INTRODUCTION TO CRYPTOGRAPHY – PROJECT 3

B.Tech. Computer Science and Engineering (Cybersecurity)

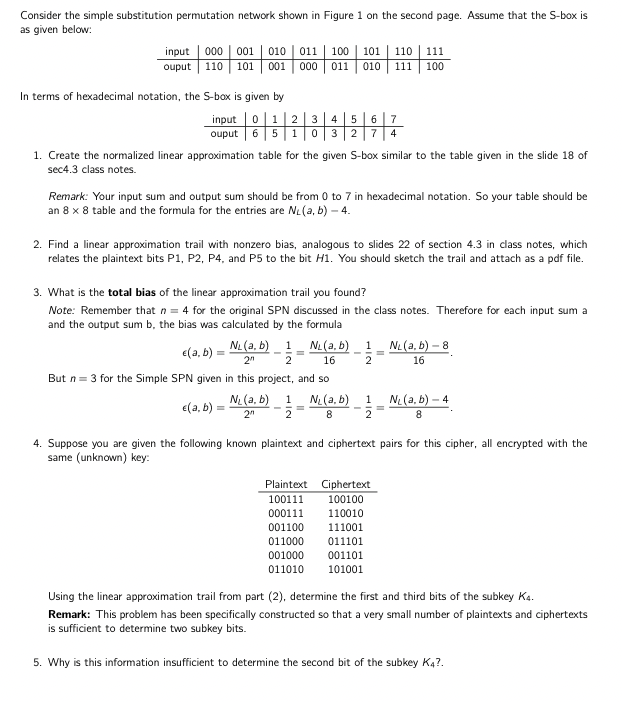
|  |  |
| --- | --- |
| Name: Anish Sudhan Nair | Roll No.: K041 |
| Batch: K2/A2 | Date of submission: 27/02/2022 |

**Code:**

Language: C

Editor: Atom

Compiler: clang/ZSH



1. Table NL(a,b)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| a | b | | | | | | | |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 0 | 8 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 1 | 4 | 2 | 2 | 4 | 4 | 1 | 6 | 4 |
| 2 | 4 | 4 | 2 |  |  |  |  |  |
| 3 | 4 | 6 |  |  |  |  |  |  |
| 4 | 4 | 4 |  |  |  |  |  |  |
| 5 | 4 | 6 |  |  |  |  |  |  |
| 6 | 4 | 5 |  |  |  |  |  |  |
| 7 | 4 | 6 |  |  |  |  |  |  |

1. Create the normalized linear approximation table for the given S-box similar to the table given in the slide 18 of sec4.3 class notes.

Remark: Your input sum and output sum should be from 0 to 7 in hexadecimal notation. So your table should be an 8 × 8 table and the formula for the entries are NL(a, b) − 4.

1. Find a linear approximation trail with nonzero bias, analogous to slides 22 of section 4.3 in class notes, which relates the plaintext bits P1, P2, P4, and P5 to the bit H1. You should sketch the trail and attach as a pdf file.
2. What is the total bias of the linear approximation trail you found?  
   Note: Remember that n = 4 for the original SPN discussed in the class notes. Therefore for each input sum a

and the output sum b, the bias was calculated by the formula

ε(a,b)= NL(a,b) − 1 = NL(a,b) − 1 = NL(a,b)−8. 2n 2 16 2 16

But n = 3 for the Simple SPN given in this project, and so  
ε(a,b)= NL(a,b) − 1 = NL(a,b) − 1 = NL(a,b)−4.

2n 2 8 2 8

1. Suppose you are given the following known plaintext and ciphertext pairs for this cipher, all encrypted with the

same (unknown) key:

Plaintext Ciphertext

100111 100100 000111 110010 001100 111001 011000 011101 001000 001101 011010 101001

Using the linear approximation trail from part (2), determine the first and third bits of the subkey K4.  
Remark: This problem has been specifically constructed so that a very small number of plaintexts and ciphertexts

is sufficient to determine two subkey bits.  
5. Why is this information insufficient to determine the second bit of the subkey K4?.

