CANNY, LUKE (19339166)

CT437 Assignment 2

Using and Benchmarking Blockciphers using OpenSSL

# Introduction

In this assignment, OpenSSL is used to encrypt and decrypt data using different blockciphers. The CPU time of each algorithm is measured and compared in this report. This report is broken down into two primary sections covering problem 1 and problem 2 as outlined in the assignment brief.

# Problem 1: Blockcipher Benchmarking

In this section, the following encryption settings are first measured (CPU time) and then contrast:

* AES, ARIA and Camellia Algorithm
* 128- and 256-bit key length
* ECB, CBC and GCM mode
* 10 MB and 100 MB of data
* encoding and decoding

In the following plot, the average time taken to complete encryption or decryption is measured for different block sizes. From the graph is it evident that AES (advanced encryption standard) algorithm is significantly faster than ARIA or Camellia regardless of the size of the plaintext.

Figure 1 Plot of average time to complete operation against configuration used.

From the graph, it may also be observed that the size of the plaintext (10 or 100 megabytes) has little impact on the performance of each algorithm in most configurations with the exception of the AES algorithm, in CBC mode. In this configuration, the algorithm is significantly slower when encrypting the data. The decryption speed of AES in CBC mode is comparable to the other AES algorithm configurations.

The graph also presents another characteristic which impacts the performance of each algorithm, the size of the key. It is clear from the figure that configurations with a 128-bit key can encrypt and decrypt faster than their 256-bit counterparts. When looking at CPU time alone, this would make 128-bit keys seem more advantageous, however it must be noted that a smaller key reduces the level of protection each algorithm provides. On average, 128-bit key configurations were 20.9% lower than its 256-bit counterpart. In my opinion, the performance gain is not significant enough to warrant the loss in resilience of the ciphertext produced.

# Problem 2: Implementing and Benchmarking Triple-DES

Yadda Yadda Yadda

# Appendix

GitHub Repo: <https://github.com/lukecanny/CT437_A2_OpenSSL>