DAT510 - Assignment 2

Frøydis Jørgensen

October 28, 2020

Abstract

A one-paragraph summary of the entire assignment - your choices of cryptographic primitives and their parameters, procedure, test results, and analysis.

Introduction

A description of the scientific background for your project, including previous work that your project builds on. (Remember to cite your sources!) The final sentence (analogous to the thesis statement in a term paper) is the objective of your experiment.

Design and Implementation

A detailed description (in paragraph format) of the design, procedure, and implementation of your project. This should be the main part of the report.

When implementing RSA, I think the most crucial thing is to find some good keys. We need two random large primes, **p** and **q**. By multiplying **p** and **q** we get **n**.

Test results

Results of testing the software, as you observed/recorded them. Note that this section is only for observations you make during testing. Your analysis belongs in the Discussion section.

Discussion

Your analysis of what your testing results mean, and your analysis.

Conclusion

A short paragraph that restates the objective from your introduction and relates it to your results and discussion, and describes any future improvements that you would recommend. Works Cited A bibliography of all of the sources you got information from in your report.

References

[1] A Security site, *Explaines how Blum Blum Shub works*, `https://www.asecuritysite.com/encryption/blum`.

[2] Wikipedia, *Wikipedia - Diffie-Hellman*, `https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange`.