

Name: _____

CSCE 611 Final Exam

Fall 2010

Complete all parts of the exam. You are given 2 hours for the exam. This is your own effort, therefore no communication with other students is allowed. Ask any questions to the professor or the TA. All exam question sheets must be turned in along with the printouts.

“*encrypter*” – A Simple Encryption Device

You are to design a device that does a simple (if not very secure) encryption of the payload of a data packet comprised of a series of 8-bit words. The packet format is the following:

synch byte 1	synch byte 2	Length byte	data payload
1-byte	1-byte	1-byte	'length' -bytes

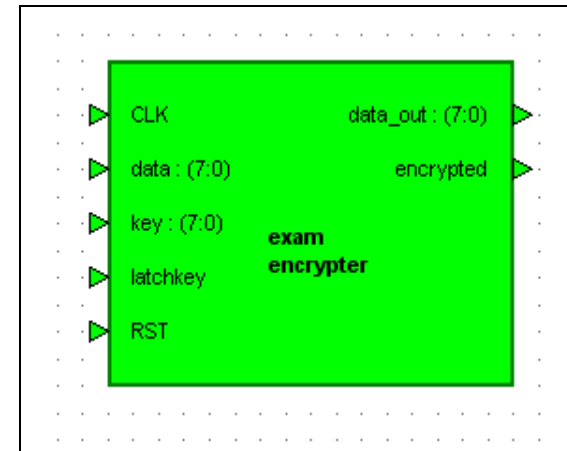
The input/output specification and corresponding symbol are shown here. **SINCE YOU WILL BE TESTING THIS DEVICE WITH SIMULATOR DATA FILES THAT WE PROVIDE, YOU MUST USE IDENTICAL NAMES (INCLUDING CASE) FOR ALL INPUT/OUTPUT SIGNALS AS WELL AS USE THE NAME ‘encrypter’ FOR THE DEVICE.**

Your device has the following **input signals** (for definitive information on the operation of the device, you must refer to the timing diagram on the next page):

- **clk** – clock input
- **data** – 8-bit bus that receives the input packet as a sequence of bytes
- **rst** – active-high asynchronous reset
- **key** – input for setting an 8-bit encryption key
- **latchkey** – input for latching the 8-bit encryption key (synchronous to clock signal)

The device will have the following **output signals**:

- **encrypted** – high when a packet’s data payload is being encrypted, low at all other times
- **data_out** – during data encryption, this is the encrypted form of the input byte; at all other times, it mirrors the input data byte



NOTES

Your device should sample the input on each clock cycle and watch for the synch characters. The synch characters signal the beginning of a new packet. Synch character 1 is “00110011” and synch character 2 is “11001100”. The length byte immediately follows the second sync byte and specifies how many bytes are contained in the data portion of the packet. The next “length” number of bytes is the data payload (which can be anything) that your device should encrypt.

Your device should output the packet with the payload encrypted and the sync and length bytes unchanged. The ‘valid’ output should be high whenever the device is sending encrypted output (see timing diagram). The output is encrypted using a simple XOR encryption protocol, computed by performing a bit-wise XOR between the input byte and the encryption key.

The encryption key can be set at any time. Typically, the key is set sometime before the input packet is sent to the device. To set the key, an 8-bit encryption key is put on the **key** input bus and the **latchkey** signal is asserted for one clock cycle. The key is latched on the falling edge of the clock.

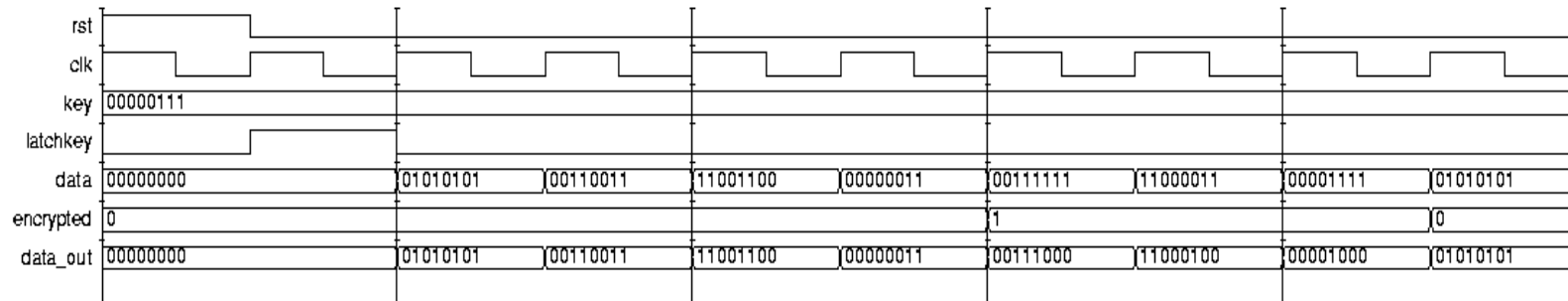
Specific Tasks:

1. Close all open libraries in the design browser.
2. Create a library called “exam” in your HOME directory. Use this library to implement your design. Name the component “encrypter” and make sure your input/output signal names match.
3. Map the library called **examlib** in your design browser. The files are located on the class volume /usr/local3rdparty/csce611 in the top-level directory.
4. You may not use any components from any library other than **examlib**. There are 2 components in this library: an 8-bit register and a subtracter.
5. Once your design is entered, compile it and start ModelSim. Within ModelSim execute the “do-file” for the test, which is located at **examlib\exam.do**. If your design is working correctly, this do-file will open a wave window and generate a timing identical to the one on the next page.

You need to turn in the following printouts:

- All design diagrams and VHDL code created by you (not the generated code).
- Any descriptive text that you think is necessary to explain your design. This can be in the form of comments added to the design files or in a separate sheet.
- Simulation waveform created by running exam.do file on your design.

Make sure your printouts are identifiable (include your name somewhere on the pages), because you will not be the only person printing on the same printer.



Good luck!