Hjemmeeksamen *2020*

6. oktober 2020

– Diskrete logaritmeproblemet –

La $\mathcal{G}$ være en endelig syklisk gruppe, for eksempel $\mathbb{Z}/n$, og fiksér en generator g. Dette betyr altså at, hvis $a \in \mathcal{G}$, fins et unikt $k \in \mathbb{Z}$ slik at $a = g^k$. Da er den *diskrete logaritmen til* a, $\log_n(a)$, tallet k.

Det *diskrete logaritmeproblemet* er problemet å finne, gitt $\mathcal{G}$, $a \in \mathcal{G}$ og g, tallet k slik at $a = g^k$.

Hvis parameterene $\mathcal{G}$ og g er «godt valgt» (for eksempel må vi velge $n \gg 0$) er dette problem antatt å være veldig vanskelig å løse i rimelig tid. Det er å andre siden viktig å observere at vanskelighetsgraden er avhengig av valg av g (for gitt $\mathcal{G}$). For generelle valg av $\mathcal{G}$ og g fins ikke noen kjent algoritme som har polynomial kompleksitet.

Protokollen som dere skal se på bygger på (den antatte) vanskeligheten av diskrete log-problemet.

– Diffie–Hellman nøkkelutveksling –

Dere er sikkert vel bekjente med Diffie–Hellman når $\mathcal{G} = \mathbb{Z}/n$, men det generaliserer direkte til alle sykliske grupper på følgende måte.

La Alice og Bob være våre protagonister som bruklig er.

(i) Alice og Bob blir enige om et valg av syklisk gruppe $\mathcal{G}$ av orden $n \gg 0$ og et valg av generator g. Paret $(\mathcal{G}, g)$ er en åpen nøkkel;

(ii) Alice velger et tall $1 < a < n$ med noen form av tilfeldighet og sender g^a til Bob;

(iii) Bob velger et tall $1 < b < n$, også under viss tilfeldighet, og sender g^b til Alice;

(iv) Alice beregner $\left(g^b\right)^a$;

(v) Bob beregner $\left(g^a\right)^b$.

Observér at både Alice og Bob har beregnet samme element i $\mathcal{G}$, nemlig

$$\left(g^b\right)^a = g^{ba} = g^{ab} = \left(g^a\right)^b.$$

Dette bygger selvsagt på at gruppen er abelsk. Dette element

$$\sigma := g^{ab}$$

er Alice og Bobs hemlige nøkkel.

For at Eve skal finne nøkkelen må hon kunne løse diskrete log-problemet for $(\mathcal{G}, g)$. Tenk på at hon vet $\mathcal{G}$, g, g^a og g^b, men ikke a

eller b. For å finne nøkkelen $\sigma = g^{ab}$ må hon altså kunne beregne $\log_n(g^a)$ og $\log_n(g^b)$.

Dette betyr at, hvis $\mathcal{G}$ og g er godt valgt slik at diskret log-problemet for $(\mathcal{G}, g)$ er vanskelig, er nøkkelen sikker og kan sendes på en åpen kanal mellom Alice og Bob.

Det er viktig å være obs på at, gitt $\mathcal{G}$, kan det finnes dårlige valg av generator g, slik at diskret log-problemet er løsbart i rimelig tid.

– Oppgaver –

– ElGamal –

Krypteringsprotokollet som går under navnet *ElGamal* (etter Taher El Gamal som fant på det 1985) bygger på Diffie–Hellman idén for gruppen[1] $\mathcal{G} = (\mathbb{Z}/p)^{\times}$, $p \in \mathrm{Spec}(\mathbb{Z})$.

Oppgaven deres er å implementere dette protokoll i valgfritt programmeringsspråk. Implementasjonen skal være realistisk i det forstand at man skal kunne bruke store primtall p.

Det er en del av oppgave å finne informasjon om algoritmen. Ett godt startpunkt er Wikipedia-artikkelen.

[1] Man kan bruke vilkårlig syklisk gruppe, men i praksis er det nok $(\mathbb{Z}/p)^{\times}$ som brukes mest.

– Elliptiske kurver –

Her er $\mathcal{G}$ en gruppe som genereres av et punkt på en elliptisk kurve over en endelig kropp. Hvis det er noen som er interessert i å jobbe med dette så ta kontakt med meg så skal dere få litteratur.

Denne oppgave er relativt vanskelig og jeg anbefaler ikke at dere gjør denne hvis dere ikke ønsker å spendere mye tid.

Å andre siden, hvis dere er villige å legge litt ekstra tid, kommer dere å lære veldig mye fin matematikk og få innblikk i et protokoll som brukes i veldig mange sammenheng.