CS 741 Assignment 2

Team Information :

Roll No.	Name
203050003	Aditya Jain
203050054	Fenil Mehta
203050110	Vipin Mahawar
203059003	Rajiv Vaidyanathan

Question 2 :

Algorithm Explanation

DFS + Branch and Bound + Pruning strategy is used with multiple optimizations on it.
We try all combinations for input and output. Where, the input and output columns are taken in binary format. Each 1 at the ith position denotes that the ith bit of the plain text/cipher text/round key will be selected in the path.

- Input: from 1_2 to $(2^{PlainTextBits} - 1)_2$ where subscript 2 denotes base 2, i.e. binary format
- Output: from 1_2 to $(2^{PlainTextBits} - 1)_2$ where subscript 2 denotes base 2, i.e. binary format

In order to reduce the running time, we performed optimizations:

- To get rid of cases where some n^{th} S-Box has input bits 1 and all output bits 0 or vice versa
- While going down the path, if bias becomes 0 at any point in time, we do not explore that path
- If the bias for any path/subpath calculated is less than the max bias seen till then, then we do not explore that path

Time Complexity = $O\,(SizeOfPlainText * 2^{NumberOfStages * SizeOfPlainText}) = O\,(N * 2^{T * N})$

Output Format :

```
(dev) →  Q2 git:(main) ✗ g++ -O2 part2_linear_expression_max_bias.cpp
(dev) →  Q2 git:(main) ✗ ./a.out
3
9
0 3 6 1 4 7 2 5 8
3
0 2 1 4 7 5 6 3
Max Bias = 0.5
Max Bias Path = P(4) P(5) K(0,4) K(0,5) K(1,4) K(1,7) K(2,1) K(2,2) K(2,7) K(2,8) C(1) C(2) C(7) C(8)
```

Max Bias, Max Bias Path

The claim "A greedy strategy will always work" is false.
Greedy Strategy : Picking path with max local absolute bias.
Explanation: We can observe the image below. If we use the above greedy strategy then we will take Path 1 as the first bias which we encounter there is 0.5 which is greater than the first bias which we encounter in Path 2 which is 0.25. We can clearly see that Path 2 has a better total bias of $1/4$ (or 0.25) which is better than Path 1 (selected by the greedy strategy) where total bias is just $1/16$ (or 0.0625).