Homework #4
Elliptic Curves

CNS Course Sapienza

Riccardo Prinzivalle, 1904064

November 20, 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 operation modes are implemented and finally it will illustrate a comparison with world known AES implementation.

Input text	6bc1bee22e409f96e93d7e117393172a ae2d8a571e03ac9c9eb76fac45af8e51 30c81c46a35ce411e5fbc1191a0a52ef f69f2445df4f9b17ad2b417be66c37
Key	2b7e151628aed2a6abf7158809cf4f3c
IV (where needed)	5468617473206D79204B756E67204675

Table 1: Parameter used in testing of AES operation modes

2 Mathematical background

3 Discrete Logarithm Problem with Elliptic Curves

(a) Core

(b) Preprocessing

Figure 1: Mix columns base functions

4 Use of Elliptic Curves in Cryptography

5 Conclusion

Even if the implementation proposed is much slower than the standard library chosen as comparison, it works well and it does its dirty job. The code may not be much optimized or it can have been written in a better way but my knowledge in python is not so huge, but this was an opportunity to dust and improve my experience.