# Digital Circuit Lab — Lab 2 User Manual

## RSA Decrypter

Date: 04/12/2017

Team 05 Member: 郭子生 b03901032、曾耕森 b03901154、楊其昇 b03901101

Github: https://github.com/awinder0230/Digital-Circuit-Design-Lab

- **Usage**

  A step-by-step guide of using the RSA256 Decrypter.

  1. Clone our codes from Github
  2. Connect the FPGA to your computer by cable. Note that you must have driver installed to your computer.
  3. Open Quartus II and click "Tools → Programmer".
  4. Click "Hardware setup" and choose the FPGA board connected to your computer.
  5. Click "Add file", select "DE2_115.sof" under directory "output_files".
  6. Choose mode "JTAG" and click "Start" to write the program to the FPGA board.
  7. Connect the RS232 cable to your computer and the FPGA board. Note that you must have the driver of the cable installed to your computer.
  8. Find the name of the port that is connected to the FPGA board. On windows, go to Device Manager and check the Ports section.
  9. On command line, change your directory to "pc_sw/".
  10. Type "python rs232.py [name_of_your_port]" and press Enter.
  11. The decoded "dec.bin" should appear in the pc_sw directory.
  12. Note that you must press reset(KEY_0) on the FPGA board before you run the decoding program every time.

- **Simulation**

  1. Premise: to run simulation, you should have the permission to access NTU DCLab server.
  2. Connect to DCLab work station.
  3. Type "tool 2" to enable verdi, ncverilog, and nWave.
  4. Change directory to where your code stores.
  5. To test Rsa256Core, type "ncverilog + access + r tb.sv Rsa256Core.sv". The result of "dec" and "gold" should be the same. If not, you can use nWave to check your waveform and debug.
  6. To test Rsa256Wrapper, type "ncverilog + access + r test_wrapper.sv PipelineCtrl.v PipelineTb.v Rsa256Wrapper.sv Rsa256Core.sv".