CPSC 121: Models of Computation
Lab #7: Circuit Design Option: Ciphers

Objectives

Cryptography is the study of techniques used in transmitting data secretly. It is a historically and socially significant subfield of computer science. We use cryptographic schemes frequently in day-to-day life, such as when we log in to our email accounts or when we do online banking. There is considerable variation in the security of these schemes: the encryption on your cell phone, for example, is much weaker than what is used by Statistics Canada to secure your Census data, or by the military to communicate intelligence. In this lab, you will be designing and implementing a cipher, which is an algorithm for performing encryption or decryption.

1 Prelab: Block ciphers

There are a number of ways to categorize ciphers. Two main categories come from how the encryption is done: *substitution ciphers* and *transposition ciphers*. **TODO (prelab): Define these two terms and give an example of each. Also define a *block cipher*.** Cite any sources you use to find these definitions.

1.1 Prelab: design

TODO (prelab): Research and then design a block cipher with 3-bit blocks. It can either be a substitution cipher, a transposition cipher, or a blend of the two. Provide a circuit diagram for your design. It must include at least two different circuit components (AND, XOR, MUX, Flip-flop, etc). To help you get started, here are some examples: route ciphers, Caesar ciphers, and stream ciphers. You are welcome to use any of these for your circuit but be sure to cite any sources you use in your design. *Please do not design an overly complex circuit that will take you too long to implement or to test.*

TODO (prelab): Provide a truth table for how your circuit will encrypt a 3-bit block.

1.2 Prelab

TODO (prelab): Is it possible for your encryption scheme to be decrypted? That is, given a 3-bit block that's been encrypted with your cipher, will you be able to get the decrypted result you expect? Why or why not? You do NOT have to design a circuit for decryption.

1.3 In-lab: your circuit

TODO: Implement your circuit on Logisim. Then, test it using your methods from the prelab. Record your results/observations.

TODO: Scale your circuit up to support a message one bit bigger than it currently does. Then test your circuit again using your own methods from the prelab. Record your results/observations. Show your circuit to your TA.

TODO: Does your circuit encrypt data as you expected? How well does it scale up? Write down your findings and show it to your TA.

1.4 In-lab: Cryptanalysis

Cryptanalysis is the study of techniques used in breaking encryption schemes. Much of the history of modern computers derives from the use of early computing technology for cryptanalysis.

TODO: Look up some methods used for cryptanalysis of substitution and transposition ciphers. To help you get started, consider frequency analysis, index of coincidence and brute force methods. Come up with a plan for trying to break a classmate's block cipher. Go over your plan with your TA.

We are now going to have you try to break a classmate's cipher:

1. Pick the name of a classmate of yours.
2. Convert this name into 8-bit ASCII here: http://www.roubaixinteractive.com/PlayGround/Binary_Conversion/Binary_To_Text.asp
3. Take the resulting binary string and encrypt it block-by-block with your cipher.
4. Find another group to exchange encrypted messages with.
5. **TODO: Try to decrypt the other team's message. The link above will translate binary back into text. If you are not successful at decrypting the message, figure out how, in theory, you could eventually decrypt it.** Write down your work and show it to your TA.

The ASCII table might help you in decrypting the message: http://www.asciitable.com/

1.5 In-lab: analysis and discussion

TODO (further analysis): Suppose you wanted to send encrypted messages back and forth with a friend in another room, but cannot see for yourself whether or not they are the one receiving your message.

1. **When beginning the conversation, why would you not want to start by sending your entire message into that room?**
2. **How could you determine whether the recipient of your messages is actually your friend? How could you do this using the encryption scheme? (This is known as *authentication*.)**
3. **Think of two different strategies for authentication and compare them.**

Go over your answers with your TA.

2 End of Lab Survey

TODO: To help us improve these labs both this term and for future offerings, complete the survey at http://www.tinyurl.com/cs121labs.

A Challenge problem

TODO (challenge): Read up on the the cryptographic scheme known as the *one-time pad*, which Wikipedia describes as "impossible to crack if used correctly". What is meant by this? How is it theoretically impossible to crack? What does proper use require, and is this practically possible?

B Marking scheme

All labs are out of ten marks, with two marks for prelabs, and eight marks for in-lab work. In more detail:

- Two marks - Prelab questions
- Five marks - In-lab questions. It is one mark for your results, one for scaling up, one for results; two for the cryptanalysis section.
- Two marks - Further analysis questions with more than one sentence of work. (TAs at their discretion may occasionally award these marks for detailed analysis seen in other parts of the lab.)
- One mark - End of lab survey.

TAs may at their discretion award one bonus mark, such as for completing a challenge problem. It is expected that most students will achieve 6-8. If you feel you're heading for 0-5, **get immediate help from the TAs!**