**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN KHOA MẠNG MÁY TÍNH & TRUYỀN THÔNG**



MÔN MẬT MÃ HỌC

BÀI TẬP THỰC HÀNH 06: Mật mã học

GVHD: Nguyễn Ngọc Tự

Sinh viên thực hiện:

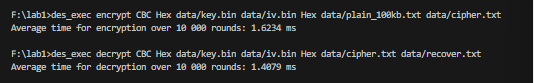
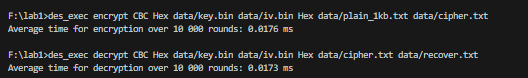
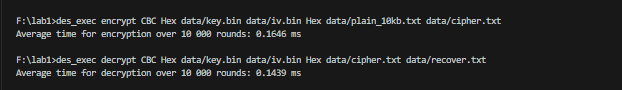
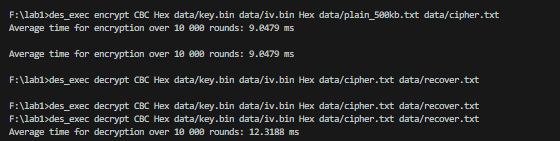
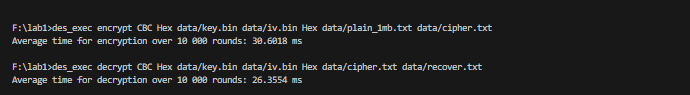
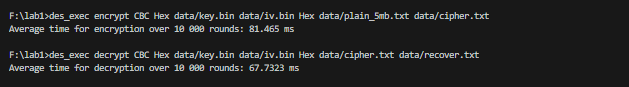
Trần Hồng Quân (23521271)

 Tp. Hồ Chí Minh, 05/06/2025 

\*DES:

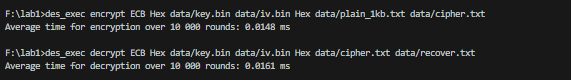
-CBC:

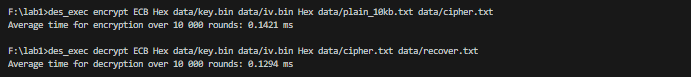
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Input size | Mode | OS | Encrypt Time (ms) | Decrypt Time (ms) |
| 1KB | CBC | Win | 0.0176 | 0.0173 |
| 10KB | CBC | Win | 0.1646 | 0.1439 |
| 100KB | CBC | Win | 1.6234 | 1.4079 |
| 500KB | CBC | Win | 9.0479 | 12.3188 |
| 1MB | CBC | Win | 30.6018 | 26.3554 |
| 5MB | CBC | Win | 81.465 | 67.7323 |

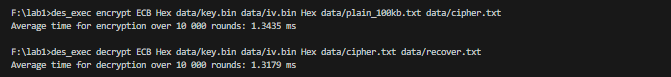


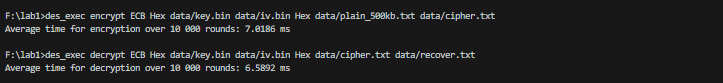
-ECB:

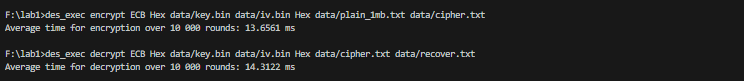
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Input size | Mode | OS | Encrypt Time (ms) | Decrypt Time (ms) |
| 1KB | ECB | Win | 0.0148 | 0.0161 |
| 10KB | ECB | Win | 0.1421 | 0.1294 |
| 100KB | ECB | Win | 1.3435 | 1.3179 |
| 500KB | ECB | Win | 7.0186 | 6.5892 |
| 1MB | ECB | Win | 13.656 | 14.3122 |
| 2MB | ECB | Win | 27.8738 | 29.3418 |

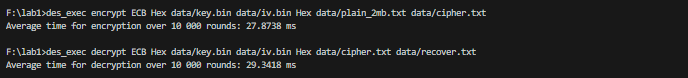






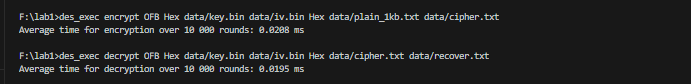


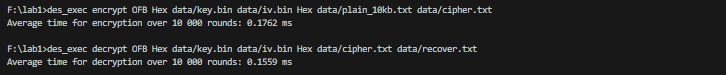


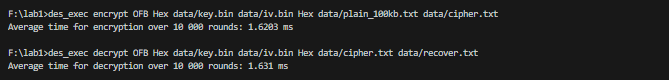


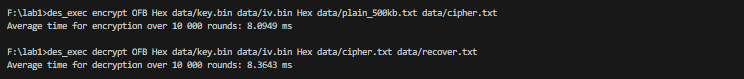
-OFB:

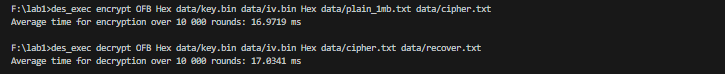
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Input size | Mode | OS | Encrypt Time (ms) | Decrypt Time (ms) |
| 1KB | OFB | Win | 0.0208 | 0.0195 |
| 10KB | OFB | Win | 0.1762 | 0.1559 |
| 100KB | OFB | Win | 1.6203 | 1.631 |
| 500KB | OFB | Win | 8.0949 | 8.3643 |
| 1MB | OFB | Win | 16.9719 | 17.0341 |
| 2MB | OFB | Win | 32.401 | 31.6228 |

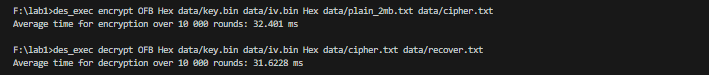






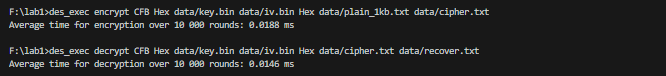


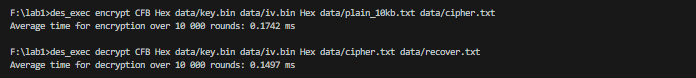


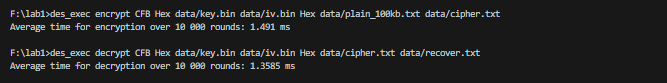


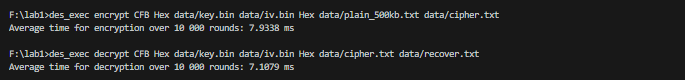
-CFB:

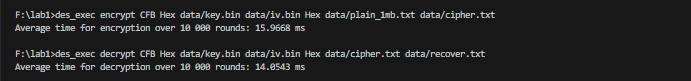
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Input size | Mode | OS | Encrypt Time (ms) | Decrypt Time (ms) |
| 1KB | CFB | Win | 0.0188 | 0.0146 |
| 10KB | CFB | Win | 0.1742 | 0.1497 |
| 100KB | CFB | Win | 1.491 | 1.3585 |
| 500KB | CFB | Win | 7.9338 | 7.1079 |
| 1MB | CFB | Win | 15.9668 | 14.0543 |
| 2MB | CFB | Win | 32.2219 | 28.5955 |

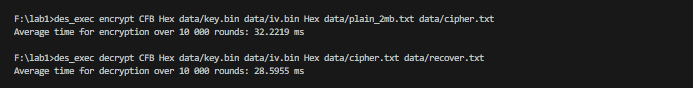






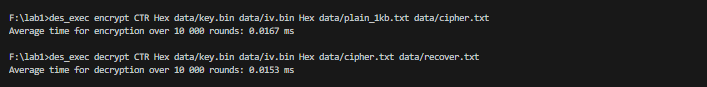


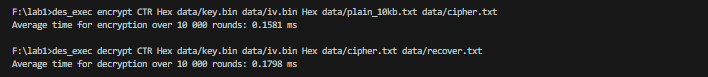


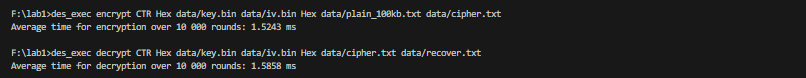


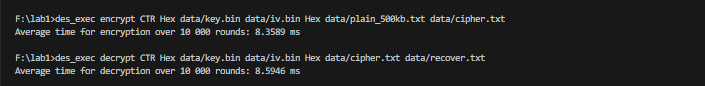
-CTR:

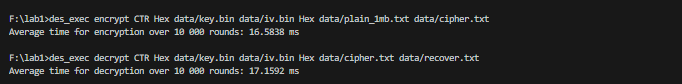
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Input size | Mode | OS | Encrypt Time (ms) | Decrypt Time (ms) |
| 1KB | CTR | Win | 0.0167 | 0.0153 |
| 10KB | CTR | Win | 1.1581 | 0.1798 |
| 100KB | CTR | Win | 1.5243 | 1.5858 |
| 500KB | CTR | Win | 8.3589 | 8.5946 |
| 1MB | CTR | Win | 16.5838 | 17.1592 |
| 2MB | CTR | Win | 32.8151 | 32.2253 |

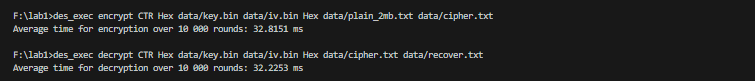








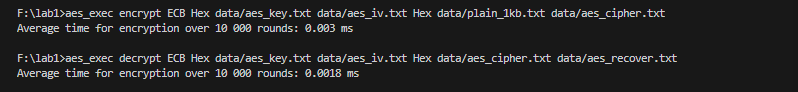


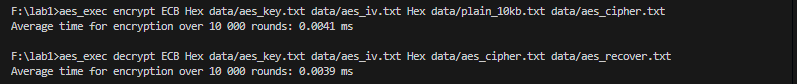


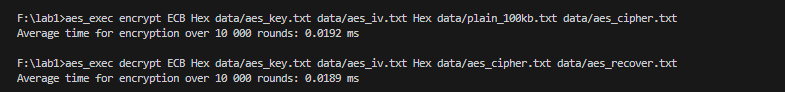
\*AES:

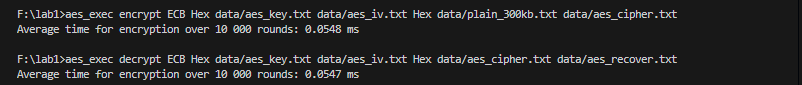
-ECB

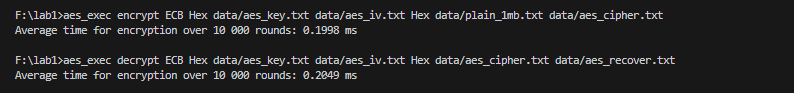
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Input size | Mode | OS | Encrypt Time (ms) | Decrypt Time (ms) |
| 1KB | ECB | Win | 0.003 | 0.0018 |
| 10KB | ECB | Win | 0.0041 | 0.0039 |
| 100KB | ECB | Win | 0.0192 | 0.0189 |
| 300KB | ECB | Win | 0.0548 | 0.0547 |
| 1MB | ECB | Win | 0.1998 | 0.2049 |
| 2MB | ECB | Win | 0.421 | 0.4264 |

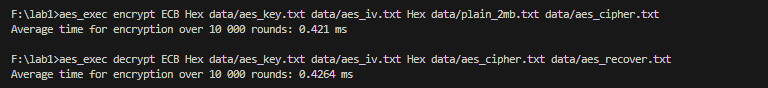






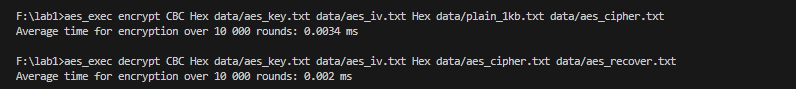


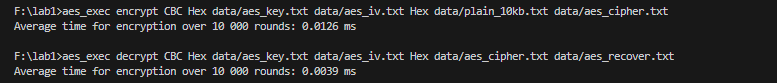


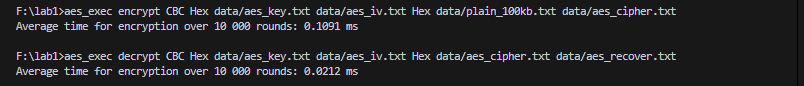


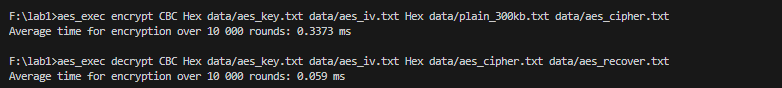
-CBC:

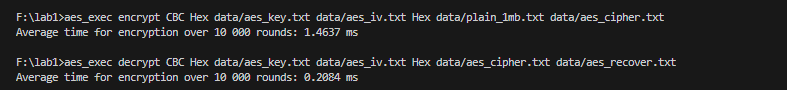
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Input size | Mode | OS | Encrypt Time (ms) | Decrypt Time (ms) |
| 1KB | CBC | Win | 0.0034 | 0.002 |
| 10KB | CBC | Win | 0.0126 | 0.0039 |
| 100KB | CBC | Win | 0.1091 | 0.0212 |
| 300KB | CBC | Win | 0.3373 | 0.059 |
| 1MB | CBC | Win | 1.4637 | 0.2084 |
| 2MB | CBC | Win | 2.9926 | 0.5098 |

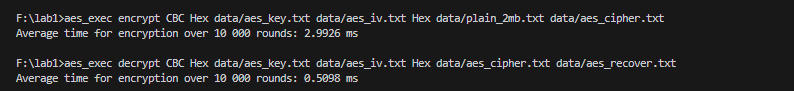






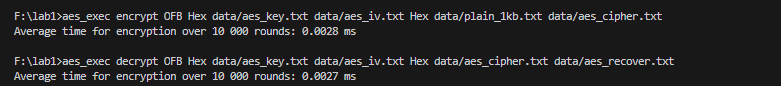


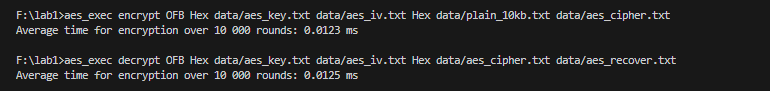


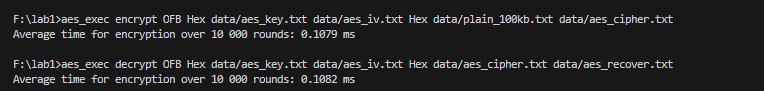


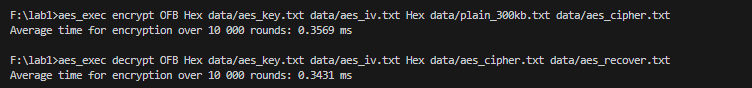
-OFB:

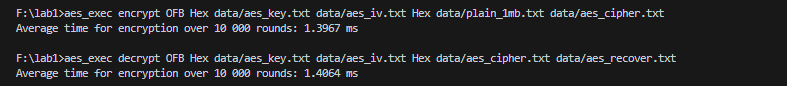
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Input size | Mode | OS | Encrypt Time (ms) | Decrypt Time (ms) |
| 1KB | OFB | Win | 0.0028 | 0.0027 |
| 10KB | OFB | Win | 0.0123 | 0.0125 |
| 100KB | OFB | Win | 0.1079 | 0.1082 |
| 300KB | OFB | Win | 0.3569 | 0.3431 |
| 1MB | OFB | Win | 1.3967 | 1.4064 |
| 2MB | OFB | Win | 2.9486 | 3.6237 |

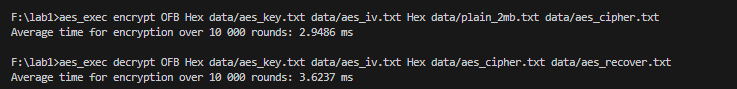






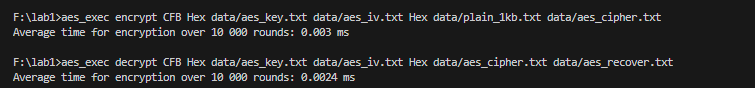


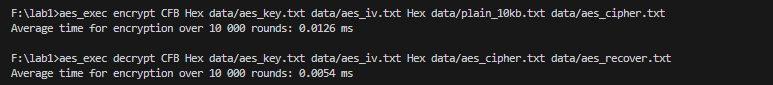


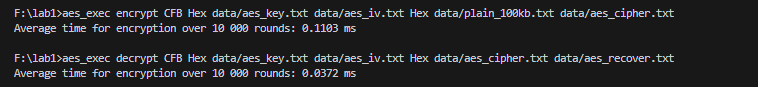


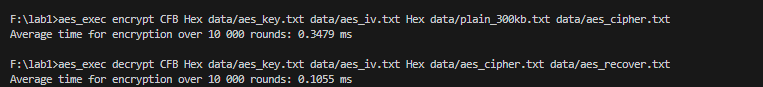
-CFB:

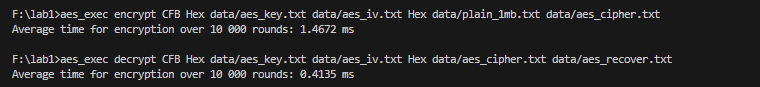
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Input size | Mode | OS | Encrypt Time (ms) | Decrypt Time (ms) |
| 1KB | CFB | Win | 0.003 | 0.0024 |
| 10KB | CFB | Win | 0.0126 | 0.0054 |
| 100KB | CFB | Win | 0.1103 | 0.0372 |
| 300KB | CFB | Win | 0.3479 | 0.1055 |
| 1MB | CFB | Win | 1.4672 | 0.4135 |
| 2MB | CFB | Win | 3.1055 | 0.9519 |

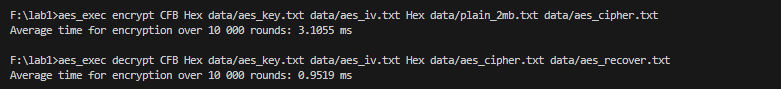






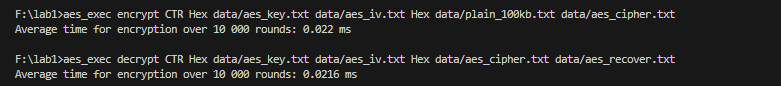
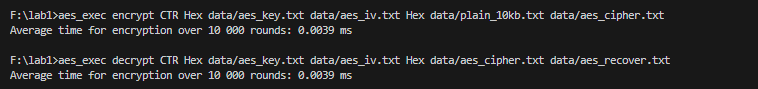
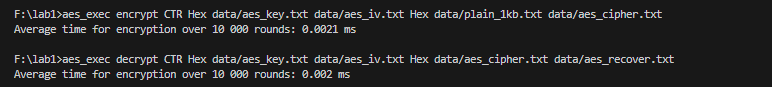


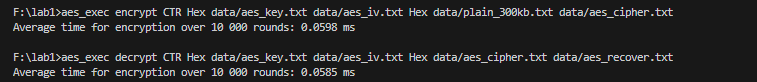


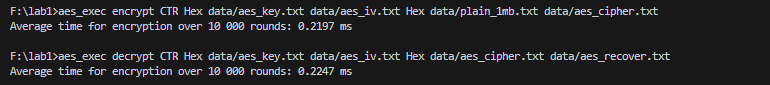


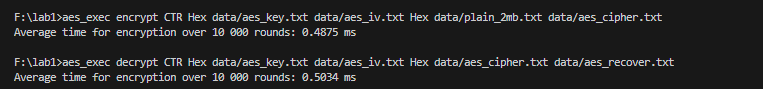
-CTR:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Input size | Mode | OS | Encrypt Time (ms) | Decrypt Time (ms) |
| 1KB | CTR | Win | 0.0021 | 0.002 |
| 10KB | CTR | Win | 0.0039 | 0.0039 |
| 100KB | CTR | Win | 0.022 | 0.0216 |
| 300KB | CTR | Win | 0.0598 | 0.0585 |
| 1MB | CTR | Win | 0.2197 | 0.2247 |
| 2MB | CTR | Win | 0.4875 | 0.5034 |



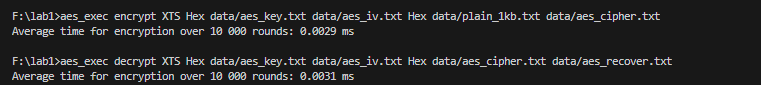


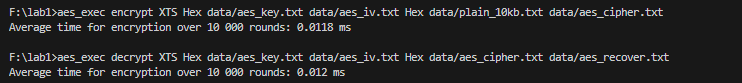


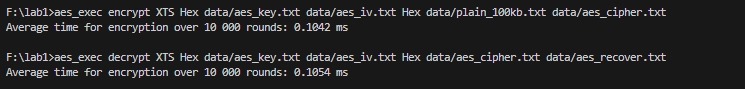


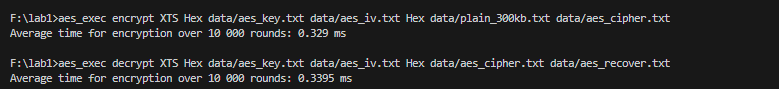
-XTS:

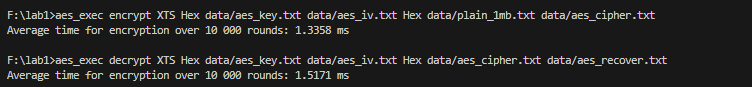
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Input size | Mode | OS | Encrypt Time (ms) | Decrypt Time (ms) |
| 1KB | XTS | Win | 0.0029 | 0.0031 |
| 10KB | XTS | Win | 0.0118 | 0.012 |
| 100KB | XTS | Win | 0.1042 | 0.1054 |
| 300KB | XTS | Win | 0.329 | 0.3395 |
| 1MB | XTS | Win | 1.3358 | 1.5171 |
| 2MB | XTS | Win | 2.9563 | 3.4957 |

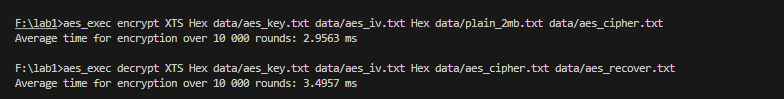






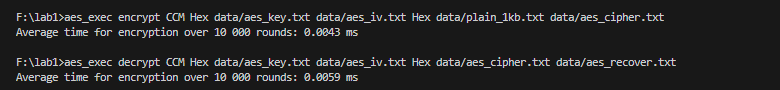


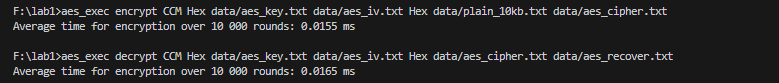


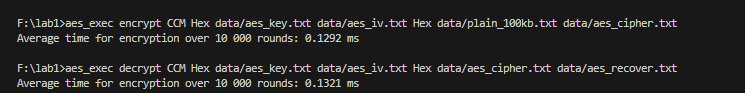


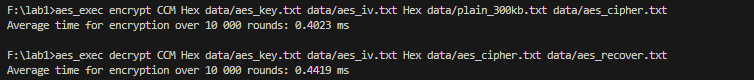
-CCM:

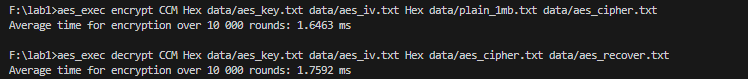
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Input size | Mode | OS | Encrypt Time (ms) | Decrypt Time (ms) |
| 1KB | CCM | Win | 0.0043 | 0.0059 |
| 10KB | CCM | Win | 0.0155 | 0.0165 |
| 100KB | CCM | Win | 0.1292 | 0.1321 |
| 300KB | CCM | Win | 0.4023 | 0.4419 |
| 1MB | CCM | Win | 1.6463 | 1.7592 |
| 2MB | CCM | Win | 3.4688 | 4.3719 |

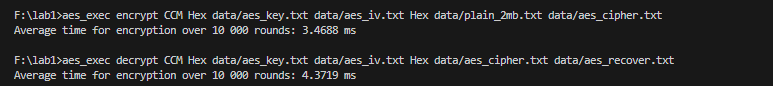












-GCM:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Input size | Mode | OS | Encrypt Time (ms) | Decrypt Time (ms) |
| 1KB | GCM | Win | 0.0034 | 0.005 |
| 10KB | GCM | Win | 0.0063 | 0.0074 |
| 100KB | GCM | Win | 0.0329 | 0.0349 |
| 300KB | GCM | Win | 0.0979 | 0.0987 |
| 1MB | GCM | Win | 0.3513 | 0.3513 |
| 2MB | GCM | Win | 0.8187 | 0.7827 |

