Question Number 3

Random Sbox

- Generate a 4-bit random Sbox in your favourite programming language

- State it in the main assignment and also document in the notebook.

- Submit the code file separately with comments briefly stating your approach

- Follow file naming convention

- It is expected that your Sbox-es will be unique

Solution.

Python Code to Generate Random Sbox:

```python
import random

HEX = [0,1,2,3,4,5,6,7,8,9,0xa,0xb,0xc,0xd,0xe,0xf]

sbox = []
for i in HEX.copy():
    j = random.choice(HEX)
    sbox.append((i,j))
    HEX.remove(j)

print("Sbox:")
for i in sbox:
    print(i)
```