Hardware Security for internet of things: Assignment 4
Due Date: November 5, 2022 (11:59 PM)

General Instructions:

- This will be a group assignment. Every group consists of five members. The allocated group numbers are uploaded separately.
- Only electronic submissions will be accepted.
- Late submissions will have penalties.
- Any sort of plagiarism will be penalised. If you are referring to any materials online or books, please cite them accordingly otherwise it will be considered as plagiarism.
- Please submit a detailed report explaining how you have solved the assignment.

Question

In this assignment, you have to implement a Differential Fault Attack on AES. You would be supplied with two pairs of faulty and correct ciphertext and using that you need to recover the first column (first 32 bits) of the round 10 key. The two pairs of faulty and correct ciphertext for each group are as given below:

- Group 1:

Correct Ciphertext1: 0xd8fdc9b896a929cb33df86b634e0dc04
Correct Ciphertext2: 0xaa5e77e2064d15e14babd14f5feafa77
Faulty Ciphertext1: 0x32622c1f5deed912b18a59996444273f
Faulty Ciphertext2: 0xb7565eced22c123b2d6e2fc9101d2315

- Group 2:

Correct Ciphertext1: 0xb21eeb73953e7a2771db222ecbeea788
Correct Ciphertext2: 0xcabe3e9988d6666a96a39e7b659ca91
Faulty Ciphertext1: 0x33cf60141fd2f121ff9a6126fefd03e6
Faulty Ciphertext2: 0x92317b8a9e24f1960f37385a4085b0d5

- Group 3:

Correct Ciphertext1: 0x317982fa5666677f86b021f313e21725
Correct Ciphertext2: 0xeeade76ae853cceca45dddfe257c63c0
Faulty Ciphertext1: 0x77f3dac61758cdb2cd9ab5d532d4ec8d
Faulty Ciphertext2: 0xc1531c070f9303ef23fca1f5bab1007

- Group 4:

Correct Ciphertext1: 0x6559ddd4dde1df14a4888fb98dde1e67
Correct Ciphertext2: 0x7bde21b7f4a53022be2788696816249
Faulty Ciphertext1: 0xf289ba7cea98d64fa982fe226f4bdf48
Faulty Ciphertext2: 0x488a3c55b75ba66f857ca45b6ad47335

- Group 5:

Correct Ciphertext1: 0xcb9e460f86b40b7d3b9ec48a0726acef
Correct Ciphertext2: 0xe38830724a96247185621d21458c16fb

Faulty Ciphertext1: 0x7fb5bd33e30867882ad89d326d824dc9
Faulty Ciphertext2: 0x48c3b33b3516a1f8c31d08f90479b7b5

- Group 6:

Correct Ciphertext1: 0x3bbef03bda5e6125efc486d2fe0821d5
Correct Ciphertext2: 0x5d384a1c2fe264e6932b1762170c1e12
Faulty Ciphertext1: 0x56fa7358210307a95c322f931df5be7b
Faulty Ciphertext2: 0x46b15f4bdb9f30fa1d4ae117979899f7

- Group 7:

Correct Ciphertext1: 0x5ac34223b23627e417ff32d15dc62b3a
Correct Ciphertext2: 0x620f470b13743f5f9f1026a0eed920eb
Faulty Ciphertext1: 0xf4cc767bbddd6637aebd12ed264f360e
Faulty Ciphertext2: 0xea9403be8583cd160ff038e449701213

- Group 8:

Correct Ciphertext1: 0xda97114931cbd335500ee62b48fb6995
Correct Ciphertext2: 0x3c78541c6878b4b5fceb32ab3b807841
Faulty Ciphertext1: 0xc3629082c8831cce1f11d90545576548
Faulty Ciphertext2: 0xb04312979271e8eff1e4dc3f269b907a

- Group 9:

Correct Ciphertext1: 0x602711bfc28503c231ead1896c8a7bdf
Correct Ciphertext2: 0x61f89da50a8ef28a8d76cc17fc9bc1ff
Faulty Ciphertext1: 0x386b33963d6fc849285c601eff95f0eb
Faulty Ciphertext2: 0x2421ed67d3d9d447dd753c6084e255aa

- Group 10:

Correct Ciphertext1: 0x4cd85c0098347a815bb1e10570ca3b4a
Correct Ciphertext2: 0xeda5c644b23810b6214e7967a0740436
Faulty Ciphertext1: 0x6a076d5594e53e14a004abd11e7d39fb
Faulty Ciphertext2: 0x3d8f745b817c036335ba1e891a72524d

Note: In case of 31 characters in the above correct or faulty cipher texts, please append ‘0’ in the beginning.

Deliverables:

1. Even though you are working in group, you need to submit solutions individually.
2. The solution for the assignment should be submitted as a zip file. The file should be named as StudentNameRollNumber.zip.
3. The submission should contain the following:

- A python file.
- The report (as pdf).