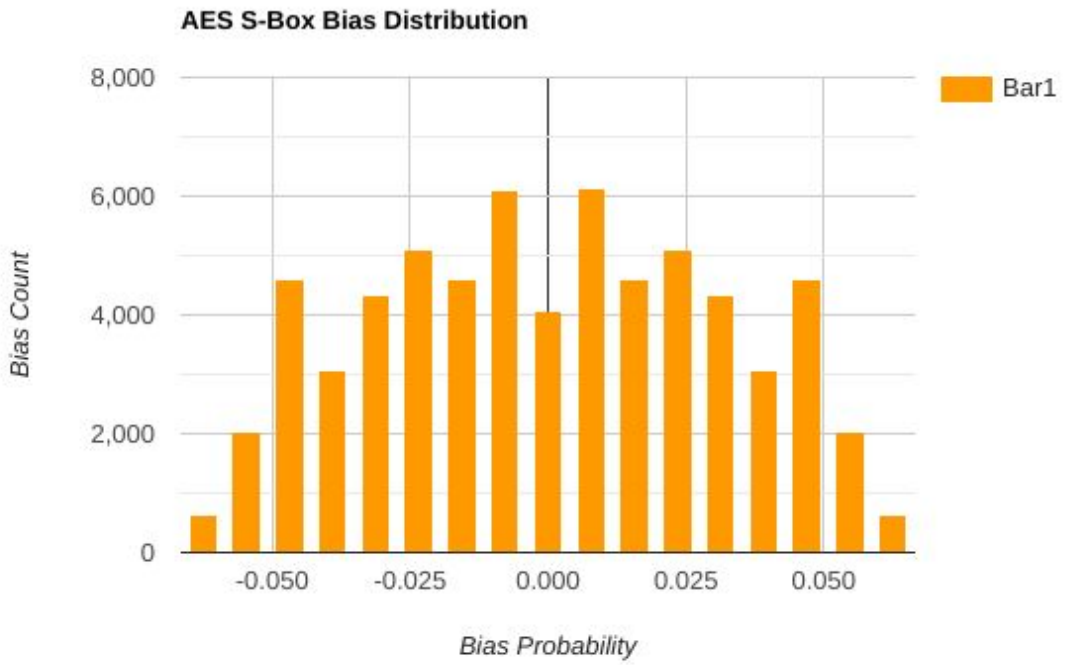
CS 741 Assignment 2

Team Information :

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

Question 1 :

Bias Probability	Bias Count
-0.0625	640
-0.0546875	2040
-0.046875	4592
-0.0390625	3064
-0.03125	4334
-0.0234375	5096
-0.015625	4592
-0.0078125	6112
0	4080
0.0078125	6128
0.015625	4588
0.0234375	5104
0.03125	4336
0.0390625	3056
0.046875	4588
0.0546875	2040
0.0625	635



- **Program Execution Time =** 0.160 seconds
- **Time Complexity =** $O(8 * 8 * 2^8 * 2^8) = O(2^{22})$
- The Bias count will always be a positive number because occurrence of zero in the XOR of all columns cannot be negative (it has to be either 0 or more).
- Bias is even because, for the S-Box to be invertible, the number of 0's and 1's in any column of input and output shall be equal (i.e. 128 in case of AES S-Box). Had the S-Box not been invertible, then the bias may not be even.
- Graph was plotted using: https://www.rapidtables.com/tools/line-graph.html