Project Ideas

Avinash Rajaraman

02/02/2016

The Objective

The Purpose of this assignment was to implement the following encryption methodologies and document the time taken for encryption and decryption by these algorithms on a file size greater than 100 MB. I have used these algorithms on a video file of size 197.5 MB. This video belongs to the Tonight show with Jimmy Fallon. The Algorithms are as follows: AES128, CTR Mode AES256, CTR Mode RSA1024 RSA4096 HMAC MD5 HMAC SHA1 HMAC SHA256.
Each of these algorithms was to run 100 times each against the file, and the mean and median times for the completion were to be recorded.

System Specifications

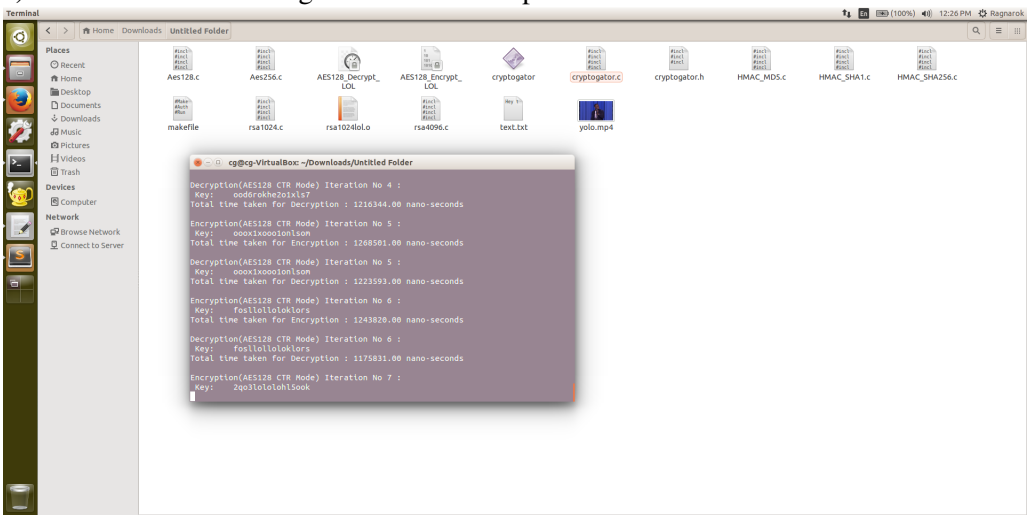
The system I used are of the following specifications. I am running Ubuntu 64 bit on Oracle Virtual Machine.The allocated storage space is 20 GB and the RAM allocated is 4GB. The execution cap is set at 100 percent and the number of processors allocated are 3.The VRAM allocated is 128 MB.

Observations:

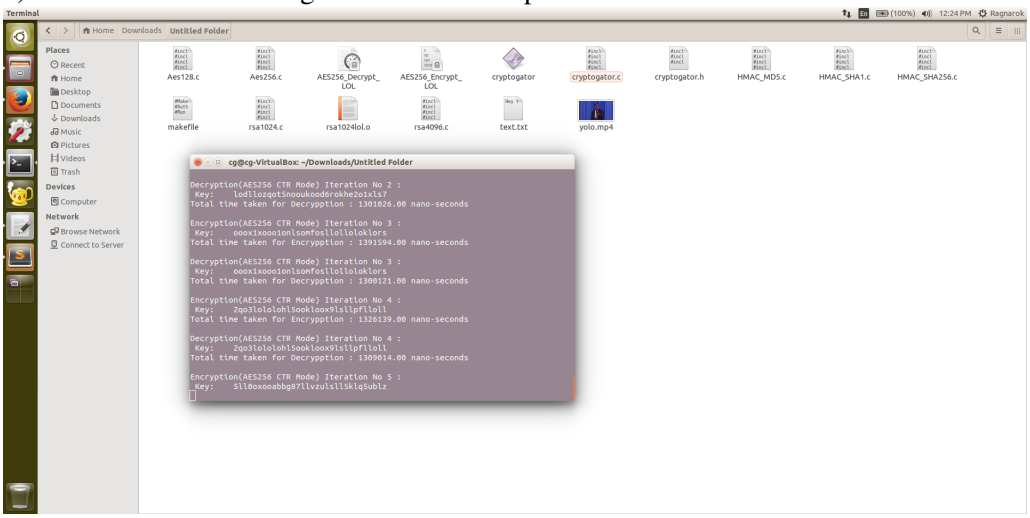
a) AES128 Encryption: This encryption technique was implemented in the Counter mode. This was successfully run 100 times. The average encryption time was:1.222s and Decryption time was:1.21s.The median encryption time was:1.225s and Decryption time was:1.119s .
b) AES256 Encryption: This encryption technique was implemented in the Counter mode. This was successfully run 100 times. The average encryption time was:1.311s and Decryption time was:1.313s .The median encryption time was:1.306s and Decryption time was:1.3101s
c) HMAC MD5: This encryption technique was implemented and successfully run 100 times. The average hash time was:7900ns and the median hash time was:6000ns
d) HMAC SHA1: This encryption technique was implemented and successfully run 100 times. The average hash time was:5100ns and the median hash time was:4000ns:
e) HMAC SHA256: This encryption technique was implemented and successfully run 100 times. The average hash time was:8400ns and the median hash time was:7000ns
f) RSA1024: I successfully implemented this, but I could not run it 100 times due to time constraints. Based on 20 executions, The average encryption time and Decryption time was: 1681.08s and the median of these times were: 1663.02
g) RSA4096: I successfully implemented this, but I could not run it even once due to time constraints. But it has successfully executed on files of substantially smaller size

ScreenShots:

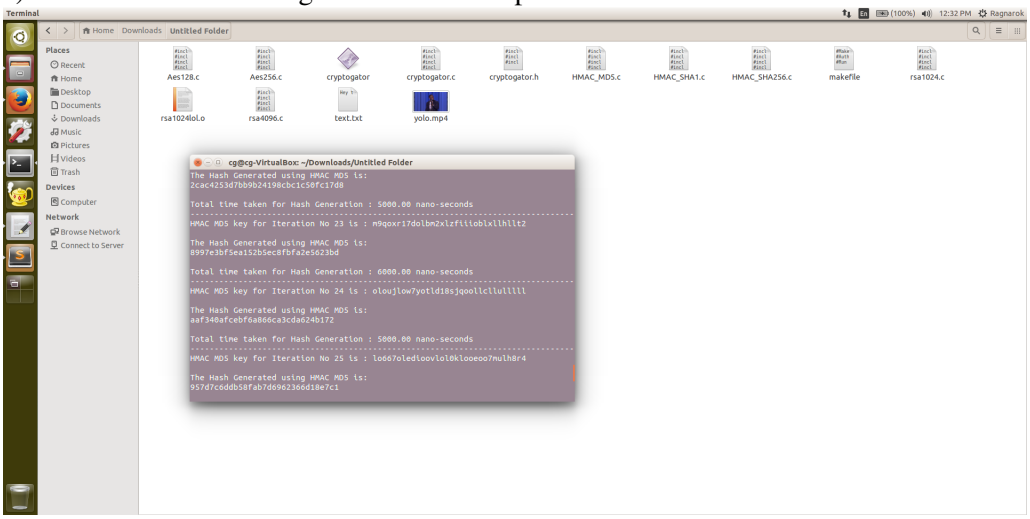
a) The screenshot showing AES128 CTR Implementation:



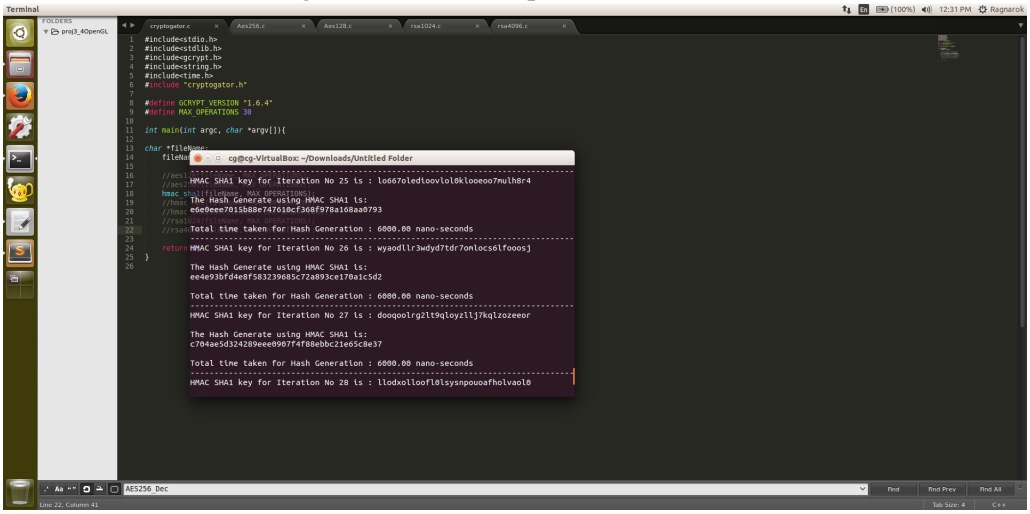
b) The screenshot showing AES256 CTR Implementation:



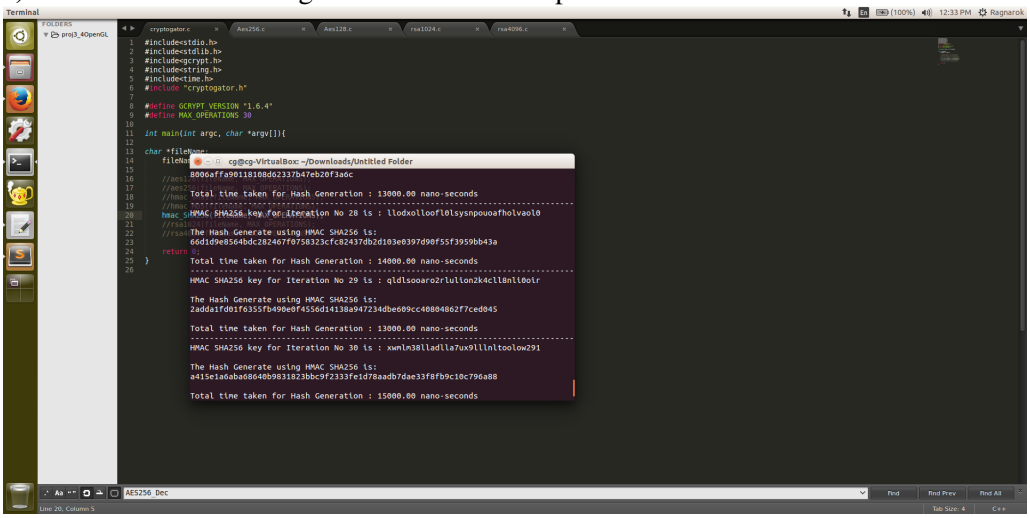
c) The screenshot showing HMAC MD5 Implementation:



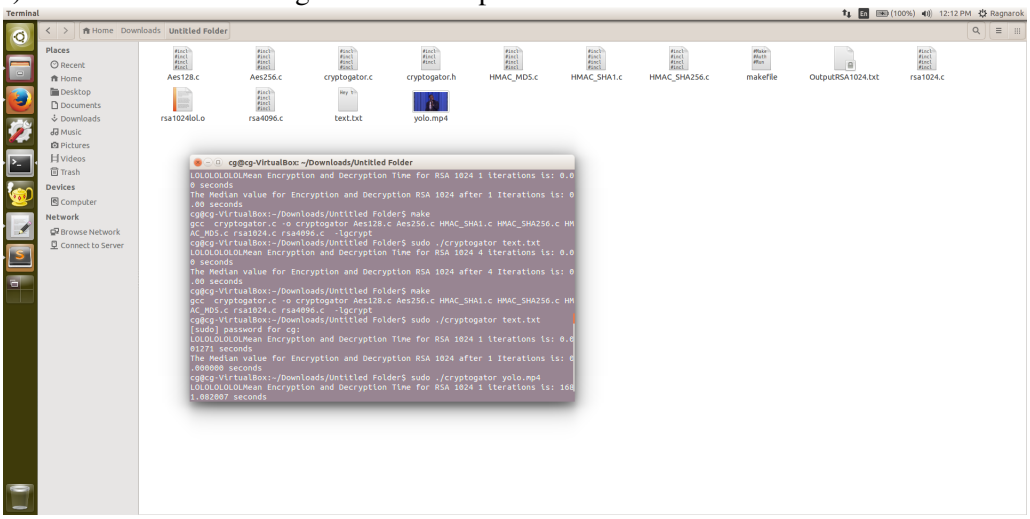
d) The screenshot showing HMAC SHA1 Implementation:



e) The screenshot showing HMAC SHA256 Implementation:



f) The screenshot showing RSA 1024 Implementation:



Conclusions:

My findings based on the time taken n=100, by all the algorithms are that RSA 4096 costs the most, as the encryption and Decryption time of this is the maximum. In the increasing order of execution times, the algorithms are as follows: HMAC SHA1, HMAC MD5,HMAC SHA256,AES128 CTR,AES256 CTR,RSA 1024, RSA 4096.