Ronan GUILLAUME
Paula GOMBAR

Comments on the homework

Cryptographic Engineering: Digital design tutorial #1: AES project

1 Did we find this homework difficult?

In our opinion, we can say that this homework was difficult, even if the work produced at the end was easy. Indeed, the work we have sent you was only the tip of the iceberg, maybe more than 75% of the time we spent on the homework was just to understand the code, install the setup and understand the project. Because, always in our opinion, two hours is definitely not enough to learn a new language (VHDL), a new software and to learn how can we analyze a digital system figure. But we can admit that this is a part of the work, so we have done it but this why the homework becomes difficult.

Maybe some enhancements are possible for the next year in order to make the homework easier. Firstly, maybe you should be more explicit when you explain how to install the setup. We have lost something like 3 or 4 days just searching how to install the setup: install virtual box, find the link to the VM, understand we must download all the elements because it was only one archive divided into 13 parts, then create the VM from the virtual disk. We think all this stuff should be explained as explicitly as the tutorial to run the project (which is very good). Secondly, maybe your project needs some comments into the code in order to simplify our comprehension of the code or maybe another document which describes the structure of a VHDL file (what is a component, a signal, a chip enable, etc.). Finally, it would have been good if we had some tutorial on how to interpret signals in order to debug our project with gtkwave.

2 What problems we have met and how we solved it?

2.1 Solve the “enc_dec” problem

In your subject, you speak about a problem we will encounter about the enc_dec signal. Indeed, you have written “that the circuit, when receiving a key for key derivation, can have the port enc_dec in the decryption mode, and in this case, we want our circuit to work in encryption mode”.

So, after a lot of time searching why this problem can appear and ask the teacher by mail. We researched how to solve it. Our first idea was to add a “AND” logical operation between enc_dec and round_number_key_generation just after the “OR” one.

2.2 Understand the project and what we must do

The most difficult part of this project was to understand the project, the structure, what we have and what it asked us.

But after asking the teacher some questions via mail and a lot of work, we achieved to solve this difficulty.

2.3 Analyze the digital system and the current code

Another problem was that we didn’t know the language of the project and the digital system. So, we have done a lot of research in order to learn it.

2.4 State machine’s outputs

We weren’t sure if it was an error or if we didn’t understand the project but there were not anymore outputs in the figure 16. But after asking the teacher, it was an error of his.

2.5 To_integer problem

We have a lot of warnings from this function but we don't understand where they came from because we don't use this function. Maybe we try to change a STD_LOGIC_VECTOR into a STD_LOGIC but we didn't find where or maybe because one of our signals is not initialized. In fact, the warnings were already here in the original project so they don't matter.

2.6 Gtkwave

Another difficulty during this project was to use a new tool: gtkwave. In fact, we didn't understand how it works but especially how can it help us in our project. So we spent a lot of time with Mr.Massolino and he was able to show us how to use this tool to debug our project.