Laboratory 2 – AISC

A simplified version of AES

Agnetta Stefano, Brozzo Doda Umberto, Macario Davide

March 29$^{\text{th}}$, 2023

A.Y. 2021–2022

1 Introduction

This laboratory revolved around the analysis of a simplified version of AES (Advanced Encryption Standard), which was provided as a python script, which can be found at [1], and which also contained all necessary sub–blocks for each round (SBox, ShiftRows, MixColumns and AddKey). These blocks are designed to work on 16–bit inputs, organized as 2–by–2 matrices of 4–bit '*nibbles*'. Also the key is a 16-bit

2 Avalanche effect

3 Improperly implemented block cipher

4 Conclusions

References

[1] https://jhafranco.com/2012/02/11/simplified-aes-implementation-in-python/