**BÁO CÁO**

**BÀI THỰC HÀNH SỐ 01 – 02**

**MÔN: MẬT MÃ HỌC**

Họ và tên: Nguyễn Văn Thọ

MSSV: 20521974

Lớp: NT219.M21.ANTN

**TASK 1: CODING AES & DES USING CRYPTOPP LIBRARY**

* **Hardware resources**

|  |  |
| --- | --- |
| **Tên phần cứng** | **Thông số** |
| CPU | Intel core i5 8300H CPU @2.3GHz |
| RAM | 8GB |

**1**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Windows AES Encryption** | | | | | | |
| Input  Mode | 100KB | 200KB | 500KB | 1MB | 2MB | 5MB |
| ECB | 0.04ms | 0.06ms | 0.12ms | 0.32ms | 0.84ms | 1.25ms |
| CBC | 0.14ms | 0.18ms | 0.57ms | 1.02ms | 2.93ms | 5.05ms |
| OFB | 0.15ms | 0.23ms | 0.62ms | 1.14ms | 3.16ms | 5.28ms |
| CFB | 0.15ms | 0.25ms | 0.55ms | 1.05ms | 2.71ms | 5.11ms |
| CTR | 0.04ms | 0.07ms | 0.17ms | 0.29ms | 0.75ms | 1.27ms |
| XTS | 0.23ms | 0.33ms | 0.73ms | 0.80ms | 3.71ms | 6.67ms |
| CCM | 0.17ms | 0.23ms | 0.98ms | 1.01ms | 4.02s | 6.38ms |
| GCM | 0.08ms | 0.17ms | 0.17ms | 0.25ms | 0.95ms | 2.05ms |

**2.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Windows AES Decryption** | | | | | | |
| Input  Mode | 100KB | 200KB | 500KB | 1MB | 2MB | 5MB |
| ECB | 0.04ms | 0.06ms | 0.08ms | 0.50ms | 0.25ms | 1.35ms |
| CBC | 0.06ms | 0.06ms | 0.91ms | 0.39ms | 1.23ms | 1.38ms |
| OFB | 0.09ms | 0.16ms | 0.44ms | 0.82ms | 2.06ms | 4.85ms |
| CFB | 0.06ms | 0.07ms | 0.23ms | 0.57ms | 1.85ms | 2.02ms |
| CTR | 0.11ms | 0.05ms | 0.07ms | 0.62ms | 1.77ms | 1.55ms |
| XTS | 0.15ms | 0.25ms | 0.22ms | 0.72ms | 3.37ms | 3.92ms |
| CCM | 0.15ms | 0.32ms | 0.37ms | 1.28ms | 2.60ms | 6.33ms |
| GCM | 0.06ms | 0.12ms | 0.14ms | 0.65ms | 0.91ms | 2.21ms |

**3.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Linux AES Encryption** | | | | | | |
| Input  Mode | 100KB | 200KB | 500KB | 1MB | 2MB | 5MB |
| ECB | 0.04ms | 0.05ms | 0.12ms | 0.40ms | 0.52ms | 1.28ms |
| CBC | 0.15ms | 0.17ms | 0.42ms | 0.77ms | 1.02ms | 5.02ms |
| OFB | 0.05ms | 0.08ms | 0.62ms | 0.67ms | 1.85ms | 5.85ms |
| CFB | 0.08ms | 0.12ms | 0.55ms | 1.22ms | 1.97ms | 5.88ms |
| CTR | 0.10ms | 0.17ms | 0.15ms | 0.34ms | 1.15ms | 1.92ms |
| XTS | 0.05ms | 0.07ms | 0.60ms | 1.26ms | 1.72ms | 9.93ms |
| CCM | 0.08ms | 0.13ms | 0.55ms | 1.17ms | 1.33ms | 7.55ms |
| GCM | 0.06ms | 0.12ms | 0.18ms | 0.50ms | 1.02ms | 1.70ms |

**4.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Linux AES Decryption** | | | | | | |
| **Input**  **Mode** | 100KB | 200KB | 500KB | 1MB | 2MB | 5MB |
| ECB | 0.04ms | 0.06ms | 0.15ms | 0.37ms | 0.85ms | 1.75ms |
| CBC | 0.04ms | 0.06ms | 0.15ms | 0.35ms | 1.12ms | 2.05ms |
| OFB | 0.12ms | 0.14ms | 0.48ms | 0.91ms | 2.25ms | 6.33ms |
| CFB | 0.04ms | 0.11ms | 0.20ms | 0.77ms | 1.12ms | 2.91ms |
| CTR | 0.02ms | 0.05ms | 0.19ms | 0.42ms | 0.91ms | 2.11ms |
| XTS | 0.11ms | 0.18ms | 0.53ms | 1.42ms | 1.67ms | 4.81ms |
| CCM | 0.17ms | 0.16ms | 0.63ms | 0.85ms | 1.97ms | 7.12ms |
| GCM | 0.05ms | 0.08ms | 0.13ms | 0.50ms | 1.33ms | 2.12ms |

**5.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Windows DES Encryption** | | | | | | |
| Input  Mode | 100KB | 200KB | 500KB | 1MB | 2MB | 5MB |
| ECB | 1.01ms | 1.83ms | 4.05ms | 9.12ms | 26.06ms | 43.23ms |
| CBC | 1.35ms | 2.75ms | 4.37ms | 9.67ms | 29.97ms | 52.11ms |
| OFB | 0.87ms | 2.77ms | 3.78ms | 11.12ms | 30.16ms | 50.31ms |
| CFB | 0.93ms | 1.91ms | 4.51ms | 10.55ms | 30.33ms | 50.93ms |
| CTR | 1.17ms | 2.52ms | 4.25ms | 11.35ms | 32.15ms | 55.05ms |

**6.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Windows DES Decryption** | | | | | | |
| Input  Mode | 100KB | 200KB | 500KB | 1MB | 2MB | 5MB |
| ECB | 1.25ms | 1.64ms | 4.28ms | 8.06ms | 16.35ms | 47.55ms |
| CBC | 1.27ms | 1.85ms | 4.33ms | 8.12ms | 16.75ms | 48.12ms |
| OFB | 1.33ms | 2.15ms | 5.01ms | 8.21ms | 17.11ms | 49.87ms |
| CFB | 1.36ms | 2.09ms | 4.65ms | 8.20ms | 17.03ms | 48.75ms |
| CTR | 1.40ms | 2.23ms | 5.12ms | 8.69ms | 17.98ms | 51.65ms |

**7.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Linux DES Encryption** | | | | | | |
| Input  Mode | 100KB | 200KB | 500KB | 1MB | 2MB | 5MB |
| ECB | 1.05ms | 1.81ms | 5.55ms | 10.56ms | 24.16ms | 58.02ms |
| CBC | 1.13ms | 2.44ms | 6.15ms | 10.88ms | 26.36ms | 59.73ms |
| OFB | 1.11ms | 2.26ms | 6.06ms | 10.72ms | 25.92ms | 59.36ms |
| CFB | 1.06ms | 2.20ms | 5.89ms | 10.85ms | 26.03ms | 59.40ms |
| CTR | 1.57ms | 2.84ms | 6.15ms | 11.21ms | 26.95ms | 62.51ms |

**8.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Linux DES Decryption** | | | | | | |
| Input  Mode | 100KB | 200KB | 500KB | 1MB | 2MB | 5MB |
| ECB | 1.12ms | 2.36ms | 5.23ms | 11.36ms | 21.64ms | 57.35ms |
| CBC | 1.09ms | 2.34ms | 5.14ms | 11.01ms | 21.34ms | 57.42ms |
| OFB | 1.26ms | 2.47ms | 5.95ms | 12.25ms | 22.17ms | 60.66ms |
| CFB | 1.33ms | 2.40ms | 5.35ms | 11.29ms | 21.36ms | 60.14ms |
| CTR | 1.35ms | 2.52ms | 6.06ms | 12.20ms | 23.35ms | 65.16ms |

**Nhận xét:**

* Thực thi trên hệ điều hành Windows có vẻ chạy nhanh hơn trên linux.
* Thời gian thực thi tăng theo kích thước file (tăng theo cấp số nhân)
* Chương trình mã hóa DES chạy lâu hơn so với AES