AES Block Cipher Modes

1. Introduction 3

1.1. ECB 3

1.2. CBC 3

1.3. OFB 3

1.4. CTR 3

1.5. CFB 4

2. Programs 4

2.1. Key Generation 4

2.1.1. Run 4

2.1.2. Input 4

2.1.3. Output 4

2.2. Encryption 4

2.2.1. Run 4

2.2.2. Input 5

2.2.3. Output 5

2.3. Decryption 5

2.3.1. Run 5

2.3.2. Input 5

2.3.3. Output 5

3. Software Libraries 5

3.1. Cryptopp 5

4. Performance Analysis 5

4.1. Overview 6

4.2. ECB 6

4.3. CBC 6

4.4. OFB 6

4.5. CTR 6

4.6. CFB 6

4.7. Encryption 6

4.8. Decryption 8

4.9. Conclusions 10

# Introduction

This document presents a view into and an analysis of the block cipher modes for the block cipher AES. AES is the Advanced Encryption Standard with a fixed block size of 128 bits. We will be analyzing the various block cipher modes for AES. The modes to be analyzed are ECB, CBC, OFB, Counter, and CFB. Each of these modes have different levels of security and efficiency. The primary focus of the program presented is to analyze the efficiency of each block cipher mode and compare them with each other. The comparisons will be made encrypting messages of varying lengths and with keys of varying lengths.

## ECB

Electronic codebook mode is a mode that breaks down the plaintext into a series of blocks and then passes the plaintext block into an encryption algorithm with another input of a private key. Each block of plaintext is treated in this manner without any block relying on the previous block. Because of this, ECB is a deterministic mode and does not provide indistinguishability. This mode is generally not used as it is not a very secure method but is included in the analysis as it is a valid mode and is needed for completeness.

## CBC

Cipher Block Chaining mode breaks the plaintext down into block of plaintext. For the first block, the plaintext is XORed with an IV (initialization vector - generally a random value) and the output form this is sent to the encryption algorithm along with the key. For the remaining blocks, the output ciphertext from the previous encryption is then XORed with the plaintext block for the input into the encryption algorithm along with the key. Since each block is linked to the previous block, the name chaining is used. This mode does provide indistinguishability with a chosen message attack.

## OFB

Output feedback mode makes a stream of keys that are XORed with the plaintext to create the ciphertext. The plaintext message is broken down into blocks. On the first block, an IV and the key are input into the encryption algorithm and the output is XORed with the plaintext block to generate the ciphertext. The output is also sent as the input of the next run with the key. The generation of the key stream can be ran independently of the XORing with the plaintext and so can be precomputed to allow for parallelization of the XOR process when the plaintext is available. This mode is also secure with the sense of indistinguishability for chosen message attack.

## CTR

Counter mode creates a key stream similar to that of OFB. This mode will take an IV as the first input along with the key to the stream and then each additional run will increment the initial IV as a counter does. The output of each round is XORed with the plaintext block to generate the ciphertext. As with OFB, CTR is secure in the sense of indistinguishability for chosen message attack.

## CFB

Cipher Feedback mode combines the ideas from CBC and OFB. The first round will take an IV and key as the input into the encryption algorithm and the output will be XORed with the plaintext block to generate the ciphertext. For each additional round, the ciphertext from the previous round will be used as the input along with the key into the encryption algorithm of that round. The plaintext block is then XORed with the output from that to generate the ciphertext. As this is closely related with CBC and OFB, this mode should be secure in the sense of indistinguishability for chosen message attacks as long as the encryption algorithm is a pseudorandom permutation.

# Programs

The program used for analyzing these modes is written in C++ with three programs: keygen, encrypt, decrypt.

## Key Generation

The program keygen generates the private key that will be used for encryption and decryption. This key is generated with an random generator and will generate multiple key lengths.

### Run

To run keygen, at the command line type:

#>./keygen -s keysize

If no key size is defined then the default of 16 will be used. The values for key size are 16, 24, and 32 which correspond to key sizes of 128 bit, 192 bit, and 256 bit respectively.

### Input

The input is just the size of the key desired. Either 16, 24, or 32.

### Output

The output will be a text file called key.txt which will hold the key in hex format.

## Encryption

The program encrypt will encrypt plaintext into ciphertext with AES using the modes of operation that were discussed in the introduction. Each mode is timed to allow for analyzation of the running of each mode.

### Run

To run encrypt, at the command line type:

#> encrypt [-bv] [-k key\_file=""key.txt""] [-s key\_size (16, 24, 32)] [-m mode (CBC, OFB, CFB, ECB, CTR)] [-l loop\_count] [-p plaintext\_file] [-c ciphertext\_file]

### Input

The input to the encrypt program is the key file and the plaintext file along with the options for mode of operation.

### Output

The program outputs a file with the ciphertext based on the mode of operation. Also, timing information is output for analyzation of the modes of operation.

## Decryption

The decrypt program will take the ciphertext and decrypt it into plaintext using AES and a mode of operation as discussed in the introduction. The program times each mode of operation so that the mode can be analyzed.

### Run

To run encrypt, at the command line type:

#> decrypt [-bv] [-k key\_file] [-s key\_size (16, 24, 32)] [-m mode (CBC, OFB, CFB, ECB, CTR)] [-l loop\_count] [-p plaintext\_file] [-c ciphertext\_file]

### Input

The input to the program decrypt is the key file, the ciphertext file and the mode of operation.

### Output

The program decrypt outputs a plaintext file based on the ciphertext and the mode of operation used. Also, timing information is output for analyzation of the modes of operation.

# Software Libraries

As the program is a C++ program, it was chosen to use the public library cryptopp for implementing the various modes of operation for AES.

## Cryptopp

http://www.cryptopp.com/ - more explanations to come as to what is useful from this library such as random generators, modes of operation, and file and string handling.

# Performance Analysis

The encrypt and decrypt programs used timing mechanisms in order to provide information on the running of each program. The analysis is based on the key size, the size of the plaintext, and the time it took to encrypt and decrypt the files for each mode of operation.

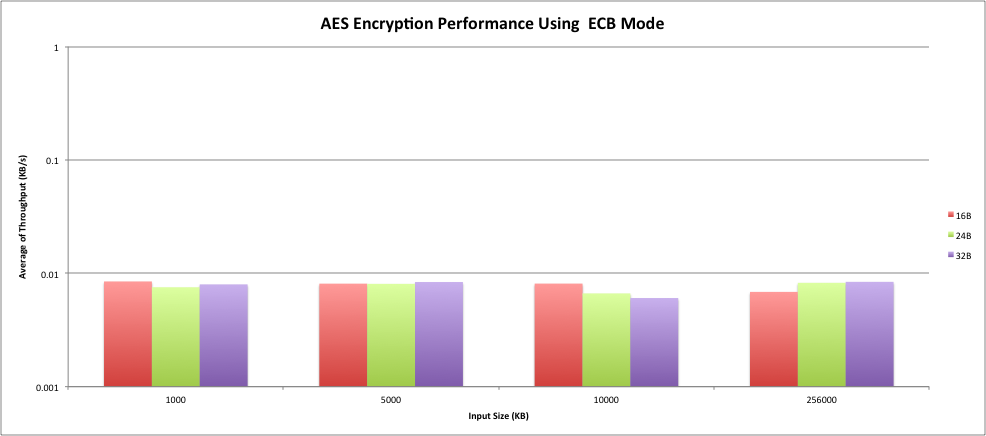
## Overview

The analysis for the performance of each mode of operation is based on the comparison of each mode individually and then each mode comparatively. First we look at how each mode of operation handles the different key sizes with the different text file sizes. Then we show how each mode of operation compares with each other based on key size and file size. The goal is to see how the size of the key can affect the performance and how the size of the file can affect the performance.

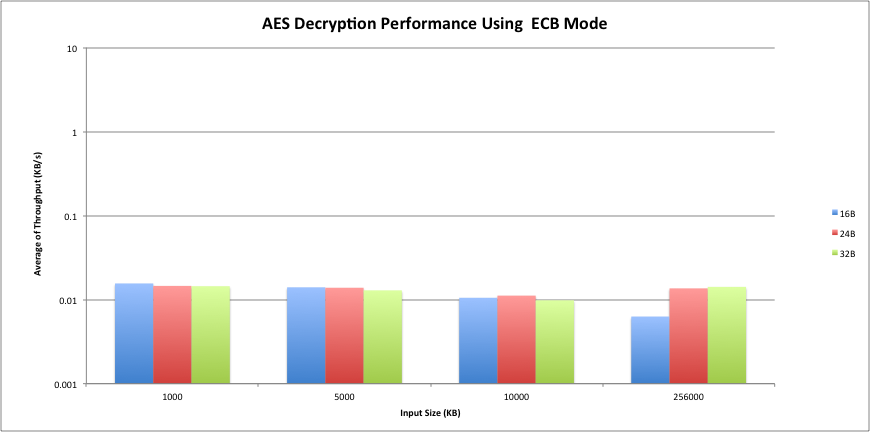
## ECB

This shows graphs for ECB mode of operation:

Encryption:



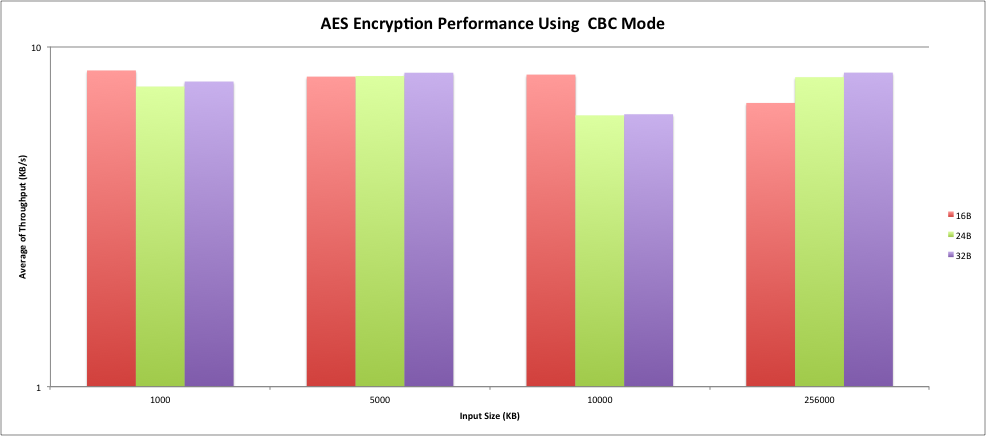
Decryption:



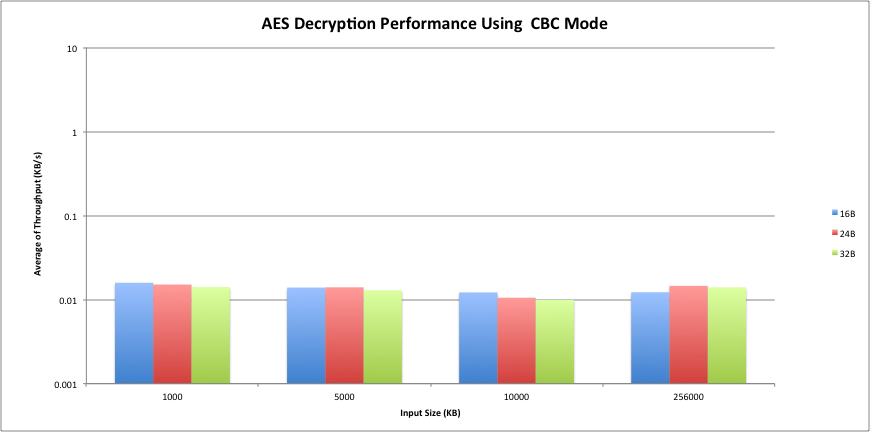
## CBC

This shows graphs for CBC mode of operation:

Encryption:



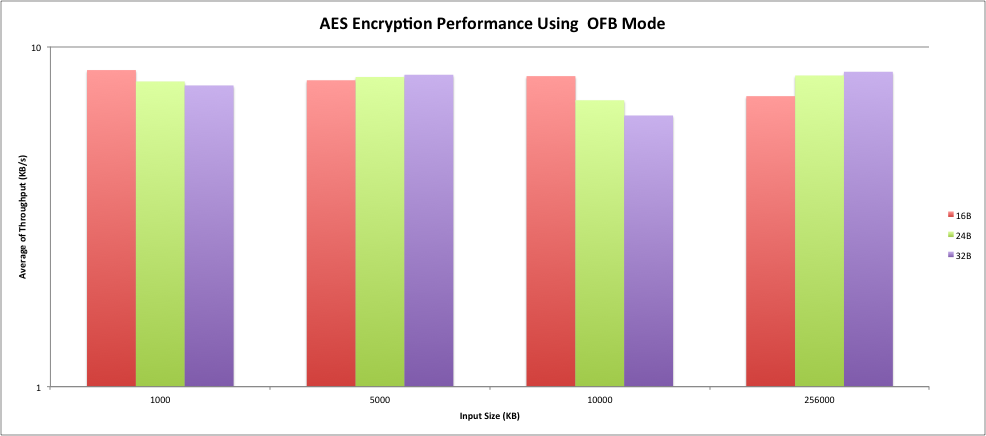
Decryption:



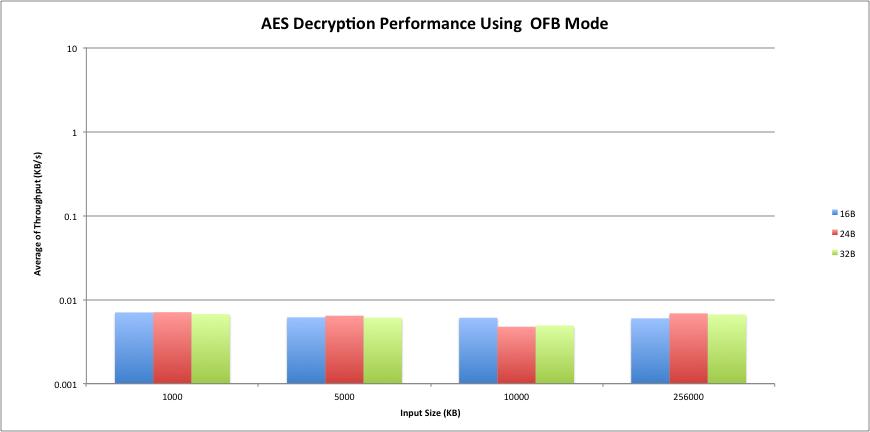
## OFB

This shows graphs for OFB mode of operation:

Encryption:



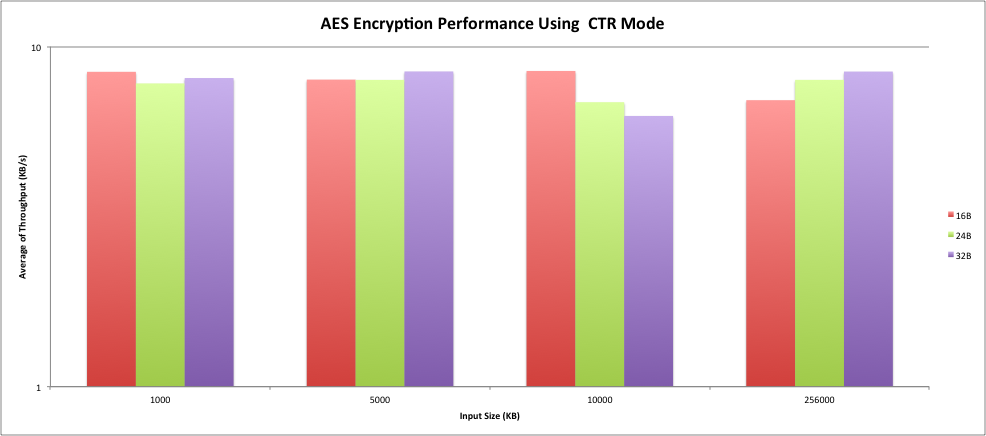
Decryption:



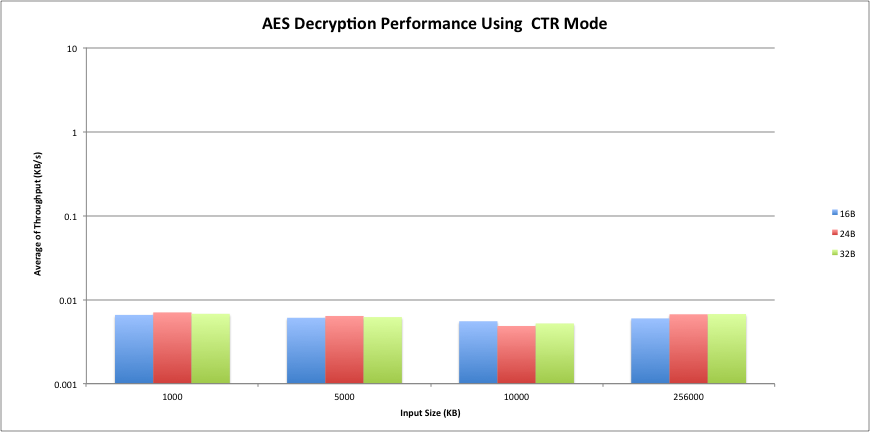
## CTR

This shows graphs for CTR mode of operation:

Encryption:



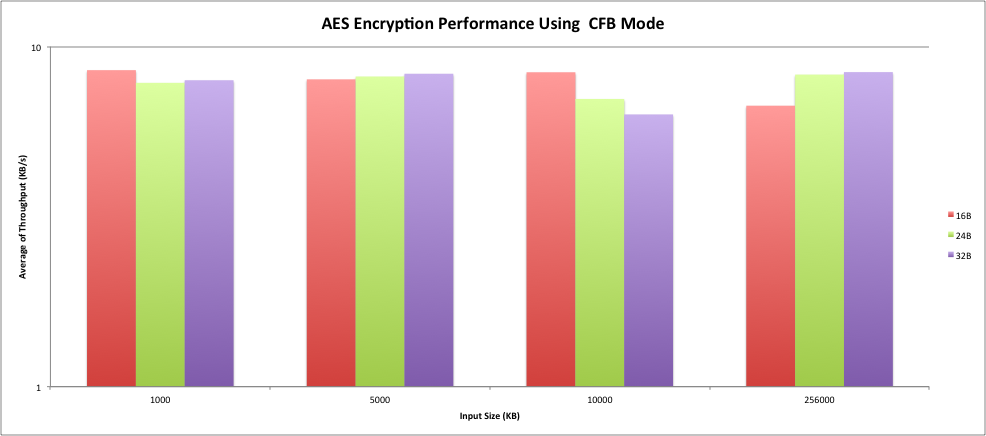
Decryption:



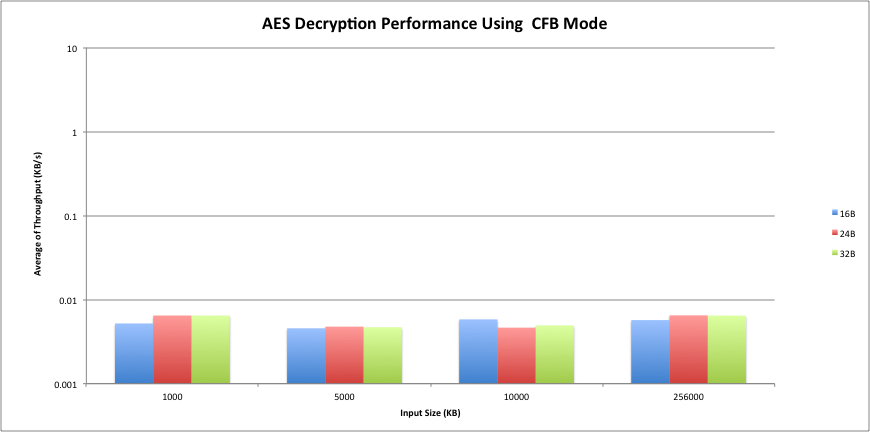
## CFB

This shows graphs for CFB mode of operation:

Encryption:



Decryption:



## Encryption

This section will show a comparison of the modes of operation with each other for encryption. A table will also show the min, max and average values for throughput for each mode.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Cipher Block Mode | Key Length | Message Length | Min (ms) | Max (ms) | Avg (ms) |
| ECB | 128 bit | 16 B |  |  |  |
|  | 128 bit | 32 B |  |  |  |
|  | 128 bit | 10 MB |  |  |  |
|  | 128 bit | 256 MB |  |  |  |
| CBC | 128 bit | 16 B |  |  |  |
|  | 128 bit | 32 B |  |  |  |
|  | 128 bit | 10 MB |  |  |  |
|  | 128 bit | 256 MB |  |  |  |
| OFB | 128 bit | 16 B |  |  |  |
|  | 128 bit | 32 B |  |  |  |
|  | 128 bit | 10 MB |  |  |  |
|  | 128 bit | 256 MB |  |  |  |
| CFB | 128 bit | 16 B |  |  |  |
|  | 128 bit | 32 B |  |  |  |
|  | 128 bit | 10 MB |  |  |  |
|  | 128 bit | 256 MB |  |  |  |
| CTR | 128 bit | 16 B |  |  |  |
|  | 128 bit | 32 B |  |  |  |
|  | 128 bit | 10 MB |  |  |  |
|  | 128 bit | 256 MB |  |  |  |
|  |  |  |  |  |  |
| ECB | 192 bit | 16 B |  |  |  |
|  | 192 bit | 32 B |  |  |  |
|  | 192 bit | 10 MB |  |  |  |
|  | 192 bit | 256 MB |  |  |  |
| CBC | 192 bit | 16 B |  |  |  |
|  | 192 bit | 32 B |  |  |  |
|  | 192 bit | 10 MB |  |  |  |
|  | 192 bit | 256 MB |  |  |  |
| OFB | 192 bit | 16 B |  |  |  |
|  | 192 bit | 32 B |  |  |  |
|  | 192 bit | 10 MB |  |  |  |
|  | 192 bit | 256 MB |  |  |  |
| CFB | 192 bit | 16 B |  |  |  |
|  | 192 bit | 32 B |  |  |  |
|  | 192 bit | 10 MB |  |  |  |
|  | 192 bit | 256 MB |  |  |  |
| CTR | 192 bit | 16 B |  |  |  |
|  | 192 bit | 32 B |  |  |  |
|  | 192 bit | 10 MB |  |  |  |
|  | 192 bit | 256 MB |  |  |  |
|  |  |  |  |  |  |
| ECB | 256 bit | 16 B |  |  |  |
|  | 256 bit | 32 B |  |  |  |
|  | 256 bit | 10 MB |  |  |  |
|  | 256 bit | 256 MB |  |  |  |
| CBC | 256 bit | 16 B |  |  |  |
|  | 256 bit | 32 B |  |  |  |
|  | 256 bit | 10 MB |  |  |  |
|  | 256 bit | 256 MB |  |  |  |
| OFB | 256 bit | 16 B |  |  |  |
|  | 256 bit | 32 B |  |  |  |
|  | 256 bit | 10 MB |  |  |  |
|  | 256 bit | 256 MB |  |  |  |
| CFB | 256 bit | 16 B |  |  |  |
|  | 256 bit | 32 B |  |  |  |
|  | 256 bit | 10 MB |  |  |  |
|  | 256 bit | 256 MB |  |  |  |
| CTR | 256 bit | 16 B |  |  |  |
|  | 256 bit | 32 B |  |  |  |
|  | 256 bit | 10 MB |  |  |  |
|  | 256 bit | 256 MB |  |  |  |

More text here

## Decryption

This section will show a comparison of the modes of operation with each other for decryption. A table will also show the min, max and average values for throughput for each mode.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Cipher Block Mode | Key Length | Message Length | Min (ms) | Max (ms) | Avg (ms) |
| ECB | 128 bit | 16 B |  |  |  |
|  | 128 bit | 32 B |  |  |  |
|  | 128 bit | 10 MB |  |  |  |
|  | 128 bit | 256 MB |  |  |  |
| CBC | 128 bit | 16 B |  |  |  |
|  | 128 bit | 32 B |  |  |  |
|  | 128 bit | 10 MB |  |  |  |
|  | 128 bit | 256 MB |  |  |  |
| OFB | 128 bit | 16 B |  |  |  |
|  | 128 bit | 32 B |  |  |  |
|  | 128 bit | 10 MB |  |  |  |
|  | 128 bit | 256 MB |  |  |  |
| CFB | 128 bit | 16 B |  |  |  |
|  | 128 bit | 32 B |  |  |  |
|  | 128 bit | 10 MB |  |  |  |
|  | 128 bit | 256 MB |  |  |  |
| CTR | 128 bit | 16 B |  |  |  |
|  | 128 bit | 32 B |  |  |  |
|  | 128 bit | 10 MB |  |  |  |
|  | 128 bit | 256 MB |  |  |  |
|  |  |  |  |  |  |
| ECB | 192 bit | 16 B |  |  |  |
|  | 192 bit | 32 B |  |  |  |
|  | 192 bit | 10 MB |  |  |  |
|  | 192 bit | 256 MB |  |  |  |
| CBC | 192 bit | 16 B |  |  |  |
|  | 192 bit | 32 B |  |  |  |
|  | 192 bit | 10 MB |  |  |  |
|  | 192 bit | 256 MB |  |  |  |
| OFB | 192 bit | 16 B |  |  |  |
|  | 192 bit | 32 B |  |  |  |
|  | 192 bit | 10 MB |  |  |  |
|  | 192 bit | 256 MB |  |  |  |
| CFB | 192 bit | 16 B |  |  |  |
|  | 192 bit | 32 B |  |  |  |
|  | 192 bit | 10 MB |  |  |  |
|  | 192 bit | 256 MB |  |  |  |
| CTR | 192 bit | 16 B |  |  |  |
|  | 192 bit | 32 B |  |  |  |
|  | 192 bit | 10 MB |  |  |  |
|  | 192 bit | 256 MB |  |  |  |
|  |  |  |  |  |  |
| ECB | 256 bit | 16 B |  |  |  |
|  | 256 bit | 32 B |  |  |  |
|  | 256 bit | 10 MB |  |  |  |
|  | 256 bit | 256 MB |  |  |  |
| CBC | 256 bit | 16 B |  |  |  |
|  | 256 bit | 32 B |  |  |  |
|  | 256 bit | 10 MB |  |  |  |
|  | 256 bit | 256 MB |  |  |  |
| OFB | 256 bit | 16 B |  |  |  |
|  | 256 bit | 32 B |  |  |  |
|  | 256 bit | 10 MB |  |  |  |
|  | 256 bit | 256 MB |  |  |  |
| CFB | 256 bit | 16 B |  |  |  |
|  | 256 bit | 32 B |  |  |  |
|  | 256 bit | 10 MB |  |  |  |
|  | 256 bit | 256 MB |  |  |  |
| CTR | 256 bit | 16 B |  |  |  |
|  | 256 bit | 32 B |  |  |  |
|  | 256 bit | 10 MB |  |  |  |
|  | 256 bit | 256 MB |  |  |  |

More text here.

## Conclusions