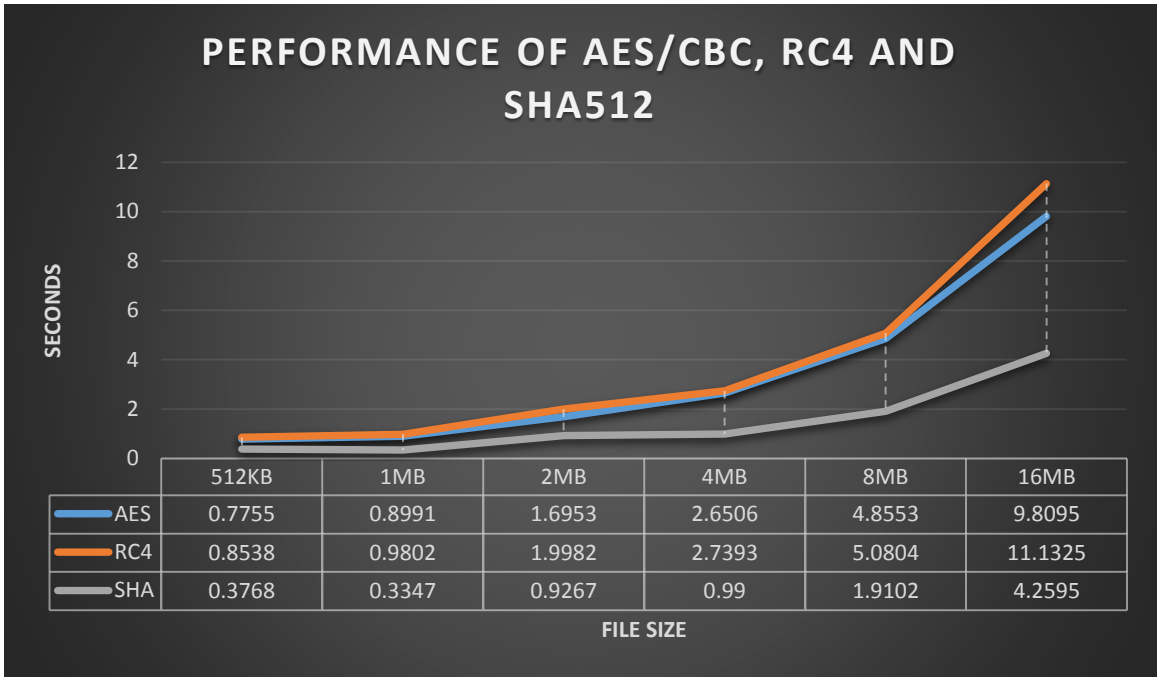
CSCI 650
Principle of Computer Security
Assignment 3

Group 1
z1744852 - Gowrinath Jarugula
z1746938 - Aienampudi Raga Tapaswi
z1748613 - Doddi Vineel

REPORT



	512KB	1MB	2MB	4MB	8MB	16MB
AES	0.7755	0.8991	1.6953	2.6506	4.8553	9.8095
RC4	0.8538	0.9802	1.9982	2.7393	5.0804	11.1325
SHA	0.3768	0.3347	0.9267	0.99	1.9102	4.2595

Running times of AES, RC4, and SHA:

From the observations we had so far, SHA consumes less time than the other two algorithms– AES and RC4 with respect to any file size considered.

RC4 and AES are almost in par with each other in times. However, AES had shown better performance than RC4 algorithm. In general, RC4 is expected to perform better than the AES as it is a stream cipher but the input block size considered might have affected this timing. When given a block size of 128bytes, RC4 took over AES by a margin of 0.1 second from the programs we had.

With respect to file sizes, the timing of all the three algorithms remain close to each other when file size is less than or equal to 1MB but SHA always have the upper hand.

Performance of AES, RC4 and SHA with respect to file size:

As the file size increased, SHA's performance surpassed the other two. SHA can be applied to any size of data and it processes message in 1024-bit blocks. SHA takes a linear increase in timing once the file size went beyond 4MB. However, as mentioned earlier SHA stands top when compared to other two.

As we know RC4 and AES both undergo symmetric encryption but AES processes data in blocks where as RC4 processes data in streams continuously. Timing of RC4 and AES increased almost at the same rate as the file size increased. However, we could see the difference only when file size is greater than 8MB, where AES shows better performance than RC4. In general RC4 performs much better than AES, however in this case RC4 performance is declined due to considered small block size.

Summary: SHA tops the three algorithms in timing irrespective of the file size. All algorithms showed a considerable performance when the file size is smaller than a Megabyte.