Final Project Observations

## Equipment.

MacBook (8GB RAM/250 SSD)

## Power Consumption (Watts):

Paper Reporting:

* ChaCha20 is concluded to perform better than others.

My Observation:

* ChaCha20 on average has a lower power consumption rate but, ARC4 leads the packs when compared with ChaCha20 for different file memory loads for the below chart/table.
* Salsa20 vs ChaCha20, ChaCha20 performance is 50% more efficient then Salsa at lower data ranges, while the margin difference reduces to < 15% at higher data loads.
* AES-CTR, is the last performing cipher of the load ARC4/ChaCha20 are 300%-500% more energy efficient.

### Chart

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Salsa20 | ChaCha20 | AES-CTR | ARC4 | AES |
| Big File (50 MB) | 0.095349 | 0.056871 | 0.292761 | 0.03859 | 0.083016 |
| Small File (250 KB) | 0.000967 | 0.000613 | 0.777558 | 0.000297 | 0.00164 |
| String Big (1 KB) | 0.0000047 | 0.0000026 | 1.525333 | 0.0000031 | 0.002119 |
| String Small (14 b) | 0.00132 | 0.000334 | 0.751916 | 0.00044 | 0.000687 |
| Large File (500 MB) | 1.243207 | 1.064654 | 4.799036 | 0.670587 | 1.322206 |

Chart, bar chart

Description automatically generated

## Throughput (MB/s).

Paper Reporting:

* ChaCha20 is concluded to perform better than other.

My Observation:

* Throughput varies between data sizes. Algorithms are tuned to perform better at larger data set then smaller and vice versa. This can be observed in the following table.
* ChaCha20 has the best throughput MB/s for data sets < 50MB, but ARC4 has the best throughput for larger data sets > 50 MB.
* ChaCha20 perform better then Salsa20 for all data sizes.

### Chart

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Salsa20 | ChaCha20 | AES-CTR | ARC4 | AES |
| Big File (50 MB) | 147.463582874745 | 247.238675796437 | 10.350000000000 | 0.020250000000 | 169.644211356174 |
| Small File (250 KB) | 114.015410958904 | 179.952972972973 | 0.141363534120 | 0.141363534120 | 66.984507042254 |
| String Big (1 KB) | 10.350000000000 | 20.585714285714 | 0.000348101129 | 0.16011111111111 | 0.224454828660 |
| String Small (14 b) | 0.020250000000 | 0.068316831683 | 0.000105769948 | 0.051879.699248 | 0.033173.076923 |
| Large File (500 MB) | 169644211.356174 | 198.095272176107 | 43.946899267184 | 314.504807389473 | 159.508353299989 |

Chart, bar chart

Description automatically generated

## Encrypted Memory Size (bytes).

Paper Reporting:

* ChaCha20 is concluded to perform better than other ciphers such has MICKEY 128, GRAIN 80.
* ChaCha20 memory consumption is an average performer of all.

My Observation:

* I disagree with the paper ChaCha20 has an average performance when it comes to memory consumption after encryption, ChaCah20 and ARC4 has the same performance.

### Chart

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Salsa20 | ChaCha20 | AES-CTR | ARC4 | AES |
| Big File (50 MB) | 42606653 | 42606641 | 42606813 | 42606641 | 42606641 |
| Small File (250 KB) | 332925 | 332913 | 333085 | 332913 | 332913 |
| String Big (1 KB) | 1449 | 1441 | 1609 | 1441 | 1441 |
| String Small (14 b) | 81 | 69 | 241 | 69 | 69 |
| Large File (500 MB) | 639098941 | 639098929 | 639099101 | 639098929 | 639098929 |

Chart, bar chart

Description automatically generated

## Time differences encryption and decryption (ms)

Paper Reporting:

* ChaCha20 is concluded to perform better than other for the time taken between encryption and decryption.

My Observation:

* I agree with the paper ChaCha20 has a better performance than others, but not much has ARC4.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Salsa20 | ChaCha20 | AES-CTR | ARC4 | AES |
| Big File (50 MB) | 0.2889369 | 0.1723359 | 0.8871550 | 0.03859 | 0.083016 |
| Small File (250 KB) | 0.0029290 | 0.0018580 | 2.3562349 | 0.0009009 | 0.0049709 |
| String Big (1 KB) | 0.0001430 | 0.0000789 | 4.6222209 | 0.0000929 | 0.0064200 |
| String Small (14 b) | 0.0040010 | 0.0010109 | 2.2785329 | 0.0013320 | 0.0020830 |
| Large File (500 MB) | 3.7672949 | 3.2262230 | 14.5425319 | 2.0320819 | 4.0066850 |

## Chart

Chart, bar chart

Description automatically generated

Conclusion

* ARC4 performance is better by far than any other Ciphers in the list, but ARC4 is considered to have the weak cipher with security in mind, this makes ARC4 has the preferred choice for data that doesn’t need any added layer of security.
* ChaCha20 does perform slightly better than Salsa20 but when larger data sets are used this slight difference starts becoming negligible.