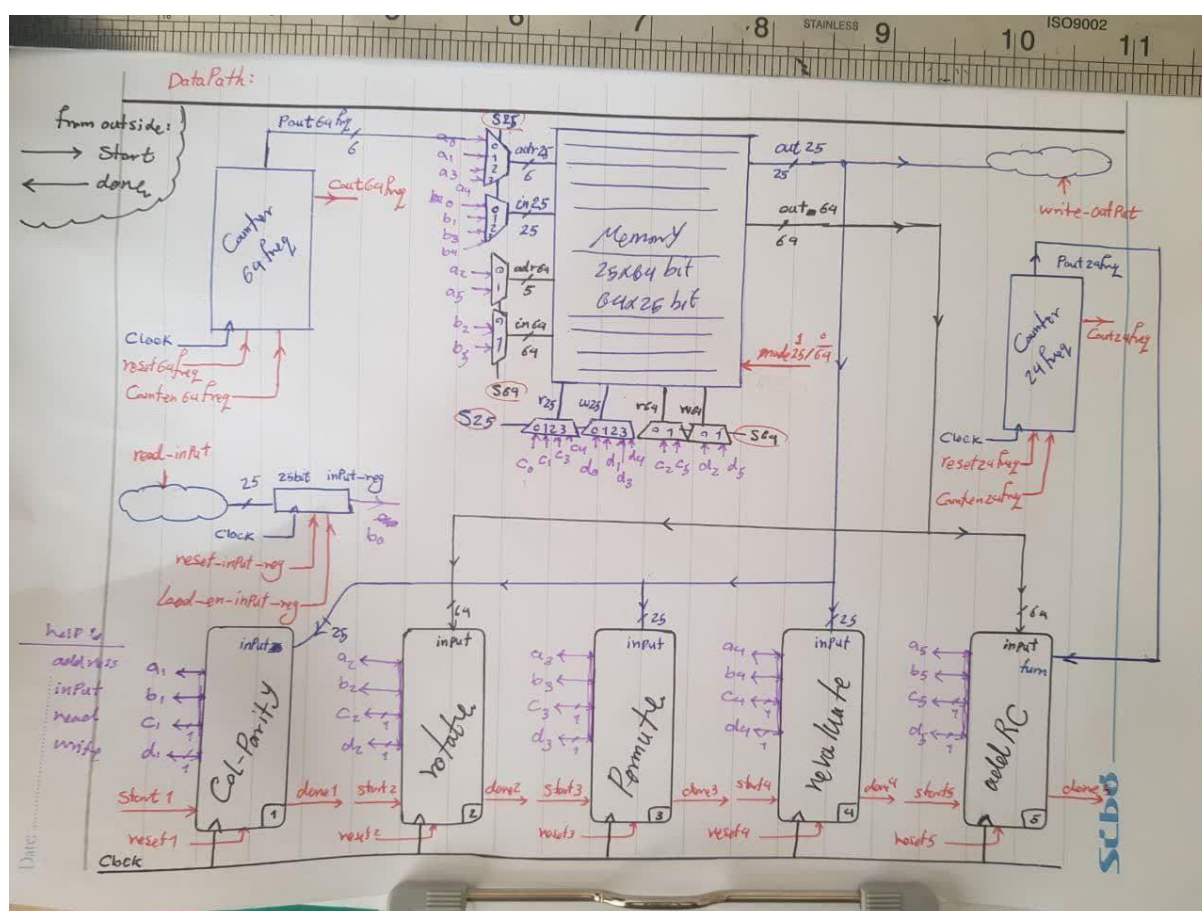




مقدمه

در این تمرین، ما یک encoder رمز گذاری را پیاده سازی می کنیم. برای این کار ۵ مازول را به صورت ترتیبی روی ورودی اجرا می کنیم و این کار را ۲۵ بار تکرار می کنیم.
۳ تا از توابع قبلا پیاده سازی شده و دو تای دیگر را نیز پیاده سازی خواهیم کرد.

مسیر داده:



همانگونه که مشاهده می‌کنید مسیر داده از یک مموری تشکیل شده است که در دو حالت ۲۵ و ۶۴ بیتی می‌توان از آن استفاده کرد و ۵ مائول با توجه به نیازشان از آنها استفاده می‌کنند و مسیر داده توسط mux هایی در هر مرحله، آن مائول مورد نظر را به مموری وصل می‌کند.

از یک counter 64 freq برای شمردن ۶۴ ورودی و از یک کانتر ۲۴ تایی برای شمردن ۲۴ بار اجرای فرآیند استفاده می‌شود.

تمام مائول ها یک بیت start ورودی و یک بیت done دارند که با دادن start شروع به کار می‌کنند و در پایان done داده می‌شود.

تابع addrc به اینکه در کدام سری اجرا نیاز هست هم نیاز دارد که با بیت turn به آن می‌دهیم.

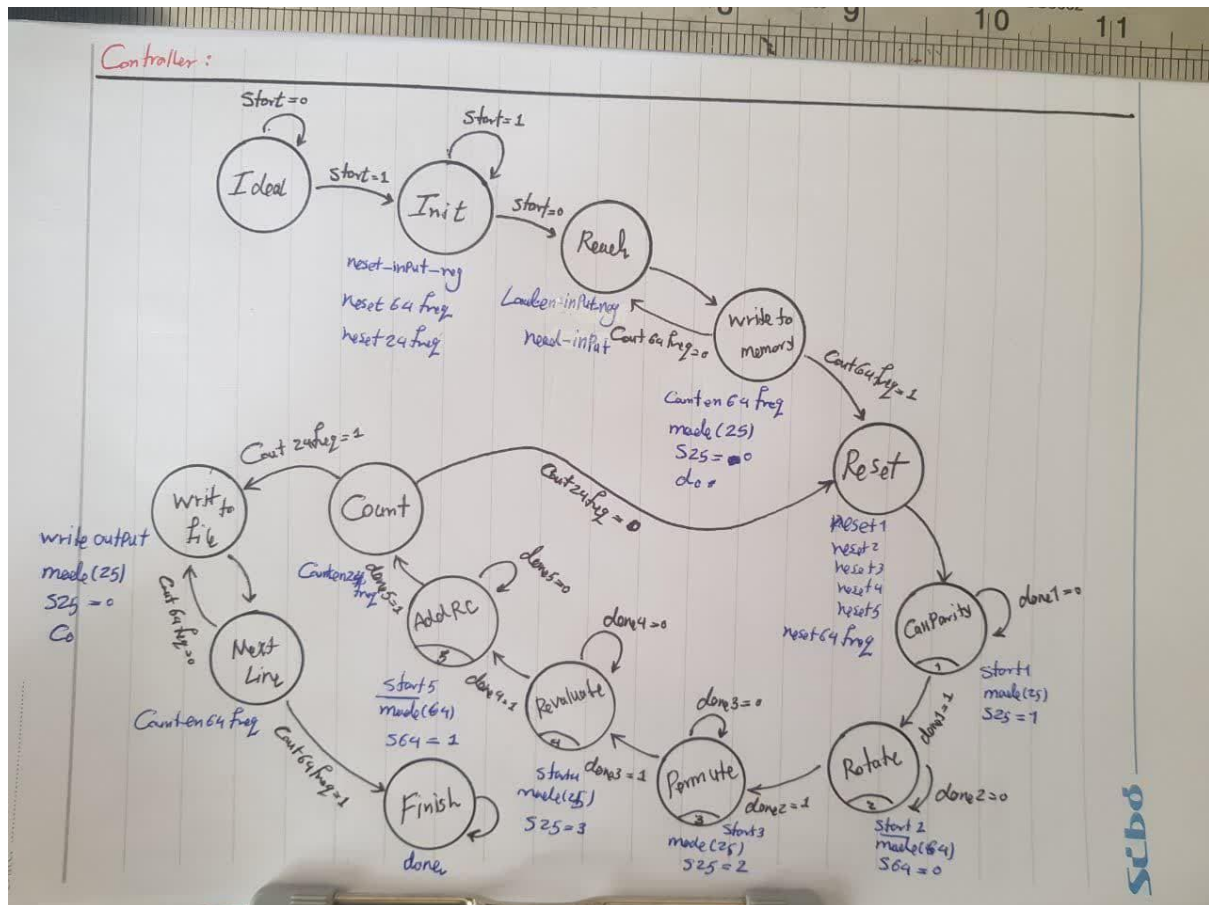
کد مربوط به مسیر داده که دارای ۵ مائول، به مموری و mux ها مطابق شکل است را می‌توانید در زیر مشاهده نمایید.

```

4
5 reg clock = 0, start = 0;
6 wire start_addr, start_colparity, start_permute, start_revaluate, start_rotate;
7 wire done, done_addr, done_colparity, done_permute, done_revaluate, done_rotate;
8 wire reset_addr, reset_colparity, reset_permute, reset_revaluate, reset_rotate;
9 wire mode; //remember to change this to 0 for 64 bit mode
10 wire sel64;
11 wire [1 : 0] sel25;
12 wire [4 : 0] turn;
13 wire wr_file;
14 wire count_en, reset_counter, cout;
15
16 wire [5 : 0] a0, a1, a3, a4, out_mux1;
17 wire [24 : 0] b0, b1, b3, b4, out_mux2;
18 wire [4 : 0] a2, a5, out_mux3;
19 wire [63 : 0] b2, b5, out_mux4;
20 wire c0, c1, c2, c3, c4, c5, d1, d2, d3, d4, d5, out_mux5, out_mux6, out_mux7, out_mux8;
21
22 wire [0:24]out25;
23 wire [0:63]out64;
24
25 mux_4 #(.bits(6)) m1(a0, a1, a3, a4, out_mux1, sel25);
26 mux_4 #(.bits(25)) m2(b0, b1, b3, b4, out_mux2, sel25);
27
28 mux_2 #(.bits(5)) m3(a2, a5, out_mux3, sel64);
29 mux_2 #(.bits(64)) m4(b2, b5, out_mux4, sel64);
30
31 mux_4 #(.bits(1)) m5(c0, c1, c3, c4, out_mux5, sel25);
32 mux_4 #(.bits(1)) m6(d0, d1, d3, d4, out_mux6, sel25);
33
34 mux_2 #(.bits(1)) m7(c2, c5, out_mux7, sel64);
35 mux_2 #(.bits(1)) m8(d2, d5, out_mux8, sel64);
36
37
38 >Memory #(.input_file("input_1.txt")) Memory_ ( ~
53 );
54
55 >Colparity Colparity_ ( ~
65 );
66
67 >Rotate Rotate_ ( ~
77 );
78
79 >Permute Permute_ ( ~
89 );
90
91 >Revaluate Revaluate_ ( ~
101 );
102
103 >Addr Addr_ ( ~
114 );
115
116 >counter24 counter6bit_ ( ~
122 );
123
124 cu cu_
125 > ( ~
138 );
139
140
141

```

کنترلر:



نحوه ی کار کنترلر بدین گونه است که پس از گرفتن یک پالس استارت، ابتدا ورودی را سطر به سطر و ۲۵ بیت، ۲۵ بیت از فایل ورودی می گیرد و در مموری می نویسد.

برای این کار از کانتر ۶۴ تایی استفاده می کند.

پس از آن، داخل یک لوپ می افتد:

- یکی یکی سیگنال های start پنج مازول را فعال می کنیم و منتظر می مانیم تا تمام شوند

- سپس این کار را ۲۴ بار ادامه می دهیم.

- برای این کار از کانتر ۲۴ بیت استفاده می کنم.

پس از اتمام، باز هم ۲۵ بیت و سطر به سطر از مموری در فایل خروجی می نویسیم و تمام!

به استتیت پایان می رویم و سیگنال پایان را فعال می کنیم.

کد مربوط به کنترلر را در زیر مشاهده می‌کنید که مدل هافمن و جدا کردن مدل ترتیبی و ترکیبی رعایت شده و از سه حلقه ی `always` استفاده شده.

```
1 // In the Name of God
2
3 module cu
4 (
5     input clock, start,
6     input done_addr, done_colparity, done_permute, done_revaluate, done_rotate,
7     input [4 : 0] turn,
8     input cout,
9     output reg start_addr, start_colparity, start_permute, start_revaluate, start_rotate,
10    output reg reset_addr, reset_colparity, reset_permute, reset_revaluate, reset_rotate,
11    output reg mode, sel64,
12    output reg [1 : 0] sel25,
13    output reg wr_file,
14    output reg done,
15    output reg count_en,
16    output reg reset_counter
17 );
18
19 reg [4:0] ps, ns;
20 parameter Idle = 0, Init = 1, ResetColParity = 2, StartColParity = 3, DoneColParity = 4, ResetRotate = 5,
21 StartRotate = 6, DoneRotate = 7, ResetPermute = 8, StartPermute = 9, DonePermute = 10, ResetRevaluate = 11, StartRevaluate = 12, DoneRevaluate = 13,
22 ResetAddrRc = 14, StartAddrRc = 15, DoneAddrRc = 16, Finish = 17;
23
24 always @(posedge clock) begin
25     ps <= ns;
26 end
27
28 always @(ps, start, cout, done_addr, done_colparity, done_permute, done_revaluate, done_rotate) begin
29     ns = Idle;
30     case (ps)
31         Idle: ns = start ? Init : Idle;
32         Init: ns = start ? Init : ResetColParity;
33         ResetColParity: ns = StartColParity;
34         StartColParity: ns = done_colparity ? DoneColParity : StartColParity;
35         DoneColParity: ns = ResetRotate;
36         ResetRotate: ns = StartRotate;
37         StartRotate: ns = done_rotate ? DoneRotate : StartRotate;
38         DoneRotate: ns = ResetPermute;
39         ResetPermute: ns = StartPermute;
40         StartPermute: ns = done_permute ? DonePermute : StartPermute;
41         DonePermute: ns = ResetRevaluate;
42         ResetRevaluate: ns = StartRevaluate;
43         StartRevaluate: ns = done_revaluate ? DoneRevaluate : StartRevaluate;
44         DoneRevaluate: ns = ResetAddrRc;
45         ResetAddrRc: ns = StartAddrRc;
46         StartAddrRc: ns = done_addr ? DoneAddrRc : StartAddrRc;
47         DoneAddrRc: ns = cout ? Finish : ResetColParity;
48         Finish: ns = Finish;
49         default: ns = Idle;
50     endcase
51 end
52
53 always @(ps, start, cout) begin
54     case (ps) -
55     endcase
56 end
57
58 assign state = ps;
59
60 endmodule
```

توضیح ماژول ها:

memory:

همانگونه که قبلا گفته شد، مسیر داده از یک مموری تشکیل شده است که در دو حالت ۲۵ و ۶۴ بیتی می توان از آن استفاده کرد و ۵ ماژول با توجه به نیازشان از آنها استفاده می کنند و مسیر داده توسط mux هایی در هر مرحله، آن ماژول مورد نظر را به مموری وصل می کند.

همچنین یک تست برای اطمینان از درستی اش نوشته شد.

در زیر می توانید کد مربوط به مموری و تست را مشاهده نمایید:

```
1 module Memory #(parameter input_file)
2 (
3     input [5:0]adr25,
4     input [0:24]in25,
5     input r25,
6     input w25,
7     output reg [0:24]out25,
8
9     input [4:0]adr64,
10    input [0:63]in64,
11    input r64,
12    input w64,
13    output reg [0:63]out64,
14
15    input mode,
16    input wr_file
17 );
18 // craete 64x25 bit memory
19 reg [0:24] memory[0:63];
20
21
22
23 //for testing
24 initial begin
25     $readmemb(input_file, memory);
26 end
27
28 integer i;
29
30 parameter Mode64 = 0;
31 parameter Mode25 = 1;
32
33 always @(adr25 or in25 or r25 or w25 or adr64 or in64 or r64 or w64 or mode)begin
34     case (mode)
35         Mode64: begin
36             if (r64) begin
37                 for (i = 0; i < 64; i = i + 1) begin
38                     out64[i] <= memory[i][adr64];
39                 end
40             end
41             if (w64) begin
42                 for (i = 0; i < 64; i = i + 1) begin
43                     memory[i][adr64] <= in64[i];
44                 end
45             end
46         end
47         Mode25: begin
48             if (r25) begin
49                 out25 <= memory[adr25];
50             end
51             if (w25) begin
52                 memory[adr25] <= in25;
53             end
54         end
55     endcase
56 end
57 always @(wr_file) begin
58     if(wr_file) begin
59         $writememb("output.txt", memory);
60     end
61 end
62 endmodule
```

```

1 | timescale 1ns/1ns
2
3 module tb_memory ();
4
5 reg [5:0]adr25;
6 reg [0:24]in25;
7 reg r25;
8 reg w25;
9 wire [0:24]out25;
10
11 reg [4:0]adr64;
12 reg [0:63]in64;
13 reg r64;
14 reg w64;
15 wire [0:63]out64;
16
17 reg mode;
18
19 Memory uut (
20     .adr25(adr25),
21     .in25(in25),
22     .r25(r25),
23     .w25(w25),
24     .out25(out25),
25
26     .adr64(adr64),
27     .in64(in64),
28     .r64(r64),
29     .w64(w64),
30     .out64(out64),
31
32     .mode(mode)
33 );
34
35 initial begin
36     adr25 = 0;
37     in25 = 0;
38     r25 = 0;
39     w25 = 0;
40
41     adr64 = 0;
42     in64 = 0;
43     r64 = 0;
44     w64 = 0;
45
46     mode = 0;
47 end
48
49 initial begin
50     //write with 25
51     adr25 = 5'd3;
52     in25 = 25'b00000_11101_00000_00000_00000;
53     r25 = 0;
54     w25 = 1;
55     mode = 1;
56     #100
57     //write with 64
58     adr64 = 4'd3;
59     in64 = 64'b1111_1111_1111_1111_1111_1111_1111_1111_1111_1111_1111_1111_0101_0101;
60     r64 = 0;
61     w64 = 1;
62     mode = 0;
63     #100
64     //read with 64

```

Rotate:

با فعال کردن سیگنال start، تابع از یک کانتر ۲۵ تایی استفاده می‌کند و در هر کلاک، ۶۴ بیت یک لاین را می‌گیرد.

سپس با استفاده از بیت مورد استفاده، مقدار X, Y این لاین را حساب می‌کند.

y/x	$x = 0$	$x = 1$	$x = 2$	$x = 3$	$x = 4$
$y = 4$	18	2	61	56	14
$y = 3$	41	45	15	21	8
$y = 2$	3	10	43	25	39
$y = 1$	36	44	6	55	20
$y = 0$	0	1	62	28	27

پس از آن توسط جدول زیر، که به ازای هر x, y مقدار شیفت را مشخص می‌کند، شروع به شیفت دادن آن لاین می‌کند.

در آخر نیز نتیجه را در همان لاین می‌نویسد.

در زیر می‌توانید کد مربوط به Rotate و تست را مشاهده نمایید:

```

1 `timescale 1ns/1ns
2
3 module Rotate
4 (
5     input [0:63] in,
6     input start,
7     input clock,
8     input reset,
9     output reg done,
10    output reg [4:0] mem_adr,
11    output reg [0:63] mem_in,
12    output reg mem_r,
13    output reg mem_w
14 );
15
16 integer i, x, y, final_index, lane = 0;
17
18 reg [0:63] in_temp;
19
20 reg [5:0] f [0:4] [0:4];
21
22 initial begin
23     f[0][0] = 0;
24     f[0][1] = 36;
25     f[0][2] = 3;
26     f[0][3] = 41;
27     f[0][4] = 18;
28     f[1][0] = 1;
29     f[1][1] = 44;
30     f[1][2] = 10;
31     f[1][3] = 45;
32     f[1][4] = 2;
33     f[2][0] = 62;
34     f[2][1] = 6;
35     f[2][2] = 43;
36     f[2][3] = 15;
37     f[2][4] = 61;
38     f[3][0] = 28;
39     f[3][1] = 55;
40     f[3][2] = 25;
41     f[3][3] = 21;
42     f[3][4] = 56;
43     f[4][0] = 27;
44     f[4][1] = 20;
45     f[4][2] = 39;
46     f[4][3] = 8;
47     f[4][4] = 14;
48 end
49
50 reg [5:0] rotate_f;
51
52 always @(posedge clock, posedge reset) begin
53     if (reset) begin
54         lane = 0;
55     end
56     else if (start && lane < 25) begin
57         mem_r = 1;
58         mem_adr = lane;
59         mem_w = 0;
60
61         x = ((lane % 5) + 3) % 5;
62         y = ((lane / 5) + 3) % 5;
63
64         rotate_f = f[x][y];

```



```

1 `timescale 1ns/1ns
2
3 module tb_rotate ();
4
5 reg clock = 0;
6 reg start = 0;
7 reg reset = 0;
8 reg mode = 0; //remember to change this to 0 for 64 bit mode
9
10
11 wire [5:0]adr25;
12 wire [0:24]in25;
13 wire r25;
14 wire w25;
15 wire [0:24]out25;
16
17 wire [4:0]adr64;
18 wire [0:63]in64;
19 wire r64;
20 wire w64;
21 wire [0:63]out64;
22
23
24 Memory m1 (
25     .adr25(adr25),
26     .in25(in25),
27     .r25(r25),
28     .w25(w25),
29     .out25(out25),
30
31     .adr64(adr64),
32     .in64(in64),
33     .r64(r64),
34     .w64(w64),
35     .out64(out64),
36
37     .mode(mode)
38 );
39
40 Rotate r1 (
41     .in(out64),
42     .start(start),
43     .clock(clock),
44     .done(done),
45     .reset(reset),
46     .mem_adr(adr64),
47     .mem_in(in64),
48     .mem_r(r64),
49     .mem_w(w64)
50 );
51
52 always #200 clock = ~clock;
53
54 initial begin
55     #100
56     start = 1;
57     #50000
58     $stop;
59 end
60
61
62
63 endmodule

```

addRc:

این تابع، لاین $x = 0, y = 0$ را با جدول زیر XOR می کند.

RC[0] = 0x0000000000000001	RC[12] = 0x000000008000808B
RC[1] = 0x0000000000008082	RC[13] = 0x800000000000008B
RC[2] = 0x800000000000808A	RC[14] = 0x8000000000008089
RC[3] = 0x8000000080008000	RC[15] = 0x8000000000008003
RC[4] = 0x000000000000808B	RC[16] = 0x8000000000008002
RC[5] = 0x0000000080000001	RC[17] = 0x8000000000000080
RC[6] = 0x8000000080008081	RC[18] = 0x000000000000800A
RC[7] = 0x8000000000008009	RC[19] = 0x800000008000000A
RC[8] = 0x000000000000008A	RC[20] = 0x8000000080008081
RC[9] = 0x0000000000000088	RC[21] = 0x8000000000008080
RC[10] = 0x0000000080008009	RC[22] = 0x0000000080000001
RC[11] = 0x000000008000000A	RC[23] = 0x8000000080008008

این لاین در ۲۵ لاین ورودی برابر با لاین ۱۲ می‌باشد. (لاین ۱۳ ام)

این تابع به عنوان ورودی، turn را می‌گیرد و بر حسب آن تصمیم می‌گیرد که از کدام یک از مقادیر جدول استفاده کند.

پس از XOR کردن، نتیجه را در همان لاین ورودی می‌نویسیم.

کد مربوط به addrc و تست آن را در زیر مشاهده می‌کنید.

```
1 timescale 1ns/1ns
2
3 module Addrc
4
5     input [0:63] in,
6     input start,
7     input clock,
8     input reset,
9     input [4:0] turn,
10    output reg done,
11    output reg [4:0] mem_adr,
12    output reg [0:63] mem_in,
13    output reg mem_r,
14    output reg mem_w
15 ];
16
17 integer i, x, y, final_index, lane = 0;
18
19 reg [0:63] in_temp;
20
21 reg [0:63] rc [0:23];
22
23 initial begin
24     done = 0;
25     rc[0] = 64'h0000000000000001;
26     rc[1] = 64'h0000000000000002;
27     rc[2] = 64'h800000000000000A;
28     rc[3] = 64'h8000000000000000;
29     rc[4] = 64'h000000000000000B;
30     rc[5] = 64'h0000000000000001;
31     rc[6] = 64'h8000000000000001;
32     rc[7] = 64'h8000000000000009;
33     rc[8] = 64'h000000000000000A;
34     rc[9] = 64'h0000000000000008;
35     rc[10] = 64'h0000000000000009;
36     rc[11] = 64'h000000000000000A;
37     rc[12] = 64'h000000000000000B;
38     rc[13] = 64'h800000000000000B;
39     rc[14] = 64'h8000000000000009;
40     rc[15] = 64'h8000000000000003;
41     rc[16] = 64'h8000000000000002;
42     rc[17] = 64'h8000000000000000;
43     rc[18] = 64'h000000000000000A;
44     rc[19] = 64'h800000000000000A;
45     rc[20] = 64'h8000000000000001;
46     rc[21] = 64'h8000000000000000;
47     rc[22] = 64'h0000000000000001;
48     rc[23] = 64'h8000000000000008;
49 end
50
51 always @(posedge clock, posedge reset) begin
52     if (reset) begin
53         done = 0;
54     end
55     else if (start && ~done) begin
56         mem_r = 1;
57         mem_adr = 5'd12;
58         mem_w = 0;
59         #3;
60         in_temp = in;
61         #2;
62         in_temp = in_temp ^ rc[turn];
63         #2;
64         mem_in = in_temp;
```

```

1 timescale 1ns/1ns
2
3 module tb_addrc ();
4
5 reg clock = 0;
6 reg start = 0;
7 reg reset = 0;
8 reg mode = 0; //remember to change this to 0 for 64 bit mode
9 reg [4:0] turn = 5'd0;
10
11
12 wire [5:0]adr25;
13 wire [0:24]in25;
14 wire r25;
15 wire w25;
16 wire [0:24]out25;
17
18 wire [4:0]adr64;
19 wire [0:63]in64;
20 wire r64;
21 wire w64;
22 wire [0:63]out64;
23
24
25 Memory m1 (
26     .adr25(adr25),
27     .in25(in25),
28     .r25(r25),
29     .w25(w25),
30     .out25(out25),
31
32     .adr64(adr64),
33     .in64(in64),
34     .r64(r64),
35     .w64(w64),
36     .out64(out64),
37
38     .mode(mode)
39 );
40
41 AddrC a1 (
42     .in(out64),
43     .start(start),
44     .clock(clock),
45     .done(done),
46     .reset(reset),
47     .turn(turn),
48     .mem_adr(adr64),
49     .mem_in(in64),
50     .mem_r(r64),
51     .mem_w(w64)
52 );
53
54 always #100 clock = ~clock;
55
56 initial begin
57     #400
58     start = 1;
59     #5000
60     $stop;
61 end
62
63
64

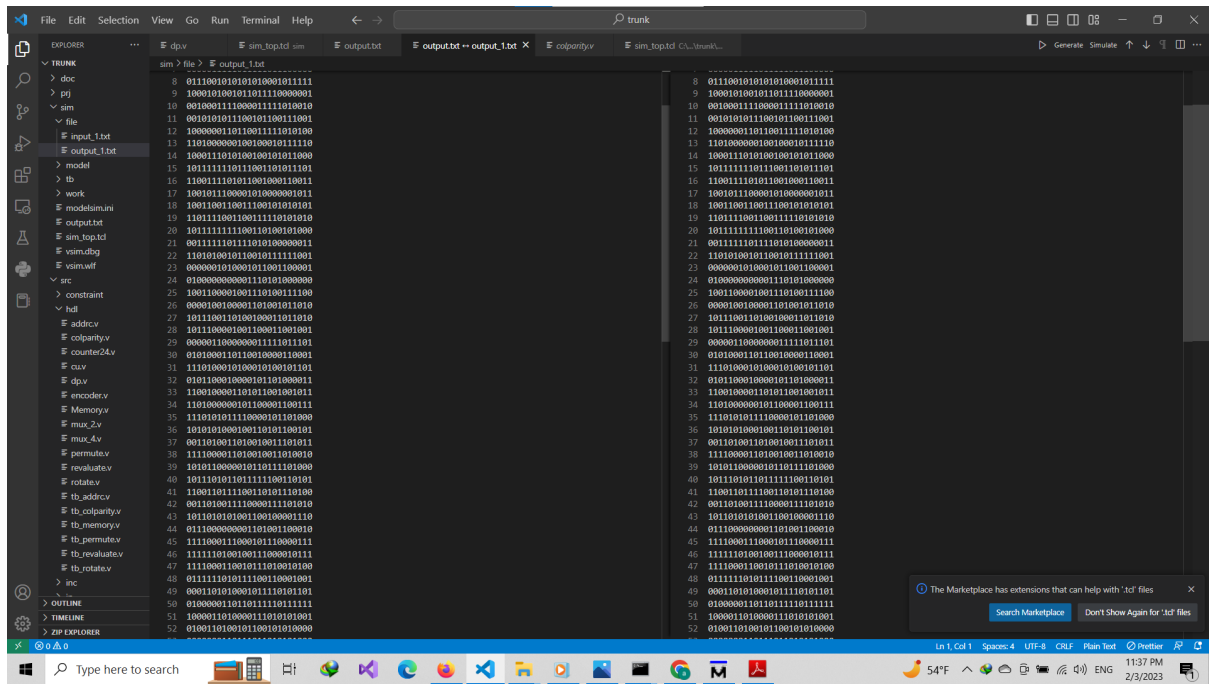
```

نتایج:

فقط کافیت تست بنچ بنویسیم و در آن سیگنال های کلاک و start را به مدل اصلی بدهیم.

در زیر می‌توانید تست بنچ و نتیجه ی نهایی پس از ۲۴ بار و اتمام پروسه و نوشته شدن نتیجه در فایل خروجی مشاهده می‌کنید که با نتیجه ی داده شده یکسان است.

```
1 0010011011001101111001100
2 0000001001110010100010101
3 1110010010100001001100100
4 000111100000111101111100
5 0001000111000011111110010
6 1011100010111011110100000
7 000001111011111011100000
8 0111001010101010001011111
9 1000101001011011110000001
10 0010001111000011111010010
11 001010101100101100111001
12 100000110110011111010100
13 1101000000100100010111110
14 100011101010010010101000
15 101111110111001101011101
16 11001111011001000110011
17 1001011100001010000001011
18 1001100110011100101010101
19 1101111001100111110101010
20 101111111100110100101000
21 0011111101111010100000011
22 1101010010110010111111001
23 0000001010001011001100001
24 010000000001110101000000
25 1001100001001110100111100
26 0000100100001101001011010
27 1011100110100100011011010
28 1011100001001100011001001
29 0000011000000011111011101
30 0101000110110010000110001
31 1110100010100010100101101
32 0101100010000101101000011
33 1100100001101011001001011
34 1101000000101100001100111
35 1110101011110000101101000
36 1010101000100110101100101
37 0011010011010010011101011
38 1111000011010010011010010
39 1010110000010110111101000
40 1011101011011111100110101
41 1100110111100110101110100
42 0011010011110000111101010
43 1011010101001100100001110
44 0111000000001101001100010
45 1111000111000101110000111
46 1111110100100111000010111
47 1111000110010111010010100
48 0111111010111100110001001
49 0001101010001011110101101
50 0100000110110111110111111
51 1000011010000111010101001
52 0100110100101100101010000
53 0000000110111011010101000
54 0011111001010011010101010
55 0101000011001011001111110
56 0100100110001100000100010
57 0000000101001100110001000
58 0010100010001011111110101
59 1001110011110010001000011
60 1100001010101001110110010
61 1111001000111110000001010
62 0111111001000110100010110
63 1100011011110010011011010
64 0100000101000011110101001
```



پایان