ECE 545 Fall 2010
Exam 1

Introduction & tasks:

The SHA-1 (Secure Hash Algorithm-1) circuit is specified below using its

a. pseudocode
b. block diagram of one of its units called Message Scheduler
c. top-level block diagram
d. interface
e. table of input/output ports
f. timing requirements.

Perform the following four phases of the design process for the SHA-1 implementation:

1. **Draw a block diagram of the unit called Message Digest.**
2. **Draw interfaces between**
   a. **Control Unit and Message Scheduler**
   b. **Control Unit and Message Digest.**
3. **Write RTL VHDL code of the Message Scheduler only.**
4. **Write simple testbench for the entire circuit.**

Pseudocode:

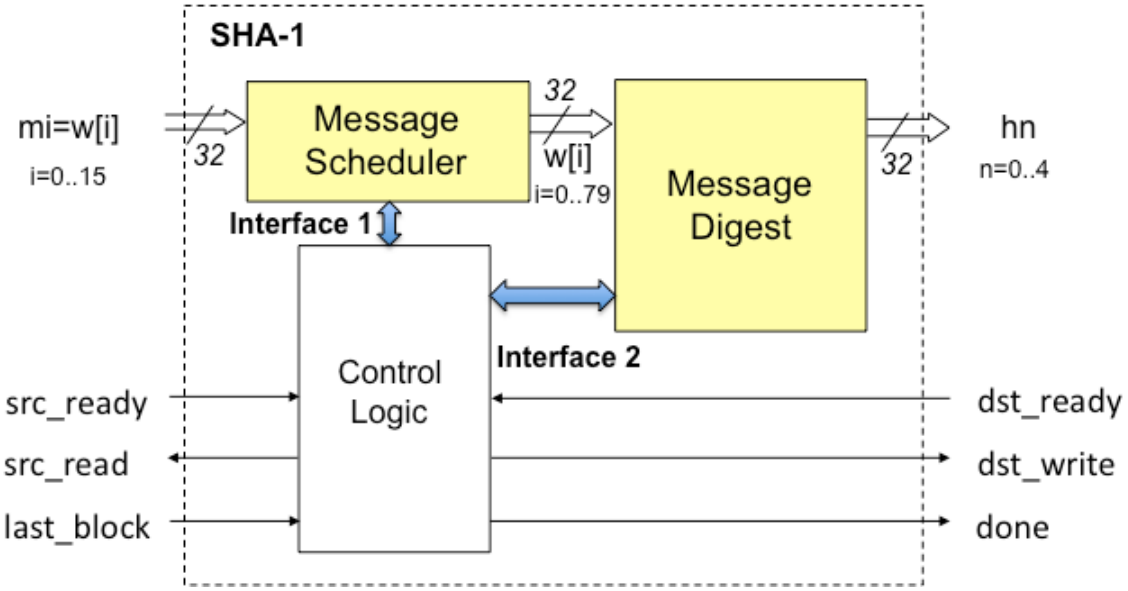
```
; Initialization - part of Message Digest
h0 = iv0; h1 = iv1; h2 = iv2; h3 = iv3; h4 = iv4;
; end of Initialization - part of Message Digest
break message into 512-bit chunks
for each chunk
    break chunk into sixteen 32-bit words w[i], 0 ≤ i ≤ 15;

    Message scheduler [given also as a block diagram]
    for i from 16 to 79
        w[i] = (w[i-3] xor w[i-8] xor w[i-14] xor w[i-16]) <<< 1
    end for
    ; end of Message Scheduler

    Message Digest
    a = h0; b = h1; c = h2; d = h3; e = h4;

    Main loop:
    for i from 0 to 79
        if 0 ≤ i ≤ 19 then
            f = (b and c) or ((not b) and d)
            k = k0
        else if 20 ≤ i ≤ 39
            f = b xor c xor d
            k = k1
        else if 40 ≤ i ≤ 59
            f = (b and c) or (b and d) or (c and d)
            k = k2
        else if 60 ≤ i ≤ 79
```

```
            f = b xor c xor d
            k = k3
        end if

        temp = (a <<< 5) + f + e + k + w[i]
        e = d
        d = c
        c = b <<< 30
        b = a
        a = temp
    end for

    h0 = h0 + a; h1 = h1 + b; h2 = h2 + c; h3 = h3 + d; h4 = h4 + e
end for
Output sequentially
   h0, h1, h2, h3, h4
; end of Message Digest
```

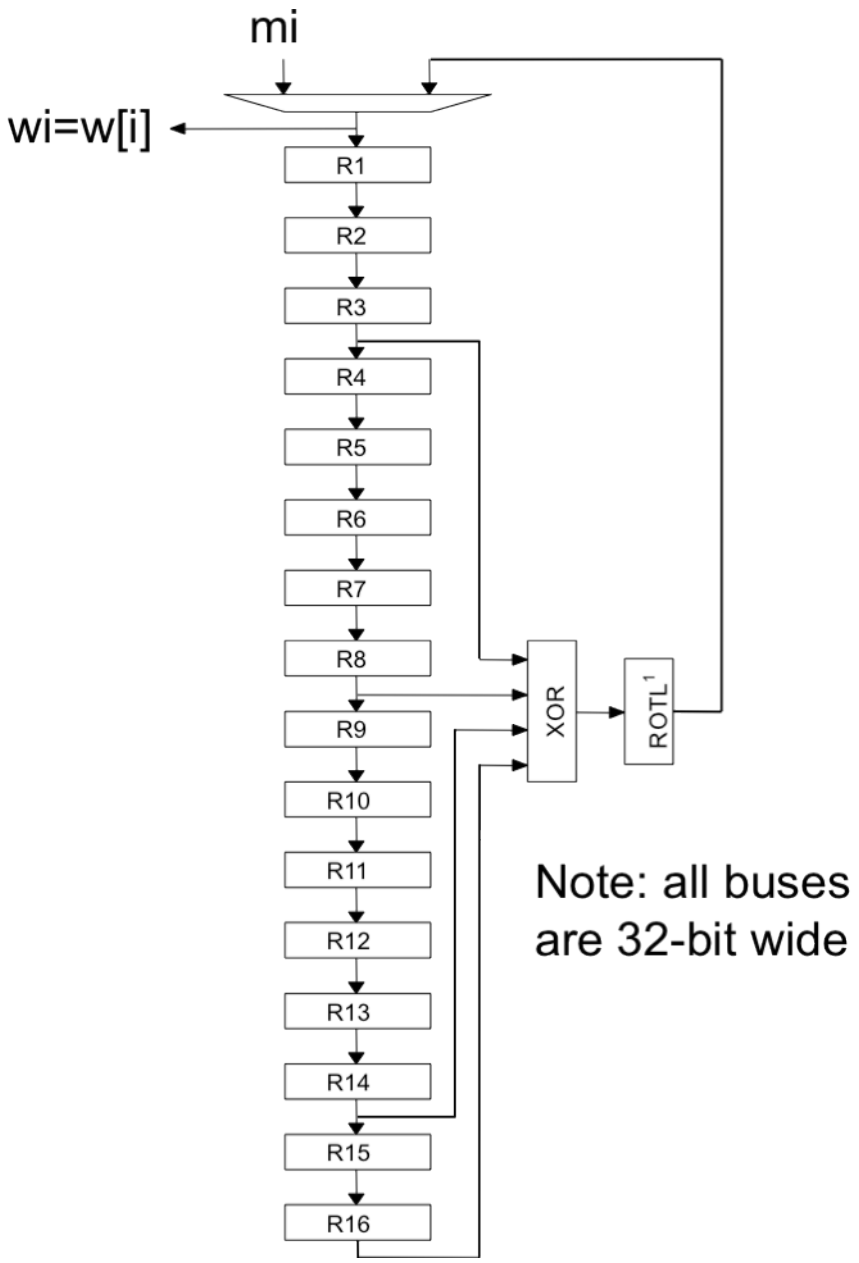
Notation:

All variables represent 32-bit words.
iv0..iv4 : initialization vector.
h0..h4 : hash value.
k0..k3 : round constants.
not : one's complement of a 32-bit word.
xor, and, or : Boolean operations on 32-bit words.
a <<< k : rotation of the variable **a** by **k** positions to the left.

Top-Level block diagram is given below:



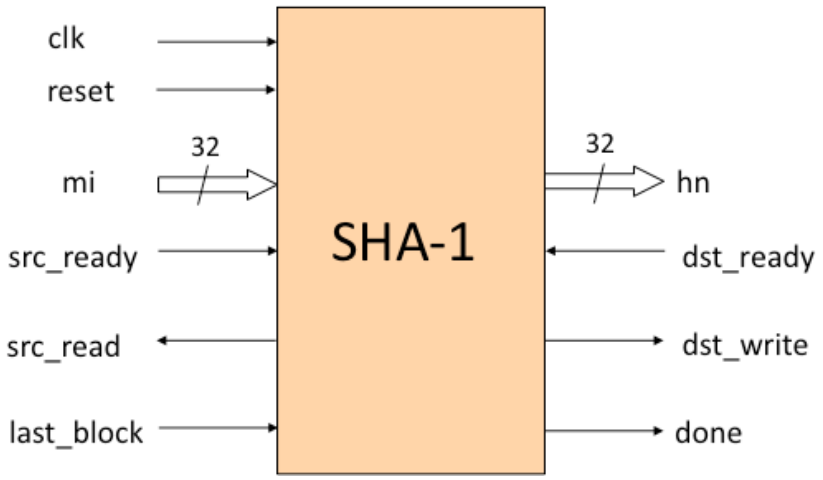
Message Scheduler is given by the following block diagram



Notation:
Rn (n=1..16) represent 32-bit registers with enable (en) and asynchronous reset (reset).
The signals clk, reset, and en are not shown in the diagram.
ROTL^1 denotes rotation of a 32-bit word left by one position.

Interface:

Assume the following interface to your circuit:



Port	Width	Meaning
clk	1	System clock.
reset	1	System reset – clears all internal register in the datapath and resets control unit.
mi	32	Message input. Message blocks are read from the source one word at a time.
hn	32	Hash value output. The hash value is written to the destination one word at a time.
src_ready	1	Input control signal indicating that the source of data is ready with the next message word.
src_read	1	Output control signal indicating reading the next message word from the source of data.
dst_ready	1	Input control signal indicating that the destination of data is ready to receive the next output word.
dst_write	1	Output control signal indicating writing the next output word to the destination of data.
done	1	Set to '1' when the entire hash value was written to the destination.

Tasks & Assumptions:

Task 1 [40 points]: Draw block diagram of the Message Digest part of the circuit only

Assume that

- **one clock cycle is used for initializations:**
  `h0 = iv0; h1 = iv1; h2 = iv2; h3 = iv3; h4 = iv4;` **[once per entire message]**
  `a = h0; b = h1; c = h2; d = h3; e = h4;` **[once per message block]**
- **one round of the main for loop of the pseudocode executes in one clock cycle; there are a total of 80 rounds.**
- **one clock cycle is used for finalization:**
  `h0 = h0 + a; h1 = h1 + b; h2 = h2 + c; h3 = h3 + d; h4 = h4 + e;`

As a result, hashing of a single message block M, consisting of 512-bits (=16 32-bit message words) should last 1+80+1=82 clock cycles. The hash value is then written to the destination circuit in 5 clock cycles.

Please clearly mark the widths and directions of all buses in your block diagram.

Please show an internal structure of the PISO (Parallel In Serial Out) circuit connected to the output hn.

Task 2 [10 points]: Draw two interfaces shown in the Top-Level block diagram

a. **Interface 1: between Control Unit and Message Scheduler**
b. **Interface 2: between Control Unit and Message Digest**

Show the names and widths of all signals forming these interfaces.

Task 3 [30 points]: Write syntesizeable RTL VHDL code for the Message Scheduler part of the circuit only.

Task 4 [20 points]: Testbench for the entire circuit

Write a simple testbench for the entire SHA-1 unit, following specified above interface, assuming that:

- **the message provided by the source circuit consists of one 512-bit block of all ones**
- **the source circuit is always ready until all message words are read by the SHA-1 unit**
- **when the last message word is read, the source circuit sets the input `last_block` to '1'**
- **the destination circuit is always ready to receive data.**