University of Maryland Baltimore County
CMPE/ENEE 691
Hardware Security
Spring 2023

Hw3: Advanced Encryption Standard (AES) Due Date: 03/07/2023

Deliverables

1. A .zip file containing your source code and testbench (.v and/or .vhd files). Your testbench code should read the input from in.txt and print the output in the out.txt.

a)

In this lab, you are to implement the rounds 9 and 10 (only encryption) of the Advanced Encryption Standard (AES) as shown in Figure 1, and a testbench to simulate your design. Your source and testbench files should be written in Verilog or VHDL. **Assume that the key in the input file is the key of round 9** and then you implement key scheduling algorithm and extract key of round10 from that algorithm to feed your second round in this implementation.

b) In your code for part *a* instead of using the Irreducible polynomial as f(x)= $x^8+x^4+x^3+x+1$, deploy the following polynomial f(x)=$x^7+x^5+x^3+1$.

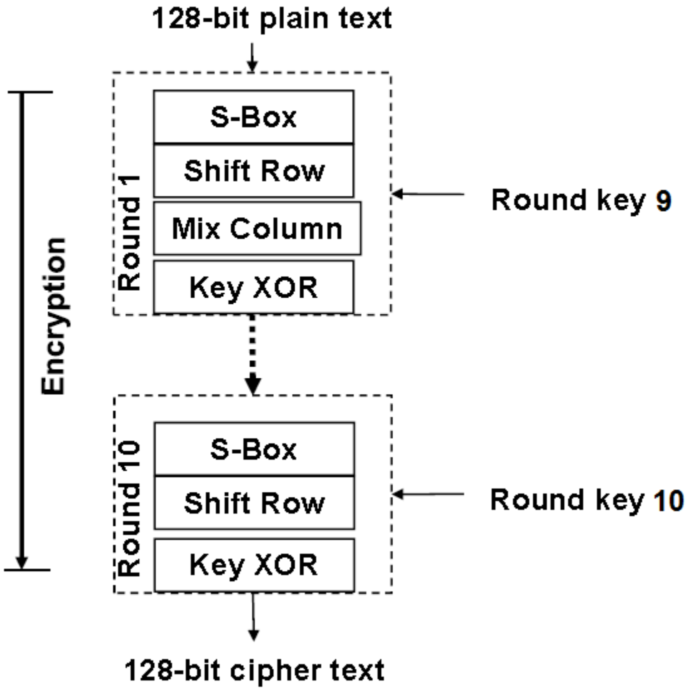
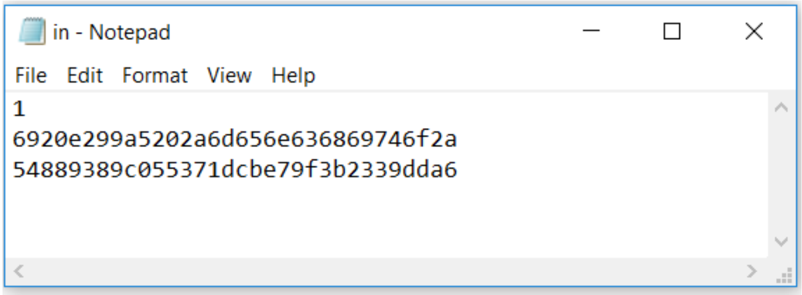


Figure 1: Last 2 rounds of AES. Note that round 10 does not include a “Mix Column” Operation.

Your testbench should read an input file called “in.txt”. The first line includes a binary value. If the value is ‘1’ the AES encryption (part a) is running. While if the value is ‘0’, the modified AES (the AES with the new polynomial given in part b) is running. The second line includes the key (in hex) and the third line includes the plaintext (in hex). Figure 1 shows a sample input file.

Note that Figure 1 is an example. Your code should be able to read any text included in “in.txt” and perform encryption accordingly.

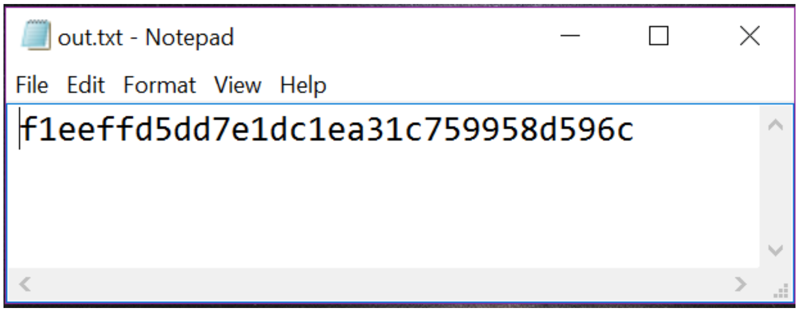


```
1
6920e299a5202a6d656e636869746f2a
54889389c055371dcbe79f3b2339dda6
```

Figure 1. Input Data File

The testbench should write the output string (ciphertext) in to an output data file called “out.txt”.

Figure 2 shows a sample output (this is only a sample output and it is not the output of Fig.1)



```
f1eeffd5dd7e1dc1ea31c759958d596c
```

Figure 2. Output Data File

Note that the file called “sbox.txt” includes the S-box table you need for encryption.

Bonus:

You can get 15 point extra, if you implement the 10-round AES for both parts a and b. Please note that you get the bonus if the 10-round implementation works correctly.