



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.

- Svært at primtalsfaktorisere et stort tal.
- Bruges over alt — virkelig.
- Metoder som RSA og hashing bliver sjældent brugt alene.
- Sikkerhedsfaktoere ved login.

SOP som metodefag

Matematik:

1. Talteori.
2. Deduktion & ræsonnement.
3. Analytiske løsninger.
4. Eksempelføring.

Programmering:

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

Empiri brugt til udarbejdelse af projektet.

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

Tværfaglige metoder.

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