Hung Nguyen – Data Security Project 3

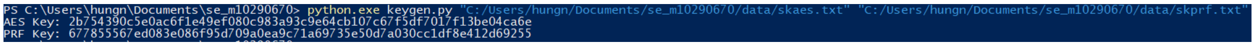
I. How to run:

a. The following command calls and runs the key generation function:

```
python.exe keygen.py "C:/Users/hungn/Documents/se_m10290670/data/skaes.txt" "C:/Users/hungn/Documents/se_m10290670/data/skprf.txt"
```

where the arguments are location of the aes key and prf key

Screenshot:



```
PS C:\Users\hungn\Documents\se_m10290670> python.exe keygen.py "C:/Users/hungn/Documents/se_m10290670/data/skaes.txt" "C:/Users/hungn/Documents/se_m10290670/data/skprf.txt"
AES Key: 2b754390c5e0ac6f1e49ef080c983a93c9e64cb107c67f5df7017f13be04ca6e
PRF Key: 677855567ed083e086f95d709a0ea9c71a69735e50d7a030cc1df8e412d69255
```

b. The following command calls and runs the encryption function:

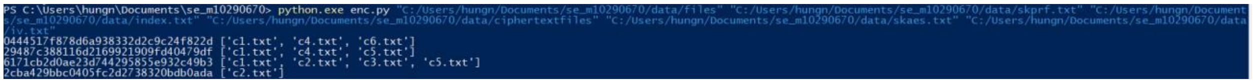
```
python.exe enc.py "C:/Users/hungn/Documents/se_m10290670/data/files" "C:/Users/hungn/Documents/se_m10290670/data/skprf.txt" "C:/Users/hungn/Documents/se_m10290670/data/index.txt"
```

"C:/Users/hungn/Documents/se_m10290670/data/ciphertextfiles"
"C:/Users/hungn/Documents/se_m10290670/data/skaes.txt"

"C:/Users/hungn/Documents/se_m10290670/data/iv.txt"

where the arguments are the directory where the files are, the location of the prf key, the location of the index file, the directory where the ciphertext files are, the location of the aes key, location of the iv

Screenshot:



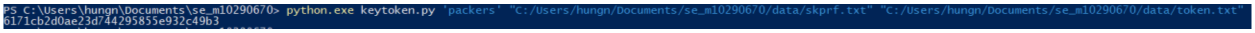
```
PS C:\Users\hungn\Documents\se_m10290670> python.exe enc.py "C:/Users/hungn/Documents/se_m10290670/data/files" "C:/Users/hungn/Documents/se_m10290670/data/skprf.txt" "C:/Users/hungn/Document
s/se_m10290670/data/index.txt" "C:/Users/hungn/Documents/se_m10290670/data/ciphertextfiles" "C:/Users/hungn/Documents/se_m10290670/data/skaes.txt" "C:/Users/hungn/Documents/se_m10290670/data
/iv.txt"
0444517f878d6a938332d2c9c24f822d ['c1.txt', 'c4.txt', 'c6.txt']
29487c388116d2169921909fd40479df ['c1.txt', 'c4.txt', 'c5.txt']
6171cb2d0ae23d744295855e932c49b3 ['c1.txt', 'c2.txt', 'c3.txt', 'c5.txt']
2cba429bbc0405fc2d2738320bdb0ada ['c2.txt']
```

c. The following command calls and runs the token generation function:

python.exe keytoken.py 'packers'
"C:/Users/hungn/Documents/se_m10290670/data/skprf.txt"
"C:/Users/hungn/Documents/se_m10290670/data/token.txt"

where the arguments are the keyword, location of the prf key, location of the token file

Screenshot:



```
PS C:\Users\hungn\Documents\se_m10290670> python.exe keytoken.py 'packers' "C:/Users/hungn/Documents/se_m10290670/data/skprf.txt" "C:/Users/hungn/Documents/se_m10290670/data/token.txt"
6171cb2d0ae23d744295855e932c49b3
```

d. The following command calls and runs the search function:

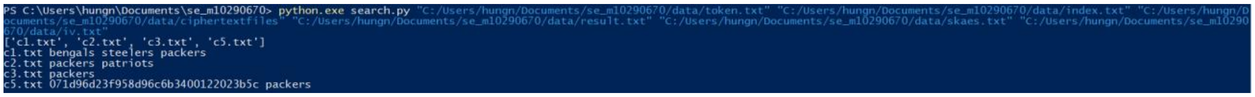
```
python.exe search.py
"C:/Users/hungn/Documents/se_m10290670/data/token.txt"
"C:/Users/hungn/Documents/se_m10290670/data/index.txt"
"C:/Users/hungn/Documents/se_m10290670/data/ciphertextfiles"
"C:/Users/hungn/Documents/se_m10290670/data/result.txt"
"C:/Users/hungn/Documents/se_m10290670/data/skaes.txt"

"C:/Users/hungn/Documents/se_m10290670/data/iv.txt"
```

where the arguments are the location of the token file, the location of the index file, the location of the result file, the location of the aes key file, the location of the iv.

Full disclosure, the text sometimes does not decrypt properly even though the encryption process is the

same for all files. If it doesn’t decrypt properly, the encrypted string is printed instead.

Screenshot:



```
PS C:\Users\hungn\Documents\se_m10290670> python.exe search.py "C:/Users/hungn/Documents/se_m10290670/data/token.txt" "C:/Users/hungn/Documents/se_m10290670/data/index.txt" "C:/Users/hungn/D
ocuments/se_m10290670/data/ciphertextfiles" "C:/Users/hungn/Documents/se_m10290670/data/result.txt" "C:/Users/hungn/Documents/se_m10290670/data/skaes.txt" "C:/Users/hungn/Documents/se_m10290
670/data/iv.txt"
['c1.txt', 'c2.txt', 'c3.txt', 'c5.txt']
c1.txt bengals steelers packers
c2.txt packers patriots
c3.txt packers
c5.txt 071d96d23f958d96c6b3400122023b5c packers
```