ECE 3894 Lab 1

Josh Moore, jmoore344@gatech.edu, 903112555

Samuel Yeomans, syeomans3@gatech.edu, 902857613

1. Submit all the code (C code and VHDL files) with in-line comments pointing out the modifications you did in the files.
    a. See attached in des_c and des_vhdl
2. The dump file sim_results.vcd of the simulated design.
    a. See attached in top level folder
3. The exported waveform image of the simulated design.
    a. See attached in top level folder
4. Brief explanation of the modification that you did to the main function and to the VHDL testbench.
    a. Main function in C: We set up file I/O to read two files: key.txt and plaintextin.txt. As the function reads key.txt line-by-line in an outer for loop, it reads plaintextin.txt line-by-line in an inner for loop. Executing the existing main function inside the inner for loop, we placed each line of key.txt into the variable “key” and each line of plaintextin.txt into the variable “x”. From there, we printed the output of the DES implementation to the necessary output files as ASCII characters in addition to the existing print statements that output to the console. On the note of our output files: we chose to open them to append as opposed to write, so if you want to run our code again, you’ll want to delete all plaintextout and ciphertextout files before you run it.
    b. VHDL: We changed the testbench in VHDL to match our eighth test case for the third key. The third key was selected (after checking against the known bad keys) to be “jumpoffs” in ASCII (6a756d706f666673 in hex), and our plaintext was a random 8-letter word, “pizzeria” (70697a7a65726961 in hex). The simulation waveform showed an encryption of “pizzeria” using the key “jumpoffs” and decrypted it to the original plaintext. This matched what we saw in our C code, proving the implementation of DES is correct.
5. Simulation results compiled into .txt files as described in Section III showing all keys, plaintext and ciphertext values.
    a. See attached in top level folder
6. Waveforms in the lab report verifying one encryption testcase and one decryption testcase in Section III for key3 only. Please provide a text file called "Waveformskey3.txt" with the specific values of the input plaintext and input ciphertext chosen for the waveforms.
    a. See attached in top level folder