ELEC2760 - Exercise Session #2: Software Implementations

Exercise #1. Create a new project in AVR Studio.

a. Type : AVR Atmel assembler.

b. Debug : AVR Simulator 2.

c. Device : ATmega644P.

d. Entry file : rijndaelfurious.asm (source : http://point-at-infinity.org/avraes/).

Exercise #2. Read and understand:

a. *main*.

b. *encrypt*, related to the FIPS-197 standard, Chapter 5.

c. *mixcolumns*, note the link with the implementation presented in Lecture 5.

Exercise #3. Assemble the code and record the space taken in the program memory.

Exercise #4. Simulate the code.

a. See the effect of *key_expand* in the RAM (at the beginning of the execution).

b. How many clock cycles does it take to execute:

   i. *encrypt* ?

   ii. *decrypt* ?

   iii. *mixcolumns* ?

c. What is the ciphertext of the plaintext 0 enciphered with the master key 0 ?

Exercise #5. Write a function *xtime2*, as compact as possible, that is using no table.

Exercise #6. Insert this function in *mixcolumns*, and delete the now useless table *xtime*.

Exercise #7. Compare *xtime* and *xtime2* in terms of:

a. execution time

   i. for *mixcolumns*.

   ii. for a complete encryption.

b. space consumed in the program memory.

Exercise #8. Improve *xtime2* into *xtime3* with data-independent execution time. Why is this feature important? What is its cost in terms of execution time and memory space ?