CS6630 : Assignment 3

Fault Attack : 100 Marks

Deadline: September 15th

Luther Stickell has access to the device where an encryption algorithm is running. Luther used fault injection techniques to obtain some correct and faulty ciphertext pairs. You have been given information about the online phase of the attack. Your mission, should you decide to accept it, is to perform the offline phase of the attack.

Let's use the following assumptions to find the secret key.

Assumptions:

- Fault Model Used: Single-Byte Fault
- Cipher Algorithm Used for Encryption: AES
- Location of Fault Injected: 8th round before MixColumn

To be Answered:

1. Which round key were you able to obtain from the information given? **(5 marks)**
2. The number of key bytes retrieved after the offline Analysis? **(10 marks)**
3. Python script to perform the offline Analysis **(60 marks)**
4. Detailed report : **(25 marks)**
    a. Describe the steps used for the Analysis
    b. Time taken to obtain the round key?
    c. Minimum pair of ciphertext/faulty ciphertext pair to retrieve all bytes of round key?

Submission Format:

Folder rollnum1_rollnum2 should contain the following files

1. Python script for the analysis - **dfa_8.py**
2. **roundkeys.txt** should include the round keys values obtained
   Example:
   round 1 : [117, 4, 184, 16, 195, 49, 154, 87, 75, 44, 133, 255, 97, 59, 253, 136]
3. Report (in PDF)

PS: Evaluation will be strictly based on this format. Please make sure you follow the format for the first two files.