INTRODUCTION TO CRYPTOGRAPHY – PROJECT 3

B.Tech. Computer Science and Engineering (Cybersecurity)

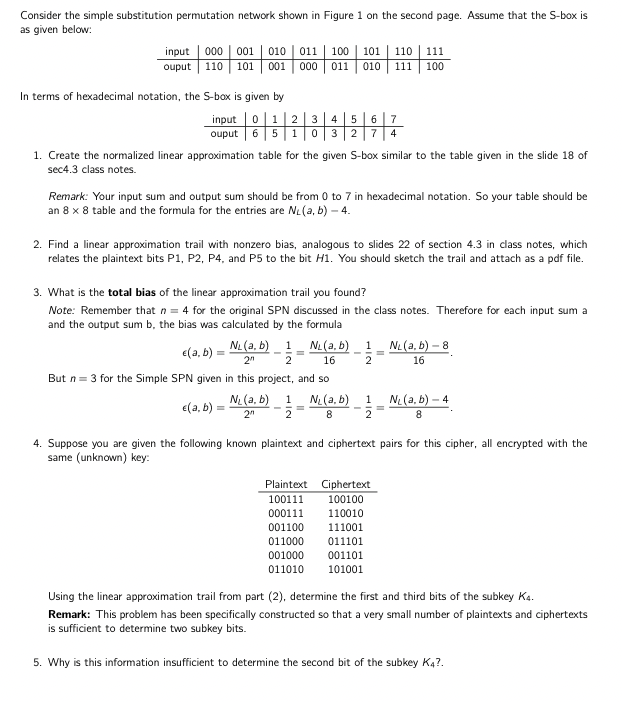
|  |  |
| --- | --- |
| Name: Anish Sudhan Nair | Roll No.: K041 |
| Batch: K2/A2 | Date of submission: 02/03/2022 |

**Code:**

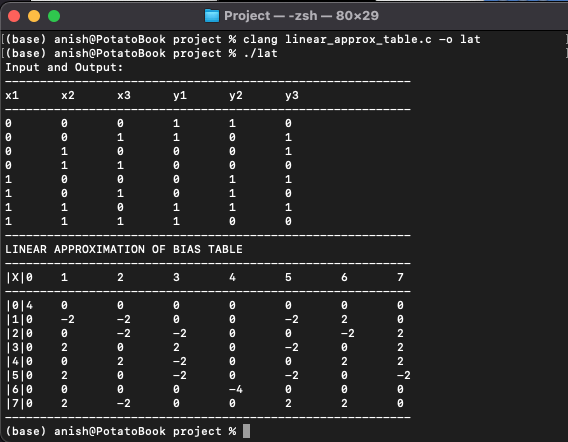
Language: C

Editor: Atom

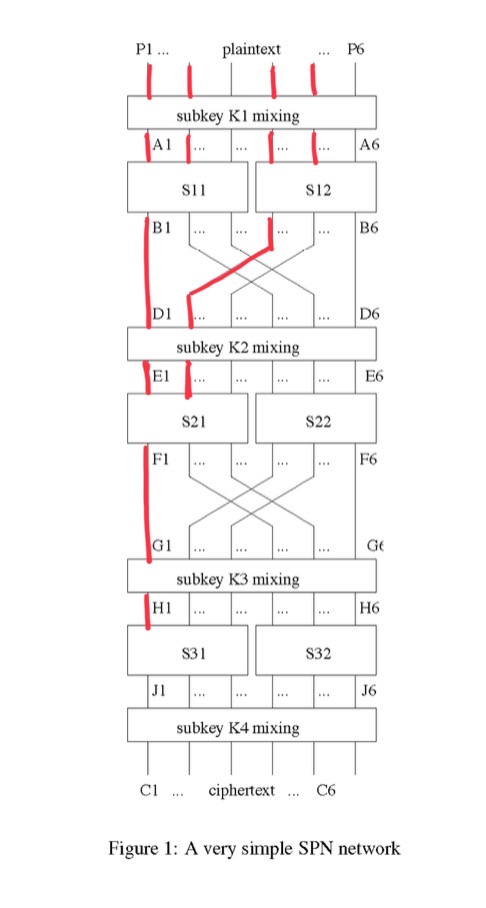
Compiler: clang/ZSH



1. Question 1



1. Question 2

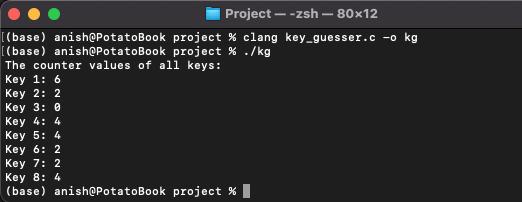


1. Question 3  
   ε(a,b)=e(110,100)= (4-8)/8 = -1/2

Since, n=3 and no.s of s boxes equals 3,

Total bias = 22(-1/2)3 = -1/2

1. Question 4



From the counter values, 6 & 0 are applicable as possible key values considering (6/2 +or- 6/2)=0 or 6. These two counter values are analogues to keys 010 and 000.

Hence, Key chosen -> 010 or 000

Therefore, first bit=0

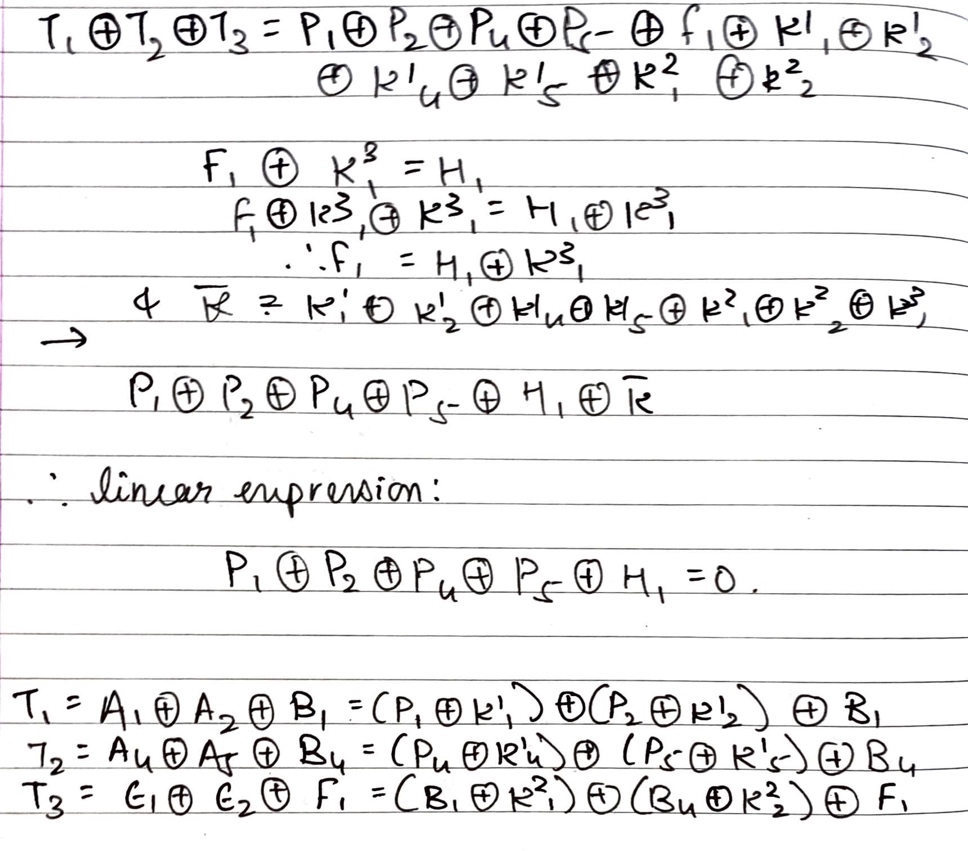
Third bit=0

1. Question 5

As stated in the previous question, due to the limited set of plaintext-ciphertext pairs, the counter values when put through the formula for choosing the appropriate keys yields two possible keys for whom the value of the second bit differ. Hence, it’s not possible to determine the second key bit.

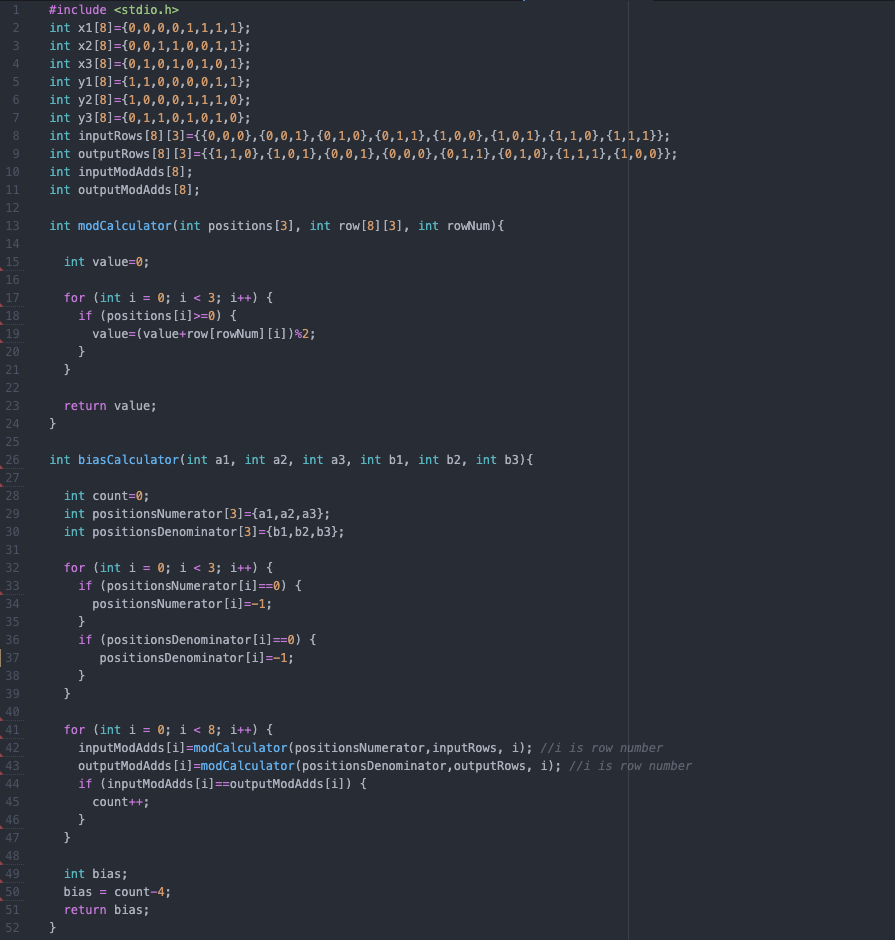
CALCULATION:

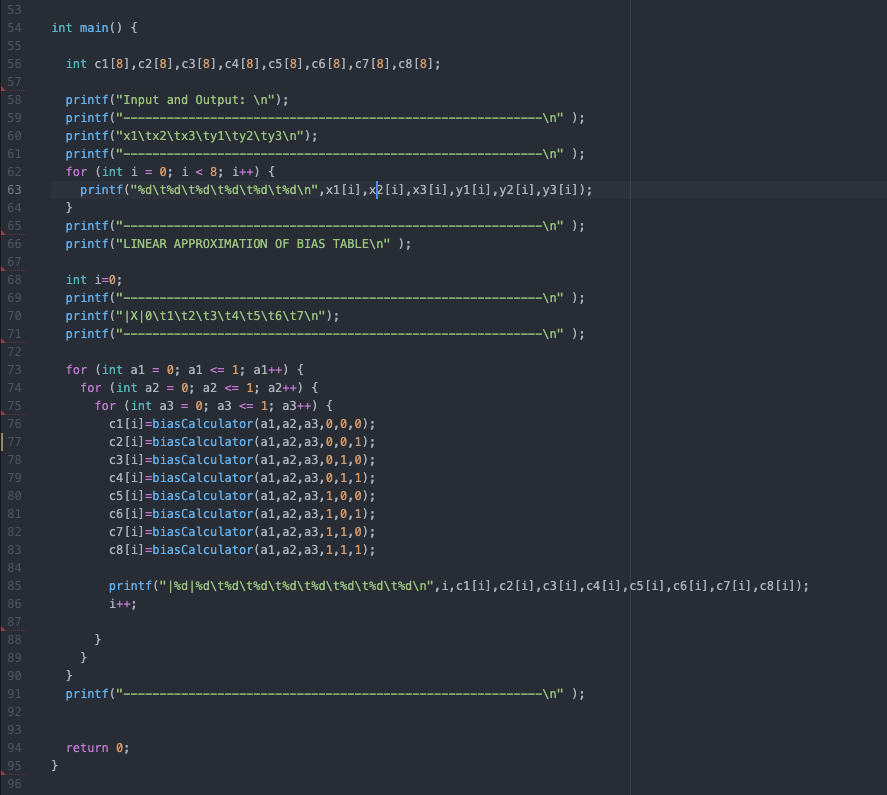
For Linear Expression:



CODES:

For Normalised Linear Approximation Table:





For Counter Values (of keys):



