ECE 545 Fall 2012
Final Exam

Problem 1

Develop an ASM chart for the circuit from Homework 1, described below using its

A. **pseudocode**
B. **table of input/output ports**
C. **block diagram.**

Please use ACTIONS (such as a:=a', i++, etc.) inside of your states and conditional output boxes, and CONDITIONS (such as i=63) inside of your decision boxes.

Then, create a table with translation of ACTIONS and CONDITIONS into names or expressions involving the corresponding control and status signals.

A. Pseudocode

```
h0 := iv0
h1 := iv1
h2 := iv2
h3 := iv3
last_block_stored :=0

while (last_block_stored != 1)
do
    wait until src_ready
    r := m
    last_block_stored := last_block

    a := h0
    b := h1
    c := h2
    d := h3

    for i = 0 to 63 do
        ki := k[i mod 16]
        ri := r[i mod 4]
        f := (17*ri) mod 2^8
        e := (2d+1)*f mod 2^8
        d := d' :=(4c+2)*c mod 2^8
        c := c' := b <<< 3
        b := b' := a >>> i
        a := a' := e ⊕ ki
    end for

    h0 := (h0 + a)  mod 2^8
    h1 := (h1 + b)  mod 2^8
    h2 := (h2 + c)  mod 2^8
    h3 := (h3 + d)  mod 2^8
end while

y := h0 || h1 || h2 || h3
done := 1
```

Notation:

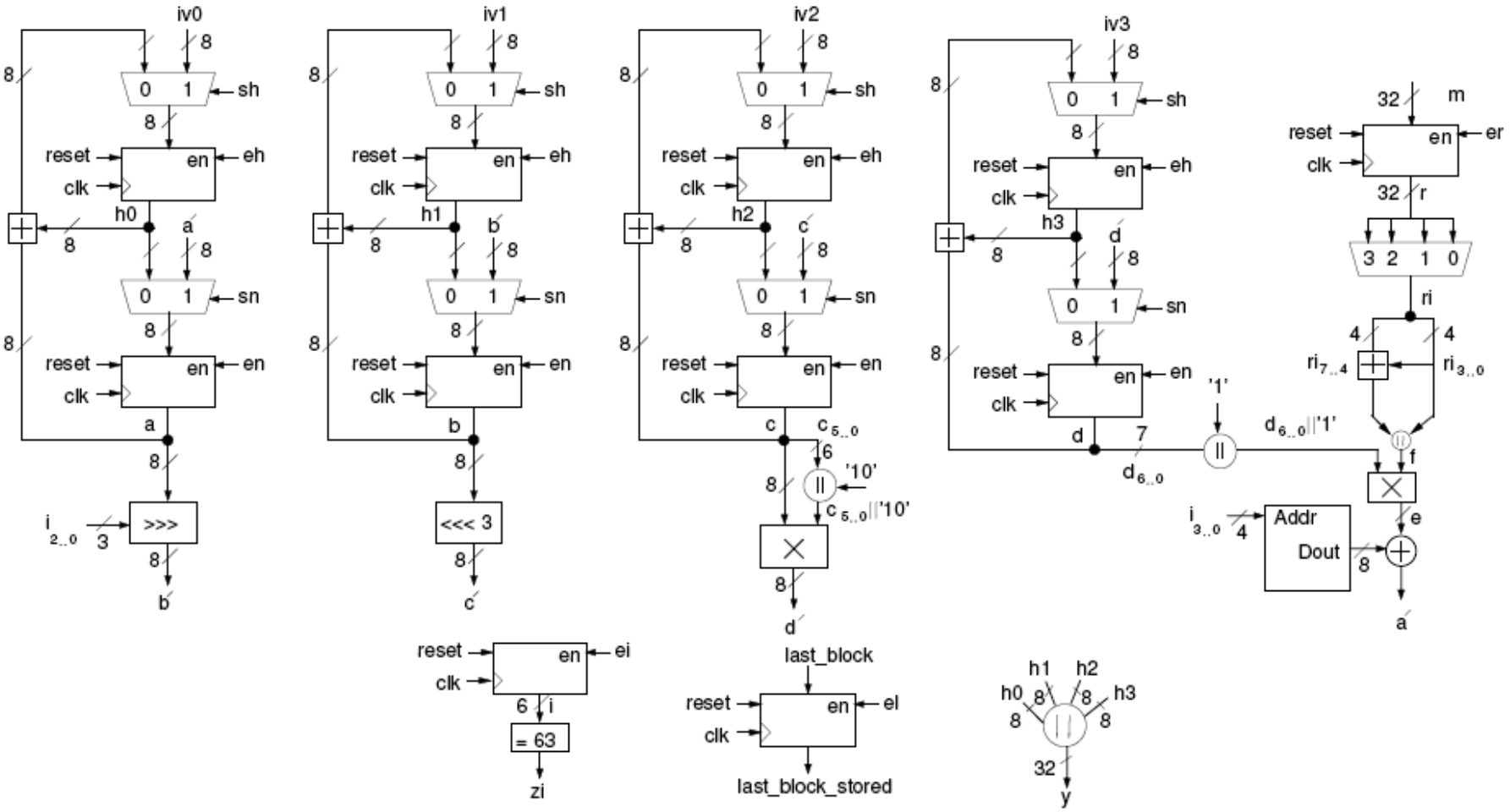
m: 32-bit message block (input)
r: 32-bit register
y: 32-bit circuit output (output)
iv0..iv3 : 8-bit initialization vectors (constants)
a..f, h0..h3, ki, ri : 8-bit intermediate values, treated as 8-bit unsigned integers
k[i] : 8-bit round constants: k[0]..k[15], stored in ROM
r[i]: bytes of the 32-bit register r, where r[0] represents the least significant byte of r, and r[3] represents the most significant byte of r.

Operations:
⊕ : XOR
X <<< Y : rotation of X to the left by the number of positions given in Y
X >>> Y : rotation of X to the right by the number of positions given in Y
X || Y: X concatenated with Y.

B. Table of input/output ports

Port	Mode	Width	Function
clk	Input	1	System clock.
reset	Input	1	Asynchronous system reset.
m	Input	32	32-bit message block.
src_ready	Input	1	Control signal indicating that the source is ready. Must remain active until source is read.
src_read	Output	1	Control signal confirming that the source was read. Active for one clock cycle.
last_block	Input	1	Control signal indicating the last block of the message.
done	Output	1	Control signal indicating that the output is ready.
y	Output	32	Output y = h0 || h1 || h2 || h3.

C. Block Diagram



Problem 2

Perform timing analysis of the circuit from Problem 1, by answering the following questions:

A. Derive formulas for

a. **Execution time as a function of the number of message blocks N, expressed in clock cycles.**

b. **Minimum Latency = Execution time for a single message block, expressed in clock cycles.**

c. **Minimum time between two consecutive input blocks (in clock cycles).**

d. **Throughput for short messages as a function of the clock period, T, and the number of message blocks N (calculated as a ratio of the total message size and the total execution time).**

e. **Throughput for long messages as a function of the clock period, T (calculated as a ratio of the message block size and the time between inputting two consecutive message blocks).**

B. Calculate values of all four parameters for T=10 ns and N=10.

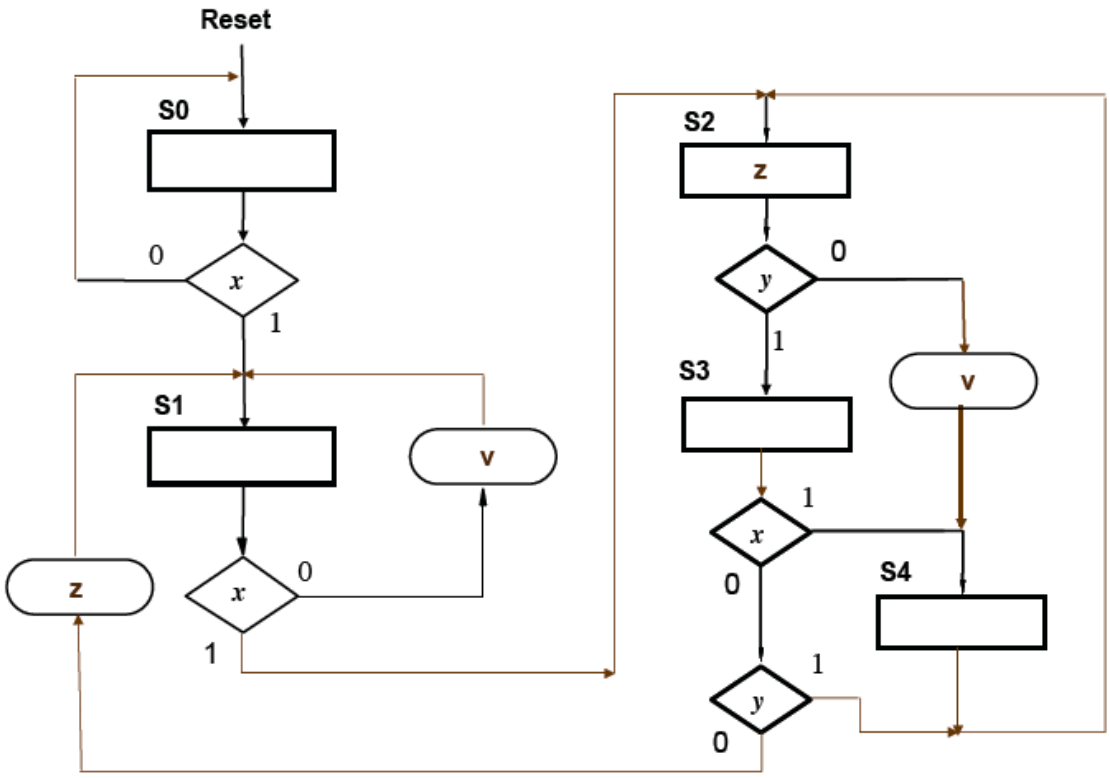
C. Identify the most likely critical path in your circuit, and mark it in your block diagram (in the answer sheet).

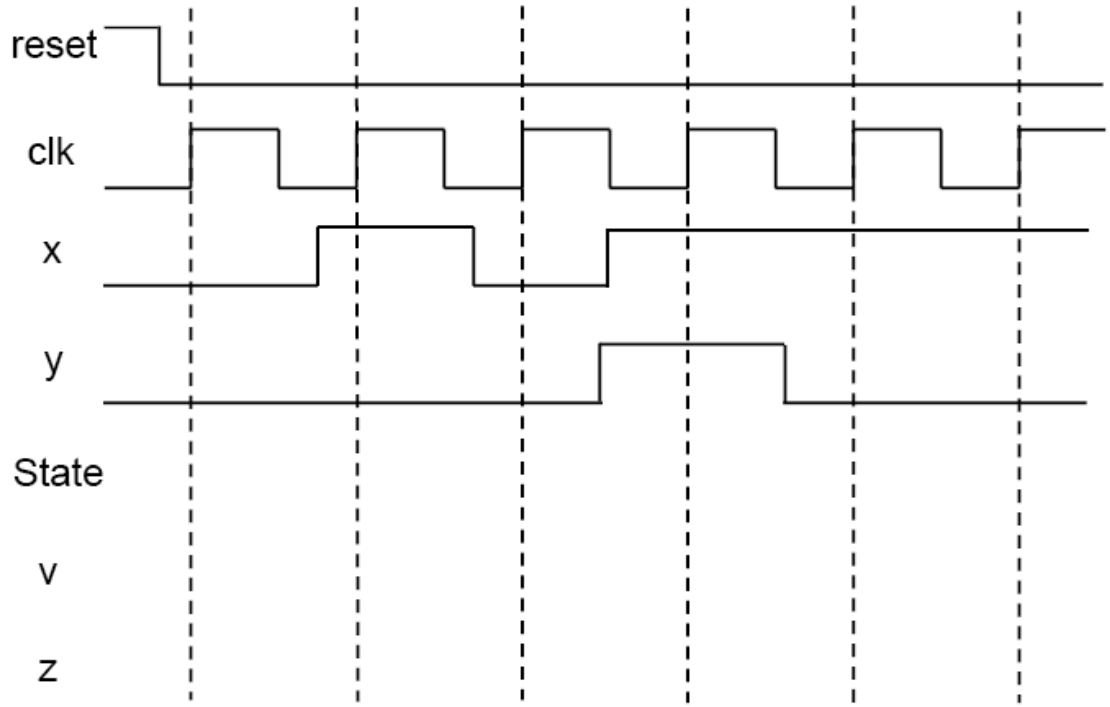
D. By how much and in what direction would the latency and throughput of this circuit changed if the clock skew between the destination register and the source register in the critical path was -2 ns (i.e., the clock signal arrived first at the source register, and only 2 ns later at the destination register)?

Justify your answer by
- drawing timing waveforms necessary to determine a new value of the clock period T', and
- providing formula for T'.

Problem 3

Supplement timing waveforms given below (and repeated in the answer sheet) with correct values of outputs v and z for the controller described using the following ASM chart:





Problem 4

Squaring of m-bit operands, $y=i^2$, can be implemented using a look-up table defined as follows:

$$\text{TABLE}[i] = i^2 \quad \text{for } i = 0 \text{ to } 2^m\text{-}1.$$

A. Determine the largest value of m, for which such a table can be built using a single Block RAM of Spartan 3 FPGAs.

Multiplication of two k-bit numbers a and x can be computed using the following dependence:

$$p = a*x = ((a+x)^2 - (a-x)^2\ ) / 4$$

B. Draw a block diagram of a circuit capable of performing *unsigned* multiplication using this dependence and the method for squaring defined above.

Obey the following requirements:

- The circuit should operate correctly for an arbitrary dependence between a and x, and an arbitrary value of k.
- Use the minimum number of adders and Block RAMs.
- Assign names and denote widths for all signals and buses in your design.
- Clearly specify the sizes of all memories you use.

Hint: A Block RAM in a Spartan 3 FPGA can be configured as dual port RAM of the size of up to 18 kbits, with different aspect ratios, i.e., different widths of the address bus vs. data bus leading to the same capacity.

Problem 5

Answer the following questions regarding modern FPGAs.

A. What are the maximum sizes of operands that can be used for an unsigned multiplication implemented using a SINGLE:
    a. Embedded multiplier of Xilinx Spartan 3
    b. Embedded multiplier of Altera Cyclone II
    c. DSP unit of Xilinx Virtex 5
    d. A half-DSP block of Altera Stratix III ?
B. How many data bits and parity bits per word can be stored in ONE
    a. BRAM of Xilinx Spartan configured to have 512 words
    b. M4K memory block of Altera Cyclone II configured to have 256 words?
C. What is a name of the hardwired microprocessor/microcontroller implemented as a part of
    a. Xilinx Virtex II Pro
    b. Xilinx new Extensible Processing Platform called Zynq?