Assignment 2

Saurabh Singh Rana

02/02/2016

1. System Description

Operating system: Ubuntu 14.04 LTS
Systems RAM: 4 GB
Hard DISK: 1 TB
Processor: Intel core i5@2.30GHz.

2. Performance

AES 128

Mean and Median for AES128

```
98. Key : Q4mutzmrQT9tAqnJ
Encrypption Time : 0.708698
Decrypption Time : 0.001658

99. Key : cIoiR3W4Zw5KGCCe
Encrypption Time : 0.666289
Decrypption Time : 0.000596

100. Key : ExW5wIwLm5Euu2BU
Encrypption Time : 0.749773
Decrypption Time : 0.000514


AES128
------
Mean Encryption Time : 0.742196
Mean Decryption Time : 0.000584
Median Encryption Time : 0.731097
Median Decryption Time : 0.000514

Press ENTER to continue AES256 ...
```

AES 256

Mean and Median for AES256

```
97. Key : 1TMqkV19vtd7y8irEa5IHcwSecQEKRxL
Encrypption Time : 0.823726
Decrypption Time : 0.002974

98. Key : tH9dn8kgzNnyWTpi2u0HUwj8Y7LqZIBQ
Encrypption Time : 0.926241
Decrypption Time : 0.000699

99. Key : XI3IQlyQ9jMdB9LD3JUXDCdlJybqEkGk
Encrypption Time : 0.841831
Decrypption Time : 0.001638

100. Key : 0H0O3zmAg8nrH64IPXnchPLyLupYc3Ia
Encrypption Time : 0.841093
Decrypption Time : 0.000634


AES256
------
Mean Encryption Time : 0.840118
Mean Decryption Time : 0.000797
Median Encryption Time : 0.822538
Median Decryption Time : 0.000726

Press ENTER to continue ...
```

MD5

Mean and Median for HMAC MD5

```
95. Time : 0.289041
ae4572360d43c48a9a763895129ebcbc
96. Time : 0.298222
5e438e71810e38582f13d9cd1f29224c
97. Time : 0.293556
20d4bd49ebbe61d0c429cf563851e74e
98. Time : 0.377532
2928f8936f4e157d9cef5c666aec9c3b
99. Time : 0.336321
737372199d25e618c256edaeb2436c85
100. Time : 0.350352
Mean :: 0.355809
Median :: 0.358020
End of MD5 ..Press any ENTER to continue ...
```

SHA1

Mean and Median for SHA1

```
94. Time : 0.341195
ff21560a46b4f3f2d00fe8d82291721463da9568
95. Time : 0.331455
2f8bc5bc3a850113b01011d781f20fa953614315
96. Time : 0.421426
2311d0b2c7e45435abb6a1a6dca48fc45d8b46ff
97. Time : 0.363052
b7a8d67374759c5b4909edcca7317d0575350a81
98. Time : 0.381556
62946380c908e9d63f901de0bc51189bc2e38717
99. Time : 0.395384
a70d53e91f2d7f37ab92c9ebe62a556eda129d9a
100. Time : 0.342837
Mean :: 0.387678
Median :: 0.379451
End of SHA1 ..Press any ENTER to continue ...
```

SHA256

Mean and Median for SHA256

```
c064adedd5154fdcc40c4ef31812ae649b85b992b060552702aa98585a729e94
96. Time : 0.584563

93cdc94372df0ee994b7d9184daa10a7ac1868e557f8d45ba18b1cbab9f268d8
97. Time : 0.646910

3741154b0b72a4af8d1407c7f975716d00100ff4d897b41cfa488ac18a2e9ce0
98. Time : 0.574718

3a90ca5015e104b3b4901a13b1f0c9120f09767485c843f3837cbf957b37c132
99. Time : 0.542577

f9af4f084aec3b14bfd95a34c882580d5b527bd76ed8edbda1e5db648796e18a
100. Time : 0.588170



SHA256
------
Mean :: 0.537317
Median :: 0.538887
```

3. Summary

ENCRYPTION time for AES128 Mean TIME: 0.7422 Median TIME: 0.7312

ENCRYPTION time for AES256 Mean TIME: 0.8401 Median TIME: 0.8225

ENCRYPTION time for HMAC MD5 Mean TIME: 0.3558 Median TIME: 0.3580

ENCRYPTION time for HMAC SHA1 Mean TIME: 0.3877 Median TIME: 0.3794

ENCRYPTION time for HMAC SHA256 Mean TIME: 0.5373 Median TIME: 0.5388

4. File Selection

The following test is performed on 104.9 MB randomly generated text file.

5. Conclusion

The order of their performance is :
MD5-SHA1-SHA256-AES128-AES256

6. Run

make
./cryptogator filename