Technical Objective:

Digital communications are ubiquitous in today's connected society. We take for granted that we can just as easily communicate with somebody who is across campus as with somebody who is across the globe. Often times the information that is being transmitted is confidential and has to be protected from interception. Protection of data is known as encryption. In encryption, an encryption key is used to scramble the data prior to its transmission. Upon reception, the same key is used to unscramble the data back to its original form.

In this lab communication and encryption will be investigated. A very simple encryption algorithm will be used to encrypt a four digit pin and a communication protocol will be used to transmit the encrypted data. A receiver will also be developed to receive and decrypt the data.

TRANSMITTER

Pre-Laboratory:

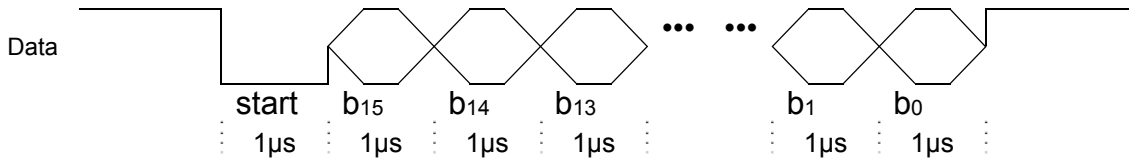
This is a partner lab. Your partner does not have to been in your lab section, but you must both be present for a signoff.

Transmitter: The transmitter works as follows

1. The user inputs a 4 digit PIN (data) in HEX using 16 switches
2. The PIN is locked in using KEY1
3. The user then enters a 16 bit encryption key on the switches
4. The encryption key is locked in using KEY2
5. The PIN is then encrypted by XOR'ing it with the encryption key
6. The encrypted data is then loaded into a 16 bit shift register
7. The shift register is then shifted 16 times (msb first) at a 1 us rate
8. The serial output of the shift register is output on a GPIO pin

A state machine should be used to enable each step of the process. A rough block diagram of the system can be found in MyCourses.

Communication Protocol: The signal that will be used for transmission will remain in the high state until a transmission is started. At the start of a transmission, the line will drop low and stay low for 1 us. After that, a new data bit will be output every 1 us. After 16 bits are transmitted, the line returns to the high state.



The transmitter should be designed for week 1prelab. This is not an easy design and you should plan on working on it prior to arriving in lab.

Procedure:

1. Simulate your transmitter design using the test bench provided. YOU MUST SIMULATE FIRST. Obtain a signoff when your simulation works
2. Assign pins and download your design to the DE2 board.
3. Verify operation of the design using an oscilloscope. Obtain a signoff for a working board.

*Note: You will not receive help for the hardware design unless the simulation is working. Debug is nearly impossible with only the hardware. The simulation will show you where the design errors are.

RECEIVER

Pre-Laboratory:

There is no prelab for the receiver.

Receiver: The receiver works as follows

1. The user enters a 16 bit encryption key on the switches
2. The encryption key is locked in using KEY2
3. The receiver then waits for the incoming data (it will 'wake up' when the data line drops.)
4. The16 bits of data are shifted into the shift register at a 1us rate
5. The data is then decrypted by XOR'ing it with the key
6. If SW17 = 1 then the encrypted data is displayed on the 7 segment displays. If SW17=0 then the decrypted data is displayed on the 7-segment displays.

Procedure:

1. Simulate your receiver design using the test bench provided. YOU MUST SIMULATE FIRST. Obtain a signoff when your simulation works
2. Assign pins and download your design to the DE2 board.
3. Using two DE2 boards verify operation of your transmitter/receiver pair. Be sure to ground the boards to each other.
4. Obtain a signoff for your work.

Signoffs and Grade

Names_____

Transmitter Simulation results _____

Transmitter Working board _____

Receiver Simulation results _____

Working encryption/decryption _____

Component	Received	Possible
Prelab		20
Transmitter Signoffs		40
Receiver Signoffs		40
	-	
Total		100

***last day for signoffs is Friday May 13, 2016 at 12 noon**