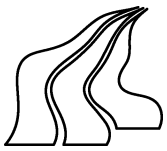
Elektronisk Afstemning

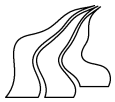
P2-PROJEKT, 4. FEBRUAR — 27. MAJ 2002

Af
Anders Gorst-Rasmussen
Lea Mwelwa Grønager
Lars Hornbæk Jensen
Linda Østervig Jensen
Dorte Klerke
Charlotte Kramer
Helene Pilgaard Larsen

Aalborg Universitet
Det Teknisk-Naturvidenskabelige Fakultet
Storgruppe 0134



Det Teknisk-Naturvidenskabelige Fakultet
Aalborg Universitet



TITEL:

Elektronisk afstemning

TEMA:

Netværk og algoritmer.

PROJEKTPERIODE:

P2, 4. februar - 27. maj, 2002

PROJEKTGRUPPE:

0134, B337

GRUPPEMEDLEMMER:

Anders Gorst-Rasmussen
Lea Mwelwa Grønager
Lars Hornbæk Jensen
Linda Østervig Jensen
Dorte Klerke
Charlotte Kramer
Helene Pilgaard Larsen

VEJLEDERE:

Leif Kjær Jørgensen
Claus Monrad Spliid

OPLAGSANTAL: 11

SIDEANTAL: 126

BILAGSANTAL OG -ART: 0

AFSLUTTET DEN 27/5 - 2002

SYNOPSIS:

I denne rapport undersøges mulighederne for at indføre elektronisk afstemning via internettet i Danmark som supplement til traditionel afstemning. Dette gøres dels gennem en undersøgelse af de tekniske muligheder, dels ved en analyse af markedet for en sådan afstemningsløsning.

I forbindelse med den tekniske redegørelse vil vi opstille en række matematisk-kryptografiske metoder baseret på beregninger i grupper og endelige legemer. Vi vil redegøre for, at en specialiseret kombination af disse metoder gør det muligt at konstruere en afstemningsprotokol. Denne protokol opfylder langt de fleste af de sikkerhedskrav, der er til afstemning og valg i Danmark i dag og på visse områder er mere sikker end traditionelle afstemningsmetoder. Ydermere vil vi argumentere for, at protokollen er et godt udgangspunkt for videre udvikling og kan anvendes direkte i forbindelse med afstemninger og mindre valg.

Igennem markedsanalysen belyses de yderligere forudsætninger for indførelse af elektronisk afstemning, herunder primært vælgerinteressen for løsningen. Vi vurderer, at Danmarks IT-situation og de politiske ambitioner gør elektronisk afstemning til en oplagt mulighed på længere sigt. Endelig vil vi præsentere en mindre spørgeskemaundersøgelse, hvor omtrent halvdelen af respondenterne viste interesse for at stemme via internettet til folketingsvalg. Vi vil udfra undersøgelsen argumentere for, at interessen for elektronisk afstemning bl.a. hænger sammen med erfaring og fortrolighed med computere og internet.

Forord

Denne rapport er udarbejdet af projektgruppe B337 som P2-projekt på den Teknisk-Naturvidenskabelige Basisuddannelse, Aalborg Universitet, under temaet "Virkelighed og modeller — netværk og algoritmer". Rapporten indeholder to overordnede dele — en primært teoretisk orienteret opstilling af en afstemningsprotokol samt en markedsanalyse med fokus på protokollens muligheder i en større kontekst. Endelig følger tre appendicer.

Tak til vores hovedvejleder Leif Kjær Jørgensen for sin tålmodige og pædagogiske respons på arbejdsblade og tak til bivejleder Claus Monrad Spliid for mange konstruktive og nyttige forslag i forbindelse med arbejdet med den kontekstuelle faglighed.

God fornøjelse med læsningen!

Anders Gorst-Rasmussen

Lea Mwelwa Grønager

Lars Hornbæk Jensen

Linda Østervig Jensen

Dorte Klerke

Charlotte Kramer

Helene Pilgaard Larsen

Indhold

Kapitel 1

Introduktion til problemstillingen

Danmarks lange tradition for folkeligt demokrati har gjort valg og afstemninger til en naturlig del af danskernes hverdag. Siden grundloven af 1915, har hele den myndige del af befolkningen med jævne mellemrum kunnet sætte sit kryds og dermed markere den demokratiske ret, enten til folkeafstemninger eller ved de tilbagevendende folketings- og kommunalvalg. Dette er den enkelte vælgers mest grundlæggende måde at tilkendegive mening på i et demokrati. Hidtil har denne foregået traditionelt v.h.a. blyant og papir, men det ændrede kommunikationsmiljø har givet nye muligheder. Som følge af internettets mange muligheder oplever vi en øget digitalisering, der i bred udstrækning er med til at forbedre dagligdagen på mange punkter. Regeringens mange IT-visioner arbejder mod en øget digitalisering af den offentlige sektor og kommunikationen mellem borger og myndigheder, og metoder for at overføre valg- og afstemningsprocesser til internettet er så småt begyndt at tage form på en mindre skala. Senest forsøgte man i 2001 at afholde ældrerådsvalg i Høje-Taastrup kommune via internettet med stor succes.

Perspektiverne i denne ændrede afstemningsform gør det til en interessant og relevant opgave at undersøge, hvorvidt det er muligt at afholde valg og afstemninger på national skala via internettet og dermed integrere den demokratiske proces i den digitale hverdag som et supplement til de eksisterende valg- og afstemningsformer. Det kunne give fordele såsom fornyet demokratisk engagement hos den enkelte vælger og øget bekvemmelighed.

Opstillingen af et sådant system er imidlertid langtfra en triviel opgave, som kan sidestilles med den gængse digitale informationsudveksling, der finder sted overalt i dag. Afstemnings- og valgprocessen er netop ikke informationsudveksling i traditionel forstand, men derimod en handling med ofte vidtrækkende konsekvenser.

Det er derfor et vigtigt spørgsmål, om der overhovedet eksisterer en tilfredsstillende teknologisk løsning, om digital informationsudveksling overhovedet kan bære en så vigtig proces som afstemning og valg? Og er der interesse for, at denne proces integreres i hverdagen på lige fod med anden digital færden?

Det er primært disse spørgsmål, vi vil forholde os til i denne rapport.

1.1 Problembeskrivelse og struktur

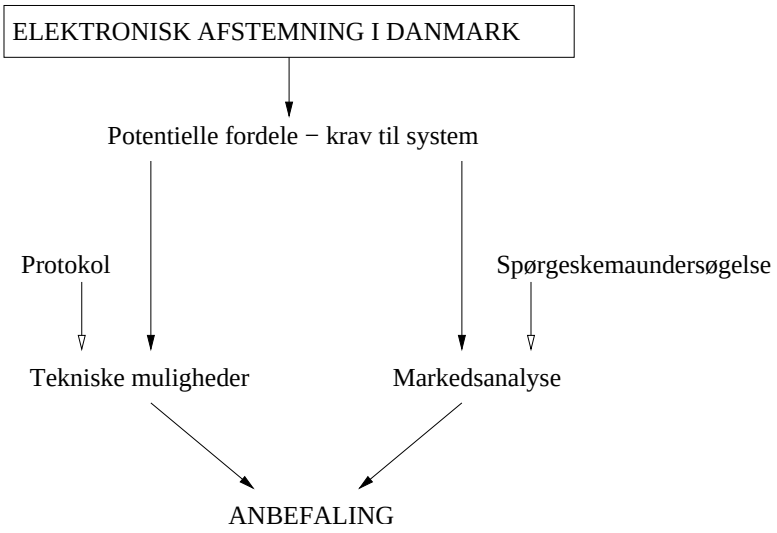
Vi vil i rapporten, Kapitel 2, først give et overblik over de potentielle fordele ved elektronisk afstemning. Efterfølgende vil vi analysere kravsspecifikationerne for et afstemningssystem — hvad skal være opfyldt?

Ud fra dette vil vi opstille en teoretisk afstemningsprotokol, Kapitel 3.2.1 — 9, og give en vurdering af dens egenskaber. Opfylder den de tidligere opstillede krav, og har den en chance i praksis?

Efterfølgende vil vi i Kapitel 10 foretage en analyse af markedet for en afstemningsprotokol og vurdere, hvorvidt der er vælgerinteresse for et sådant alternativ samt hvilke sammenhænge, der påvirker denne interesse. Dette vil vi gøre ud fra en mindre spørgeskemaundersøgelse.

Til sidst vil vi give en samlet vurdering i form af en anbefaling om, hvorledes der bør arbejdes videre på dette område.

Figur 1.1 illustrerer opbygningen af rapporten.



Figur 1.1: Overblik over hovedindholdet af rapporten.

Kapitel 2

E-demokrati og internetafstemning

En effektiv digitalisering af en afstemningsproces på en sådan måde, at det for den enkelte vælger vil være muligt at afgive sin stemme digitalt via internettet fra kommunikationsmidler som f.eks. PC'er, håndholdte computere og mobiltelefoner ville kunne revolutionere afstemningsprocessen på flere punkter.

Vi vil i dette kapitel opsummere de mulige fordele ved elektronisk afstemning og vurdere en række modargumenter. Dernæst vil vi opstille en række præcise krav til det afstemningssystem, vi ønsker at opstille.

2.1 Muligheder i elektronisk afstemning

Mulighederne i elektronisk afstemning via internettet er mange — det afgørende perspektiv er, at elektronisk afstemning vil kunne bidrage til en *øget bekvemmelighed og hjælpe marginaliserede grupper til en nemmere deltagelse i valg- og afstemningsprocesser*.

Vi vurderer, at der er følgende umiddelbare fordele ved elektronisk afstemning.

Øget bekvemmelighed Dette er en af de mest oplagte forbedringer ved elektronisk afstemning via internettet i forhold til traditionel afstemning. Elektronisk afstemning vil gøre det muligt at stemme stort set uafhængigt af geografisk placering og på meget kort tid.

Øget valgdeltagelse Internettet og digital kommunikation er i dag en integreret del af mange danskeres liv. Et effektivt og mobilt system til elektronisk afstemning vil gøre det lettere og mere attraktivt at stemme for marginaliserede grupper, der af forskellige grunde ikke har mulighed for at møde op på valgsteder, f.eks ferierejsende, handicappede, danskere med arbejde i udlandet o.s.v.

Danmark som foregangsland At indføre elektronisk afstemning som alternativ til eksisterende afstemningsmetoder, vil være et signal til omverdenen, der kunne konsolidere den danske IT-status, men også Danmark som moderne demokrati.

Reduceret optællingstid — øget præcision Når optælling foregår digitalt, giver computeranvendelsen mulighed for offentliggørelse af valgresultatet *umiddelbart efter* afstemningens afslutning, selv for meget store valg. Desuden elimineres risikoen for optællingsfejl.

En direkte økonomisk besparelse ved indførelse af elektronisk afstemning kan også synes oplagt — internettet har en velfungerende infrastruktur, der ikke kræver nye investeringer fra gang til gang. Såfremt elektronisk afstemning skulle eksistere som supplement til traditionelle afstemninger vil reduktionen af omkostninger være marginal; og etableringen af systemet vil i sig selv være forbundet med betydelige omkostninger. På længere sigt kunne man imidlertid forestille sig besparelsesmuligheder — f.eks. vil det være oplagt at overveje afskaffelse af brevstemmesystemet, hvis elektronisk afstemning eksisterer som et gennemprøvet og troværdigt alternativ. Dette vil kunne give betydelige besparelser.

Vi vurderer, at ovenstående fordele er de primære, *objektive* perspektiver ved elektronisk afstemning. Politisk kan man argumentere, at der bl.a. bliver mulighed for flere afstemninger eller ligefrem direkte demokrati, men sådanne perspektiver ønsker vi *ikke* at tage stilling til i denne rapport.

Det er vigtigt at se elektronisk afstemning i forhold til disse *mulige* forbedringer. Elektronisk Afstemning er *ikke* kun interessant ud fra et teknologisk synspunkt. Den kan derimod også anskues som et alternativ til den traditionelle afstemning med mange perspektiver, der vil kunne lette valghandlingen for både vælgere og myndigheder.

2.1.1 Kritik af muligheder

Mange af de ovenstående potentielle fordele kan anskues i en mere kritisk vinkel og har derfor to sider.

Ligegyldighed Man kan argumentere, at elektronisk afstemning vil fjerne det rituelle aspekt ved folkeafstemninger og valg — og gøre folk ligegyldige overfor disse og dermed have negativ effekt på valgdeltagelsen. Betydningen af valghandlingen vil ganske enkelt udviskes og blot blive en del af den daglige kommunikationsstrøm. Betydningen heraf er dog diskutabel i den situation, hvor elektronisk afstemning blot *supplerer* den traditionelle afstemning — ligesom brevstemning i dag supplerer stemmeafgivelse på valgstederne.

I denne sammenhæng vil elektronisk afstemning blot være en yderligere mulighed, der vil kunne lette afstemningsprocessen for visse grupper af vælgere, f.eks. handicappede, folk i udlandet o.s.v. uden at genere de grupper, der foretrækker traditionel afstemning.

Manglende sikkerhed En af internettets svagheder er sårbarheden overfor angreb fra hackere, vira m.m. Elektronisk afstemning vil være et oplagt mål for f.eks. politiske aktivister, der ønsker at sabotere afstemning. I denne rapport vil vi argumentere for, at det gennem nøje overvejelser og specialiserede metoder er muligt at opbygge et afstemningssystem, der formår at håndtere sådanne problemer.

Mistro Elektronisk afstemning giver ikke på samme måde en følelse af håndgribelighed og nærvær i valghandlingen som traditionel afstemning. Dette kunne i værste fald medføre at afstemnings- og valgresultater var tvivlsomme som følge af mistillid til afstemningssystemet. Igen anser vi dog ikke dette for et afgørende modargument, idet elektronisk afstemning blot er tænkt som et supplement til traditionel afstemning. Har man ikke den fornødne tillid til systemet, vil det være muligt at afgive sin stemme som normalt — man kan dog sætte spørgsmålstegn ved, hvor tilfredsstillende det er, at man ikke har tillid til alle de stemmer, der er afgivet elektronisk.

Digital diskriminering Elektronisk afstemning vil ikke give lige muligheder for alle — visse befolkningsgrupper har bedre forudsætninger for at kunne anvende de nye metoder end andre. Eksempelvis har yngre mennesker større adgang til internet og computere (og større erfaring hermed) end den ældste del af befolkningen. Dette modargument kan dog håndteres gennem en massiv IT-indsats fra regeringen, der sikrer lige muligheder for alle.

Alle disse modargumenter er vigtige at forholde sig til i opstillingen af et elektronisk afstemningssystem. Det ville være fatalt for elektronisk afstemning, hvis den allerede i indfasningsperioden bliver afskrevet fordi modargumenterne vægter for tungt. Vi vil derfor løbende forholde os til disse gennem rapporten.

2.2 Den teknologiske mulighed og udfordring

Redegørelsen for mulighederne i elektronisk afstemning viser, at der i høj grad er tale om en teoretisk mulighed med mange perspektiver. Dog er disse perspektiver afhængige af eksistensen af et *sikkert og effektivt* underliggende system, der opfylder en lang række kravsspecifikationer, som gør afstemning elektronisk til en ligeså sikker proces som traditionel afstemning. Det er vigtigt at indskærpe, at det ved valg og afstemninger *ikke* drejer sig om simpel informationsudveksling, men en kompleks *handling*, der er underlagt en lang række retningslinjer. Dette betyder tilsvarende, at udviklingen af et elektronisk afstemningssystem langtfra blot er en simpel programmeringsopgave.

Elektronisk afstemning som alternativ til traditionel afstemning vil kun kunne accepteres, såfremt kravsspecifikationerne er opfyldt til perfektion — og helst bedre end traditionel afstemning.

Vi vil i det følgende redegøre for en lang række kravsspecifikationer, som vil danne grundlag for opstillingen af en afstemningsprotokol.

2.2.1 Traditionel afstemning

Gyldigheden af en afstemning eller et valg i Danmark er i høj grad et *tillidsspørgsmål*. Når befolkningen i dag betragter et demokratisk valg som gyldigt, skyldes det tilliden til, at det er foregået som foreskrevet. Det betyder f.eks., at kun myndige kan stemme — at det kun er muligt at stemme en gang, at stemmerne bliver talt korrekt op o.s.v.

Disse grundlæggende, objektive krav er et fortrinligt udgangspunkt for konstruktionen af et system til elektronisk afstemning. Det påpeges bl.a. i [Neff, 2001], at et elektronisk afstemningssystem bør opstilles ud fra en række grundlæggende kvalitetskrav, der er karakteriseret ved at være videnskabelige og absolutte. Konstruktionen af systemet er i sig selv en videnskabelig proces, hvor det endelige produkt gerne skal kunne vurderes ud fra en række præcise krav.

Vi vil derfor nu opstille en række fundamentale krav, som vil danne basis for det videre arbejde med opstillingen af en elektronisk afstemningsprotokol.

✘	Berettigelse	Kun registrerede vælgere kan stemme.
✘	Entydighed	Hver vælger kan højst afgive én stemme.
✘	Korrekthed	Valgresultatet er summen af de afgivne stemmer.
✘	Anonymitet	Ingen kan vise, hvordan den enkelte vælger har stemt.
✘	Transparens	Det skal være muligt for observatører at verificere at berettigelse, entydighed, korrekthed og anonymitet er opfyldte.

Tabel 2.1: Krav til elektronisk afstemning

Bemærk, at kravene udelukkende repræsenterer det absolut grundlæggende, der er minimumskrav til næsten enhver demokratisk afstemning. Vi vil i Afsnit 2.3 skærpe disse krav yderligere under hensyntagen til øvrige procedurer og krav, der optræder i traditionelle danske afstemninger og valg.

Sikkerhedsaspektet — forbedringer?

Ovennævnte forhold er, under hensyntagen til mindre afvigelser, opfyldte i traditionelle valgsituationer i Danmark. Under selve valghandlingen med sit valgkort, og i tvivlstilfælde kan de valgtilforordnede forlange yderligere legitimation. Denne identificeringsmetode giver ikke optimal sikkerhed og i særlige situationer vil det være muligt at snyde og f.eks. udnytte sit stemmepotentiale flere gange o.s.v.

Generelt kan vi opsummere sikkerhedsrisici ved en traditionel valghandling som betinget af *menneskelige fejl*.

Heriblandt er følgende

- Mulighed for udnyttelse af flere stemmepotentialer.
- Optællingsfejl.
- Bevidst snyd[1]

[1] Som det f.eks. var tilfældet under kommunevalget 2001 i Ramsø kommune.

Ved elektronisk afstemning er det muligt at eliminere disse menneskelige fejl helt eller delvist; men sideløbende er det vigtigt at være opmærksom på de *nye svagheder*, et elektronisk system vil kunne give — jf. Afsnit 2.1.1.

2.3 Kravsspecifikationer og målsætning

Vores målsætning er at opstille den teoretiske fundering for et generelt system, der kan anvendes til afstemning via internettet til danske afstemninger og valg.

Denne teoretiske fundering vil bestå af en række retningslinjer for, hvordan de enkelte aktører under afstemningen skal handle, for at man når frem til et korrekt valgresultat, samt at de enkelte krav til valghandlingen er opfyldte under hele processen.

En sådan konstruktion kaldes en *protokol*.

Det er vores mål, at denne protokol for elektronisk afstemning skal kunne imødegå.

1. De basale kravsspecifikationer, jf. Tabel 2.1.
2. Mulighed for verificering for *enhver interesseret observatør*.
3. Mobilitet.
4. Øget bekvemmelighed for vælgeren.

I tilfælde hvor vi skønner det relevant, vil vi desuden påpege yderligere mulige revisioner af denne liste, der harmonerer med overordnede bestemmelser for valg og afstemninger i Danmark.

Kapitel 3

Overblik over afstemningsprotokol

Vi vil i dette kapitel arbejde med konstruktionen af en afstemningsprotokol ud fra kravsspecifikationerne i Afsnit 2.3. Sikring af samtlige krav på en effektiv og pålidelig måde kræver anvendelse af en række specialiserede metoder.

Dernæst vil vi redegøre for de grundlæggende principper i afstemningsprotokollen, og påpege, at en kryptografisk metode giver en mulig løsning. Efter denne redegørelse følger en *problematisering* af de enkelte antagelser i forbindelse med denne tænkte protokol — det er primært disse, der vil danne baggrund for det videre arbejde.

3.1 Vanskeligheden ved internetafstemning

Som det kort blev antydet i Afsnit 2.2, er konstruktionen af en både effektiv og sikker metode til elektronisk afstemning ikke nogen simpel opgave. Alle kravene vægter tungt, og elektronisk afstemning som alternativ til traditionel afstemning vil næppe kunne accepteres, medmindre samtlige krav er opfyldt til perfektion.

I den allersimpleste form for stemmeafgivelse kunne man forestille sig, en situation, der ligner de allerede eksisterende "quick polls" på internettet, blot med krav om sikring af identifikation. Her afgiver vælgeren sin stemme via hjemmeside eller e-mail og identificere sig via f.eks. CPR-nummer eller en PIN-kode.

De enkelte vælgeres berettigelse bliver da undersøgt af serveren. En sådan metode sikrer umiddelbart mobilitet og enkelthed ved stemmeafgivelse og vil give en ganske økonomisk afstemningsløsning. Sikkerhedsmæssigt er løsningen dog i høj grad uholdbar.

- Udpræget risiko for svindel — f.eks. er CPR-numre ikke hemmelige og kan derfor misbruges.
- Ingen anonymitet — en udenforstående kan forholdsvis uproblematisk aflytte kommunikationen og lære hver enkelt vælgers stemme at kende; samt i værste fald ændre eller tilbageholde afsendte stemmer.

- Ingen fejltolerance — går optællingsserveren ned, f.eks. efter angreb fra hackere, skal valget gå om.

Dette lille eksempel fremhæver desuden et yderligere vigtigt punkt — de elektroniske metoders sårbarhed! Vi argumenterede i Afsnit 2.2.1 for, at traditionelle afstemninger var sårbare i den forstand, at der var udpræget mulighed for menneskelige fejl, i form af fejloptællinger og bevidst snyd på en mindre skala. Denne sårbarhed er imidlertid mindre fatal, end det er tilfældet for ovenstående forslag til et system, fordi optælling foregår decentraliseret og i høj grad kontrolleret; hvorimod ovenstående eksempel vanskeligt kan kontrolleres.

Det er derfor oplagt at imitere metoderne i traditionel afstemning og arbejde hen mod et *distribueret system* med flere optællere. Som det vil fremgå af Afsnit 3.2 giver dette også store fordele i forbindelse med anonymitetsproblematikken.

3.2 Mod en kryptografisk afstemningsprotokol

Den i Afsnit 3.1 beskrevne metode lider under den afgørende svaghed, at der ikke er nogen form for anonymitet. Yderligere er der ingen form for fejltolerans.

Anonymitetsproblemet i forhold til udenforstående kan løses, ved at lade den enkelte vælger *kryptere* sin stemme, således at kun optællingsserveren kan *dekryptere* stemmen. Det vigtige identifikationsproblem kan som nævnt f.eks. løses ved anvendelse af de såkaldte *digitale signaturer*, en slags elektronisk underskrift [1], som vi imidlertid ikke vil beskrive yderligere i denne rapport. For behandling af denne ellers vigtige byggesten i et afstemningssystem henvises der til f.eks. [Goldwasser and Bellare, 2001, Kap. 9]

Sådanne tiltag er imidlertid ikke tilstrækkeligt, eftersom vi i konstruktionen med blot en enkelt optællingsserver får det alvorlige problem, at valgautoriteterne (myndighederne) herved lærer hver individs stemme at kende. Yderligere er konstruktionen også uhensigtsmæssig, idet al tillid til afstemningen reelt set er placeret i *én server*.

Som tidligere nævnt er det imidlertid muligt at løse denne problematik v.h.a. flere servere, hvor tilliden er fordelt mellem disse — i stil med den decentraliserede optællingsproces i traditionel afstemning.

Følgende eksempel er inspireret af [Schoenmakers, 2000]. Antag, at der er tale om den simpleste type afstemning, et ja/nej-valg (uden mulighed for blanke stemmer), samt at der er givet to optællingsservere, S_1 og S_2. For at afgive en stemme vælges et tilfældigt tal $x \in \mathbb{Z}$ og afsendes til til S_1, for stemmerne "ja" eller "nej" afgives hhv. $-x$ *eller* $-x+1$ i S_2, jf. Tabel 3.1.

Summen af resultatet fra S_1 og S_2 angiver antallet af afgivet ja-stemmer, dette antal fratrækkes det samlede antal stemmer og valgresultatet er givet. Såfremt serverne ikke samarbejder om bevidst at afsløre de enkelte vælgeres identitet og stemme, er

[1] Konkret er en digital signatur en datastreng, der kun kan frembringes af ejeren, er unik, personlig og fremfor alt bindende

Vælger	**Stemme**	S_1	S_2
Peter	*Ja*	123	-122
Ulla	*Nej*	-2341	2341
Aage	*Nej*	37	-37
		2501	-2500

Tabel 3.1: Princippet i optælling og verificering med flere servere.

anonymiteten sikret. Denne model kan naturligvis konstrueres med et arbitrært antal optællingsservere.

Denne opbygning kan udvides til en opsætning, hvor et givet antal optællingsservere, som vi fremover vil kalde valgautoriteter — samarbejder om at dekryptere stemmerne. Den fordelte tillid kan ydermere suppleres med en fejltolerans, således at hvis n servere er givet, kan op til t ($t < n$) servere være fejlagtige eller ligefrem korrupte, uden at dette påvirker dekryptering og stemmeoptælling.

En sådan konstruktion kaldes et *tærskel kryptosystem* og er en oplagt metode i forbindelse med en afstemningsprotokol, eftersom det sikrer både anonymitet og fejltolerans. Dette sikrer systemet mod ellers fatale småfejl, der kan gøre valgresultatet tvivlsomt eller direkte ubrugeligt. En formel introduktion til tærskel kryptoystemer kan findes i Afsnit 4.1.2.

Vi vil nu kort beskrive principperne i en kryptografisk protokol, hvis sikkerhed bygger på et sådant tærskel kryptosystem og præsentere de umiddelbare problemer, en sådan mulig løsning giver i praksis — herunder problematikken angående verificeringskravet, jf. Afsnit 2.3.

3.2.1 Overblik over afstemningsprotokol

I forbindelse med protokollen vil vi beskæftige os med tre grupper af aktører

1. Vælgere.
2. Observatører.
3. Valgautoriter (myndigheder/optællere).

Det er muligt at tilhøre op til flere af disse grupper.

Kommunikation mellem de enkelte parter foregår via et særligt *offentligt kommunikationsforum*, en eller flere servere, som opfylder følgende.

- Alle interesserede kan læse informationer.
- Adgang til at skrive kræver særlige rettigheder.
- Ingen informationer kan slettes.

D.v.s. hver aktør i systemet har skriverettigheder på en unik del af dette kommunikationsforum, hvortil adgang opnås med den anvendte identifikation.

Dette kommunikationsforum er et skridt på vejen mod verificeringsmuligheden for aktører. Alle informationer i systemet offentliggøres herpå, og det giver bl.a. mulighed for udenforstående at undersøge valgautoriteternes handlinger (f.eks. konstatere, om der har været korrupte valgautoriteter — i forbindelse med tærskelsystemet — og i givet fald hvor mange).

PROTOKOL 1 (SIMPEL AFSTEMNING)

Initialisering *De n valgautoriteter initaliserer tærskelsystemet med en passende værdi for t (fejltoleransen) og opsætter kommunikationsforumet.*

Stemmeafgivelse *Vælgeren afsender en krypteret stemme til sin personlige del af kommunikationsforumet.*

Stemmeoptælling *Valgautoriteterne foretager en* distribueret dekryptering *i henhold til tærskelsystemet (hvor op til t kan være fejlagtige/korrupte).*

3.2.2 En kort vurdering og problematisering

Under *antagelse* af, at det rent faktisk er muligt at udføre de i Protokol 1 beskrevne metoder og procedurer, er det klart, at vi har en mobil protokol, der opfylder

- Berettigelse — kun vælgere med registreret identifikation kan afgive stemme.
- Anonymitet — både overfor valgautoriteter og udenforstående under antagelse af, at maksimalt t valgautoriter er korrupte.
- Fejltolerans — en delmængde af valgautoriteterne kan være korrupte uden at afstemningen må gå om.

Imidlertid kunne det ved første øjekast blot se ud som om, disse egenskaber er fremkommet ved at se stort på andre forhold, herunder *transparens* og *entydighed* (jf. Afsnit 2.3).

Opstillingen giver ingen mulighed for, at udenforstående kan undersøge hverken entydighed eller korrekthed, eftersom kun de krypterede stemmer er synlige for udenforstående. Dette gør også korrektheden mindre pålidelig, eftersom valgautoriterne da i princippet ikke kan underkastes nogen form for ekstern kontrol.

Det kan vi forholde os til ved at forlange, at valgautoriteterne, i stedet for at dekryptere stemmerne én efter én, dekrypterer en *kombination af de krypterede stemmer verficérbart* og herudfra kan finde resultatet.

D.v.s. sådan at en observatør selv kan danne denne kombination af stemmerne og konstatere, at valgresultatet virkelig er en dekryptering heraf. Dette giver dog et alvorligt entydighedsproblem, eftersom det bliver umuligt (for både valgautoriteter og observatører) at undersøge, hvorvidt de enkelte stemmer er korrekte.

Dette er dog blot få af de mange praktiske problemer, man skal forholde sig til før en afstemningsprotokol opbygget efter grundideen i Protokol 1 kan blive en realitet.

Konkret vil vi i de kommende kapitler bl.a. tage stilling til følgende:

1. Hvordan konstrueres et sikkert tærskel kryptosystem i praksis?
2. Hvordan sikrer man, at vælgeren afgiver en korrekt stemme?
3. Hvordan omformes metoden, så resultatet kan tjekkes af enhver interesseret observatør?

De teoretiske ideer og konstruktioner, vi vil beskæftige os med i de kommende kapitler er baseret på [Cramer et al., 1997], der er hovedkilde for den tekniske del af denne rapport.

Kapitel 4

Basal kryptografi

Vi vil i dette kapitel redegøre for en række grundlæggende kryptografiske begreber, der vil danne fundament for det videre arbejde med protokollen. Af stor vigtighed er begrebet *public key kryptosystemer*, der viser sig at være velegnede til en afstemningssituation på internettet.

Vi vil redegøre for disse og introducere *faldlems en-vejs funktioner*, der er afgørende for eksistensen af sikre public key kryptosystemer. Slutteligt vil vi kort opstille de formelle principper i tærskel public key kryptosystemer.

Kryptografi er kort fortalt den grundlæggende disciplin, der beskæftiger sig med studiet af matematiske teknikker til informationssikkerhed. Man kan ikke tale om kryptografi som en sammenhængende disciplin, men snarere et udvalg af metoder til sikring for validiteten af informationer mellem to unikke parter. Dette er et uhyre bredt studie, der spænder over både hemmeligholdelse af beskeder, autenticitet af beskeder, autenticitet af de involverede parter o.s.v. Alle disse er egenskaber, som vi forlanger i forbindelse med elektronisk afstemning.

For en nærmere behandling af kryptografiens arbejdsområder henvises til [Menezes et al., 1996, Kap. 2].

4.1 Kryptosystemer

En af de vigtigste byggesten i kryptografien er de såkaldte *kryptosystemer*; en generel metode til hemmeligholdelse af beskeder, der udveksles mellem to parter.
Dette begreb kan defineres helt generelt.

DEFINITION 4.1 ***Kryptosystem***
Et kryptosystem *er en tretuppel* $(\mathcal{G}, \mathcal{E}, \mathcal{D})$*, hvor*

- $\mathcal{G}$ *er en algoritme som tager en bit-streng* 1^k*, (*sikkerhedsfaktoren*), som input, og returnerer en tilfældig nøgle*

$$(e, d) \in \mathcal{K} \times \mathcal{K} \subset \{0,1\}^* \times \{0,1\}^*.$$

- $\mathcal{E} = \{E_e : e \in \mathcal{K}$ *er en mængde af* krypteringstransformationer *som tager en* meddelelsestekst $m \in L \subset \{0,1\}^*$ *og returnerer en* kodetekst $c \in \{0,1\}^*$.

- $\mathcal{D} = \{D_d : d \in \mathcal{K}\}$ *er en mængde af* dekrypteringstransformationer *som tager en kodetekst* $c \in \{0,1\}^*$ *og returnerer den tilhørende meddelelsestekst* $m \in \{0,1\}^*$.

Det gælder, at for ethvert $e \in \mathcal{K}$ *eksisterer et* $d \in \mathcal{K}$*, således at*

$$D_d(E_e(m)) = m, \quad \forall m \in L \subset \{0,1\}^*.$$

Definitionen skal forstås således, at vi har tre algoritmer. Den første algoritme G genererer nøglen til brug for systemet. Denne nøgle genereres ud fra sikkerhedsfaktoren, som er bestemmende for *antallet af bits i nøglen*. Vi har desuden en krypteringstransformation (algoritme), som tager en nøgle e og en besked m (en binær streng) som input og giver en krypteret tekst, kodeteksten (tilsvarende en binær streng). Den tilhørende dekrypteringstransformation anvendes da på kodeteksten og nøglen e og returnerer den oprindelige besked (dette krav kan slækkes til, at den oprindelige tekst gives med *overvældende stor sandsynlighed*).

Det bemærkes, at vi ikke forlanger, at krypteringstransformationer er funktioner. Dette ville ellers være oplagt — for hver meddelelse skulle være en og kun en kodetekst. Dette er et tilstrækkeligt, men ikke nødvendigt krav. Overvej f.eks. situationen, hvor mængden, $\mathcal{M}$, af strenge er meget lille — i denne situation vil det ved kendskab til kodeteksten $E_e(m)$ være urimeligt nemt at bestemme den oprindelige meddelelse m ved simpel sammenligning.

Denne problematik optræder netop i opstillingen af afstemningsprotokoller, hvor der typisk kun er et mindre antal mulige stemmer, der kan krypteres — og vil blive diskuteret nærmere i Afsnit Afsnit 6.

Man skelner mellem to typer kryptosystemer.

DEFINITION 4.2 ***Symmetrisk/asymmetrisk***
Lad $S = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ *være et kryptosystem.* S *siges da at være* symmetrisk, *hvis der for et nøglepar* $(e, d) \in \mathcal{K} \times \mathcal{K}$ *gælder, at* $e = d$ *eller* d *kan beregnes i overkommelig tid (polynomiel tid) ved kendskab til* e.
Hvis dette ikke er tilfældet, siges S *at være* asymmetrisk.

Symmetriske kryptosystemer er i praktiske situationer ofte uhensigtsmæssige, bl.a. fordi de kræver sikre metoder til udveksling af nøgler. Dette kan gøres v.h.a. en *sikker*

kommunikationskanal, d.v.s. en kanal, som en tredjepart ikke har adgang til, men i store kommunikationsnetværk som f.eks. internettet er det i høj grad urealistisk at antage eksistensen af sådanne kanaler.

Ydermere fremgår det, at man i en større organisation vil have brug for et stort antal nøgler. Såfremt vi antager, at der er n personer i organisationen, og at hver person udvekslede nøgler med de øvrige $n-1$ personer, vil det samlede antal af nøgler N for at sikre krypteret information mellem alle parter være $N = \binom{n}{2} = \frac{n(n-1)}{2}$.

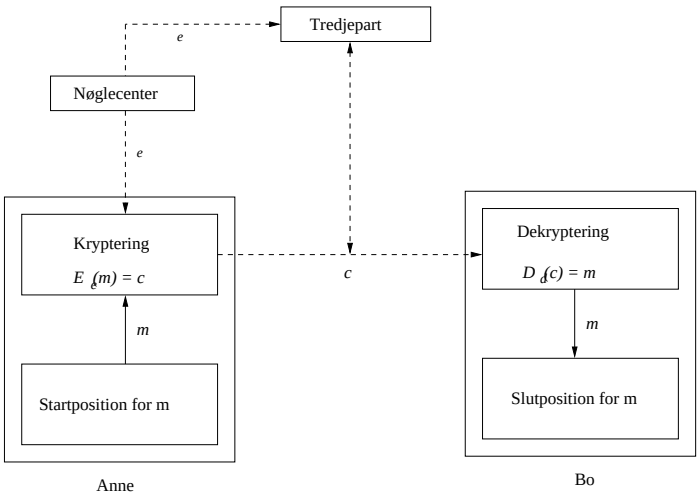
Indtil videre lader vi dette være tilstrækkelig begrundelse for ikke at uddybe symmetriske kryptosystemer. Vi vil i det kommende afsnit, Afsnit 4.1.1, beskrive grundprincipperne og fordele i det asymmetriske kryptosystem, der viser sig at være særdeles velegnet i forbindelse med opstilling af en afstemningsprotokol.

4.1.1 Asymmetriske kryptosystemer

Asymmetriske kryptosystemer, d.v.s. kryptosystemer, hvor der eksisterer to forskellige, uafhængige nøgler, (e, d) (jf. Definition 4.2) er specielle i den forstand, at man frit kan offentliggøre krypteringsnøglen e, mens dekrypteringsnøglen d er privat. Asymmetriske kryptosystemer kaldes også *public key kryptosystemer*.

Et sådant system er ideelt i sammenhænge, hvor det på intet tidspunkt er muligt at udveksle nøgler gennem en sikker kommunikationskanal; f.eks. ved kommunikation via internettet.

Sammenlignet med symmetrisk kryptering er systemet ydermere oplagt i den forstand, at antallet af nøgler reduceres markant. I en større organisation kunne man forestille sig et *nøglecenter*, hvor alle parters offentlige nøgler blev opbevaret. Lad n være antal personer i organisationen. Antallet af nøgler, N, kunne da reduceres til kun $N = 2n$.



Figur 4.1: Skematisk opstilling af public key koncept

På Figur 4.1 starter Bo med at sende krypteringsnøglen til nøglecenteret. Her henter Anne en nøgle e og bruger den til at kryptere en besked m til Bo. Den krypterede besked c sender hun afsted til Bo uden bekymring for, om nogen kan kigge med, idet

hun ved, at ingen tredjepart har mulighed for, ud fra c og e at finde frem til hverken d eller m.

Opstillingen af effektive public key kryptosystemer hviler i høj grad på den formodede eksistens af en bestemt type funktioner, en variant af de såkaldte *en-vejs funktioner*. Vi vil her præsentere en mindre formel definition, som viser sig afgørende for vort videre arbejde med asymmetriske kryptosystemer. For en formel definition af envejsfunktioner jf. [Goldwasser and Bellare, 2001, Kap. 2]

DEFINITION 4.3 ***En-vejs funktion***
Funktionen $f : D \to R$ siges at være en en-vejs funktion*, hvis*

1. *Beregning af $f(x)$ er beregningsmæssigt let for alle $x \in D$.*
2. *Givet et tilfældigt y,*

$$y \in \{z \in R \mid f(x) = z, \quad \textit{for et } x \in D\},$$

er det beregningsmæssigt uoverkommeligt at finde et $x \in D$, således at $y = f(x)$.

Det vides ikke, om en-vejs funktioner overhovedet eksisterer (jf. [Goldwasser and Bellare, 2001, Kap. 2]; men der eksisterer adskillige eksempler på funktioner, der formodes at være en-vejs (se bl.a. Kapitel 6).

Konceptet med en-vejs funktioner kan udvides til såkaldte *faldlems en-vejs funktioner*. Disse er karakteriseret ved, at beregning af den inverse funktion er let ved kendskab til ekstra information. Atter vil vi ikke give en præcis definition her.

DEFINITION 4.4 ***Faldlems en-vejs funktion***
En faldlems en-vejs funktion *er en en-vejsfunktion med den yderligere egenskab, at ved kendskab til særlig information (faldlems-information) er det beregningsmæssigt let givet et tilfældigt*

$$y \in \{z \in R \mid f(x) = z, \quad \textit{for et } x \in D\}$$

at finde et $x \in D$, således at $y = f(x)$.

D.v.s. faldlems-informationen er en ekstra parameter, hvor kendskab hertil gør det muligt indenfor en overskuelig tidsramme at invertere f blot givet billedet.

Netop en familie af sådanne funktioner er en oplagt kandidat som krypteringstransformation i forbindelse med public key kryptosystemer. Her kan selve en-vejs funktionen anvendes som krypteringsnøgle e, mens faldlems-informationen tjener som en privat nøgle d.

Det fremgår, at et public key kryptosystem er velegnet til hemmeligholdelse af stemmer i forbindelse med elektronisk afstemning. Man kunne forestille sig, at valgautoriterne genererede et nøglepar (h, s) i et passende sikkert krypteringssystem og offentliggjorde den offentlige nøgle på kommunikationsforumet, således at enhver vælger vil kunne kryptere sin stemme hermed. En sådan løsning er ideel i den forstand,

at kun *to nøgler* er påkrævet, samtidig med at løsningen er sikker uden antagelser om eksistens af sikre kommunikationskanaler (hvilket ikke vil kunne eksistere under en internetafstemning).

Vi vil nu kort redegøre for, hvordan et generelt public key kryptosystem kan omformes til et tærskel public key kryposystem, der sikrer fejltolerans og anonymitet som beskrevet i Afsnit 3.2.

4.1.2 Verficérbar tærskel public key

Som beskrevet i Afsnit 3.2 er en tærskelopbygning af et kryptosystem en oplagt måde at sikre fordeling af tillid under afstemningsprocessen samt fejltolerans.

Vi vil nu kort beskrive de formelle principper i et tærskel public key system med en betroet instans baseret på deling af hemmeligheder. Yderligere beskrivelser kan findes i [Pedersen, 1992, Kap. 3+5]

Lad Γ være en mængde af delmængder af $\{0, 1, 2, \ldots, n\}$. Et (t, n)-tærskel system til deling af hemmeligheder beskriver da, hvordan en betroet instans, som besidder en hemmelighed s kan fordele denne til n instanser $A_1, A_2, \ldots, A_n$ således, at for den såkaldte *adgangsstruktur*

$$\Gamma_t = \{P \subseteq \{1, 2, \ldots, n \mid |A| > t\},$$

gælder følgende

- Hvis $P \notin \Gamma_t$ så får $\{A_i\}_{i \in P}$ ***ingen*** information om s.
- Hvis $P \in \Gamma_t$ kan instanserne i P beregne s (i overkommelig tid).

En sådan struktur kan anvendes i forbindelse med et public key kryptosystem, hvor en betroet instans fordeler den private nøgle s i kryptosystemet, således at

- Enhver kan verificere, at vedkommende har modtaget en korrekt nøgleandel.
- Dekryptering kan kun foregå, hvis mindst $t + 1$ instanser samarbejder, d.v.s. i en delmængde $\{A_i\}_{i \in P}$, $P \subseteq \Gamma_t$.

Den første egenskab sikrer, at systemet er *verificérbart*, mens anden egenskab sikrer fejltolerans.

Vi vil i Afsnit 6.3.3 vise en konkret metode til deling af hemmeligheder og i Kapitel 7 opstille et verficérbart, fejltolerant tærskel kryptosystem, hvor der ikke er behov for en betroet instans, men den rolle er fordelt blandt instanserne $A_1, A_2, \ldots, A_n$. I relation til elektronisk afstemning sikrer dette korrekthed og ved den distribuerede metode undgår man på noget tidspunkt at skulle stole fuldt på en enkeltpart.

Kapitel 5

Grundlæggende tal- og gruppeteori

I det følgende kapitel vil vi redegøre for en lang række grundlæggende talteoretiske og algebraiske metoder, som vi senere vil anvende til opstillingen af et specielt public key kryptosystem, *ElGamal kryptosystemet*. Primært viser dette kryptosystem sig at være særdeles velegnet til en specialiseret form for tærskel kryptografi — og giver også andre fordele i forbindelse med elektronisk afstemning, herunder oplagte metoder til kombination af krypterede meddelelser (stemmer) og (verificérbar) dekryptering heraf. I Afsnit 3.2.2 nævnte vi kort, at dette var et skridt på vejen mod sikring af transparens på, d.v.s. sikre, at en observatør kan undersøge, at valgresultatet virkelig er en dekryptering af de afgivede stemmer — desuden giver dette en oplagt måde at udføre dekryptering på i tærskelsystemet.

5.1 Talteori

Følgende afsnit om talteori er skrevet på grundlag af [Thorup, 1998] samt [Beachy and Blair, 1996]. Vi vil her introducere en række begreber, der leder op til definitionen på en særlig algebraisk konstruktion, *restklasser* samt regning med disse.

DEFINITION 5.1 ***Divisor***
Et heltal $d \neq 0$ kaldes en divisor *i et heltal a, hvis der findes et heltal q, således at*

$$a = qd.$$

Dette skrives $d|a$.

De naturlige tal er karakteriseret ved bl.a. den vigtige egenskab, at *enhver ikke-tom mængde af tal har et mindste element*. Denne egenskab er fundamental i bl.a. konstruktionen af de naturlige tal, men skal også vise sig nyttig i forbindelse med bevisførelsen i mange af de kommende sætninger.

AKSIOM 5.1 ***Velordningsprincippet***
Enhver ikke-tom mængde af naturlige tal har et mindste element.

Vi har valgt at præsentere dette resultat som et aksiom — det er muligt at opstille det som en konsekvens af *Peano postulaterne*, jf. [Beachy and Blair, 1996, Appendiks A.2].

Ud fra Aksiom 5.1 er det muligt at udlede den såkaldte *divisionsalgoritme*.

SÆTNING 5.1 ***Divisionsalgoritmen***
For vilkårlige hele tal a og $d > 0$ gælder, at der findes entydigt bestemte heltal q (kvotienten) og r (resten), således at

$$a = qd + r, \qquad 0 \leq r < d.$$

Bevis:
Vi vil først bevise eksistensen af en sådan opskrivning. Lad $R = \{a - qd \mid q \in \mathbb{Z}\}$ — det er klart, at dette er mængden af potentielle rester r. Mængden R^+ af ikke-negative potentielle rester er ikke-tom, da den indeholder $a - d(-|a|) = a + d \cdot |a|$ og $d > 0$.

D.v.s. ifølge Aksiom 5.1 indeholder R^+ da et mindste element $r \geq 0$. For et heltal q må da gælde, at $r = a - qd$. Antag nu, at $r \geq d$, og da s er det mindste element, fås, at $s = r - d = a - d(q + 1) \in R^+$ — dette er i modstrid med, at r er den mindste rest, d.v.s. $r < d$.

Entydighed for q og r ses af følgende. Antag, at der eksisterer andre heltal p, t, således at $a = pd + t$, hvor $0 \leq t < d$. Da det også gælder, at $0 \leq r < d$ fås $|t - r| < d$. Da $pd + t = qd + r \Leftrightarrow t - r = d(q - p) \Rightarrow d|(t - r)$. Dette er kun muligt, hvis $t - r = 0 \Leftrightarrow t = r$ — hermed fås også, at $pd = qd$ og entydighed er bevist. ■

Blandt de naturlige tal er en speciel familie af tal, primtal, særlig interessant. Vi vil anføre de grundlæggende resultater om primtal, der senere gør det muligt at vise, at ethvert heltal kan skrives unikt, op til rækkefølgen, som et produkt af primtal. Primtal viser sig ydermere at være en fundamental del af de algebraiske konstruktioner, vi vil beskæftige os med i Afsnit 5.1.1 og 5.2.2.

DEFINITION 5.2 ***Primtal***
Et heltal $p > 1$ kaldes et primtal, *hvis og kun hvis p udelukkende har de trivielle divisorer* 1 *og* p.
Et heltal, som ikke er et primtal kaldes et sammensat tal.

Følgende sætning vil vi præsentere uden bevis (jf. evt. [Beachy and Blair, 1996, p. 17])
.

LEMMA 5.1 ***Euklid***
Et tal $p > 1$ er primtal hvis og kun hvis $p|ab \Rightarrow p|a \vee p|b$ for heltal a, b.

Ved hjælp af primtal er det muligt at opskrive ethvert heltal på *faktoriseret form*. Der gælder følgende.

SÆTNING 5.2 ***Aritmetikkens fundamentalsætning***
Ethvert heltal $n > 1$ kan entydigt (op til rækkefølgen) opskrives som et produkt af primtal på formen

$$n = p_1 p_2 \cdots p_n.$$

Bevis:
Vi viser først eksistens.

Antag, at der eksisterer heltal, for hvilket en sådan opskrivning ikke er mulig. Da er mængden B af heltal større end nul, der ikke har en sådan faktorisering, ikke-tom og har derfor et mindste element b, jf. Aksiom 5.1. Da b ikke kan være et primtal fås, at $b = b_1 b_2$ for $b_1, b_2 < b$. Af antagelsen følger, at b_1, b_2 har en primfaktorisering (idet de ikke kan tilhøre B), d.v.s. b har en faktorisering, og vi har opnået modstrid.

Dernæst vises entydighed. Antag, at n har to forskellige primfaktoriseringer

$$n = p_1 p_2 p_3 \cdots p_s = t_1 t_2 t_3 \cdots t_r,$$

hvor p_i og t_j er primtal for $i = 1, 2, \ldots, s$ og $j = 1, 2, \ldots r$. Af Lemma 5.1 følger, at der må findes et t_j, således at $p_1 | t_j$. Men da t_j er et primtal, der kun har divisorerne 1 og t_j må $p_1 = t_j$. Vi kan fortsætte tilsvarende med ethvert p_i og t_j. Entydighed følger derfor op til rækkefølge. ■

SÆTNING 5.3 ***Uendeligt mange primtal***
Der findes uendeligt mange primtal.

Bevis:
Antag, at mængden af primtal $M = \{p_1, p_2, \ldots, p_r\}$ er endelig. Betragt da tallet

$$n = p_1 p_2 \cdots p_r + 1.$$

Dette tal må være sammensat og ifølge Sætning 5.2 have en primfaktor p. D.v.s. $p \in M$, så $p | p_1 p_2 \cdots p_r$, og også $p | (n - p_1 p_2 \cdots p_r) \Leftrightarrow p | 1$ hvilket er en modstrid, da p ikke kan være en divisor i 1. ■

For et par af heltal vil vi indføre begrebet *største fælles divisor* $\texttt{sfd}(a, b)$ og herudfra definere en egenskab, der minder om egenskaberne for primtal, blot her for *par af tal*.

DEFINITION 5.3 ***Fælles divisor***
Et heltal $d > 0$ siges at være største fælles divisor *for to tal a og $b \in \mathbb{Z}$, hvis $d|a$ og $d|b$, og for enhver divisor i a eller b er disse divisorer i d.*
Dette skrives $d = \texttt{sfd}(a, b)$.

Vi vil i Sætning 5.4 vise et generelt resultat, der sikrer eksistens af største fælles divisor. Entydighed følger umiddelbart. Antag, at d og d' begge er største fælles divisorer for $a, b \in \mathbb{Z}$. Så følger af Definition 5.3, at $d'|d$ og $d|d'$, d.v.s. $d = d' \Rightarrow d = d'$ da største fælles divisor er positiv.

DEFINITION 5.4 ***Primiske tal***
Hvis to tal $a, b \in \mathbb{Z}$ har den største fælles divisor 1, da siges a og b at være indbyrdes primiske *eller blot primiske.*

Følgende sætning viser eksistensen af største fælles divisor for et talpar og giver desuden en repræsentation for denne, som vi vil anvende i Afsnit 5.1.1.

SÆTNING 5.4 ***Største fælles divisor som linearkombination***
Lad $a, b \in \mathbb{Z}$, hvor $(a, b) \neq (0, 0)$. Så findes $x, y \in \mathbb{Z}$ således, at

$$\texttt{sfd}(a, b) = xa + yb.$$

Bevis:
Lad S være mængden af alle linearkombinationer af a og b

$$S = \{am + bn \mid m, n \in \mathbb{Z} \quad \text{og} \quad am + bn > 0\}.$$

Ifølge Aksiom 5.1 har S et mindste element, $d = as + bt$. Vi påstår, at $d = \texttt{sfd}(a, b)$. For at bevise dette bruger vi Sætning 5.1 og skriver $a = dq + r$, hvor $0 \leq r < d$. Hvis $r > 0$, da har vi $r = a - dq = a - (as + bt)q = a - asq - btq = a(1 - sq) + b(-tq) \in S$. Dette er i modstrid med, at d er det mindste element i S, og derfor har vi at $r = 0$. Dette medfører, at $d|a$ og på samme måde kan vises, at $d|b$. Dermed har vi, at d er fælles divisor i a og b.

Vi skal nu blot vise at d også er den største divisor. Antag, at d' også er en fælles divisor i a og b. Derfor har vi, at $a = d'h$ og $b = d'k$. Dette medfører $d = as + bt = (d'h)s + (d'k)t = d'(hs + kt)$. Heraf ses, at $d'|d$. Dette medfører, at blandt alle divisorer i a og b er d den største.

■

5.1.1 Ækvivalens- og restklasser

Vi vil nu give en definition på *ækvivalensklasser* og herudfra indføre begrebet *restklasser*. Kort fortalt udtaler denne sig om, at mængden af heltal, der har samme rest ved division med et andet fast heltal, kan opfattes som et abstrakt objekt, for hvilket vi kan definere generelle regneregler som addition og multiplikation.

Disse regler beror dog i høj grad på generelle egenskaber for de såkadte ækvivalensrelationer og ækvivalensklasser.

DEFINITION 5.5 ***Ækvivalensrelationer***
Lad S være en mængde. En delmængde $R \subseteq S \times S$ kaldes en ækvivalensrelation på S, hvis

1. *for alle $a \in S$, $(a, a) \in R$ (refleksivitet).*
2. *for alle $a, b \in S$, hvis $(a, b) \in R \Leftrightarrow (b, a) \in R$ (symmetri).*
3. *for alle $a, b, c \in S$, hvis*

$$(a, b) \in R \quad \wedge \quad (b, c) \in R \Rightarrow (a, c) \in R(transitivitet).$$

Vi vil i det følgende bruge symbolet "$\sim$" for ækvivalensrelationer.

EKSEMPEL 5.1 ***"Lig med"***
Et eksempel på en ækvivalensrelation er relationen "er lig med" $(=)$*. Reflexiv, da* $x = x$*. Symmetrisk, da* $x = y \Leftrightarrow y = x$*. Transitiv, da* $x = y \wedge y = z \Rightarrow x = z$*.*

◆

Vi kan opfatte mængden af alle ækvivalenser mellem et fast element og et andet element i mængden S som en særlig mængde i sig selv.

DEFINITION 5.6 ***Ækvivalensklasser***
Lad "$\sim$*" være en ækvivalensrelation på mængden* S*.*
For hvert element $a \in X$ *lad* $[a]$ *være delmængden*

$$[a] := \{x \in S | x \sim a\}.$$

Delmængder af X*, som er på formen* $[a]$ *med et passende element* a *i* X*, kaldes* ækvivalensklasser.

DEFINITION 5.7 ***Klassedeling***
Lad S *være en mængde. En mængde* P *af delmængder af* S *kaldes en* klassedeling *af* S*, hvis ethvert element i* S *tilhører netop en af disse delmængder.*

SÆTNING 5.5 ***Ækvivalensrelationer og klassedeling***
For en ækvivalensrelation $\sim$ *på en mængde* X *udgør ækvivalensklasserne* $[a]$*, for* $a \in X$*, en klassedeling af* X*. To elementer* $a, b \in X$ *ligger i samme ækvivalensklasse, hvis og kun hvis* $a \sim b$*. Endvidere er* $[a] = [b]$*, hvis og kun hvis* $a \sim b$*. Omvendt gælder at givet en klassedeling af* X*, da er relationen "ligger i samme klasse som" en ækvivalensrelation.*

Bevis:
For at vise, at ækvivalensklasserne udgør en klassedeling, vil vi vise, at $[a]$ er den eneste, der indeholder b. Hvis $a \in [b]$ ønsker vi altså at bevise, at $[a] = [b]$.
Vi antager, at $a \in [b] \Rightarrow a \sim b$. Vi betragter et element $x \in [a] \Rightarrow x \sim a$. Ifølge transiviteten får vi, $x \sim a \wedge a \sim b \Rightarrow x \sim b$, altså $x \in [b]$.
Derfor må der gælde, at $[a] \subseteq [b]$. Betingelsen $a \sim b$ er symmetrisk, og derfor gælder $[b] \subseteq [a]$ også. Det medfører derfor, at $[a] = [b]$, og første del er hermed bevist.
Anden påstand bevises ved at antage $a \sim b$. Deraf følger, at $a \in [b]$ og $a \in [a]$. Dermed er $[a]$ og $[b]$ samme ækvivalensklasse. Elementerne a og b ligger altså i samme ækvivalensklasse $[a] = [b]$. Derefter antages, at a og b ligger i samme ækvivalensklasse. Denne ækvivalensklasse må være $[b]$. Da den er den eneste ækvivalensklasse, som indeholder b. Altså er $a \in [b]$, det vil sige $a \sim b$. Hermed er anden påstand bevist.
Endelig antages, at der er givet en klassedeling af X. Relationen "ligger i samme klasse som" er reflexiv, da a ligger i samme klasse som sig selv. Den er symmetrisk, idet a og b ligger i samme klasse, og b og a også ligger i samme klasse. Den er transitiv, hvis a og b ligger i samme klasse, og b og c gør ligeså, så medfører det, at a og c

ligger i samme klasse. Netop den entydigt bestemte klasse, som indeholder b. Relationen er altså en ækvivalensrelation, og de tilhørende ækvivalensklasser er øjensynligt delmængderne fra den givne klassedeling. ■

Disse definitioner og sætninger for ækvivalensrelationer kan vi anvende i forbindelse med begrebet, *kongruens* og rest.

DEFINITION 5.8 ***Kongruens***
For et givet tal $n \in \mathbb{N}$ siges to tal $x, y \in \mathbb{Z}$ at være kongruente modulo n *hvis $n|(x-y)$. Vi skriver også*

$$x \equiv y \pmod{n}.$$

Vi vil jævnligt i rapporten også blot bruge notationen $a = b \mod n$.

Definition 5.8 er den lettest tilgængelige definition på kongruens — men en definition, der er mere intuitiv for det følgende, vil nok snarere være, at to heltal x, y er kongruente modulo n, hvis de har samme rest ved division med n.

SÆTNING 5.6 ***Kongruenser er ækvivalensrelationer***
Kongruens modulo n er en ækvivalensrelation.

Bevis:
Da $n|(x-x)$ er relationen reflexiv. Hvis $n|(x-y)$ så går n også op i $(y-x) = -(x-y)$, og relationen er derfor også symmetrisk. Den er også transitiv, idet n går op i $(x-y)$ og $(y-z)$, så går n op i $(x-z) = (x-y)+(y-z)$. Hermed har vi vist, at kongruens modulo n er en ækvivalensrelation. ■

For hvert $a \in \mathbb{Z}$ er ækvivalensklassen en delmængde af $\mathbb{Z}$. Den indeholder de tal $x \in \mathbb{Z}$ for hvilke $n|(x-a)$ — eller alternativt, alle tal, der har samme rest ved division med n. Denne mængde kan vi derfor opskrive således

$$[a] = \{\ldots a-2n, a-n, a, a+n, a+2n \ldots\}. \tag{5.1}$$

Disse ækvivalensklasser kaldes også *restklasser* modulo n. Mængden af restklasser betegnes $\mathbb{Z}/n\mathbb{Z}$. Som den gængse repræsentant for en restklasse anvendes den *mindste* ikke-negative rest.

Af Sætning 5.1 fremgår det, at der højest kan være n forskellige rester ved division med n. Det følger derfor, at mængden $\mathbb{Z}/n\mathbb{Z}$ indeholder netop n forskellige restklasser

$$[0], [1], \ldots, [n-1].$$

En afgørende egenskab ved restklasser er, at det er muligt at indføre operationer på abstrakte restklasser, svarende til addition og multiplikation på hele tal.

SÆTNING 5.7 ***Addition og multiplikation af restklasser***
For to restklasser A og B modulo n lad a være et arbitrært element i restklassen A, og b et arbitrært element i restklassen B.
Da er følgende regler for addition og multiplikation veldefinerede.

$$\begin{aligned} A+B &\equiv [a+b] \\ A\cdot B &\equiv [ab]. \end{aligned} \tag{5.2}$$

Bevis:
Vi skal vise, at operationerne er uafhængige af valg af a og b. Lad a' være et andet tal i restklassen A, og b' er et andet tal i restklassen B.

Da a' og a ligger i samme restklasse, er de kongruente modulo n, og derfor findes der et tal $q \in \mathbb{Z}$, således at $a' = a + qn$. Tilsvarende findes et tal $s \in \mathbb{Z}$, således at $b' = b + sn$. Vi får så, at

$$a' + b' = a + qn + b + sn = a + b + (q+s)n,$$

samt

$$a'b' = (a+qn)(b+sn) = ab + (qb + as + qsn)n.$$

Det følger, at $a' + b' \equiv a + b$ og $a'b' \equiv ab$. Altså er $[a' + b'] = [a + b]$ og $[a'b'] = [ab]$. Sætningen er da bevist. ■

SÆTNING 5.8 ***Regneregler for restklasser***
For regning med restklasser A, B, C $modulo$ n gælder følgende regler

Kommutativitet $A + B = B + A$ *og* $AB = BA$.

Associativitet $A + (B + C) = (A + B) + C$ *og* $A(BC) = (AB)C$.

Distributivitet $A(B + C) = AB + AC$.

Neutrale selementer $A + [0] = A$ *og* $A \cdot [1] = A$.

Additivt invers $A + (-A) = [0]$.

Bevis:
Vælg tallene a og b i restklasserne A og B.

Vi har da ligningerne

$$A + B = [a + b] = [b + a] = B + A.$$

Det første og sidste i ligningen er definitionen på addition af restklasser. Den midterste følger af, at addition af hele tal, er kommutativ. Dermed er den første regel bevist. På samme måde følger de øvrige regler. ■

EKSEMPEL 5.2 ***Lige/ulige tal***
V.h.a. restklasser kan vi repræsentere lige og ulige tal v.h.a. elementerne i mængden $\mathbb{Z}/2\mathbb{Z}$*. Elementerne i denne mængde er*

$$\begin{aligned}[0] &= \{\ldots, -4, -2, 0, 2, 4, \ldots\} \\ [1] &= \{\ldots, -5, -3, 1, 1, 3, 5, \ldots\}.\end{aligned}$$

Af regneregler for restklasser følger, at $[0] + [0] = [0]$ *(summen af to lige tal er lige),* $[0]+[1] = [1]$ *(summen af et lige og et ulige tal er ulige), samt* $[1]+[1] = [0]$ *(summen af to ulige tal er lige) — og vi har således med restklassebegrebet vist de velkendte regler for addition af lige/ulige tal.*

◆

5.2 Gruppeteori

I det følgende afsnit vil vi bl.a. gøre rede for, at mængden af restklasser modulo n, $\mathbb{Z}/n\mathbb{Z}$ kan opfattes som en særlig type algebraisk objekt, en *gruppe*. Det er operationer på denne gruppe, der skal danne grundlag for vores senere opstilling af et konkret kryptosystem. Det viser sig nemlig, at der kan opstilles en formodet en-vejs funktion baseret på gruppeoperationer — udfra denne vil vi i Afsnit 6.1 opstille ElGamal kryptosystemet.

Efter redegørelse for grundlæggende gruppeteoretiske begreber vil vi undersøge en række afgørende matematiske operationer på $\mathbb{Z}/n\mathbb{Z}$ og elementer heri ud fra et beregningsmæssigt synspunkt. Ydermere vil vi demonstrere, at der findes algoritmer til multiplikation og eksponentiation af restklasser, der har *polynomiel kompleksitet* m.h.t. bit-længden af inputstrengen.

Endelig vil vi kort belyse nogle få algoritmer til beregning af *diskrete logaritmer* i grupper og gøre rede for, at dette er et vanskeligt problem.

5.2.1 Grundlæggende begreber

Vi vil nu indføre det vigtige algebraiske begreb en *gruppe*. I sig selv er begrebet uhyre simpelt, men dets nærmere egenskaber viser sig at have mange følger, der i forbindelse med opstillingen af et effektivt kryptosystem er afgørende.
Afsnittene 5.2.1-5.2.3 er baseret på [Beachy and Blair, 1996, Kap. 2].

DEFINITION 5.9 ***Gruppeaksiomerne***
En gruppe $(G, *)$ er en ikke-tom mængde G med en komposition $* : G \times G \to G$, der opfylder:

Lukkethed *For alle $a, b \in G$ gælder, at $a * b \in G$.*

Associativitet *For alle $a, b, c \in G$ er $(a * b) * c = a * (b * c)$.*

Neutralt element *Der eksisterer et neutralt element $e \in G$, således at for ethvert $a \in G$ er $e * a = a * e = a$.*

Invers *For ethvert $a \in G$ eksisterer der et inverst element $a^{-1} \in G$, således at $a * a^{-1} = a^{-1} * a = e$.*

For fremtiden vil vi blot skrive $(G, *)$ som G og lade kompositionen være indforstået, d.v.s. vi skriver $a * b$ som ab (eller $a \cdot b$).
Definition 5.9 udtaler sig udelukkende om *eksistens* af hhv. neutralt element og inverse elementer, men ikke om entydighed. Det gælder imidlertid, at der i enhver gruppe G eksisterer netop et neutralt element $e \in G$. Antag, at dette ikke var tilfældet. Så eksisterer der et andet neutralt element e'. Der må derfor gælde, at $e'e = e$ samt $e'e = e'$, hvorfor $e = e'$.
Associativitetskravet medfører desuden entydighed for inverse elementer. Lad G være

en gruppe og antag, at for et element a er både b og b' inverse elementer, d.v.s. $ab = ab' = e \wedge ba = b'a = e$. Da fås

$$b' = eb' = (ba)b' = b(ab') = be = b.$$

SÆTNING 5.9 ***Reduceringsegenskaber for grupper***
Lad G være en gruppe, og lad $a, b, c \in G$. Så gælder

1. *Hvis $ab = ac$, så er $b = c$*
2. *Hvis $ac = bc$, så er $a = b$.*

Bevis:
Der er givet $ab = ac$. Ved multiplikation på begge sidder af udtrykket med a^{-1} fås $a^{-1}(ab) = a^{-1}(ac)$. Af den associative lov fås $(a^{-1}a)b = (a^{-1}a)c$. Så er $eb = ec \Leftrightarrow b = c$. Beviset for anden del af sætningen forløber på samme måde. ■

D.v.s. der gælder, som i elementær algebra, at vi kan "dividere" med fælles elementer på højre- og venstresiden af lighedstegnet (også selvom det ikke forlanges, at den anvendte komposition er kommutativ).

Vi definerer *ordenen* af en gruppe som følger.

DEFINITION 5.10 ***Orden af en gruppe***
En gruppe G siges at være endelig, hvis G har et endeligt antal elementer. Antallet af elementer kaldes da ordenen af G og skrives $|G|$.

Det er ofte tilfældet, at en gruppe ikke er endelig. Et oplagt eksempel er den additive gruppe af hele tal, $\mathbb{Z}$. Det er oplagt, at dette er en gruppe under addition af heltal med neutralt element 0 og inverst element $a^{-1} = -a$, så $a + a^{-1} = a + (-a) = 0$. Imidlertid er denne gruppe ikke endelig, eftersom $|\mathbb{Z}| = \infty$. I denne rapport vil vi udelukkende beskæftige os med endelige grupper.

Bemærk, at det i gruppeaksiomerne ikke er et krav, at kompositioner er kommutative. Dette er generelt ikke tilfældet, men grupper, der har denne specielle egenskab, kaldes *abelske* eller blot kommutative.

DEFINITION 5.11 ***Abelsk gruppe***
Lad G være en gruppe. G siges da at være abelsk, *hvis $ab = ba$ for alle $a, b \in G$.*

Ydermere er det oplagt, at man for en gruppe G kan definere undermængder, der i visse tilfælde vil arve de oprindelige egenskaber fra gruppen G — som f.eks. vektorrum (der iøvrigt også er additive grupper).
Sådanne mængder kaldes *undergrupper* til gruppen G.

DEFINITION 5.12 ***Undergruppe***
Lad G være en gruppe, og lad $H \subseteq G$. Så kaldes H en undergruppe *til G, hvis H er en gruppe under den oprindelige komposition i G. Dette skrives $H \preceq G$.*

EKSEMPEL 5.3 ***Vektorrum***
Et reelt vektorrum V er en gruppe under addition af vektorer. Hvis $\mathbf{v}$,$\mathbf{u} \in V$, så gælder at $\mathbf{v}$+$\mathbf{u} \in V$. Ydermere gælder den associative lov, og der eksisterer et neutralt element, nulvektoren. Endelig findes der for enhver vektor $\mathbf{v} \in V$ et inverst element, $-\mathbf{v} = (-1) \cdot \mathbf{v}$.
Af aksiomerne for et vektorrum ses, at V er en abelsk gruppe, samt at V ikke har endelig orden. Desuden fremgår det, at ethvert underrum $H \subseteq V$ er en undergruppe til gruppen V. Det modsatte gælder dog ikke generelt. F.eks. er mængden af polynomier

$$P = \{p(t) \,|\, p(t) = \sum_{i=0}^{3} a_i t^i, \quad a_i \in \mathbb{Z}\},$$

ikke et underrum til $\mathbb{P}_3$, da P ikke er lukket under skalarmultiplikation (med reelle skalarer). Imidlertidig er P en undergruppe til den additive gruppe $\mathbb{P}_3$.

◆

Der gælder et nyttigt generelt resultat for sammenhængen mellem ordenen af en arbitrær undergruppe til en gruppe G og ordenen af G selv, som oprindeligt blev vist af franskmanden Joseph Louis Lagrange (1736-1813). Resultatet danner basis for mange vigtige gruppeteoretiske resultater, men i denne rapport vil vi kun anvende det i begrænset omfang. P.g.a. dets vigtighed har vi imidlertid valgt at tage det med.

LEMMA 5.2
Lad G være en gruppe, og lad $H \preceq G$. For alle $a, b \in G$ defineres relationen $a \sim b$, hvis $ab^{-1} \in H$. Så er $\sim$ en ækvivalensrelation.

Bevis:
Vi skal blot vise refleksivitet, symmetri og transitivitet for $\sim$.
Det ses, at $\sim$ er refleksiv, idet $aa^{-1} = e \in H$. Ydermere er $\sim$ symmetrisk, eftersom $a \sim b \Leftrightarrow ab^{-1} \in H$, hvorfor også $(ab^{-1})^{-1} = ba^{-1} \in H \Leftrightarrow b \sim a$. Slutteligt er relationen transitiv, thi hvis $a \sim b$ og $b \sim c$ for $a, b, c \in G$, så gælder at $ab^{-1}, bc^{-1} \in H$, hvorfor $ab^{-1}bc^{-1} = ac^{-1} \in H$ og $a \sim c$. ■

SÆTNING 5.10 ***Lagrange***
Lad G være en endelig gruppe, og lad $H \preceq G$. Så er ordenen af H en divisor i ordenen for G.

Bevis:
Lad $\sim$ betegne ækvivalensrelationen defineret i Lemma 5.2, og lad $[a]$ betegne ækvivalensklassen for ethvert $a \in G$. Da gælder, at funktionen $f_a : H \to [a]$ defineret ved $f_a(x) = xa$ for alle $x \in H$ er en bijektion. Antag, at $h, k \in H$, således at $f_a(h) = f_a(k) \Leftrightarrow ha = ka$. Da det i enhver gruppe er tilladt at reducere, fås $h = k$, d.v.s. f_a er injektiv. Det ses desuden, at f_a er surjektiv, idet hvis $y \in G$, hvor $y \sim a$, så er $ya^{-1} = h$ for et $h \in H$, hvorfor ligningen $f_a(x) = y$ har løsningen $x = h$, da $ha = (ya^{-1})a = y$.
Ifølge Sætning 5.5 klassedeler en ækvivalensrelation $\sim$ en mængde G, således at

ethvert element $a \in G$ tilhører netop en ækvivalensklasse. Eftersom f_a er en bijektion på H, må hver ækvivalensklasse have $|H|$ elementer. Antag, at der er n forskellige ækvivalensklasser. Så må vi have, at $|G| = n|H|$, d.v.s. ordenen af H er en divisor i ordenen for G. ■

Vi indfører følgende notation for *potensen* af et element i en gruppe.

DEFINITION 5.13 ***Potens af gruppeelement***
Lad G være en gruppe, og lad $a \in G$. Med notationen a^n menes

$$a^n = \underbrace{a \cdot a \cdot a \cdot \cdots \cdot a}_{n\text{gange}}.$$

Desuden defineres $a^0 = e$, samt $a^{-n} = (a^{-1})^n$.

V.h.a. induktionsargumenter kan det vises, at de gængse potensregneregler også holder i grupper.

Definition 5.13 har naturligvis forskellige former alt afhængigt af den valgte komposition — i en additiv gruppe er

$$na = \underbrace{a + a + \cdots + a}_{n\text{gange}}.$$

I det følgende vil vi anvende den generelle notation a^n. Vi vil af overskuelighedshensyn også jævnligt gennem resten af rapporten anvende notationen a/b for produktet ab^{-1} (og tilsvarende $a/b^n = a(b^n)^{-1}$).

DEFINITION 5.14 ***Orden af et element***
Lad G være en endelig gruppe. Et element $a \in G$ siges at have ordenen $n = o(a)$, hvis $o(a) = \min_{n \in \mathbb{Z}_+}(n)$, således at $a^n = e$.
Såfremt der ikke findes et sådan n, siges ordenen af a at være uendelig.

LEMMA 5.3
Lad G være en gruppe, og lad $a \in G$ samt $m \in \mathbb{Z}$. Så er $a^m = e$, hvis og kun hvis $o(a)|m$.

Bevis:
Lad $o(a) = n$. Hvis $m = kn$ fås

$$a^m = a^{kn} = a^{nk} = e^k = e.$$

Omvendt, lad $a^m = e$ og antag, at n *ikke* er en divisor i m, d.v.s. antag, at $m = qn + r$, $0 \leq r < n$.
Så er

$$a^r = a^{m-qn} = a^m(a^n)^{-q} = e.$$

Da r er mindre end n, og vi har antaget, at $n = o(a)$ er det mindste tal, således at $a^n = e$, må der nødvendigvis gælde, at $r = 0$, og lemmaet er hermed bevist. ■

Dette lemma kan vi bruge til at vise et generelt resultat, der sammenknytter ordenen af en arbitrær potens af et element med ordenen af selve elementet.

SÆTNING 5.11 ***Orden af potens***
Lad G være en gruppe, og lad $a \in G$ være et element af endelig orden $n = o(a)$. Så er ordenen af a^i

$$o(a^i) = \frac{n}{\texttt{sfd}(n,i)}.$$

Bevis:
Vi har

$$(a^i)^{n/\texttt{sfd}(n,i)} = (a^n)^{i/\texttt{sfd}(n,i)} = e^{i/\texttt{sfd}(n,i)} = e.$$

Ifølge Lemma 5.3 er $\frac{n}{\texttt{sfd}(n,i)}$ da et multiplum af ordenen af a^i.
Antag, at

$$e = (a^i)^k = a^{ik}.$$

Så følger, ligeledes af Sætning 5.3, at $n|ik$ og $\frac{n}{\texttt{sfd}(n,i)}|k$ og sætningen er bevist. ■

5.2.2 Grupper af restklasser

Det er oplagt, at mægnden af restklasser modulo n, $\mathbb{Z}/n\mathbb{Z}$, er en gruppe under addition af restklasser. Vi gjorde i Afsnit 5.1.1 rede for, at addition var veldefineret, associativ og kommutativ, samt at mængden er lukket under denne operation. Ydermere findes der et neutralt element, $e = [0]$.

Det er derfor oplagt at spørge, hvorvidt det samme gælder for den multiplikative gruppe af restklasser modulo n? Følgende eksempel viser, at dette ikke nødvendigvis er tilfældet.

EKSEMPEL 5.4 ***Multiplikative grupper af restklasser***
Overvej mængden $(\mathbb{Z}/4\mathbb{Z})\backslash[0]$. Denne mængde er ikke *lukket under multiplikation, idet $[2][2] = [0]$, og mængden er således ikke en gruppe under multiplikation.*

◆

Det gælder imidlertid, at mængden af restklasser $[a]_n$, er en gruppe, $(\mathbb{Z}/n\mathbb{Z})^*$, når a og n er indbyrdes primiske, d.v.s. $\texttt{sfd}(a,n) = 1$.

SÆTNING 5.12 ***Multiplikativ gruppe af restklaser***
Mængden

$$\{[a] \in \mathbb{Z}/n\mathbb{Z} \mid \texttt{sfd}(a,n) = 1\},$$

er en abelsk gruppe under multiplikation af restklasser. Denne gruppe skrives $(\mathbb{Z}/n\mathbb{Z})^*$.

Bevis:
Lad $[a], [b] \in (\mathbb{Z}/n\mathbb{Z})^*$, da følger af Definition 5.3, at

$$\texttt{sfd}(a,n) = \texttt{sfd}(b,n) = 1 \Rightarrow \texttt{sfd}(ab,n) = 1.$$

Associativitet og kommutativitet for multiplikation er indlysende. Der eksisterer et neutralt element $e = [1]$. Ydermere har ethvert element $[a] \in (\mathbb{Z}/n\mathbb{Z})^*$ en multiplikativ invers. Hvis $\texttt{sfd}(a, n) = 1$ følger af Sætning 5.4, at der findes $x, y \in \mathbb{Z}$, så $\texttt{sfd}(a, n) = xa + yn = 1$, d.v.s. $a \equiv 1 \pmod{n}$, og $[x] = [a]^{-1}$.

Sætningen er da bevist. ■

Faktisk gælder, at det *kun* er denne mængde, der giver anledning til en multiplikativ gruppe af restklasser, idet der kun eksisterer multiplikative inverse for alle elementer i netop denne mængde.

Følgende er da umiddelbart indlysende, thi for ethvert $a \in \mathbb{Z}$, er $\texttt{sfd}(a, p) = 1$, hvor p er et primtal.

KOROLLAR 5.1
$(\mathbb{Z}/p\mathbb{Z})^*$ er en multiplikativ abelsk gruppe.

Vi indfører nu den særlige funktion, *Eulers phi-funktion*, der angiver ordenen af $(\mathbb{Z}/n\mathbb{Z})^*$

DEFINITION 5.15 ***Phi-funktionen***
Lad afbildingen $\varphi : \mathbb{N} \to \mathbb{N}$ være givet ved

$$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|.$$

Denne funktion kaldes Eulers phi-funktion *eller blot phi-funktionen.*

Phi-funktionen er her indført i en gruppeteoretisk sammenhæng, men det er indlysende, at den også i en talteoretisk sammenhæng har en berettigelse, i den forstand, at $\varphi(n)$ netop er antallet af tal $m \leq n$, for hvilke $\texttt{sfd}(n, m) = 1$ — altså antallet af tal, der er indbyrdes primiske med n. Specielt gælder, at $\varphi(1) = 1$.
Af denne iagttagelse kan vi ydermere konkludere, at såfremt p er et primtal, er $\varphi(p) = p - 1$ ud fra Definition 5.2 om primtal. Desuden har funktionen følgende egenskab

SÆTNING 5.13 ***Sum af divisorer***

$$\sum_{d|n,\ d>0} \varphi(d) = n.$$

Bevis:
Da mængden $\{d \mid d|n, d > 0\} = \{\frac{n}{d} \mid d|n, d > 0\}$ har vi

$$\sum_{d|n,\ d>0} \varphi(d) = \sum_{d|n,\ d>0} \varphi(n/d).$$

D.v.s. det må gælde, at

$$\begin{aligned} \sum_{d|n,\ d>0} \varphi(d) &= \sum_{d|n,\ d>0} |\{k \mid \texttt{sfd}(k, \frac{n}{d}) = 1, \quad 1 \leq k \leq \frac{n}{d}\}| \\ &= \sum_{d|n,\ d>0} |\{m \mid \texttt{sfd}(m, n) = d, \quad 1 \leq m \leq n\}|. \end{aligned}$$

Imidlertid er $|\{m \mid \texttt{sfd}(m,n) = d, \quad 1 \leq m \leq n\}| = n$. Dette følger, idet

$$\{1, 2, \ldots, n\} = \bigcup_{d|n,\ d>0} \{m|\ \texttt{sfd}(m,n) = d, 1 \leq m \leq n\}.$$

Dette vises som følger.
Vi skal undersøge om både $\{1, 2, \ldots, n\} \supseteq \bigcup_{d|n,\ d>0}\{m|\ \texttt{sfd}(m,n) = d, 1 \leq m \leq n\}$ og $\{1, 2, \ldots, n\} \subseteq \bigcup_{d|n,\ d>0}\{m|\ \texttt{sfd}(m,n) = d, 1 \leq m \leq n\}$. Hvis dette er opfyldt er mængderne ens. Det første er umiddelbart klart, da foreningen er disjunkt og dermed er indeholdt i $\{1, 2, \ldots, n\}$. Undersøgelse af det andet kræver flere overvejelser.
Lad $m_0 \in \{1, 2, \ldots, n\}$, og sæt $d = \texttt{sfd}(m_0, n)$. Så er $d|n,\ d > 0$, og $m_0 = \{m|\ \texttt{sfd}(m,n) = d, 1 \leq m \leq n\} \subseteq \bigcup_{d|n,\ d>0}\{m|\ \texttt{sfd}(m,n) = d, 1 \leq m \leq n\}$.
Da d er entydig, er m_0 indeholdt i netop en af mængderne, som derfor er disjunkte. Dermed er sætningen bevist. ■

Den multiplikative gruppe $(\mathbb{Z}/p\mathbb{Z})^*$, vil danne baggrund for vore videre studier. Det viser sig, at særlige operationer i denne gruppe er relativt lette at udføre, mens den omvendte operation i praksis, for grupper af høj orden, er umulig. Specielt formodes, at disse kan betragtes som en-vejs funktioner.

5.2.3 Cykliske grupper

En *cyklisk gruppe* G er en særlig type gruppe, der har den egenskab, at et enkelt element i gruppen frembringer G.

SÆTNING 5.14 ***Cyklisk undergruppe***
Lad G være en gruppe, og lad $a \in G$. Da gælder, at

$$\langle a \rangle = \{x \in G \,|\, a^n = x \text{ for et } n \in \mathbb{Z}\},$$

er en undergruppe til G. $\langle a \rangle$ kaldes den cykliske undergruppe *frembragt af a.*

Bevis:
Resultatet er oplagt, da $\langle a \rangle$ er lukket under multiplikation, idet $a^n, a^m \in G$, hvorfor $a^n a^m = a^{n+m} \in \langle a \rangle$. $\langle a \rangle$ indeholder neutral elementet, da $a^0 = e$, og der eksisterer inverse elementer, idet $(a^n)^{-1} = a^{-n} \in \langle a \rangle$. ■

Elementerne i en cyklisk undergruppe $\langle a \rangle \preceq G$ er parvist forskellige; hvis $a^i = a^j$, $0 \leq i < j \leq o(a) - 1$ fås, at $a^{i-j} = e$ i modstrid med definitionen på orden af element, jf. Definition 5.14.

Vi har følgende definition.

DEFINITION 5.16 ***Cyklisk gruppe***
Lad G være en gruppe. G siges at være cyklisk, *hvis der findes et element $a \in G$, således at $\langle a \rangle = G$.*
I så fald kaldes a en frembringer *for G.*

Vi vil nu vise, at gruppen $(\mathbb{Z}/p\mathbb{Z})^*$, hvor p er et primtal, er cyklisk

Bemærk, at vi her gør kort brug af, at $\mathbb{Z}/n\mathbb{Z}$ under både multiplikation og addition er et såkaldt *legeme*, d.v.s. vi kan tale om *polynomier* over dette. Jf. Appendiks A for en kort introduktion til polynomier og legemer.

SÆTNING 5.15 ***Antal elementer af orden*** d
Lad d være en divisor i $p-1$, hvor p er et primtal.
I gruppen $(\mathbb{Z}/p\mathbb{Z})^*$ eksisterer der da netop $\varphi(d)$ elementer af orden d.

Bevis:
Vi har, at $\texttt{sfd}(a,p) = 1$. Lad h være ordenen af et element a, d.v.s. det mindste tal, således at $a^h = e$.
Givet den cykliske undergruppe $\langle a \rangle$ fås af Sætning 5.10, at ordenen af denne undergruppe er en divisor i ordenen af den oprindelige gruppe, d.v.s. $h \mid (p-1)$. Ydermere er det klart, at for $i = 0, 1, \ldots, h-1$ er a^i parvis forskellige og rødder i polynumiet $x^h - 1$. Dette ses, idet $(a^i)^h - 1 = (a^h)^i - 1 = 1 - 1 = 0$. Dette polynomium har højst h rødder jf. Appendix A. D.v.s. polynomiet har præcist h rødder på formen a^i. Derfor er ethvert element i $(\mathbb{Z}/n\mathbb{Z})^*$ af orden h rod i $x^h - 1$ og derfor på formen a^i for $i = 0, 1, \ldots, h-1$. Ordenen af a^i er da netop, ifølge Sætning 5.11, $\frac{h}{\texttt{sfd}(i,h)}$, d.v.s. for elementer med orden h, er $\texttt{sfd}(i,h) = 1$.
Af definitionen på Eulers phi-funktion, Definition 5.15, er der netop $\varphi(h)$ af disse. D.v.s. for ethvert h, der er divisor i $p-1$ er der enten 0 eller $\varphi(h)$ elementer af orden h. Lad n_h betegne dette tal. Vi har da

$$p - 1 = \sum_{h|p-1} n_h \leq \sum_{h|p-1} \varphi(h) = p - 1.$$

Lighedstegnet i ovenstående gælder, hvis og kun hvis $n_h = \varphi(h)$ for alle $h|(p-1)$, d.v.s. der er netop $\varphi(h)$ elementer af orden h. ■

Det følger da umiddelbart af ovenstående, at der eksisterer netop $\varphi(p-1)$ elementer af orden $p-1$, d.v.s. elementer a for hvilke $o(a) = |(\mathbb{Z}/p\mathbb{Z})^*|$. Det giver følgende korollar.

KOROLLAR 5.2
Gruppen $(\mathbb{Z}/p\mathbb{Z})^*$ er cyklisk.

Dette resultat giver muligheden for at indføre den særlige operation, *eksponentiation af frembringere*. Hvis $g \in (\mathbb{Z}/p\mathbb{Z})^*$ er en frembringer, lad da $\texttt{exp}$ være givet ved $\texttt{exp} : \langle g \rangle \times \mathbb{N} \to \langle g \rangle$

$$\texttt{exp}(g, x) = g^x, \qquad 0 \leq x \leq p-2,$$

en bijektion. Dette gør det muligt at indføre en omvendt funktion

DEFINITION 5.17 ***Diskret logaritme i*** $(\mathbb{Z}/p\mathbb{Z})^*$
Lad $g, y \in (\mathbb{Z}/p\mathbb{Z})^*$. Antag ydermere, at g frembringer $(\mathbb{Z}/p\mathbb{Z})^*$. Den diskrete logaritme *af y m.h.t. g defineres da som det tal $0 \leq n < p-2 \in \mathbb{Z}$, for hvilket $g^n = y$.*

Ovenstående er en definition af den diskrete logaritme netop i $(\mathbb{Z}/p\mathbb{Z})^*$, men da eksponentiationsfunktionen kan udvides til generelle cykliske grupper, følger at diskret logaritme kan indføres som et generelt begreb.

Der er god evidens for, at netop eksponentiation af frembringere i $(\mathbb{Z}/p\mathbb{Z})^*$ *er en envejs funktion* for tilstrækkeligt store p, d.v.s. (jf. Afsnit 4.1.1) er det beregningsmæssigt uoverkommeligt at udregne diskrete logaritmer. På nuværende tidspunkt har de bedste algoritmer til beregning af denne *eksponentiel kompleksitet* m.h.t. bit-længden af p. Dette vil der blive argumenteret nærmere for i Afsnit 5.3.1.

I Afsnit 5.3 viser vi desuden, at eksponentiation i denne gruppe kan gøres i polynomiel tid m.h.t. bit-længden af inputstrengene, d.v.s. beregning af den oprindelige funktion er beregningsmæssigt let.

Det er denne formodede en-vejs funktion, vi i Afsnit 6.1 vil anvende til opstillingen af ElGamal kryptosystemet.

5.3 Beregninger i $(\mathbb{Z}/p\mathbb{Z})^*$

Vi har i de foregående afsnit argumenteret matematisk for egenskaberne ved gruppen $(\mathbb{Z}/p\mathbb{Z})^*$, heriblandt selve regneoperationerne samt at gruppen er cyklisk. Ud fra en matematisk vinkel er dette tilstrækkeligt, men i Kapitel 6 er det imidlertid også afgørende, at sikre sig, at en række relevante operationer også i praksis kan udføres for denne type grupper af meget stor orden.
Specielt er det afgørende at redegøre for metode og kompleksitet af følgende problemer:

1. Multiplikation af restklasser.
2. Eksponentiation.
3. Beregning af frembringere.

I dette afsnit vil vi undersøge ovenstående og redegøre for konkrete metoder og kompleksiteten af disse. Afsnittet er baseret på [Buchmann, 2000, Afsnit 2.12].
Vi vil kort redegøre for, uden egentlige beviser, at multiplikation kan udføres i kvadratisk tid m.h.t. bit-længderne af inputstrengene. Bemærk, at øvrige operationer ikke er relevante i den sammenhæng, vi betragter problemstillingen, d.v.s. ud fra en rent gruppeteoretisk vinkel ($\mathbb{Z}/p\mathbb{Z}$ er imidlertid også en additiv gruppe, heraf følger bl.a., at gruppen er et såkaldt *endeligt legeme*, jf. [Beachy and Blair, 1996, Kap. 6.5]).
Idet dette afsnit fokuseres på de beregningsmæssige aspekter, vil vi antage, at de indgående størrelser er i binær repræsentation, d.v.s. et tal $a \in \mathbb{Z}$ repræsenteres i base 2

$$a = \sum_{i=0}^{k-1} a_i 2^i, \quad a_i \in \{0, 1\}.$$

Tallet a siges da at have bit-længde k.

5.3.1 Kompleksitet af algoritmer

Vi vil i det følgende samt kommende afsnit jævnligt anvende begrebet *kompleksitet af algoritmer*.

DEFINITION 5.18 ***O*-notation**
Lad $f : X \subseteq \mathbb{N} \to \mathbb{R}_+$ og $g : Y \subseteq \mathbb{N} \to \mathbb{R}_+$ være funktioner.
Funktionen f siges da at være $O(g)$, hvis der findes positive heltal C, B, således at for alle $n \in X \cap Y$, $n > B$, er

$$f(n) \leq Cg(n).$$

Der gælder desuden, at O-estimatet for to funktioner med O-estimatet $g(n)$ og $f(n)$ er $\max(f(n), g(n))$. Resultatet er intuitivt oplagt, for detaljer henvises til [Rosen, 1999, Afsnit 1.8].

En algoritme A, der tager input af længde n, siges da at have tidskompleksiteten $g(n)$ med hensyn til antallet af bit-operationer, hvis antallet af bit-operationer ved udførelse af A er $O(g(n))$. Kompleksiteten er derfor et mål for det maksimale antal bit-operationer ved udførelse af algoritmen.

I denne rapport vil vi støde på en række generelle kompleksitetsestimater anført i Tabel 5.1.

Kompleksitetstype	**O-estimat**
Konstant	$O(b)$
Lineær	$O(bn)$
Polynomiel	$O(n^b)$
Eksponentiel	$O(b^n)$

Tabel 5.1: Kompleksitetstyper

Bemærk, at kompleksitetsvurderingen altid er relativ i forhold til målet. Det er gængs praksis at måle kompleksitet i antal bit-operationer; dette vil vi gøre i de kommende afsnit.

I situationer, hvor antal bit-operationer i underliggende algoritmer kan variere, er det imidlertid mere hensigtsmæssigt at måle kompleksiteten i andre operationer (f.eks. antallet af multiplikationer). Vi vil naturligvis anføre, hvad kompleksiteten måles i i forhold til de enkelte tilfælde.

5.3.2 Modulær multiplikation

Klassisk modulær multiplikation i $(\mathbb{Z}/n\mathbb{Z})^*$ kan udføres ved en relativt enkel procedure — foretag en multiplikation og reducer produktet modulo n, d.v.s. beregn resten

ved division med n.
Antag, at $[a], [b] \in (\mathbb{Z}/n\mathbb{Z})^*$, samt at de respektive bit-længder er $|a| = |b| = n$.

Multiplikation af $a, b \in \mathbb{Z}$ kræver da, ved brug af den klassiske multiplikationsalgoritme, [Rosen, 1999, Kap. 2.4] $O(n^2)$ bit-operationer. Efterfølgende beregning af resten ved division med n, $ab \mod n$ kan gøres med tilsvarende kvadratisk kompleksitet m.h.t. bit-længden n, ganske enkelt ved brug af den oplagte papir-og-blyant metode for division af (binære) heltal med rest; dette kan vises at have kompleksitet $O(n^2)$.
Den samlede kompleksitet er således $O(n^2)$.

For mere effektive multiplikationsmetoder, jf. [Crandall and Pomerance, 2001, Kap. 9].

5.3.3 Eksponentiation er polynomiel i $(\mathbb{Z}/n\mathbb{Z})^*$

Dette er en af de allermest afgørende operationer i den sammenhæng, vi senere skal anvende modulær aritmetik i. Modulære operationer har i denne sammenhæng den interessante egenskab, at kompleksiteten som funktion af inputstrengenes bit-længde er polynomiel — ved beregninger i f.eks. $\mathbb{Z}$ er den eksponentiel[1].
Eksponentiation af et element $a \in (\mathbb{Z}/n\mathbb{Z})^*$ vil sige beregning af

$$a^m \mod n, \qquad m > 0.$$

En naiv metode vil blot være at udføre m gentagne multiplikationer, men dette er klart en omkostningsfyldt fremgangsmåde rent beregningsmæssigt.

I stedet anvendes en alternativ metode, og herudfra demonstrere en algoritme til modulær eksponentiation, som er betydeligt mere effektiv end den umiddelbare.

Den binære udvidelse af b er da, $b = \sum_{i=0}^{k-1} b_i \cdot 2^i$, hvor $b_i \in \{0, 1\}$. Vi betragter da følgende udregning

$$\begin{aligned} a^{\sum_{i=0}^{k-1} b_i 2^i} &= a^{b_0} \cdot (a^2)^{\sum_{i=1}^{k-1} b_i 2^{i-1}} \\ &= a^{b_0} \cdot (a^2)^{b_1} \cdot (a^4)^{\sum_{i=2}^{k-1} b_i 2^{i-2}} \\ &\vdots \quad \vdots \\ &= \prod_{i=0}^{k-1} (a^{2^i})^{b_i} = \prod_{0 \le i \le k, b_i = 1} a^{2^i}. \end{aligned}$$

Denne metode kan anvendes til en effektiv implementering af eksponentiation i $\mathbb{Z}/n\mathbb{Z}$. Vi har følgende pseudokode

[1] Ved beregning af a^b, (hvor $\log_2 a = |a|$ og $\log_2 b = b$) er bit-længden af resultatet $|a^b| = \log_2 a^b = b \log_2 a = \log_2 a \cdot 2^{\log_2 b}$, d.v.s. bit-længden af resultatet er eksponentiel, og en algoritme må da være ligeså.

```
Procedure modexp(a, b, n)
  let b := b_{k-1} b_{k-2} ··· b_0
  let x := a
  let y := 1
    For i = 0, 1, ..., k − 1 do
      if b_i = 1 let y := yx mod n
      let x := x^2 mod n
    return y
```

Antag, at $|x| = |y| = n$, samt at $|b| = k$. Da foretages for hvert skridt maksimalt to modulære multiplikationer, hvilket gøres k gange, d.v.s. kompleksiteten er $O(kn^2)$.

5.3.4 Beregning af frembringere

Vi vil nu overveje problematikken, *hvordan* man konkret beregner frembringere i den cykliske gruppe $(\mathbb{Z}/p\mathbb{Z})^*$. Vi gjorde i Afsnit 5.2.3 rede for, at der eksisterer netop $\varphi(p-1)$ frembringere i $(\mathbb{Z}/p\mathbb{Z})^*$. Hvordan kan man da bestemme en frembringer alene ved kendskab til p?

Dette viser sig for store primtal p at være beregningsmæssigt umuligt. Antag, at $g \in (\mathbb{Z}/p\mathbb{Z})^*$ er en formodet frembringer. Dette kan i praksis kun undersøges ved konsekvent at beregne $g^1, g^2, \ldots, g^n$, hvor $g^n = e$. Hvis $n = p-1$ er g da en frembringer.

Det er indlysende, at sådanne beregninger er alt for omfattende i praktiske situationer, og en alternativ metode er derfor påkrævet.

Der gælder følgende sætning

SÆTNING 5.16 ***Beregning af frembringere***
Givet gruppen $(\mathbb{Z}/p\mathbb{Z})^*$, antag at faktoriseringen af $p-1$ er kendt, d.v.s.

$$p - 1 = \prod_{i=1}^{r} q_i^{\alpha_i}.$$

Et element $g \in G$ er da en frembringer, hvis og kun hvis

$$g^{\frac{p-1}{q_i}} \neq e,$$

for alle primfaktorer $q_1, q_2, \ldots, q_r$ i $p-1$.

Bevis:
Antag, at der findes et q_i således at

$$g^{\frac{p-1}{q_i}} = e.$$

Så ville $o(g)$ maksimalt være $\frac{p-1}{q_i} < p-1$, og g er således ikke en frembringer.

Omvendt, antag at $o(g) = h < p-1$ og vælg et i, således at $q_i \mid \frac{p-1}{h}$. Da har vi

$$\begin{aligned} g^{\frac{p-1}{q_i}} &= (g^h)^{\frac{p-1}{q_i h}} \\ &= e^{\frac{p-1}{q_i h}} \\ &= e. \end{aligned}$$

Sætningen er da bevist.

■

Det fremgår af ovenstående, at kendskab til faktoriseringen af $p-1$ er påkrævet for effektiv beregning af frembringere.

Hvis dette er tilfældet kan frembringere beregnes ved en non-deterministisk algoritme, der tilfældigt udtager elementer i $(\mathbb{Z}/p\mathbb{Z})^*$ og undersøger disse v.h.a. resultatet i Sætning 5.16.

Konkret er det naturligvis oplagt at vælge et p, således at $p-1$ har en "nem" faktorisering; dette giver yderligere effektivitet ved beregning af frembringere ved tilfældig udvægelse, idet kun få faktorer skal undersøges.

Antag derfor, at p er på formen $2q+1$, hvor q er et primtal, d.v.s. $p-1=2q$. Givet et tilfældigt element $g \in (\mathbb{Z}/p\mathbb{Z})^*$, hvad er da sandsynligheden for at g er en frembringer, $\Pr[\langle g\rangle = (\mathbb{Z}/p\mathbb{Z})^*]$?

Af Sætning 5.16 fremgår, at alle elementer på formen g^i, $i = 0, 1, 2, \ldots, 2q$, hvor $2 \nmid i$ og $q \nmid i$, er forskellig fra e d.v.s. der må være netop $q-1$ frembringere.

Vi får dermed, at sandsynligheden for, at man udtager en frembringer på l forsøg er

$$\Pr[\langle g\rangle = (\mathbb{Z}/p\mathbb{Z})^*] = 1 - \left(\frac{q+2}{2q+1}\right)^l \approx 1 - 2^{-l}.$$

D.v.s. allerede efter et enkelt forsøg er sandsynligheden for succes $0,5$ — og denne metode er derfor oplagt at anvende.

Et oplagt problem er imidlertid, hvordan man rent faktisk frembringer store primtal på formen $p = 2q+1$, hvor q er et primtal. Vi vil ikke tage videre stilling til den problematik i denne rapport, men blot nævne, at der eksisterer effektive Monte-Carlo metoder [2] til at teste, hvorvidt selv meget store tal er primtal. Dette samt fordelingen af primtal gør det muligt at sample de nødvendige primtal fra en tilfældig stikprøve af heltal i et givet interval. For en grundig behandling af disse metoder, jf. [Crandall and Pomerance, 2001, Afsnit 3.4].

[2] D.v.s. algoritmer, der giver det korrekte resultat med en vis sandsynlighed.

5.3.5 Algoritmer til beregning af diskrete logaritmer

I dette afsnit vil vi undersøge nogle få algoritmer til beregning af diskrete logaritmer og redegøre for, at selv de bedst kendte metoder har eksponentiel kompleksitet m.h.t. inputlængden.

Vi betragter $(\mathbb{Z}/p\mathbb{Z})^*$, hvor p er et primtal (metoderne i afsnittet kan imidlertid generaliseres til enhver cyklisk gruppe).

Lad g være en frembringer, og h være et arbitrært element i gruppen. Vi ønsker da at løse $g^x = h \mod p$.

Den simple metode

Den simple metode er bare at prøve sig frem. Man beregner ganske enkelt $g^0, g^1, g^2, \ldots$ og sammenligner med a indtil den diskrete logaritme findes. I værste tilfælde kræver dette en modulær multiplikation (og sammenligning) for ethvert element i gruppen, d.v.s. hvis $|p| = n$ kræves op mod 2^n gruppeoperationer. Det følger, at denne metode har en kompleksitet (m.h.t. antal operationer) $O(2^n)$ for værste tilfælde,hvilket gør den ubrugelig for tilstrækkeligt store værdier af p (i kryptografisk sammenhænge er bit-længden af p ofte 768 eller derover).

Pollard ρ metoden

Pollard ρ metoden er en såkaldt *Las Vegas metode* til beregning af diskrete logaritmer, d.v.s. den giver altid det korrekte resultat, men beregningstiden kan variere.

Den benytter sig af pseudo non-deterministiske funktioner, der minder om de lineære kongruens metoder, der anvendes i mange pseudo non-deterministiske talgeneratorer, jf. [Rosen, 1999, Kap. 2.2]. Ved anvendelse af denne beregnes u, v, der opfylder

$$g^u = h^v \mod p.$$

Ud fra denne kan den diskrete logaritme af h m.h.t. g beregnes.

Ideen er at beregne en tilfældig række af gruppeelementer $x_1, x_2, \ldots$ indtil det ovenfor beskrevne er opfyldt. Lad $S_1 \cup S_2 \cup S_3$ være en inddeling af $\mathbb{Z}/p\mathbb{Z}$, således at $|S_1| \approx |S_2| \approx |S_3|$. Da er den nævnte række defineret rekursivt som

$$\begin{aligned} x_0 &= 1 \\ x_{i+1} &= \begin{cases} gx_i, & \text{hvis} \quad x \in S_1 \\ x_i^2, & \text{hvis} \quad x \in S_2 \\ hx_i, & \text{hvis} \quad x \in S_3. \end{cases} \end{aligned}$$

Det ses, at elementerne i denne række er på formen $x_i = g^{a_i} h^{b_i} \mod p$.

Værdierne af a_i og b_i er tilsvarende fastlagt rekursivt ved

$$
\begin{aligned}
a_0 &= 0 \\
a_{i+1} &= \begin{cases} a_i, & \text{hvis} \quad x_i \in S_1 \\ 2a_i, & \text{hvis} \quad x_i \in S_2 \\ a_i + 1, & \text{hvis} \quad x_i \in S_3, \end{cases}
\end{aligned}
$$

samt

$$
\begin{aligned}
b_0 &= 0 \\
b_{i+1} &= \begin{cases} b_i + 1, & \text{hvis} \quad x_i \in S_1 \\ 2b_i, & \text{hvis} \quad x_i \in S_2 \\ b_i, & \text{hvis} \quad x_i \in S_3. \end{cases}
\end{aligned}
$$

V.h.a. disse definitioner er rækken $x_1, x_2, \ldots$ tilnærmelsesvist tilfældig (dette er naturligvis ikke helt korrekt i praksis, eftersom den i sidste ende vil være periodisk).

Algoritmen beregner nu tre-tuplerne $\{(x_i, a_i, b_i)\}$, $i = 0, 1, 2, \ldots$ indtil $x_i = x_{2i}$. Dette sætter minimale krav til den nødvendige hukommelse, idet det da blot er nødvendigt at gemme to tretupler per skridt, d.v.s. beregning af (x_i, a_i, b_i) og (x_{2i}, a_{2i}, b_{2i}) — $(x_{i+1}, a_{i+1}, b_{i+1})$ og $(x_{2i+2}, a_{2i+2}, b_{2i+2})$ o.s.v.

Vi har nu

$$g^{a_i} h^{b_i} = g^{a_{2i}} h^{b_{2i}} \Leftrightarrow g^{a_i - a_{2i}} = g^{x(b_{2i} - b_i)},$$

umiddelbart, idet $g^l = g^k \Leftrightarrow g^{l-k} = e$, men dette betyder ifølge Lemma 5.3 at $(p-1)|(l-k)$, d.v.s. $l = k \mod p - 1$.

Vi får således kongruensen

$$a_i - a_{2i} = x(b_{2i} - b_i) \mod p - 1.$$

Hvis $\texttt{sfd}(a_i - a_{2i}, p-1) = 1$ har kongruensen en unik løsning, idet $b_{2i} - b_i$ da er invertibel modulo $p-1$. Dette følger, idet ethvert element i $(\mathbb{Z}/(p-1)\mathbb{Z})^*$ er invertibelt.

Antag, at $\texttt{sfd}(a_i - a_{2i}, p-1) > 1$. Dette er en instans af det generelle problem *at løse en lineær kongruens*, som vi *ikke* vil overveje her. I [Beachy and Blair, 1996, Afsnit 1.3] er der imidlertid en generel beskrivelse af en algoritme. Det gælder, at der kun eksisterer løsninger såfremt $\texttt{sfd}(a_i - a_{2i}, p-1)|(b_{2i} - b_i)$. Man kan risikere at skulle undersøge op til
$\texttt{sfd}(a_i - a_{2i}, p-1)$ mulige løsninger, så hvis denne værdi er stor, er det mere hensigtsmæssigt at fortsætte med at finde ligheder i den tilfældige række $\{x_i\}$.

Betegnelsen ρ kommer af udseendet på den graf, der kan dannes ud fra rækken $x_1, x_2, \ldots$ — denne starter med en "hale" svarende til de begyndende iterationer og ender med en uendelig gentaget løkke med en givet periode, altså formet som det græske bogstav rho.

Lad os kort se på kompleksiteten af Pollard ρ metoden. Metodens tilnærmede non-deterministiske natur gør det kun muligt at give en vurdering af det gennemsnitlige antal

operationer ved én beregning. D.v.s. vi ønsker at vurdere, hvor mange operationer der i gennemsnit skal til, før man finder et $x_i = x_j$, $j > i$. Betegn denne hændelse R. Antag, at rækken $\{x_i\}$ giver rent tilfældige gruppeelementer (dette er naturligvis en idealiserende antagelse). Da gælder *fødselsdagsparadokset* (jf. [Menezes et al., 1996, Afsnit 2.15]) — efter $\sqrt{p}$ elementer er undersøgt, er der 50% chance for hændelsen R. D.v.s. det *gennemsnitlige* antal operationer (kompleksiteten) er $O(\sqrt{p})$ (i værste tilfælde er algoritmen ligeså ineffektiv som den først beskrevne).

Vi vil nu illustrere Pollard ρ metoden til beregning af diskrete logaritmer i $(\mathbb{Z}/1439\mathbb{Z})^*$. Da $p = 2 \cdot 719 + 1$ (hvor 719 er primtal) kan det v.h.a. Sætning 5.16 hurtigt eftervises, at $7 \mod 1439 = 7$ er en frembringer. Vi ønsker da at løse

$$7^x = 666 \mod 1439.$$

Anvendelse af den beskrevne algoritme giver da følgende værdier, idet $(x_0, a_0, b_0) = (1, 0, 0)$. Inddelingen af S_1, S_2 og S_3 er valgt, så $S_1 = \{1, 2, \ldots, 479\}$, $S_2 = \{480, \ldots, 959\}$ og $S_3 = \{960, \ldots, 1438\}$.

i	(x_i, a_i, b_i)	(x_{2i}, a_{2i}, b_{2i})
1	$(972, 0, 2)$	$(1048, 1, 2)$
2	$(1048, 1, 2)$	$(1, 2, 3)$
3	$(141, 2, 2)$	$(972, 2, 5)$
4	$(1, 2, 3)$	$(141, 4, 5)$
5	$(347, 2, 4)$	$(347, 4, 7)$

Tabel 5.2: Beregnede værdier ved anvendelse af ρ-metoden.

Det ses, at vi efter 10 iterationer finder $x_5 = x_{10}$. For beregning af den diskrete logaritme x skal følgende kongruens da løses

$$a_{10} - a_5 = x(b_5 - b_{10}) \mod p - 1 \Leftrightarrow 2 = -3x \mod 1438.$$

Da $\texttt{sfd}(-3, 1438) = 1$ har -3 en invers modulo 1438, og kongruensen har en unik løsning

$$x = 2 \cdot (-3)^{-1} \mod 1438 = 958.$$

D.v.s. $\log_7 347 = 958$, hvilket let verificeres ved efterregning.

Indeks analyse

De bedst kendte algoritmer til beregning af diskrete logaritmer idag, er de såkaldte *indeks analyse algoritmer*. Vi vil ikke beskrive disse algoritmer, men henviser til [Menezes et al., 1996, Afsnit 9.6]. Den mest effektive metode baseret på indeks analyse princippet er *number field sieve* metoden, der pt. er den hurtigste algoritme til beregning af diskrete logaritmer — denne har imidlertid stadig eksponentiel kompleksitet, jf. [Buchmann, 2000, Afsnit 9.6].

Vurdering

Afsnit 5.3.5 giver god evidens for, at eksponentiation af frembringere i $(\mathbb{Z}/p\mathbb{Z})^*$ virkelig er en en-vejsfunktion. Beregning af diskrete logaritmer har med selv de bedste metoder eksponentiel kompleksitet, og såfremt ordenen af den betragtede gruppe er tilstrækkelig stor, er det i praksis umuligt at beregne diskrete logaritmer.

Kompleksiteten af de bedste algoritmer til sådanne beregninger har omtrent samme kompleksitet som de bedste algoritmer til faktorisering af store tal. Dette er de to mest oplagte eksempler på formodede en-vejsfunktioner, der finder hyppig anvendelse i kryptografien.

Kapitel 6

Kryptografiske grundenheder

I dette kapitel vil vi give en beskrivelse af en række mere eller mindre uafhængige, konkrete kryptografiske værktøjer, som i Kapitel 8 vil blive kombineret og danne den endelige protokol. Fælles for disse metoder er, at de supplerer hinanden i opbygningen af et meget stærkt tærskel kryptosystem.

I Afsnit 6.4.2 beskrives desuden en særlig vigtig metode, såkaldte beviser for viden om diskrete logaritmer. Sådanne beviser er essentielle i verificeringsprocessen, og vi vil redegøre for, at specielle protokoller med overvældende stor sandsynlighed sikrer, at vælgeren altid afgiver en korrekt stemme, samt at myndighederne dekrypterer korrekt.

6.1 ElGamal kryptosystemet

Vi vil nu beskrive et public key kryptosystem, *ElGamal kryptosystemet*, der bygger på vanskeligheden ved beregning af diskrete logaritmer. I vores specifikke eksempel vil vi opstille det oprindelige kryptosystem, der er baseret på beregninger i gruppen $\mathbb{Z}/p\mathbb{Z}$. Jf. [Elgamal, 1985]. Det er muligt at opstille kryptosystemet for tilsvarende grupper, hvor beregning af diskrete logaritmer betragtes som vanskeligt.

Netop ElGamal viser sig at have fortræffelige egenskaber til sikring af anonymitet i forbindelse med elektronisk afstemning, idet den

- Er velegnet til tærskelkryptografi, jf. Afsnit 4.1.2 samt det senere Kapitel 7.
- Giver mulighed for at *kombinere krypteringer* og dekryptere kombinationen, således at det ikke er nødvendigt at dekryptere enkeltbeskeder. Vigtigheden af en sådan egenskab i forbindelse med elektronisk afstemning er kort beskrevet i Afsnit 3.2.2 og er bl.a. med til at sikre mulighed for verificering for observatør.

Følgende er en komplet beskrivelse af ElGamal kryptosystemet.

Nøglegenerering Følgende beskriver *nøglegenereringsalgoritmen* $\mathcal{G}$ med 1^k (sikkerhedsfaktoren) som input, jf. Afsnit 4.1

1. Der genereres et stort tilfældigt primtal p, $|p| = k$, og en frembringer g for $(\mathbb{Z}/p\mathbb{Z})^*$.
2. Vælg et tilfældigt tal $s \in \mathbb{Z}$ for $1 \leq a \leq p-2$ og beregn $h = g^s$.
3. Den offenlige nøgle er da (p, g, h) — den private nøgle er s.

Kryptering Ved besiddelse af den offentlige (krypterings)nøgle anvendes da følgende metode (krypteringstransformation) til kryptering af en besked.

1. Lader beskeden blive repræsenteret som et element $m \in (\mathbb{Z}/p\mathbb{Z})^*$.
2. Vælger et tilfældigt tal α, $1 \leq \alpha \leq p-2$.
3. Beregner $x = g^\alpha$ og $y = h^\alpha m$.
4. Kodeteksten er så $c = (x, y) = (g^\alpha, h^\alpha m)$.

Dekryptering Meddelelsesteksten m gendannes ud fra den private nøgle ved anvendelse af *dekrypteringstransformationen* givet ved yx^{-s}.

SÆTNING 6.1 ***Korrekthed***
En meddelelsestekst m gendannes korrekt i ElGamal kryptosystemet.

Bevis:
Dekryptering giver altid den korrekte kodetekst, idet

$$\frac{y}{x^s} = h^\alpha (g^\alpha)^s = \frac{(g^s)^\alpha m}{(g^\alpha)^s} = m.$$

Korrektheden følger, idet vi udelukkende anvender tilladte gruppeoperationer. ■

Fremover vil vi lade h betegne den offenlige nøgle (p, g, h).

Vi har således en krypteringstransformation E_h, der som input tager (p, g, h, m, k) og giver (x, y) som output. Dekrypteringstransformationen D_s tager så (x, y, s) som input og giver os m. Vi vil i Afsnit 9.1.1 redegøre for, at denne metode må formodes sikker, såfremt beregning af diskrete logaritmer er vanskeligt.

Vi vil nu illustrere ElGamal ved et eksempel hvor vi regner de forskellige stadier igennem. Det skal bemærkes at størrelsen på de værdier vi bruger her er *kunstigt* små i forhold til hvad kravet måtte være under brug i en faktisk situation.

EKSEMPEL 6.1 ***Brug af ElGamal***

Nøglegenerering *Vi finder først et primtal p, som vælges på formen $p = 2 \cdot q + 1$, hvor q også er et primtal, i overensstemmelse med Afsnit 5.3.4, $p = 2 \cdot 1019 + 1 = 2039$. Bit-længden er $\log_2 2039 \approx 11$. d.v.s. sikkerhedsparamteren er i dette tilfælde $k = |p| = 11$. Derefter beregnes en frembringer ud fra den i Sætning 5.16 beskrevne metode*

$$2^{\frac{2038}{2}} \mod 2039 = 1 = e.$$

Vi får det neutrale element, og 2 er derfor ikke en frembringer. Vi tester nu 13

$$13^{\frac{2038}{2}} \mod 2039 = 2038 \neq 1, \quad \textit{og} \quad 13^{\frac{2038}{1019}} \mod 2039 = 169 \neq 1.$$

Vi har derfor at $g = 13 \mod 2039 = 13$ er en frembringer for $\mathbb{Z}/2039\mathbb{Z}$.
Dernæst skal vi vælge den private nøgle $s \in \mathbb{Z}$ for $1 \leq s \leq p - 2$.
Vi sætter $s = 312$ og beregner da den offentlige nøgle

$$h = g^s \mod p = 13^3 12 \mod 2039 = 5.$$

Den offenlige nøgle er derfor $h = 5$ og den private $s = 312$.

Kryptering *Beskeden m, som skal sendes bliver repræsenteret ved tallet $m = 1238 \mod 2039 = 1238$, og det tilfældige tal $\alpha \in \mathbb{Z}$ for $1 \leq \alpha \leq p - 2$ vælges $\alpha = 1695$.*
Vi udregner så

$$x = g^\alpha \mod p = 13^{1695} \mod 2039 = 339.$$

Tilsvarende beregnes y

$$y = mh^\alpha \mod p = 1238 \cdot 5^{1695} \mod 2039 = 1981.$$

Den krypterede tekst er så $c = (x, y) = (339, 1981)$.

Dekryptering *Når c er modtaget, beregnes*

$$x^{-s} \mod p = 339^3 12 \mod 2039 = 963.$$

Meddelelsesteksten m kan da umiddelbart gendannes

$$m = yx^s \mod p = 1981 \cdot 963 \mod 2039 = 1238.$$

◆

6.1.1 Egenskaber ved ElGamal

Der er flere interessante egenskaber ved netop ElGamal kryptosystemet. Primært bemærker vi, at der er en *meddelelsesudvidelse* på, generelt, en faktor to — meddelelsesteksten er et element i den oprindelige gruppe $(\mathbb{Z}/p\mathbb{Z})^*$, mens kodteksten er et element

i det kartesiske produkt af denne gruppe med sig selv. Dette gør ElGamal uegnet til kommunikation af større datamængder; men i tilfælde, hvor der kun udveksles mindre mængder information (som netop ved afstemning og valg) er denne egenskab uden betydning.

Ydermere hører ElGamal kryptosystemet til den særlige klasse af kryptosystemer, der er såkaldt non-deterministiske.

Hermed menes, at krypteres den samme meddelelsestekst ved gentagne gange at danne en ny kodetekst, er den dannede kodetekst jævnt fordelt blandt elementerne i $(\mathbb{Z}/p\mathbb{Z})^*$. Dette er et resultat af det tilfældige valg, der foretages under krypteringen. Såfremt ElGamal kryptosystemet anvendes til kryptering af stemmesedler ved elektronisk afstemning giver det desuden den yderligere fordel, at selvom meddelelsesrummet kun består af nogle få elementer (i afstemningen: nogle få muligheder), vil det være umuligt for en udenforstående ved simple sammenlignings- og statistiske metoder at afsløre værdien af en givet stemme. Denne egenskab er derfor ikke blot en tilfældig kuriositet, men derimod afgørende for anvendelsen ved elektronisk afstemning.

6.2 Modificering af ElGamal

I Afsnit 3.2.2 redegjorde vi for, at såfremt det var muligt at kombinere krypteringer af de enkelte stemmer, ville det være et skridt på vejen mod verificeringsmuligheder, under antagelse af, at det er muligt at opstille metoder, der gør det muligt at undersøge, hvorvidt en værdi virkelig er en dekryptering af en sådan kombination. Desuden sikrer dekryptering af en sådan kombination en effektiv måde at foretage dekryptering på i tærskelsystemet, eftersom en metode, der ikke afslører den enkelte vælgers identitet, er påkrævet.

Vi vil i det følgende vise, at med få modifikationer kan ElGamal kryptosystemet forholdsvis let omformes, således at dekrypteringen af "produktet" af krypteringerne giver summen af de krypterede talværdier.

Vi definerer følgende

DEFINITION 6.1 ***Homomorfi***
Lad E_e være en krypteringstransformation. E_e siges at være $(\oplus, \odot)$-homomorf, hvis det gælder, at

$$E_e(x) \odot E_e(y) = E_e(x \oplus y) \quad \forall \ x, y \in \{0,1\}^*.$$

Produkt og sum dækker i denne sammenhæng over abstrakte operationer på meddelelsesrummet — helt præcis forlanges det i den generelle definition, at mængden af kodetekster er en gruppe under kompositionen $\odot$, mens mængden af meddelelsestekster er en gruppe under kompositionen $\oplus$.

For ElGamal kryptosystemet ses umiddelbart, at der er tale om $(\odot, \odot)$-homomorfe egenskaber. Dette fremgår, idet mængden af meddelelsestekster $(\mathbb{Z}/p\mathbb{Z})^*$ er en multiplikativ gruppe. Mængden af kodetekster er det kartesiske produkt $(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/p\mathbb{Z})^*$,

og under komponentvis multiplikation kan det hurtigt eftervises, at dette tilsvarende er en gruppe. Lad $c_1 = (x_1, y_1)$ og $c_2 = (x_2, y_2)$ være to ElGamal kodetekster.

Vi har da

$$c_1 \odot c_2 = (x_1 x_2, y_1 y_2) = (g^{\alpha_1} g^{\alpha_2}, h^{\alpha_1} h^{\alpha_2} m_1 m_2) = (g^{\alpha_1+\alpha_2}, m_1 m_2 h^{\alpha_1+\alpha_2}).$$

ElGamal er derfor $(\odot, \odot)$-homomorf. I forbindelse med elektronisk afstemning er vi imidlertid interesseret i en modifikation, hvor mængden af oprindelige meddelelsestekster er heltal, således at dekrypteringen af et produkt af krypterede summer rent faktisk giver summen af stemmerne og dermed valgresultatet (evt. efter yderligere beregninger). Dette kræver kun en mindre række ændringer.

Lad G være en tilfældig frembringer for $(\mathbb{Z}/p\mathbb{Z})^*$, og lad den *oprindelige meddelelsestekst* m være repræsenteret ved et heltal, $m \in \mathbb{Z}$. Vi danner da den *modificerede meddelelsestekst* givet ved G^m og krypterer den som foreskrevet af metoden, side 6.1.

Lad nu $c_1 = (x_1, y_1)$ og $c_2 = (x_2, y_2)$ være to ElGamal kodetekster for modificerede meddelelsestekster.

Vi har

$$c_1 \odot c_2 = (x_1 x_2, y_1 y_2) = (g^{\alpha_1} g^{\alpha_2}, h^{\alpha_1} h^{\alpha_2} G^{m_1} G^{m_2}) = (g^{\alpha_1+\alpha_2}, G^{m_1+m_2} h^{\alpha_1+\alpha_2}).$$

En dekryptering vil dermed give resultatet $G^{m_1+m_2}$, og summen af de oprindelige kodetekster kan nu beregnes som $m_1 + m_2 = \log_G G^{m_1+m_2}$. Beregningen af diskrete logaritmer er *generelt* et vanskeligt problem, men såfremt de oprindelige meddelesesværdier kun kan antage et på forhånd kendt, begrænset antal værdier, er udregningen triviel. Dette faktum vil vi gøre brug af i Afsnit 8, men tilsvarende påpege, at i særlige situationer bliver denne beregning alt for vanskelig.

I Afsnit 7 vil det blive detaljeret beskrevet, hvorfor og hvordan de homomorfe egenskaber dels giver et effektivt tærskel kryptosystem samt (i kombination med de særlige *beviser for viden*) oplagte verificeringsmuligheder i forbindelse med elektronisk afstemning.

6.3 Deling af hemmeligheder

I foregående afsnit blev der redegjort for ElGamal kryptosystemet og dets nyttige egenskaber i relation til de krav, vi kort antydede i Afsnit 3.2.2.

Vi vil nu opstille en grundlæggende matematisk metode, til deling af hemmeligheder, der kan anvendes til opbygningen af et tidligere omtalt (t, n)-*tærskel kryptosystem*, jf. Afsnit 4.1.2, d.v.s. et kryptosystem, hvor generering af nøgler og dekryptering af meddelelser er distribueret. I dette afsnit beskrives blot den grundlæggende metode — denne tilpasses yderligere til vore behov i Kapitel 7.

En vigtig matematisk byggesten for et sådant tærskelsystem er interpolation af datasæt, d.v.s. problemet at tilpasse en bestemt funktionstype til et på forhånd givet datasæt.

6.3.1 Interpolationsproblemet

Følgende Afsnit er baseret på [von zur Gathen and Gerhard, 1999, Kap. 5]. Vi definerer følgende

DEFINITION 6.2 ***Interpolerende funktion***
Lad $\mathbb{F}$ være et legeme, og lad $D = \{(z_1, f_1), (z_2, f_2), \ldots, (z_n, f_n) \in \mathbb{F} \times \mathbb{F}\}$. En funktion $f : \mathbb{F} \to \mathbb{F}$, der opfylder

$$\begin{aligned} f(z_1) &= f_1 \\ f(z_2) &= f_2 \\ &\vdots \quad \vdots \quad \vdots \\ f(z_n) &= f_n, \end{aligned}$$

kaldes en interpolerende funktion *for datasættet D.*

Interpolerende funktioner kan have mange former — man kan anvende rationelle funktioner, trigonometriske funktioner o.s.v. Et oplagt valg af interpolerende funktioner for et givet datasæt i forbindelse med vilkårlige legemer er imidlertid polynomier, som jf. Appendiks A er defineret over ethvert legeme. Denne funktionstype er også karakteriseret ved, at evaluering og kombination af polynomier beregningsmæssigt er forholdsvis let. Vi kan da betragte interpolationsproblemet som det inverse problem til evaluering af funktionsværdier for et polynomium givet dets koefficienter — her ønsker vi at bestemme koefficienterne givet punkterne.

Det er klart, at mængden af polynomier over et legeme $\mathbb{F}$ af grad højest n er et underrum af mængden af funktioner på et interval I, $\{f : I \subseteq \mathbb{F} \to \mathbb{F}\}$. Dette kan let eftervises ved aksiomerne for et vektorrum, jf. [Lay, 2000, Kap. 4.1]. Vi vil i det følgende kalde denne mængde af polynomier $\mathbb{P}_{n,\mathbb{F}}$ for at understrege, at der er tale om polynomier over legemet $\mathbb{F}$. Interpolationsproblemet er da en instans af det generelle problem, at finde repræsentationen for en bestemt vektor i en på forhånd givet basis.

Det er klart, at man her bør være varsom med valg af basis alt afhængig af i hvilken sammenhæng, metoden skal anvendes. Den oplagte basis er $\{1, z, z^2, \ldots\}$, men af

beregningsmæssige og notationsmæssige årsager viser det sig mere hensigtsmæssigt at anvende en anden basis, den såkaldte *Lagrange basis*.

6.3.2 Lagrange interpolation

Lad $L_i(z)$, $1 \leq i \leq n$ være polynomiet af grad højest $n-1$, således at

$$L_i(z_j) = \delta_{ij} = \begin{cases} 1 & \text{hvis } i = j \\ 0 & \text{hvis } i \neq j \end{cases}.$$

Lad $D = \{(z_1, f_i) \in \mathbb{F} \times \mathbb{F}\}_{i=1}^{n}$ være et datasæt, for vi ønsker at bestemme et interpolerende polynomium.

Det er da klart, at polynomiet

$$P(z) = \sum_{i=1}^{n} f_i L_i(z), \tag{6.1}$$

er et interpolerende polynomium for D. Vi definerer nu følgende.

DEFINITION 6.3 ***Lagrange polynomier***
Lad $z_1, z_2, \ldots, z_n \in \mathbb{F}$. Lagrange polynomierne *defineres som følger*

$$L_i(z) = \prod_{j=1, i \neq j}^{n} \frac{z - z_j}{z_i - z_j}.$$

Lagrangepolynomierne viser sig netop at opfylde Ligning 6.1 — d.v.s. de interpolerer datasættet D. Ydermere gælder det vigtige resultat, at dette faktisk er det eneste interpolerende polynomium af grad højest $n-1$ for dette datasæt.

Der gælder følgende sætning.

SÆTNING 6.2 ***Eksistens og entydighed***
Lad $D = \{(z_1, f_i) \in \mathbb{F} \times \mathbb{F}\}_{i=1}^{n}$ *være et datasæt på* n *forskellige punkter. Da gælder, at der eksisterer netop et interpolerende polynomium* $P(z)$ *for* D *over* $\mathbb{F}$ *af grad højest* $n-1$

$$P(z) = \sum_{i=1}^{n} f_i \left(\prod_{j=1, i \neq j}^{n} \frac{z - z_j}{z_i - z_j} \right).$$

Bevis:
Det er klart, at $P(z)$ er et interpolerende polynomium, idet

$$P(z_i) = \sum_{i=1}^{n} f_i \left(\prod_{j=1, i \neq j}^{n} \frac{z_i - z_j}{z_i - z_j} \right) = f_i,$$

for alle $j = 1, 2, \ldots, n$.

Entydighed bevises som følger. Antag at der eksisterer to polynomier $P(z)$ og $Q(z)$ af grad højest $n-1$, som begge interpolerer D. Så er $R(z) = P(z) - Q(z)$ et polynomium af grad højest $n-1$, som har n rødder, $z_1, z_2, \ldots, z_{n-1}$, idet $P(z_i) = Q(z_i) = 0$. Ifølge Korollar A.2 har et polynomium af grad $n-1$ højest $n-1$ rødder, derfor må $Q(z) = 0$, og entydighed er bevist. ■

Det interpolerende polynomium i en basis af Lagrangepolynomier kaldes *Lagrange-formen* for det interpolerende polynomium.

Vi vil illustrere interpolation med følgende eksempel.

EKSEMPEL 6.2 ***Interpolation***
Lad datasættet $\{(1,1),(2,18),(3,71),(4,178) \in \mathbb{R} \times \mathbb{R}\}$. *Vi konstruerer da fire Lagrange-polynomier*

$$\begin{aligned} L_1(z) &= \left(\frac{z-2}{1-2}\right) \cdot \left(\frac{z-3}{1-3}\right) \cdot \left(\frac{z-4}{1-4}\right), \\ L_2(z) &= \left(\frac{z-1}{2-1}\right) \cdot \left(\frac{z-3}{2-3}\right) \cdot \left(\frac{z-4}{2-4}\right), \\ L_3(z) &= \left(\frac{z-1}{3-1}\right) \cdot \left(\frac{z-2}{3-2}\right) \cdot \left(\frac{z-4}{3-4}\right), \\ L_3(z) &= \left(\frac{z-1}{4-1}\right) \cdot \left(\frac{z-2}{4-2}\right) \cdot \left(\frac{z-3}{4-3}\right). \end{aligned}$$

Polynomiet $P(z)$ er da et interpolerende polynomium for datasættet (mellemregninger udeladt)

$$P(z) = L_1(z) + 18L_2(z) + 71L_3(z) + 178L_4(z) = 3z^3 - 4z + 2.$$

◆

Vi kan notere os følgende interessante fakta for interpolationsproblemet

- Såfremt datasættet indeholder *mindre* end n forskellige punkter, eller datasættet stammer fra et polynomium af grad mindre end $n-1$, vil det interpolerende polynomium have grad mindre end n.
- Hvis datasættet indeholder mere end n forskellige punkter, eksisterer det interpolerende polynomium generelt *ikke*. Dog kan disse punkter stamme fra et polynomium af grad højest $n-1$, og det interpolerende polynomium eksisterer da.

6.3.3 Shamir deling af hemmeligheder

Metoderne præsenteret i dette afsnit er baseret på [Shamir, 1979].

Antag, at vi er givet n autoriteter, og en *hemmelighed* $S \in \mathbb{Z}/p\mathbb{Z}$. V.h.a. polynomiel interpolation kan vi dele denne hemmelighed i n dele med en sikkerhedsfaktor t, således

at minimum $t+1$ skal bidrage med deres andel for at gendanne n, hvorimod t autoriteter intet kan gendanne. Dette kaldes et (t,n)-tærskel system og er et oplagt alternativ til den simple deling af hemmeligheder beskrevet i Afsnit 4.1.2.

Metoden er som følger.

Antag, at $S \in \mathbb{Z}/p\mathbb{Z}$ er en hemmelighed, der skal fordeles blandt n personer som vi benævner *autoriteter*.

En betroet instans, *omdeleren* konstruerer da følgende polynomium over $\mathbb{Z}/p\mathbb{Z}$, hvor det antages, at a_i er tilfældigt valgt.

$$P(z) = S + \sum_{i=1}^{t} a_i z^i.$$

Bemærk, at i ovenstående er $P(0) = S$.

Efterfølgende beregnes de enkelte autoriteter respektive dele af S ved f.eks. følgende

$$\begin{aligned} s_1 &= P(1) \\ s_2 &= P(2) \\ &\vdots \quad \vdots \quad \vdots \\ s_n &= P(n). \end{aligned}$$

Der beregnes altså n funktionsværdier, der fordeles blandt de n autoriteter. Af Sætning 6.2 følger nu, at givet $t+1$ andele af hemmeligheden S, findes der netop et interpolerende polynomium af grad t for et sådant datasæt, d.v.s. det oprindelige polynomium $P(z)$, ud fra hvilket hemmeligheden $S = P(0)$ kan beregnes v.h.a. Lagrange-interpolation

$$S = \sum_i s_i \prod_{i \neq j} \frac{0 - z_j}{z_i - z_j} = \sum_i s_i \prod_{i \neq j} \frac{z_j}{z_j - z_i}.$$

Omvendt, hvis der er givet $m < t$ andele vides *intet* om S, idet det interpolerende polynomium af grad t da ikke er unikt.

Denne metode har bl.a. den store fordel, at den er *dynamisk*, jf. [Shamir, 1979]

- Andele frit kan fjernes og tilføjes ved beregning af nye funktionsværdier for det givne polynomium.
- Andelene kan ændres uden at ændre hemmeligheden S blot ved at konstruere et nyt polynomium $Q(z)$ for hvilket $Q(0) = P(0) = S$.

Imidlertid er det, som vi skal se i Afsnit 7.1.2, et betydeligt sikkerhedsproblem (i det mindste i forbindelse med elektronisk afstemning), at Shamir tærskel systemet antager eksistensen af en enkelt *betroet* instans.

6.4 Beviser for viden

I dette afsnit vil vi undersøge, hvorledes man kan *bevise, at man besidder en viden uden at afsløre indholdet af denne*. Dette er essentielt i elektronisk afstemning — primært i forbindelse med stemmeafgivelsen, eftersom den enkelte vælgers stemme aldrig dekrypteres som følge af anvendelsen af homomorf kryptering. Kun ved at vise, at man har afgivet en korrekt stemme (uden at afsløre denne) kan man sikre entydighed. Vi vil opstille generelle bevismetoder, der sikrer, at observatører frit kan undersøge de enkelte beviser og dermed bekræfte gyldigheden af valget.

Tilsvarende bevismetoder vil også vise sig relevante i tærskel kryptosystemet, som vi tidligere (Afsnit 4.1.2 har omtalt bør være verificérbart.

Vi har valgt *ikke* at give en længere formel beskrivelse af den generelle, teoretiske baggrund, men vil give en kort, mindre præcis beskrivelse af det generelle begreb *bevis for viden* og overføre dette på de relevante konstruktioner. Afsnittet er baseret på [Damgaard, 2002b] og [Damgaard, 2002a] — i disse tekster forefindes en kortfattet, formel beskrivelse af de bagvedliggende begreber.

6.4.1 Kort introduktion

Antag, at vi har givet en situation, hvor en person B (bevisaktøren), påstår, at hun kender løsningen w til et bestemt beregningsmæssigt problem x i en given klasse af problemer L. Hun ønsker at overbevise V (verificeringsaktøren) — der kun kender x — om, at hun rent faktisk kender løsningen. Vi kan da forestille os en proces, hvor Viggo frit kan stille spørgsmål, indtil han "føler sig overbevist" om, at Bente har ret. Dette er et generelt eksempel på et kryptografisk bevis, hvor kun *kendskab* til en given størrelse skal vises.

Kryptografiske beviser kan på ingen måde sidestilles med deciderede matematiske beviser. Der er snarere tale om en mere intuitiv proces, hvor en part skal forsøge at overbevise en anden part om gyldigheden af en påstand gennem en række skridt. Populært sagt, er et bevis i en sådan situation et eller flere argumenter, der virker tilstrækkeligt overbevisende overfor den anden part.

Den skrevne bevisproces opbygges v.h.a. protokoller, der foreskriver, hvorledes de to parter skal agere og hvornår. I det følgende vil vi antage, at der er givet en *bevisaktør* B, som skal overbevise *verificeringsaktøren* V om, at vedkommende kender løsningen w til et beregningsmæssigt problem x.

Et typisk bevis for viden er opbygget omkring tre fundamentale skridt for den enkelte aktør

1. Modtager en besked fra den anden aktør.
2. Foretager et antal private beregninger på baggrund af beskeden.
3. Sender en besked til den anden aktør.

Bevisfører		Verficeringsaktør
(x, w)		x
	$\xrightarrow{a}$	
	$\xleftarrow{e}$	$e \in_R \{0,1\}^t$
	$\xrightarrow{z}$	accept/afslag.

Tabel 6.1: Tre-skridtsprotokol

Tabel 6.1 viser en generel opbygning af denne proces i form af en såkaldt *treskridts-protokol*.

D.v.s. B afsender en besked a, får en *tilfældig* udfordring e (derfor det sænkede R, *random*, i skridt 2) tilbage — ud fra svaret herpå enten accepterer eller afslår V beviset z.

Denne form for beviser kan være vidt forskellige i udformning og egenskaber, alt efter hvilken sammenhæng, de skal anvendes i. I vores situation er vi primært interesserede i beviser for viden, hvor *ingen information* om løsningen w afsløres overfor V. Beviset siges i så fald at være *zero-knowledge*.

6.4.2 Bevis for kendskab til diskrete logaritmer

Vi vil nu beskrive en protokol til bevis for kendskab til diskrete logaritmer.

Antag, at B er i besiddelse af to elementer $h, g \in (\mathbb{Z}/p\mathbb{Z})^*$, hvor g er en frembringer, og hævder at han kender et hemmeligt w, således at $h = g^w$. Det antages, at p, h og g er offentlige.

Denne påstand kan han bevise v.h.a. følgende protokol, der oprindeligt blev præsenteret i [Schnorr, 1991]. Følgende er delvist baseret på denne rapport, men primært på [Damgaard, 2002b].

PROTOKOL 2 (SCHNORR)

1. *B vælger et tilfældigt r, $0 < r \leq p - 1$ og beregner $a = g^r$ som afsendes.*
2. *V sender en tilfældig udfordring e, $0 \leq e \leq 2^t < p - 1$ (hvor t har betydning for sikkerheden, jf. senere).*
3. *B afsender $z = r + ew \mod p - 1$, og V undersøger $g^z \stackrel{?}{=} ah^e$ og accepterer, hvis og kun hvis ligheden er opfyldt.*

Vi vil nu gennemgå protokollens egenskaber én efter én og løbende vurdere betydningen heraf i forbindelse med praktiske situationer.

Fuldstændighed

Protokollen SCHNORR siges at være *fuldstændig*. Det betyder, at hvis B og V følger protokollen, og B virkelig kender den diskrete logaritme, accepterer V altid beviset.

Denne egenskab følger umiddelbart af gyldigheden af beregningerne i protokollen, idet

$$g^z = g^{r+ew} = g^r g^{we} = g^r h^e,$$

hvis og kun hvis $h = g^w$.

Sikkerhed

Antag nu, at B ikke kender den diskrete logaritme, men forsøger at gennemføre protokollen alligevel og således snyde sig til accept fra V. Antag desuden, at han kan besvare to udfordringer korrekt, d.v.s. han kan finde (a, e, z) og (a, e', z'), hvor $e \neq e'$ således at V accepterer begge. D.v.s. han kender z og z', så $g^z = ah^e$ og $g^z = ah^{e'}$ — derfor kender han også (eller i det mindste kan beregne) den diskrete logaritme w, idet

$$w = \frac{z - z'}{e - e'}.$$

Dette resultat gælder, da vi må have $g^z = ah^e$ og $g^{z'} = ah^{e'}$. Ved divison af den første ligning med den anden fås $g^{z-z'} = h^{e-e'} = (g^w)^{e-e'}$. Eftersom vi antager, at $e - e' = 0 \mod p - 1$, har $g^{e-e'}$ en multiplikativ invers, og vi får $h = g^w = g^{(z-z')(e-e')^{-1}}$.

Denne vigtige egenskab betyder, at B *maksimalt kan besvare én udfordring korrekt*, såfremt han ikke kender w — i modsat fald kan han rent faktisk beregne w.

Sandsynligheden for fejl i denne protokol, d.v.s. risikoen for, at B kan gætte sig til et w er blot $\Pr(fejl) = 2^{-t}$ (sandsynligheden for, at et tilfældigt valgt w opfylder en udfordring
$0 \leq e \leq 2^t$).

Hvis $|t| \approx |p|$ er denne sandsynlighed *forsvindende lille* i en kryptografisk sammenhæng, hvor bit-længden af p typisk er 768 bit eller derover [1]. Det betyder også, at blot en udførelse af protokollen (med relativt få operationer for begge parter) vil være tilstrækkeligt i stort set enhver sammenhæng.

Zero-knowledge

Antag, at B kender den diskrete logaritme w. Hvis V er "ærlig", og bit-længden af p er tilstrækkelig stor, får V *ingen* viden om løsningen, d.v.s. den diskrete logaritme. Med ærlig menes her, at V ikke bevidst forsøger — f.eks. gennem en omfattende strategi ved gentagne udførelser af protokollen — at afsløre værdien af den diskrete logaritme.

[1] Bemærk, at i [Schnorr, 1991] anvendes en lignende konstruktion i en undergruppe af $(\mathbb{Z}/p\mathbb{Z})^*$ af primtalsorden q ($|q| \approx 140$) for at imødegå specialiserede metoder til beregning af diskrete logaritmer som bl.a. indeks analyse. Dette sætter begrænsninger på størrelsen af 2^t, men under alle omstændigheder vil $\Pr(fejl)$ være forsvindende lille.

Denne påstand holder under antagelsen af, at det er beregningsmæssigt uoverkommeligt at beregne diskrete logaritmer, jf. Afsnit 5.3.5.

Schnorr-protokollen kan med få modifikationer generaliseres til en lignende protokol, hvor man — tilsvarende i tre skridt — givet to elementer $x, y \in (\mathbb{Z}/p\mathbb{Z})^*$ kan bevise kendskab til et α, $0 < \alpha < p-1$, således at $x = g^\alpha$, og $y = h^\alpha$. Netop denne protokol vil vi gøre intensivt brug af i forbindelse med elektronisk afstemning, hvor den er afgørende i forbindelse med både vælgerens anonymitet og korrektheden af stemmeoptællingen.

Varianten blev oprindeligt præsenteret i [Chaum and Pedersen, 1992].

PROTOKOL 3 (DISKLOG-BEVIS)

1. *B vælger et tilfældigt r, $0 < r < p-1$ og sender $(a, b) = (g^r, h^r)$ til V.*
2. *V vælger en tilfældig udfordring e, $0 \leq e < p-1$ og sender denne til B.*
3. *B sender $z = r + e\alpha \mod p-1$ til V, og V undersøger*

$$g^z \stackrel{?}{=} ax^e \quad \text{og} \quad h^z \stackrel{?}{=} by^e.$$

Hvis og kun hvis ovenstående ligheder holder, godtager V beviset.

Protokol 3, DISKLOG-BEVIS, arver naturligvis de beskrevne egenskaber i SCHNORR-protokollen. At den er zero-knowledge kun overfor ærlige verificeringsaktører skal vise sig tilstrækkelig til vores anvendelse (yderligere argumentation følger i Afsnit 9.1.1).

Bemærk, at ovenstående protokol *ikke* giver samme resultat som gentagen anvendelse af SCHNORR.

Dette skyldes, at DISKLOG-BEVIS kan opfattes som et bevis for ligheden

$$\log_g x = \log_h y.$$

Denne er øjensynligt kvalitativt forskelligt fra et bevis alene for *kendskab* til en diskret logaritme (SCHNORR).

6.4.3 Ikke-interaktive beviser

I den sammenhæng vi ønsker at anvende beviser for viden, er det uhensigtsmæssigt, at Protokol 3 (DISKLOG-BEVIS) kræver *interaktion* fra bevisaktøren V, d.v.s. at V vælger udfordringerne og slutteligt tjekker gyldigheden af beviset for enten at acceptere eller afslå. Dette umuliggør, at observatører uafhængigt kan undersøge bevisets gyldighed, og det universelle verificeringsprincip, som er nødvendigt i forbindelse med en afstemningsprotokol. Det er derfor nødvendigt at omforme protokollen til en *ikke-interaktiv protokol*, hvor udfordringen e f.eks. kan genereres ud fra betroet kilde af tilfældige bits (eksempelvis ved omformning af atmosfærisk støj eller lignende).

Kapitel 7

Fejltolerant tærskel system

I Kapitel 6 præsenterede vi en række metoder, som vi i dette kapitel vil anvende til at opstille et såkaldt fejltolerant verificérbart tærskel kryptosystem baseret på ElGamal. Dette er hjertet i afstemningsprotokollen og består grundlæggende af en række mindre protokoller, der under en række antagelser kan vises at sikre

- Anonymitet,
- Transparens,
- Korrekthed.

7.1 Generel opsætning

Antag, at der er givet n instanser, som vi her blot vil kalde *autoriteter*. Vi vil ydermere antage, at der, som i beskrivelsen i Afsnit 3.2.1, eksisterer et offentligt kommunikationsforum, hvorigennem kommunikation mellem de enkelte instanser foregår. Endelig vil vi antage, at de hver især har mulighed for at signere digitalt.

7.1.1 Generering af delte nøgler i ElGamal

Umiddelbart er det nødvendigt at opstille en metode, hvormed man kan generere nøgler i ElGamal kryptosystemet, således at disse er fordelt blandt de n autoriteter. Vi kan anvende Shamir tærskel systemet direkte til effektiv generering af en delt nøgle, hvis vi antager eksistensen af en *betroet instans*, d.v.s. en instans, der kender den private nøgle.

Proceduren i ElGamal kryptosystemet kan overføres direkte fra den i Afsnit 6.3.3 omtalte metode, Shamir deling af hemmeligheder. Lad T betegne den betroede instans, og lad
$A_1, A_2, \ldots, A_n$ betegne autoriteterne. Vi har følgende *forslag* til en protokol.

PROTOKOL 4 (USIKKER SHAMIR)

1. *T genererer et tilfældigt polynomium $P(z)$ af grad t over $\mathbb{Z}/p\mathbb{Z}$. Der gælder her, at $S = f(0)$ er den hemmelige nøgle. Yderligere offentliggøres den offentlige nøgle, $h = g^s$, hvor g er en frembringer for $(\mathbb{Z}/p\mathbb{Z})^*$.*

2. *De enkelte ubetroede instanser modtager hver deres andel af nøglen,*

$$S_1 = f(1), S_2 = f(2), \ldots, S_n = f(n)$$

i overensstemmelse med Shamir tærskel systemet.

3. *For gendannelse af den private nøgle kræves mindst $t + 1$ andele af nøglen S,*

$$\{z_1, z_2, \ldots, z_t, z_{t+1}\} \subseteq \{1, 2, \ldots, n\},$$

hvorefter enne genskabes ved Lagrange interpolation

$$S = P(0) = \sum_{i=1}^{t+1} s_i \left(\prod_{j=1, i \neq j}^{t+1} \frac{z_j}{z_j - z_i} \right).$$

Ovenstående skitse til en protokol er utilfredsstillende af flere grunde.

- Den betroede instans kender under hele forløbet (eller i det mindste i et mindre tidsrum) den private nøgle og har derfor til ethvert tidspunkt mulighed for at dekryptere en kodetekst.
- Protokollen er ikke offentlig i den forstand, at ovenstående opstilling umuliggør verificering for udenforstående.
- Gendannelse af den private nøgle foregår også centralt, d.v.s. atter mulighed for alvorlige fejl.

Protokol 4 udnytter i denne situation på ingen måde den sikkerhed, som vi ellers kunne håbe ville blive opfyldt af Shamir tærskel systemet — og lever slet ikke op til de krav, der er til en sådan protokol i forbindelse med elektronisk afstemning.

Der eksisterer imidlertid alternative løsninger, der bygger på samme metode, men er uden de ovennævnte sikkerhedshuller. Disse protokoller kaldes *distribueret nøglegenerering*.

7.1.2 Distribueret nøglegenerering

Ud fra den korte redegørelse for usikkerheden ved Protokol 4 forlanger vi, at den distribuerede nøglegenereringsprotokol (DNP) som minimum opfylder følgende krav

- Ingen enkeltstående autoritet skal kende den private nøgle.
- Udførelsen af protokollen skal kunne verificeres af udenforstående observatører.

Første krav er indlysende — opstilling af et tærskel system i denne sammenhæng bygger jo netop på den antagelse, at ingen autoriteter kan betros alene, men derimod kun tilpas store delmængder af alle autoriteter. Andet krav er blot et af de krav, vi tidligere opstillede for elektronisk afstemning — hele processen skal være *transparent for observatører*. Dette krav betyder bl.a. også, at enhver autoritet skal bindes til vedkommendes nøgleandel under udførelse af DNP.

Generelt for en optimal distribueret nøglegenereringsprotokol for n autoriteter ved anvendelse af ElGamal kryptosystemet gælder, jf. [Gennaro et al., 1999], at følgende skal være opfyldt

Korrekthed:

- Der findes en effektiv metode til beregning af den private nøgle S, der ved input af nøgleandele og tidligere offentliggjorte værdier giver den unikke private nøgle, selv hvis op til $n - t$ autoriteter er korrupte for en givet sikkerhedsfaktor t (fejltolerans og effektivitet).
- Alle ærlige autoriteter har den samme værdi af den offentlige nøgle $h = g^s$.
- Den private nøgle har en jævn fordeling iblandt værdierne $1, 2, \ldots, p - 1$.

Sikkerhed:

- En udenforstående kan ikke opnå nogen viden om den private nøgle S, udover kendskabet til den private nøgle h.

Første krav under korrekthed skal forstås således, at der findes effektive og fejltolerante metoder til dekryptering, der evt. anvender yderligere værdier genereret i forbindelse med DNP for at opnå dette.

Vi har valgt at beskrive en ældre protokol, Feldman-Pedersen-protokollen kort beskrevet i [Gennaro et al., 1999] [1], og argumentere for, at den *i praksis* lever op til ovenstående krav. Det er imidlertid blevet påpeget, at denne protokol ikke er tilstrækkelig sikker overfor visse typer angreb. I [Gennaro et al., 1999] foreslås en modificeret udgave, der fjerner disse problemer. Den bygger imidlertid på nogenlunde de samme principper, og af overskuelighedshensyn har vi derfor valgt at betragte den oprindelige protokol, der er betydeligt simplere.

Vores mål med protokollen er at imitere metoden i Shamir tærskel systemet, blot således, at det genererede polynomium af grad t genereres *distribueret*.

I det følgende, lad g være en frembringer for $\mathbb{Z}/p\mathbb{Z}$. Antag desuden, at *privat kommunikation* kan implementeres ved kryptering, samt at de enkelte autoriteter ved indbyrdes kommunikation identificerer sig med digital signatur.

PROTOKOL 5 (DNP)

1. *Enhver autoritet A_i vælger et tilfældigt polynomium $f_i(t)$ over $\mathbb{Z}/p\mathbb{Z}$,*

$$f_i(z) = \sum_{l=0}^{t} a_{il} z^l.$$

[1] jf. også den oprindelige rapport, [Pedersen, 1992, Afsnit 3.6]

A_i offentliggører da værdierne $g^{a_{il}}$, $l = 0, 1, \ldots, t$, og værdien $f_i(j)$ sendes privat til autoriteten A_j, $j = 1, 2, \ldots, i-1, i+1, \ldots, n$.

2. *Lad u_i betegne den værdi, A_j modtager fra A_i. Da undersøges korrektheden af denne del, d.v.s. om den stammer fra A_i's oprindelige polynomium, $u_i \stackrel{?}{=} f_i(j)$. Dette er ækvivalent med $g^{u_i} \stackrel{?}{=} g^{f_i(j)}$, hvilket kan undersøges ud fra de af A_i offentliggjorte værdier*

$$g^{u_i} \stackrel{?}{=} g^{f_i(j)} = g^{\sum_{l=0}^{t} a_{il} j^l} = \prod_{l=0}^{t} (g^{a_{il}})^{j^l} .$$

Hvis $g^{u_i} = g^{f_i(j)}$, fortsætter protokollen. Hvis ikke, klager *A_j over A_i, og A_i skal offentliggøre $f_i(j)$. Såfremt værdien virkelig er korrekt fortsætter protokollen, i modsat fald er A_i diskvalificeret og udgår efter denne runde.*

3. *Lad Ω betegne mængden af kvalificerede autoriteter.*
   A_j beregner nu

$$S_j = \sum_{i \in \Omega} f_i(j) = \sum_{i \in \Omega} a_{i0}.$$

Desuden beregnes og offentliggøres h_j givet ved

$$h_j = \prod_{i \in \Omega} g^{f_i(j)} = g^{\sum_{i \in \Omega} f_i(j)} = g^{S_j}.$$

Denne kan tilsvarende beregnes ud fra de tidligere offentliggjorte værdier.

Lad $P(t) = \sum_{i \in \Omega} f_i(t)$. Vi har nu følgende offentlige nøgle h

$$h = g^{P(0)} = \prod_{i \in \Omega} g^{f_i(0)}.$$

Denne kan beregnes ud fra de offentliggjorte værdier af alle interesserede instanser.

Ydermere kender enhver A_j $P(j)$, idet $P(j) = \sum_{i \in \Omega} f_i(j)$, d.v.s. v.h.a. Lagrange interpolation kan vi genskabe den oprindelige nøgle, såfremt $|\Omega| > t$.

Vi har nu opstillet en protokol for *verficérbar, distribueret nøglegenerering*.

Betydningen af den offentlige værdi h_j for hver A_j vil fremgå af Protokol 6, men er nødvendig for at binde den enkelte autoritet til vedkommendes nøgleandel under dekryptering (d.v.s. der er tale om en værdi, der som tidligere omtalt skal sikre en optimal, fejltolerant dekrypteringsproces).

Ovenstående skitse til en distribueret nøglegenereringsprotokol opfylder de tidligere opstillede krav.

Ingen enkeltstående autoritet kender på noget tidspunkt den private nøgle, og enhver observatør kan undersøge, at processen forløber korrekt under antagelse af, at maksimalt t autoriteter er korrupte, d.v.s. forsøger at ødelægge protokollen.

Yderligere er de to sidste punkter under korrekthed af distribueret nøglegenerering opfyldt, mens sikkerhed også er indlysende, idet den private nøgle på intet tidspunkt eksisterer "frit".

Et mindre forbehold; m.h.t. sidste punkt under korrekthed kan man i særlige tilfælde støde ind i problemer. Dette diskuteres nærmere i Afsnit 9.1.1, hvor vi desuden argumenterede for, at protokollen i de fleste tilfælde kan betragtes som tilstrækkelig sikker; men *ikke* optimalt.

7.1.3 Dekryptering

Distribueret dekryptering (DD) af en ElGamal kodetekst, hvor de nødvendige nøgler er genereret ved brug af Feldmann-Pedersen protokollen eller en analog variant heraf er forholdsvis simpelt.

Antag, at vi er givet en kodetekst $(x, y) = (g^\alpha, h^\alpha m)$. Da udføres følgende protokol

PROTOKOL 6 (DD)

1. *Hver autoritet offentliggører værdien $w_j = x^{S_j}$, og det bevises endvidere, at der anvendes den korrekte nøgleandel S_j. Dette gøres ud fra den fra Feldmann-Pedersen protokollen offentliggjorte værdi $h_j = g^{S_j}$, idet følgende bevises i zero-knowledge*

$$\log_g h_j = \log_x w_j. \tag{7.1}$$

Dette gøres v.h.a. en ikke-interaktiv udgave af DISKLOG-BEVIS*, Protokol 3. Bemærk, at et bevis herfor er et bevis for, at den korrekte nøgleandel anvendes, idet*

$$\log_g h_j = \log_x w_j \Leftrightarrow h_j = g^{S_j} \wedge w_j = x^{S_j}.$$

2. *Lad Ω betegne mængden af autoriteter, der har givet et korrekt bevis for Ligning 7.1. Meddelelsesteksten m kan da gendannes v.h.a. Lagrange interpolation. Givet, at $S = P(0)$ for det konstruerede polynomium $P(z)$ i Feldmann-Pedersen protokollen, haves*

$$S = P(0) = \sum_{j \in \Omega} S_j \lambda_j,$$

hvor vi har

$$\lambda_j = L_j(0) = \prod_{k \in \Omega \setminus \{j\}} \frac{0-k}{j-k} = \prod_{k \in \Omega \setminus \{j\}} \frac{k}{k-j}.$$

Det følger, at

$$x^S = \prod_{j \in \Omega} w_j^{\lambda_j}.$$

Meddelelsesteksten m kan nu gendannes som

$$m = \frac{h^\alpha m}{(h^\alpha)} = \frac{h^\alpha m}{(g^\alpha)^S} = \frac{h^\alpha m}{x^S} = \frac{y}{\prod_{j \in \Omega} w_j^{\lambda_j}} = \frac{y}{x^s}.$$

Skridt 1 sikrer, at korrupte autoriteter ikke anvender ukorrekte nøgleandele under dekrypteringen og dermed saboterer resultatet. Uden beviset ville ukorrekte nøgleandele uden videre kunne anvendes — men ved dekryptering vil man da *ikke* finde den oprindelige meddelelsestekst.

Dekrypteringen er dermed også verificérbar.

Skridt 2 følger direkte som konsekvens af Lagrange interpolation, hvor det naturligvis atter tolereres, at op til t autoriteter er korrupte eller fejlagtige.

Kapitel 8

Trin-for-trin oversigt

Vi vil nu give en trin-for-trin oversigt over den samlede afstemningsprotokol — alle de nødvendige begreber er allerede nævnt, men den følgende redegørelse viser, hvordan disse kan samles til en helhed, der giver en meget sikker afstemningsprotokol.

Vi vil i den overordnede gennemgang antage, at der alene er tale om et ja/nej-valg. Der er således *ikke* mulighed for f.eks. blanke stemmer (som det jo kræves under danske afstemninger og valg), men dette krav diskuteres yderligere i Afsnit 8.2.

Vi vil antage, at vi har m vælgere, $V_1, V_2, \ldots, V_m$ og n optællingsservere, *valgautoriteter*, $A_1, A_2, \ldots, A_n$. De øvrige konkrete forhold er ligeledes beskrevet i Afsnit 3.2.1, heriblandt antagelsen om eksistensen af et offentligt kommunikationsforum. Som påpeget i Afsnit 3.2.1 skal et sådant system opfylde en lang række sikkerhedskrav, som vi *ikke* vil overveje her. Yderligere antages eksistensen af unik identifikation i forbindelse med skrivning af beskeder på kommunikationsforumet.

8.1 Afstemningsprotokol

Initialisering En delmængde af myndighederne genererer ud fra den valgte sikkerhedsfaktor for ElGamal kryptosystemet, 1^k, $(\mathbb{Z}/p\mathbb{Z})^*$, $|p| = k$ og sampler to (forskellige) tilfældige frembringere g og G. Da dette er den grundlæggende offentlige information, er det afgørende, at valgautoriteterne er enige om disse værdier. En mulig metode beskrives i [Pedersen, 1992, Afsnit 4.3].

Nøglegenerering Myndighederne udfører DNP, Protokol 5, og genererer herved en offentlig nøgle h og en delt privat nøgle.

Nøglen h offentliggøres på kommunikationsforumet og også en logfil for udførelse af nøglegeneringsprotokollen offentliggøres. Dette gør det muligt for observatører at verificere, at nøglegenereringen er foregået korrekt.

Stemmeafgivelse Vælgeren V_i krypterer sin stemme $G^{-1} = v_{\text{nej}} \vee G = v_{\text{ja}}$ i overensstemmelse med metoden for ElGamal kryptosystemet beskrevet i Afsnit 6.2.

D.v.s. V_i vælger et tilfældigt α, $0 \leq \alpha \leq p-1$ og konstruerer kodeteksten

$$(x_i, y_i) = (g^\alpha, h^\alpha G^b) = (g^\alpha, h^\alpha v_i).$$

Ydermere konstrueres v.h.a DISKLOG-BEVIS, Protokol 3, et ikke-interaktivt bevis for følgende

$$\log_g x = \log_h(y/G^{-1}) \quad \vee \quad \log_g x = \log_h(y/G).$$

Det ses, at dette virkelig er et bevis for, at den afgivne stemme er korrekt.

Vi har, at for første lighed

$$\log_g x = \log_h(y/G^{-1}) \Leftrightarrow \alpha = \log_h\left(\frac{h^\alpha G^{-1}}{G^{-1}}\right) = \alpha.$$

Tilsvarende kan vises for anden lighed. Bemærk, at netop én af disse uligheder kan bevises for en given stemme, samt at beviset er zero-knowledge og intet afsløres om den afgivne stemme.

Kald dette bevis for $\mathbf{proof}_i$. V_i afsender da $((x_i, y_i), \mathbf{proof}_i)$ til kommunikationsforumet (ved anvendelse af den antagede digitale signatur, $\mathrm{signatur}_i$) [1]).

Validitetsundersøgelse Når stemmefristen udløber, undersøges $\mathbf{proof}_i$ for alle V_i, og ukorrekte stemmeafgivelser sorteres fra.

Lad $\Lambda \subseteq \mathcal{V}$ betegne mængden af korrekte stemmer. Da beregnes

$$(X, Y) = \left(\prod_{V_i \in \Lambda} x_i, \prod_{V_i \in \Lambda} y_i\right).$$

Optælling De homomorfe egenskaber ved ElGamal kryptosystemet (jf. Afsnit 6.2) kan nu anvendes, idet $E_h(a)E_h(b) = E_h(a+b)$.

Valggautoriterne dekrypterer således (X, Y) v.h.a. DD, Protokol 6 (hvor DISKLOG-BEVIS indgår som underprotokol). Herved fås værdien

$$W = \sum_{v_i \in \Lambda} v_i = \frac{Y}{X^s} = G^T.$$

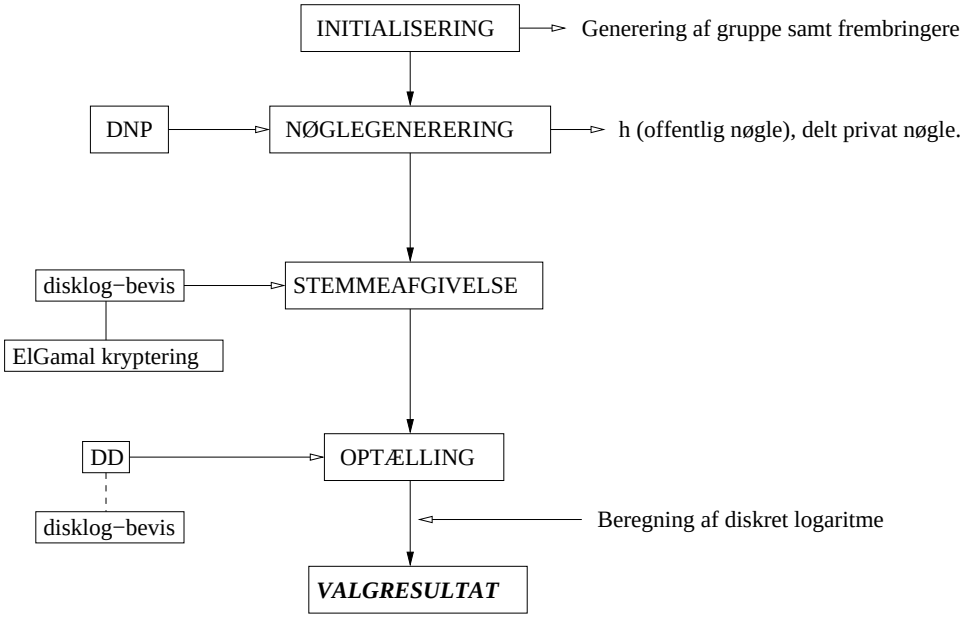
Ud fra de forudberegnede værdier eller med passende algoritmer beregner valgautoriteterne nu $\log_G G^T = T$, og valgresulatet er da givet som differensen mellem ja- og nej-stemmer, og stemmer i de enkelte kategorier er da trivielt at beregne.

Vi kan i ovenstående hurtigt gøre os klart, at såfremt protokollen udføres korrekt, tæller den enkelte vælgers (korrekte) stemme altid i det endelige resultat. Figur 8.1 viser et grafisk overblik over de enkelte underprotokoller.

I Kapitel 9 vil vi vurdere protokollen, hovedsageligt ud fra de tidligere opstillede kriterier. I tilknytning hertil vil vi gennemgå de enkelte metoder/algoritmer og underprotokoller og forsøge at vurdere sikkerheden heraf.

Særligt vil vi fokusere på

[1] Der vurderes på kravet om digital signatur i Kapitel 9.



Figur 8.1: Overblik over de enkelte underprotokoller involveret.

- Sikkerheden af ElGamal kryptosystemet.
- Sikkerheden af Protokol 5, DNP — kan den forbedres?
- Mulige tiltag i forbindelse med Protokol 3, DISKLOG-BEVIS.

Endelig vil vi kort vurdere henholdsvis beregnings- og kommunikationskompleksiteten for de involverede parter.

Desuden vil vi vise, at den i ovenstående form ikke er optimal i alle henseender sammenlignet med en traditionel afstemning; samt at stor varsomhed er nødvendig, hvis protokollen skal implementeres i en virkelig situation.

Inden da vil vi kort argumentere for, hvordan protokollen kan modificeres, således at den kan anvendes til en typisk dansk afstemning

8.2 Generalisering af protokol

Indtil videre har vi blot set på det simple tilfælde, hvor valget står mellem to muligheder, f.eks. ja og nej. Dette kan synes tilstrækkeligt for f.eks. ja/nej folkeafstemninger, men indebærer det alvorlige problem, at det ikke er muligt at afgive blanke stemmer under sådanne omstændigheder.

Dette må vi imidlertid kræve er muligt for anvendelse under danske valg og afstemninger. Det viser sig imidlertid, at der er en oplagt løsning på problemet, der samtidig kan udvides til mindre, mere komplekse valgsituationer som f.eks. folketingsvalg (hvor muligheden for et stort antal valgmuligheder er påkrævet).

Metoden hertil er imidlertid, på baggrund af Afsnit 8.1, forholdsvis simpel. Såfremt man ønsker k valgmuligheder, genereres blot, uafhængigt, k frembringere $G_1, G_2, \ldots, G_k$ for $(\mathbb{Z}/p\mathbb{Z})^*$, og en krypteret stemme v_i er da blot ElGamal krypteringen af en given frembringer. Beviset for viden følger samme princip, blot her skal én ud af k ligheder bevises i zero-knowledge.

Dette løser bl.a. spørgsmålet angående blanke stemmer i binære valg, idet vi for denne situation kan generere tre frembringere.

Selve dekrypteringsspørgsmålet er kort beskrevet i Afsnit 9.2.4, men det viser sig, at arbejdet med dekryptering stiger dramatisk ved et øget antal valgmuligheder.

Situationer som f.eks. under "tripel-valget" i efteråret 2001, hvor der blev stemt til både folketings, kommunal- og amtsrådsvalg vil kunne håndteres med et antal parallelle implementationer af vores system.

Kapitel 9

Vurdering af protokollen

I dette kapitel vil vi give vurderinger af den opstillede protokol i henhold til de oprindelige kravsspecifikationer, jf. Afsnit 2.3.

I denne forbindelse vil vi særligt fokusere på de to afgørende parametre

- Sikkerhed.
- Bekvemmelighed.

Afsluttende følger en vurdering af opfyldelse af de øvrige krav, samt en kritisk stillingtagen til elektronisk afstemning som mulighed generelt.

9.1 Opfyldelse af kravsspecifikationer

Vi kan umiddelbart gøre rede for, at den opstillede afstemningsprotokol opfylder størstedelen af de krav, vi allerede i Afsnit 2.3 opstillede til en afstemningsprotokol.

Berettigelse Det er kun muligt for stemmeberettigede at stemme, idet vi antager eksistensen af *unikke digitale signaturer* (kort omtalt i Afsnit 2.2), der giver tilstrækkelig sikkerhed.

De politiske forudsætninger for digitale signaturer omtales i Afsnit 10.2.1 — det er dog vigtigt at forstå, at dette virkelig er en af de *absolutte grundenheder*, såfremt protokollen skal fungere korrekt. Sikkerheden i selve kernen af protokollen er, groft sagt, uden betydning, hvis der ikke kan opnås en tilstrækkelig sikker løsning for disse signaturer.

Entydighed Det vil ikke være muligt for en givet vælger at stemme mere end én gang. Dette skyldes zero-knowledge beviset under stemmeafgivelsen, der sikrer, at accepterede stemmer *altid* har den korrekte form.

Yderligere vil det i praksis naturligvis være muligt at afgive stemme, bevis og signatur indtil flere gange, men idet kun et zero-knowledge bevis for korrekthed af stemme godtages, vil der blive taget højde for dette under verificeringsproceduren, f.eks. kunne man indføre, at kun den sidste stemme talte.

Korrekthed Stemmerne optælles korrekt — dette følger af de homomorfe egenskaber for ElGamal kryptosystemet samt dekrypteringsprotokollen, hvor valgautoriterne skal kunne bevise, at den korrekte nøgleandel anvendes.

Verificeringsmulighed Det er muligt for enhver observatør at undersøge, hvorvidt valget er foregået korrekt, idet alle de zero-knowledge beviser genereret gennem udførelse af diverse underprotokoller er offentligt tilgængelige og kan verificeres. Konkret kan observatøren tjekke

- Hvorvidt de afgivne stemmer er korrekte eller ej (zero-knowledge bevis for korrekthed af kryptering).
- Om valgautoriteterne netop dekrypterer produktet af alle korrekte, krypterede stemmer.
- Korrekthed af dekryptering (zero-knowledge bevis for korrekthed af kryptering).

Anonymitet Under antagelse af, at maksimalt t myndigheder er korrupte, kan *ingen* udenforstående dekryptere de enkelte stemmer. Under korrekt udførelse af protokollen dekrypteres derimod kun summen af stemmerne, og anonymitet er bevaret under antagelse af, at ElGamal kryptosystemet i praksis er ubrydeligt, samt at det er beregningsmæssigt umuligt at udregne diskrete logaritmer (bevis for korrekthed af stemme).

I systemet eksisterer en indbygget fejltolerans i det anvendte tærskelsystem, men det er tilsvarende nødvendigt at sikre fejltoleransen for det vigtige kommunikationsforum. I [Cramer et al., 1997] foreslås dette udført med et tærskelsystem af servere, hvor systemet er oppe, blot et vist antal af serverne fungerer. Denne foranstaltning vil forhindre såkaldte *denial-of-service* angreb, d.v.s. angreb, med det formål at forhindre vælgerne i at stemme. Opstillingen af et sådant effektivt og sikkert serversystem er afgørende, hvis afstemningsprotokollen skal være anvendelig i praksis.

Kvitteringsproblemet

Et alvorligt problem i den opstillede protokol, der dels har relation til det, der må betegnes som "generelle krav for afstemninger" og dels til det mere tekniske sikkerhedsspørgsmål er *kvitteringer for stemmer*. Dette vil sige, at vælgeren efter endt afstemning kan bevise, hvad vedkommende har stemt.

Det fremgår, at den opstillede protokol *ikke* er sikret mod den slags problemer. En udenforstående U vil kunne benytte sig af de non-deterministiske (vælgerafhængige) aspekter af ElGamal kryptosystemet til at true en vælger V_i til at afgive en bestemt stemme, $v \in \{G, G^{-1}\}$. U kan forlange, at V_i anvender et på forhånd kendt α og herudfra danner kodeteksten $v_i = (x, y) = (g^\alpha, h^\alpha v_i)$. Da den krypterede stemme er offentlig kan U uden problemer undersøge, hvorvidt V_i har stemt som forlangt.

Problemet påpeges i [Cramer et al., 1997], og det omtales, at det vil kunne løses med et modificeret kryptosystem, der opfylder

- Er homomorf.
- Er velegnet til tærskel kryptografi.
- Er *benægteligt* (deniable). Hermed menes, at afsenderen kan generere "falske" tilfældige valg under krypteringen, således at kodeteksten ligner en kodetekst for en anden meddelelsestekst.

Der redegøres i [Canetti et al., 1997] for, at sådanne kryptosystemer er teoretisk mulige, men der præsenteres ingen eksempler på sådanne. Under vores arbejde er vi imidlertid ikke stødt på protokolkonstruktioner, der anvender denne krypteringsmetode.

9.1.1 Sikkerhed af protokol

Vi har nu redegjort for opfyldelse af en række af de oprindelige kravsspecifikationer ud fra den antagelse, at de anvendte metoder i protokollen virkelig er så sikre, som de er forsøgt konstrueret til at være.

Vi vil nu vise, at dette i praksis er tilfældet — herunder vil vi forsøge at tage stilling til, hvorvidt protokollen virkelig forbedrer de eksisterende, traditionelle afstemningsmetoder. Særligt vil vi fremhæve de svage led og i nogen grad forsøge at udpege metoder, der kan afhjælpe eventuelle problemer.

Sikkerheden af ElGamal

Det fremgik af Afsnit 6.1, at kryptering i ElGamal kryptosystemet er baseret på eksponentiation af frembringere, og problemet at bryde ElGamal kryptosystemet er derfor relateret til beregning af diskrete logaritmer. Vi redegjorde i Afsnit 5.3.5 for, at selv de bedste algoritmer til beregning af diskrete logaritmer i gruppen $(\mathbb{Z}/p\mathbb{Z})^*$ har eksponentiel kompleksitet; derfor vil vi anse ElGamal for ubrydelig i praksis såfremt bitlængden af p er tilstrækkelig stor. Kryptografisk standard er i dag 768 bit eller mere.[1].

Bemærk dog, at ElGamal ikke vides at være *ækvivalent* med beregning af diskrete logaritmer, derfor er ovenstående kun en *vejledende* vurdering.

Sikkerheden af ElGamal formodes at være bedst, såfremt man vælger p, således at $p-1$ har få primfaktorer (som f.eks. $p = 2q + 1$). Dette vanskeliggør anvendelsen af visse algoritmer, der kan udnytte eventuelle mange små primfaktorer i $p - 1$. Blandt disse algoritmer er indeks analyse (jf. Afsnit 5.3.5) samt en anden algoritme, *Pohlig-Hellman metoden*, jf. [Buchmann, 2000, Afsnit 9.5].

Sikkerhed af nøglegenerering

Vi gjorde i Afsnit 7.1.2 opmærksom på, at den opstillede nøglegenereringsprotokol ikke var gennemført sikker. Dette påpeges bl.a. i [Gennaro et al., 1999], og i dette afsnit

[1] I DSA (Digital Signature Algorithm), den amerikanske standard for digital signatur baseret på ElGamal, anbefales f.eks. en bit-længde af p for gruppen $(\mathbb{Z}/p\mathbb{Z})^*$ på mellem 524 og 1024 bits, jf. `http://www.itl.nist.gov/fipspubs/fip186.htm`

vil vi kort redegøre for disse resultater og vurdere risikoen i relation til elektronisk afstemning.

I [Gennaro et al., 1999, Afsnit 3.2] redegøres det, at en udenforstående kan påvirke protokollen, således at ikke alle sikkerhedskrav i definitionen på et distribueret nøglegenereringssystem er opfyldt, jf. side 63. Specifikt, under visse omstændigheder kan en udenforstående påvirke fordelingen af mulige nøgler, således at fordelingen ikke er jævn.

Følgende eksempel beskrives i [Gennaro et al., 1999].

Antag, at der findes to korrupte autoriteter A_1 og A_2, der samarbejder om at ændre fordelingen af nøgler, så sandsynligheden, for at sidste bit i den offentlige nøgle er 1, er større end $\frac{1}{2}$.

I 1. fase afsender A_1 korrekte signerede andele u_i til alle deltagere $A_3, A_4, \ldots, A_n$ samt både en korrekt og en ukorrekt signeret andel til A_2. Dernæst beregner A_1 følgende

$$a = \prod_{i=1}^{n} y_i \quad \text{og} \quad b = \prod_{i=2}^{n} y_i.$$

Sandsynligheden for, at hhv. a og b ender med 1 er $\frac{1}{2}$. Hvis bit-strengen a ender med et 1 fortsætter protokollen, idet A_2 anvender den korrekte andel, og protokollen fortsætter som foreskrevet. I modsat fald får han A_2 til at indgive en klage mod ham, således at A_1 diskvalificerer sig, og værdien b anvendes i det videre forløb af protokollen. Sandsynligheden for hændelsen E, at den offentlige nøgle da har sidste bit 1, bliver da

$$P(E) = 1 - \left(\frac{1}{2}\right)^2 = \frac{3}{4}.$$

Dette giver en skæv fordeling af både offentlige og private nøgler på mængden af mulige nøgler, og dette er endda på trods af eksistensen af tærskel tilliden i nøglegenereringsfasen.

Eksistensen af dette problem er et faktum, men relevansen kan naturligvis diskuteres. I forbindelse med elektronisk afstemning vil bit-længden af nøglen formentlig være 768 bit eller højere. Derfor kan ovenstående angreb næppe forventes at kompromittere sikkerheden i nogen betydelig grad, men er snarere en konstatering af, at protokollen ikke lever op til de teoretisk fastsatte krav for denne type protokol.

Dette ændrer imidlertid ikke på, at protokollen *kan* forbedres, og at det naturligvis bør overvejes i forbindelse med et så krævende system, rent sikkerhedsmæssigt, som elektronisk afstemning — også i relation til vælgerskarens tillid til systemet. Vi vurderer dog, at dette sikkerhedshul er af mindre betydning sammenlignet med f.eks. problematikken angående digitale signaturer.

Vurdering af DISKLOG-BEVIS

Vi opstillede Protokol 3 for disklog-bevis i Afsnit 6.4 netop ud fra sikkerhedskravene. Vi redegjorde for, at overfor den *ærlige verificeringsaktør* var beviset zero-knowledge. Hvorfor har vi ikke konstrueret en protokol, der var regulær zero-knowledge?

Dette har flere årsager, den primære er kompleksiteten af sådanne protokoller. I [Cramer et al., 1997] nævnes et alternativ, som er zero-knowledge generelt, men uhensigtsmæssig i den forstand, at kompleksiteten af protokollerne øges betydeligt. For netop vælgeren er dette ikke ønskeligt.

Yderligere er der gode argumenter for, at en protokol kan betragtes som tilstrækkelig i forbindelse med afstemningsprotokollen — som beskrevet i Afsnit 6.4.3, skal beviset modificeres til et ikke-interaktivt bevis v.h.a. eksempelvis en betroet kilde af tilfældige bits. Under antagelse af, at denne løsning er sikker, kan vi argumentere, at der i bevissituationen virkelig er tale om en ærlig verificeringsaktør.

9.1.2 En samlet sikkerhedsvurdering

Det fremgår af ovenstående gennemgang, at de involverede underprotokoller må formodes tilstrækkeligt sikre til praktisk anvendelse i forbindelse med elektronisk afstemning. Ydermere har vi redegjort for, at ElGamal må formodes sikkert.

Er dette en acceptabel begrundelse for, at protokollen kan betragtes som sikker? I en teoretisk sammenhæng må dette antages at være et tilstrækkeligt grundlag — ud fra de opstillede sikkerhedskrav og antagelser har vi argumenteret, at vores løsning virkelig er meget sikker. Men dette er ikke nødvendigvis ensbetydende med ubetinget sikkerhed såfremt metoderne skulle implementeres i praksis.

En gennemgribende analyse af sikkerheden i en kryptografisk protokol er betydeligt vanskeligere end analyse af f.eks. sikkerheden ved et kryptosystem. Grundformen kan måske synes sikker, men når denne optræder i en konkret sammenhæng, hvor vi har en praktisk implementation af f.eks. kommunikationsforum og kommunikation er påkrævet, er situationen en helt anden.

Vi har valgt kun at redegøre for grundprincipperne og sikkerheden af disse, primært sikkerheden af underprotokoller. Denne analyse viser, at følgende bør være det primære i fokus i en mere dybdegående sikkerhedsanalyse

- Implementation af kommunikationsforum.
- Anvendelse af digital signatur.

9.2 Bekvemmelighed

Bekvemmelighedsaspektet er først og fremmest vigtigt i relation til vælgeren. Det er afgørende, at kommunikations- og beregningskompleksiteten ved stemmeafgivelsen er minimeret særligt for denne aktør — ligesom det også bør være beregningsmæssigt overkommeligt at verificere valgresultaterne, d.v.s. for observatørerne.

Endelig vil vi give en kortfattet vurdering af beregningskompleksiteten for myndighederne, men det bør bemærkes, at denne i høj grad afhænger af de valgte nøglegenererings- og dekrypteringsprotokoller.

Det er imidlertid klart, at alle disse størrelser afhænger af valgets udformning, d.v.s. hvor mange valgmuligheder den enkelte vælger gives. For at holde vurderingen simpel, vil vi primært overveje hovedeksemplet, et binært valg.

I vurderingen af henholdsvis beregnings- og kommunikationskompleksitet står det klart, at dette for alle aktører i høj grad afhænger af valgets udformning. Såfremt der er flere valgmuligheder, øges kompleksiteten, jf. Afsnit 9.2.4. For at holde vurderingen tilstrækkelig simpel, har vi i det følgende valgt primært at beskæftige os med eksemplet, det binære valg.

Vi vil dog også give en kort vurdering af kompleksitet i tilfældet med flere myndigheder.

9.2.1 Arbejde for vælger

Vi vil i det følgende anvende antallet af modulære multiplikationer af $O(k)$-bit tal, hvor k er sikkerhedsfaktoren i ElGamal kryptosystemet, som et mål for *arbejdet* (kompleksiteten).

I [Cramer et al., 1997] argumenteres for, at arbejdet for vælgeren er $O(k)$ — og at dette er optimalt i forhold til tidligere foreslåede protokoller for elektronisk afstemning. Sidstnævnte kan vi ikke tage stilling til, men det er let at se, at antallet af modulære parvise multiplikationer af tal, hvis bit-længde er $O(k)$.

ElGamal-kryptering af stemme Jf. Afsnit 6.1 kræver dette to modulære eksponentiationer og en multiplikation.

Afgivelse af bevis for viden Ved anvendelse af protokollen DISKLOG-BEVIS foretages atter to modulære eksponentiationer.

En modulær eksponentiation (hvor k er den maksimale eksponent) af et $O(k)$-bit tal kræver maksimalt $O(k)$ modulære multiplikationer ved brug af metoden beskrevet i Afsnit 5.3.3, og det følger at antallet af modulære multiplikationer er $O(k)$ for vælgeren.

Det er her værd at bemærke, at kompleksiteten faktisk er helt uafhængig af alle andre faktorer end lige netop sikkerhedsfaktoren — d.v.s. eksempelvis er antallet af valgautoriteter uden betydning.

Kommunikationskompleksiteten er indlysende $O(k)$.

9.2.2 Arbejde for valgautoriteter

Under selve afstemningen skal de enkelte valgautoriteter dels

Vælgers ZK-bevis Undersøge hver enkelt vælgers zero-knowledge bevis for korrekthed af stemme for m vælgere. For hvert bevis kræves to modulære eksponentiationer, d.v.s. et samlet arbejde $O(mk)$.

Valgautoriteters ZK-bevis Undersøge de øvrige valgautoriteters zero-knowledge bevis i forbindelse med dekrypteringen, atter med arbejde $O(k)$ for hvert tjek. Samlet arbejde $O(nk)$.

Desuden afgiver hver enkelt valgautoritet et zero-knowledge bevis for korrekthed af nøgleandel med arbejde $O(k)$ (jf. Afsnit 9.2.1), hvilket kan betragtes som negligibelt i forhold til det øvrige.

Det samlede arbejde er derfor $O(mk + nk)$. Typisk vil antallet af valgautoriteter være meget mindre end antallet af vælgere, d.v.s. arbejdet kan tilnærmes med $O(mk)$.

I fællesskab skal valgautoriteterne desuden beregne en diskret logaritme, $\log_G G^T$, hvor T er differensen mellem ja- og nej-stemmer. Dette kan f.eks. gøres ved konsekvent (iterativ) beregning af de mulige værdier, $G^{-n}, G^{-n+1}, \ldots, G^n$, d.v.s. med arbejdet $O(l)$.

9.2.3 Arbejde for observatør

Observatøren skal tilsvarende undersøge korrektheden af de enkelte zero-knowledge beviser, d.v.s. arbejdet er som for valgautoriteterne $O(mk + nk)$ eller tilnærmelsesvis $O(mk)$.

9.2.4 Arbejde i udvidede afstemninger

Vurderingen af ja/nej-afstemningstypen giver lovende estimater for de enkelte aktørers arbejde — men hvad med arbejdet under afstemninger med flere valgmuligheder?

Det er klart, at arbejdet for vælgeren *ikke* ændres. Arbejdet for myndighederne stiger imidlertid drastisk, idet valgresultatet skal beregnes ud fra resultatet af dekrypteringen, der i tilfældet med K valgmuligheder (og dermed K frembringere) er

$$G_1^{T_1} G_2^{T_2} \cdots G_K^{T_K}.$$

En simpel metode til udregning af de enkelte T_i, $i = 1, 2, \ldots$ er at efterprøve samtlige mulige kombinationer ud fra kendskab til sammenhængen

$$n = \sum_{i=1}^{K} T_i.$$

Dette giver $O(l^{K-1})$ multiplikationer, d.v.s. arbejdet er eksponentielt i antallet af valgmuligheder.

I hvilken grad det influerer på protokollens anvendelighed under et dansk valg — f.eks. kommunal valg og folketingsvalg, hvor der typisk er mange valgmuligheder — kan ikke umiddelbart vurderes. Under alle omstændigheder står det klart, at metoden *ikke* er optimal for alle situationer. I Afsnit 9.3.2 nævnes mulige alternativer.

9.3 Konklusion

Vi har nu opstillet og analyseret en protokol for elektronisk afstemning baseret på homomorf, verificérbar og fejltolerant tærskel ElGamal kryptering. Samlet konkluderer vi, at protokollen i tilstrækkelig grad lever op til de tidligere opstillede kravsspecifikationer, idet vi forventer, at vores antagelse om eksistens af f.eks. sikkert kommunikationsforum og digitale signaturer som en sikker identifikationsløsning er korrekte. Vi har påpeget, at disse naturligt vil være svage punkter i protokollen.

Desuden påviser vi, at det nødvendige arbejde for de enkelte aktører i protokollen i mindre afstemningssituationer vil være ideelt for en praktisk implementering. Dette sikrer også mobiliteten, idet de tekniske krav til det anvendte kommunikationsudstyr er minimalt. I forbindelse med f.eks. valg på national skala viser arbejdet med udregning af valgresultatet sig dog yderst krævende, og protokollen er her mindre velegnet.

Samlet vurderer vi, at den opstillede protokol vil være et glimrende *udviklingsgrundlag* for en endelig løsning, der kan dække det danske behov på alle punkter. Samlet giver grundelementerne i protokollen en effektiv anvisning på, hvordan et afstemningssystem kan opbygges, v.h.a. et homorf, verficérbart tærskel system baseret på et non-deterministisk kryptosystem. Den grundlæggende opbygning kan optimeres ved anvendelse af alternative kryptosystemer, f.eks. *Paillier*, jf. Afsnit 9.3.2.

Hvad angår sikkerhed er dog den betænkning, at den her opstillede protokol udelukkende præsenterer et system, hvori der påvises *teoretisk sikkerhed*. I praksis kan vi ikke forvente, at systemet vil fungere helt som planlagt, og sikkerheden af en konkret implementering af protokollen bør derfor undersøges ved yderligere, praktiske eksperimenter og sikkerhedsanalyser.

Det er et faktum, at elektronisk afstemning via internettet har nogle principielle begrænsninger, der ikke vil kunne løses uanset udformningen af et system. Kontrol under valghandlingen vil *aldrig* blive så fuldstændig, som det er tilfældet under traditionel afstemning.

Disse begrænsninger er gode argumenter *mod* elektronisk afstemning og kun gennem en længere offentlig debat, kan det afgøres, hvorvidt de mange øvrige fordele opvejer begrænsningerne.

9.3.1 Varianter af ElGamal

I hovedparten af den videnskabelige litteratur, vi har brugt i forbindelse med opstilling af protokollen, anvender man en variant af ElGamal, hvor man i stedet for at arbejde i selve $(\mathbb{Z}/p\mathbb{Z})^*$ arbejder i *undergrupper G_q af primtalsorden q*.

Da q har betydeligt mindre bit-længde end p (som oftest anvendes $p = 2q + 1$), er beregninger i G_q generelt langt mere effektive end det traditionelle ElGamal kryptosystem.

Ydermere tyder det på, at sikkerheden i høj grad er bevaret. Den mest effektive metode til beregning af diskrete logaritmer, indeks analyse (jf. Afsnit 5.3.5), kan *ikke* udnytte G_q's undergruppestruktur, men må anvendes på den oprindelige gruppe $(\mathbb{Z}/p\mathbb{Z})^*$ (jf.

[Buchmann, 2000, Afsnit 11.5]). Andre metoder som f.eks. Pollard ρ kræver mindst $\sqrt{q}$ gruppeoperationer, og er således også i praksis uanvendelige når $|q| > 160$.

Når vi i denne rapport har valgt at arbejde i den oprindelige gruppe, uden disse yderligere foranstaltninger, er det primært af overskuelighedshensyn. En praktisk implementation bør naturligvis benytte sig af denne mulighed.

9.3.2 Alternative løsninger og eksisterende systemer

Som påpeget er den opstillede protokol uhensigtsmæssig i tilfældet, hvor der optræder mange valgmuligheder, og i nogen grad i valgsituationer med mange vælgere.

Dette grundlæggende problem foreslås i [Damgaard and Jurik, 2001] løst ved anvendelse af en generaliseret udgave af et alternativt kryptosystem, *Paillier kryptosystemet* (jf. [Paillier, 1999]), et non-deterministisk kryptosystem baseret på vanskeligheden ved at afgøre *sammensatte* n*. restklasser modulo* n^2, d.v.s. afgøre om der for givet $z \in (\mathbb{Z}/n^2\mathbb{Z})^*$ eksisterer y, så

$$z = y^n \mod n,$$

hvor $n = pq$ for store primtal p, q.

Det vises i [Damgaard and Jurik, 2001], at dette system kan udvides med mulighed for zero-knowledge beviser og tærskel opbygning, således at det kan anvendes i samme stil som ElGamal kryptosystemet.

Ydermere vises, at dette system muliggør stemmeafgivelse for t ud af K valgmuligheder, en egenskab, der heller ikke er til stede i vort system og muligvis kan være nyttig i visse sammenhænge. Under traditionelle valg- og afstemningssituationer er dette dog ikke relevant, eftersom man maksimalt kan stemme på én kandidat eller valgmulighed.

Det danske firma *Cryptomathic* har fremstillet et afstemningssystem baseret på Paillier og principperne i zero-knowledge beviser for viden og tærskel kryptografi. Af deres hjemmeside [2] fremgår, at

> *"As the first company in the world, Cryptomathic now offers a toolkit for electronic voting that guarantees secrecy and validity of votes, which can be combined with authentication of votes. The toolkit can be used for e-Voting solutions, scalable up to millions of voters and hundreds of candidates."*

[2] `http://www.cryptomathic.com`

Kapitel 10

Markedsanalyse

Vi har nu gjort rede for, at de tekniske forudsætninger for elektronisk afstemning faktisk er til stede. Den opstillede afstemningsprotokol, jf. Kapitel 8, opfylder de i Afsnit 2.3 opstillede kravsspecifikationer (under mindre forbehold), og vi har vurderet, at protokollen i sin nuværende form er en glimrende basis for videreudvikling af et egentligt, praktisk afstemningssystem.

Den tekniske baggrund kan dog ikke betragtes som tilstrækkelig begrundelse for at indføre elektronisk afstemning. Vi vil derfor i dette kapitel undersøge, om der er et *marked* for et sådant produkt, d.v.s. om der er basis for at videreudvikle protokollen til et endeligt produkt.

Specifikt vil vi forsøge at tage stilling til følgende spørgsmål:

- Er der politisk stemning for anvendelse af elektronisk afstemning?
- Er diverse øvrige forudsætninger for elektronisk afstemning til stede?
- Er befolkningen interesseret i at afgive stemme via internettet?

Ud fra denne stillingtagen vil vi opstille en konklusion i form af en anbefaling — bør man i Danmark allerede nu arbejde med elektronisk afstemning som alternativ?

Hovedvægten af undersøgelsen vil ligge på befolkningens interesse, som vi har valgt at belyse gennem vores egen *spørgeskemundersøgelse*, jf. Afsnit 10.4. De øvrige spørgsmål vil vi tage stilling til ud fra sekundært materiale.

Den teoretiske baggrund for denne analyse [Andersen et al., 2000, kap. 9-11].

10.1 Struktur af analysen

I forbindelse med elektronisk afstemning er markedsanalysen, kort beskrevet, en analyse, hvis formål er at afdække, hvorvidt der er basis for at videreudvikle og senere indføre et nyt produkt (elektronisk afstemning), eller om de eksisterende muligheder (traditionelle afstemningsmetoder) er tilstrækkelige.

I henhold til opdelingen af analysekategorier i [Andersen et al., 2000, Kap. 9], har vi valgt at opdele vores analyse i to forskellige faser

Eksplorativ analyse Denne del af analysen har til formål at belyse, hvilke omstændigheder, der som minimum skal være til stede, før indførelse af EA kan blive en realitet.

Deskriptiv analyse Det må formodes, at i hvert fald en del af befolkningen er interesseret i EA; men hvilke sammenhænge skyldes denne interesse, og hvilke omstændigheder gør, at dele af befolkningen *ikke* er interesseret i EA? Dette vil blive vurderet ud fra en række hypoteser, der undersøges ud fra den tidligere nævnte spørgeskemaundersøgelse.

Valg af spørgeskemaundersøgelse som analysemetode skyldes primært, at vores analysefelt er så specialiseret, at der til vort kendskab ikke eksisterer undersøgelser, der tager stilling til de spørgsmål, vi ønsker besvaret. Vi erfarede dog undervejs i analyseforløbet, at der er udført en lignende undersøgelse i 2001 omhandlende danskernes internetvaner, heriblandt holdningen til afstemning via internettet. Jf. Afsnit 10.3.

Afsnittet er suppleret med to bilag, hhv. selve spørgeskemaet, Appendiks B samt resultaterne, Appendiks C.

10.2 Umiddelbare forudsætninger

Vi vil i dette afsnit forsøge at beskrive, primært hvilke politiske omstændigheder, der skal være opfyldte og vurdere disse — men også sammenholde dette med de øvrige forudsætninger både socialt og praktisk. Det bør bl.a. være et krav, at EA giver lige muligheder for hele den myndige befolkning, jf. Afsnit 2.1.1 — men hvordan er f.eks. fordelingen af adgang til internettet; og hvordan ser den fremtidige situation ud sammenholdt med regereringens IT-planer?

10.2.1 Politisk stemning og målsætning

Såfremt EA skulle indføres, ville dette blive som resultat af en række politiske overvejelser. Det er derfor klart, at politisk velvilje overfor dette alternativ er et bydende nødvendigt krav for indførelse af EA. I Danmark kan man imidlertid argumentere, at forudsætningerne allerede på nuværende tidspunkt er gode. Under den tidligere regering blev IT-området for alvor sat i fokus; tidligere statsminister Poul Nyrup Rasmussen udtalte i sin nytårstale 2001: “Jeg vil gerne have et Danmark, der ganske enkelt er verdens bedste IT-nation.”

Dette er et godt miljø for IT-muligheder, der i første omgang vil være af eksperimentel karakter,som netop EA. Den tidligere regerings IT-linie er ført videre under den nye regering.

IT-handlingsplan 2002

Vi vil argumentere for, at der i høj grad banes vej for EA i de omfattende IT målsætninger, Danmark har sat sig. Af Regeringens IT- og telepolitiske redegørelse 2002, [for videnskab teknologi og udvikling, 2002] fremgår, at

> *"Regeringen vil satse intensivt på uddannelse, forskning, innovation og IT. En fokuseret og sammenhængende indsats på disse områder vil sikre dansk vækst og velfærd i det 21. århundrede."*

I den nuværende handlingsplan nævnes ikke specifikt muligheden for elektronisk afstemning, men der optræder adskillige initiativer og målsætninger, der peger i retning af en gennemgribende digitalsering af det offentlige og den enkelte borgers kontakt med offentlige services. Specifikt nævnes under målsætningerne om en IT-baseret offentlig sektor i [for videnskab teknologi og udvikling, 2002] følgende sigtelinie:

> *"Den offentlige sektor arbejder og kommunikerer digitalt internt og i kontakten med borgere og virksomheder."*

En del af denne sigtelinie er det såkaldte *projekt digital forvaltning*, der i den nye handlingsplan udvides med mulighed for den enkelte borger inden udgangen 2002 at få en *digital signatur*. Denne ordning suppleres naturligvis med passende juridiske forhold.

Dette er et vigtigt tiltag i relation til elektronisk afstemning — vi redegjorde i Afsnit 9.1 for, at adgangen til en unik digital signatur var en af de vigtigste tekniske forudsætninger for en elektronisk afstemnningsprotokol. Hvorvidt den planlagte teknologi er tilstrækkelig sikker til anvendelse i forbindelse med elektronisk afstemning er dog uvist.

Selvom mulighederne synes oplagte, anføres dog i [for videnskab teknologi og udvikling, 2002], at man må forvente en anden IT-indstilling af den nye regering, end det var tilfældet under den tidligere. Særligt i forbindelse med nye og mere eksotiske projekter som netop EA er følgende af interesse

> *"Der er behov for en mere nyttig, nuanceret og nøgtern IT-politik i Danmark. I stedet for kun at fokusere på teknologien skal IT-politikken fremover handle om, hvordan ny teknologi kan bidrage til at skabe værdi for den enkelte, for virksomhederne og for samfundet."*

Det er således af stor betydning, at man i en markedsføring af EA markerer sig direkte med *målrettede resultater*, såfremt den nødvendige politiske interesse skulle skabes.

Vi argumenterede i Afsnit 2.1 for, at EA bl.a. vil kunne give følgende fordele

- Større bekvemmelighed.
- Mulighed højere valg/afstemningsdeltagelse.
- Øget præcision.

Den større bekvemmelighed og den øgede præcision er fordele, der ligger implicit i selve muligheden. En øget deltagelse er derimod en gevinst, der må skabes af befolkningens interesse og velvilje overfor metoden specielt i de marginaliserede grupper, der vil kunne drage særlig fordel af EA.

En yderligere fordel, der indirekte kunne tænkes at give økonomisk gevinst, er konsolideringen af Danmarks status som moderne IT-nation. En sådan veletableret status gør Danmark til et attraktivt område for internationale IT-virksomheder, der har behov for forsøgsområder — og netop indførelse af muligheden for at stemme elektronisk vil være et klart signal til omverdenen om, at vi her i landet er parate til at give os i kast med nyskabende informationsteknologiske eksperimenter. Endelig er det signalet om, at Danmark sætter mangfoldigheden af demokratiet højt også af ren omdømmemæssig interesse.

Samlet er elektronisk afstemning absolut en relevant mulighed set ud fra regeringens målsætninger, men den vil næppe have mange chancer uden en bred og oprigtig vælgerinteresse.

KL og e-demokrati

Kommunernes Landsforening omtaler i skrivelsen *"E-demokrati"* af 19. oktober 2001, [Landsforening, 2001], muligheden for elektronisk afstemning som et led i digitaliseringen af den offentlige sektor. Internetafstemning præsenteres som et af de mere konkrete projekter; specifikt omtales projektet Høje-Taastrup Kommune, hvor man ved ældrevalget den 30. oktober 2001 gav kommunens ca. 7.500 ældre muligheden for at stemme via internettet.

Skrivelsen afrundes som følger:

> *"Samlet set ser KL et stort demokratisk potentiale i e-demokrati og de forsøg, der bliver udført i dag, er væsentlige for udviklingen på dette område. [...] Ydermere viser nogen forsøg samt undersøgelser (se den i dette nyhedsbrev omtalte PLS-rapport [red. [Management, 2001]]), at der er en noget afmålt efterspørgsel fra borgerne på e-demokrati. Derfor mener vi fra KL's side, at e-demokrati på nuværende tidspunkt ikke har første prioritet i forhold til den digitale forvaltning."*.

På kommunalt plan er politisk interesse derfor også i høj grad til stede — dog vurderes efterspørgslen for lille til at sidesætte e-demokrati projekter med det igangværende projekt digital forvaltning. Som for regeringens IT-handlingsplan må vi derfor tilsvarende konkludere, at et evt. politisk projekt først ville kunne skabes på baggrund af udbredt interesse blandt vælgerne.

10.2.2 Yderligere forudsætninger

Vi vil nu tage stilling til yderligere forudsætninger, primært ud fra den kritiske stillingtagen til fordele i Afsnit 2.1.1.

Digitale kløfter

Som tidligere omtalt er en afgørende forudsætning for indførelse af elektronisk afstemning, en udjævning af de *digitale kløfter*, der eksisterer mellem forskellige samfundsgrupper, således at der er lige muligheder for enhver myndig og digital diskriminering undgås.

Det fremgår af [Statistik, 2002], at i første kvartal af 2002 havde 75 % af den danske befolkning, der har adgang til internettet fra enten hjem eller arbejdsplads.

Dette udgør en stigning på ca. 2 % siden første kvartal 2001. Af de 75 %, er der 62 % der har adgang til internettet hjemmefra.

Den største stigning med adgang til internettet er i aldersgruppen 60 år og over. Denne er steget med 20 % sammenlignet med samme kvartal i 2001. Det er dog stadig i denne aldersgruppe, der er færrest, der har adgang til internettet. Desuden fremgår det, at uddannelse har fået mindre betydning for adgang til internettet. Antallet af personer med grundskole som højeste uddannelse, der har adgang til internettet er steget fra blot 13 % i 2001 til 49 % i første kvartal af 2002.

Disse statistikker er lovende for elektronisk afstemning, for de antyder, at den fremtidige udvikling går mod en mere eller mindre jævn fordeling på vælgere, der har adgang til internettet.

Ydermere, i [for videnskab teknologi og udvikling, 2002] nævnes den målsætning, at "flere danskere får adgang til og anvender internettet". Denne målsætning nævner ikke konkret metoder til udjævning af digitale kløfter mellem forskellige samfundsgrupper, men af handlingsplanen fremgår yderligere mål såsom øget konkurrence i telesektoren — en omstændighed, der kan forventes at give billigere internetadgang og flere borgere på nettet, også blandt de ældre.

Under alle omstændigheder bør elektronisk afstemning suppleres med muligheden for at afgive sin stemme elektronisk på offentlige institutioner — f.eks. kunne man forestille sig kommunale datastuer, eller særlige muligheder for afstemning på f.eks. de lokale biblioteker.

Mistro

Som nævnt tidligere er ligegyldighed og mistro til afstemninger og valg en alvorlig trussel mod EA. Vi vurderer, at mistroen kun vil kunne håndteres ved en længerevarende og omfattende offentlig debat og efterfølgende informationskampagne, hvor vælgerne bliver præcist og objektivt informeret om den nye afstemningsform, sikkerhed og procedurer.

10.3 Vælgerinteresse for elektronisk afstemning

Vi har indtil videre påpeget, at der er bred politisk interesse for et digitaliseret Danmark, samt at EA på sigt vil være en oplagt mulighed.

Ydermere har vi givet en kort vurdering af de yderligere forudsætninger og konkluderet, at den digitale kløft på sigt ikke er problematisk, ligesom mistillidsspørgsmålet formentlig vil kunne håndteres gennem en offentlig debat og informationskampagne.

I dette afsnit vil vi forholde os til det vigtigste spørgsmål: Er vælgeren interesseret i at stemme via internettet?

Som primærkilde for undersøgelse af denne interesse, har vi anvendt spørgeskemaundersøgelse på en mindre skala, d.v.s. en undersøgelse med mindre vægt på metoden, hvor målgruppen dels er begrænset, og dels hvor resultaterne ikke kan betrages som en dækkende måling for hele befolkningen. Der er altså blot tale om en undersøgelse, der kan give en føling med, hvordan stemningen blandt vælgerne er.

P.g.a. disse naturlige metodiske begrænsninger vurderede vi også, at undersøgelsen ikke i sig selv kunne betragtes som tilstrækkeligt vurderingsgrundlag. Derfor anvendte vi som supplerende materiale rapporten "Den Digitale Borger 2001" udført af PLS RAMBØLL Management ([Management, 2001]), en redegørelse for danskernes internetvaner, særligt i relation til anvendelse af offentlige services. Selvom en direkte sammenligning med denne ikke er mulig, vil vi dog forsøge at vurdere vores undersøgelse ud fra resultater i denne.

10.3.1 Hypoteseopstilling

Vi vil nu opstille de hypoteser for vælgerinteressen og dennes sammenhæng med øvrige variable. Disse hypoteser søges så vidt muligt belyst gennem spørgeskemaundersøgelsen.

Det bør bemærkes, at enkelte af hypoteserne under processen viste sig uhyre vanskelige at omforme til brugbare spørgsmål, som det vil fremgå af Afsnit 10.3.2.

Hypotese 1 (mistillid) Folk vil være utrygge m.h.t. EA, da en digitalt afgivet stemme ikke giver den samme håndgribelighed som regulære papirstemmer ved traditionelle valg og afstemninger. Man kan ikke "føle på stemmen" — valgsituationen føles mindre nærværende og uoverskuelig, når alt foregår digitalt. Desuden er elektronisk afstemning et meget stort spring fra den traditionelle afstemning, og generel utryghed må derfor forventes.

Hypotese 2 (fortrolighed med computer/internet) Vi forventer, at fortroligheden med computer og erfaring og tillid til udveksling af fortrolige oplysninger via internettet har en stor betydning for den enkelte vælgers holdning til EA. Personer, der er uvante med computere og internet og er skeptiske overfor sikkerheden vil formentlig udvise betydeligt større modvilje end personer, der anvender computer og internet dagligt og har større tillid til udveksling af fortrolige oplysninger.

Hypotese 3 (demografisk afhængighed Vi forventer, at alderen tilsvarende har en stor betydning for holdningen til EA. Dette vurderer vi ud fra de tidligere nævnte statistiskker, ifølge hvilken kun en mindre andel af ældre har adgang til f.eks. internet. D.v.s. fortroligheden må være tilsvarende mindre, jf. Hypotese 2. Omvendt

forventer vi, at helt unge mennesker er positive overfor EA. M.h.t. afhængighed af køn forventer vi ingen forskel.

Hypotese 4 (demokratisk engagement) Det må antages, at folks demokratiske engagement har en betydning for, hvordan de ønsker at afgive stemme. Personer, der føler det mindre vigtigt at markere deres deltagelse i demokratiet ved stemmeafgivelse vil formentlig være mere tilbøjelige til at acceptere alternative (mindre kendte og mindre håndgribelige) afstemningsmetoder og omvendt.

Hypotese 5 (det sociale aspekt) Det sociale aspekt ved den nærmest rituelle handling, en afstemning eller et valg må også forventes at spille ind. Den traditionelle afstemningsprocedure indeholder f.eks. det at stå i kø, snakke med venner og bekendte, sætte sit kryds og putte stemmen i stemmeurnen og at følge stemmeoptællingens forløb og resultat på fjernsynet; hyggen og traditionen. Tilsvarende omstændigheder er ikke til stede ved elektronisk afstemning, og dette forventer vi også har en betydning for folks indstilling.

Hypotese 6 (uddannelse/profession) Det er rimeligt at formode, at en faktor som uddannelse og profession har en tilsvarende betydning for holdningen. Autoritetstro eller mangel på samme hænger formentlig i nogen grad sammen med uddannelsesmæssig baggrund — og netop antiautoritære dele af vælgerskaren vil formentlig være særdeles kritiske overfor EA.

10.3.2 Omformning af hypotesegrundlag til spørgeskema

Det var fra starten planen, at spørgeskemaet skulle omdeles på offentlige steder i Aalborg og omegn — og det satte visse begrænsninger for spørgeskemaets omfang. Udformningen blev gjort på baggrund af følgende overordnede kravsspecifikationer

- De relevante hypoteser skulle belyses med så få spørgsmål, som muligt (overskuelighed og lethed for utålmodige respondenter).
- Analysérbare resultater — vi ønskede data, vi kunne analysere numerisk og tolke mere eller mindre absolut.

Kravet til muligheden for at analysere resultaterne numerisk førte naturligt til, at de enkelte spørgsmål blev formuleret på *lukket form*, d.v.s. respondenten har et fast antal svarmuligheder. Dette muliggør en meget målrettet og præcis undersøgelse, men med den sideeffekt, at de få frihedsgrader udjævner nuancer i besvarelserne. Derfor supplerede vi ved en række respondenter med kortfattede spørgsmål til besvarelserne af enkelte spørgsmål.

Ydermere forsøgte vi at følge anvisningerne i [Andersen et al., 2000] på den korrekte opbygning af et spørgeskema. I denne kilde nævnes bl.a., at man under konstruktionen skulle sikre

1. Entydige og præcist formulerede spørgsmål — for at undgå misforståelser.
2. Jævn opbygningen af spørgsmål frem mod hovedspørgsmål.

Ud fra de nævnte specifikationer forsøgte vi at udforme spørgsmålene, så de bedst muligt belyste flest muligt af hypoteserne i Afsnit 10.3.1. For det endelige spørgeskema, jf. Appendiks B. Der følger nu en redegørelse for de enkelte spørgsmål.

Spørgsmål 1 og 2 De nødvendige demografiske oplysninger for belysning af Hypotese 3 samt for at sikre, at vi i undersøgelsen har adspurgt en tilstrækkelig varieret befolkningsgruppe. Vi valgte en intervalinddeling af alderen, dels for at undgå for personlige spørgsmål, dels for at lette det senere analysearbejde. Vi vurderede, at den valgte inddeling var tilstrækkelig fin til vort formål. Vi valgte desuden kun at spørge myndige personer, primært p.g.a. de øvrige spørgsmåls karakter.

Spørgsmål 3, 4 og 5 For belysning af Hypotese 2, fortrolighed med computer og internet (samt tillid). Vi fandt det nødvendigt at indlægge en vis tolkning i en belysning af hypotesen i *konkrete spørgsmål* — for hvad er tillid og fortrolighed til computere og internet? Vi valgte at måle dette på anvendelse af computer, erfaring med udveksling af fortrolige oplysninger via Internet — og slutteligt tilliden hertil. Igen af hensyn til den senere analyse fandt vi en gradinddeling af svarmulighederne mest oplagt.

Spørgsmål 6 For belysning af Hypotese 4; hænger folks holdning til EA sammen med deres demokratiske engangement? Vi valgte at måle dette demokratiske engagement ud fra hvor vigtigt respondenten fandt det at deltage i folketingsvalg. Dette specifikke valg af afstemning/valgtype blev gjort på baggrund af den vurdering, at entydighed ville gå tabt såfremt vi spurgte til generelt valg/afstemning. Et valg til europaparlamentet er for de fleste af noget mindre betydning end et folketingsvalg.

Spørgsmål 7 Selve hovedspørgsmålet. Som for spørgsmål 6 valgte vi her at være meget konkrete og specifikt spørge, om respondenten var interesseret i at stemme via internettet til *folketingsvalg*. Begrundelsen er den samme som ovenfor.

Et yderligere spørgsmål vi havde med var — *"Er folkeafstemning en vigtig social begivenhed for Dem?"*, hvis formål var at belyse Hypotese 5. Vi fravalgte imidlertid dette spørgsmål senere i forløbet, idet vi vurderede, at formuleringen var så abstrakt, at respondenternes tolkning næppe ville blive entydig. Hvad menes der med "social begivenhed"? Vi fandt det ikke muligt at konkretisere dette spørgsmål i så tilstrækkelig grad, at både tolkning var let samtidig med at det belyste Hypotese 5 tilfredsstillende.

Bemærk, at vi i spørgeskemaet ikke fandt det muligt at belyse Hypotese 1 og 6. Førstnævnte skyldes at det er svært at stille et spørgsmål, som omhandler vælgernes følelser omkring afstemningsprocessen. Vi har også den formodning, at mange vælgere ikke har anskuet problemstillingen ud fra denne vinkel og derfor vil have svært ved at svare på et spørgsmål herom. M.h.t. Hypotese 6 vurderede vi, at et spørgsmål omhandlende respondenternes uddannelsesmæssige baggrund dels kunne opfattes for personligt (taget i betragtning, at anonymiteten i vores undersøgelse var begrænset, se senere), samt at en spørgeskemaundersøgelse på en så forholdsvis lille skala som vores ikke vil kunne give noget anvendeligt resultat.

Spørgeskemaarket er sat op med en kort indledende præsentation af formålet og emnet. Vi havde med vilje valgt ikke at uddybe selve de nærmere omstændigheder ved moderne kryptografiske afstemningsprotokoller — simpelthen fordi vi ønskede folks *umiddelbare* holdning og de evt. ubegrundede forudindstillinger, denne måtte indeholde (f.eks. en forventning om, at det ikke er teknologisk muligt eller at sikkerheden vil være alt for dårlig).

10.4 Resultater af undersøgelse

I det følgende vil vi præsentere resultaterne af den udførte spørgeskemaundersøgelse. Undersøgelsen omfattede 70 respondenter, der blev opsøgt i henholdsvis Aalborg midtby og Aalborg Storcenter mandag eftermiddag d. 22/4-2002. Det stod respondenten frit for, om vedkommende selv ville udfylde spørgeskemaet eller om udfyldelsen skulle foregå på interviewform.

Udvælgelsen af respondenter var ikke baseret på nærmere fastlagte retningslinier udover, at de enkelte interviewere så vidt muligt skulle forsøge at fordele sig jævnt over de forskellige aldersintervaller og køn.

10.4.1 Målgruppevurdering

De demografiske oplysninger for respondenterne fordelte sig som følger

	Mænd	**Kvinder**	**Ialt**
18-30 år:	16	16	32
31-50 år:	6	7	13
51-70 år:	12	8	20
71-? år:	3	2	5
Ialt:	37	33	70

Tabel 10.1: Demografisk fordeling

Det fremgår, at der er en nogenlunde lige fordeling mellem respondenternes køn. Hvad angår aldersfordelingen, er der en kraftig overvægt af yngre mennesker, mens der er så godt som ingen af de ældste respondenter. Dette afspejler i høj grad aldersfordelingen i de omgivelser, spørgeskemaet blev uddelt i — men det er afgørende at være opmærksom herpå i forbindelse med den videre analyse.

Fordelingen afspejler *ikke* den faktiske befolkningsfordeling i Danmark, og resultaterne af den øvrige undersøgelse kan derfor kun betragtes som vejledende.

10.4.2 Databehandling

Vores oprindelige mål med spørgeskemaet var at undersøge sammenhængen mellem svar på de *enkelte spørgsmål* og holdningen til elektronisk afstemning (specifikt elektronisk afstemning til folketingsvalg); d.v.s. en deskriptiv analyse.

Ud fra en metodisk synsvinkel er dette imidlertid vanskeligt. De enkelte spørgsmål har relativt få frihedsgrader (få svarmuligheder), og vi vurderede, at det ville være mere relevant at gruppere de indledende spørgsmål i tre hovedgrupper

1. Demografiske oplysninger.

2. Anvendelse og fortrolighed med computer/internet.

3. Demokratisk engagement.

Under punkt 2 vil vi senere argumentere for en alternativ fortolkning, der dels forenkler den samlede analyse i betydelig grad og dels må formodes at give mere pålidelige resultater.

Spørgeskemaundersøgelsen viste, jf. Appendiks C, at respondenternes demokratiske engagement over hele linien, med få afvigelser, lå i top. Dette resultat giver ikke belæg for en vurdering af hypotese 4, og det demokratiske engagement vil ikke blive kommenteret yderligere.

Det primære resultat viste, at 50% af respondenterne ville stemme elektronisk, 34,2% ønskede ikke at stemme elektronisk, mens de sidste 15,8% svarede måske. Dette resultat vil vi nu analysere i relation til respondenternes demografiske oplysninger og vurdere, om køn og alder har en afgørende betydning for holdningen til EA.

Demografiske oplysninger og holdning til EA

I dette afsnit vil vi kort redegøre for sammenhængen mellem svaret på Spørgsmål 7 i spørgeskemaet og de respektive demografiske oplysninger.

Nedenstående, Tabel 10.2, viser fordelingen af svar i forhold til køn.

	Ja	**Nej**	**Måske**	**Samlet**
Kvinder:	52,8%	33,3%	13,9%	100%
Mænd:	47,1%	35,3%	17,6%	100%

Tabel 10.2: Holdning til EA, køn

Der ses kun meget lille forskel i de afgivede svar, og usikkerheden i netop vores undersøgelse taget i betragtning, må dette vurderes som statistiske tilfældigheder — d.v.s. mænd og kvinders holdning til EA er stort set ens.

Tilsvarende ses heller ikke nogen betydende variation i svar i forhold til aldersgruppe, jf. Tabel 10.3.

	Ja	**Nej**	**Måske**	**Samlet**
18-30 år:	46,9%	31,2%	21,9%	100%
31-50 år:	69,2%	30,8%	0%	100%
51-70 år:	40%	45%	15%	100%
71-? år:	60%	20%	20%	100%

Tabel 10.3: Holdning til EA, alder

Det ser ganske vist ud som om, at 31-50 årige er mere interesserede i EA end f.eks. 18-30 årige, men taget i betragtning, at der er relativt få respondenter i denne aldersgruppe, kan denne konklusion næppe forsvares. M.h.t. de 71-? årige kan resultatet synes overraskende. Der er en bemærkelsesværdig positiv indstilling til EA i denne aldersgruppe ifølge vores undersøgelse. Det ville være interessant at undersøge, om dette også ville være tilfældet, såfremt antallet af respondenter i denne aldersgruppe havde været større, men ud fra vores resultater alene er det umuligt at drage nogen konklusioner.

Fortrolighed med computer/internet

Vi valgte under denne analyse at sammenfatte Spørgsmål 3,4 og 5 og tildele de enkelte svar en heltallig værdi, hvis sum vi da opfatter som et *samlet* udtryk for "fortrolighed med computer/internet".

Dette er et yderst kritisk skridt i analysen, der i høj grad kræver, at man er opmærksom på de konsekvenser, dette kan få for de endelige resultater. Vi vil nu redegøre for, at metoden er berettiget.

Baggrunden for at vælge denne tilgang var primært, at vi vurderede frihedsgraden i de enkelte spørgsmål til at være for lille til at foretage en sigende analyse på hvert enkelt spørgsmål. Ydermere forventede vi, at metoden var det bedste alternativ fremfor at forsøge at vurdere sammenhænge enkeltvis og senere forsøge at kombinere disse til en samlet vurdering — dette ville blive for uoverskueligt.

Vores fremgangsmåde var som følger: Under Spørgsmål 3,4 og 5 blev de enkelte svarmuligheder tildelt en heltallig værdi

Spørgsmål 3 Fra 0 til 3 startende med "aldrig" og de derpå følgende grader af anvendelse.

Spørgsmål 4 Fra 0 til 3 startende med "aldrig" og de derpå følgende grader af anvendelse.

Spørgsmål 5 Fra -2 til 2 startende med "slet ikke", værdien 0 for "ved ikke" og 2 for "i høj grad".

Den enkelte respondents svar på Spørgsmål 3,4 og 5 kan da repræsenteres ved en enkelt talværdi i intervallet -2 til 8, summen af værdien for de enkelte svar, som vi under et vil betegne *fortrolighed med computer/internet*.

En sådan fremgangsmåde har følgende konsekvenser

- Der er samme relative forskel mellem de enkelte svarmuligheder (f.eks. at "slet ikke" er ligeså stærkt i forhold til "i mindre grad", som "i høj grad" i forhold til "en del").
- De enkelte spørgsmåls betydning vægtes ens.

Førstnævnte er naturligvis i høj grad en forenklende antagelse, men en mere detaljeret opstilling af relativ forskel mellem svarmuligheder vil give en større fortolkningsdiskussion, som vi ikke ønsker her.

M.h.t. vægtningen af de enkelte spørgsmål er det klart, at i relation til elektronisk afstemning er det erfaring med og tillid til udveksling af oplysninger via internettet, der bør vægtes tungest (anvendelse af computer i hverdagen bør være af mindre betydning). Denne vægtning sikres imidlertid ved ovenstående fortolkning, idet to af spørgsmålene relaterer hertil. Dette berettiger også, at f.eks. personer, der arbejder med computere til dagligt, men kun sjældent har udvekslet fortrolige oplysninger via nettet og ingen tillid har hertil, vil score temmelig lavt. Ud fra denne vægtningsovervejelse skal den samlede betegnelse "fortrolighed med computer/internet" primært opfattes som erfaring med og tillid til udveksling af fortrolige oplysninger via internettet — og kun i mindre grad anvendelsen af computere i hverdagen.

Den numeriske fortolkning gør det muligt at knytte den enkelte respondents fortrolighed med computere og internet direkte op på de øvrige svar ved en enkelt sammenligning.
Nedenstående tabel viser sammenhængen mellem fortrolighed og holdning til elektronisk afstemning

	Ja	**Nej**	**Måske**
Antal personer:	35	24	11
Samlet fortrolighed:	139	36	38
Gennemsnitlig fortrolighed:	4,0	1,5	3,4

Tabel 10.4: Holdning til EA og fortrolighed med computer/internet

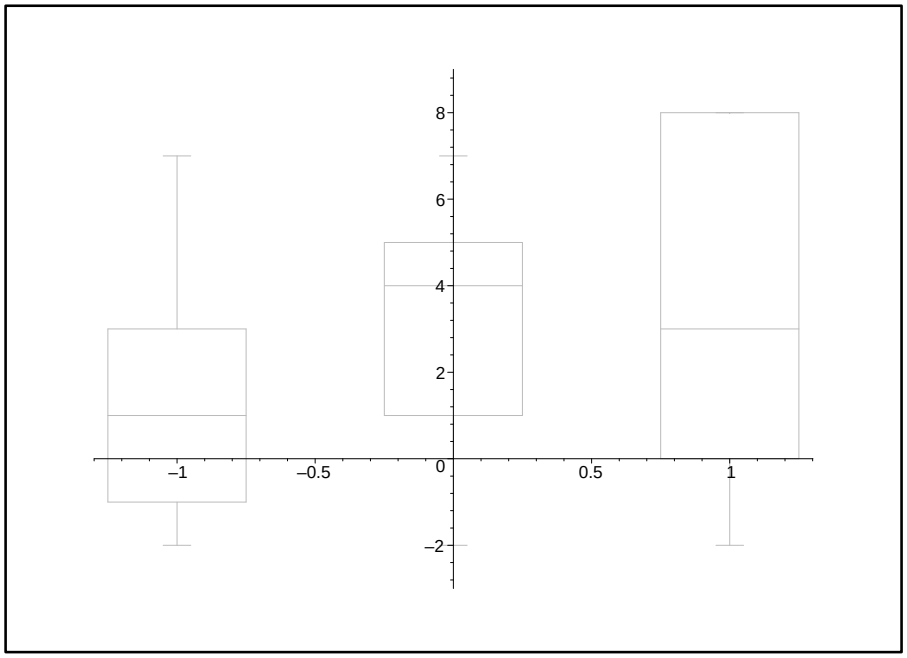
Disse resultater underbygger hypotesen om, at holdningen til elektronisk afstemning i høj grad afhænger af forholdet til computer/internet. Det ses, at ja-respondenterne har betydeligt større fortrolighed med computer/internet, end nej-respondenterne. Hvad angår måske-respondenterne kan vi ikke umiddelbart slutte noget af ovenstående, udover, at de lader til at have større fortrolighed med computer/internet, end nej-respondenterne.

Resultaterne fra ovenstående kan behandles mere indgående ved opstilling af et boksdiagram for hver af de tre svarmuligheder for sidste spørgsmål. Diagrammet, jf. Figur 10.1, er fremstillet i matematikprogrammet Maple. Boksdiagrammet skal forstås således:

- De enkelte rektangler repræsenterer svarene *nej*, *måske* og *ja* fra venstre mod højre.
- Det enkelte rektangels begyndelseslinie er *nederste kvartil* og ender ved *øverste kvartil*, d.v.s. 50% af svarene har fortrolighedsværdi indenfor rektanglet for de enkelte svarmuligheder.
- Linien gennem hver rektangel er *medianen*, d.v.s. 50% af besvarelserne har fortrolighedsværdi over denne linie og 50% under.

- De linier, der går ud fra hvert rektangel repræsenterer henholdsvis de maksimale og de minimale værdier for fortrolighedsværdien indenfor den pågældende svargruppe.

Ovenstående gælder dog ikke ubetinget i vores tilfælde, da vi arbejder med diskrete værdier — d.v.s. markeringer af rektanglets start og slut samt median skal betragtes som omtrentlige værdier, som det også fremgår af følgende analyse. I Figur 10.2 er der opstillet mere nøjagtige grafiske afbildninger.



Figur 10.1: Boksdiagram

Af boksdigrammet kan vi aflæse følgende for de enkelte svargrupper.

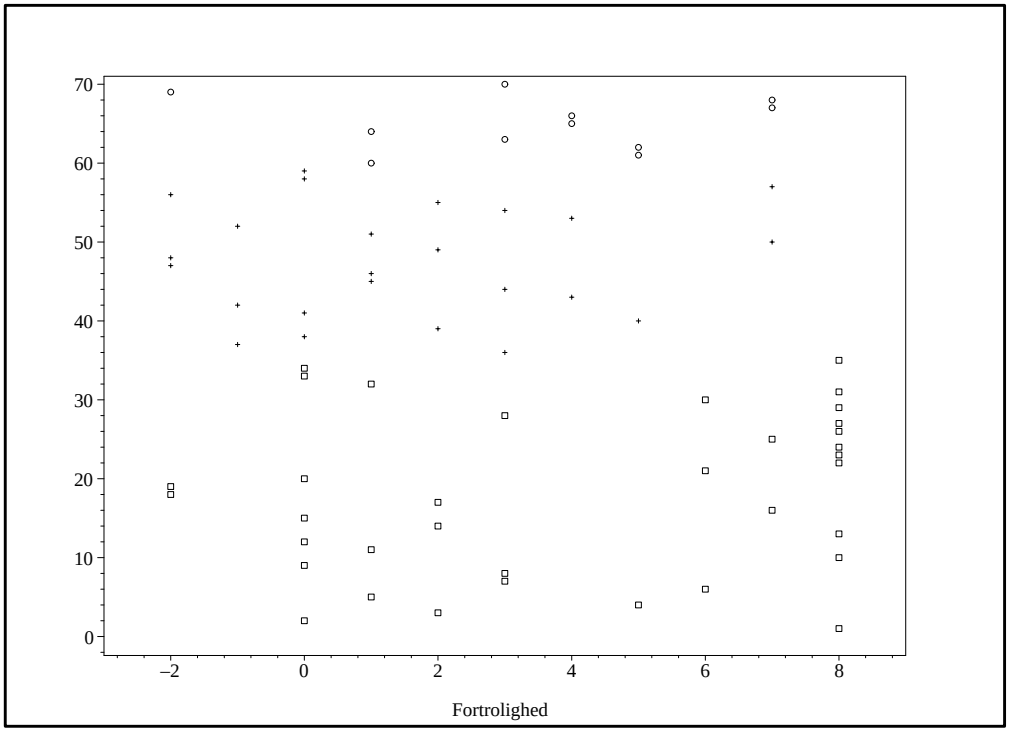
Nej-respondenterne Det ses, at ca. 50% af respondenterne har en forholdsvis lav og temmelig afgrænset fortrolighedsværdi (rektanglet er forholdsvis lille). Medianen befinder sig omkring værdien 1, d.v.s. ca. 50% af nej-respondenterne havde fortrolighedsværdi større end ca. 1 og ca. 50% mindre. Det fremgår imidlertid, at der også er nej-respondenter, der har forholdsvis høj fortrolighedsværdi.

Måske-respondenterne Her ligger ca. 50% af respondenterne med en betydeligt højere fortrolighedsværdi, hvor medianen viser, at halvdelen af måske-respondenterne har en relativt høj fortrolighedsværdi. Igen har vi både folk med lave og høje fortrolighedsværdier i denne kategori.

Ja-respondenterne Det ser umiddelbart ud til, at ca. 50% har en fortrolighedsværdi mellem 0 og 8, d.v.s. de øvrige ca. 50% må have fortrolighedsværdi mindre end 0. Dette er imidlertid en fejlagtig slutning. Diagrammets udformning skyldes, at mere end 25% (10 ud af 32) har maksimal fortrolighedsværdi, jf. spørgeskemaresultaterne i Appendiks C. D.v.s. *for ja-respondenterne indeholder rektanglet ca. 75% af besvarelserne*. Medianens placering (ca. 3) viser iøvrigt en

særdeles jævn fordeling mellem personer, der har en fortrolighedsværdi højere end middel og dem med mindre end middel.

Ud fra ovenstående overvejelser er det rimeligt at konkludere, at ja-respondenterne generelt er mere fortrolige med computer/internet. Tilsvarende kan vi også konkludere, at nej-respondenterne har betydeligt mindre fortrolighed hermed.



Figur 10.2: Plot af fortrolighedsværdien for besvarelser

I Figur 10.2 er nej-respondenterne markeret med $+$, måske-respondenterne med $\circ$ og ja-respondenterne med $\square$. Inddelingen af andenaksen er uden betydning.

10.4.3 Demografiske oplysninger og fortroligheden

I dette afsnit vil vi undersøge, hvorvidt der var en sammenhæng med de demografiske oplysninger og fortroligheden med computer.

Vi ser en klar forskel mellem kønnene jf. Tabel 10.5. Mænd er, i følge vores undersøgelse og fortolkning, mere fortrolige med computer/internet. Dette er en interessant konsekvens af fortolkningen, der bør overvejes nøje, for ifølge Tabel10.2 er der en forholdsvis lige kønsfordeling mellem ja- og nej-respondenterne. D.v.s. ja-respondenter blandt kvinder har generelt lavere fortrolighed end mænd. Denne observation vil vi i Afsnit 10.4.4 forsøge at vurdere ud fra [Management, 2001].

I Tabel 10.6 ser vi også en klar nedgang i fortroligheden med stigende alder. En grafisk afbildning vil vise, at denne falder tilnærmelsesvist lineært med alderen (imidlertid kan vi grundet det lave antal respondenter i visse aldersgrupper, ikke stole på dette resultat).

	Kvinder	Mænd
Antal personer	36	34
Samlet fortrolighed	82	131
Gennemsnitlig fortrolighed	2,28	3,85

Tabel 10.5: Fortrolighed, køn

	18-30	31-50	51-70	71-?
Antal personer:	32	13	20	5
Samlet fortrolighed:	136	39	36	2
Gennemsnitlig fortrolighed:	4,25	3,0	1,8	0,4

Tabel 10.6: Fortrolighed, alder

I henhold til Tabel 10.3 er dette resultat interessant. Umiddelbart skulle man tro at på baggrund af fortroligheden fordelt på alderen skulle være muligt at se en tendens som gik mod lavere interesse for EA med alderen. Dette fremgår dog ikke af vores analyse. Dog er vores datamateriale for den ældste befolkningsgruppe desværre for begrænset til, at vi kan konkludere, at dette er en generel tendens.

10.4.4 Sammenligning med "Den Digitale Borger 2001"

Vi vil nu kort vurdere vores resulateter i relation til en undersøgelse foretaget i 2001 af PLS RAMBØLL Management, "Den Digitale Borger 2001", [Management, 2001]. Undersøgelsen belyser primært danskernes anvendelse af internet og offentlige services over internettet.

Ifølge [Management, 2001, p. 23] ønsker 48% af danskerne, at det skal være muligt at afgive stemme via internettet — 43% mener ikke, det skal være muligt. Selvom resultatet ikke direkte belyser, hvorvidt den enkelte ønsker at stemme via internettet, ser vi dog god overensstemmelse mellem denne undersøgelse og vores. Omtrent 50% er positivt indstillede overfor internetafstemning.

Vi nævnte tidligere, at kvinder ud fra vores fortolkning af spørgeskemaresultater, havde en gennemsnitligt lavere fortrolighed med computer/internet end mænd. Vi har desværre ikke haft mulighed for at påvise gyldigheden af denne konklusion ud fra andet datamateriale — i [Management, 2001] påpeges dog, at kvinder gennemgående er knap så flittige internetbrugere som mændene. Bl.a.

- 3 ud af 10 kvinder anvender internettet dagligt mod 4 ud af 10 mænd.
- 62% af kvinderne har prøvet internettet mod 69% af mændene.

- Kun 3 ud af 10 kvinder bruger homebanking mod 4 ud af 10 mænd
- 39% af kvinderne er interesserede i adgang til offentligt registrerede personlige oplysninger mod 55% af mændene.

De undersøgte forhold er naturligvis af en kvalitativt anden karakter end de forhold, vi har undersøgt, men vi vurderer, at ovenstående kan betragtes som et mål for fortrolighed og anvendelse (dog primært af internet). Det ses, at der ifølge [Management, 2001] *er* en forskel mellem kønnene; dog er denne ikke særlig stor.

I vores undersøgelse må vi derfor konkludere, at vi ikke kan slutte, at mænd generelt har markant højere fortrolighed med computer/internet, men det er rimeligt at konkludere, at den generelt *er* højere.

10.5 Konklusion på markedsanalyse

Vi har nu undersøgt vælgerinteressen for elektronisk afstemning — hovedresultatet viste, at omtrent 50 % af respondenterne ønskede at stemme via internettet, 30 % ønskede ikke, mens 20 % svarede måske. Desuden blev det vurderet, at der er en sammenhæng mellem fortroligheden med computer/internet og interessen for elektronisk afstemning. Ud fra vores forholdsvis begrænsede undersøgelse var det ikke muligt at se nogen sammenhæng mellem demografiske oplysninger og interessen for EA. Med hensyn til demokratisk engagement og interessen for elektronisk afstemning konstaterede vi ingen sammenhæng.

Sammenholdt med resultaterne i Afsnit 10.2, kan vores konklusion på markedsanalysen formuleres som følger

- Indførsel af elektronisk afstemning harmonerer godt med den nuværende regerings IT-målsætninger. Det fremgår af [for videnskab teknologi og udvikling, 2002], at den nye danske IT-politik sigter mod værdier for den enkelte, for virksomhederne og samfundet. Vi har redegjort for, at vores system giver mulighed for øget bekvemmelighed og højere afstemningsdeltagelse — og dette må i høj grad siges at være værdier både for den enkelte og for demokratiet.
- Muligheden for lige adgang til computere og internet er en problematik, som vi må forholde os til før indførelse af EA. Alle vælgere bør have samme mulighed for at anvende EA. Statistikkerne viser en tendens til udjævning af digitale kløfter, og stigende adgang til internettet på tværs af aldersgrupperne. Denne udvikling bør hjælpes på vej af politiske initiativer.

  Samtidig må vi forholde os til den mistro, som naturligt vil eksistere i forbindelse med en så banebrydende teknologi, f.eks. gennem længere offentlig debat og stor åbenhed i dette omfattende projekt.
- Vi vurderer, at der er vælgerinteresse til stede. Hvorvidt denne er tilstrækkelig for at indføre elektronisk afstemning, kan ikke umiddelbart vurderes — det afhænger i høj grad af de politiske forventninger til EA. Ønsker man at udbrede

det digitale demokrati på en stor skala, er 50% langtfra nok — ønsker man at supplere de nuværende processer med EA og herigennem hjælpe marginalgrupperne, er 50% sikkert rigeligt.

Ud fra vores målsætning om at skabe et sådant supplement mener vi, at 50% er tilstrækkeligt for videre arbejde med ideen allerede nu.

Kapitel 11

Konklusion

Vi har i denne rapport undersøgt muligheden for indførelse af elektronisk afstemning via internettet til nationale valg og afstemninger i Danmark og vurderet, hvorvidt det er relevant at arbejde videre med et sådant projekt — dels m.h.t. de teknologiske muligheder, dels m.h.t. vælgernes interesse for en sådan løsning.

Indledende redegjorde vi for de mange interessante perspektiver i elektronisk afstemning, primært den øgede bekvemmelighed og de forbedrede muligheder for marginaliserede grupper.

Det blev fremhævet, at konstruktionen af et system til elektronisk afstemning ikke kunne sidestilles med ordinær informationsudveksling, eftersom afstemningsprocessen er en *handling*. Denne iagttagelse dannede grundlag for opstillingen af en mindre række basale specifikationer baseret på videnskabelige, entydige krav til et afstemningssystem.

Ud fra specifikationerne argumenterede vi for, at et afstemningssystem baseret på kryptografiske metoder var intuitivt den mest oplagte løsning såfremt grundlæggende krav som anonymitet og entydighed af stemmen skulle være opfyldte i et system, der skal kunne integreres med internettets struktur.

Herefter fulgte en præsentation af en række nødvendige kryptografiske elementer, og på baggrund af gruppeteoretiske konstruktioner gjorde vi rede for, at eksponentiation af frembringere i gruppen $(\mathbb{Z}/p\mathbb{Z})^*$ formentlig er en en-vejsfunktion. Dette blev anvendt i formuleringen af et kryptosystem baseret på vanskeligheden ved beregning af diskrete logaritmer — ElGamal kryptosystemet. Dette kryptosystem viste sig at give en række fordele i forbindelse med en afstemningsprotokol.

Vi redegjorde for, hvordan ElGamal kryptosystemet kan udvides til et *fejltolerant* (t, n)*-tærskel kryptosystem*, der sikrer en fordeling af tillid blandt valgautoriteterne. Dette blev gjort ud fra principperne i deling af hemmeligheder ved interpolation af polynomier og omformningen af disse til *distribuerede, verifcérbare metoder*, hvor generering af nøgler og dekryptering foregår fordelt på n valgautoriteter hvor op til t af disse kan være korrupte eller fejlagtige. Som baggrund herfor opstillede vi en *zero-knowledge* protokol til bevis for kendskab til diskrete logaritmer og redegjorde for, at denne beviskonstruktion sikrer, at valgresultatet er verficérbart for enhver observatør.

Disse teoretiske metoder omformede vi til en afstemningsprotokol, som vi gennem en omfattende sikkerhedsvurdering argumenterede for opfylder størstedelen af de først opstillede kravsspecifikationer.

Blandt manglerne var primært, at det i protokollen er muligt at "købe stemmer" — og beregningskompleksiteten ved f.eks. folketingsvalg er eksponentiel i antallet af kandidater, hvilket gør protokollen vanskeligt anvendelig på en større skala.

I forbindelse med ja/nej-afstemninger og regulære valg på mindre skala er beregningskompleksiteten for alle parter acceptabel og sikrer effektivitet. Desuden muliggør protokollens meget generelle opbygning implementering på en lang række digitale kommunikationsapparater, d.v.s. mobilitet er også til stede.

Samlet konkluderede vi, at protokollen i dens nuværende form er et fortræffeligt *grundlag* for videreudvikling af et elektronisk afstemningssystem, der skal kunne fungere under *alle* typer afstemninger og valg. I forbindelse med f.eks. ja/nej-afstemninger og mindre valg, kan protokollen anvendes direkte. Det blev dog påpeget, at elektronisk afstemning via internettet uanset implementation indeholder nogle teoretisk uoverkommelige problemer i forhold til traditionel afstemning. Sikring af den demokratiske ret vil *aldrig* kunne foregå med samme sikkerhed som under traditionel afstemning og valg.

Efterfølgende undersøgte vi gennem en markedsanalyse de yderligere forudsætninger for en realisering af elektronisk afstemning. Vi påpegede, at den store politiske interesse for digitalisering af kommunikation mellem borgeren og det offentlige gav gode muligheder for et projekt som netop elektronisk afstemning, samt en række af perspektiverne (bl.a. øget bekvemmelighed) var i overensstemmelse med visionerne fra regeringens nyeste IT- og telepolitiske redegørelse. Tilsvarende vurderede vi, at de øvrige forudsætninger var gode i Danmark — en stor del af befolkningen vil have mulighed for elektronisk afstemning via internettet.

I tilknytning hertil undersøgte vi vælgerinteressen for elektronisk afstemning og sammenhænge, som vi forventede havde indflydelse på denne interesse. Dette blev gjort ud fra en mindre spørgeskemaundersøgelse udført i Aalborg midtby. Resultaterne viste, at respondenter, der ikke ønskede at stemme via internettet generelt havde lavere fortrolighed med computere og internet end respondenter, der var positive overfor denne mulighed. Ud fra resultaterne var det ikke muligt at slutte noget endegyldigt om interessen i relation til alder og køn.

Samlet vurderer vi, at elektronisk afstemning vil være en oplagt mulighed indenfor overskuelig fremtid, og anbefaler, at et sådant system videreudvikles som *supplement* til traditionel afstemning. Blandt de vigtigste perspektiver er øget bekvemmelighed og øget variation i valghandlingen, samt bedre mulighed for deltagelse for marginaliserede grupper. De kortsigtede besparelsesaspekter bør dog ikke vægte i overvejelserne, eftersom elektronisk afstemning kun kan blive en realitet ved større udstyrsinvesteringer og en omfattende oplysningskampagne sideløbende med de faste udgifter til traditionelle afstemningsformer. På længere sigt kan elektronisk afstemning imidlertid godt vise sig at give økonomiske gevinster efterhånden, såfremt denne afstemningsform bliver tilstrækkelig udbredt og accepteret. Denne anbefaling er dog ikke uden betænkninger — som påpeget er den manglende kontrol i forbindelse med elektronisk afstemning en alvorlig svaghed ved sådanne systemer; og kun gennem

en større politisk debat kan der dannes et solidt beslutningsgrundlag for, om denne svaghed opvejes af de indlysende fordele ved elektronisk afstemning.

11.1 Perspektivering og muligheder

Efter markedsanalysen og på baggrund af opstillingen af et afstemningssystem er det rimeligt at spørge — hvad er egentlig teknologiens dybere betydning i demokratiets tjeneste?

Vi omtalte allerede i starten af rapporten, at afstemning og valg er en betydningsfuld del af den enkelte borgers demokratiske færden. Ganske vist oplever vi for tiden en stigende digitalisering af de offentlige services, men i sig selv er det ikke et argument for indførelse af EA. Afstemning og valg er jo et eksempel på en situation, hvor møde mellem myndigheder og borger bliver eksistentielt — et afstemningsresultat medfører en direkte indgriben i den enkeltes hverdag. I det 21. århundrede er bekvemmelighed en værdi, der vægtes højt og en kobling mellem bekvemmelighed og demokratiudøvelse er et attraktivt supplement til eksisterende metoder — men næppe en erstatning for den traditionelle valghandling, der repræsenterer selve det grundlæggende i mødet mellem det ekstremt individuelle og det store kollektiv. Internettet er i dag muligheden for kommunikation, men langtfra en ideel ramme alene for en så betydende handling som valghandlingen — at erstatte den rituelle handling med to museklik er farligt og indebærer en alvorlig risiko for, at selve demokratiet fortaber sig i kommunikationsstrømmen.

I det hele taget er det en højrelevant diskussion, hvordan vi ønsker, at informationsteknologien skal anvendes i demokratiet fremover. I [Ministerråd, 1999] omtales, at informationsteknologien vil kunne styrke et svækket demokrati ved bl.a. øget indflydelse på politiske beslutninger og et styrket offentlighedsprincip. Her vil elektronisk afstemning i høj grad kunne være en hjælp som middel til at sikre et gennemskueligt demokrati i en tid, hvor den politiske debat ofte bevæger sig på et så abstrakt plan, at det egentlige beslutningsgrundlag i høj grad forplumres for borgeren.

Man kunne forestille sig omfattende meningstilkendegivelser som pejlemærker for politiske beslutninger; herigennem vil EA kunne bidrage til en øget føling med befolkningens krav og forventninger helt ned på lokalplan. Samtidig vil den politiske beslutningsproces være mere nærværende for den enkelte, bidrage til en nuanceret og engageret offentlig debat samt modarbejde et pseudo-demokrati, hvor informationsteknologien blot giver en illusion af øget demokratisk kontakt (jf. [Ministerråd, 1999]).

En sådan udvikling vil gøre det muligt at skabe lettilgængelige digitale hybrider på tværs af de demokratiske kommunikationsformer, en mellemting mellem folkelig debat og den bindende afstemning, der kan anvendes på alle politiske niveauer.

Det er ikke kun et spørgsmål om at gøre de rigtige ting — det er i lige så høj grad et spørgsmål om at gøre tingene rigtigt (ifølge den amerikanske filosof Peter F. Drucker). Elektronisk afstemning er en reel og oplagt mulighed — men hvordan skal vi bruge den?

Appendiks A

Polynomier over vilkårlige legemer

I dette appendiks vil vi kort redegøre for begrebet *legemer* og *polynomier over vilkårlige legemer*. Vi vil påpege legemesstrukturen af $\mathbb{Z}/p\mathbb{Z}$, et resultat, der første gang anvendes i Afsnit 6.3.

Ydermere vil vi bevise, at et polynomium af grad n over et legeme $\mathbb{F}$ maksimalt har n rødder. Bl.a. dette resultat samt den generelle teori om polynomier anvendes i Afsnit 6.3. Ydermere anvendes resultatet kort i beviset for, at den multiplikative gruppe $(\mathbb{Z}/p\mathbb{Z})^*$ er cyklisk, jf. Afsnit 5.2.3.

Vi vil først indføre det abstrakte begreb *et legeme*. De velkendte legemer er mængder som $\mathbb{R}, \mathbb{Q}$ og $\mathbb{C}$ — men det viser sig, at egenskaberne ved disse mængder kan defineres generelt.

DEFINITION A.1 ***Legeme***
Et legeme er en ikke-tom mængde $\mathbb{F}$ med to kompositioner $+$ og $*$, således at $(\mathbb{F}, +)$ og $(\mathbb{F}\backslash\{0\}, *)$ begge er abelske grupper.
Ydermere er de to operationer forbundet ved den distributive lov

$$a * (b + c) = a * b + a * c, \qquad \text{for alle} \quad a, b, c \in \mathbb{F}.$$

I det følgende vil vi blot skrive $a * b$ som ab. En lang række af regneregler for legemer følger direkte af regneregler for grupper, men det er nødvendigt at opstille yderligere regler for forbindelsen mellem addition og multiplikation. Der gælder følgende, idet $a, b \in \mathbb{F}$

- $a \cdot 0 = 0$.
- $a \neq 0 \wedge b \neq 0 \Rightarrow ab \neq 0$.
- $-(-a) = a$.
- $a(-b) = (-a)b = -ab$.

- $(-a)(-b) = ab$.

For bevis herfor jf. [Beachy and Blair, 1996, Afsnit 4.1].

EKSEMPEL A.1
Mængden af restklasser modulo et primtal p, $\mathbb{Z}/p\mathbb{Z}$, er et legeme. Dette resultat følger af regnereglerne for restklasser samt egenskaberne for den underliggende additive gruppe og multiplikative gruppe.

◆

Vi vil nu tilsvarende definere polynomier generelt.

DEFINITION A.2 ***Polynomium***
Lad $\mathbb{F}$ være et legeme. Et polynomium i én variabel *over $\mathbb{F}$ er et udtryk på formen*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \qquad a_i \in \mathbb{F}, \quad i = 0, 1, 2, \ldots, n.$$

Såfremt $a_n \neq 0$ siges polynomiet at have graden n*, Koefficienten a_n siges at være den* ledende koefficient*. Graden af et polynomium $f(x)$ skrives* $\deg f(x)$*. Mængden af alle polynomier over $\mathbb{F}$ skrives $\mathbb{F}[x]$.*

DEFINITION A.3 ***Addition og multiplikation***
Lad $f(x), g(x) \in \mathbb{F}[x]$ være givet ved

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0. \\ g(x) &= b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + a_0. \end{aligned}$$

Vi definerer da summen *af $f(x)$ og $g(x)$ som*

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots .$$

Tilsvarende defineres produktet *af $f(x)$ og $g(x)$*

$$f(x)g(x) = c_{n+m}x^{m+n} + c_{n+m-1}x^{n+m-1} + \cdots + c_0,$$

hvor

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}, \qquad 0 \leq k \leq n + m.$$

Ud fra ovenstående definition er det en simpel beregningsopgave at vise, at disse operationer opfylder de samme forhold, som f.eks. naturlige tal. Det betyder, at den associative, kommutative og distributive lov gælder, samt at der eksisterer neutrale elementer (neutral elementerne i legemet $\mathbb{F}$ — polynomier af grad 0) samt additive inverse. Bemærk, at multiplikative inverse *ikke* er defineret.

DEFINITION A.4 ***Rod i polynomium***
Lad $\mathbb{F}$ være et legeme, og lad $f(x) \in \mathbb{F}[x]$. Et element $c \in \mathbb{F}$ siges at være en rod i $f(x)$, hvis c er en løsning til ligningen $f(x) = 0$.

I ovenstående anvender vi et polynomiums egenskaber som *funktion* til at definere rødder. Bemærk, at der er afgørende forskel mellem polynomier som abstrakte elementer i $\mathbb{F}[x]$ og *polynomiumsfunktioner* fra $\mathbb{F}$ ind i $\mathbb{F}$ (det er f.eks. muligt, at to forskellige polynomier definerer den samme polynomiumsfunktion, jf. [Beachy and Blair, 1996, p. 164].

Vores mål er nu at vise, at et polynomium af grad n over et arbitrært legeme højest har n rødder. Til dette formål vil vi anvende en sætning, der i høj grad ligner divisionsalgoritmen for heltal, jf. Sætning 5.1, blot her for polynomier.

LEMMA A.1 ***Grad af produkt af polynomier***
Lad $f(x), g(x) \in \mathbb{F}[x]$, $g(x) \neq 0$. Så er

$$\deg f(x) \deg g(x) = \deg f(x) + \deg g(x).$$

Bevis:
Resultatet følger umiddelbart ved udregning ud fra reglen for multiplikation. ■

SÆTNING A.1 ***Division af polynomier***
Lad $\mathbb{F}$ være et legeme, og lad $f(x), g(x) \in \mathbb{F}[x]$, $g(x) \neq 0$. Så findes der entydige polynomier $q(x), r(x) \in \mathbb{F}$, $\deg r(x) < \deg g(x)$, således at

$$f(x) = q(x)g(x) + r(x).$$

Bevis:
Lad $n = \deg f(x)$ og $m = \deg g(x)$.
Først bemærkes, at det udelukkende er nødvendigt at vise resultatet generelt for tilfældet $m \leq n$. Dette følger, da $m > n \Rightarrow f(x) = 0 \cdot q(x) + f(x)$, og sætningen gælder da.

Vi anvender nu induktion på graden af f.

$n = 0$*:*
Vi har, $n = 0 \Rightarrow m = 0$. D.v.s. $f(x), g(x) \in \mathbb{F}$, og får $f(x) = (f(x)g(x)^{-1})g(x)$.

$n > 0$*:*
Vi har

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0. \\ g(x) &= b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0. \end{aligned}$$

Lad nu

$$T(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x).$$

Da er enten $\deg T(x) = 0$ eller $\deg T(x) < n$, eftersom sidste led på højresiden vil være leddet af højeste grad i $f(x)$.

Af induktionshypotesen findes der polynomier $q(x)$ og $r(x)$, så

$$T(x) = q(x)g(x) + r(x),$$

hvor $0 \leq \deg r(x) < \deg g(x)$. Da opfylder $f(x) = (\frac{a_n}{b_m}x^{n-m} + q(x))g(x) + r(x)$ antagelsen.

Entydighed vises som følger. Antag, at $f(x) = q(x)g(x)+r(x) = q'(x)g(x)r'(x)$. Da fås $(q(x) - q'(x))g(x) = r'(x) - r(x)$ — eftersom graden af venstresiden er mindre end $\deg g(x)$, følger af Lemma A.1 at $\deg(q(x) - q'(x))g(x)) = \deg(r'(x) - r(x))$, hvilket kun er muligt, hvis $q(x)-q'(x) = 0 \Leftrightarrow q(x) = q'(x)$, og dermed $r(x) = r'(x)$.

Sætningen er da bevist. ■

KOROLLAR A.1
Lad $f(x) \in \mathbb{F}[x]$, $f(x) \neq 0$. Hvis a er et nulpunkt i f, så er

$$f(x) = (x - a)q(x).$$

Bevis:
Af sætning A.1 følger, at der eksisterer et polynonium $q(x)$, således at

$$f(x) = (x - a)q(x) + r,$$

hvor $r < \deg x = 1$. Derfor er $f(a) = 0 = r$, og sætningen er bevist. ■

KOROLLAR A.2
Lad $f(x) \in \mathbb{F}[x]$, $f(x) \neq 0$, og lad $\deg f(x) = n$. Så har $f(x)$ højest n rødder.

Bevis:
Vi beviser dette ved induktion på graden af n.
For $n = 0$ holder påstanden, idet $f(x)$ pr. definition da blot er en konstant forskellig fra nul.

Antag nu, at påstanden er sand for alle polynomier $f(x)$ af grad $n - 1$.

Hvis $f(x)$ ingen rødder har, gælder resultatet umiddelbart.

Omvendt, antag at $f(x)$ har roden a. Da følger af A.1, at

$$f(x) = (x - a)q(x),$$

hvor $\deg q(x) = \deg f(x) - 1 = n - 1$. Af induktionshypotesen har $q(x)$ maksimalt $n - 1$ rødder, og det følger, at $f(x)$ har højest n rødder. ■

Appendiks B

Spørgeskema

Vi er en gruppe 1. års matematik-studerende ved Aalborg Universitet, som arbejder på et projekt omhandlende elektronisk afstemning. Elektronisk afstemning vil kunne give mulighed for at afvikle bl.a. folketingsvalg via Internettet.
I denne forbindelse vil vi gerne høre Deres mening om denne måde at afvikle valg på.

Køn?
☐ Kvindelig dansk statsborger ☐ Mandlig dansk statsborger

Alder?
☐ 18-30 ☐ 31-50 ☐ 51-70 ☐ 71-?

Hvor meget anvender De computer i Deres hverdag?
☐ dagligt ☐ ugentligt ☐ af og til ☐ aldrig

Har De prøvet at udveksle fortrolige oplysninger, såsom selvangivelse, homebanking, handel o.s.v. via Internettet?
☐ ofte ☐ flere gange ☐ enkelte gange ☐ aldrig

I hvor høj grad har De tillid til at udveksle disse fortrolige oplysninger via Internettet?
☐ i høj grad ☐ en del ☐ i mindre grad ☐ slet ikke ☐ ved ikke

Hvor vigtigt er det for Dem at deltage i folketingsvalg?
☐ i høj grad ☐ en del ☐ i mindre grad ☐ slet ikke ☐ ved ikke

Hvis det var muligt at stemme til folketingsvalget via Internettet, ville De så gøre det?
☐ ja ☐ nej ☐ måske ☐ ved ikke

Tak for hjælpen !

Appendiks C

Resultater for undersøgelse

Køn	Alder	Fortrolighed	Demokratisk engagement	Holdning til EA
Mand	*18-30*	6	2	*ja*
Mand	*18-30*	8	2	*ja*
Mand	*18-30*	8	1	*ja*
Mand	*18-30*	8	−1	*ja*
Mand	*18-30*	7	2	*ja*
Mand	*18-30*	8	1	*ja*
Mand	*18-30*	8	2	*ja*
Mand	*18-30*	2	2	*nej*
Mand	*18-30*	7	2	*nej*
Mand	*18-30*	1	1	*nej*
Mand	*18-30*	−1	2	*nej*
Mand	*18-30*	7	2	*nej*
Mand	*18-30*	7	2	*måske*
Mand	*18-30*	7	1	*måske*
Mand	*18-30*	7	2	*måske*
Mand	*18-30*	7	1	*måske*
Mand	*31-50*	3	2	*ja*
Mand	*31-50*	8	1	*ja*
Mand	*31-50*	6	2	*ja*
Mand	*31-50*	8	2	*ja*
Mand	*31-50*	1	1	*ja*
Mand	*31-50*	3	2	*nej*

Tabel C.1: Spørgeskemaresultater

Køn	Alder	Fortrolighed	Demokratisk engagement	Holdning til EA
Mand	*31-50*	2	2	*nej*
Mand	*51-70*	0	2	*ja*
Mand	*51-70*	0	2	*ja*
Mand	*51-70*	8	2	*ja*
Mand	*51-70*	−2	−1	*nej*
Mand	*51-70*	7	2	*nej*
Mand	*51-70*	0	2	*nej*
Mand	*51-70*	−2	2	*måske*
Mand	*51-70*	3	2	*måske*
Mand	*71-?*	−2	−1	*ja*
Mand	*71-?*	0	2	*nej*
Kvinde	*18-30*	8	1	*ja*
Kvinde	*18-30*	0	−1	*ja*
Kvinde	*18-30*	2	−1	*ja*
Kvinde	*18-30*	5	2	*ja*
Kvinde	*18-30*	1	−2	*ja*
Kvinde	*18-30*	6	2	*ja*
Kvinde	*18-30*	3	2	*ja*
Kvinde	*18-30*	3	2	*ja*
Kvinde	*18-30*	3	−1	*nej*
Kvinde	*18-30*	−1	2	*nej*
Kvinde	*18-30*	0	2	*nej*
Kvinde	*18-30*	2	2	*nej*
Kvinde	*18-30*	5	2	*nej*
Kvinde	*18-30*	1	2	*måske*
Kvinde	*18-30*	5	−1	*måske*
Kvinde	*18-30*	5	1	*måske*
Kvinde	*31-50*	0	2	*ja*
Kvinde	*31-50*	8	2	*ja*
Kvinde	*31-50*	1	2	*ja*
Kvinde	*31-50*	0	2	*ja*
Kvinde	*31-50*	0	1	*nej*
Kvinde	*31-50*	−1	2	*nej*

Tabel C.2: Spørgeskemaresultater

Køn	Alder	Fortrolighed	Demokratisk engagement	Holdning til EA
Kvinde	*51-70*	8	−1	*ja*
Kvinde	*51-70*	2	2	*ja*
Kvinde	*51-70*	0	2	*ja*
Kvinde	*51-70*	7	2	*ja*
Kvinde	*51-70*	2	2	*ja*
Kvinde	*51-70*	4	2	*nej*
Kvinde	*51-70*	3	2	*nej*
Kvinde	*51-70*	1	1	*nej*
Kvinde	*51-70*	1	2	*nej*
Kvinde	*51-70*	−2	−1	*nej*
Kvinde	*51-70*	−2	2	*nej*
Kvinde	*51-70*	3	2	*måske*
Kvinde	*71-?*	−2	−1	*ja*
Kvinde	*71-?*	0	2	*ja*
Kvinde	*71-?*	1	2	*nej*

Tabel C.3: Spørgeskemaresultater

Litteratur

F. R. Andersen, K. Jetsen, P. Schmatz, and T. Trojel. *International Markedsføring*. Trojka, August 2000.

J. A. Beachy and W. D. Blair. *Abstract Algebra*. Waveland Press, Inc., second edition, 1996.

J. A. Buchmann. *Introduction to Cryptography*. Undergraduate Texts in Mathematics. Springer, 2000.

R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky. Deniable encryption. *Lecture Notes in Computer Science*, 1294, 1997.

D. Chaum and T. Pedersen. Wallet databases with observers. In *Advances in Cryptology — Proceedings of EUROCRYPT'92*. Springer-Verlag, 1992.

R. Cramer, R. Gennaro, and B. Schoenmakers. A secure and optimally efficient multi-authority election scheme. In *Advances in Cryptology — Proceedings of EUROCRYPT'97*. Springer-Verlag, 1997.

R. Crandall and C. Pomerance. *Prime Numbers — A Computational Perspective*. Springer, 2001.

I. Damgaard. Commitment schemes and zero-knowledge protocols. Forelæsningsnoter, 2002a.

I. Damgaard. On sigma protocols. Forelæsningsnoter, 2002b.

I. Damgaard and M. Jurik. A generalisation, a simplification and some applications of paillier's probabilistic public-key system, 2001.

T. Elgamal. A public-key cryptosystem and a signature scheme based on discrete logarithms. In *Advances in Cryptology — Proceedings of CRYPTO'84*. Springer Verlag, 1985.

Ministeriet for videnskab teknologi og udvikling. It- og telepolitisk handlingsplan 2002, Maj 2002.

R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Secure distributed key generation for discrete-log based cryptosystems. In *Theory and Application of Cryptographic Techniques*, pages 295–310, 1999.

S. Goldwasser and M. Bellare. Lecture notes on cryptography. elektronisk format, august 2001.

Kommunernes Landsforening. E-demokrati, Oktober 2001. URL `http://www.kl.dk/244164/`. Skrivelse.

D. C. Lay. *Linear Algebra and its Applications*. Addison-Wesley, 2 edition, 2000.

PLS RAMBØLL Management. Den digitale borger 2001, 2001.

A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

Nordisk Ministerråd. Rapport om it og demokrati og elektronisk handel, august 1999.

C. Andrew Neff. The business of electronic voting. Technical report, VoteHere, 2001.

P. Paillier. Public-key cryptosystems based on composite degree residue classes. In *Advances in Cryptology — Proceedings of EUROCRYPT'99*. Springer Verlag, 1999.

T. Pedersen. *Distributed Provers and Verifiable Secret Sharing Based on the Discrete Logarithm Problem*. PhD thesis, Aarhus Universitet, marts 1992.

K. H. Rosen. *Discrete Mathematics and Its Applications*. WCB/McGraw-Hill, fourth edition, 1999.

C.P. Schnorr. Efficient signature generation by smart cards. Technical report, Universität Frankfurt, marts 1991.

B. Schoenmakers. Fully auditable secret ballot elections, 2000.

A. Shamir. How to share a secret. *Communications of the ACM 22*, pages 612–613, 1979.

Danmarks Statistik. *Statistisk Årbog, første kvartal 2002*. Danmarks Statistik, april 2002.

A. Thorup. Matematik 2al, algebra — 2. udgave. Forelæsningsnoter til kurset 2AL på Københavns Universitet, 1998.

J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 1999.