RSACrackstation

Rapport over RSACrackstation projektet

Daniel Nettelfield og Gustav Nybro

A thesis presented for the degree of
Doctor of Philosophy

Teknisk Gymnasium Silkeborg
3x
31/10 - 2022

Indhold

1 Abstract

Your introduction goes here! Simply start writing your document and use the Recompile button to view the updated PDF preview. Examples of commonly used commands and features are listed below, to help you get started.

Once you're familiar with the editor, you can find various project settings in the Overleaf menu, accessed via the button in the very top left of the editor. To view tutorials, user guides, and further documentation, please visit our help library, or head to our plans page to choose your plan.

2 Problemformulering

2.1 Beskrivelse

Hjemmesiden er en side der kan faktorisere primtal ved hjælp at af API call til en ekstern database. Derudover kan hjemmesiden bruges til at bryde krypteringsalgoritmen RSA, og dertil dekryptere indtastet tekst. Derudover kan hjemmesiden også bruges til at kryptere tekst med RSA. Hjemmesidens målgruppe er primært CTF spillere, cybersikkerheds entusiaster og andre der skal kryptere og dekryptere med RSA.

2.2 Krav

- Hjemmesiden skal kunne faktorisere primtal.
- Hjemmesiden skal kunne bryde RSA kryptering.
- Hjemmesiden skal kunne kryptere med RSA.

3 Hvad er RSA?

RSA er en asymmetrisk kryptografialgoritme, som er udviklet af Ron Rivest, Adi Shamir og Leonard Adleman i 1977. En asymmetrisk kryptografialgoritme er en kryptografialgoritme der bruger to forskellige nøgler til at kryptere og dekryptere, og bruges ofte af blandt andet banker, til at sikre deres data. Idéen er er man kan offenliggøre krypteringsnøglen, men beholde dekrypteringsnøglen privat, så brugere kan kryptere data på deres egen maskine, og sende den krypterede tekst til banken.

4 Hvad er en API?

API står for "Application programming interface", hvilket er en måde for noget kode at intergere med noget andet kode. En API er modsætningen til en bruger interface, som er et interface ment til mennesker. API calls kan enten ændre data eller hente data fra en server. APIs er overalt på internettet og største delen af populære hjemmesider bruger APIs. Et godt eksempel på en API der

bliver brugt af mange mennesker, er Rejseplanen. Rejsplanen fungerer ved at en bruger indtaster noget data, som bliver sendt til backenden. Backenden sender kun rå JSON data tilbage, som frontenden behandler og viser på en måde, brugeren lettere kan forestå.

5 Frontend

```
1     // Shows the snackbar for 5 seconds
2     function showSnackbar(message) {
3         $("#failText").text(message);
4         $("#snackbar").addClass("show-bar");
5         setTimeout(function () {
6             $("#snackbar").removeClass("show-bar");
7         }, 5000);
8     }
9
```

6 Backend

6.1 RSA Funktionalitet

6.2 API call

7 Konklusion

Litteratur