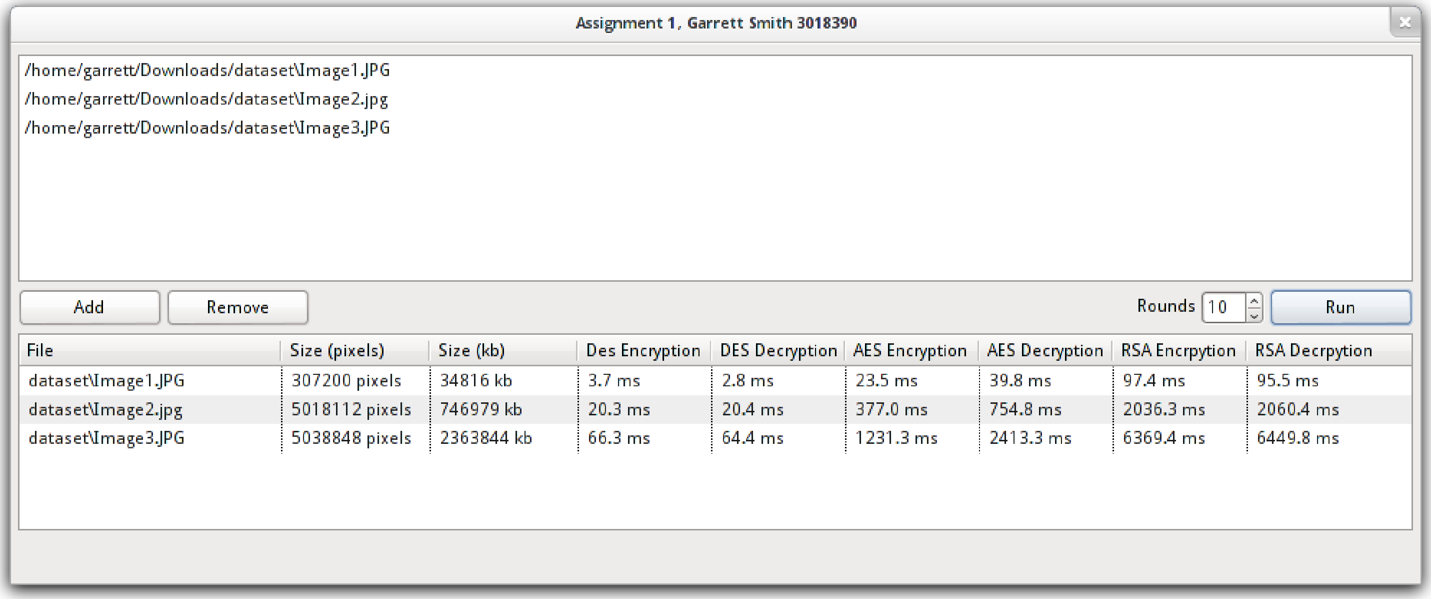
Computer Security and Privacy

Assignment 1, Symmetric and Asymmetric Encryption

Garrett Smith, 3018390



Assignment 1, Garrett Smith 3018390

/home/garrett/Downloads/dataset\Image1.JPG
/home/garrett/Downloads/dataset\Image2.jpg
/home/garrett/Downloads/dataset\Image3.JPG

Rounds 10

File	Size (pixels)	Size (kb)	Des Encryption	DES Decryption	AES Encryption	AES Decryption	RSA Encrpytion	RSA Decrpytion
dataset\Image1.JPG	307200 pixels	34816 kb	3.7 ms	2.8 ms	23.5 ms	39.8 ms	97.4 ms	95.5 ms
dataset\Image2.jpg	5018112 pixels	746979 kb	20.3 ms	20.4 ms	377.0 ms	754.8 ms	2036.3 ms	2060.4 ms
dataset\Image3.JPG	5038848 pixels	2363844 kb	66.3 ms	64.4 ms	1231.3 ms	2413.3 ms	6369.4 ms	6449.8 ms

Results

Debian Linux Testing 64-bit
Core 2 Duo CPU E3400 @ 3.86 GHz
4 GB Ram
N = 100

File Name	Size (pixels)	Size (kb)	DES Encryption	DES Decryption	AES Encryption	AES Decryption	RSA Encryption	RSA Encryption
dataset\Image1.JPG	307200	34816	0.93 ms	0.96 ms	17.68 ms	34.87 ms	94.21 ms	94.27 ms
dataset\Image2.JPG	5018112	746979	20.49 ms	20.62 ms	393.8 ms	768.34 ms	2007.2 ms	2013.98 ms
dataset\Image3.JPG	5028848	2363844	64.34 ms	64.46 ms	1202.54 ms	2376.71 ms	6405.76 ms	6427.28 ms

Findings

I found that DES was by far the fastest method of encryption, while RSA was the slowest. That being said, RSA was my own implementation and is very likely not nearly as efficient as it could be when implemented properly. All the algorithms scaled comparably with the larger sized files. Additionally, Encryption and decryption times are the same using DES and RSA, but decryption takes twice as long as encryption using AES. Even with decryption taking twice as long as encryption, AES was still approximately three times faster than RSA.

By far the most challenging part of implementing RSA was breaking the input into blocks so the values were less than the modulus calculated for the key pairs. The math required to generate keys and encrypt and decrypt was all fairly straight forward thanks to the Java API’s BigInteger class.