Hunter Nelson

Performance Evaluation of Cryptography Algorithms

6/6/2022

Planned methodology

For me to compare the encryption and decryption algorithms in-depth I must complete many tests and compare the data afterwards. My initial idea would be something along the lines of running each algorithm 5 times but after researching them in depth I noticed that I would need to go far more in-depth than that. I first want to be able to compare the algorithms when using different length inputs, so for this I plan to use a word, a sentence, and a paragraph and run them 10 times each through the algorithms then averaging the times and errors if some are produced. Next, I want to compare the encryption and decryption so for this I will do the same as before but this time I will only encrypt and only decrypt each input and compare the times and errors, this will let me see if either encrypting or decrypting has a bigger impact on the time. Finally, I want to compare the security, so for this I am thinking of trying to find a brute force algorithm or something that cracks encryption and running it 5 times on each input and seeing if it can crack it. We can also compare other things like key length, memory used, avalanche effect. I want to focus on these 3 goals, however I know a lot more information will come to the scene when I run my test and get the data.

The Avalanche Effect refers to the fact that for a good cipher, changes in the plaintext affect the ciphertext. The algorithm produces a completely different output for a minimally changed input.

https://www.cryptovision.com/en/glossary/avalanche-effect/

https://www.geeksforgeeks.org/avalanche-effect-in-cryptography/