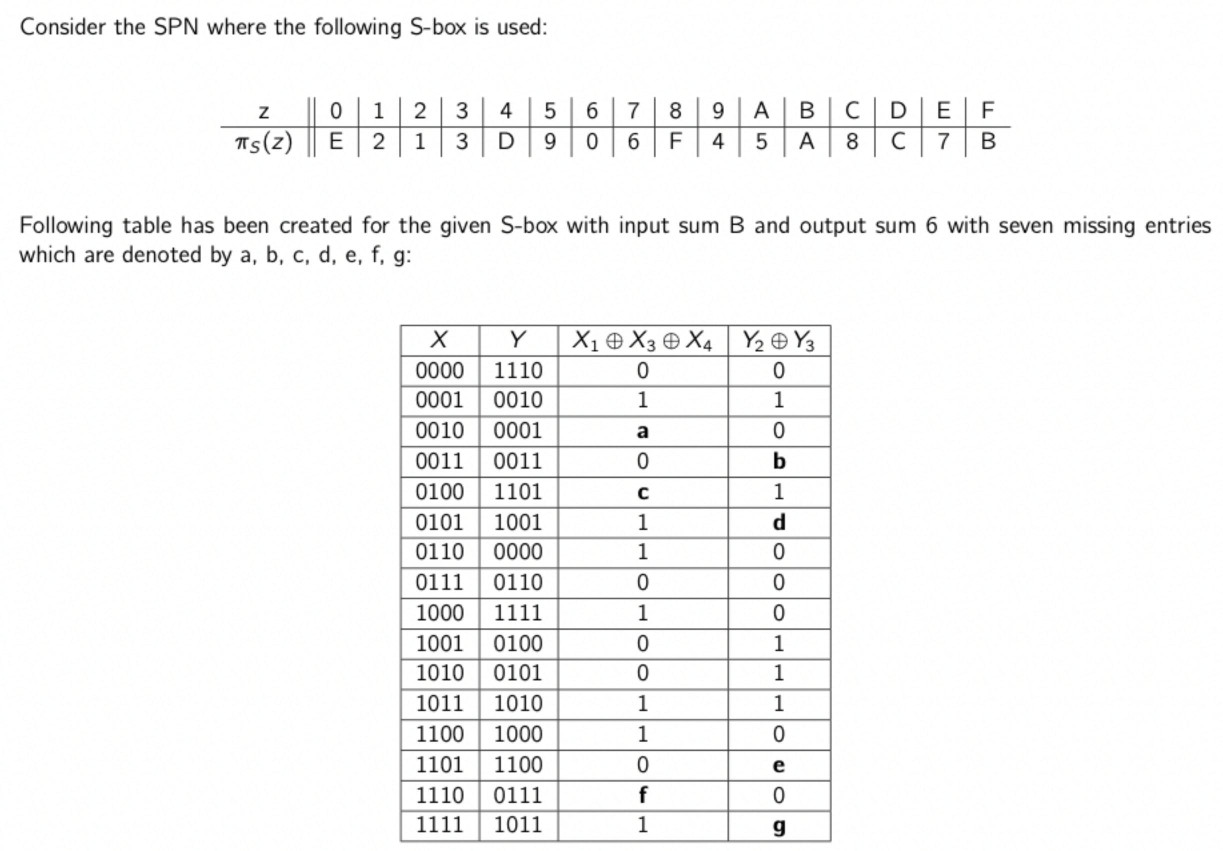
INTRODUCTION TO CRYPTOGRAPHY – QUIZ 8
B.Tech. Computer Science and Engineering (Cybersecurity)

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

Quiz



Consider the SPN where the following S-box is used:

z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi_S(z)$	E	2	1	3	D	9	0	6	F	4	5	A	8	C	7	B

Following table has been created for the given S-box with input sum B and output sum 6 with seven missing entries which are denoted by a, b, c, d, e, f, g:

X	Y	$X_1 \oplus X_3 \oplus X_4$	$Y_2 \oplus Y_3$
0000	1110	0	0
0001	0010	1	1
0010	0001	**a**	0
0011	0011	0	**b**
0100	1101	**c**	1
0101	1001	1	**d**
0110	0000	1	0
0111	0110	0	0
1000	1111	1	0
1001	0100	0	1
1010	0101	0	1
1011	1010	1	1
1100	1000	1	0
1101	1100	0	**e**
1110	0111	**f**	0
1111	1011	1	**g**

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

2. (2 points) Compute $N_L(B,6)$ and ∈(B,6).

➔ B= $X_1 \oplus X_3 \oplus X_4$
6= $Y_2 \oplus Y_3$

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

$X_1 \oplus X_3 \oplus X_4$	$Y_2 \oplus Y_3$	
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

$N_L(B,6) = 6$
$\in(B,6) = 6/16 – 1/2 = 6-8/16 = -2/16 = -1/8$

3. (2 points) Compute ∈ (*B,*6).

➔ $N_L(B,6) = 6$
$\in(B,6) = 6/16 – 1/2 = 6-8/16 = -2/16 = -1/8$

4. (2 points) Can this pair be used to construct linear approximation?

➔ Yes.
B=6
$X_1 \oplus X_3 \oplus X_4 = Y_2 \oplus Y_3$
$(X_1 \oplus X_3 \oplus X_4) \oplus (Y_2 \oplus Y_3)=0$