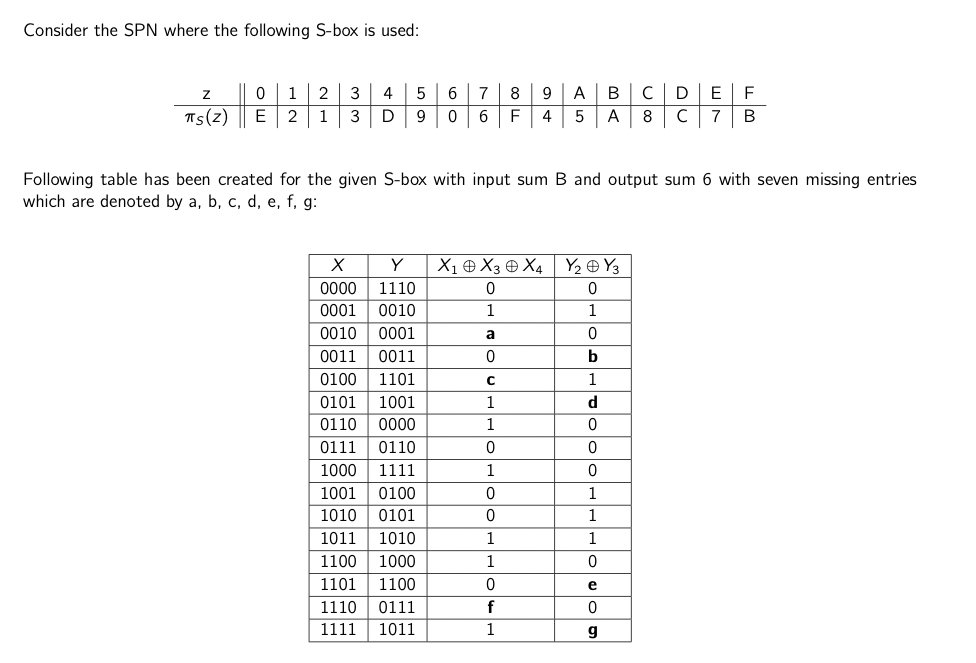
INTRODUCTION TO CRYPTOGRAPHY – QUIZ 8

B.Tech. Computer Science and Engineering (Cybersecurity)

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

Quiz



1. (14 points) Find the values of a, b, c, d, e, f, g in the above table. (2 points each)

* a=0⊕1⊕ 0 = 1

b=0⊕1= 1

c=0⊕0⊕ 0 = 0

d=0⊕ 0 = 0

e=1⊕ 0 = 1

f=1⊕1⊕ 0 = 0

g=0⊕1 = 1

1. (2 points) Compute *NL*(*B,*6) and (*B,*6).

* B= X1⊕X3⊕ X4

6= Y2⊕Y3

The table for linear approximation is already provided, therefore we simply count the no. of “Yes”

|  |  |  |
| --- | --- | --- |
| X1⊕X3⊕X4 | Y2⊕Y3 |  |
| 0 | 0 | Yes |
| 1 | 1 | Yes |
| 1 | 0 | No |
| 0 | 1 | No |
| 0 | 1 | No |
| 1 | 0 | No |
| 1 | 0 | No |
| 0 | 0 | Yes |
| 1 | 0 | No |
| 0 | 1 | No |
| 0 | 1 | No |
| 1 | 1 | Yes |
| 1 | 0 | No |
| 0 | 1 | No |
| 0 | 0 | Yes |
| 1 | 1 | Yes |

No. of “Yes” = 6

NL(B,6) = 6

(B,6) = 6/16 – 1/2 = 6-8/16 = -2/16 = -1/8

1. (2 points) Compute (*B,*6).

* NL(B,6) = 6

(B,6) = 6/16 – 1/2 = 6-8/16 = -2/16 = -1/8

1. (2 points) Can this pair be used to construct linear approximation?

* Yes.

B=6

X1⊕X3⊕X4= Y2⊕Y3

(X1⊕X3⊕X4)⊕(Y2⊕Y3)=0