CSE 563 Final Project Milestone 1 Report

Chris Barnes, Eric Neblock, Linghan Zhu

April, 25, 2020

List of Figures

1 Overview

The goal of this project is to design and layout of a modified RSA algorithm to encrypt a single byte given an encryption key. In addition, we are to test how fast we are able to run our chip and provide an analysis.

2 Block Diagram and Timing

As an idea, we present the following Block Diagram and Timing Diagram1 to illustrate how we expect the process to play out.

From our timing diagram1, we have a constant clock as well as an enable line. When Enable is high, our process moves along a pipeline each clock cycle until completion where our output becomes valid. The various Key# represent the different bits of the input key, likewise for Input and Output, with high being a logic 1 and low being a logic 0.

From our block diagram2, we have several stages as explained:

1. Key generation to $Shift(P10)$ and $Shift_3(P(10))$
2. Key generation finish
3. $P(IP)$
4. $EP(R)$
5. $EP(R) \oplus key1$
6. $SBoxes(EP(R) \oplus key1)$
7. $P4(SBoxes(EP(R) \oplus key1))$
8. $SW(EP(R) \oplus key1)$
9. $EP(R)$
10. $EP(R) \oplus key2$
11. $SBoxes(EP(R) \oplus key2)$
12. $P4(SBoxes(EP(R) \oplus key2))$
13. $IP^{-1}(R, L)$
14. Put it out on the line.

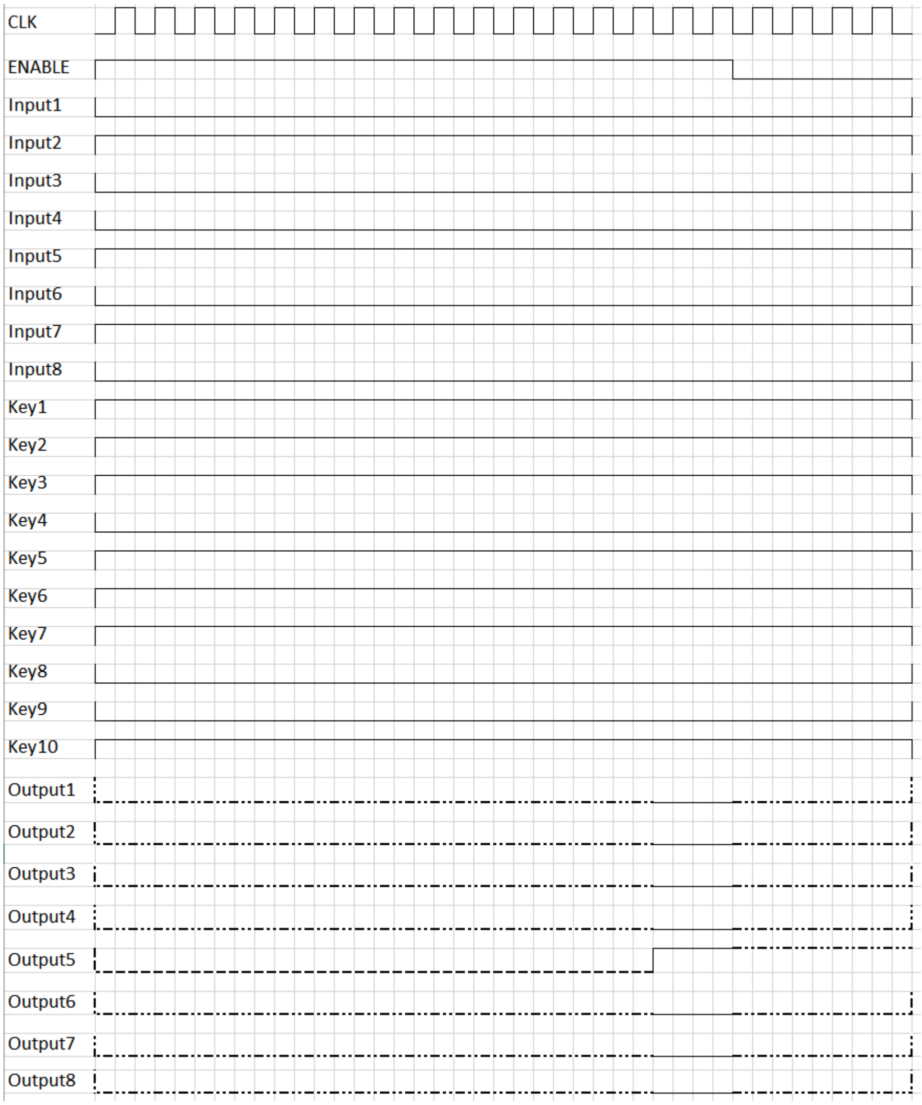

Figure 1: Expected Timing Diagram

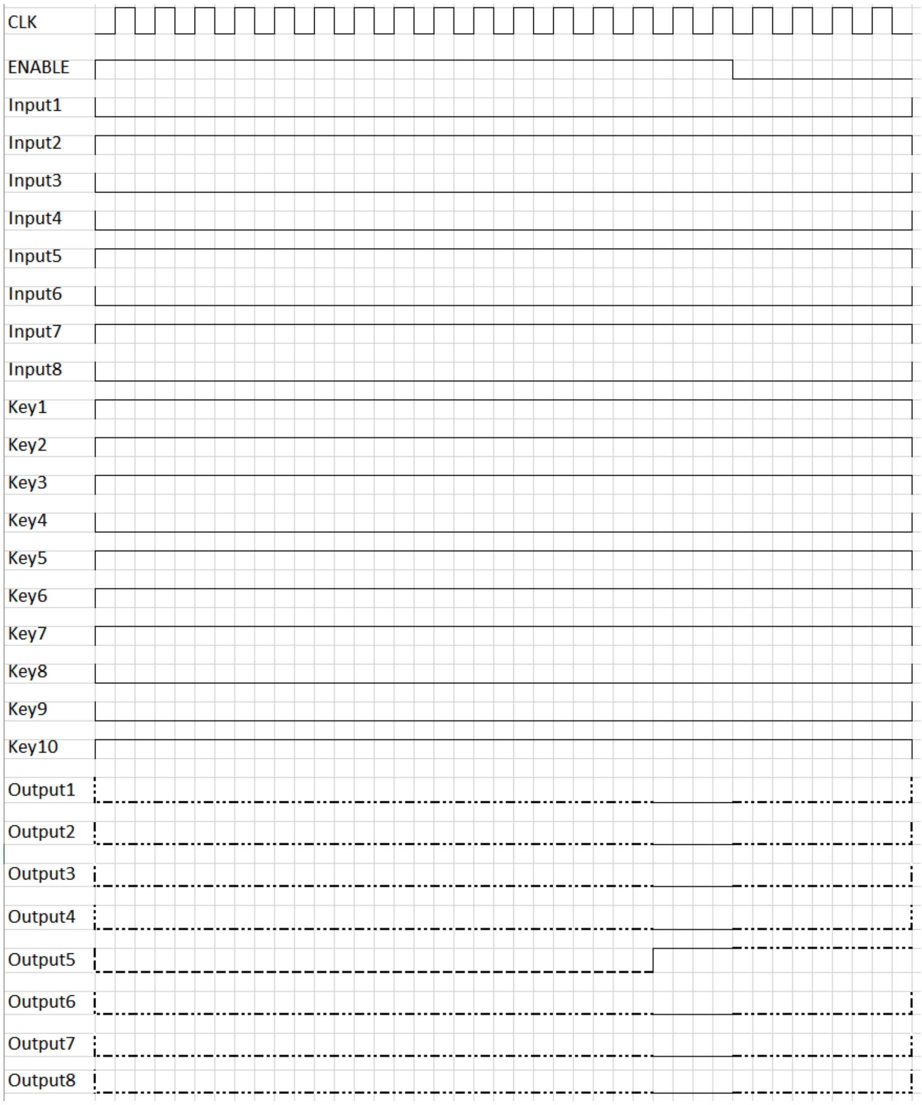

Figure 2: Expected Block Diagram