Homework #2
AES implementation

CNS Course Sapienza

Riccardo Prinzivalle, 1904064

October 30, 2020

1 Homework Goal

This homework contains a basic python implementation of AES algorithm. Throughout the work, it has been chosen to make a compromise: the implementation is in midpoint between complete Galois Field and precomputed look-up tables for every step. Both encryption and decryption are studied and implemented, then the operatives modes are implemente and finally we will illustrate a comparison with world known AES implementations.

2 Encryption

AES encryption can be decomposed into a sequence of the following four big blocks:

1. Byte Substitution
2. Shift Row
3. Mix Columns
4. Key Addition

The following subsections contains implementation details and choices made to build the single blocks.

2.1 Byte Substitution

2.2 Shift Row

2.3 Mix Columns

2.4 Key Addition

3 Decryption

Stoichiometry The relationship between the relative quantities of substances taking part in a reaction or forming a compound, typically a ratio of whole integers.

Atomic mass The mass of an atom of a chemical element expressed in atomic mass units. It is approximately equivalent to the number of protons and neutrons in the atom (the mass number) or to the average number allowing for the relative abundances of different isotopes.

4 Operation Modes

Mass of empty crucible	7.28 g
Mass of crucible and magnesium before heating	8.59 g
Mass of crucible and magnesium oxide after heating	9.46 g
Balance used	#4
Magnesium from sample bottle	#1

5 Real World Standard Comparison

Mass of magnesium metal	= 8.59 g - 7.28 g
	= 1.31 g
Mass of magnesium oxide	= 9.46 g - 7.28 g
	= 2.18 g
Mass of oxygen	= 2.18 g - 1.31 g
	= 0.87 g

Because of this reaction, the required ratio is the atomic weight of magnesium: 16.00 g of oxygen as experimental mass of Mg: experimental mass of oxygen or $\frac{x}{1.31} = \frac{16}{0.87}$ from which, $M_{\mathrm{Mg}} = 16.00 \times \frac{1.31}{0.87} = 24.1 = 24\,\mathrm{g\,mol^{-1}}$ (to two significant figures).