Searchable Encryption

Authors: Kevin Bockenstette - M06637408

Adam Karrasch - M06200572

Matthew Thomas - M05745757

==

Language:

Python 2.7.13 (v2.7.13:a06454b1afa1, Dec 17 2016, 20:53:40)

Operating System:

Windows 10 Home 64-bit (10.0, Build 16299)

==

Compiling instructions:

Program is compiled with the following command

```
python -m py_compile se.py
```

Note, specifying the build directory caused permission errors, so the command builds the .pyc file in the src folder.

==

Libraries Used:

Pycrypto

Used for AES encryption

Hashlib

Used for SHA encryption to emulate a PRF

==

Encryption Parameters:

AES key generated by OS specific random function.

IV declared as a global constant for ease.

SHA256 and AES with λ = 256 used for encryption functions

Implementation of Search:

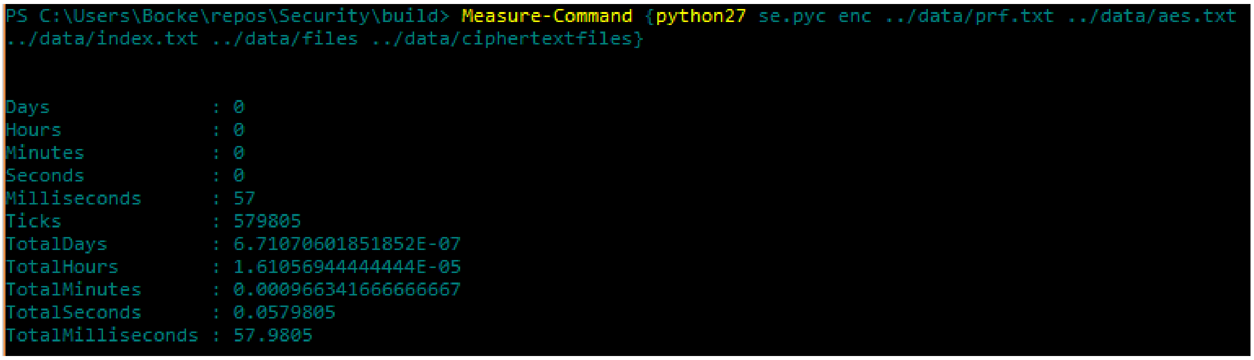
The search has been implemented using native Python dictionaries. Which are hash tables. Each encrypted file name is inserted into the dictionary as the key, with the files kept in the form of a list as the value. When a keyword is searched, first the program checks to see if the key exists within the dictionary, then if it is it retrieves the filenames and proceeds to decrypt them.

===

Running Time:

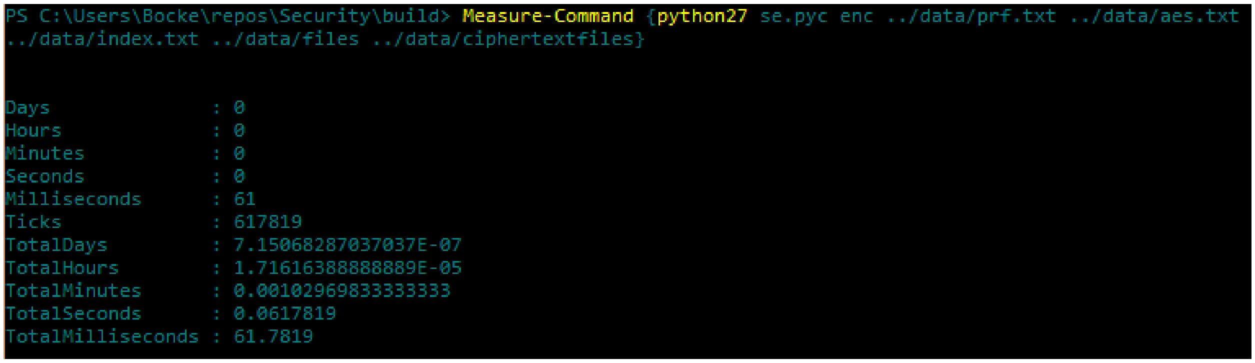
10 total runs were done for both index generation/encrypting and searching/decrypting. Of those 10, the longest and shortest runtimes were screenshot.

Index Generation/Encrypting



```
PS C:\Users\Bocke\repos\Security\build> Measure-Command {python27 se.pyc enc ../data/prf.txt ../data/aes.txt
../data/index.txt ../data/files ../data/ciphertextfiles}


Days              : 0
Hours             : 0
Minutes           : 0
Seconds           : 0
Milliseconds      : 57
Ticks             : 579805
TotalDays         : 6.71070601851852E-07
TotalHours        : 1.61056944444444E-05
TotalMinutes      : 0.000966341666666667
TotalSeconds      : 0.0579805
TotalMilliseconds : 57.9805
```

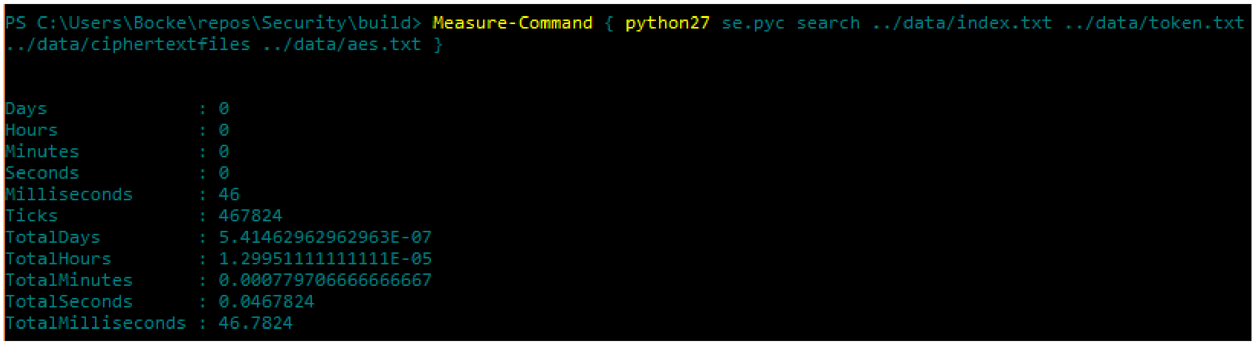


```
PS C:\Users\Bocke\repos\Security\build> Measure-Command {python27 se.pyc enc ../data/prf.txt ../data/aes.txt
../data/index.txt ../data/files ../data/ciphertextfiles}


Days              : 0
Hours             : 0
Minutes           : 0
Seconds           : 0
Milliseconds      : 61
Ticks             : 617819
TotalDays         : 7.15068287037037E-07
TotalHours        : 1.71616388888889E-05
TotalMinutes      : 0.00102969833333333
TotalSeconds      : 0.0617819
TotalMilliseconds : 61.7819
```

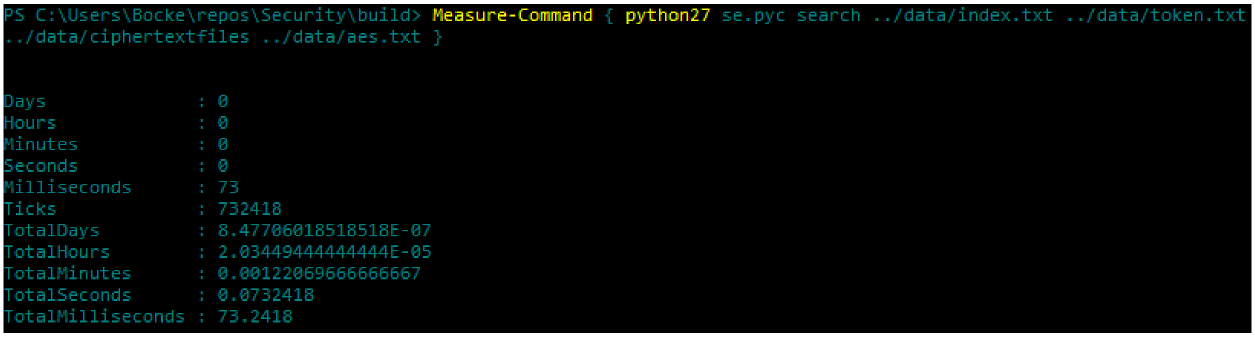
Average Runtime: 59.8812ms

Searching/Decrypting



```
PS C:\Users\Bocke\repos\Security\build> Measure-Command { python27 se.pyc search ../data/index.txt ../data/token.txt
../data/ciphertextfiles ../data/aes.txt }


Days              : 0
Hours             : 0
Minutes           : 0
Seconds           : 0
Milliseconds      : 46
Ticks             : 467824
TotalDays         : 5.41462962962963E-07
TotalHours        : 1.29951111111111E-05
TotalMinutes      : 0.000779706666666667
TotalSeconds      : 0.0467824
TotalMilliseconds : 46.7824
```



```
PS C:\Users\Bocke\repos\Security\build> Measure-Command { python27 se.pyc search ../data/index.txt ../data/token.txt
../data/ciphertextfiles ../data/aes.txt }


Days              : 0
Hours             : 0
Minutes           : 0
Seconds           : 0
Milliseconds      : 73
Ticks             : 732418
TotalDays         : 8.47706018518518E-07
TotalHours        : 2.03449444444444E-05
TotalMinutes      : 0.00122069666666667
TotalSeconds      : 0.0732418
TotalMilliseconds : 73.2418
```

Average Runtime: 60.0121ms

==

Usage:

Key Generation

python se.pyc keygen prf-key-path aes-key-path

Index Generation/Encryption

python se.pyc enc prf-key-path aes-key-path index-path plaintext-directory ciphertext-directory

Token Generation

python se.pyc token token-word prf-key-path token-path

Search/Decryption

python se.pyc search index-path token-path ciphertext-directory aes-key-path