ELL305 Computer Architecture
Assignment 2
Implementation of Cryptographic Ciphers

Anshul Yadav (2017EE10565)

October 16, 2019

1 Analysis and Justification of Design

- While loading the inputs to the RAM (containing 5 inputs) using the terminal, we used a 3 bit counter whose value decides the address bit of the RAM and the corresponding value in RAM is stored in a register enabled using a decoder.
- The clock is replaced with a constant after completion of desired no. of iterations (32 in case of main circuit and 8 in the case of loading RAM) using the carry bit of the counter which becomes 1 after the counter reaches its maximum value.
- We designed an input splitter which converts the 16 bit MSB format to 16 bit LSB format as our circuit assumes format which has 32 bit MSB.
- We use an AND gate to provide clock with the main circuit which AND's the carry bit of RAM counter and clock making clock available to the main circuit only after all the inputs are loaded.
- The select bit of MUX is simply an OR of all the bits of the main counter which is zero only at the beginning of the counter. The OR then remains 1 till the counter reaches 31 and the MUX selects the feedback.
- While providing feedback we have observed that it induces apparent oscillation error. We tackled this using a register in the feedback loop.
- We designed the P-Boxes using a 16bit P-Box which we are using to make 32-bit P-box and 64-bit P-box.
- We designed S-box using Combinational analysis of input and outputs. The 13-bit shifter is simply designed using rearrangement of bits using Splitter tool.
- We required an extra circuitry to display only the final output. A halt pin is required to stop the circuit's output on the terminal which is simply an output pin labelled as halt. It remains at 0 and becomes 1 to halt the further execution. We simply use a MUX to output only when the counter's carry bit becomes 1 i.e. after the completion of 32 iterations.