A Study in the Effectiveness of Encryption Algorithms

Ryan Sadler

Final year project. Supervisor: David Lightfoot

Introduction

This study aims to improve the data available to others about the security and effectiveness of various historic and modern algorithms for encrypting data. It should also be user accessible with a good UI for easy use by anyone.

Literature

By far the best paper for this study was: (Rizvi, S.A.M, Hussain, S.Z. and Wadhwa, N., 2011, pp.76-79) as this was the only paper that I was able to find that detailed audio encryption as well as images and text. It also talks (briefly) about how theses algorithms can be used for more harm than good, for example randsomware.

The second most helpful paper was definitely: (Yadav and Majare, 2016, pp. 70-73) as it helped me detail how I would score the algorithms, based on Throughput, Key Size, Encryption and Decryption Speed and Time, Encryption Ratio and Level of Security Issues. However, there is no details on image or audio encryption.

References

1. Rizvi, S.A.M, Hussain, S.Z. and Wadhwa, N. (2011) 'Performance Analysis of AES and TwoFish Encryption Schemes' 2011 International Conference on Communication Systems and Network Technologies, Katra, India, pp. 76-79. DOI: www.doi.org/10.1109/CSNT.2011.160
2. G. Yadav and A. Majare (2016) 'A Comparative Study of Performance Analysis of Various Encryption Algorithms' *International Journal on Recent and Innovation Trends in Computing and Communication*, 5 (3) pp. 70-73 Available at https://ijritcc.org/download/conferences/ICEMTE_2017/Track_2_(EXTC)/1487794878_22-02-2017.pdf Accessed: 04/10/2023

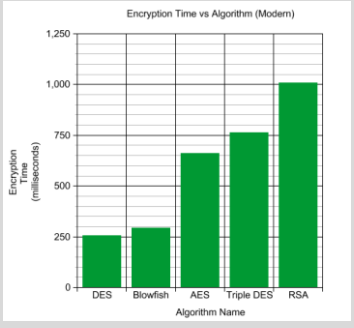
Source code is found at: https://drive.google.com/drive/folders/17DeizhKS4BJnlb1lybjJ13VMIqkyzF_H?usp=drive_link

Project Artefact

I have created an original implementation of 10 separate encryption algorithms and a UI application for the use of these algorithms

Results

In the results, you can see that there is a clear balance between speed, security and compolexity.
In the graph below of the results for encryption speed, you can see that AES, despite being the overally winner is not the fastest, but this is a sacrifice you have to make for the added security. NOTE: all historical algorithms have been omitted as modern algorithms are all several orders of magnitude slower.



Conclusions

In general, it was found that, unsurprisingly, AES was the best candidate for almost any use of encryption. However, there are exceptions, such as devices with limited computational power.
It would be interesting to see what other people can do using this project as a basis for further experiments, and I look forward to the results.

Methodology

This project is being developed using the agile model, as it will be built and tested, piece by piece until it is all fully completed. For version management, GitHub will be used as it is very good managing different versions of software and I am able to roll back code if I ever encounter any major issues.