Midterm Part II

CS59

November 3, 2024

Question 1 - Arm assembler and debugging

You have received a program called "**state02**"; it should be in your home directory under

CS59/VirtualMachine/VM_Shared_Directory

on *thepond*. This will allow you to access the file through the QEMU virtual machine under the **/mnt** directory. If you did not get an executable, let Pete Brady know as soon as possible. The operation of the virtual machine is the same as in Homework 1.

This program will ask for four words, one word at a time. **Hint**: each word is lower case, no special characters or spaces. Execute the program, enter each word when prompted, and a plaintext token will be returned to you. If you type in an incorrect word, the program loops back to word 1.

You will need to turn in the following for Question 1:

1. Explain the encryption method used in the program.
2. Explain the method you used to arrive at that conclusion.
3. Provide the returned plaintext token.

Question 2 - Elisp disassembly and coding

A DNA codon table is used to translate a genetic code into a sequence of amino acids, in this case a triplet of nucleotide bases that make the amino acids. There are four nucleotide bases that make up each amino acid, each with a letter: **T** (thymine), **C** (cytosine), **A** (adenine), and **G** (guanine). For example, the code for glutamine is CAA.

For part 1 of this question, you've been given a byte-coded Elisp file called **recog1.elc** in your home directory under **CS59** on *thepond*. Use the Elisp disassembler to figure out which codon will return true (a "t"), and all other codons will return a "nil".

For part 2, take what you learned about recog1.elc and create a source Elisp file that parses not only the one codon you found, but also will return true for the two codons for aspartic acid, GAT and GAC.

Once you are in an interactive lisp window in emacs, you can use (load "recog1.elc") to load the code and (recog-dna "TTT") to run the command to see if your codon is correct. (Hint: TTT is not the correct codon!)

You will need to turn in the following for Question 2:

1. Explain how recog1.elc works.

2. What amino acid does it recognize? The triplet of nucleotides and which amino acid (you should be able to easily find that online.)

3. Provide the elisp source code for part 2. It will be tested to see if it works correctly.

Question 3 - Capture the Flag

You will find a byte-coded file called **pl-mystery.elc** in your home directory under **CS59** on *thepond*. If you open this up in emacs on *thepond* (**very important**, this is done on *thepond* and not anywhere else (natively on the pond, NOT in the VM)) you can try to find your secret. (Reminder to load emacs byte code, open an emacs buffer in lisp interaction

mode, and then run the command "load-file" (you can use M-x to execute a command) and give it pl-mystery.elc)

Execute: (get-the-secret)

If you haven't done anything at all, it will give you the message "Speak 59 and Enter!" You will have to look through the bytecode to try to understand what you need to do in order to have it give you your secret! Hint: try (disassemble #'get-the-secret) to start.

You will need to turn in the following for Question 3:

1. Write down the necessary steps to get the flag.

2. Provide the secret flag.

Good luck!!

Terms and Conditions

This midterm is open-book, open-shell, open-Internet (in your submission, make note of the resources you used). You are allowed to discuss tools and techniques with your classmates (please, make a note of your discussion). The one rule you must abide by is **do not disclose actual solutions or their parts**.

Midterm Part II is due by midnight, **November 10th, 2024**. **Do not** wait until the last minute to start this work; it should not be difficult but may take more time than you realize.

Please email your results to Pete Brady (jpb@cs.dartmouth.edu) for grading.