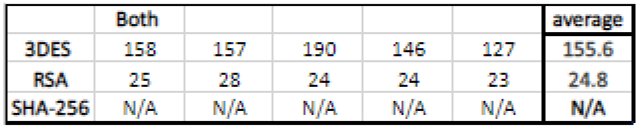
Hunter Nelson

Performance Evaluation of Cryptography Algorithms

6/20/2022

Results

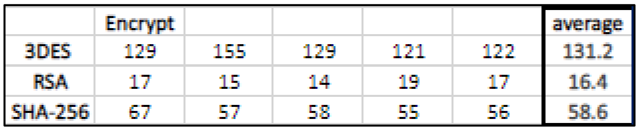
From the results we can conclude many things about these 3 algorithms. First, we will start with both categories, encryption and decryption using the 3 algorithms. We can see when using a word as our target object we get an average of 155.6 milliseconds with 3DES and an average of 24.8 milliseconds with RSA as seen in figure 1, this seems like a reasonable finding and time for each because 3DES is DES but 3 times making the encryption and decryption time around 3 times longer than RSA which is 1 pass with the key provided. The same conclusions can be seen in the other target objects.



	Both					average
3DES	158	157	190	146	127	155.6
RSA	25	28	24	24	23	24.8
SHA-256	N/A	N/A	N/A	N/A	N/A	N/A

Figure 1: Both category for all 3 algorithms with time in milliseconds.

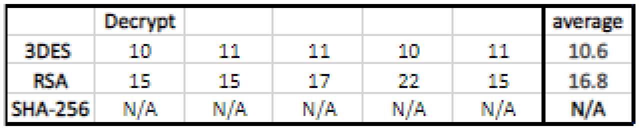
We were unable to decrypt the SHA-256 because it is a hashing algorithm and that is why figure 1 shows N/A value. However, when it comes to encryption, we can get time for all 3 algorithms and compare them. Figure 2 shows this, we can see that when it comes to encryption both RSA and SHA-256 beat out 3DES, however RSA still seems to be the fastest and these results stay true over the decryption and different target objects as well. While I only ran a small number of tests, when performing this test on a larger scale you would expect this trend to continue because of the way the encryption happens for each algorithm. Although we would be unsure when using larger files such as full papers or other string entry forms.



	Encrypt					average
3DES	129	155	129	121	122	131.2
RSA	17	15	14	19	17	16.4
SHA-256	67	57	58	55	56	58.6

Figure 2: comparison of the encryption times in milliseconds for the word target object

When looking at the decryption of the target objects we can find something odd. This being the 3DES seems to have a shorter decryption time since RSA is beaten in all 3 target objects, we can see this in figure 3.



	Decrypt					average
3DES	10	11	11	10	11	10.6
RSA	15	15	17	22	15	16.8
SHA-256	N/A	N/A	N/A	N/A	N/A	N/A

Figure 3: Decryption times in milliseconds of the word target object.

This can seem to make sense when we think about the types of algorithms they are. 3DES is symmetric key algorithm, this meaning the key to encrypt and decrypt is the same. While the RSA algorithm is an asymmetric key encryption, this means there is a public and private key to encrypt and decrypt the algorithm. With this being said we would think the 3DES algorithm should have a shorter to decrypt because all it must do is pass the password over and use it 3 times compared to the RSA accessing its private key. I decided to put the following charts into graphs such as the one in figure 4 because I felt it would help people compare the times of each algorithm better than a table.

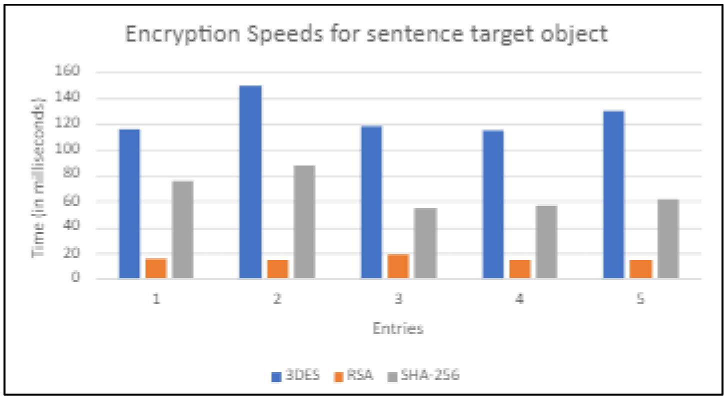


Figure 4: Graph for the encryption speed of each algorithm when using the sentence target object.

Conclusion

The results I was able to conclude were not the exact results we would expect but this could be because of the sample size and variables such as the target object or the language used. We would have expected the 3DES to have a faster encryption and decryption speed because of the complexity and more power needed by the RSA algorithm however that was not the case when it came down to encryption testing. In the end we were able to get some results but not the exact ones we expected.