



Studieområdeprojekt 2019

Sikkerhed bag login-formular på en hjemmeside

Jens Tinggaard

27. januar 2020

Odense Tekniske Gymnasium

- Redegør for talteorien bag RSA kryptering. Forklar nødvendigheden af primtal og hvordan RSA metoden fungerer.
- Gør kort rede for hashing.
- Analyser forskellen på hashing og kryptografi og hvilken rolle de har i forhold til sikkerhed.
- Vurder hvorfor RSA er vigtigt i forbindelse med sikkerhed ved logins.

- Hvorfor er RSA så vigtig - hvor bruges det?
- Hvad RSA bygger på.
- Metoder som RSA og hashing bliver sjældent brugt alene.

Matematik:

1. Talteori.
2. Beviser.
3. Vurdering & Sammenligninger.

Programmering:

1. Protokoller.
2. Skitsering af idéer.
3. Dokumentationslæsning.

Empiri brugt til udarbejdelse af projektet.

- Litteratur.
- Dokumentation af programmer som `hashcat` og `gpg`.
- Standarder og protokoller til håndtering af disse.
- Virkelighedsdata som UNI-login.

Sammenspil mellem fagene

- Logisk tankegang.
- Protokol → matematisk fremgangsmåde.
- Anvendt matematik → programmering.

Hvordan jeg har forholdt mig kildekritisk.

- Bøger.
- Udgivet materiale.
- Pålidelig dokumentation.