2017EE10505 Yash Singla ELL305 Assignment 2

Present Cipher

1. I have made Sbox with help of Multiplexer
2. Then I have made S layer and P layer in same 1 file by using splitter and then combined accordingly
3. Then I have made Key transform using splitter and taking 80 bit as input and also provided it with counter
4. Then I have done all the assembly of above three files as per the design of Present cipher with help of Mux,Nand gates,OR gates and provided counter to run 31 cycles with clock as input to it and halted after we completed the 31 cycles
5. Then I taken 5 ram and provide it with addresses with help of constant feature and then it takes input at first cycle (actually we are delaying the present cipher clock by 1 clock only).It helps in loading data and after 31 cycles of completion we get our required output.

ESF Cipher

1. I have made Sboxes(8 sboxes) with help of Multiplexer .
2. Then I have made S layer and P layer in same 1 file by using splitter and then combined accordingly.It is our F block which takes input of XOR of Rightmost 32 bit and 32 bit of round key.
3. Then I have made Key schedule using splitters and taking 80 bit as input and also provided it with counter as per the procedure
4. Then I have done all the assembly of above three files as per the design of ESF cipher with help of Mux,Nand gates,OR gates and provided counter to run 31 cycles with clock as input to it and halted after we completed the 31 cycles
5. Then I taken 5 ram and provide it with addresses with help of constant feature and then it takes input at first cycle (actually we are delaying the present cipher clock by 1 clock only).It helps in loading data and after 31 cycles of completion we get our required output.

   How I have taken my ram input?

   Ans. I give all input to our ciphers in one clock cycle only so I taken 5 ram(3 for key and 2 for plaintext of 32 bit).Then also we wants our clock to be delayed by 1 clock cycle which is going as input to ciphers so I have taken counter which can delay by 1 clock cycle and then provide with splitter to take value of 1th clock.