



# CS666 Assignment 3

DOM and CPA Attack

SEPT 2022

**ASSIGNMENT BY:**

DR. URBI CHATTERJEE

**GROUP 1**

SOHAM GHOSAL (180771)

TARUN KANODIA (190902)

TUSHAR SINGLA (190918)

AYUSH SHAKYA (180178)

# DOM Attack

---

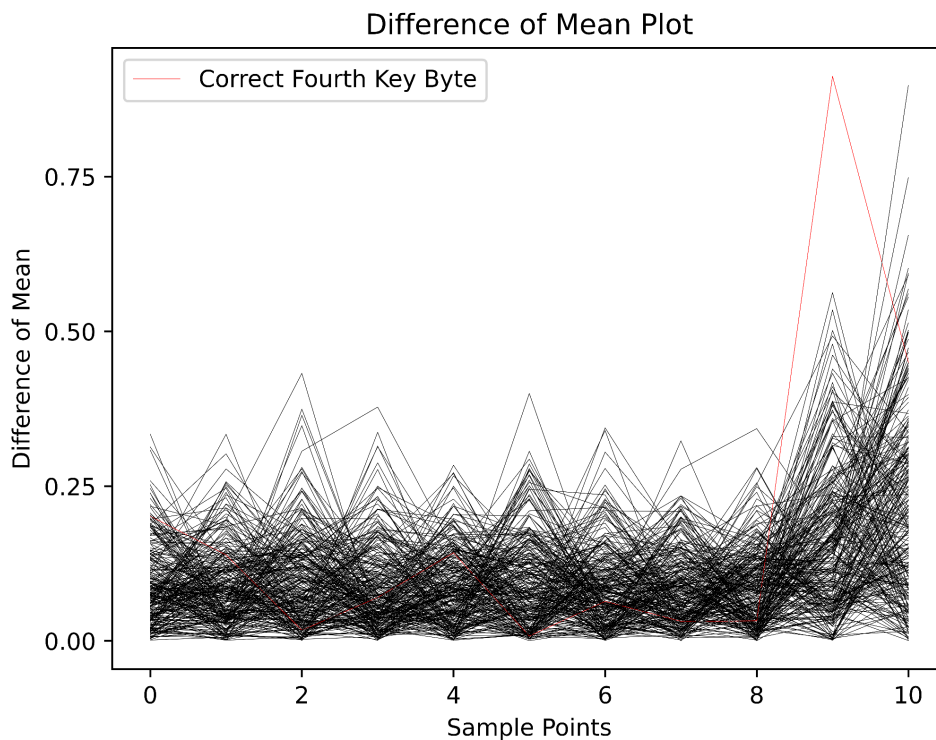
## Introduction

This assignment required the group to find the 4th and 5th bytes of the key in AES using the Difference of Means (DOM) attack. A sample code for finding the 0th byte of the key of the AES was provided as a reference, which we modified to implement the DOM attack on the 4th and 5th bytes.

- We assumed that power consumption was correlated with the 0th bit of the S-Box.
- We disregarded the inverse shift row operation since we are concerned with a particular byte of the key.

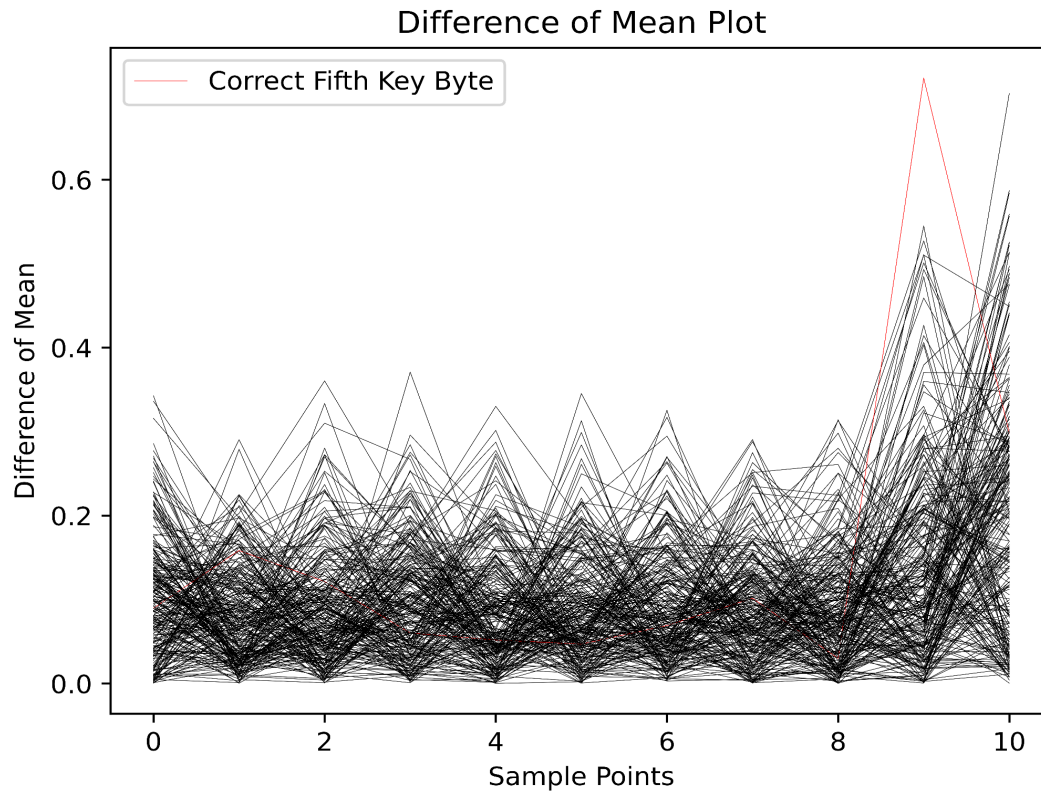
This report summarises the results obtained for the 4th and 5th byte among all possible key-value pairs.

### Plot for the 4th byte



---

## Plot for the 5th byte



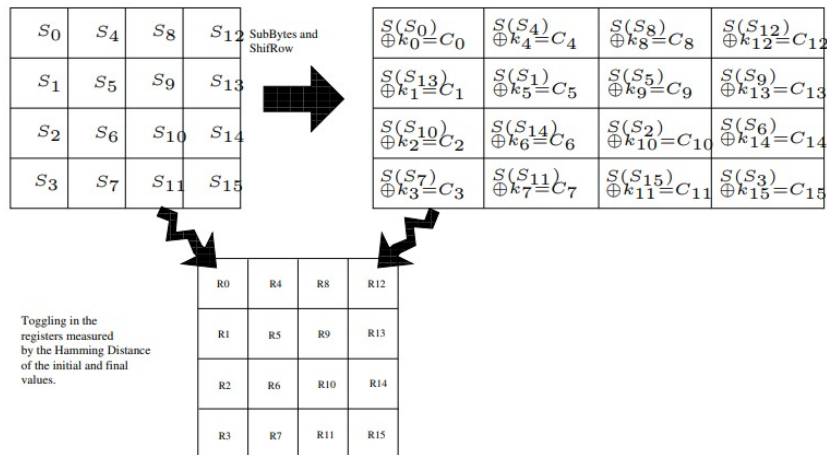
## Conclusions

We can conclude from the plots for the 4th byte that the key value is **0xE3**. In the same way, the key value for the 5th byte is **0x94**. The peak in the DOM plot has been shown in red.

# CPA Attack

## Introduction

In this assignment, we were given the power consumption of the last round of AES. A CSV file containing the power traces is provided. The group was required to write a code for Correlation Power Attack and use that code on the given power trace to recover the 1st byte (Assigned to Group 1). A sample code for finding the 0th byte of the key of the AES was provided as a reference, which we modified to implement the CPA attack on 1st byte.



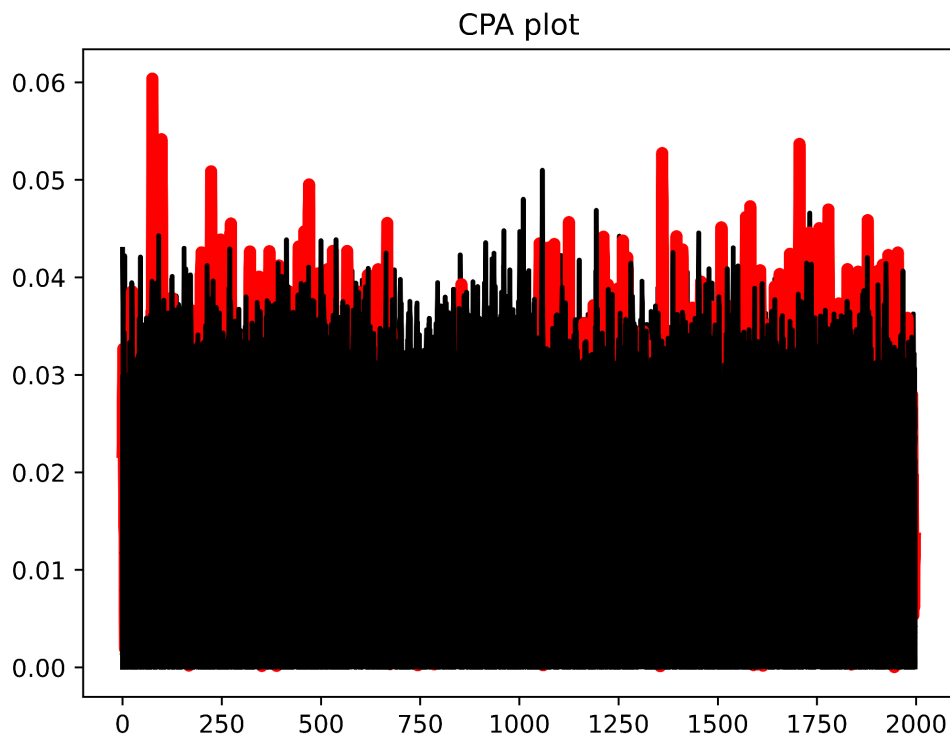
From the above figure, it can be seen that the first key byte involves 13th byte of the S box input ( $S_{13}$ ). We hence generate the following equation for hypothetical power involving change in value of register 13 using Hamming Distance Model:

$$HD(C_{13}, S_{13}) = HD(C_{13}, S^{-1}(C_1 \oplus K_1))$$

---

So if our guess for first key byte is correct, according to the above equation, we must obtain a peak in correlation between hypothetical power trace and given power trace for all points, as is visible in the plot ahead.

The results obtained for the 1st byte among all possible key-value pairs:



## Conclusions

We can conclude from the plots and our modified code for the 1st byte that the key value upon a successful CPA attack is **0x8C**.