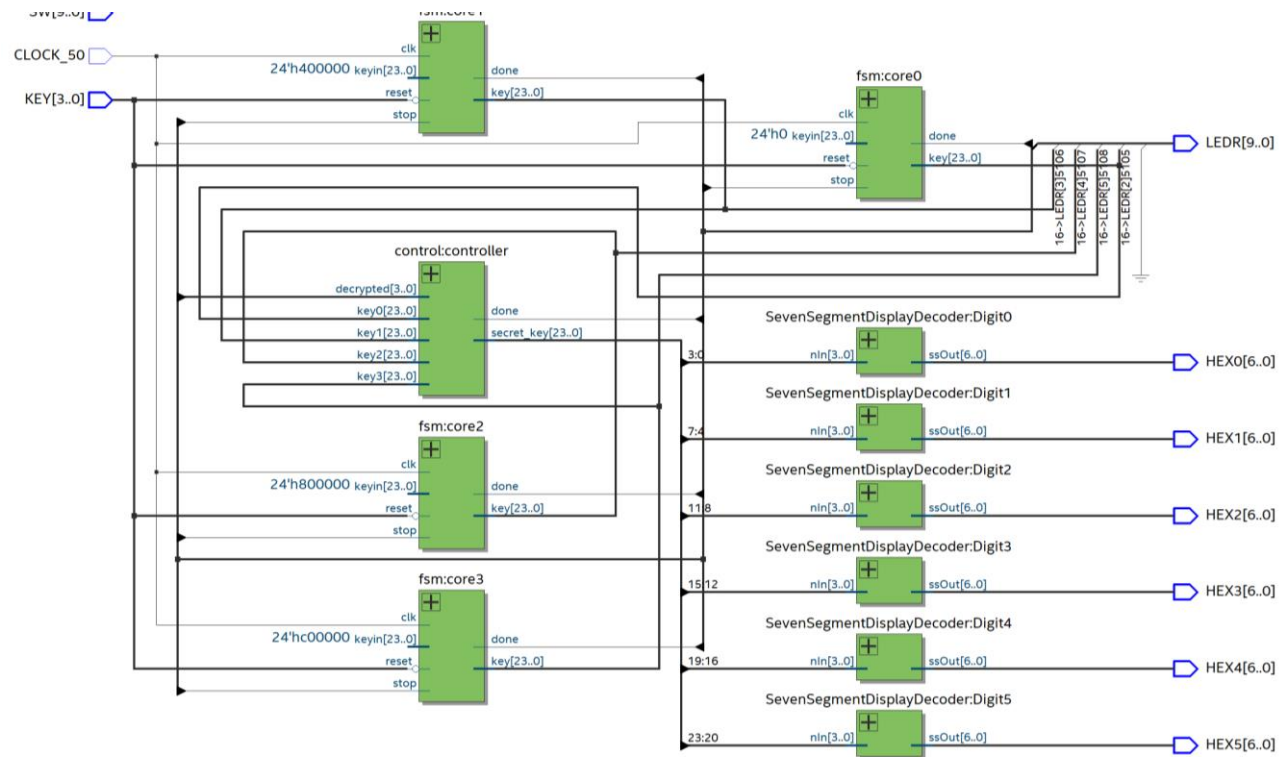
# Simulation: Step3



- When message is finally decrypted, k runs out to 31, and decrypted message is stored in decrypted\_mem.

- Blue box: swap2
- Yellow box: value of k
- Red box: Idle state
- Green box: Decrypted message

# Bonus



- Design: Run 4 cores, each one has its own memories, and each one runs different decryption range.
  - Core0: Start from 24'h0
  - Core1: Start from 24'h400000
  - Core2: Start from 24'h800000
  - Core3: Start from 24'hC00000
- Once a solution is found, stop all cores and display the result.

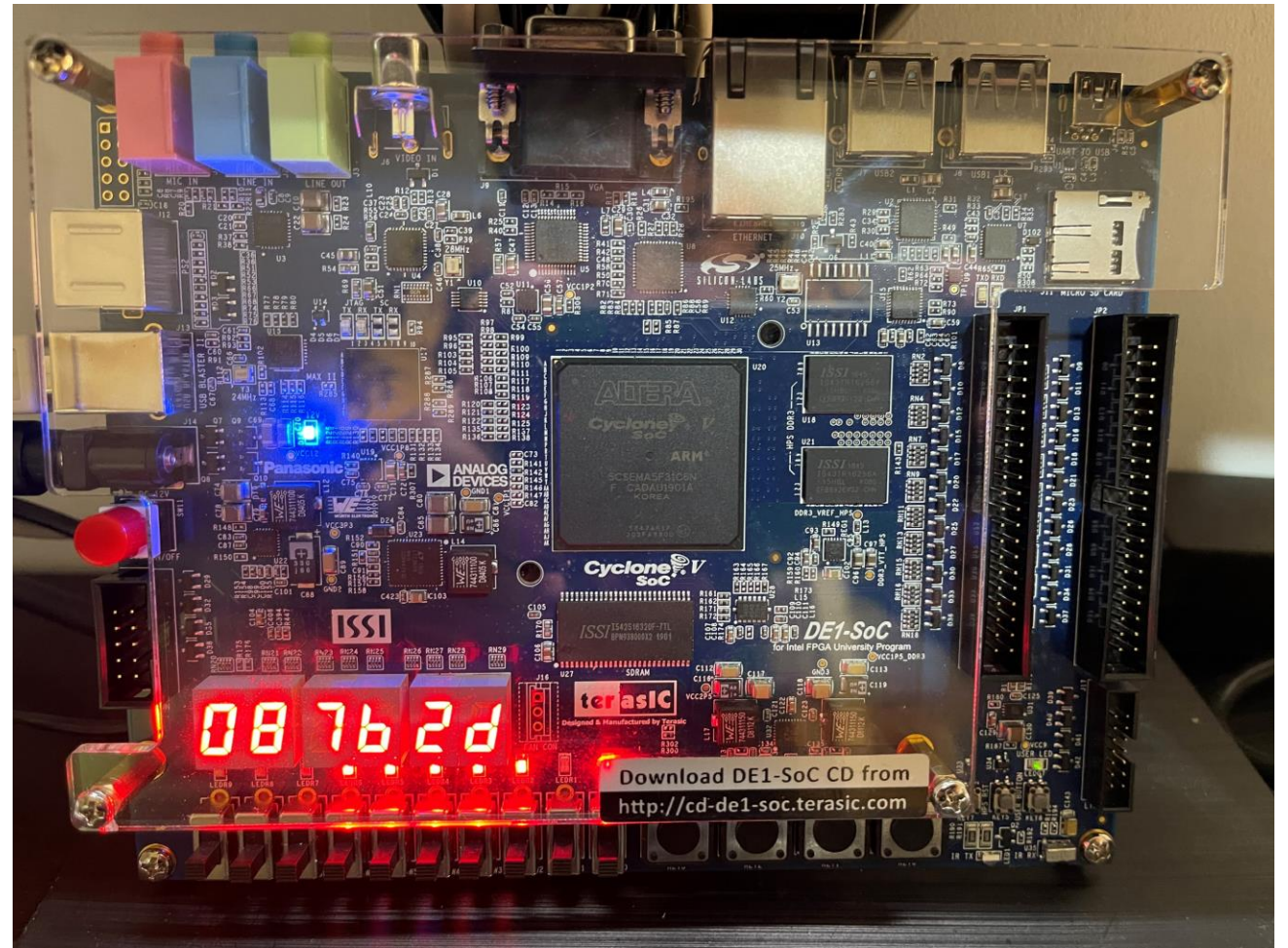
# Interface design

LED[9:6]: which core decrypted data first

LED[5:2]: toggle if running

LED[0]: on if done

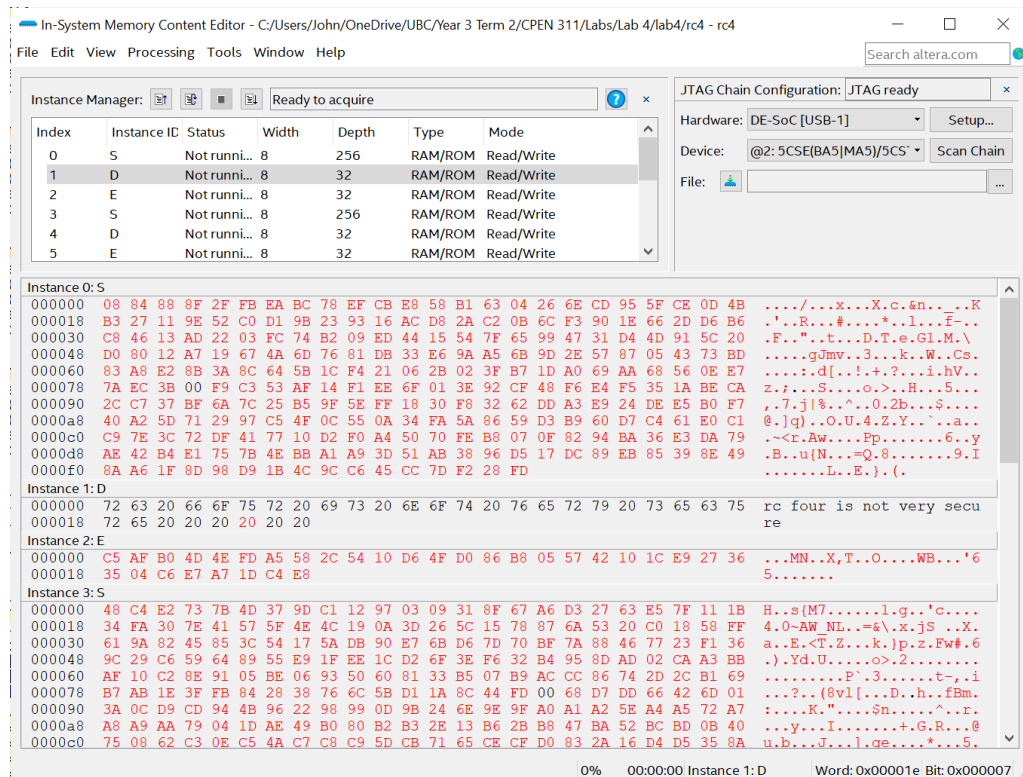
HEX: decrypted key



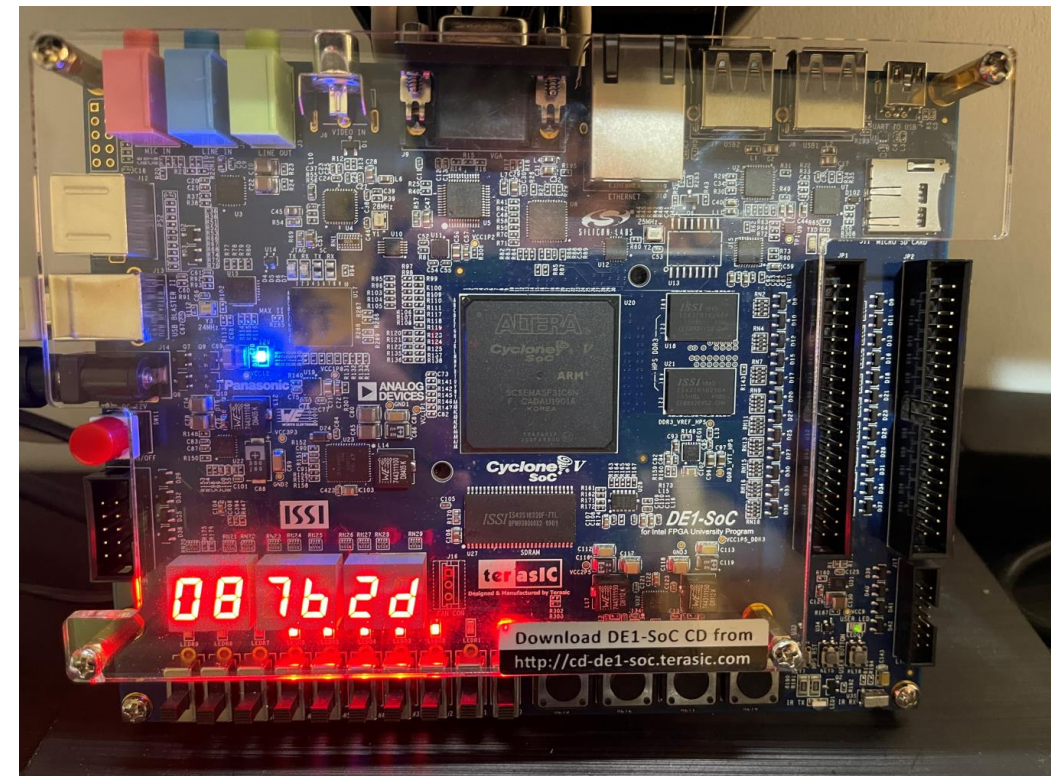


# Bonus-Example Decrypted Messages 4

## Message



## Secret Key



LED[9:6] indicate core[3:0] separately.

LED on means the message is decrypted by which core.

# Bonus-Example Decrypted Messages 5

## Message

In-System Memory Content Editor - C:/Users/John/OneDrive/UBC/Year 3 Term 2/CPEN 311/Labs/Lab 4/lab4/rc4 - rc4

File Edit View Processing Tools Window Help

Search altera.com

Instance Manager: Ready to acquire

Index	Instance ID	Status	Width	Depth	Type	Mode
1	D	Not runni...	8	32	RAM/ROM	Read/Write
2	E	Not runni...	8	32	RAM/ROM	Read/Write
3	S	Not runni...	8	256	RAM/ROM	Read/Write
4	D	Not runni...	8	32	RAM/ROM	Read/Write
5	E	Not runni...	8	32	RAM/ROM	Read/Write
6	S	Not runni...	8	256	RAM/ROM	Read/Write

JTAG Chain Configuration: JTAG ready

Hardware: DE-SoC [USB-1] Setup...

Device: @2: 5CSE(BA5)MA5]5CS Scan Chain

File:

Instance 0: S

```
000000 23 7A B0 34 33 44 36 D2 28 CD 43 72 E7 A8 D8 C2 BE 7C 6B 15 87 4D 99 B3 #z.43D6.(.Cr....|k..M..
000018 82 B4 F5 92 55 0E 21 4C 75 52 D1 E5 E1 CE 2A 20 9D C8 F6 F9 09 06 AC FE ....U!LuR...* .....
000030 26 90 79 9A 46 DB 70 88 9B A7 57 2C 3F 86 E4 0A F4 D0 3A 12 A5 EE 22 29 &.y.F.p...W,?.....")
000048 47 85 4A DA 73 FA C9 8E 25 1D 83 B5 38 7D E3 FC 1C 18 BC 16 2E 13 77 AD G.J.s...&{.8}.....w.
000060 94 24 48 58 89 32 C4 5F 98 B2 1B FF 8B DC DF C6 51 35 8F E8 2F 9E 50 1A .SHX.2.....Q5../.P.
000078 D5 C5 03 BD B1 37 63 CA 59 EF C3 67 7F AB 45 A9 CF A0 95 8A 39 F7 4F 05 .....7c.Y.g.E.....9.O.
000090 31 3B 7B CC D6 3C A2 0F EA 6A 96 D7 B8 CB 5D 10 71 27 DE 97 17 19 5E F1 l;{.<...j...].q'....^
0000a8 BB 14 C0 8D 5A AE 53 00 E0 B7 54 E6 6F 3D D4 30 C7 C1 02 EC 5B F8 42 93 ....Z.S...T.o=0...[.B.
0000c0 DD 2D 76 6C 65 1E 41 0B 7E E2 84 40 F0 04 FD D3 9F 60 49 2B 0D F2 08 11 -.vle.A...<@.....It....
0000d8 5C A1 78 4B 07 F3 BA A4 64 61 66 6E 0C 1F 8C 3E 74 EB 69 ED 91 81 A6 BF \.xK....dafn...>t.i....
0000f0 E9 6D B9 4E A3 56 01 62 9C AF 80 68 FB B6 AA D9 .m.N.V.b...h....
```

Instance 1: D

```
000000 79 6F 75 20 6E 6F 77 20 68 61 76 65 20 73 6F 6C 69 64 20 76 68 64 6C 20 you now have solid vhdl
000018 73 6B 69 6C 6C 73 20 20 skills
```

Instance 2: E

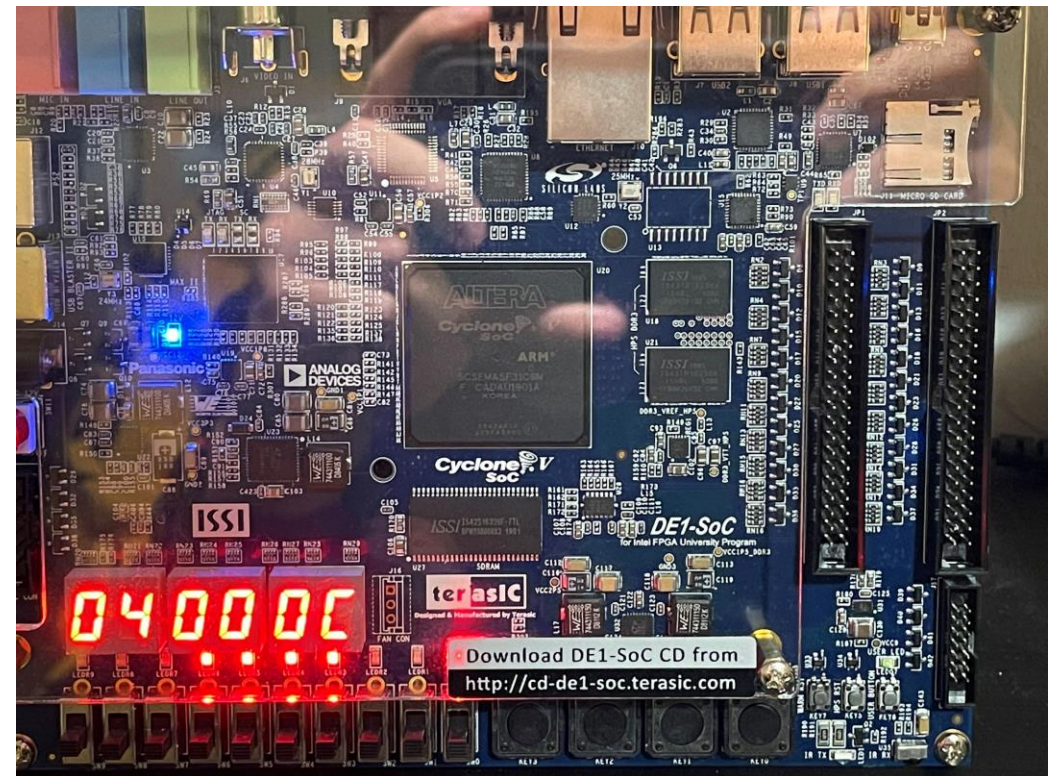
```
000000 22 03 BC 50 91 2E 28 9A 2B F0 E7 D6 54 D3 F2 17 B5 C4 FF 96 5C 38 18 A3 "...P..(+...T.....\8..
000018 0F DC B5 62 C0 70 8E 03 ...b.p..
```

Instance 3: S

```
000000 2E 00 42 39 8B 10 D6 DC E1 2D AE 3E 7C 1A 97 28 8D 55 68 78 89 08 26 36 ..B9.....->|..(Uhx..&6
000018 65 AD 94 F2 0A 27 03 5D C3 84 19 12 61 F3 53 2A AA 77 34 5E 85 3D 43 87 e....'.].....a.S*.w4^.=C.
000030 22 8E FE 74 41 0B 99 52 2C 7F 3C 33 66 D3 31 6B 75 9D 45 02 BA 79 38 CB ".tA..R,<3f.lku.E.y8.
000048 5A 11 1F 4D 98 E0 71 4A 73 A0 06 0F BD 8C 64 4C 13 AB 62 A3 FB 9B C5 1D Z..M.qJs.....d..b...
000060 C4 CF 83 C7 C0 B0 F1 5B C2 6E D7 B7 EE 9F C0 AC 15 2F DE 05 1E 16 B5 63 .....[n...../....c
000078 96 49 81 91 50 48 BB 8B B6 A9 5C 6D 5F A5 A1 B1 EB FC C9 CC 58 0E 24 54 .I..PH.....m.....X.$T
000090 90 17 0D F4 C1 30 76 A4 32 4E 95 A6 57 7A 23 B2 EA F6 B9 A2 7E 92 BF 6C ....0v..2N..Wz#.....l
0000a8 D9 09 86 6D 72 7D 7B B8 93 A7 2B B3 B4 01 80 3F AF 67 44 56 BC 8F BE 4F ...r}{...+....?gDV...0
0000c0 69 C1 9E 20 59 9A C6 29 C8 8A CA 47 04 CD CE 35 D0 D1 D2 21 D4 D5 37 6A i..Y....G...5...!..7i
```

0% 00:00:00 Instance: Word: Bit:

## Secret Key



LED[9:6] indicate core[3:0] separately.

LED on means the message is decrypted by which core.



# Bonus-Example Decrypted Messages 6

## Message

In-System Memory Content Editor - C:/Users/John/OneDrive/UBC/Year 3 Term 2/CPEN 311/Labs/Lab 4/lab4/rc4 - rc4

File Edit View Processing Tools Window Help

Search altera.com

Instance Manager: Ready to acquire

Index	Instance ID	Status	Width	Depth	Type	Mode
0	S	Not runni...	8	256	RAM/ROM	Read/Write
1	D	Not runni...	8	32	RAM/ROM	Read/Write
2	E	Not runni...	8	32	RAM/ROM	Read/Write
3	S	Not runni...	8	256	RAM/ROM	Read/Write
4	D	Not runni...	8	32	RAM/ROM	Read/Write
5	E	Not runni...	8	32	RAM/ROM	Read/Write

JTAG Chain Configuration: JTAG ready

Hardware: DE-SoC [USB-1] Setup...

Device: @2: 5CSE(BA5)MA5]5CS Scan Chain

File:

Instance 0: S

```
000000 00 C6 0A 25 FD C0 AB B7 63 08 90 67 D0 BF 95 09 F4 F3 5E 96 A9 97 D2 11 ...%.c.g.....^....
000018 DD 32 20 BA D4 7A 48 C8 EC 2A E4 23 C3 F5 03 5B CE 17 EB 1B 8A 12 8F FA .2 .zh.*.#. [...] ^sg
000030 D6 4C 7B D9 84 F9 CB 7F 40 3E 21 3C F8 55 B1 06 8E 53 6E 8C 29 87 C4 EE .L{...@>!<.U..Sn)...
000048 9C F2 8D 43 05 B9 83 3F 89 2B AC 79 46 86 ED 82 19 2C 99 A6 4E C9 0C 77 ..C...?.+yF...C#.w
000060 D7 07 7E 72 61 0B 35 04 FE 2D 66 85 E6 58 C1 81 A0 7C 54 6C EF BD 98 78 ...ra.5...f.X...[Tl...x
000078 73 CF EA B0 56 9D A4 BB 47 01 0F 3A 1D 15 2E 91 F7 A2 5F E5 0D E2 9F AF s..V..G.....
000090 38 64 60 CA 65 B2 9A 2F CD 6A 94 68 5D 70 1A A5 80 F6 92 DA 42 D3 41 5A 8d`.e./j.hp)...B.AZ
0000a8 FC 13 28 31 DF AE FF 33 4D E3 30 DC A8 76 E0 62 4B 69 7D C7 49 52 39 B5 ..(1..3M.0..v.bKi).IR9.
0000c0 51 AD 44 34 E8 16 02 D8 71 1E 6D A3 5C 3D 0E 24 26 E1 4F E7 AA F0 14 DB Q.D4...q.m.\=$&.O...
0000d8 CC A1 B4 BC 74 BE F1 C5 B3 57 4A 93 50 36 45 10 A7 DE 88 D5 37 B6 8B 18 ...t...WU.P6E...7...
0000f0 D1 FB 3B 1C 6F 59 9B 9B C2 6B E9 22 75 B8 1F 27 ...;oY...k."u..'
```

Instance 1: D

```
000000 74 68 69 73 20 6F 6E 65 20 69 73 20 74 72 69 63 6B 79 20 77 69 74 68 20 this one is tricky with
000018 7A 65 72 6F 20 6B 65 79 zero key
```

Instance 2: E

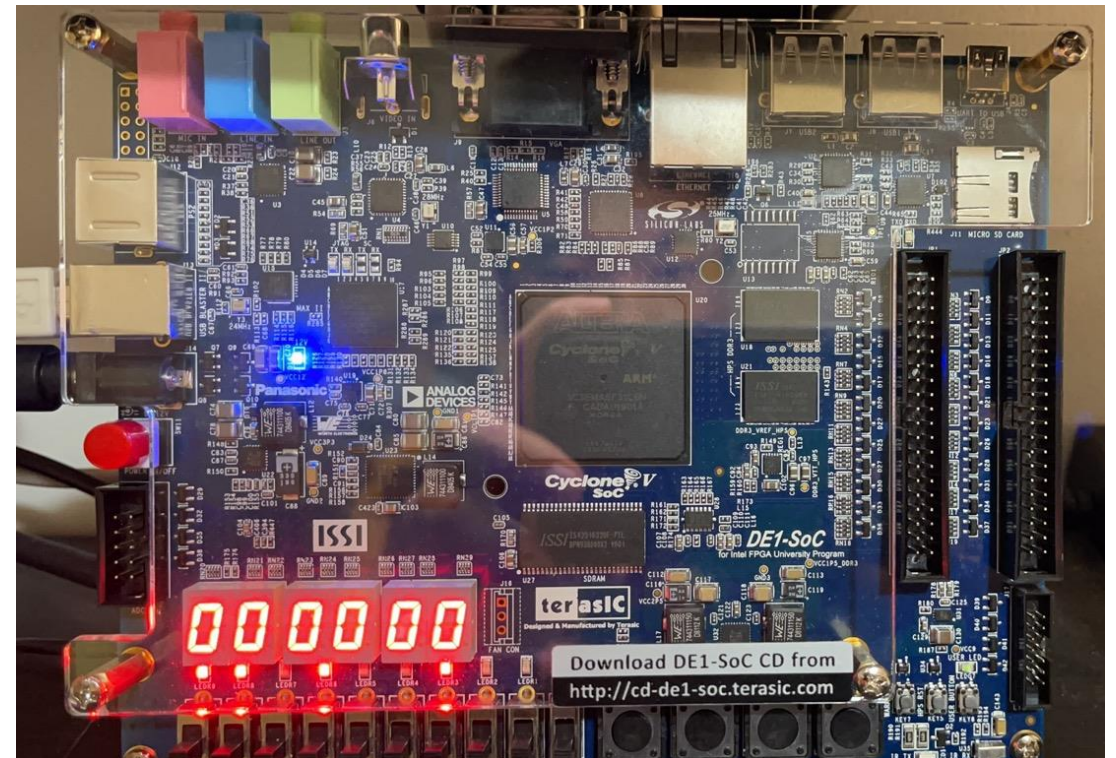
```
000000 AA 70 E0 32 83 58 33 5F AA 6F 6D 47 23 1C FB 0E AC 63 5F D4 99 B8 83 B7 ..p.2.X3..omG#....c.....
000018 3F 4E 3F 5D 07 FD 3A E7 ?N?]....
```

Instance 3: S

```
000000 11 01 F4 3E 7E 64 0B 19 F7 31 0F 03 57 87 1E 72 74 26 48 E7 6B C3 17 9B ...>d...l..W..rt&H.k...
000018 F8 8A 24 37 1D 4D 90 CC 22 10 2F B1 D7 7D 3F 25 E3 A9 E9 29 EC 5E 73 67 ..$7.M..".(.)?%....^sg
000030 BA B9 EB 63 D5 78 B2 4C 2D 70 5D 6A 30 9E 3C 59 A6 88 E2 E8 1A 43 23 C7 ..c.x.L-p]j0.<Y...C#.
000048 5A C1 21 00 09 91 B0 81 B4 5B C4 E6 46 A7 9C B3 83 45 65 A4 FD 60 CB 98 T.!...[.F...Ee...
000060 E8 D9 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 ..bdefghijklmnopqrstuvw
000078 78 79 7A 7B 7C 7D 7E 04 80 81 82 07 01 85 86 87 88 89 8A 8B 8C 8D 8E 8F xyz{ }~
000090 0A 91 92 93 94 95 96 97 98 99 9A 1C 12 9D 9E 9F A0 A1 A2 A3 17 A5 0D A7 .....
0000a8 A8 A9 AA AB AC AD AE AF B0 0E B2 B3 53 B5 B6 B7 B8 B9 BA BB BC BD 22 BF .....S.....".
0000c0 C0 03 C2 2E C4 10 4B 47 C8 C9 15 55 CC CD CE CF 51 60 40 D3 76 04 30 D7 .....KG...U...O'@.v.O..
```

0% 00:00:00 Instance: Word: Bit:

## Secret Key



LED[9:6] indicate core[3:0] separately.

LED on means the message is decrypted by which core.

# Bonus-Example Decrypted Messages 7

## Message

**In-System Memory Content Editor** - C:/Users/John/OneDrive/UBC/year 3 Term 2/CPEN 311/Labs/Lab 4/lab4/r4 - rc4

File Edit View Processing Tools Window Help

Search altera.com

---

**Instance Manager:**

Index	Instance ID	Status	Width	Depth	Type	Mode
0	S	Not runni...	8	256	RAM/ROM	Read/Write
1	D	Not runni...	8	32	RAM/ROM	Read/Write
2	E	Not runni...	8	32	RAM/ROM	Read/Write
3	S	Not runni...	8	256	RAM/ROM	Read/Write
4	D	Not runni...	8	32	RAM/ROM	Read/Write
5	E	Not runni...	8	32	RAM/ROM	Read/Write

**JTAG Chain Configuration:** JTAG ready

**Hardware:** DE-Soc [USB-1] Setup...

**Device:** @2:5CSE(BA5|MA5)/5CS Scan Chain

**File:** [Icon] ...

---

**Instance 0: S**

000000	4A 2D 1C 25 B0 51 62 FF D9 E2 AA C2 3A 1B 93 16 A7 EF EA E0 2F F3 D6 27	J-.%Qb...../..'
000018	42 A1 57 13 DC C7 97 5A 95 69 9F D1 05 09 3B DE 07 82 CE B2 CA 46 59 AB	B.W...Z.i.....FY.
000030	BB 50 91 A8 FD 6C 01 54 60 7B 53 9D 6F 40 C9 AC AE FE CB 08 39 5C 87 EA	.P...l.T\`S.o@.....9\.
000048	9E 4B A4 4E 0C 08 B5 41 AF 38 74 79 CF 28 A9 F6 BE EC C3 83 72 DA 68	.K.N...A.8ty.(.M...r.h
000060	5B 49 35 90 7C A5 2B 67 F5 8C B3 EC 10 0E E7 44 EB D2 48 64 00 88 B1	[I5.+>.g.....D..Hd....
000078	B9 F1 7A D3 D8 9B 19 47 1A E9 34 C4 03 E6 F7 9C FB 6A D0 58 D8 B4 CE 23	..Z...G:.4.....j.X...#
000090	A6 F9 9A BC B7 37 14 29 1F 56 1D F2 20 A0 26 00 84 06 8A 70 02 A3 10	..(7.)V...@...P.0
0000a8	CD 6E 32 89 FA 2E 73 DB B8 55 D7 96 22 8B 3C DD 15 99 8B C8 B5 71 E3	n2...s.U"...<.....
0000c0	BD C5 ED DA 86 52 36 7E 65 2A 98 3E 33 77 EE 31 C1 12 11 FC 3F AD 6B 5D	..R6-e^>3w1...?.k]
0000d0	63 4F 94 F0 1E 6D CC 24 BF 81 2C 4C 45 75 E1 32 F4 D5 0A 5F D0 3D 8F 04	cO...m?!,LEU..._-..
0000f0	66 18 43 45 DF 78 76 5E 21 A2 B6 7D 7F BA 61 0F	f.C.xv?...!...a.a.

**Instance 1: D**

000000	76 68 64 6C 20 5E 69 6E 6A 61 20 73 61 76 65 73 20 74 68 65 20 64 61 71 79	vhd1 ninja saves the day
000018	20 20 20 20 60 20 20 20 20	

**Instance 2: E**

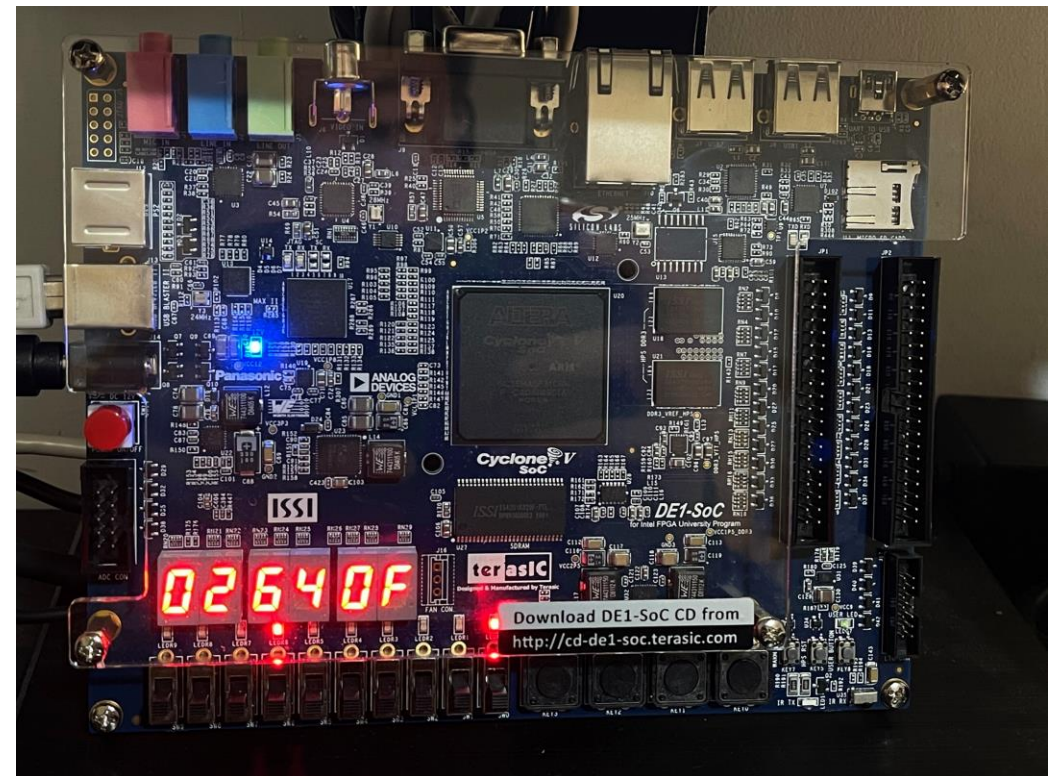
000000	C1 0C 35 D0 C8 25 72 66 4B 0D AD 4B B6 31 29 32 C2 90 0D 68 1E 76 5E 02 62	..5..'fk(K.1)2...h.v^.b
000018	DA 45 70 0D A5 92 74 BE	Exp...t.

**Instance 3: S**

000000	20 A6 A7 EC 43 57 9F 33 10 59 23 D0 1E 8E 9B 03 05 28 BB 31 16 0E 4C 14	...CW.3.Y#.....(.1.L.
000018	8A 1A 42 38 41 26 5F E1 2B 63 E8 3A 7D FB 67 86 1D 39 92 08 4B BA 2C 79	..B8A@_+c.:p.g.^9.K.,y
000030	EB 61 17 09 9E D2 4A E4 76 3F 3A 50 7B 04 27 DC F5 5E 53 2A 34 47 8C	..Mdef.jvjv.R.(.''.S*4G
000048	44 C2 F7 11 48 62 F2 A4 F3 29 5D B8 D4 46 1F 19 58 07 5A 5B 5C 3B 00 0C	D...Hb...)].F.X.Z([...]w
000060	60 13 AD 21 64 65 62 E8 6B 6A 6B 6C 6D 6E 6F 24 71 72 73 74 75 1B 77	x/z= )~.....Q.....U..
000078	78 2F 7A 3D 7C 7D 7E 7F 80 81 82 83 18 85 51 87 88 89 8A 8B 55 8D 0F 8F	..2.....E.....O.....
000090	90 91 32 93 94 95 96 97 98 99 9A 15 9C 9D 45 06 A0 A1 A2 A3 4F A5 01 02	.....>.....T.....
0000a8	A8 A9 AA AB AC AD AE AF B0 B1 B2 B3 B4 B5 B6 B7 B8 B9 2D 12 BC BD BE BF	
0000c0	C0 C1 49 C3 C4 C5 0A C7 C8 C9 CA CB CC CD CE CF 0B D1 D3 54 D5 D6 D7	

0% 00:00:00 Instance: Word: Bit:

## Secret Key



LED[9:6] indicate core[3:0] separately.

LED on means the message is decrypted by which core.



# Bonus - Example Decrypted Messages 8

## Message

In-System Memory Content Editor - C:/Users/John/OneDrive/UBC/Year 3 Term 2/CPEN 311/Labs/Lab 4/lab4/rc4 - rc4

File Edit View Processing Tools Window Help

Search altera.com

Instance Manager: Ready to acquire

Index	Instance ID	Status	Width	Depth	Type	Mode
0	S	Not runni...	8	256	RAM/ROM	Read/Write
1	D	Not runni...	8	32	RAM/ROM	Read/Write
2	E	Not runni...	8	32	RAM/ROM	Read/Write
3	S	Not runni...	8	256	RAM/ROM	Read/Write
4	D	Not runni...	8	32	RAM/ROM	Read/Write
5	E	Not runni...	8	32	RAM/ROM	Read/Write

JTAG Chain Configuration: JTAG ready

Hardware: DE-SoC [USB-1] Setup...

Device: @2: 5CSE(BA5)MA5)/5CS- Scan Chain

File: ...

Instance 0: S

```
000000 00 5F 9F A1 A4 30 53 41 61 92 DC 8F B2 83 EA E1 3F FF 1F D8 62 50 95 60 .....0SAa.....?..bP.`
000018 40 8C 57 FD DB C3 3A 44 FC A2 37 38 22 BF E4 F6 71 99 3E 0A 56 F8 EF D9 @.W...:D..78"...q>..V...
000030 0C AE 03 14 1A 73 10 94 6E A5 C4 78 75 F7 4D 4C A0 43 4F F9 3C BB 19 8B .....s..n..xu..ML.CO.<...
000048 13 81 D6 EB C7 5E E6 35 11 79 CA A6 5C 93 F2 27 CC 6C 5A 1C 74 65 9A AB .....^..5.y..\..'.lZ.te..
000060 CF AA E0 96 5B F0 23 68 1D 8A BD D5 80 63 DD D0 42 0B 2F B8 84 87 85 A3 ....[. #h...c..B./...
000078 B3 DA 7F BD 54 24 B1 21 6D 6F DF 31 A7 3B 49 9C 5D A9 48 BA D2 58 B0 D7 ...T$.!mo.l;I;].H..X..
000090 D4 01 2C 69 09 15 EC 82 0E B7 66 AC 07 45 76 CD 55 8E E8 B6 C8 16 1B 4A ...i...mo..f..Ev.U....J
0000a8 59 C0 25 46 ED E9 86 32 6A 17 C6 A8 90 EE 1E E7 33 2B 52 12 3D C9 20 91 Y.%F...2j.....3+R.=.
0000c0 47 9E CB FB 7B 0F BE AD 36 FA E3 77 D3 29 89 02 64 26 28 18 B5 9D DE AE G...{...6..w.)..d&{...p...N
0000d8 88 D1 0D 98 B9 67 7A B4 F4 E2 BC 4B 72 CE 06 08 FE 70 04 F3 E5 05 2D C5 .....gz...Kr....p.....
0000f0 6B 97 F5 7D 2E 7C 34 2A C2 7E C1 F1 9B AF 51 39 k...|.4*~....Q9
```

Instance 1: D

```
000000 67 6F 6F 64 20 6C 75 63 6B 20 6F 6E 20 79 6F 75 72 20 65 78 61 6D 73 20 good luck on your exams
000018 20 20 20 20 20 20 20 20
```

Instance 2: E

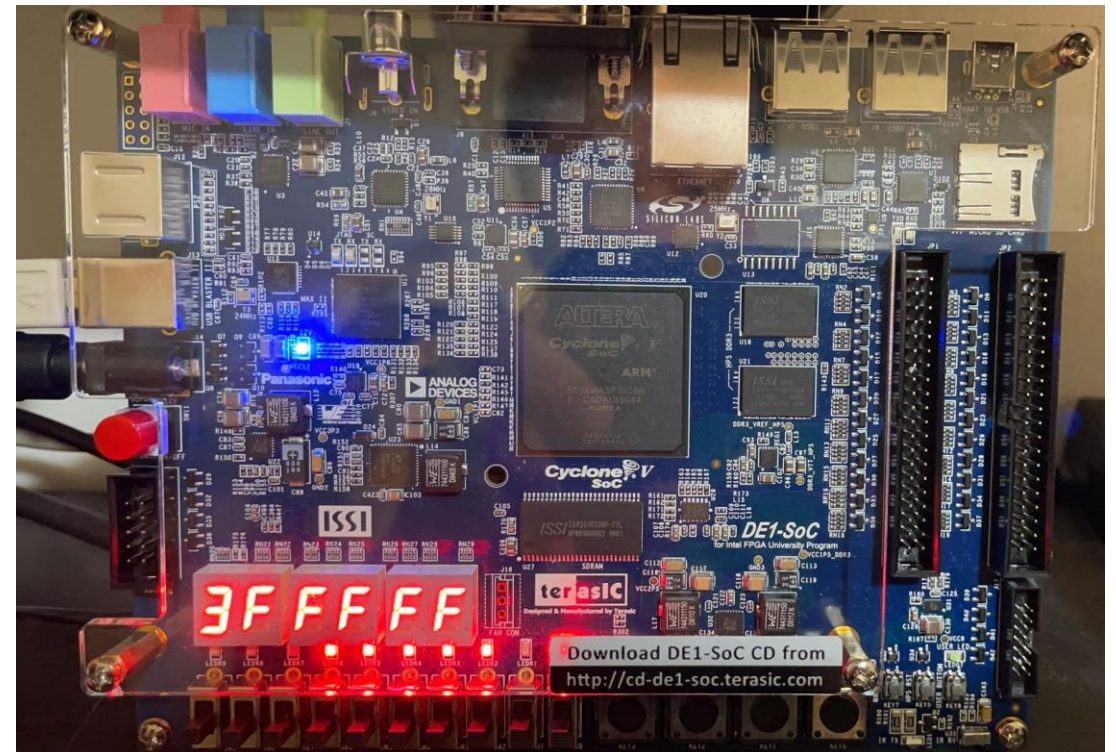
```
000000 CC 11 01 FD A2 DC 6A 16 85 41 60 7A 71 DE F0 21 6A DD 2F 26 02 E0 07 AD .....j..A`zq...!j./&....
000018 0A B8 08 95 D5 3E 91 5E .....>..^
```

Instance 3: S

```
000000 7F 00 71 40 3B EB 02 60 6E 4C FF FA 85 91 8F 6F 27 2D BE 4E 06 68 7D 84 ...q@?...nL.....o'-.N.h).
000018 1B 33 3D 14 56 EE B8 A9 B9 08 7A 10 30 54 66 2C 5F 6D F9 8D 2B B3 E0 45 .3=.V.....z.0Tf;_m...+.E
000030 A2 D2 F4 8C 41 E4 99 43 E8 A0 46 F6 34 D8 70 73 07 65 F5 C0 6B 0A 4D AB .....A..C..F.4.ps.e..k.M.
000048 72 58 51 12 04 74 D0 61 22 32 9B DE 5B 4F EF E2 BA 5A 0B 82 39 7C 3A 37 rXQ..t..a"2..[O...Z..9!;7
000060 76 D6 A7 89 EC BF 6A 19 0D 79 9E 31 BD 50 59 1D D4 3E CD C4 75 D9 F3 62 v.....j..y.l.EY.>..u..b
000078 26 69 29 7B 5D 16 7E 01 80 81 25 83 17 0C 86 87 88 63 8A 1E 67 23 8E 0E &i){}...%......c..g#..
000090 90 15 92 93 94 95 96 97 98 36 9A 52 9C 9D 26 9F 5C A1 24 A3 A4 A5 A6 77 .....6.R.&..\$.s..w
0000a8 A8 1F AA 47 AC AD AE AF B0 B1 B2 11 B4 B5 B6 B7 B8 20 49 BB BC 6C 4B 3C (...G.....6.R.&..\$.s..w
0000c0 28 C1 C2 C3 3F C5 C6 C7 C8 C9 CA CB CC 48 CE CF 13 D1 44 D3 18 D5 55 D7 (...?.....H....D...U..
```

0% 00:00:00 Instance 1: D Word: 0x000019 Bit: 0x000007

## Secret Key: 3FFFFFF



LED[9:6] indicate core[3:0] separately.

LED on means the message is decrypted by which core.

# Bonus - Example Decrypted Messages 8

Secret Key: 3FFFFFF

Setting:

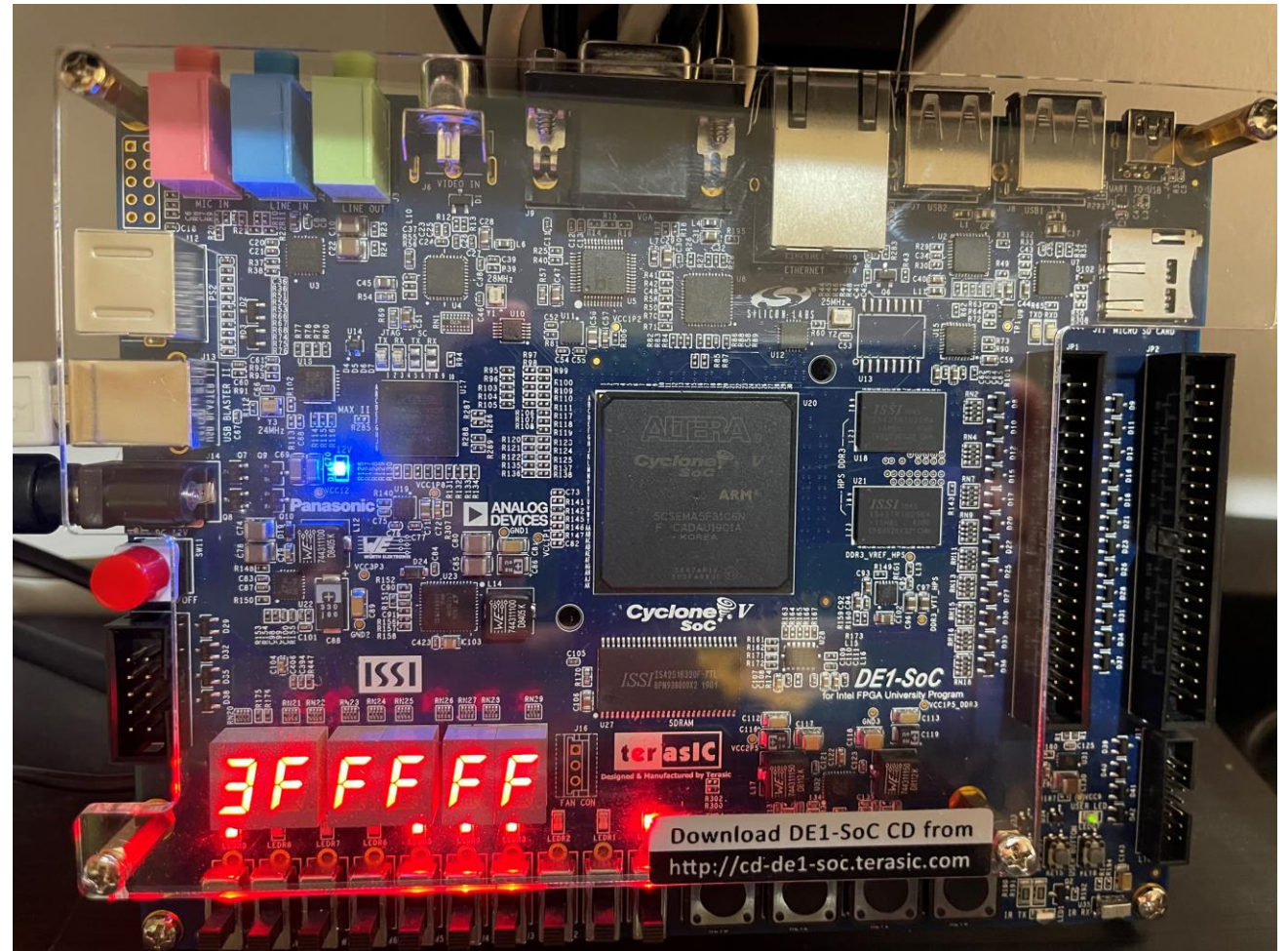
Core0: Start from 24'h0

Core1: Start from 24'h010000

Core2: Start from 24'h020000

Core3: Start from 24'h030000

The result is as expected: Multicore  
decryption works fine.





# Design Integrity

No latch found

