Question Number 1

Each group has an oracle of Sypher00A
Sypher00A.zip

You need to perform linear cryptanalysis of Sypher00A and retrieve both keys - k_0 and k_1.

Finding the keys by brute force is not allowed.

You need to submit the following things in a pdf

1. Description of the process you used to find the keys
2. The keys itself
3. All the linear equations used to find the keys
4. Linear masks used to retrieve the corresponding linear equation

Please submit the code written to automate the process. If you have done the process manually, please mention that in the pdf. Submit the code even if you automated only a small part of the process

Solution. Steps

a) First we will find message and cipher text pair using `getPair()` function from `Utils.py` file

b) Then we will select pairs of α and β masks form the `Linear Approximation Table` where

$$abs(Lat[\alpha][\beta]) >= 4 \tag{1}$$

c) For each pair of mask, we will find the values of counters T_0 and T_1

d) Then we use Value of LHS(max from counter T_0 and T_1) to get correspondig equation as follows

$$(\alpha \cdot K_0) \oplus (\beta \cdot K_1) = LHS \tag{2}$$

where LHS is as follows:

$$LHS = \begin{cases} 1 & \text{if } T_1 > T_0 \\ 0 & \text{if } T_1 < T_0 \end{cases}$$

e) Then we will get 8 eqution with 8 variables as follows

K_0				K_1			
K_{00}	K_{01}	K_{02}	K_{03}	K_{10}	K_{11}	K_{12}	K_{13}

f) Using `solver()` function we are eliminating key space upto it resize to 1

g) And finally we get our key as

$$K_0 = 15$$
$$K_1 = 2$$

All this process is automated by the python file `Sypher00A.py`. (**Change Oracle path mention in main() function**)