Abstract

Public key-kryptering er et spændende område indenfor anvendt matematik. Det er især blevet relevant i forbindelse med NSA-afsløringerne. Inden vi begyndte havde vi et lille kendskab til kryptering generelt, men overhovedet ingen viden om ElGamal, eller elliptiske kurver generelt, som vi nu har arbejdet med. Vores formål med projektet har været at blive klogere på moderne public key-kryptering og derefter at bruge denne viden til at vurdere hvilke anvendelser, som udviklingen af kryptering gør mulige. Samtidig har vi været interesserede i, hvordan man øger sikkerheden af kryptosystemer.

Vi vil i denne opgave undersøge moderne kryptering, herunder private key- og public key-kryptering samt redegøre for grupper, legemer, ringe og polynomiumsringe. Dette fortsættes i en redegørelse for public key-systemet ElGamal og det bagvedliggende diskrete logaritmeproblem. Der redegøres også for ElGamal over legemet $\mathbb{F}_{p^n}$. Der regnes også et eksempel for ElGamal over $\mathbb{F}_{2^3}$. Dernæst redegøres der for ElGamal over elliptiske kurver på både Weierstrass- og på Edwardsform, herunder også binære kurver. Der redegøres både for elliptiske kurver over $\mathbb{F}_p$, over $\mathbb{F}_{p^n}$. Vi har kigget på en forholdsvis simpel implementering af ElGamal over binære Edwardskurver over legemet $\mathbb{F}_{2^8}$ i programmeringssproget *C*. Undervejs analyseres de fordele, der findes ved de forskellige typer af ElGamal. Heriblandt implementeringsfordelene ved karakteristik 2-legemer og hastigheds- og sikkerhedsfordelene ved Edwardskurver.

Der perspektiveres til de anvendelser som udviklingen af public key-systemer medfører. Dette handler især om mobile implementeringer, som udnytter et mindre krav til regnekraft. Dernæst præsenteres idéer til produkter og videre arbejde som bygger på indholdet af denne opgave. Dette handler igen om mobile anvendelser. Heriblandt digital signatur. Vi kunne særligt godt tænke os at arbejde videre med en implementering af binære Edwardskurver over et større legeme end bare $\mathbb{F}_{2^8}$. Vi snakker i stedet en implementering med legemet $\mathbb{F}_{2^n}$, hvor $n \approx 160$, da dette svarer til sikkerheden af et RSA-system baseret på et 1000-bit primtal. Da vi allerede har arbejdet med en implementering i *C* er det oplagt at vi arbejder på at lave en iPhone app, idet iOS er er bygget op omkring *C*.