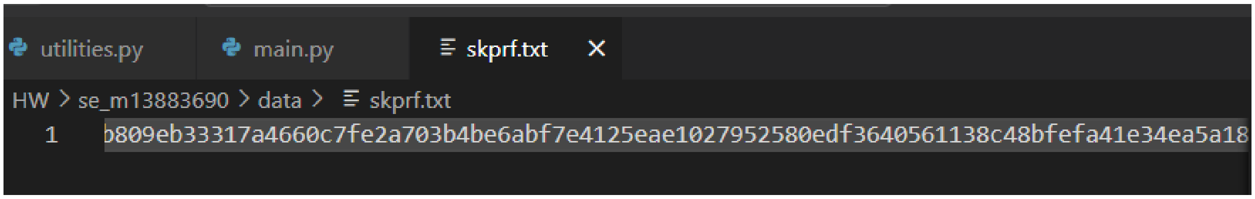
CS 5158/6058 Data Security and Privacy, Fall 2023
Project 3: Searchable Encryption

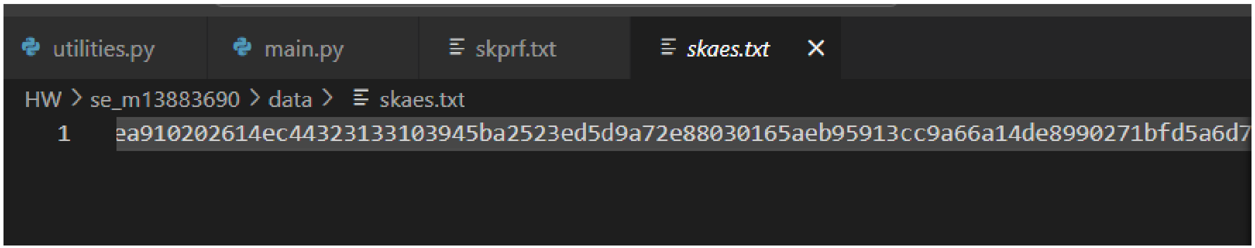
A report by Mabon Ninan

Prof: Boyang Wang

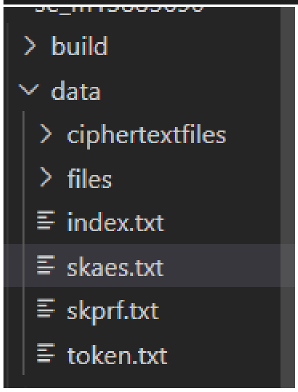
1. Key Generation Function:



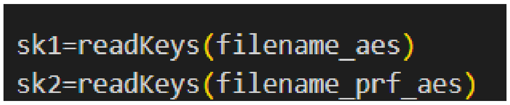
```
b809eb33317a4660c7fe2a703b4be6abf7e4125eae1027952580edf3640561138c48bfefa41e34ea5a18
```



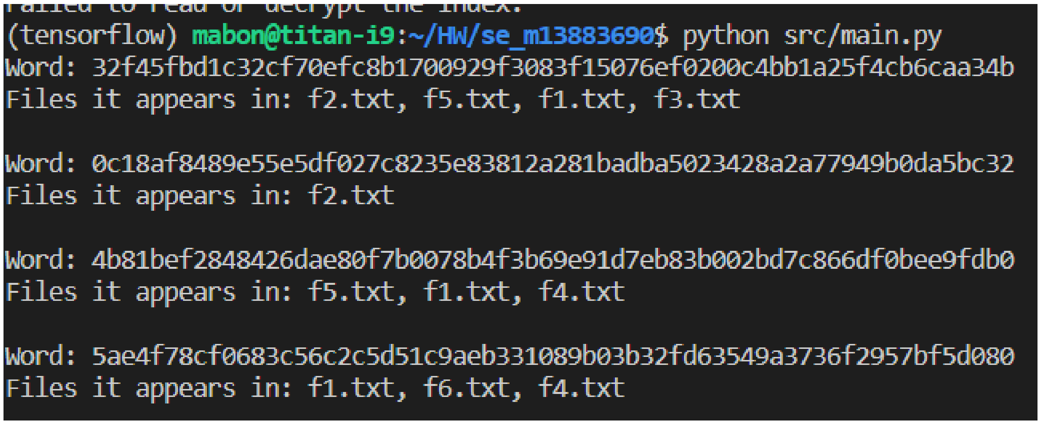
```
ea910202614ec443231331O3945ba2523ed5d9a72e88030165aeb95913cc9a66a14de8990271bfd5a6d7
```



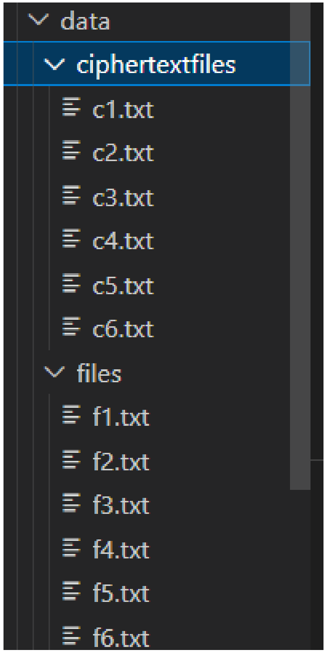
2. Encryption Function



```
sk1=readKeys(filename_aes)
sk2=readKeys(filename_prf_aes)
```

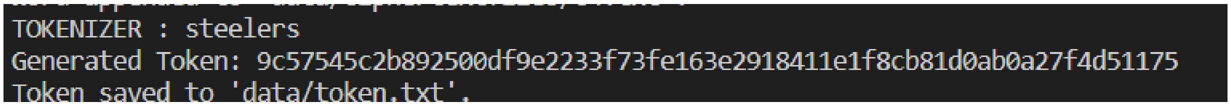


```
Failed to read or decrypt the index.
(tensorflow) mabon@titan-i9:~/HW/se_m13883690$ python src/main.py
Word: 32f45fbd1c32cf70efc8b1700929f3083f15076ef0200c4bb1a25f4cb6caa34b
Files it appears in: f2.txt, f5.txt, f1.txt, f3.txt

Word: 0c18af8489e55e5df027c8235e83812a281badba5023428a2a77949b0da5bc32
Files it appears in: f2.txt

Word: 4b81bef2848426dae80f7b0078b4f3b69e91d7eb83b002bd7c866df0bee9fdb0
Files it appears in: f5.txt, f1.txt, f4.txt

Word: 5ae4f78cf0683c56c2c5d51c9aeb331089b03b32fd63549a3736f2957bf5d080
Files it appears in: f1.txt, f6.txt, f4.txt
```



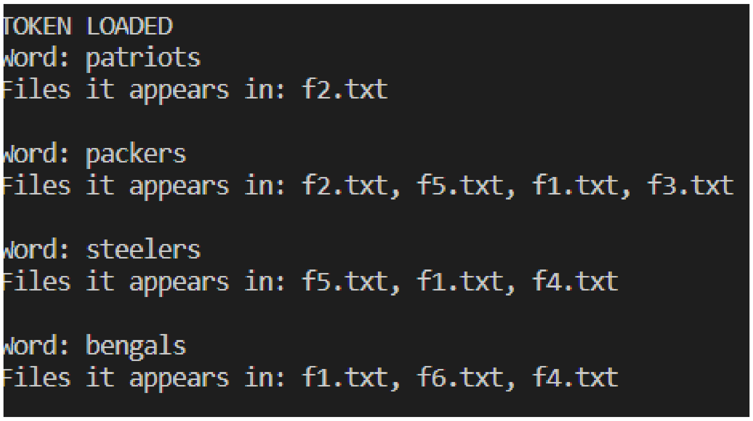
```
data
  ciphertextfiles
    c1.txt
    c2.txt
    c3.txt
    c4.txt
    c5.txt
    c6.txt
  files
    f1.txt
    f2.txt
    f3.txt
    f4.txt
    f5.txt
    f6.txt
```

3. Token Generation Function:



```
TOKENIZER : steelers
Generated Token: 9c57545c2b892500df9e2233f73fe163e2918411e1f8cb81d0ab0a27f4d51175
Token saved to 'data/token.txt'.
```

4. Search Function:



```
TOKEN LOADED
Word: patriots
Files it appears in: f2.txt

Word: packers
Files it appears in: f2.txt, f5.txt, f1.txt, f3.txt

Word: steelers
Files it appears in: f5.txt, f1.txt, f4.txt

Word: bengals
Files it appears in: f1.txt, f6.txt, f4.txt
```