

Project 3 SE

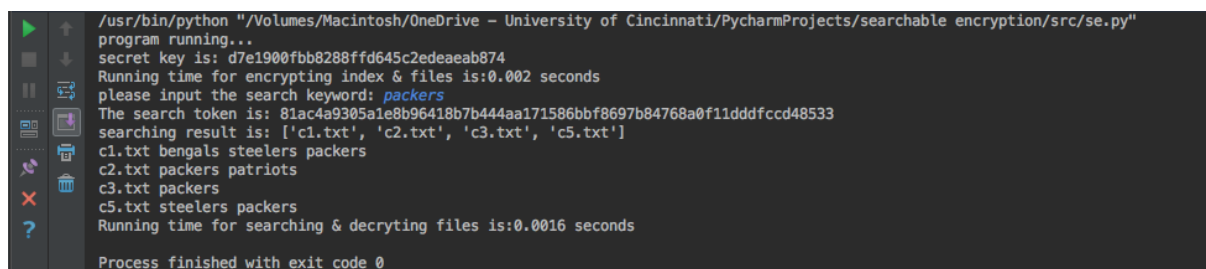
Hao Liu, Niraj Agarwal, Zheng Liu

1. Details

- This SE script is written in python2.7
- For each running, all original files should be providing in '../data/files' folder, and would output token.txt , index.txt skaes.txt, iv.txt, all encrypted files {c1,c2...} and result.txt, the details presented in readme.txt
- The program is tested in a Mac computer with 12G memories and 2.5GHz intel core i5 processor
- IDE: Pycharm

2. Comparison

The following is one result by running programs based on the all keywords in the files:
For keyword: packers, the search result details as fig1, fig2 is the related results, such as search token, ciphertexts, encrypted inverted index, secret key.



```
/usr/bin/python "/Volumes/Macintosh/OneDrive - University of Cincinnati/PycharmProjects/searchable encryption/src/se.py"
program running...
secret key is: d7e1900fbb8288ffd645c2edeaeab874
Running time for encrypting index & files is:0.002 seconds
please input the search keyword: packers
The search token is: 81ac4a9305a1e8b96418b7b444aa171586bbf8697b84768a0f11dddfccd48533
searching result is: ['c1.txt', 'c2.txt', 'c3.txt', 'c5.txt']
c1.txt bengals steelers packers
c2.txt packers patriots
c3.txt packers
c5.txt steelers packers
Running time for searching & decrypting files is:0.0016 seconds
Process finished with exit code 0
```

Figure 1

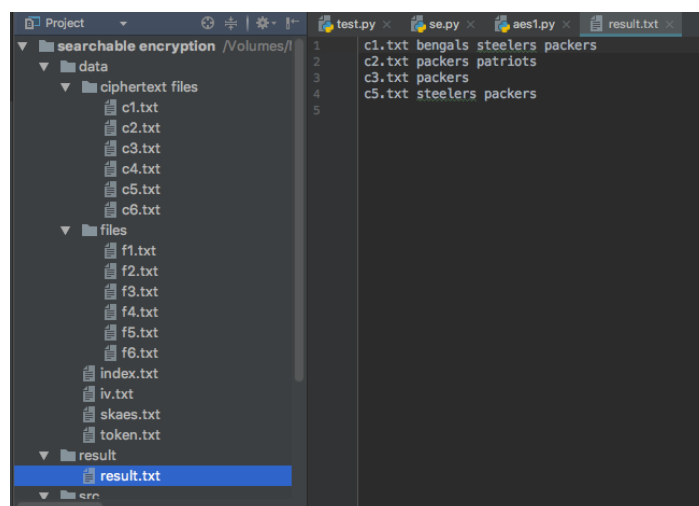


Figure 2

From figure1, keyword 'packers'

- corresponding searching token is '81ac4a9305a1e8b96418b7b444aa171586bbf8697b84768a0f11dddfccd48533'
- search result is 'c1.txt', 'c2.txt', 'c3.txt', 'c5.txt'
- decrypted results:
 - c1.txt bengals steelers packers

- c2.txt packers patriots
- c3.txt packers
- c5.txt steelers packers
- running time for encrypting index & files: 0.002 seconds
- running time for searching & decrypting files: 0.0016 seconds

For keywords: steelers, bengals, patriots, the search result are showing as below:

```

/usr/bin/python "/Volumes/Macintosh/OneDrive - University of Cincinnati/PycharmProjects/searchable encryption/src/se.py"
program running...
secret key is: a427bab7f0384dd50eb7f2bf6c86e7c6
Running time for encrypting index & files is:0.0027 seconds
please input the search keyword: steelers
The search token is: aae0a09ff5c9b924621f84fecff5989846af92b22624bbfca50eadb94d7e5aeb
searching result is: ['c1.txt', 'c4.txt', 'c5.txt']
c1.txt bengals steelers packers
c4.txt steelers bengals
c5.txt steelers packers
Running time for searching & decrypting files is:0.0063 seconds
Process finished with exit code 0

```

Figure 3

```

/usr/bin/python "/Volumes/Macintosh/OneDrive - University of Cincinnati/PycharmProjects/searchable encryption/src/se.py"
program running...
secret key is: e369d3286c702eb32a0604334711621f
Running time for encrypting index & files is:0.0033 seconds
please input the search keyword: bengals
The search token is: 0bfe298af0976c9460d159cd802af953354c3c15344ef3240ceb16a15d23819a
searching result is: ['c1.txt', 'c4.txt', 'c6.txt']
c1.txt bengals steelers packers
c4.txt steelers bengals
c6.txt bengals
Running time for searching & decrypting files is:0.0014 seconds

```

Figure 4

```

/usr/bin/python "/Volumes/Macintosh/OneDrive - University of Cincinnati/PycharmProjects/searchable encryption/src/se.py"
program running...
secret key is: f666aa90409cc64635d1ba62eb0f9068
Running time for encrypting index & files is:0.0023 seconds
please input the search keyword: patriots
The search token is: 462aec2ca8883242483416b27326b2258b9ae4d116aef0c55c38b1820d07355e
searching result is: ['c2.txt']
c2.txt packers patriots
Running time for searching & decrypting files is:0.0006 seconds
Process finished with exit code 0

```

Figure 5

3. Robust testing

Insert 6 files into the './data/files' folder, so there will be 12 files in this folder, to test this program is generic. The detail information of all files is present in Table1.

Table 1

f1	bengals	steelers	packers
f2	packers	patriots	
f3	packers		
f4	steelers	bengals	
f5	steelers	packers	
f6	bengals		
f7	hao	liu	uc
f8	hao		
f9	liu	uc	
f10	hao	uc	
f11	uc		
f12	basketball	uc	

One thing need to be mentioned in this program is that the order of original files are not seriously related to ciphertexts, but the correctness of search results are not affected. (e.g. 'f2.txt' does not corresponding to 'c2.txt')

```
/usr/bin/python "/Volumes/Macintosh/OneDrive - University of Cincinnati/PycharmProjects/searchable encryption/src/se.py"
program running...
secret key is: 812562d29f9ad1520250b95b845feefd
Running time for encrypting index & files is:0.0049 seconds
please input the search keyword: uc
The search token is: dbdbc8ce6333f81b460c72bf6fdc4e3c37903773aab075474eaa21bf7b7ce595
searching result is: ['c2.txt', 'c3.txt', 'c4.txt', 'c10.txt', 'c12.txt']
c2.txt hao uc
c3.txt uc
c4.txt basketball uc
c10.txt hao liu uc
c12.txt liu uc
Running time for searching & decrypting files is:0.0017 seconds
Process finished with exit code 0
```

Figure 6

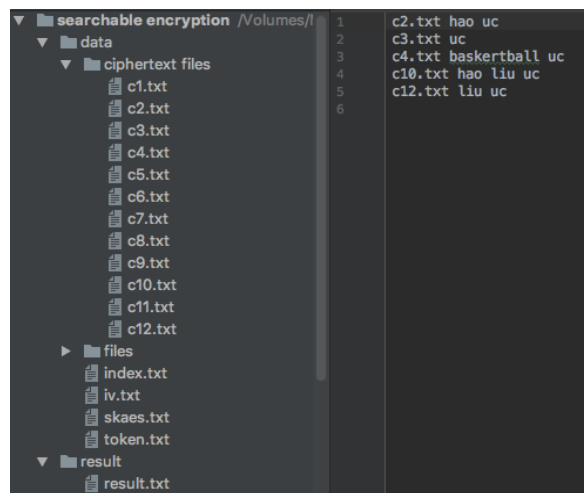


Figure 7

To test this program is generic, 6 files are inserted for test (12 files in total). When I search keyword 'uc', the result shows as figure6-7. From the result present above, we can conclude that this program is generic and effective.