Lab 2 Report: Triple DES

Josh Moore, 903112555, jmoore344

Samuel Yeomans, 902857613, syeomans3

1. Submit all the code (C code and VHDL files) with in-line comments pointing out the modifications you did in the files.
    a. Included in folders des_c and des_vhdl

2. Brief explanation of the modification that you did to the main function and to the VHDL testbench.
    a. C: We modified the main function in C to read three keys at a time and encrypt plaintext with keys 1, then 2, then 3. For decryption, the script uses key 3, then 2, then 1. At the end of each encryption/decryption, the script writes the output to a file.
    b. VHDL: We modified the test bench file by making each plaintext go through three rounds of encryption and three rounds of decryption. We decided to do this by hard coding all the necessary values, however we quickly discovered this required an unreasonable amount of code. To handle this, we wrote a Python script (scratch.py) to generate the VHDL code for us.

3. Simulation results compiled into .txt files as described in Section III showing all keys, plaintext and ciphertext values.
    ✓ Keys.txt (5 sets) *Note: this file is 15 lines. Each group of 3 lines is one set.*
    ✓ Plaintextin.txt (10 plaintext test cases)
    ✓ Ciphertextout1.txt (10 ciphertext from using set1 and the plaintextin.txt)
    ✓ Ciphertextout2.txt (10 ciphertext from using set2 and the plaintextin.txt)
    ✓ Ciphertextout3.txt (10 ciphertext from using set3 and the plaintextin.txt)
    ✓ Ciphertextout4.txt (10 ciphertext from using set4 and the plaintextin.txt)
    ✓ Ciphertextout5.txt (10 ciphertext from using set5 and the plaintextin.txt)
    ✓ Ciphertextin.txt (10 ciphertext test cases, please pick two ciphertext outputs from each of the ciphertextout.txt (ciphertextout1.txt, ciphertextout2.txt...ciphertextout5.txt)
    ✓ Plaintextout1.txt (10 plaintext from using set1 and the ciphertextin.txt)
    ✓ Plaintextout2.txt (10 plaintext from using set2 and the ciphertextin.txt)
    ✓ Plaintextout3.txt (10 plaintext from using set3 and the ciphertextin.txt)
    ✓ Plaintextout4.txt (10 plaintext from using set4 and the ciphertextin.txt)
    ✓ Plaintextout5.txt (10 plaintext from using set5 and the ciphertextin.txt)

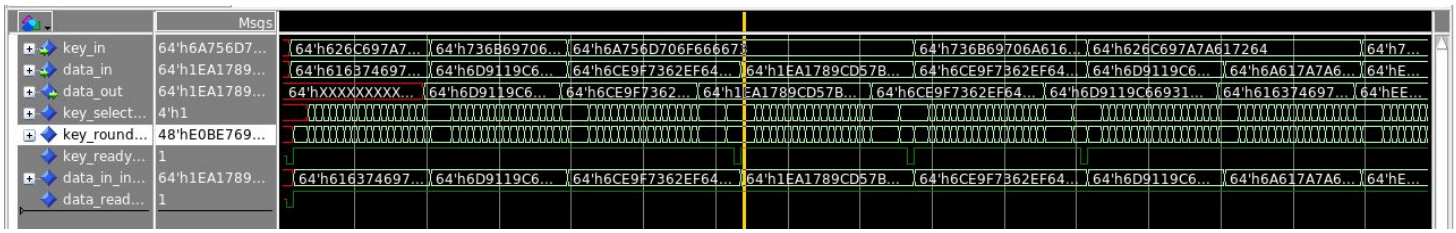
4. Answers to questions in section IV.
    a. A generic definition of throughput is an amount of something per unit time. Please write down what is your VHDL implementation's throughput for (1)a triple-DES encryption and (2)a triple-DES decryption. Please also indicate the clock period of your design.
        i. The clock period of our implementation was 10 ns. Due to this, our throughput for both three rounds of encryption and three rounds of decryption were the same at approximately 639 ns (based on the waveform image).
    b. Just like software programming, there are multiple ways to implement a hardware function. Please describe one other way(different from your own implementation) to

implement Triple DES's encryption and decryption algorithm that may or may not result in the same throughput.

i. Our implementation performed three encryptions to encrypt and three decryptions to decrypt. Another implementation of triple DES encrypts, decrypts, then encrypts again for encryption; and vice-versa, decrypts, encrypts, then decrypts for decryption. This implementation and ours both perform the same operations, but in different orders, so they have the same throughput.

5. The dump file sim_results.vcd of the simulated design.
    a. Included in folder des_vhdl

6. Waveforms in the lab report verifying one encryption testcase and one decryption testcase in Section III. Please provide a text file called "Waveformskey.txt" with the specific values of the input plaintext, ciphertext and keys chosen for the waveforms. Please make sure the values shown on the waveform is legible.



Yellow cursor shows where DES switches from encryption to decryption. The value of data_out displayed by the cursor is the final decrypted value. Note the original encryption input matches final decryption output. This image is really small, so it has been included in the turn-in document.

a. Waveformskey.txt included in parent folder