

Performance Analysis of Encryption Algorithms

vikram0602@ufl.edu, Ufid: 66921015

29 January, 2015

1 To run code:

```
tar xvfz khurana-assign2.tar.gz
cd khurana-assign2
make
./cryptogator <input_file>
< display results >
```

Press any key and then press enter after every algo runs to proceed(may have to enter key twice if buffer doesnot skip any statement)

2 System Description:

operating system: Linux based system

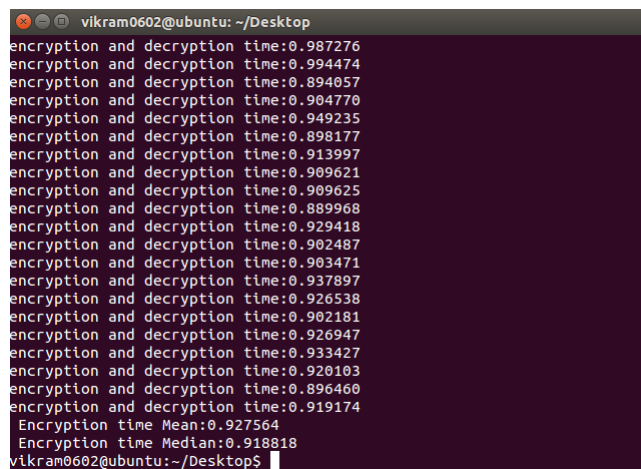
Systems RAM: 6 GB

Hard DISK: 200 GB

Processor: Intel core i5@2.30GHz.

File Description: It is a ebook of type txt of of size 114 mb created for testing these algorithms

3 Performance Analysis:



```
vikram0602@ubuntu: ~/Desktop
encryption and decryption time:0.987276
encryption and decryption time:0.994474
encryption and decryption time:0.894057
encryption and decryption time:0.904770
encryption and decryption time:0.949235
encryption and decryption time:0.898177
encryption and decryption time:0.913997
encryption and decryption time:0.909621
encryption and decryption time:0.909625
encryption and decryption time:0.889968
encryption and decryption time:0.929418
encryption and decryption time:0.902487
encryption and decryption time:0.903471
encryption and decryption time:0.937897
encryption and decryption time:0.926538
encryption and decryption time:0.902181
encryption and decryption time:0.926947
encryption and decryption time:0.933427
encryption and decryption time:0.920103
encryption and decryption time:0.896460
encryption and decryption time:0.919174
Encryption time Mean:0.927564
Encryption time Median:0.918818
vikram0602@ubuntu:~/Desktop$
```

The above image shows the mean and median time calculated for the encryption of file using AES128

```

vikram0602@ubuntu: ~/Desktop
The Bytes Read 16
[263] offer com

encBuffer =
outBuffer = [263] offer com
The Bytes Read 16
prehensive intro

encBuffer =
outBuffer = prehensive intro
The Bytes Read 16
duction11111111

encBuffer =
outBuffer = duction11111111

Encryption time Mean:2.846300
Encryption time Median:2.800279
Decryption time Mean:0.000001
Decryption time Median:0.000001

```

The above image shows the mean and median time calculated for the encryption of file using AES256

```

vikram0602@ubuntu: ~/Desktop
Encryption Time Taken: 0.000028
9e59da4888c8292e40a5a6c595e8600974bbb17
Encryption Time Taken: 0.000027
7c3463205afa8bb6a677f2e09f4dfacce349a19d
Encryption Time Taken: 0.000041
7b9787ccf600eea00ba72eaaa1eb43f44fd84d20
Encryption Time Taken: 0.000040
c96a96309919a5ba04b614917d0d12ff451839
Encryption Time Taken: 0.000051
7ad8acbfd23f1917973b7910583460652f7edc1
Encryption Time Taken: 0.000042
e3652e5212b7f359427b10d5745a09358a6af18
Encryption Time Taken: 0.000041
d34db0b464520a1ee2ac730f54ae9346e76a06b
Encryption Time Taken: 0.000041
8eb0eed5262135965350d9b0a6511f3bf74817d7
Encryption Time Taken: 0.000027
7965f313a0c8356ddc7fdb630d0416c5baba6c4a
Encryption Time Taken: 0.000027
16c82765cfb876a2bf0b965186302ac77522db6
Encryption Time Taken: 0.000027
Encryption time Mean:0.058348
Encryption time Median:0.000127
vikram0602@ubuntu:~/Desktop$

```

The above image shows the mean and median time calculated for the encryption of file using HMAC SHA1.

```

vikram0602@ubuntu: ~/Desktop
Encryption Time Taken: 0.000098
bb8123ce23b5ae91a2981ead424f16f24e9328264818de700a46505561b1f98a
Encryption Time Taken: 0.000097
0959feb6e86fee70741c49f5e909b6aee369caee4e3cece063f6d1a9da0d491e
Encryption Time Taken: 0.000211
cef373cf3239af2759ba7ddcad48c1ca8977132d9d4c57405ceac1094837b8e2
Encryption Time Taken: 0.000182
55aa63e35cc1de40c8f8cab392fa4d01f7bc17fbb0f1a36b702780d3901fc55
Encryption Time Taken: 0.000290
19a38369a340c5fb68e1849eb9a551f9f56d56dc6ad33231bf584ad0e08a1277
Encryption Time Taken: 0.000223
53154f2fc4051de2a2a27e2a8dce2253acf479edb2f25f1d15d4a19ef6c4239b
Encryption Time Taken: 0.000154
76784ada74ff9afa0de1221c804f789aaa2537aa736b3155d695023e1adaf309
Encryption Time Taken: 0.000145
5abeaa10e23c8fc970f51dec626a7b4018f7bbe38fc20b3725658ecaf004ccb1
Encryption Time Taken: 0.000098
ab66ecb5b6133cec570bf2874af591cf99d97607e264bf99664b79219b1e08f9
Encryption Time Taken: 0.000112
7376be75d0633e5454436c284d8ded63d563a5e0fada30735238a070fd60a043
Encryption Time Taken: 0.000101
Encryption time Mean:0.083403
Encryption time Median:0.000144
vikram0602@ubuntu:~/Desktop$

```

The above image shows the mean and median time calculated for the encryption of file using HMAC SHA256

```

vikram0602@ubuntu: ~/Desktop
Encryption Time Taken: 0.000027
ed4d230f982c85be768d0a8ed52aa16
Encryption Time Taken: 0.000027
88833e3edc3c886d59f9b33bc6b9a9c
Encryption Time Taken: 0.000042
5fadee3d4e7be7e6442108e1a96b14
Encryption Time Taken: 0.000041
b9cfcdd931b756ad83739cce5bd76aa
Encryption Time Taken: 0.000042
3d6a13691a27522be4b2bf081915462
Encryption Time Taken: 0.000042
dbcd4c054c190e18ab4026de8f8b13
Encryption Time Taken: 0.000061
af250e0544c27e850e24580e7d44ee
Encryption Time Taken: 0.000042
4bd115e60092f99ce9f3a06fc9be20a
Encryption Time Taken: 0.000027
f7ddd26f1a230bfe4bb210a57c90229
Encryption Time Taken: 0.000027
43d89434920dc45ff0300335f3134b8
Encryption Time Taken: 0.000027
Encryption time Mean:0.080695
Encryption time Median:0.000042
vikram0602@ubuntu:~/Desktop$

```

The above image shows the mean and median time calculated for the encryption of file using HMAC MD5

```

vikram0602@ubuntu: ~/Desktop
8DAC8C5B34A905E009B8D73017954FF007C50D86FFB971A5855001F2BBE4EF8C277CE4523423F20
29A638A379A1EE2113E35AAD888363B7A716D0557701455B98BF4369BDAC31A41D98BD85BCDF01C
2221F75349AAAB8E3B5A0D#)
)
)
The Bytes Read 16
Plain Text:
course, you should
Cipher Text:
(enc-val
(rsa
(a #4951FCB4693FBF3C4CC56199D70465370FCDB0C37BD3C100A801670F173B4892D06B723D4
0EA9B637E1AB07FFA2E69DD083939B75CC80ACECSF70E68EA8E25973C4D30CE31EE874478DD4AD
70230703FB01295EE49B1CF4272C3908DA2F470BE16A387779EB1771D45996506AC03C06E29823
F32D023B4AC9A33B1E90DC#)
)
)
Fatal error: out of core in secure memory
Aborted (core dumped)
vikram0602@ubuntu:~/Desktop$

```

The above image shows the working of RSA algorithm. I was unable to create to calculate encryption type for large file as memory got dumped. And end of file was not reached.

```

Signature:
(sig-val
(rsa
(s #57ED3E5535367D7D78E8880C31872AC3286DD8909882BFB082C52B44288B5D865164077E0
CFAA35FCE78966D61E1EC8C2F7361DA5AF19012274AA7A50738D78247D1FECA142A6F9EDE132C49
5D251B56613B8518FFC9765D51EAA3061C88FD9D0ED0E12861103A97908FEC17014B62CEC55FB3BE
5A70C8F6F95F4E732208DB#)
)
)

```

Digital Signature for RSA1024

ENCRYPTION time for AES128 Mean TIME: 0.92 Median TIME:0.91
 ENCRYPTION time for AES256 Mean TIME: 2.84 Median TIME:2.86
 ENCRYPTION time for HMAC SHA1 Mean TIME: 0.058 Median TIME:0.000127
 ENCRYPTION time for HMAC SHA256 Mean TIME: 0.084 Median TIME:0.000144
 ENCRYPTION time for HMAC MD5 Mean TIME: 0.0806 Median TIME:0.000042

So according to time analysis SHA1 is best for quick hashing/encryption as it is also better than MD5 algorithm in context with security.

incontext with time in ascending order: SHA1-MD5-SHA256-AES128-AES256