Comparing RSA and AES Throughput

Mark Nakamae

Cal Poly SLO

August 2020

Description

This project compared the differing throughputs of RSA and AES using the OpenSSL interface. Throughput is measured by dividing the number of bytes processed by the time taken to process those bytes. For the differing AES processes, a larger block size always correlated to a lower throughput. Similarly for the RSA public and private keys, a larger key size always correlated to a lover throughput.

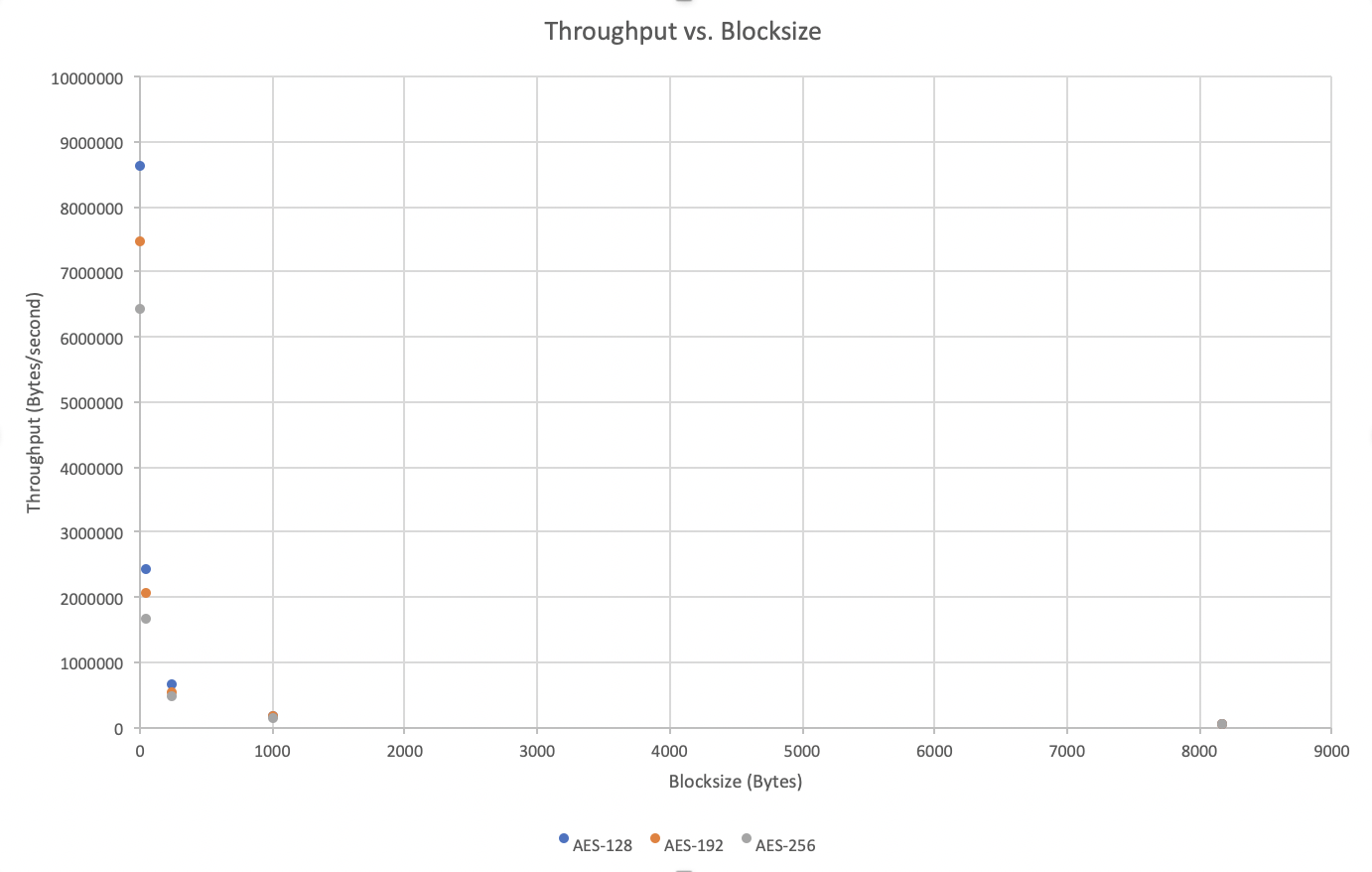
One of the returned results for both operations is a measure of throughput: operations per time (e.g. signatures per second).

*Run these operations and report your findings. Include two graphs: one that plots the block size vs. throughput for the various AES modes of operations and one that plots the RSA key size vs. throughput for each RSA operation. How do the results compare? Make sure to include these plots in your report.*

As expected, as block or key size increases, the throughput decreases since more time is taken to process the same amount of data. Moreover, we noted that the public RSA key encryption had a significantly higher throughput compared to that of the private RSA key encryption. Additionally, AES-n generally lowered in throughput as n increased. Comparing their throughputs against each other, AES performed considerably faster than RSA.

-- AES Data --

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Blocksize (Bytes) | Bytes Processed | Time Elapsed (s) | Throughput (Bytes/s) |
| AES-128 | 16 | 24764706 | 2.88 | 8598856.25 |
| 64 | 6970721 | 2.9 | 2403696.897 |
| 256 | 1797955 | 2.91 | 617853.9519 |
| 1024 | 455360 | 2.91 | 156481.0997 |
| 8192 | 57739 | 2.92 | 19773.63014 |
| AES-192 | 16 | 21627322 | 2.91 | 7432069.416 |
| 64 | 6001032 | 2.93 | 2048133.788 |
| 256 | 1467900 | 2.9 | 506172.4138 |
| 1024 | 375407 | 2.9 | 129450.6897 |
| 8192 | 46900 | 2.91 | 16116.83849 |
| AES-256 | 16 | 18593863 | 2.9 | 6411676.897 |
| 64 | 4545360 | 2.77 | 1640924.188 |
| 256 | 1281752 | 2.92 | 438956.1644 |
| 1024 | 322987 | 2.89 | 111760.2076 |
| 8192 | 28452 | 2.23 | 12758.74439 |



-- RSA Data --

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Key size (bits) | Bytes Processed | Time Elapsed (s) | Throughput (Bytes/s) |
| Public Key | 512 | 1521426 | 9.53 | 159645.9601 |
| 1024 | 591019 | 9.53 | 62016.68416 |
| 2048 | 156077 | 8.78 | 17776.42369 |
| 4096 | 45001 | 9.56 | 4707.217573 |
| Private Key | 512 | 175155 | 9.19 | 19059.30359 |
| 1024 | 53961 | 9.56 | 5644.456067 |
| 2048 | 9089 | 9.2 | 987.9347826 |
| 4096 | 1244 | 9.57 | 129.9895507 |

