Project: AES Secure System Design

Introduction

In the final course project, we will design and implement an AES encryptor. One thing to note is that the requirements clearly stated in this document are only basic requirements, and any feature additions and performance improvements will result in extra points for you. You can find all the information about the algorithm in the attachment, which is not covered in this document.

Object

1. There are six functions that need to be implemented:
   a) 128-bit AES encryption
   b) 192-bit AES encryption
   c) 256-bit AES encryption
   d) 128-bit AES decryption
   e) 192-bit AES decryption
   f) 256-bit AES decryption
2. Complete 1.a) 128-bit AES encryption and pass post-synthesis timing, get **45** points. If you cannot complete this work, you will get no more than **40** points based on the work that has been completed. You can still get scores for other parts.
3. **7** point **bonus** are awarded for each additional functions with behavior simulation pass.
4. **3** point **bonus** are awarded for each additional function with post-synthesis timing simulation pass.
5. You need to complete a set of testbench to test the functions of AES entity. This test should at least include the four steps:
   a) reading the test case and send to the unit under test (UUT)
   b) capturing the output from the UUT
   c) comparing the output with the reference result
   d) obtaining the number of failuresthe pass rate.
   【Remark: You can use other languages to write scripts for auxiliary testing instead of all VHDL code. A complete test system is worth **40** points.】
6. Any additional work will receive **extra** points as **bonus**. All additional work must be reflected in the HDL code. All additional work must be verified by post-synthesis timing simulation. All additional work must be clearly marked in the README file.
7. You need to draw a system block diagram for your design. A complete system block diagram that matches the code is worth **5** points.
8. You need to complete a simple report summarizing the problems encountered during the project and your solutions. Report worth **10** points.
9. The full score for this project is **200** points. Overflowing scores will be ignored. **Points greater than 100 will be used to make up for the deductions of other labs.**

Item	Points
128-bit AES encryption (pass post-synthesis timing)	45
complete test system	40
system block diagram	5
Report	10
Each additional function (only pass behavior simulation)	7 (bonus)
Each additional function (pass post-synthesis timing simulation)	10 (bonus)
Extra work	Depends on workload and innovation

Code format

1. The capitalization of keywords, library names, function names, variable names and signal names should be consistent respectively. Otherwise, **3** points will be deducted.
2. Naming must be **meaningful**. Please use uppercase letters and underscores to make your name easier to read and understand. Otherwise, **5** points will be deducted.
3. Use **four Spaces** or **a Tab** to indent your code. Please use reasonable indentation to makes your code easier to read and understand. Otherwise, **5** points will be deducted.

Materials provided

1. AES Introduction.ppt
   Introduced the complete process of AES, you should read this material first.
2. AES Algorithm.pdf
   Describes the details of the AES algorithm.
3. AES Example.pdf
   Provides an AES example and includes an Easter egg.
4. AES reference C code.c
   AES C code which can be used to copy S-BOX.
5. AES_testcases_128.txt
   Used to test the encryption and decryption of AES when the key is 128 bits. Will keep the same format as provided in autolab.
6. AES_testcases_192.txt
   Used to test the encryption and decryption of AES when the key is 192 bits. Will keep the same format as provided in autolab.
7. AES_testcases_256.txt
   Used to test the encryption and decryption of AES when the key is 256 bits. Will keep the same format as provided in autolab.
8. AES_results_decryption_128.txt
   An example of the file generated by the automatic test. Your automated test system should be able to generate result files with the same format on autolab.

9. statement.txt

   Used to declare the work you have completed. You should change the content of the file according to the actual situation.

Files to be submitted

1. VHDL file

   Contains all vhdl codes for encryption and decryption functions.
2. Automatic test script

   All scripts required for automatic testing can be used in any language you like. Must include the python script grade.py, which is the main function and used to start automatic testing with one command.
3. statement.txt

   Used to declare the work you have done. Please declare in accordance with the actual situation, do not lie or conceal. If you declare unfinished work, double points will be deducted. If you do not declare completed work, you will not receive points from this part.
4. README.md

   This is your report.
5. System_Block_Diagram.pdf

   Please ensure that the lines are straight and clear. You can only draw the top-level system block diagram.

Autolab's behavior

1. After receiving the submission, autolab will extract the compressed file you submitted to the current path.
2. Then it will extract the compressed file containing the test data to the current directory. Now the test path should look like this

```
Test_Folder
├──eval
│    ├──AES_testcases_128.txt
│    ├──AES_testcases_192.txt
│    └──AES_testcases_256.txt
├──script
│    ├──grade.py
│    └──*.*
├──src
│    └──*.vhd
├──sim
│    └──*.vhd
├──statement.txt
├──README.md
└──System_Block_Diagram.pdf
```

3. Then it will run the following command:

```
python3 ./script/grade.py
```

4. Then the automatic test starts to run. Your automated test script should be able to read the test data in the eval folder and use it for encryption and decryption tests.
5. In the testcase file, if the first number of a line is 0, then this line should be used for encryption test, if it is 1, it should be used for decryption test.
6. Your automated test script should generate test results for each testcase: passed (P), failed (F), and not tested (N). Each result occupies one line and is saved in the corresponding file. Now the eval folder should look like this

```
eval
├──AES_testcases_128.txt
├──AES_testcases_192.txt
├──AES_testcases_256.txt
├──AES_results_decryption_128.txt
├──AES_results_decryption_192.txt
├──AES_results_decryption_256.txt
├──AES_results_encryption_128.txt
├──AES_results_encryption_192.txt
└──AES_results_encryption_256.txt
```

7. Finally, autolab runs the automatic scoring script, reads your statement.txt and result file, and outputs the corresponding score.

Attention

- **In this lab, the TA CAN do these:**
  - Explain experimental materials and experimental requirements.
  - Explain the scoring criteria and scoring methods (not including specific information about test cases).
  - Explain the algorithm.
  - Explain the logs and error messages on the auto-scoring platform
- **In this lab, the TA CAN NOT do these:**
  - Operate your computer.
  - See your code.
  - See the error message on your computer.

Submit

1. **All files (except pdf file) you submit must not contain any non-ASCII characters.**

2. **It should be noted that vhdl code must be readable, so high-level synthesis tools are not allowed to be used unless you modify the generated code to make it easy to read.**

3. Compress the diagrams, scripts and HDL codes, and **name the compressed package as follow the format**:

   Project_[YourNameInEnglish]_[YourStudentNumber].zip

4. **File Organization Schema in Package**:

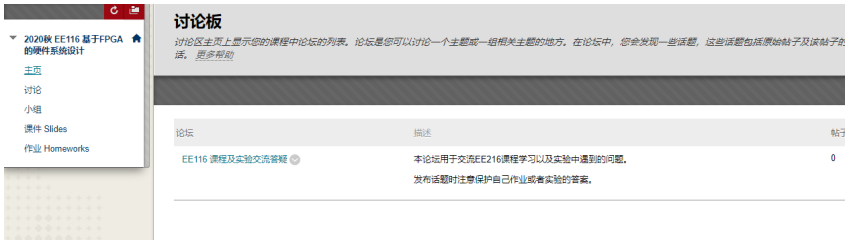
```
Project_[YourName]_[YourStudentNumber].zip
├──script
│    ├──grade.py
│    └──*.*
├──src
│    └──*.vhd
├──sim
│    └──*.vhd
├──statement.txt
├──README.md
└──System_Block_Diagram.pdf
```

Deadline: 2020-12-09 15:00

- Submit on time, get all scores.
- Submission time does not exceed 24 hours of the deadline, get half of the score.
- Submitted more than 24 hours from the deadline, get no score.

Any Question?

Any questions on course or labs can be proposed in the Discussing Forum on BB.



We recommend you subscribe to the forum to receive the newest topics on time.