

# Basismethoden Cryptografie

**dr.ir. J.C.A. van der Lubbe**

Vakgroep Informatietheorie  
Faculteit der Elektrotechniek  
Technische Universiteit Delft

# Voorwoord

Door de voortschrijdende technologische ontwikkelingen heeft de automatisering in alle lagen van onze maatschappij zijn intrede gedaan, alsmede zijn onze communicatiemogelijkheden steeds groter geworden. Op grote schaal wordt er gebruik gemaakt van methoden voor geautomatiseerde gegevensverwerking en datacommunicatie. Voorbeelden zijn er te over: medische en fiscale computerbestanden, automatisch betaalverkeer, beeldtelefoon, abonnee-tv, fax-verkeer, tele-shopping, wereldwijde computernetwerken etc. etc. Bij al deze voorbeelden is er sprake van een toenemende behoefte voor de beveiliging van opslag en transport van informatie. De redenen voor het optreden van deze behoefte zijn van velerlei aard. Beveiliging kan noodzakelijk zijn om economische belangen te beschermen, om fraude tegen te gaan of om de privacy van de burger te waarborgen etc.

Cryptografie is de wetenschap die zich in meest algemene zin bezighoudt met methoden voor de beveiliging van opslag en transport van informatie.

In het voor u liggende boek zal aandacht besteed worden aan de basismethoden voor de beveiliging van opslag en transport van informatie, zoals deze momenteel ontwikkeld zijn en gehanteerd worden. Het is het doel van dit boek de lezer vertrouwd te maken met de diverse mogelijkheden die cryptografie biedt, maar zeker ook met de onmogelijkheden van en de randvoorwaarden voor het gebruik van cryptografie.

Het boek is bedoeld voor een ieder die op een of andere manier betrokken is bij beveiliging en beveiligingsaspecten van gegevensverwerking en communicatie: ingenieurs, systeemontwerpers, applicatieprogrammeurs, informatie-analisten, security officers, EDP-auditors etc.

Het boek is ontstaan uit colleges die de schrijver de laatste jaren heeft gegeven aan studenten van de Faculteiten Elektrotechniek, Technische Wiskunde en Informatica, Technische Bestuurskunde en Technische Natuurkunde van de Technische Universiteit Delft en op basis van de bankgerichte cursus Cryptografie verzorgd door TopTech Studies, welke verantwoordelijk is voor het postdoctorale onderwijs van de Technische Universiteit Delft, en waaraan de schrijver als directeur van genoemde cursus is verbonden.

De schrijver wil van de gelegenheid gebruik maken dr.ir. J.H. Weber te bedanken, met wie hij gedurende een aantal jaren de colleges Cryptografie aan de Technische Universiteit Delft heeft verzorgd. Verder zou ondergetekende alle collega's van de

TopTech cursus Cryptografie willen bedanken, in het bijzonder ir. R.E. Goudriaan van de Internationale Nederlandse Bank, omdat ze schrijver dezes veel geleerd hebben ten aanzien van de praktische aspecten van het gebruik van cryptografie.

J.C.A. van der Lubbe  
januari 1994

## Voorwoord bij de tweede druk

In deze nieuwe druk zijn paragrafen over IDEA (International Data Encryption), openbare-sleutelsystemen gebaseerd op elliptische curven, DSA (Digital Signature Algorithm) en fair cryptosystemen toegevoegd. Voorts is een aantal kleine verbeteringen aangebracht.

J.C.A. van der Lubbe  
januari 1997

# Inhoud

VOORWOORD	5
BEKNOPTE INHOUD	9
NOTATIES	11
1. INLEIDING CRYPTOGRAFIE	13
1.1. Cryptografie en cryptanalyse	13
1.2. Beveiligingsaspecten	15
1.3. Cryptanalytische aanvallen	20
2. KLASSIEKE CIJFERSYSTEMEN	22
2.1. Inleiding	22
2.2. Transpositiecijfers	22
2.3. Substitutiecijfers	26
2.4. De Hagelin-machine	31
2.5. Statistiek en cryptanalyse	36
3. DE INFORMATIETHEORETISCHE BENADERING	49
3.1. Het algemene schema	49
3.2. Hoeveelheid informatie en absolute veiligheid	50
3.3. De uniciteitsafstand	56
3.4. Foutkans en veiligheid	60
3.5. Praktische veiligheid	70
4. DE DATA ENCRYPTION STANDARD	72
4.1. Het DES-algoritme	72
4.2. Eigenschappen van DES	83
4.3. Alternatieve beschrijvingen	89
4.4. Analyse van DES	95
4.5. De modes van DES	99
4.6. Toekomst van DES	105
4.7. IDEA (International Data Encryption Algorithm)	107
5. SCHUIFREGISTERS	110
5.1. Stroom- en blokvercijfering	110
5.2. Automatentheorie	112
5.3. Schuifregisters	115
5.4. Random-eigenschappen van schuifregister reeksen	118
5.5. De genererende functie	126

5.6. Cryptanalyse met betrekking tot lineair-teruggekoppelde schuifregisters	130
5.7. Niet-lineaire schuifregisters	136
6. OPENBARE-SLEUTELSYSTEMEN	143
6.1. Inleiding	143
6.2. Het RSA-systeem	144
6.3. Het knapzakstelsel	155
6.4. Het breken van het knapzakstelsel	158
6.5. Openbare-sleutelsystemen gebaseerd op elliptische curven	163
7. AUTHENTICATIE	169
7.1. Protocollen	169
7.2. Berichtintegriteit met behulp van Hash-functies	174
7.3. Bronauthenticatie met symmetrisch algoritme	181
7.4. Berichtauthenticatie met een 'Message Authentication Code' (MAC)	184
7.5. Berichtauthenticatie met digitale handtekeningen	185
7.6. Zerokennistechnieken	192
8. SLEUTELBEHEER EN NETWERKBEVEILIGING	202
8.1. Aspecten van sleutelbeheer	202
8.2. Sleuteldistributie met asymmetrische systemen	205
8.3. Sleuteldistributie met symmetrische algoritmen	207
8.4. Netwerkbeveiliging	210
8.5. Fair cryptosystemen	213
BIJLAGE A. DE INFORMATIEMAAT VAN SHANNON	217
BIJLAGE B. BEELDVERCIJFEREN	221
LITERATUUR	228
LIJST VAN FIGUREN	234
LIJST VAN TABELLEN	237
TREFWOORDENREGISTER	238

# Beknopte inhoud

In Hoofdstuk 1 wordt vooral aandacht besteed aan de rol die cryptografie speelt binnen de totale beveiligingsproblematiek. De verschillende doelen van beveiliging worden beschouwd alsmede wordt een eerste overzicht gegeven van de cryptografische methoden die daarvoor gehanteerd kunnen worden.

In Hoofdstuk 2 komen de meer klassieke cijfersystemen aan de orde, zoals transpositie en substitutiecijfers. Tevens wordt enige aandacht besteed aan de methoden die cryptanalisten ('krakers') toepassen om genomen beveiligingsmaatregelen te doorbreken.

In vele gevallen valt of staat de sterkte van cryptografische algoritmen met de mate waarin veiligheid bereikt kan worden. Het begrip veiligheid zelf is echter verre van eenduidig. In Hoofdstuk 3 wordt met behulp van informatietheorie nagegaan wat er met veiligheid bedoeld wordt en hoe deze bereikt kan worden.

Een van de thans meest toegepaste cryptografische algoritmen, gebaseerd op vercijfering op basis van geheime sleutels, is het DES-algoritme. De principes van dit algoritme worden gegeven in Hoofdstuk 4.

In Hoofdstuk 5 wordt aandacht geschonken aan schuifregisters voor het opwekken van pseudo-random reeksen, welke laatste gebruikt kunnen worden voor het genereren van sleutels dan wel voor het vercijferen van bitstromen. Het begrip randomness wordt zelf ook nader bestudeerd.

Hoofdstuk 6 is gewijd aan de zogenaamde openbare-sleutel systemen; cryptografische algoritmen waarbij sprake is van een geheime en openbare sleutel. Het RSA-algoritme is hier een belangrijk voorbeeld van.

Hoofdstuk 7 is betrokken op andere soorten van beveiliging, te maken hebbend met authenticatie en integriteit. Het gaat hierbij om technieken op basis waarvan men zich ervan kan gewisselen dat een verzonden bericht ongeschonden is en dat een door zeg A verzonden bericht inderdaad van A afkomstig is etc. De verschillende methoden passeren de revue, waarbij ook digitale handtekeningen en zerokennis-technieken aan de orde komen.

In het algemeen geldt dat hoe goed de cryptografische algoritmen ook zijn, de overall veiligheid valt of staat vaak met de mate waarin de geheime sleutel geheim gehouden wordt. In Hoofdstuk 8 wordt aandacht besteed aan sleutelbeheer, dat zich bezighoudt met het veilig genereren, distribueren etc. van sleutels, alsook aan de specifieke aspecten van beveiliging van netwerken.

Ter afsluiting zijn twee bijlagen toegevoegd. Bijlage A handelt over de informatie-maat van Shannon en is bedoeld voor degenen die met het oog op Hoofdstuk 3 onvoldoende vertrouwd zijn met de informatietheoretische basisbegrippen. Bijlage B behandelt enige specifieke technieken voor het vercijferen van beelden.

# 1

## Inleiding cryptografie

### 1.1. Cryptografie en cryptanalyse

In de titel van dit boek komt het woord *cryptografie* voor. Cryptografie is een onderdeel van wat men noemt de *cryptologie*. De term cryptologie is de samentrekking van twee Griekse woorden “*cruptos*” (= verborgen) en “*logos*” (= woord, leer). Het woord cryptologie betekent dan ook letterlijk de leer van het verbergen. In zoverre behelst het de ontwikkeling van methoden om boodschappen en signalen te *vercijferen* alsook de ontwikkeling van methoden om gecijferde boodschappen te *ontcijferen*.

Ten aanzien van cryptologie kan onderscheid gemaakt worden tussen twee deelgebieden: *cryptografie* en *cryptanalyse*.

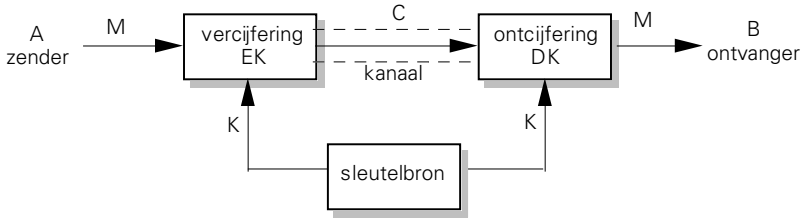
In engere zin kan cryptografie opgevat worden als dat deel van de cryptologie dat zich bezighoudt met technieken om data te versluieren of te vercijferen, waarbij veelal gebruik gemaakt wordt van geheime sleutels. Alleen degene die over de geheime sleutels beschikt is in staat de gecijferde informatie te ontcijferen. Voor ieder ander is dit in principe ondoenlijk.

Cryptanalyse is dat deel van de cryptologie dat zich bezighoudt met technieken om de gecijferde data te ontcijferen zonder a priori volledige kennis over bijvoorbeeld de sleutel. Het gaat hier om wat in het dagelijks taalgebruik ook wel aangeduid wordt met de term “kraken”.

Het spreekt voor zich dat zowel cryptografie als cryptanalyse nauw met elkaar samenhangen. Zo zal een ontwerper van cryptografische algoritmen eigenlijk alleen maar in staat zijn goede (dat wil zeggen sterke) cryptografische algoritmen te ontwikkelen als hij voldoende kennis heeft met betrekking tot de methoden en gereedschappen die door cryptanalisten gehanteerd worden. Dit geldt ook voor degene onder wiens verantwoordelijkheid bepaalde beveiligingsmaatregelen geïmplementeerd worden. Ook hij zal op de hoogte moeten zijn van de technieken die een potentiële indringer kan hanteren.

Omgekeerd geldt natuurlijk dat cryptanalyse alleen maar succesvol kan zijn als men minimaal enige kennis heeft over de toegepaste cryptografische algoritmen en methoden.

In dit boek zal de nadruk vooral liggen op cryptografie.



Figuur 1.1. Vercijfersysteem.

Om hier een eerste indruk te geven van wat een cryptografisch algoritme doet en tevens om enkele notaties te introduceren, beschouw de volgende situatie. Neem aan dat *A* (de zender) een bericht in vercijferde vorm, dat wil zeggen in geheimecode, wil versturen naar *B* (de ontvanger). Vaak wordt in de literatuur het originele bericht, ook wel genoemd de *klare tekst*, aangeduid met de letter *M* van het Engelse woord “Message”, terwijl het vercijferde bericht, ook wel geheten de *cijfertekst*, wordt aangeduid met de *C* van het Engelse “Ciphertext”. Een methode zou kunnen zijn, dat *A* daartoe gebruik maakt van een geheime sleutel *K* (van het Engelse woord Key) waarmee hij de boodschap *M* omzet in een cijfertekst *C*, welk bericht door *B* na ontvangst weer ontcijferd kan worden onder de aanname dat *B* ook beschikt over geheime sleutel *K*. Een en ander is weergegeven in figuur 1.1. *EK* geeft aan dat de boodschap vercijferd wordt met behulp van sleutel *K* (de letter *E* correspondeert met Encryptie (= vercijfering)); *DK* representeert de ontcijferoperatie (*D* van Decryptie (= ontcijfering)). In het navolgende zullen we de volgende notaties hanteren:

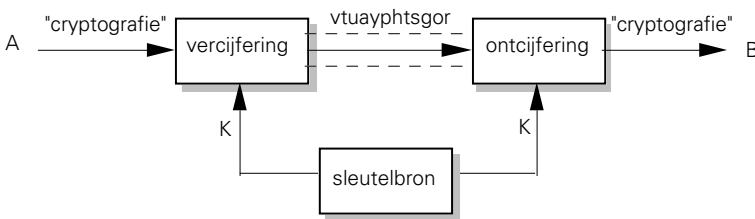
$$C = EK(M)$$

(lees: klare tekst *M* wordt met sleutel *K* vercijferd tot cijfertekst *C*)

$$M = DK(C)$$

(lees: cijfertekst *C* wordt met sleutel *K* ontcijferd tot klare tekst *M*).

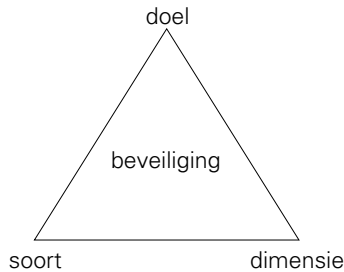
Figuur 1.2 geeft een eenvoudig voorbeeld van wat er aan zend- en ontvangzijde kan gebeuren. Het wordt aan de lezer overgelaten de gebruikte sleutel te achterhalen. Voor degene die gebruik maakt van tekstverwerkers zal dit niet al te moeilijk zijn.



Figuur 1.2. Voorbeeld van een vercijfering en ontcijfering.

## 1.2. Beveiligingsaspecten

Alvorens verder in te gaan op de methoden van de cryptografie zelf, is het hier nuttig enige aandacht te besteden aan de plaats en het gebruik van cryptografie binnen het totale beveiligingsconcept. Ten aanzien van beveiliging spelen drie aspecten een rol, welke zijn weergegeven in figuur 1.3.



Figuur 1.3. Beveiligingsaspecten.

De eerste vraag die men zich in de praktijk dient te stellen is welke het doel is van de beveiliging. Deze vraagstelling is onlosmakelijk verbonden met een adequate dreigingsanalyse, die een nauwgezet antwoord moet kunnen geven op de vragen wat men wil beveiligen en waartegen men zich wil beveiligen.

Hierna komt de vraag aan de orde welke soorten middelen voor de beveiliging daartoe gehanteerd moeten worden. Hier gaat het dus om de vragen: hoe? waarmee?

Een derde aspect welke bij het creëren van beveiligingsmaatregelen een rol speelt is wat in de figuur aangeduid wordt met de term dimensie. Daarmee wordt bedoeld of beveiligingsmaatregelen preventief gericht moeten zijn dan wel corrigerend. We komen hier later nog op terug.

Het interessante van figuur 1.3 is dat de driedeling zich ook op lagere niveaus laat doorzetten. Met betrekking tot het doel van beveiliging kunnen er een groot aantal zaken zijn, waartegen men zich wil beveiligen. Om een aantal voorbeelden te geven van waartegen men beveiligingsmaatregelen zou willen nemen:

- a. uitlezen en afluisteren van data
- b. manipuleren en modificeren van data
- c. ongeoorloofd gebruik van (computer-)netwerk
- d. aantasting van databestanden
- e. verstoren van datatransmissie
- f. verstoren van werking van apparatuur of systemen.

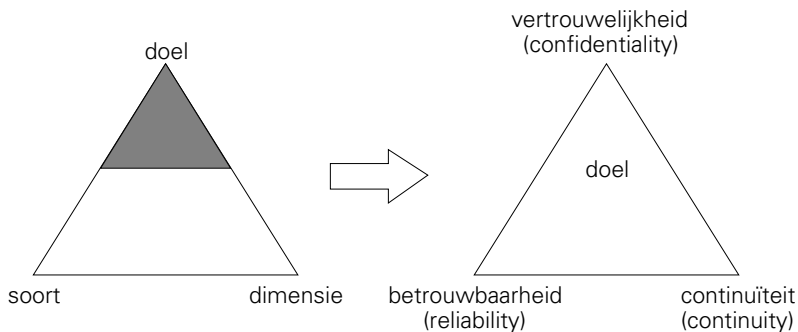
Bij a) gaat het primair om *geheimhouding, vertrouwelijkheid (confidentiality)*. Van oudsher speelt geheimhouding een belangrijke rol bij diplomatieke en militaire aangelegenheden. Vaak is er daarbij, zoals we ook hebben gezien in de vorige paragraaf, sprake van opslag van informatie of overdracht van informatie van de ene

plaats naar de andere; informatie welke men verborgen zou willen houden voor de vijand of tegenpartij. Een ander voorbeeld waar men vercijfering toepast om geheimhouding te waarborgen is bij de communicatie tussen surveillerende politiepatrouilles en de centrale meldkamer. De gevoerde gesprekken worden omgezet in een vorm, die het buitenstaanders moeilijk maakt de relevante informatie eruit te kunnen extraheren. Het kan ook voorkomen dat het feit dát er een bericht verzonden wordt op zich al vertrouwelijk is. In dat geval moeten er regelmatig dummy berichten verzonden worden om de echte berichten te camoufleren.

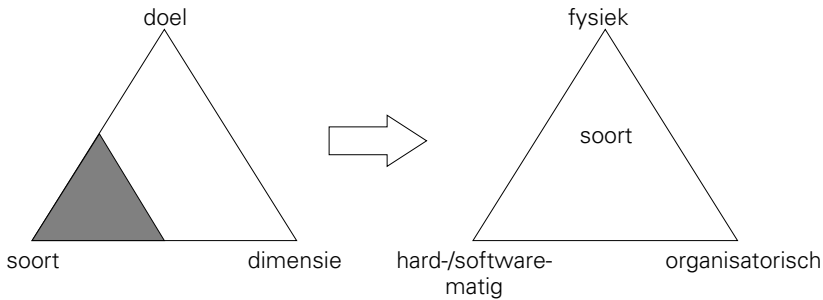
Nauw samenhangend met geheimhouding is het *sleutelbeheer* (*key management*). Het gaat hierbij om het genereren, distribueren en het opslaan van sleutels. Het is duidelijk dat hoe sterk cryptografische algoritmen ook mogen zijn, als er gewerkt wordt met geheime sleutels dan valt of staat de effectiviteit van het algoritme met de mate waarin de sleutel geheim gehouden kan worden. Een indringer die de sleutel weet te bemachtigen kan in principe de vercijferde berichten ontcijferen. Sleutelbeheer is dan ook een essentieel element in het gehele beveiligingsplan.

Bij b) t/m d) gaat het om *betrouwbaarheid* (*reliability*). Bij het elektronisch betaalverkeer zal de bank er zeker van willen zijn dat er niet met de data betreffende een financiële transactie geknoeid is, waardoor bijvoorbeeld ten onrechte hogere geldbedragen geïncasseerd kunnen worden. Men duidt dit ook wel aan met de term *integriteit*: het vaststellen van de ongeschondenheid van data. Ook zal men computer-netwerken willen beveiligen tegen binnendringers en daartoe niet-geautoriseerde gebruikers. Als men een fax-bericht ontvangt van een persoon A dan zal men de zekerheid willen hebben dat het fax-bericht inderdaad van A afkomstig is en de persoon die zich voor A uitgeeft inderdaad A is. Feitelijk zijn dit vormen van *authenticatie*: het vaststellen van de identiteit van een zich als zodanig uitgevende persoon en het vaststellen van de herkomst van gegevens.

Boven gegeven voorbeelden zijn alle voorbeelden van beveiliging waarbij de betrouwbaarheid op de voorgrond staat.



Figuur 1.4. Doelen van beveiliging.



Figuur 1.5. Soorten van beveiliging.

De punten e) en f) geven een ander doel van beveiliging weer, welke zich laat samenvatten met de term *continuïteit*. Dat wil zeggen dat men zich wil beveiligen tegen moedwillig aan te brengen verstoringen in de datacommunicatie en data-opslag. Ten aanzien van het doel van de beveiliging zijn er dus drie groepen (vergelijk figuur 1.4).

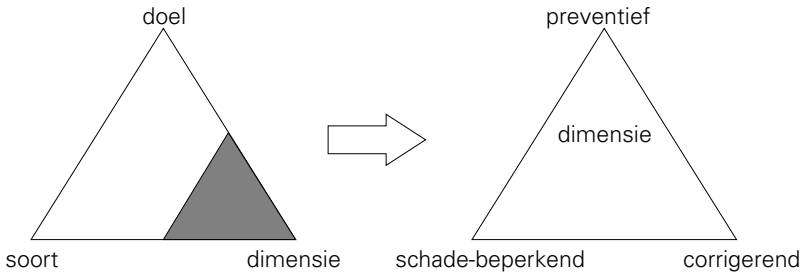
Hetzelfde geldt ook ten aanzien van het soort beveiliging dat toegepast wordt (vergelijk figuur 1.5).

De termen spreken voor zich. Bij *fysieke beveiliging* gaat het om het treffen van maatregelen om het fysiek binnen dringen in systemen, waarin bijvoorbeeld geheime sleutels opgeslagen liggen, te bemoeilijken. Dit kan door het aanbrengen van beschermingen van metaal, toepassen van bepaalde kunststoffen, aanbrengen van temperatuurs- en trillingssensoren etc.

De *hardware- en softwarematige beveiliging* is hetgene waar het in dit boek omgaat; de cryptografische algoritmen en methoden.

Hoe goed men ook fysieke beveiliging en hardware/softwarematige beveiliging kan waarborgen, zonder organisatorische maatregelen hebben ze weinig zin. *Organisatorische beveiliging* houdt in dat er randvoorwaarden gecreëerd worden waardoor inderdaad de genomen fysieke en hardware/softwarematige beveiligingsmaatregelen effectief kunnen zijn. Als de genomen beveiligingsmaatregelen in de praktijk complex en ingewikkeld zijn, dan loopt men het risico dat de gebruikers niet altijd de gewenste zorgvuldigheid in acht nemen. Bedacht dient te worden, dat hoe ver er ook geautomatiseerd wordt, ergens altijd de mens in de keten zit.

Het laatste aspect wat hier beschouwd wordt betreft de dimensie van beveiliging. Ook hier is weer sprake van een driedeling (vergelijk figuur 1.6).



Figuur 1.6. Dimensies van beveiliging.

In eerste instantie zal men bij het toepassen van cryptografie vooral *preventief* te werk willen gaan. Dat wil zeggen dat men de kans dat er iets gebeurt zal willen minimaliseren. Dit kan men bereiken door het toepassen van sterke cryptografische algoritmen en protocollen en het treffen van adequate fysieke en organisatorische maatregelen. Echter *absolute beveiliging* is per definitie onmogelijk. De kans dat er iets gebeurt kan weliswaar geminimaliseerd worden, maar zal in de praktijk nooit gelijk aan nul zijn. Een ander aspect dat men dan ook met betrekking tot de dimensie van beveiliging kan onderscheiden is het *schade-beperkende* aspect van beveiliging. Dat wil zeggen, laat de kans dat er iets gebeurt niet gelijk aan nul zijn, men dient er in ieder geval voor te zorgen dat als er iets gebeurt de schade zo beperkt mogelijk blijft. Dit betekent dat als iemand in bijvoorbeeld een computerbestand weet door te dringen dat dit slechts in een klein deel van het bestand is. Of als een indringer over een geheime sleutel beschikt, hij slechts een deel van de boodschappen kan ontcijferen, maar nooit alle boodschappen etcetera.

Het laatste aspect is het *corrigerende*. Dit houdt in dat als er iets misgaat dit spoedig te herstellen moet zijn. Als bijvoorbeeld een niet-geautoriseerde persoon over de geheime sleutel is komen te beschikken, dan moeten er eenvoudig en snel maatregelen genomen kunnen worden zodanig dat deze sleutel onbruikbaar is. Het houdt ook in dat als bijvoorbeeld vitale computerbestanden aangetast zijn deze gereconstrueerd moeten kunnen worden.

Het zal duidelijk zijn dat er in de praktijk ten aanzien van alle bovengenoemde beveiligingsaspecten een trade-off gemaakt moet worden.

Een facet dat nog niet aan de orde is gekomen is het economische aspect van de toepassing van beveiligingsmaatregelen. Feitelijk gaat het hier om de relatie tussen gewenst beveiligingsniveau, de waarde van hetgeen beveiligd wordt of waartegen beveiligd wordt en de investering die er gedaan moet worden om de gewenste beveiligingsmaatregelen te nemen dan wel die een indringer nog geacht wordt bereid te zijn te doen teneinde de gewenste informatie te verkrijgen.

Hierboven kwamen hier en daar al een aantal toepassingen van cryptografie ter sprake. De toepassingen kunnen ingedeeld worden naar twee groepen, te weten toepassingen met betrekking tot opslag en toepassingen te maken hebbende met transport van informatie.

Bij opslag moet vooral gedacht worden aan opslag in computersystemen; op schijf dan wel op magneetbanden etc. Vaak is hier de methode zelf volgens welke bijvoorbeeld gegevens, software etc. opgeslagen worden wel bekend en openbaar, maar de sleutel niet. Omdat deze gegevens vaak voor langere duur worden opgeslagen, is een cryptanalytische aanval aantrekkelijk. De cryptanalist heeft immers ruim de tijd de sleutel te vinden. Een relatief hoog beveiligingsniveau zou dan gewenst kunnen zijn.

Bij datacommunicatie (tv, satellietverbindingen) is de gecijferde boodschap, in tegenstelling tot wat bij opslag het geval is, slechts een zeer korte tijd voor de cryptanalist beschikbaar en wel op het moment van uitzenden. Er zal bovendien gemakkelijker gewisseld worden van sleutel dan in geval van opslag. De cryptanalist kan uiteraard de verzonden boodschap op een recorder of iets dergelijks opnemen, maar het ontcijferen van de boodschap is nog geen garantie dat daarmee ook andere gecijferde boodschappen ontcijferd kunnen worden; juist omdat er wellicht frequente sleutelwisseling plaatsvindt.

Daar komt nog bij dat bij datacommunicatie dikwijls sprake is van boodschappen, welke slechts gedurende een beperkte tijdsduur waarde hebben; bijvoorbeeld omdat na verloop van tijd de inhoud ervan verouderd is (denk aan nieuws, weersinformatie etc.).

In dergelijke omstandigheden waarbij er sprake is van een slechts momentane waarde van de beveiligde informatie, kan in het algemeen volstaan worden met een beperkter beveiligingsniveau en daardoor geringere investeringen.

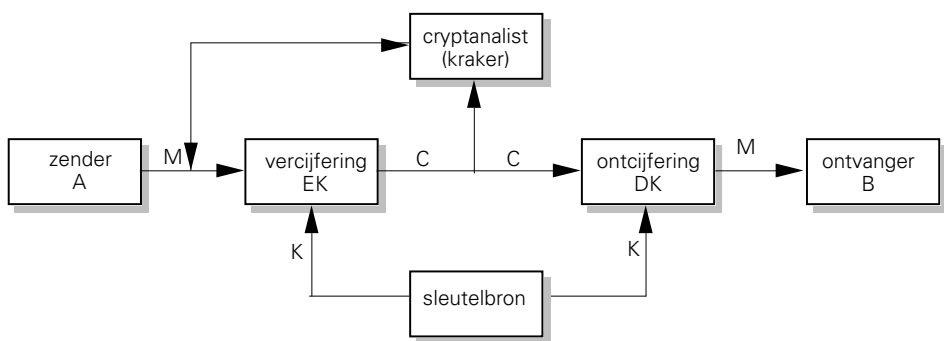
Het kostenaspect speelt ook nog op een andere manier een rol. Beschouw kabeltelevisie. Het is duidelijk dat de exploitant gebaat is bij een optimale beveiliging. Immers het bedrijf is er bij gebaat zoveel mogelijk illegaal kijken te voorkomen. Daar staat tegenover dat de kosten van het systeem bij de consument, dat er voor dient te zorgen dat het gecijferde signaal ontcijferd wordt, niet te hoog mogen zijn. Dit geldt voor de exploitant, maar ook vanuit het standpunt van de consument bezien. Immers de consumenten, waarvan het merendeel te goeder trouw geacht mag worden, zijn slechts in beperkte mate bereid een bijdrage te leveren aan beveiliging, waar zijzelf niet om gevraagd hebben. Verder hoeft het beveiligingsniveau slechts zodanig te zijn dat een potentiële zwartkijker om de programma's te kunnen zien een grotere investering moet doen dan het bedrag waarvoor hij op reguliere wijze tot het kabelnet toegelaten kan worden.

### 1.3. Cryptanalytische aanvallen

We beschouwen hier de situatie van een cryptografisch algoritme waarbij door betrokken partijen gebruik wordt gemaakt van een geheime sleutel. Vergelijk figuur 1.1. Er is sprake van een cryptanalytische aanval als de indringer anders dan alleen door proberen de klare tekst of de sleutel tracht te vinden. Het laatste, het vinden van de geheime sleutel, is vaak aantrekkelijker dan het incidenteel vinden van een klare tekst. Voordeel van het hebben van de geheime sleutel is dat dan mogelijk ook andere cijferteksten ontcijferd kunnen worden. Met betrekking tot het zoeken naar de sleutel is het natuurlijk mogelijk dat men alle mogelijke sleutels toepast op de cijfertekst totdat men de juiste gevonden heeft. Men spreekt dan van een zogenaamd *uitputtend sleutelonderzoek* (*exhaustive key search*). Toch is dit geen cryptanalytische aanval in de ware zin van het woord, omdat er bij een cryptanalytische aanval sprake moet zijn van “intelligenter” gedrag van de kant van de cryptanalist dan alleen maar proberen.

Met betrekking tot echte cryptanalytische aanvallen op cryptosystemen kunnen drie typen van aanvallen onderscheiden worden, samenhangend met de mate waarin de cryptanalist over informatie beschikt. Vergelijk ook figuur 1.7. Deze drie soorten van aanval zijn:

- aanval op basis van alleen een cijfertekst: *alleen-cijfertekst-aanval* (*cipher-text-only-attack*)
- aanval op basis van een gegeven klare tekst en de corresponderende cijfertekst: *gekende-klare-tekst-aanval* (*known-plaintext-attack*)
- aanval op basis van een gekozen klare tekst en bijbehorende cijfertekst: *gekozen-klare-tekst-aanval* (*chosen-plaintext-attack*).



Figuur 1.7. Cryptanalytische aanvallen.

In geval van een aanval op basis van alleen cijfertekst, heeft de cryptanalist alleen de beschikking over de cijfertekst (het gecijferde signaal). Op basis hiervan moet hij, door middel van een analyse van de in de cijfertekst aanwezige structuur en eventuele statistiek, trachten de onderliggende boodschap (klare tekst) te ontcijferen of wat nog

belangrijker is, trachten de sleutel te vinden. In geval van vercijferde spraak, afluisteren van autotelefoon etc. zal de cryptanalist veelal geen andere mogelijkheid hebben dan een aanval op basis van alleen cijfertekst. Het is duidelijk dat de cryptanalist in dit geval in de minst gunstige uitgangspositie zit.

De situatie, waarin de cryptanalist naast informatie over de cijfertekst ook over informatie beschikt over de corresponderende klare tekst, is al veel gunstiger. Door middel van kennis over combinaties van cijfertekst en klare tekst, kan hij trachten dat deel van de cijfertekst, waarvan de corresponderende klare tekst niet bekend is, te ontcijferen, dan wel de sleutel te vinden. Situaties waarbij de cryptanalist zowel over cijfertekst als over de corresponderende klare tekst beschikt, doen zich voor als de cryptanalist erin geslaagd is enigszins door te dringen tot het cryptosysteem dan wel tot de gebruiker ervan. Zo is het evident dat bij financiële transacties bij elke transactie sprake moet zijn van informatie over de betalende en ontvangende partij. Als de cryptanalist door inside-informatie ervan op de hoogte is, hoe informatie over de betalende partij etc. in de cijfertekst verborgen zit, zou hij kunnen trachten op basis hiervan het resterende deel van de cijfertekst te ontcijferen.

De meest gunstige situatie voor de cryptanalist doet zich voor, wanneer de cryptanalist willekeurige klare teksten kan uitzoeken en de bijbehorende cijferteksten kan genereren. Door geschikte klare teksten te kiezen en te vergelijken met de bijbehorende cijferteksten kan hij trachten delen niet ontcijferde cijferteksten te ontcijferen, dan wel de gebruikte sleutel te achterhalen. In geval van een beveiligde tekstverwerker, waarbij de geproduceerde tekst in vercijferde vorm wordt opgeslagen, kan een gekozen-klare-tekst-aanval vaak gemakkelijk uitgevoerd worden.

Bij het toepassen van cryptografische methoden geeft men er natuurlijk de voorkeur aan een systeem te ontwikkelen, wat beveiligd is tegen alle drie soorten aanvallen. In de praktijk blijkt dit moeilijk te realiseren zijn. Een systeem dat veilig lijkt tegen een alleen-cijfertekst-aanval hoeft dit niet te zijn tegen een aanval door middel van gekozen/gekende klare tekst. Wel is het zo, dat in een praktische omgeving een systeem dat een aanval op basis van een gekozen-klare-tekst kan doorstaan hoger aangeslagen wordt dan een systeem dat alleen een aanval op basis van alleen cijfertekst kan doorstaan.

In het bovenstaande is met name gekeken naar cryptanalytische aanvallen die de confidentialiteit aantasten. Aanvallen die betrekking hebben op inbreuk op betrouwbaarheid (integriteit en authenticiteit) zullen verderop in dit boek nog aan de orde komen.

# 6

## Openbare-sleutelsystemen

### 6.1. Inleiding

Tot nu toe zijn in de vorige hoofdstukken cryptografische methoden voor de versluiering van informatie beschouwd waarbij sprake is van één sleutel, die aan de zenzijde gebruikt wordt voor vercijfering van informatie en aan de ontvangzijde voor de ontcijfering. Een van de problemen is, hoe er voor te zorgen dat beide partijen, zender en ontvanger, over dezelfde sleutel te beschikken. Traditioneel werd in diplomatieke en militaire kringen daartoe gebruikt gemaakt van koeriers welke zorgen voor de sleuteluitwisseling tussen zender en ontvanger. Ook is het mogelijk de sleuteluitwisseling te doen plaatsvinden over een transmissielijn, anders dan die waarover de cijfertekst wordt verzonden. In alle gevallen dient echter tijdens transmissie de sleutel geheim gehouden te worden, omdat degene die over de sleutel komt te beschikken in principe de cijferteksten kan ontcijferen.

In een *openbare-sleutelsysteem* (*public key system*) is steeds sprake van twee sleutels: één voor het vercijferen en één voor het ontcijferen. De vercijfersleutel is in principe openbaar; dat wil zeggen ieder kan ervan kennis nemen en het gebruiken voor vercijfering. De basisidee van openbare-sleutelsystemen bestaat nu hierin, dat weliswaar iedereen een boodschap kan vercijferen, maar dat niet iedereen de aldus verkregen cijfertekst kan ontcijferen. Er wordt namelijk voor gezorgd dat het ondoenlijk is de ontcijfersleutel af te leiden uit de vercijfersleutel. Een dergelijk systeem waarbij sprake is van een geheime en een openbare sleutel wordt ook wel een *asymmetrisch systeem* genoemd. Dit in tegenstelling tot een *symmetrisch systeem*, zoals DES, waarbij sprake is van één (geheime) sleutel, welke zowel voor vercijferen als ontcijferen gebruikt wordt.

Van belang bij openbare-sleutelsystemen zijn de zogenaamde *éénrichtingsfuncties* en *'trapdoor' functies*. *Eénrichtingsfuncties* (*one-way functions*) zijn functies die zelf gemakkelijk uit te rekenen zijn, maar waarvoor het bepalen van de inverse aanzienlijk moeilijker is. Men kan bijvoorbeeld denken aan machtsverheffen. Machtsverheffen zelf kan eenvoudig uitgevoerd worden door herhaald vermenigvuldigen. De inverse van het machtsverheffen, het worteltrekken, is al heel wat ingewikkelder. *Trapdoor-functies* (letterlijk: functies-met-valluik) zijn in feite éénrichtingsfuncties, waarbij de

berekening van de inverse gewoonlijk heel moeilijk is, behalve als men over additionele informatie beschikt.

## 6.2. Het RSA-systeem

Een van de bekendste en meest gebruikte openbare-sleutelsystemen is het *RSA-systeem*, hetwelk zijn naam ontleend aan de eerste letters van de namen van degenen die dit systeem ontworpen hebben (R.L. Rivest, A. Shamir en L. Adleman van het Massachusetts Institute of Technology (MIT), zie Rivest et al. (1978)). Het RSA-systeem is gebaseerd op het feit dat het eenvoudig is een produkt van twee priemgetallen te berekenen, maar dat het aanzienlijk moeilijker is uit het produkt weer de oorspronkelijke priemgetallen te bepalen. Het RSA-schema ziet er als volgt uit.

### *Het RSA-schema*

Eerst worden er twee grote priemgetallen  $p$  en  $q$  gegenereerd. Van deze twee priemgetallen wordt het produkt  $n$  bepaald:  $n = pq$ . Vervolgens wordt een getal  $e$  bepaald, zodanig dat

$$3 < e < (p - 1)(q - 1) \quad (6.1)$$

en zodanig dat  $e$  relatief priem is ten opzichte van  $(p - 1)(q - 1)$ . Dat wil zeggen dat de grootste gemene deler van  $e$  en  $(p - 1)(q - 1)$  gelijk is aan 1.

Met behulp van dit getal  $e$  wordt een getal  $d$  berekend waarvoor geldt:

$$ed = 1 \pmod{(p - 1)(q - 1)}. \quad (6.2)$$

De openbare sleutel bestaat nu uit het getallenpaar  $(e, n)$ ; alle andere grootheden worden geheimgehouden. Het vercijferen gaat nu als volgt in zijn werk. De te vercijferen boodschap, welke gedacht wordt binair gerepresenteerd te zijn, wordt opgedeeld in blokken  $M$ . Het vercijferde blok  $C$  ontstaat nu door de decimale waarde van  $M$  tot de macht  $e$  te verheffen en het resultaat hiervan modulo  $n$  te nemen:

$$C = M^e \pmod{n}. \quad (6.3)$$

Het ontcijferen gaat op precies dezelfde wijze, maar nu met  $d$  in plaats van  $e$ :

$$M = C^d \pmod{n}. \quad (6.4)$$

●

De werking van het systeem berust op het feit dat het ondoenlijk is om op basis van alleen de openbare sleutel  $(e, n)$  de grootheid  $d$  te berekenen. Voor de berekening van  $d$  is het naast  $e$  nodig de waarden  $p$  en  $q$  te kennen (zie (6.2)). Omdat men alleen over  $n$  beschikt dient een cryptanalist hieruit  $p$  en  $q$  te bepalen. Als  $n$  in de orde van 200 decimale cijfers ligt, dan zou het op basis van de huidige technologie circa 30 miljoen

jaar kosten  $p$  en  $q$  te vinden.

Daardoor beschikt in principe alleen degene die de openbare sleutel  $(e, n)$  heeft uitgegeven over  $d$  en heeft daarmee als enige de mogelijkheid de gecijferde blokken te ontcijferen.

Het volgende voorbeeld laat zien hoe een en ander in zijn werking gaat.

### Voorbeeld

Stel dat de volgende priemgetallen gekozen waren:  $p = 3$  en  $q = 17$  (in de praktijk kiest men natuurlijk grote priemgetallen, het gaat hier echter alleen om een illustratie). Het produkt  $n$  is dus gelijk aan  $51$  en  $(p - 1)(q - 1) = 32$ .

Er moet nu een getal  $e$  gekozen worden tussen  $3$  en  $32$ , dat geen gemeenschappelijke factor met  $32$  gemeen heeft. Kies bijvoorbeeld  $e = 7$ . Nu dient de  $d$  bepaald te worden, zodanig dat  $ed = 1 \pmod{(p - 1)(q - 1)}$ . Er volgt  $d = 23$ , immers  $ed$  is dan gelijk aan  $7 \times 23 = 161 = 1 \pmod{32}$ .

De openbare sleutel wordt nu gegeven door het getallenpaar  $(7, 51)$ . Als  $M = 2$  de boodschap representeert die gecijferd moet worden, dan geldt voor de gecijfering:

$$C = M^e \pmod{n} = 2^7 \pmod{51} = 26.$$

Voor het ontcijferen dient men te beschikken over  $d$  en  $n$ . Er volgt dan:

$$\begin{aligned} M &= C^d \pmod{n} = 26^{23} \pmod{51} \\ &= 26^1 26^2 26^4 26^{16} \pmod{51} \\ &= 26 \cdot 13 \cdot 16 \cdot 1 \pmod{51} = 2, \end{aligned}$$

hetgeen weer de oorspronkelijke boodschap is. Een eventuele cryptanalist kan alleen de beschikking krijgen over de getallen  $(7, 51)$ . Ontcijfering gelukt alleen dan als hij in staat is op basis hiervan  $d = 23$  te berekenen. Daarvoor is het nodig uit het getal  $51$  de getallen  $3$  en  $17$  te vinden. Nu is dat in dit geval erg eenvoudig; op basis van het getal  $51$  is al gauw te bepalen welke  $p$  en  $q$  zijn. Als echter het getal  $n$  een  $200$  decimale cijfers telt, dat wil zeggen  $n$  ligt in de orde van  $2^{660}$ , dan is dit ondoenlijk.  $\triangle$

In het bovenstaande voorbeeld is voor het uitrekenen van  $26^{23} \pmod{51}$  gebruik gemaakt van de volgende twee eigenschappen van modulo-rekening:

$$(i) \quad a = b \pmod{n} \Rightarrow a^2 = b^2 \pmod{n}. \quad (6.5)$$

$$(ii) \quad ab \pmod{n} = [a \pmod{n}] \cdot [b \pmod{n}]. \quad (6.6)$$

Eigenschap (i) volgt direct. Immers,  $a = b \pmod{n}$  impliceert dat  $a$  gelijk is aan  $b$  op een veelvoud van  $n$  na:  $a = b + kn$ . Hieruit volgt  $a^2 = b^2 + (kn)^2 + 2bkn$ . En dus geldt  $a^2 = b^2 \pmod{n}$ .

Eigenschap (ii) kan ook direct afgeleid worden:

$$\begin{aligned} [a \pmod n] \cdot [b \pmod n] &= (a + kn)(b + k'n) \\ &= ab + ak'n + bkn + kk'n^2 = ab \pmod n. \end{aligned}$$

Eigenschap (ii) maakt dat voor de berekening van  $26^{23} \pmod{51}$  volstaan kan worden met de berekening van de samenstellende machten modulo 51. Eigenschap (i) brengt met zich mee, dat als  $26^2 = 13 \pmod{51}$  dat dan direct voor de berekening van  $26^4 \pmod{51}$  geldt:  $26^4 = 13^2 \pmod{51}$  etc.

Op deze wijze kan de rekencomplexiteit van machtsverheffen modulo  $n$  aanzienlijk beperkt worden.

Als boven reeds opgemerkt, zijn  $d$  en  $e$  zodanig dat ze altijd aanleiding geven tot inverse vercijfer- en ontcijferoperaties. Dit kan ook geconcludeerd worden uit het boven gegeven voorbeeld. Om aan te tonen waarom dit altijd zo is, moet men een beroep doen op een stelling uit de getallentheorie.

In hoofdstuk 5 werd reeds de Euler totiënt functie  $\varphi(n)$  geïntroduceerd, zijnde het aantal positieve integers kleiner dan  $n$  welke relatief priem zijn ten opzichte van  $n$ . Aangezien voor een priemgetal  $p$  geldt dat  $\varphi(p) = p - 1$ , geldt nu voor het produkt  $n = pq$  van twee priemgetallen  $p$  en  $q$ :

$$\varphi(n) = \varphi(p) \varphi(q) = (p - 1)(q - 1) = n - p - q + 1. \quad (6.7)$$

De stelling van Euler, waarop het RSA-systeem is gebaseerd, luidt als volgt.

### **Stelling 6.1 (stelling van Euler)**

Voor alle  $a$  en  $n$ , welke relatief priem zijn ten opzichte van elkaar en waarbij aangenomen wordt dat  $n > 0$  en  $0 < a < n$ , geldt:

$$a^{\varphi(n)} = 1 \pmod n. \quad (6.8)$$

### **Bewijs**

Voor gegeven  $n$  geldt dat  $a \in Z'_n$ , waarbij  $Z'_n = (r_1, \dots, r_m)$  de verzameling van alle gehele getallen tussen 0 en  $n$ , die relatief priem zijn ten opzichte van  $n$ . Eenvoudig is na te gaan dat per definitie moet gelden:

$$|Z'_n| = m = \varphi(n).$$

Voor alle  $i$  geldt nu, dat er een  $j$  is ( $1 \leq i, j \leq m$ ) zodanig dat

$$ar_i = r_j \pmod n.$$

Dit kan als volgt ingezien worden. Aangezien  $a$  en  $r_i$  relatief priem zijn ten opzichte

van  $n$ , zal ook gelden dat het produkt  $ar_i$  relatief priem is ten opzichte van  $n$ . Omdat  $Z'_n$  de verzameling is van alle getallen, die relatief priem zijn ten opzichte van  $n$ , volgt  $ar_i \pmod n \in Z'_n$ . Met andere woorden  $ar_i \pmod n$  moet gelijk zijn aan een van de elementen  $r_j$  van  $Z'_n$ . Voor iedere  $i$  is er precies één  $j$  zodanig dat  $ar_i = r_j \pmod n$ .

Er volgt nu

$$ar_1 \cdot ar_2 \dots ar_m = r_1 r_2 \dots r_m \pmod n$$

oftewel

$$a^m (r_1 r_2 \dots r_m) = (r_1 r_2 \dots r_m) \pmod n,$$

en

$$(a^m - 1)(r_1 r_2 \dots r_m) = 0 \pmod n.$$

Aangezien  $(r_1 r_2 \dots r_m)$  relatief priem zijn ten opzichte van  $n$ , moet gelden

$$a^m - 1 = 0 \pmod n \Rightarrow a^m = 1 \pmod n.$$

Door hierin  $m = \varphi(n)$  te substitueren volgt de stelling. □

### Voorbeeld

Stel  $n = 17$  en  $a = 2$ . Er geldt  $\varphi(17) = 16$ . De stelling van Euler stelt nu:  $2^{16} = 1 \pmod{17}$ . Dit is correct aangezien  $2^{16} = 65536 = 1 + 3855 \times 17$ . △

Met behulp van de stelling van Euler kan aangetoond worden dat vercijferen en ontcijferen volgens het RSA-systeem elkaars inverse zijn.

### Stelling 6.2

Stel een boodschap  $M$  wordt vercijferd volgens het RSA-systeem, waarbij de cijfertekst gelijk wordt aan:

$$C = M^e \pmod n, \tag{6.9}$$

terwijl aan de ontvangzijde wordt berekend:

$$M' = C^d \pmod n, \tag{6.10}$$

waarbij  $ed = 1 \pmod{(p-1)(q-1)}$ , dan geldt in alle gevallen:

$$M' = M. \tag{6.11}$$

### Bewijs

Aangezien  $\varphi(n) = (p-1)(q-1)$  geldt:

$$ed = 1 \pmod{(p-1)(q-1)} = 1 \pmod{\varphi(n)}$$

en dus

$$ed = k\varphi(n) + 1. \tag{6.12}$$

Aan de ontvangzijde wordt cijfertekst  $C$  ontvangen, waarvoor geldt:

$$C = M^e \pmod{n}.$$

Deze wordt ontcijferd met behulp van de op  $d$  gebaseerde ontcijferoperatie, hetgeen oplevert:

$$M' = C^d \pmod{n} = M^{ed} \pmod{n}. \quad (6.13)$$

Deze laatste uitdrukking laat zich met (6.12) schrijven als:

$$M' = M^{ed} \pmod{n} = M^{k\varphi(n)+1} \pmod{n}. \quad (6.14)$$

Deze uitdrukking kan als volgt vereenvoudigd worden. Op grond van de stelling van Euler geldt, onder de aanname dat  $M$  en  $n$  relatief priem zijn:

$$M^{\varphi(n)} = 1 \pmod{n}. \quad (6.15)$$

En dus volgt:

$$M' = M^{ed} = M^{k\varphi(n)+1} = (M^{\varphi(n)})^k M = (1)^k M \pmod{n} = M \pmod{n}. \quad (6.16)$$

Als  $M$  en  $n$  niet relatief priem zijn, zal gelden dat  $M$  en  $n$  een gemeenschappelijke factor  $p$  dan wel  $q$  hebben. Stel de gemeenschappelijk factor is  $p$ , dan zijn  $M$  en ook  $M^{\varphi(p)}$  relatief priem ten opzichte van  $q$ . Er geldt dan met de stelling van Euler:

$$(M^{\varphi(p)})^{\varphi(q)} = 1 \pmod{q}.$$

oftewel

$$M^{\varphi(n)} = 1 \pmod{q},$$

en

$$M^{k\varphi(n)+1} = M \pmod{q}. \quad (6.17)$$

Omdat in  $M$  een factor  $p$  voorkomt, geldt ook

$$M^{k\varphi(n)+1} = M \pmod{p}. \quad (6.18)$$

Combinatie van de laatste twee uitdrukkingen leidt ook nu tot

$$M' = M^{ed} = M^{k\varphi(n)+1} = M \pmod{n}. \quad (6.19)$$

Hetzelfde geldt natuurlijk, als aangenomen wordt dat de gemeenschappelijke factor van  $M$  en  $n$  is gegeven door  $q$  in plaats van  $p$ .  $\square$

Zoals al eerder vermeld ontleent het RSA-systeem zijn sterkte aan het feit dat het onmogelijk is uit  $n$  de getallen  $p$  en  $q$  af te leiden. Een en ander veronderstelt wel dat de priemgetallen voldoende groot zijn. Grote priemgetallen brengen echter met zich

mee dat bij het vercijferen en ontcijferen met zeer grote getallen gerekend moet worden.

### Voorbeeld

Stel  $p = 47$  en  $q = 59$ , er volgt dan  $n = pq = 2773$  en  $(p - 1)(q - 1) = 2668$ . Er moet een getal  $e$  gekozen worden dat tussen 3 en 2668 ligt. We kiezen  $e = 17$ . Vervolgens wordt  $d$  berekend uit  $ed = 1 \pmod{(p - 1)(q - 1)}$  oftewel  $17d = 1 \pmod{2668}$ . Dit levert op  $d = 157$ . Neem aan dat het alfabet decimaal gerepresenteerd wordt, dat wil zeggen  $a = 01$ ,  $b = 02$ ,  $c = 03$  etc., terwijl een spatie gecodeerd wordt door 00. Als de te vercijferen tekst gegeven is door

$M =$  NEEM TEN SPOEDIGSTE KONTAKT OP

dan is dit decimaal:

$M =$  1405 0513 2005 1419 1615 0504 0907 1920 0511 1514 2001 1120 1516.

De boodschap wordt nu vercijferd door steeds 4 cijfers op te vatten als een afzonderlijke boodschap en deze te vercijferen:  $M_1 = 1405$ ,  $M_2 = 513$  etc. Vercijfering van  $M_1$  levert:  $C_1 = 1405^{17} \pmod{2773} = 2641$ . Vercijferen we de rest ook zo dan wordt gevonden:

$C =$  2641 0772 0117 2025 2763 1755 0639 2109 0680 2214 2029 1002 0477.

Ontcijfering verloopt als volgt:  $C_1 = 2641$ , hieruit volgt  $M_1 = 2641^{157} \pmod{2773} = 1405$  etc. △

De al snel complexe berekeningen stellen hoge eisen aan de implementatie, teneinde het rekenen met grote getallen mogelijk te maken en het algoritme voldoende snel te doen zijn. Beschouwen we het laatste voorbeeld dan zien we dat het berekenen van  $d$  uit  $ed = 1 \pmod{(p - 1)(q - 1)}$  gegeven  $p$ ,  $q$  en  $e$  en het berekenen van termen van de vorm  $X = M^e \pmod{n}$ , vooral bij grote getallen, niet eenvoudig is. Hieronder worden twee algoritmen gegeven waarmee een en ander vergemakkelijkt wordt.

Voor de berekening van  $d$  uit  $ed = 1 \pmod{\phi(n)}$  kan gebruik gemaakt worden van een variant van het zogenaamde *Euclidisch algoritme*.

Stel  $r(0) = \phi(n)$  en  $r(1) = e$ . Waar het nu omgaat is recursief parameters  $r(2)$ ,  $r(3)$ , ...,  $r(k)$  uit te rekenen totdat  $r(k) = 1$ . Op dat moment wordt gestopt en kan  $d$  direct gevonden worden. De berekening van  $r(2)$ ,  $r(3)$  etc. geschiedt als hieronder aangegeven.

$$r(0) = a(1) \cdot r(1) + r(2)$$

$$r(1) = a(2) \cdot r(2) + r(3)$$

$$\begin{aligned} r(2) &= a(3) \cdot r(3) + r(4) \\ &\vdots \\ r(k-2) &= a(k-1) \cdot r(k-1) + r(k). \end{aligned}$$

De waarden van  $a(1)$ ,  $a(2)$  etc. zijn zodanige gehele getallen dat altijd geldt voor alle  $k$ :  $r(k) < r(k-1)$ . Op grond van bovenstaande dient men nu  $r(2)$ ,  $r(3)$  etc. tot en met  $r(k)$  uit te drukken in termen van alleen  $r(0)$  en  $r(1)$ :

$$r(2) = r(0) - a(1) \cdot r(1)$$

$$r(3) = r(1) - a(2) \cdot r(2) = -a(2) \cdot r(0) + [1 + a(1)a(2)] r(1)$$

etcetera.

Er wordt gestopt als er een  $k$  is waarvoor  $r(k) = 1$ . Deze  $r(k)$  is eveneens uit te drukken in termen van alleen  $r(0)$  en  $r(1)$ . Stel dat geldt  $r(k) = u \cdot r(0) + v \cdot r(1)$ , dan is eenvoudig in te zien dat  $v$  de waarde  $d$  is die gezocht wordt. Immers  $r(k) = 1$  impliceert  $1 = u \cdot r(0) + v \cdot r(1) = u \cdot \varphi(n) + v \cdot e$ . Hieruit volgt:  $ve = 1 \pmod{\varphi(n)}$ , waaruit blijkt dat  $v$  de gezochte  $d$  is.

### Voorbeeld

Bepaal  $d$  uit  $7d = 1 \pmod{32}$ .

Stel  $r(0) = 32$  en  $r(1) = 7$ . We vinden nu achtereenvolgens:

$$32 = 4 \times 7 + 4 \Rightarrow r(2) = r(0) - 4 r(1)$$

$$7 = 1 \times 4 + 3 \Rightarrow r(3) = r(1) - r(2) = -r(0) + 5 r(1)$$

$$\begin{aligned} 4 &= 1 \times 3 + 1 \Rightarrow r(4) = r(2) - r(3) = r(0) - 4 r(1) - (-r(0) + 5 r(1)) \\ &= 2 r(0) - 9 r(1). \end{aligned}$$

Hieruit volgt  $d = -9 = 23 \pmod{32}$ . △

In het begin van deze paragraaf gaven we een methode waarmee machten modulo een bepaald getal eenvoudig berekend kunnen worden. Meer formeel luidt het algoritme voor de berekening van uitdrukkingen van de vorm  $X = M^e \pmod{n}$  als volgt.

1. Schrijf  $e$  in binaire vorm:  $e = e_k, e_{k-1}, \dots, e_1, e_0$
2. Stel  $X := 1$
3. Laat voor  $i = k, k-1, \dots, 0$ :
  - a)  $X := \text{rest van } (X^2/n)$
  - b) als  $e_i = 1$  dan ook  $X := \text{rest van } (XM/n)$
4. Stop als  $i = 0$ . De dan geldende waarde van  $X$  is de gezochte waarde.

**Voorbeeld**

Berekening van  $X = 2^5 \pmod{11}$ . Er geldt  $M = 2$ ,  $n = 11$ ,  $e = 5$  of  $e = 101$  in binaire vorm.

Toepassing van bovenstaand algoritme levert:

$$\begin{aligned} k = 2: X &:= \text{rest van } (1/11) = 1 \\ &\text{omdat } e_2 = 1: X := \text{rest van } (1 \cdot 2/11) = 2 \\ k = 1: X &:= \text{rest van } (2^2/11) = 4 \\ k = 0: X &:= \text{rest van } (4^2/11) = 5 \\ &\text{omdat } e_0 = 1: X := \text{rest van } (5 \cdot 2/11) = 10. \end{aligned}$$

Er volgt dus  $X = 2^5 \pmod{11} = 10 \pmod{11}$ . △

De behoefte aan grote priemgetallen ten behoeve van RSA roept ook de vraag op hoe deze te verkrijgen. Genereren van voldoende grote priemgetallen is een probleem op zich. Het echt berekenen van priemgetallen vergt een aanzienlijke hoeveelheid rekentijd. De beste oplossing is met behulp van een random generator zeer grote getallen te genereren en daarvoor na te gaan of het priemgetallen zijn. Dit mag dan onbegonnen werk lijken, men dient echter te bedenken dat het procentuele aantal priemgetallen weliswaar klein is, maar hun absolute aantal niet. Daarom heeft het wel degelijk zin random getallen te genereren en vervolgens te testen of het priemgetallen zijn. Bij het testen of een getal een priemgetal is kan geen gebruik worden van factorisatie; dat zou zeer veel rekentijd vergen, en op de onmogelijkheid hiervan is juist het RSA-systeem gebaseerd. Wel zijn er testen waarmee met vrij grote zekerheid bepaald kan worden of een getal een priemgetal is. Een van deze testen is de priemgetaltest van Solovay en Strassen (1977/78).

Stel kandidaat priemgetal  $p$ . Beschouw nu getallen  $a$ , waarvoor geldt  $a \in (1, \dots, p-1)$ . Als  $\text{GGD}(a,p) \neq 1$ , dan is  $p$  geen priemgetal. Indien  $\text{GGD}(a,p) = 1$  check dan of de volgende bewering waar is:

$$J(a,p) = a^{(p-1)/2} \pmod{p}, \tag{6.20}$$

waarbij  $J(a,p)$  het *Jacobi-symbool* is, waar hieronder op teruggekomen wordt.

Er geldt nu dat als  $p$  priem is, bovenstaande bewering altijd waar is voor alle  $a$ . Is  $p$  echter niet priem dan zal in meer dan 50% van de gevallen de bewering niet waar zijn. Dit impliceert dat als voor 100 verschillende waarden van  $a$  de bewering waar blijkt te zijn, de kans dat  $p$  een priemgetal is groter is dan  $1 - 2^{-100}$ . Met andere woorden door steeds de bewering voor alle mogelijke waarden van  $a$  te toetsen, zal in geval van een steeds geldig zijn van de bewering de kans met een priemgetal te maken te hebben steeds groter worden. Absolute zekerheid kan echter niet verkregen worden. Dit betekent dat het best eens zou kunnen zijn dat ongemerkt een niet-priemgetal in het

RSA-systeem gebruikt wordt, waardoor  $n$  te schrijven is als een produkt van bijvoorbeeld 3 getallen in plaats van 2 getallen. Dit kan een potentiële mogelijkheid tot cryptanalyse met zich meebrengen.

Het Jacobi-symbool  $J(a,p)$  is een functie die alleen de waarden 1 en  $-1$  kan aannemen. Voor alle  $p$  geldt  $J(1,p) = 1$ . Het Jacobi-symbool kan voor willekeurige  $a$  en  $p$  uitgerekend worden met behulp van de volgende formules:

$$a \text{ even: } J(a,p) = J(a/2,p) \cdot (-1)^{(p^2-1)/8}$$

$$a \text{ oneven: } J(a,p) = J(p \pmod{a}, a) \cdot (-1)^{(a-1)(p-1)/4}.$$

### Voorbeeld

Beschouw  $p = 17$ . Kies een getal  $a$ , zeg  $a = 10$ . Er geldt  $\text{GGD}(10,17) = 1$ . We berekenen nu  $J(10,17)$ :

$$\begin{aligned} J(10,17) &= J(5,17) \cdot (-1)^{(17^2-1)/8} = J(5,17) \cdot (-1)^{36} = J(5,17) \\ &= J(17 \pmod{5}, 5) \cdot (-1)^{(5-1)(17-1)/4} = J(2,5) = J(1,5) \cdot (-1)^{(5^2-1)/8} \\ &= -1. \end{aligned}$$

Berekening van  $a^{(p-1)/2} \pmod{p}$  leidt tot:

$$a^{(p-1)/2} \pmod{p} = 10^8 \pmod{17} = -1 \pmod{17}.$$

Aan vergelijking (6.20) is dus voldaan. In dit geval is dit triviaal, want 17 is een priemgetal. Voor grote  $p$  betekent het waar zijn van vergelijking (6.20) dat  $p$  vermoedelijk een priemgetal is.  $\triangle$

Naast de probabilistische methoden zijn er ook deterministische methoden, waarmee bewezen kan worden dat een getal priem is. In vergelijking met de probabilistische testen zijn deze echter meer complex en minder snel.

Niet alle getallen die de priemgetaltest hebben doorstaan zijn echter even bruikbaar voor het RSA-algoritme. In het algemeen maakt men een onderscheid tussen zwakke en sterke priemgetallen. Er zijn namelijk typen van priemgetallen, waarvoor geldt dat als deze gebruikt zouden zijn voor de berekening van het getal  $n$  factorisatie niet ondoenlijk wordt. In het algemeen dient ten aanzien van de keuze van  $p$  en  $q$  het volgende te gelden.

- $p$  moet zodanig zijn dat  $p - 1$  bij ontbinding een grote priemfactor bevat; zeg  $r$ .
- $p + 1$  dient eveneens een grote priemfactor te bevatten, zeg  $s$ .
- $r - 1$  moet een grote priemfactor bevatten, zeg  $t$ .

Dezelfde eisen dienen ook opgelegd te worden aan  $q$ . Daarentegen dient men ervoor te

zorgen dat  $p$  en  $q$  weliswaar groot zijn, maar  $|p - q|$  moet ook groot zijn.

In de praktijk zal men ten aanzien van het genereren van een priemgetal  $p$  als volgt te werk kunnen gaan.

- Eerst wordt er een priemgetal  $s$  gegenereerd. Dit kan geschieden door uitgaande van een bepaalde startwaarde  $s_0$  het eerste priemgetal te zoeken dat groter is dan  $s_0$ ; bijvoorbeeld met de priemgetaltest van Solovay en Strassen. Op dezelfde wijze kan er een priemgetal  $t$  gegenereerd worden.
- Met behulp van  $t$  wordt  $r$  geconstrueerd. Aangezien  $r - 1$  priemfactor  $t$  moet bevatten en  $r$  zelf een oneven getal moet zijn, volgt  $r = 1 \pmod{2t}$ . Voor opeenvolgende waarden van  $i$  wordt  $r = 2it + 1$  nu getest op zijn priem zijn; totdat er een dergelijk priemgetal  $r$  is gevonden.
- Op basis van  $r$  en  $s$  dient nu  $p$  geconstrueerd te worden, welke voldoet aan de boven vermelde eisen  $a)$  en  $b)$ . Dit kan als volgt geschieden.
  - Bereken  $u(r,s) = s^{r-1} - r^{s-1} \pmod{rs}$
  - Indien  $u(r,s)$  oneven stel  $p_0 = u(r,s)$ ,  
anders  $p_0 = u(r,s) + rs$ .
  - Bereken voor een waarde  $j$ , afhankelijk van de gewenste orde grootte van priemgetal  $p$ :  $p = p_0 + 2jrs$  en voer een priemgetaltest uit.
  - Kies opeenvolgende waarden van  $j$  en voer priemgetaltest uit, totdat er een priemgetal  $p$  is gevonden.

Dat de gevolgde procedure inderdaad een priemgetal  $p$  oplevert, dat voldoet aan de eisen  $a)$  en  $b)$  kan als volgt worden ingezien.

Wil aan  $a)$  en  $b)$  voldaan zijn, dan moet gelden dat er een  $k$  en  $h$  zijn zodanig dat:

$$p = 2hr + 1 = 2ks - 1,$$

oftewel

$$p = 1 \pmod{2r} = -1 \pmod{2s}.$$

Met behulp van de stelling van Euler kan afgeleid worden dat geldt:

$$s^{r-1} = 1 \pmod{r}.$$

Verder geldt ook  $r^{s-1} = 1 \pmod{r}$ . Hetgeen impliceert dat

$$u(r,s) = s^{r-1} - r^{s-1} = 1 \pmod{r} = 1 + k'r.$$

Als  $u(r,s)$  even is, dat wil zeggen  $k'$  is oneven, dan volgt

$$\begin{aligned} p &= p_0 + 2jrs = u(r,s) + rs + 2jrs \\ &= 1 + k'r + (2j + 1)rs \\ &= 1 \pmod{2r}. \end{aligned}$$

Als  $u(r,s)$  oneven is ( $k'$  is nu even), dan volgt

$$\begin{aligned} p &= p_0 + 2krs = u(r,s) + 2jrs \\ &= 1 + k'r + 2jrs \\ &= 1 \pmod{2r}. \end{aligned}$$

Op dezelfde wijze kan bewezen worden dat  $p = -1 \pmod{2s}$ .

Er kan geconcludeerd worden dat de aldus gevonden  $p$  een sterk priemgetal is.

Beschouwen we de veiligheid van het RSA-systeem, dan kan opgemerkt worden dat er tot op heden geen aanval is, die sneller is dan factoriseren. We hebben hier weer te maken met praktische veiligheid. De mogelijkheid tot factoriseren en de snelheid ervan hangt grotendeels af van de beschikbare rekencapaciteit en de technologische ontwikkelingen dienaangaande. In 1988 slaagden Caron en Silverman erin met behulp van 140 parallelle SUN-workstations een getal van 90 cijfers te factoriseren in twee priemgetallen van 41 en 49 cijfers. De benodigde tijd was ongeveer 625 uur, hetgeen neerkomt op iets minder dan vier weken. In datzelfde jaar slaagden Lenstra en Manasse er in een priemgetal van 96 cijfers te factoriseren. Ze maakten daartoe gebruik van een groot aantal computers, die met elkaar verbonden waren door een combinatie van local area netwerken en electronic mail. Hetgeen 23 dagen in beslag nam, waarbij vermeldt zij dat het wel meer dan 10 jaar aan CPU tijd kostte. In 1990 factoriseerden ze een getal van 138 cijfers in 50 dagen. Dergelijke (incidentele) resultaten zijn echter moeilijk op hun waarden te schatten.

De huidige stand van zaken is dat op basis van de huidige technologie men ongeveer 500 jaar nodig heeft om een willekeurig getal van 130 cijfers te factoriseren. Hierbij wordt ervan uitgegaan dat men over een computer beschikt die 1 miljoen operaties per seconde kan uitvoeren. Het spreekt voor zich dat de hiervoor benodigde investeringen die door een cryptanalist gedaan moeten worden bijna in alle gevallen niet zullen opwegen tegen het vermeende voordeel voor de cryptanalist van het kunnen factoriseren van een groot getal. In de praktijk wordt het thans aanbevolen getallen  $n$  van 768 bits ( $\approx 230$  decimale cijfers) te gebruiken. Factorisatie kost dan minimaal  $10^8$  jaar bij 1 miljoen operaties per seconde.

Het spreekt voor zich dat de inspanning om, met dergelijke grote getallen te werken in het RSA-systeem, ondanks algoritmen die de rekeninspanningen kunnen beperken, nog steeds aanzienlijk is. RSA is dan ook in de praktijk niet geschikt voor real-time beveiliging van grote datastromen. Bij een sleutel van 512 bits (154 decimaal) bedraagt de verwerkingssnelheid van RSA in VLSI-chiptechnologie circa 64 kbit/sec. Ten aanzien van DES wordt gewerkt aan hardware, waarbij 1 Gigabit/sec gehaald kan worden. In de praktijk ziet men dan ook vaak dat RSA vooral gebruikt wordt voor de vercijfering van beperkte datahoeveelheden, bijvoorbeeld bij sleuteltransport. De eigenlijke data wordt dan bijvoorbeeld vercijferd met behulp van het DES-algoritme,

terwijl de overdracht van de bij DES gebruikte geheime sleutel beveiligd wordt met behulp van het RSA-systeem.

### 6.3. Het knapzakstelsel

Een ander voorgesteld openbaar-sleutelsysteem is gerelateerd aan het zogenaamde knapzakprobleem.

Het knapzakprobleem komt op het volgende neer. Gegeven is een vector

$$A = (a_1, a_2, \dots, a_n),$$

bestaande uit positieve getallen. Deze vector wordt elementsgewijs vermenigvuldigd met een binaire vector

$$X = (x_1, x_2, \dots, x_n),$$

waarbij elke  $x_i$ ,  $i = 1, \dots, n$ , de waarde 0 dan wel 1 aanneemt. Het resultaat is de som  $S$  gegeven door

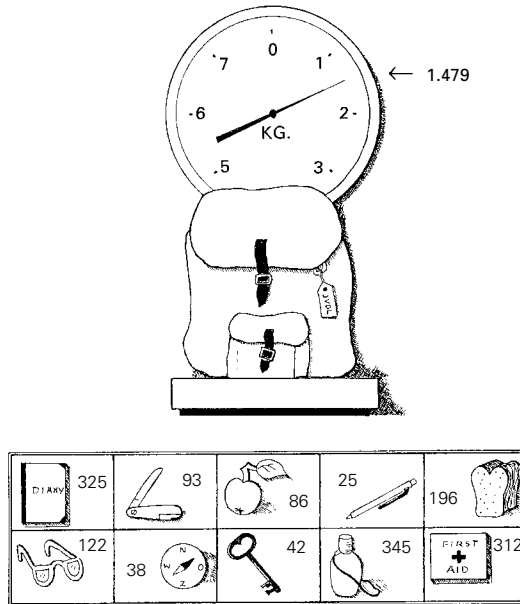
$$S = \sum_{i=1}^n a_i x_i. \quad (6.21)$$

Voor gegeven  $X$  en  $A$  is het eenvoudig  $S$  uit te rekenen. Het probleem is echter, hoe  $X$  uit te rekenen als  $S$  en  $A$  gegeven zijn. Dit probleem staat bekend als het knapzakprobleem. Vergelijk figuur 6.1.

Een knapzak is gevuld met een keuze uit een grote verzameling voorwerpen ieder met zijn eigen gewicht ( $A$  correspondeert met de gewichten van alle voorwerpen). Gegeven het totale gewicht (dit is  $S$ ), is het dan mogelijk te bepalen welke voorwerpen er in de knapzak zitten? Met andere woorden er wordt gevraagd naar de elementen van  $X$ , waarbij een 0 aangeeft dat het desbetreffende voorwerp niet in de knapzak zit en 1 dat het wel aanwezig is.

Bij voldoende grote vector  $A$  (bijvoorbeeld meer dan 100 elementen) is het berekenen van  $X$  op basis van  $S$  en  $A$  bijna ondoenlijk gebleken.

De achterliggende idee voor de ontwikkeling van een cijfersysteem is nu de volgende. Stel nu eens dat er een zodanige  $A$  gekozen kan worden, dat  $S$  gemakkelijk uit  $X$  en  $A$  berekend kan worden, maar dat het vinden van  $X$  op basis van  $S$  en  $A$  ondoenlijk is, tenzij men over additionele informatie beschikt waardoor  $X$  wel snel bepaald kan worden; men zou dan de in bits gerepresenteerde klare tekst kunnen opvatten als een vector  $X$ , welke met behulp van  $A$  omgezet wordt in cijfertekst  $S$ . Aan de ontvangzijde zou  $S$  dan weer omgezet moeten worden in  $X$ .



Figuur 6.1. Het knapsakprobleem.

Merkle en Hellmann (1978) zochten naar zodanige vectoren  $A$ , dat met behulp hiervan  $X$  gemakkelijk uit  $S$  teruggevonden kan worden. Een voorbeeld zijn de zogenaamde *superstijgende rijen*. Een superstijgende rij kan opgevat worden als een rij, waarvan elk element groter is dan de som van de voorafgaande elementen. Een voorbeeld van een superstijgende rij is

$$A' = (141, 203, 427, 981, 2406).$$

Stel nu dat  $S$  gelijk is aan 3590. Het knapsakprobleem kan dan eenvoudig opgelost worden. Als  $S = 3590$  dan moet  $x_5$  gelijk zijn aan 1. Stel dat dit niet zo zou zijn, dan zou de som van de overige elementen van  $A'$  kleiner zijn dan 2406 en daarmee nooit meer gelijk kunnen worden aan 3590. Dus 2406 maakt deel uit van  $S$ . Het restant is  $3590 - 2406 = 1184$ . Op grond hiervan valt te concluderen dat ook 981 in  $S$  moet zitten, dus  $x_4 = 1$ . Het restant wordt nu  $1184 - 981 = 203$ . Voor de vector  $X$  wordt dus gevonden  $X = (0, 1, 0, 1, 1)$ .

In het geval van superstijgende rijen kan  $X$  teruggevonden worden uit  $S$ .

Met behulp van superstijgende rijen is in principe dus een methode gevonden om bij toepassing in een cryptosysteem ontcijfering mogelijk te maken. Dit is echter niet voldoende, immers als de cijfertekst ontcijferd kan worden, kan het feitelijk door iedereen ontcijferd worden. Men dient dus een methode te bedenken waardoor de superstijgende rij zelf versluierd wordt. Dit kan als volgt geschieden.

*Knapzakstelsel met versluierde superstijgende rij*

Kies twee getallen  $u$  en  $v$ , zodanig dat ten eerste geldt dat  $u > \sum_i a_i$  en ten tweede dat  $u$  en  $v$  relatief priem zijn. Met behulp van deze twee getallen wordt de knapzakvector  $A$ , die superstijgend is, getransformeerd in een vector  $B$  met elementen:

$$b_i = va_i \pmod{u}, \text{ voor alle } i. \quad (6.22)$$

De vector  $B$  is openbaar;  $u$ ,  $v$  en  $A$  worden geheimgehouden. Met behulp van  $B$  wordt  $X$  gecijferd tot  $S$ :  $S = BX$ . Omdat  $B$  nu in het algemeen niet een superstijgende rij zal zijn is ontcijfering voor degene die over niet meer informatie beschikt onmogelijk. Alleen degene die ook over de geheime  $u$ ,  $v$  en  $A$  beschikt is in staat de cijfertekst te ontcijferen. Dit gaat als volgt in zijn werk. Op basis van  $v$  is de inverse  $v^{-1}$  uit te rekenen zodanig dat

$$v \cdot v^{-1} = 1 \pmod{u}. \quad (6.23)$$

Aan de ontvangzijde wordt nu  $S$  eerst vermenigvuldigd met  $v^{-1} \pmod{u}$ . Dit leidt tot

$$\begin{aligned} v^{-1} S \pmod{u} &= v^{-1} \sum_{i=1}^n b_i x_i \pmod{u} \\ &= v^{-1} \sum_{i=1}^n v a_i x_i \pmod{u} \\ &= \sum_{i=1}^n v^{-1} v a_i x_i \pmod{u} \\ &= \sum_{i=1}^n a_i x_i \pmod{u}. \end{aligned} \quad (6.24)$$

Op basis van de laatste term kan geconcludeerd worden, dat aan de ontvangzijde  $S$  gereduceerd is tot een som die wel betrekking heeft op een superstijgende vector en waarmee derhalve  $X$  opgelost kan worden.

### Voorbeeld

Kies bij wijze van voorbeeld de knapzakvector  $A = (3, 5, 9, 19)$ , welke een superstijgende rij is. Kies verder  $u = 40$  (er is voldaan aan  $u > 36$ ) en  $v = 7$ . De inverse  $v^{-1}$  laat zich als volgt berekenen

$$v \cdot v^{-1} = 1 \pmod{u} \Rightarrow 7v^{-1} = 1 \pmod{40} \Rightarrow v^{-1} = 23 \pmod{40}.$$

Vervolgens rekenen we de elementen van de versluierde rij uit met behulp van  $b_i = v \cdot a_i \pmod{u} = 7a_i \pmod{40}$ . De knapzakvector  $B$  wordt daarmee:  $B = (21, 35, 23, 13)$ .

Vercijfering van bijvoorbeeld  $X = (0110)$  levert dan:  $S = BX = 35 + 23 = 58$ .

Aan de ontvangzijde wordt de cijfertekst eerst vermenigvuldigd met  $v^{-1}$ , waarna  $X$  weer gevonden kan worden op basis van superstijgende rijen. Er volgt  $v^{-1} S \pmod{u}$   
 $= 23 \times 58 \pmod{40} = 14$ . Hetgeen leidt tot  $\sum_{i=1}^4 a_i x_i = 14$  en tenslotte tot  $X = (0110)$ .

△

## 6.4. Het breken van het knapzakstelsel

Lange tijd werd aangenomen dat de knapzakmethode veilig was. Beschouw echter de volgende situatie. In een of ander communicatienetwerk is sprake van een centraal systeem met daarmee verbonden een groot aantal kleinere systemen (bijvoorbeeld host-terminalverbindingen). Stel nu dat voor de communicatie tussen centraal systeem en de kleinere systemen gebruik gemaakt wordt van knapzakvectoren voor de beveiliging; voor elke verbinding een verschillende knapzakvector. Stel nu verder dat vanuit het centrale systeem het geval zich voordoet dat dezelfde boodschap  $X$  naar alle systemen gestuurd wordt. Voor de cijferteksten zal dan gelden:

$$S_k = \sum_{i=1}^n b_{ik} x_i, \quad (6.25)$$

waarbij de index  $k$  gerelateerd is aan een van de kleine systemen. In feite hebben we vanuit cryptanalytisch standpunt dan te maken met een stelsel lineair vergelijkingen. De waarden  $b_{ik}$  zijn bekend, want deze behoren tot de openbare sleutel. Als het aantal met het centrale systeem verbonden systemen groter is dan  $n$ , dan is het voor de cryptanalist in principe mogelijk de klare tekst  $X$  te bepalen! De conclusie is dus dat men in ieder geval niet één en dezelfde boodschap in meer dan één knapzak moet versturen.

In 1982 presenteerde Shamir (1984) een algemene methode, waarmee het knapzakstelsel gebaseerd op versluiting van superstijgende rijen gebroken kan worden. In de vorige paragraaf zagen we dat voor alle  $i$  geldt:

$$b_i = va_i \pmod{u}. \quad (6.26)$$

Omgekeerd zal ook gelden:

$$a_i = wb_i \pmod{u}, \text{ voor alle } i, \quad (6.27)$$

waarbij geldt  $w = v^{-1} \pmod{u}$ .

De superstijgende rij  $A$  is geheim, evenals  $w$  en  $u$ . De vraag is nu of het mogelijk is een paar  $(w, u)$  te vinden, zodanig dat de resulterende  $a_i$ 's een superstijgende rij vormen met een som kleiner dan  $u$ . Als dergelijke paren gegenereerd zouden kunnen

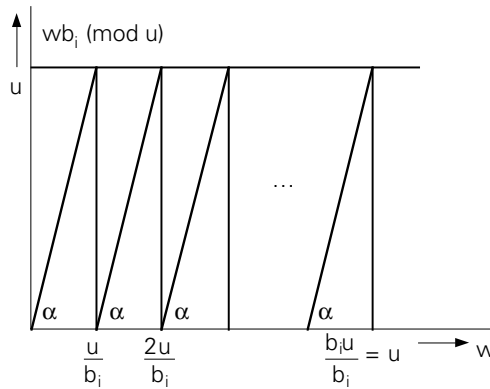
worden, dan zou met behulp hiervan de superstijgende rij  $A$  in principe gevonden kunnen worden, waarmee het algoritme dan gebroken is. Immers met de superstijgende rij kan bericht  $X$  uit som  $S$  opgelost worden. Shamir vond een methode om dergelijke paren te genereren. Zijn methode valt uiteen in twee delen:

1. Het vinden van een aantal kleine intervallen op  $[0,1]$ , waarbinnen  $w/u$  moet liggen.
2. Verdere verdeling van deze intervallen in subintervallen om gericht zoeken naar een paar gehele getallen met quotiënt  $w/u$  mogelijk te maken; waarna een kandidaat superstijgende rij  $A$  gegenereerd kan worden.

In grote lijnen komt de aanval op het volgende neer. Stel dat  $u$  in orde grootte van  $dn$  bits ligt, waarbij  $d$  een proportionele constante is. Overeenkomstig de eisen aan superstijgende rijen zullen de  $a_i$ 's van de volgende orde grootte zijn:

$$\begin{array}{ll}
 a_1: & dn - n \quad \text{bits,} \\
 a_2: & dn - n + 1 \quad \text{bits,} \\
 \dots & \dots \\
 a_i: & dn - n + i - 1 \quad \text{bits,} \\
 \dots & \dots \\
 a_n: & dn - 1 \quad \text{bits.}
 \end{array}$$

In figuur 6.2 is de curve  $w b_i \pmod{u}$  grafisch weergegeven, welke we hierna zullen aanduiden als de  $b_i$ -curve. Elke  $b_i$ -curve heeft precies  $b_i$  nulpunten. De onderlinge afstand tussen de nulpunten is  $u/b_i$ . Voor de hellingen die de ‘zaagtanden’ met de  $w$ -as maken geldt:  $\text{tg}(\alpha) = b_i$ .



Figuur 6.2. De  $b_i$ -curve als functie van  $w$ .

Beschouw nu de  $b_1$ -curve. Er moet gelden (vergelijk (6.27)):

$$a_1 = w b_1 \pmod{u}. \tag{6.28}$$

Voor de werkelijke waarde  $w$ , die in het algoritme gebruikt is en die moet voldoen aan vergelijking (6.28), geldt dat de afstand  $x_1$  van deze werkelijke  $w$  tot het dichtstbij

gelegen nulpunt links in de  $b_1$ -curve niet groter zal zijn dan ongeveer  $2^{-n}$ . Dit kan als volgt ingezien worden. Vanwege de  $(\text{mod } u)$  operatie in vergelijking (6.27) zal gelden dat alle  $b_i$ 's, inclusief  $b_1$ , ook orde grootte van  $u$  hebben, dat wil zeggen  $dn$  bits corresponderend met  $2^{dn}$ . Omdat  $\text{tg}(\alpha) = b_1$ ,  $a_1 (= wb_1)$  van orde grootte  $2^{dn-n}$  is en  $b_1$  van orde grootte  $2^{dn}$ , zal voor de afstand  $x_1$  gelden dat deze niet groter is dan  $2^{dn-n}/b_1 \approx 2^{-n}$ . Gezien de afstand tussen de nulpunten mag derhalve geconcludeerd worden, dat de gezochte  $w$  dus dichtbij een nulpunt moet liggen. Maar welke van de  $b_1$  nulpunten dit in de  $b_1$ -curve is, is niet bekend.

Stel dat dit het  $k_1$ e nulpunt is:  $k_1u/b$ . Er volgt dan

$$\frac{k_1u}{b_1} \leq w \leq \frac{k_1u}{b_1} + 2^{-n}. \quad (6.29)$$

Op dezelfde wijze zal voor de  $b_2$ -curve gelden dat, omdat  $a_2$  van orde grootte  $2^{dn-n+1}$  is, de gezochte  $w$  op een afstand niet groter dan  $2^{dn-n+1}/b_2 \approx 2^{-n+1}$  van een van de nulpunten van de  $b_2$ -curve moet liggen. Stel dit nulpunt is  $k_2$ , dan geldt:

$$\frac{k_2u}{b_2} \leq w \leq \frac{k_2u}{b_2} + 2^{-n+1}. \quad (6.30)$$

Meer algemeen zal voor de  $b_i$ -curve gelden:

$$\frac{k_iu}{b_i} \leq w \leq \frac{k_iu}{b_i} + 2^{-n+i-1}. \quad (6.31)$$

Gezien het feit dat de gezochte waarde van  $w$  voor elke  $b_i$ -curve dichtbij een nulpunt moet liggen, impliceert dat al deze nulpunten dichtbij elkaar moeten liggen. Door nu naar clusters van nulpunten te zoeken kan, weet men dat de gezochte  $w$  daar in de buurt moet liggen.

Een vraag die hiermee rijst is, over hoeveel  $b_i$ -curven men moet beschikken om met enige kans een dergelijk cluster van nulpunten te vinden. Het blijkt dat 4 bijeen gelegen nulpunten al voldoende garantie geven met een cluster te maken te hebben.

Stel we beschouwen  $t$   $b_i$ -curven. Beschouw nulpunt  $k_1u/b_1$  van de  $b_1$ -curve. Het dichtstbij gelegen nulpunt van de  $b_i$ -curve zal in het volgende interval moeten liggen:

$$\left[ \frac{k_1u}{b_1} - \frac{u}{2b_i}, \frac{k_1u}{b_1} + \frac{u}{2b_i} \right]. \quad (6.32)$$

Als we aannemen dat voor ieder punt van dit interval geldt dat de kans om een nulpunt daar aan te treffen even groot is, dan geldt dat de kans, dat het dichtstbij gelegen nulpunt van de  $b_i$ -curve op een afstand minder dan  $2^{-n+i-1}$  van het  $k_1$ e nulpunt van de  $b_1$ -curve ligt, gelijk is aan:

$$2^{-n+i-1}/(u/b_i) = 2^{-n+i-1}.$$

De kans dat de nulpunten van de  $b_2$ -curve tot en met de  $b_i$ -curve dichtbij het  $k_1e$  nulpunt van de  $b_1$ -curve liggen is:

$$2^{-n+1} \cdot 2^{-n+2} \dots 2^{-n+t-1} = 2^{-n(t-1)+t(t-1)/2}.$$

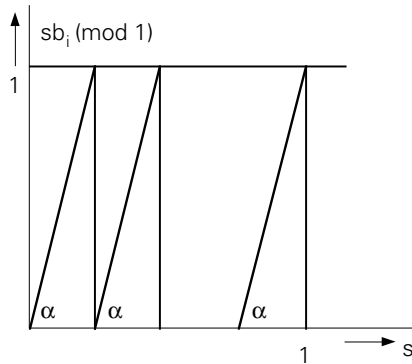
Omdat de gezochte  $w$  bij elk van de  $b_1$ -nulpunten kan liggen is de kans  $P$  op een cluster van  $t$  nulpunten gelijk aan:

$$P \approx b_1 \cdot 2^{-n(t-1)+t(t-1)/2} \approx 2^{dn-n(t-1)+t(t-1)/2}.$$

Stel  $d = 2$ ,  $n = 100$  en  $t = 4$  dan volgt  $P \approx 2^{-94}$ . Dat wil zeggen dat de kans dat het vinden van een cluster van 4 nulpunten op toeval berust zeer gering is. Daarom zal gelden dat als met 4  $b_i$ -curven een cluster van nulpunten gevonden wordt de gezochte  $w$  bijna zeker in de buurt zal liggen.

Wat tot nu toe niet aan de orde gekomen is wat met  $u$  aan te vangen; deze is immers ook niet bekend. En hoe een cluster te vinden.

We introduceren een nieuwe parameter  $s = w/u$ . Daarmee is  $w b_i \pmod{u}$  te herschrijven als  $s b_i \pmod{1}$ . Eenvoudig is na te gaan dat de curve van  $s b_i \pmod{1}$  een vorm heeft die identiek is met die van figuur 6.2. Vergelijk figuur 6.3. De helling blijft hetzelfde alsmede het aantal nulpunten. Het enige verschil is dat de afstand tussen de nulpunten een factor  $2^{dn}$  ( $u \approx 2^{dn}$ ) kleiner is. Het zoeken naar clusters van nulpunten kan dus ook aan de hand van de curven van figuur 6.3 geschieden.



Figuur 6.3. De  $b_i$ -curve als functie van  $s$ .

Het vinden van een 4-punts cluster vereist het oplossen van 3 lineaire ongelijkheden. Uit

$$\frac{k_i u}{b_i} \leq w \leq \frac{k_i u}{b_i} + 2^{-n+i-1}$$

volgt:

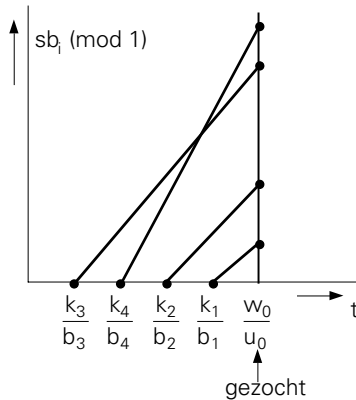
$$\frac{k_i}{b_i} \leq \frac{w}{u} \leq \frac{k_i}{b_i} + 2^{-dn-n+i-1}. \tag{6.33}$$

Hieruit volgt dat de grootste afstand die  $(k_1/b_1)$  en  $(k_2/b_2)$  uit elkaar liggen maximaal gelijk is aan  $2^{-dn-n+1}$ . We vinden achtereenvolgend:

$$\begin{aligned}
 0 &\leq \frac{k_1}{b_1} - \frac{k_2}{b_2} \leq 2^{-dn-n+1}, \\
 0 &\leq \frac{k_1}{b_1} - \frac{k_3}{b_3} \leq 2^{-dn-n+2}, \\
 0 &\leq \frac{k_1}{b_1} - \frac{k_4}{b_4} \leq 2^{-dn-n+3}.
 \end{aligned}
 \tag{6.34}$$

Met behulp van Lenstra's 'Integer programming algorithm' (Lenstra (1983)) zijn  $k_1$  tot en met  $k_4$  zonder al te veel inspanning te vinden.

Stel de gevonden waarden zijn zodanig dat de situatie van figuur 6.4 verkregen wordt, waarbij ook de hellingen van de bijbehorende 'zaagtanden' zijn gegeven. Merk op dat de hellingen steiler verlopen als  $i$  van  $b_i$  groter wordt. De gezochte  $w_0/u_0$  ligt rechts van  $k_1/b_1$  tot het volgende nulpunt van een der  $n$  curven.



Figuur 6.4. Het breken van het knapzak-algoritme.

Om gericht te kunnen zoeken verdelen we dit interval verder in subintervallen. Er zijn  $n$  lijnen/hellingen, die elkaar in maximaal  $n^2$  punten van het interval snijden. Er ontstaan daardoor maximaal  $n^2$  subintervallen. Binnen een subinterval snijden de lijnen elkaar niet. Voor elk van deze subintervallen geldt een bepaalde ordening van de grootten van de waarden van de zaagtandfuncties  $sb_i$  en daarmee van de elementen  $a_i$  van de oorspronkelijke knapzakvector. Als deze waarden een superstijgende rij vormen, dan kan men in dit interval verder zoeken naar een paar gehele getallen  $w$  en  $u$  met een quotiënt dat binnen dit subinterval ligt. Heeft men deze gevonden dan is het knapzakalgoritme gebroken. Immers nu kan uit  $S$  de originele boodschap  $X$  afgeleid worden.

Het knapzakalgoritme zou complexer gemaakt kunnen worden door eerst een superstijgende rij te versluieren met  $(v_1, u_1)$  tot  $B$ :

$$b_i = v_1 a_i \pmod{u_1} \text{ voor alle } i.$$

En vector  $B$  daarna opnieuw met  $(v_2, u_2)$  te versluieren tot  $B'$ :

$$b_i' = v_2 b_i \pmod{u_2} \text{ voor alle } i.$$

Ook dit soort systemen kunnen echter gebroken worden.

Nog steeds wordt gezien de eenvoud gezocht naar alternatieve methoden voor het knapzakprobleem, ofschoon tot op heden door de aanval van Shamir het vertrouwen in de veiligheid van enig cryptosysteem van dit type niet al te groot is.

## 6.5. Openbare-sleutelsystemen gebaseerd op elliptische curven

Zowel het RSA-systeem als het knapzakstelsysteem hebben gemeen dat ze gebaseerd zijn op zogenaamde trapdoor-functies. Functies die zelf gemakkelijk uit te rekenen zijn, maar waarvan de inverse moeilijker te berekenen is, tenzij men over additionele (geheime) informatie beschikt. Een meer recente ontwikkeling op het gebied van openbare-sleutelsystemen maakt gebruik van *elliptische curven*. Het gebruik van elliptische curven in de cryptografie is voor het eerst gesuggereerd door Miller (1986) en Koblitz (1987). Zonder al te diep in te gaan op de onderliggende wiskunde geven we een idee van hoe deze methode werkt. Voor meer details zij men verwijzen naar Menezes (1993).

Onder de *elliptische curve*  $F: y^2 = x^3 + ax + b$  gedefinieerd over  $Z_p$ , met  $Z_p$  de verzameling gehele getallen tussen 0 en  $p$ , wordt verstaan alle getallen paren  $(x, y) \in Z_p \times Z_p$  die voldoen aan:

$$y^2 = x^3 + ax + b \pmod{p}, \tag{6.35}$$

waarbij  $p$  een priemgetal,  $p > 3$  en waarbij  $a$  en  $b$  constanten zijn zodanig dat  $4a^3 + 27b^2 \neq 0 \pmod{p}$ .

Alvorens in te gaan op hoe elliptische curven gebruikt kunnen worden voor het creëren van openbare-sleutelsystemen is het noodzakelijk aandacht te besteden aan de punten die op  $F$  liggen alsmede aan hun onderlinge samenhang.

De punten op  $F$  kunnen gevonden worden door voor iedere  $x \in Z_p$ ,  $z = x^3 + ax + b \pmod{p}$  te bepalen en vervolgens op basis van vergelijking (6.35) te trachten  $y$  uit te rekenen. Dit is alleen mogelijk als  $z$  een *kwadratisch residu* is. Dat wil zeggen  $z$  is zodanig dat  $z = y^2 \pmod{p}$  een oplossing heeft. Het *criterium van Euler* (zie Kranakis (1986)) stelt dat  $z$  een kwadratisch residu modulo  $p$  is dan en slechts dan als:

$$z^{(p-1)/2} = 1 \pmod{p}.$$

Door beide zijden met  $z$  te vermenigvuldigen volgt ook:

$$z^{(p+1)/2} = z \pmod{p}.$$

Hieruit volgen dan de wortels

$$y = \pm z^{(p+1)/4}, \tag{6.36}$$

mits  $p$  geschreven kan worden als  $p = 3 \pmod{4}$ . In dat geval kunnen de punten op  $F$  gevonden worden.

### Voorbeeld

Beschouw de elliptische curve  $y^2 = x^3 + x + 5$  welke voor  $p = 11$  is gedefinieerd over  $Z_{11}$ . Nagegaan kan worden dat de constanten  $a = 1$  en  $b = 5$  voldoen aan de bij vergelijking (6.35) geformuleerde voorwaarde voor  $a$  en  $b$ . Omdat  $p = 11 = 3 \pmod{4}$ , zijn voor iedere  $x$  en daarmee corresponderende  $z$  de bijbehorende  $y$ -waarden gegeven door vergelijking (6.36). In Tabel 6.1 zijn de resultaten weergegeven.

Tabel 6.1. Punten op de elliptische curve  $y^2 = x^3 + x + 5$ .

$x$	$z = x^3 + x + 5 \pmod{11}$	kwadratisch residu	$y$	$(x, y)$
0	5	ja	4,7	(0,4) (0,7)
1	7	nee		
2	4	ja	2,9	(2,2) (2,9)
3	2	nee		
4	7	nee		
5	3	ja	5,6	(5,5) (5,6)
6	7	nee		
7	3	ja	5,6	(7,5) (7,6)
8	8	nee		
9	6	nee		
10	3	ja	5,6	(10,5) (10,6)

△

In dit geval worden er dus 10 punten gevonden. In het algemeen geldt dat het aantal punten in de orde van het priemgetal  $p$  ligt.

Door een geschikte keuze van de operator  $+$  kunnen de punten van de elliptische curve  $F$  opgevat worden als een *Abelse groep*. Dat wil zeggen de operator  $+$  is zodanig dat als  $P \in F$  en  $Q \in F$  dan ook  $P + Q \in F$ .

Stel  $P = (x_1, y_1) \in F$  en  $Q = (x_2, y_2) \in F$ , dan kiezen we de operator zo, dat als  $x_2 = x_1$  en  $y_2 = -y_1$ , dan  $P + Q = O$ , waarbij  $O$  een punt is met eigenschap  $P + O = P$  voor alle  $P \in F$ . Op basis hiervan geldt voor de inverse van  $P$  dat deze gelijk is aan

$(x_1, -y_1)$ . In alle andere gevallen geldt  $P + Q = (x_3, y_3)$ , waarbij

$$x_3 = \sigma^2 - x_1 - x_2 \pmod{p}, \quad (6.37)$$

$$y_3 = \sigma(x_1 - x_3) - y_1 \pmod{p},$$

en

$$\sigma = (y_2 - y_1)/(x_2 - x_1), \quad \text{als } P \neq Q, \quad (6.38)$$

$$= (3x_1^2 + a)/(2y_1), \quad \text{als } P = Q.$$

Door een willekeurige  $P \in F$  als uitgangspunt te kiezen, kunnen met de vergelijkingen (6.37) en (6.38) alle andere punten van de elliptische curve gegenereerd worden.

### Voorbeeld

We beschouwen wederom  $y^2 = x^3 + x + 5 \pmod{11}$ . Zoals we in het vorige voorbeeld hebben gezien is  $P = (0, 7) \in F$ . We bereken nu achtereenvolgens  $2P$ ,  $3P$ , ...,  $10P$  met behulp van de vergelijkingen (6.37) en (6.38). We beginnen met de berekening van  $2P$ .

$$2P = (0, 7) + (0, 7).$$

Met vergelijking (6.38) volgt:

$$\sigma = (3 \cdot 0^2 + 1)/(2 \cdot 7) = 1/14 = 4 \pmod{11},$$

$$\text{want } 4 \cdot 14 = 1 \pmod{11}.$$

Met vergelijking (6.37) levert dit:

$$x_3 = 16 = 5 \pmod{11},$$

$$y_3 = 4(0 - 5) - 7 = -27 = 6 \pmod{11}.$$

Hiermee wordt gevonden  $(5, 6)$ , wat inderdaad een punt van de elliptische curve is. De berekening van  $3P$  gaat als volgt.

$$3P = P + 2P = (0, 7) + (5, 6).$$

Vergelijking (6.38) geeft:

$$\sigma = (7 - 6)/(0 - 5) = -1/5 = 2 \pmod{11}.$$

Substitutie in vergelijking (6.37) levert:

$$x_3 = 2^2 - 5 = -1 = 10 \pmod{11},$$

$$y_3 = 2(0 - 10) - 7 = -27 = 6 \pmod{11},$$

waarmee het punt  $(10,6)$  wordt gevonden.

Op analoge wijze kunnen  $3P, 4P, \dots$  berekend worden. De resultaten zijn:

$$\begin{array}{ll} P = (0,7) & 6P = (7,6) \\ 2P = (5,6) & 7P = (2,9) \\ 3P = (10,6) & 8P = (10,5) \\ 4P = (2,2) & 9P = (5,5) \\ 5P = (7,5) & 10P = (0,4) \end{array}$$

Dit zijn precies de punten van tabel 6.1.

△

Bovenstaande resultaten kunnen gebruikt worden als basis voor het ontwerp van een cijfersysteem. Het is duidelijk dat voor gegeven  $P$  het voor iedere  $\alpha$  eenvoudig is het punt  $\alpha P$  te berekenen. Wat echter niet gemakkelijk is, is bij gegeven punten  $P$  en  $\alpha P$  de waarde  $\alpha$  te vinden. In het bovenstaande voorbeeld is het eenvoudig in te zien dat als  $(0,7)$  en  $(2,9)$  gegeven zijn dat dan moet gelden  $\alpha = 7$ . De waarde van  $\alpha$  kan gevonden worden door de complete lijst  $P, 2P, 3P, \dots$  etcetera aan te maken. Als echter het priemgetal  $p$  zeer groot gekozen wordt, zeg in de orde van  $2^{160}$ , dan zal het aantal punten op de elliptische curve in dezelfde orde van grootte liggen. En aldus zal het genereren van de lijst  $P, 2P, 3P, \dots$  ondoenlijk zijn.

#### *Het El-Gamal cijfersysteem gebaseerd op elliptische curven*

Laat  $F$  een elliptische curve gedefinieerd op  $Z_p$  ( $p$  priem en  $p > 3$ ).  $P$  is een punt op de elliptische curve:  $P \in F$ . Het getal  $\alpha$  is een geheim getal. Voor  $Q$  geldt:  $Q = \alpha P$  ( $Q \in F$ ). De openbare sleutel bestaat uit  $P$  en  $Q$ . Het getal  $\alpha$  maakt deel uit van de geheime sleutel.

Laat voor de te vercijferen boodschap  $M$  gelden:  $M = (u_1, u_2)$  met  $M \in F$ . Voor de vercijfering, waarbij  $k$  een random getal is, geldt nu:

$$C = e(M, k) = (v_1, v_2), \quad (6.39)$$

met

$$v_1 = kP \text{ en } v_2 = M + kQ. \quad (6.40)$$

Ontcijfering vindt plaats volgens:

$$d(C, \alpha) = v_2 - \alpha v_1. \quad (6.41)$$

○

Aangezien  $\alpha P = Q$ , is eenvoudig in te zien dat  $d(C, \alpha)$  weer de originele boodschap  $M$  oplevert. De sterkte van het algoritme is gebaseerd op de ondoenlijkheid om op basis van  $P$  en  $Q$ ,  $\alpha$  te vinden.

### Voorbeeld

Stel  $P = (0,7)$  en  $\alpha = 3$ . Hieruit volgt  $Q = 3(0,7) = (10,6)$ .

Stel de te vercijferen boodschap is  $M = (2,9)$ . Voor het random getal  $k$  geldt:  $k = 6$ .

Bij vercijfering bestaat de cijfertekst  $C$  uit twee elementen:

$$v_1 = 6P = (7,6),$$

$$v_2 = M + kQ = (2,9) + 6(10,6) = (10,6).$$

Ontcijfering geschiedt op basis van  $v_1$ ,  $v_2$  en  $\alpha = 3$ :

$$d(C,3) = v_2 - 3v_1 = (10,6) - 3(7,6) = (10,6) + 3(7,5) = (2,9).$$

Hierbij is gebruik gemaakt van het feit dat  $-(7,6) = (7, -6) = (7,5)$ .

△

Een nadeel van het algoritme is dat de te vercijferen boodschappen punten van  $F$  moeten zijn. In het cijfersysteem van Menezes-Vanstone mag een boodschap elk willekeurig getallenpaar zijn.

*Het Menezes-Vanstone cijfersysteem gebaseerd op elliptische curven*

Laat  $F$  een elliptische curve gedefinieerd op  $Z_p$  ( $p$  priem en  $p > 3$ ).  $P$  is een punt op de elliptische curve:  $P \in F$ . Het getal  $\alpha$  is een geheim getal. Voor  $Q$  geldt:  $Q = \alpha P$ .  $P$  en  $Q$  zijn openbaar.

Laat de te vercijferen boodschap zijn gegeven door  $M = (u_1, u_2)$ . Voor de vercijfering, waarbij  $k$  een random getal is, geldt nu:

$$C = e(M, k) = (y_0, y_1, y_2), \quad (6.42)$$

met

$$y_0 = kP, (c_1, c_2) = kQ, y_1 = c_1 u_1 \pmod{p}, y_2 = c_2 u_2 \pmod{p}. \quad (6.43)$$

Ontcijfering vindt plaats volgens:

$$d(C, \alpha) = (y_1 c_1^{-1}, y_2 c_2^{-1}), \quad (6.44)$$

waarbij  $\alpha y_0 = (c_1, c_2)$ . (6.45)

○

**Voorbeeld**

We nemen weer dezelfde waarden voor  $P$ ,  $Q$ ,  $k$  en  $\alpha$  als in het voorafgaande voorbeeld. De te vercijferen boodschap is  $M = (3,4)$ , wat nu geen punt op de elliptische curve  $F$  is.

Voor de elementen van de cijfertekst wordt achtereenvolgens gevonden:

$$y_0 = kP = 6(0,7) = (7,6),$$

$$(c_1, c_2) = kQ = 6(10,6) = (2,9),$$

$$y_1 = c_1 u_1 = 2 \cdot 3 \pmod{11} = 6,$$

$$y_2 = c_2 u_2 = 9 \cdot 4 \pmod{11} = 3.$$

Hieruit volgt

$$C = ((7,6), 6, 3).$$

Ontcijfering gaat als volgt:

$$(c_1, c_2) = \alpha y_0 = 3(7,6) = (2,9),$$

$$M = (y_1 c_1^{-1}, y_2 c_2^{-1}) = (6/2, 3/9) = (3,4). \quad \triangle$$

Beide van de hier behandelde methoden hebben als nadeel dat de cijfertekst tweemaal zo groot wordt als de klare tekst. Daar staat tegenover dat in het algemeen volstaan kan worden met kleinere priemgetallen dan in het geval van RSA, dat de openbare sleutel beperkt van grootte kan zijn en dat de rekencomplexiteit mede daarom ook beperkt is. In het algemeen kan gesteld worden dat vercijfering en ontcijfering op basis van elliptische curven vele malen sneller is dan bij RSA het geval is.