Hunter Nelson

Performance Evaluation of Cryptography Algorithms

6/27/2022

Abstract

Cryptography is the study of techniques for secure communication. We know cryptography can be used in many ways, but we wanted to test the performance of a handful of algorithms. Using some different text inputs, we were able to compare the difference in speeds of the algorithms picked. The result was that 3DES has a longer encryption time when compared to RSA and SHA-256 but RSA has a longer encryption time compared to 3DES.

Keywords: algorithms, cryptography, encryption, decryption, hashing, public/private keys

Conclusion

In conclusion this experiment has proved a couple of things about the 3DES, RSA, and SHa-256 algorithms. First, these experiments have proven the 3DES algorithm is slower when overall and when encrypting the target objects we used, a word, a sentence, and a paragraph. At the same we have also found out that the 3DES is fast at decrypting the same 2 target objects. In return we found out the RSA algorithm is faster at encrypting but slower in decrypting. Next, we say that the SHA-256 algorithm fails in between 3DES and SHA-256 when it comes to encrypting but it cannot be calculated in the decryption process because it is a hashing function. When it comes to falling in between each we can see the SHA-256 algorithm is roughly 45 milliseconds behind the RSA algorithm and 75 milliseconds behind the 3DES algorithm. Finally, we can see that these 3 algorithms have very different times encrypting when using the target objects. While the charts may not be a very easy way to tell, the graphs were. We can see a very large jump in the encryption types while looking at the graphs and comparing each type.

Future Work

Future work for this project could include the cracking or hacking of each key, more algorithms, and more target objects being encrypted. These implementations would allow us to see how much more in-depth the study could go and provide us with a lot more details. Trying to crack or hack the key would allow us to see what algorithms safer and what algorithms have flaws, such as an avalanche effect. Next, we could add more algorithms, this would allow us to see which algorithms were faster, stronger, etc. It would also allow us to have more experience

with the algorithms. Finally, we could add more target objects, this would allow us to see the overall effectiveness of the algorithm and if a larger target object would slow some algorithms down.