

Assignment 2 - Using Cryptographic Libraries

Siddhant Deshmukh

2-1-2016

1 Introduction

In this assignment I compared the performance trade-offs between various symmetric encryption, asymmetric encryption and hashing algorithms. I used the Gcrypt library provided by the Linux operating system and used a Macbook Pro to run the code.

2 Details of Machine

1. Processor

- 2.7GHz dual-core Intel Core i5 processor with Turbo Boost up to 3.1GHz
- 3MB shared L3 cache

2. Memory

- 8GB of 1866MHz LPDDR3 (RAM)
- 256GB PCIe-based flash storage (Internal Memory)

3. Graphics

- Intel Iris Graphics 6100

3 Input File Used

- Used input file "book.txt" which is a text file containing multiple novels.
- Length is 117.1 MB

4 AES 128

1. Block Length : 128 bits (16 bytes)
2. Mode : Counter Mode
3. Counter Length : 128 bits (16 bytes)
4. Key Length : 128 bits (16 bytes)
5. Time Analysis :

Figure 1: Output for AES 128

```
RUNNING AES 128...  
  
MEAN TIME FOR AES128 ENCRYPTION IS :8982.122734 ms  
  
MEDIAN TIME FOR AES128 ENCRYPTION IS :8543.767263 ms  
  
MEAN TIME FOR AES128 DECRYPTION IS :21736.383847 ms  
  
MEDIAN TIME FOR AES128 DECRYPTION IS :20827.561102 ms
```

- Mean Encryption Time : 8982.12 ms
- Mean Decryption Time : 21736.38 ms
- Median Encryption Time : 8543.76 ms
- Median Decryption Time : 20827.56 ms

5 AES 256

1. Block Length : 128 bits (16 bytes)
2. Mode : Counter Mode
3. Counter Length : 128 bits (16 bytes)
4. Key length : 256 bits (32 bytes)
5. Time Analysis :
 - Mean Encryption Time : 11946.21 ms
 - Mean Decryption Time : 26518.38 ms
 - Median Encryption Time : 10252.51 ms
 - Median Decryption Time : 26525.98 ms

Figure 2: Output for AES 256

```
RUNNING AES 256...  
  
MEAN TIME FOR AES256 ENCRYPTION IS :11946.219612 ms  
  
MEDIAN TIME FOR AES256 ENCRYPTION IS :10252.512243 ms  
  
MEAN TIME FOR AES256 DECRYPTION IS :26518.383600 ms  
  
MEDIAN TIME FOR AES256 DECRYPTION IS :26525.980422 ms
```

Figure 3: Output for MD5

```
MEAN TIME FOR MD5 IS :292.001170 ms  
  
MEDIAN TIME FOR MD5 IS :289.293000 ms
```

6 MD5

1. Key length : 64 bytes
2. Time Analysis :
 - Mean Hashing Time : 292.00 ms
 - Median Hashing Time : 289.29 ms

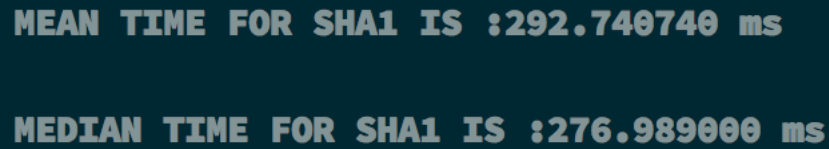
7 SHA 1

1. Key length : 64 bytes
2. Time Analysis :
 - Mean Hashing Time : 292.74 ms
 - Median Hashing Time : 276.99 ms

8 SHA 256

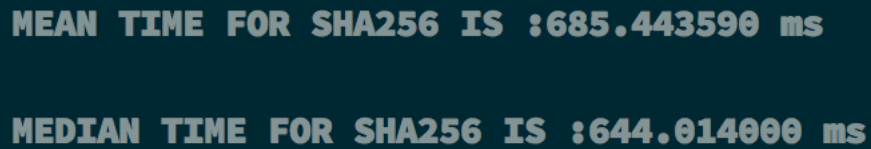
1. Key length : 64 bytes

Figure 4: Output for SHA 1



```
MEAN TIME FOR SHA1 IS :292.740740 ms  
MEDIAN TIME FOR SHA1 IS :276.989000 ms
```

Figure 5: Output for SHA 256



```
MEAN TIME FOR SHA256 IS :685.443590 ms  
MEDIAN TIME FOR SHA256 IS :644.014000 ms
```

2. Time Analysis :

- Mean Hashing Time : 685.44 ms
- Median Hashing Time : 644.10 ms

9 RSA 1024

1. Block Length : 64 bytes

2. Mode : Electronic code book (ECB)

3. Key length : 1024 bits

4. Time Analysis :

- Mean Encryption Time : 63876.03 ms (64 seconds)
- Mean Decryption Time : 2718494.11 ms (45 minutes)
- Median Encryption Time : 61432.29 ms
- Median Decryption Time : 2819290.55 ms

Figure 6: Output for RSA 1024

```
RUNNING RSA 1024...  
  
MEAN TIME FOR RSA1024 ENCRYPTION IS :63876.031000 ms  
  
MEDIAN TIME FOR RSA1024 ENCRYPTION IS :61432.290090 ms  
  
MEAN TIME FOR RSA1024 DECRYPTION IS :2718494.115001 ms  
  
MEDIAN TIME FOR RSA1024 DECRYPTION IS :2819290.547831 ms  
Siddhants-MacBook-Pro:Desktop siddhantdeshmukh$
```

10 RSA 4096

1. Block Length : 64 bytes
2. Mode : Electronic code book (ECB)
3. Key length : 4096 bits
4. Time Analysis :
 - RSA 4096 took an excruciatingly long time to run and I ran it for about 2-3 days and got readings based on that.
 - Mean Encryption Time : 362177.03 ms (6 minutes)
 - Mean Decryption Time : 53608703.11 ms (15 hours)
 - Median Encryption Time : 362177.03 ms
 - Median Decryption Time : 52649835.63 ms

Figure 7: Output for RSA 4096

```
RUNNING RSA 4096...  
  
MEAN TIME FOR RSA4096 ENCRYPTION IS :362177.031000 ms  
  
MEDIAN TIME FOR RSA4096 ENCRYPTION IS :362177.031000 ms  
  
MEAN TIME FOR RSA4096 DECRYPTION IS :53608703.115001 ms  
  
MEDIAN TIME FOR RSA4096 DECRYPTION IS :52649835.625931 ms  
Siddhants-MacBook-Pro:Desktop siddhantdeshmukh$
```

11 Digital Signature

I generated a digital signature (using HMAC SHA256 and RSA 4096). I printed the S-expression of the encrypted HMAC SHA256 of the input file.

```

RUNNING DIGITAL SIGNATURE 256...

digital signature: (7:sig-val
(3:rsa
(1:s512:*XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXrgCq;E8~4q+qL'qAq(pqtXXXXXXXXXX
}lqiNFqe
.M,CMpL_Z6q,q&qYqq.qJ:hq
tF
?
?K?V?v?z?*2B??BF[?]???X50?Q/m?
?f??
,enc [qbxxxx(m0)
)
)

the digital signature of sha256 was successfullly created.
Sucessfully verfiied digital signature!
Siddhants-MacBook-Pro:Desktop siddhantdeshmukh$ █

```

On a concluding note, I learned a tremendous amount from this assignment. Firstly, I used a low level programming language(c) for the first time and it was an extremely interesting and challenging experience. I have used all the same cryptographic libraries in a previous project(done in scala) but using gcrypt in c was much more challenging. Secondly, I learned how to use the basic security techniques and I am confident about securing any project of mine in the future. Finally, I got an insight about the running time of the various algorithms. As Professor Traynor had told us in class that some facts would be embedded deeply in our minds after we complete the project. This is exactly what happened in my case as I realized how slow RSA is compared to hashing and AES and how fast the hashing algorithms are compared to the ciphers. We should use RSA only for the initial key exchange(AES key) and encrypt all the subsequent messages and files using AES. I used charts to complete my analysis as shown on the next page.

Figure 9: Following charts show the performance comparison between the algorithms. Each chart has running time on Y-axis and algorithm on X-axis. As expected MD5 is the fastest, followed by SHA 1, SHA 256, AES 128, AES 256, RSA 1024 and finally RSA 4096. The bottom-most chart shows the order of the algorithms in terms of running time from left to right(fastest algorithm on the left).

