Winning the War against Hackers: A Hybrid Asymmetric Cryptographic Algorithm for Safe and Secure Data

Vishnubhatla, Sasank

Cryptography is the art of securing data and attacking secured data. A cryptographic algorithm implements encryption and decryption. Encryption is the method of scrambling information while decryption is the reversal of that process. In this research, a granular approach into cryptography was taken to see if one of the most renowned cryptographic algorithms, the RSA algorithm, is as secure and quick as people state. The hypothesis for this research was to determine if a hybrid cryptographic algorithm could be developed to have an entropy, encryption time, decryption time, total time, and success rate comparable to the RSA algorithm. This hybrid algorithm should also be able to resist common cyber-attacks, like a brute force attack or a man-in-the-middle attack. A hybrid algorithm which leveraged the strengths of the Diffie-Hellman Key Exchange and the RSA algorithm was mathematically formulated. In addition to make a comparison to the RSA algorithm, the hybrid algorithm was made into a personal cryptographic application for both user inputs and file security. To test the hypothesis, a fully functioning program was designed in the Python language version 2.7.5. The program included personal and testing methods so the algorithm could be deployed for home usage. Once the keys, shared values, and encrypted values were collected, fourteen 2 sample T-tests were done on the entropy and time taken to complete the task. Out of the fourteen T-tests, the hybrid algorithm was shown to be significant ten times. In conclusion, it can be stated that the hybrid algorithm is more efficient in entropy and quickness compared to the RSA algorithm.