Homework 4 (5%) Due: 2:00 PM (NYC Time), Nov 11 2022

"Simple Function" RC5 Encode and Decode Designs

Overview

In this assignment, you will design and put together all the components required for RC5 inversion.

Task:

- Throughout the lectures you have been taught about the various building blocks of RC5 (a.k.a., the simple function, rotations, ROMs, etc.). Using the lecture notes as a starting point:
    - **Draw** the datapath for the "Simple Function" (RC5) and its inverse
        - Use professional diagram software (e.g. https://draw.io)
        - The design should have the following I/O:
            - Input clk, input rst, input d_in (64 bits), output d_out (64 bits)
        - Use the Skey ROM from the slide deck
    - **Implement** and **simulate** BOTH the ENCODE and the DECODE design
        - You must design a comprehensive testbench that includes file I/O (using Verilog's built-in functions or VHDL's textio packages) where you encode/decode at least 100 plaintext/ciphertext combinations
            - (Note: We will provide a script which encodes inputs so that you can test your equivalences)
        - Your design should be a multi-cycle implementation (i.e., at least one clock cycle per round of the "for loop")
    - You should use Verilog and VHDL - make either encode or decode using one language, and use the other language for the other

- You might choose to refer to Rivest's original paper to help support your implementation: https://people.csail.mit.edu/rivest/Rivest-rc5.pdf

- **Write** a short (2 pages max.) report describing your design process. Justify your code and relate it to your datapath design. Justify your testbench, and describe how it covers all possible execution scenarios.

Deliverables:

1. Submit a zip file of your complete Xilinx project which includes your VHDL or Verilog files and a PDF report explaining the design and including your diagrams.
2. Upload a video to YouTube or your NYU drive, submit the link to that video in brightspace (in your PDF report)
    - Video can be 3 minutes max.
    - Explain the simulation of your design, including
        - A run through of your design working correctly
        - Explanations of interesting/important test cases
        - (Recommended: Perform the recording using the free OBS software)