SNFcenter - Foundations of Cryptography and Security
af *lektor Ivan Bjerre Damgård, Århus Universitet*

Nye veje til datasikkerhed – mere end bare kryptering

At kunne kode tekster er en helt uundværlig ingrediens i moderne datasikkerhed. Kryptering bruges blandt andet til at sikre betalinger ved elektronisk handel. Teknikkerne er nu så avancerede, at vi inden længe også vil kunne *stemme* via Internettet, og handle elektronisk på langt sikrere vis end i dag

Traditionelt forbindes datasikkerhed ofte med kunsten at skabe sikker kommunikation over usikre linier, dvs. man transmitterer data kodet eller *krypteret*, således at det ikke kan læses eller modificeres af uvedkommende. Men det er let at genskabe den oprindelige tekst – at *dekryptere* – hvis man ellers kender det særlige kodeord, der skal til: den såkaldte hemmelige nøgle. Processen kan sammenlignes med den måde, en almindelige nøgle virker på: Man kan beskytte et dokument ved at lægge det i en kasse og låse den. Kun den, der har nøglen, kan låse kassen op igen.

Denne problematik er stadig aktuel. Men i det moderne informationssamfund opstår der nye udfordringer og sikkerhedsproblemer, der går langt videre end blot at bringe data sikkert fra A til B. Når det gælder elektronisk handel, eller elektroniske valg og licitationer, er der brug for at adskillige parter deltager samtidigt, folk som ikke kender hinanden på forhånd, som har modsat rettede interesser, og som ikke nødvendigvis stoler på hinanden. Her er sikkerhed en mere kompleks størrelse. Ikke mindst fordi forskellige parter ofte er interesseret i helt forskellige former for sikkerhed. Tænk f.eks. på elektronisk handel: netbutikkerne og bankerne vil først og fremmest have systemer der fungerer korrekt, så man f.eks. kan forsvare sig mod svindel fra brugere der forsøger at bruge penge de ikke har. Almindelige brugere derimod, er nok interesserede i at systemerne fungerer korrekt, men der er samtidig en stigende bekymring for privatlivets fred: det er ikke behageligt hvis systemet giver mulighed for at der kan samles store mængder af private oplysninger om hvordan hver enkelt person bruger sine penge.

Det er ikke ligetil at lave systemer der forener disse alle disse hensyn. Udfra en overfladisk betragtning kunne det endda se helt umuligt ud: skal man stoppe svindel og misbrug, synes det uundgåeligt at lede til mere identifikation og overvågning af brugerne, mens hensynet til privatlivets fred trækker den stik modsatte vej. Det er derfor værd at lægge mærke til, at grundforskning i kryptologi og datasikkerhed i de senere år har vist, at disse modsætninger altid kan forenes: ligegyldigt hvad formålet med et system er, kan det altid lade sig gøre at designe det, så det er sikret mod misbrug af alle de parter der indgår, og så ingen er tvunget til at offentliggøre private data. Dette fantastiske resultat løser imidlertid ikke alle problemer, for det siger ingenting om hvor *effektivt* et system man kan lave. Så spørgsmålet er altså: kan vi lave systemer der har alle de ønskede sikkerhedsegenskaber, og gøre det på en måde så produktet er til nytte i virkelighedens verden?

Foundations of Cryptography and Security er et forskningscenter der er oprettet i samarbejde mellem Datalogisk Institut ved Århus Universitet og Matematisk Institut ved Danmarks Tekniske Universitet. Centerets mål er for det første at udvide vores viden om sikkerheden af de funda-

mentale krypteringsteknikker, som stadig er uundværlige redskaber. For det andet at designe nye *protokoller*, dvs. sikre og effektive systemer, som er i stand til at håndtere komplekse sikkerhedsproblemer af den netop den type vi har set på her.

Som et eksempel på hvad de folk der står bag centeret arbejder med, vil vi se på elektroniske afstemninger. Det kræver ikke nogen større krystalkugle at forudsige, at næsten hele den danske befolkning om føje tid vil have forbindelse til Internettet. En lang række af de transaktioner vi foretager, som tidligere krævede papirarbejde, kan i dag foregå via telefon eller computer. Det er derfor naturligt at spørge, om vi så ikke også kunne foretage afstemninger ved at besøge en passende webside, hvorefter stemmerne kunne tælles sammen automatisk?

Det er klart, at der ligger vidtrækkende politiske muligheder og venter, hvis det bliver langt lettere at foretage afstemninger på landsplan, eller for den sags skyld på amts- eller kommuneplan. Under alle omstændigheder er de økonomiske fordele lette at få øje på, men det er sikkerhedsproblemerne naturligvis også. Hvordan sikrer vi, at stemmehemmeligheden bevares? Og hvordan sikrer vi, at resultatet er det rigtige?

Begge problemer kan klares ved hjælp af en kombination af kryptering og andre teknikker. Det er således indlysende, at vi er nødt til at sende hver vælgers stemme krypteret til en central computer, der skal stå for optællingen. Krypteringen sikrer, at stemmerne ikke aflyttes af uvedkommende. Men det må heller ikke være sådan, at den centrale computer kan dekryptere de enkelte stemmer. Dermed ville vi have skabt en slags ”Big brother”, som vidste, hvem der havde stemt på hvad. Og det ville naturligvis være helt utilfredsstillende. Heldigvis findes der snedigt konstruerede krypteringsteknikker, som tillader at at man så at sige ganger alle de krypterede stemmer med hinanden, *uden at dekryptere noget som helst*. Og dermed producere resultatet af afstemningen, men altså stadig i krypteret form. Her er tale om såkaldt *homomorf kryptering* (se illustration).

Homomorf kryptering kan sammenlignes med at regne med tal med eksponenter:

10^5 gange 10^7 er 10^{12}

Selvom vi gangede tallene, blev eksponenterne lagt sammen. Man kan tænke på eksponenterne som krypteret data. For at tælle stemmer op, har vi netop brug for at lægge sammen!

Tilbage står så kun at dekryptere resultatet. Hertil skal vi bruge den hemmelige nøgle. Hvis en enkelt computer får fingre i den, kan den imidlertid også misbruges til at dekryptere de enkelte stemmer. Det problem kan vi håndtere ved en teknik, der kendes som *secret sharing*: vi kan så at sige sprede den hemmelige nøgle ud over et helt netværk af computere ved at anbringe en lille del af nøglen hvert sted. Computerne kan dekryptere valgresultatet hvis de alle samarbejder. Men samtidig har vi gjort livet surt for hackerne: man vil nemlig være nødt til at bryde ind mange forskellige steder for at få fat på alle nøglens dele.

Systemer der fungerer på denne måde findes allerede på markedet. På forskningscenteret skal vi i de kommende år i gang med at forbedre effektiviteten af systemerne og finde nye anvendelsesmuligheder.

Illustration af en elektronisk afstemning
For at stemme ja, sendes et krypteret 1-tal, for at stemme nej sendes et krypteret 0.