ECE 545
Fall 2015
Midterm Exam

Problem 1 [10 points]

Draw a block diagram of a simple microprocessor system composed of

A. Microprocessor, with the bidirectional input/output DATA (16-bits), and outputs ADDR (16 bits), WE (1 bit), CLK (1 bit)
B. 8k x 16 RAM0 visible by the microprocessor in the address range 0000-1FFF
C. 8k x 16 RAM1 visible by the microprocessor in the address range 3000-4FFF
D. 8k x 16 RAM2 visible by the microprocessor in the address range 6000-7FFF
E. 8k x 16 RAM3 visible by the microprocessor in the address range 9000-AFFF.

Assume that a memory write happens on the rising edge of the clock when WE=1, and memory read happens on the rising edge of the clock when WE=0.

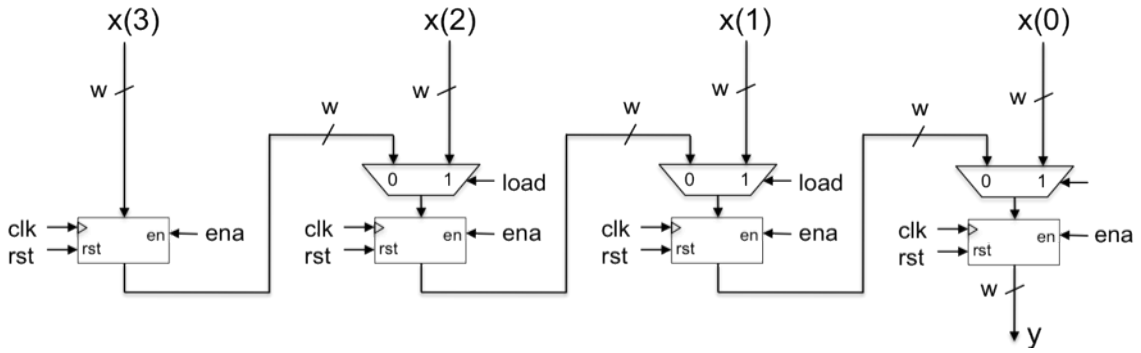
Problem 2 [15 points]

Draw block diagrams of

A. 3-to-8 decoder (with enable) built of 2-to-4 decoders (with enable) and a minimum number of logic gates
B. 5-bit priority encoder built of 2-to-1 multiplexers and a minimum number of logic gates (assume that the least significant bit of the input `w` has the highest priority, and the `z` output is equal to 1 when at least one input bit is equal to 1).
C. Variable arithmetic shift right `C = A >> B`, where `A` and `C` are 8-bit signed integers, and `B` is an 8-bit unsigned integer.

Problem 3 [15 points]

The digital circuit shown in the diagrams below is called a PISO (Parallel-In-Serial-Out) unit.



Write entity declaration and architecture of this circuit using the `for-generate` statement. Declare the size of the output bus, `w`, as a generic with the default value equal to 8. Write an instantiation of this component in VHDL-93 with the value of `w` set to 32, the input `x` connected to the bus `A`, and the output `y` connected to the bus `B`.

Problem 4 [60 points]

The key scheduling unit of the RC6 cipher is a circuit that takes a 128-bit key `K`, and converts it to 2`r`+4 round keys `S[i]`, `i`=0..2`r`+3, stored in the internal memory `S[i]`.
This unit is specified below using its

a. pseudocode
b. interface
c. table of input/output ports.

Perform the following two phases of the design process for the RC6 key scheduling unit:

1. Block diagram of the Datapath
2. Interface with the division into the Datapath and Controller

Pseudocode:
The RC6 key scheduling unit is defined using the given below pseudocode.
The input key `K` consists of four words `K[0]`, `K[1]`, `K[2]`, and `K[3]`, each of the size of 32 bits. These words are first written to the internal memory `L[j]`, `j`=0..3, using the control signal `write_key` (active high) and the key input `Kin`. This process is described using the first `for-loop` of the pseudocode. Afterwards, the remaining part of the pseudocode is executed by the controller.
`P32` and `Q32` are 32-bit constants. `r` is a parameter of RC6, with the default value of 12.

```
for j = 0 to 3 do
    while (not write_key)
          do_nothing
    end while
    L[j] = Kin
end for

S[0] = P32
for i=1 to 2r+3 do
    S[i] = S[i-1] + Q32
end for

i = j = 0
A = B = 0
for k=1 to  3·(2r+4) do
       A = S[i] = (S[i] + A + B) <<< 3
       B = L[j] = (L[j] + A + B) <<< (A+B)
       i = (i+1) mod (2r+4)
       j = (j+1) mod 4
end for
```

Notation:
`A`, `B` = 32-bit variables
`+` = unsigned addition mod 2^{32}
`X <<< Y` = rotation of the variable `X` by a number of positions given by the current value of the variable `Y`

Assume that you can use memories with the following inputs:
`ADDR`, `DIN`, `CLK`, `WE`, and the output `DOUT`,
which output data in the same clock cycle in which a new address is applied.

Writing to memory takes effect at the rising edge of the clock when `WE` = 1.

Interface:

Assume the following interface to your circuit:

Port	Width	Meaning
`clk`	1	System clock.
`rst`	1	System reset – clears internal registers.
`write_key`	1	Synchronous write control signal for the key input, `Kin`. Active high.
`Kin`	32	The key input, through which subsequent words of the key `K[0]..K[3]` are loaded to the circuit.
`n`	*m*	Index of the round key `S[n]`.
`Sn`	*w*	Value of the round key `S[n]` corresponding to the index provided through the input `n`.
`Done`	1	Asserted when the computations are completed.

m is a size of index `n`. It is a minimum integer, such that $2^m \geq 2r+4$.

Tasks & Assumptions:

Task 1: Draw a block diagram of the Datapath
Assume that

- one round of the main for loop of the pseudocode executes in one clock cycle
- you can access only one position of each internal memory per clock cycle
- after the circuit is done with computations, applying input `n` should generate value of `S[n]` at the output `Sn` in the same clock cycle.

Task 2: Draw an Interface of the circuit with the division into the Datapath and Controller.