M. Vermeulen
*Business Information Europe, Ceylonpoort 5-25*
*Postbus 1, 2000 MA Haarlem*
*m.vermeulen@bie.vnu.com*

# Code

**Je kunt tegenwoordig geen krant meer openslaan of er staat een alarmerend stuk in over de onveiligheid van informatie-uitwisseling via Internet. "Hackers kraken website", "Internet zo lek als een mandje", "Malversaties op Internet met creditcards", "Persoonlijke gegevens op het net niet veilig", "Elektronisch betalen niet zonder risico", "Amerikanen luisteren Europees telefoon-, fax- en e-mailverkeer af", "Cyberwar behoort tot mogelijkheden". Het zijn dit soort koppen die met steeds grotere regelmaat in kranten en tijdschriften terugkeren. Was informatiebeveiliging vroeger vrijwel uitsluitend voorbehouden aan overheden, het leger en enkele grote ondernemingen – met de explosieve groei van Internet en de daarmee gepaard gaande toename van informatie-uitwisseling is informatiebeveiliging voor vrijwel iedereen van belang geworden.**

Een van de wapens die tegen onveilige datatransmissie in de strijd worden gegooid is cryptografie, oftewel de kunst van het versleutelen en ontcijferen van berichten, met het doel dat alleen de zender en de bedoelde ontvanger het bericht kunnen lezen zonder dat derden dit ook kunnen. Voor cryptografie worden sinds de jaren '70 in toenemende mate wiskundige technieken gebruikt. De NSA, die zich voor de Amerikaanse overheid bezig houdt met het afluisteren van internationaal telefoon-, fax-, telex- en e-mailverkeer, is nu de grootste werkgever van wiskundigen in de wereld. Alhoewel cryptografie slechts één aspect van databeveiliging is, is het wel een van de belangrijkste aspecten, zo belangrijk dat in de Verenigde Staten zelfs geruime tijd een exportverbod op cryptografie van kracht is geweest omdat men vond dat de staatsveiligheid met de verspreiding van cryptografische technieken in het geding kwam.

In het eind vorig jaar verschenen boek *Code* (naar mijn mening helaas niet de best mogelijke titel voor dit boek!) wordt de geschiedenis van cryptografie vanaf de Oudheid tot heden op een uiterst duidelijke en onderhoudende en bij vlagen zelfs spannende manier beschreven. Het boek is geschreven door Simon Singh en het is weinigen gegeven om op een zo duidelijke en boeiende manier over een sterk aan wiskunde verwant onderwerp te schrijven. Simon Singh is onder andere de maker van een BBC documentaire over de laatste stelling van Fermat, waarover hij ook een boek geschreven heeft met de titel *Het laatste raadsel van Fermat*. Dat Singh de kunst van het aan een niet noodzakelijk wiskundig geschoold publiek uitleggen van wiskundige onderwerpen goed verstaat blijkt uit het feit dat voor het lezen en begrijpen van zowel *Code* als van *Het laatste raadsel van Fermat* eigenlijk geen of hooguit heel weinig wiskundige voorkennis nodig is.

Cryptografie komt reeds voor bij de oude Grieken, Romeinen, Arabieren en Perzen. Bekend is bijvoorbeeld het (vrij eenvoudige) geheimschrift van Julius Caesar: elke letter wordt drie plaatsen opgeschoven, dus *Veni, Vidi, Vici* wordt YHQL, YLGL, YLFL. Behalve dit eenvoudige geheimschrift worden in *Code* vele andere geheimschriften behandeld bijvoorbeeld van Mary, 'Queen of Scots', dat echter ontcijferd werd waardoor ze uiteindelijk op het schavot belandde. Een goede illustratie hoe een geheimschrift letterlijk een kwestie van leven of dood kan zijn! Simon Singh legt tevens uit hoe eenvoudige geheimschriften met bijvoorbeeld frequentieanalyse ontcijferd kunnen worden. Geheimschriften werden oorspronkelijk eigenlijk alleen gebruikt in het diplomatieke verkeer en door het leger om het vijandelijke staten en legers zo moeilijk mogelijk te maken om geheime berichten te ontcijferen. Het breken door de Engelsen van de Duitse Enigma-code in de Tweede Wereldoorlog is waarschijnlijk van doorslaggevende betekenis geweest om de oorlog te bekorten doordat onder andere de geheime routes van Duitse U-boten bij de geallieerden bekend werden.

Tegenwoordig wordt cryptografie vrijwel overal gebruikt. Bijvoorbeeld door banken om geldtransacties te versleutelen zodat ze niet door 'digitale bankrovers' onderschept kunnen worden. Ook gewone e-mail wordt tegenwoordig vaak versleuteld om de privacy van zender en ontvanger te beschermen. Dit gebeurt met wiskundige cryptografische technieken zoals het Diffie-Hellman-algoritme en RSA die in het boek duidelijk uitgelegd worden (zie kader). Beide methodes zijn gebaseerd op zogenaamde 'éénrichtingsfuncties', dat wil zeggen functies die 'één kant op' makkelijk uit te rekenen zijn maar 'terug', zonder kennis van de geheime sleutel, vrijwel ondoenlijk zijn om uit te rekenen.

Gezien het toenemende belang van cryptografie wordt in het boek geruime aandacht besteed aan het debat 'cryptografie voor de happy few' versus 'cryptografie voor iedereen'. Voorstanders van het eerste standpunt betogen dat cryptografie in de handen van vijandelijke staten, terroristische groeperingen et cetera een te gevaarlijk wapen vormt. En inderdaad is aangetoond dat dit soort groeperingen gebruik maken van versleutelde berichten voor hun onderlinge communicatie. Pleitbezorgers van het tweede standpunt, met als een van de belangrijkste voormannen Phil Zimmermann, de bedenker en verspreider van PGP (Pretty Good Privacy, een aan RSA verwante cryptografiemethodiek), menen dat iedereen recht heeft op vertrouwelijke informatie-uitwisseling zonder dat 'Big Brother' meeleest of luistert. Het lijkt er op dat de laatste groep deze strijd in zijn voordeel gaat beslechten zodat de strijd tussen geheimschrift-makers en geheimschrift-ontcijferaars voorlopig nog wel even door zal gaan... Er zijn nog geen praktisch

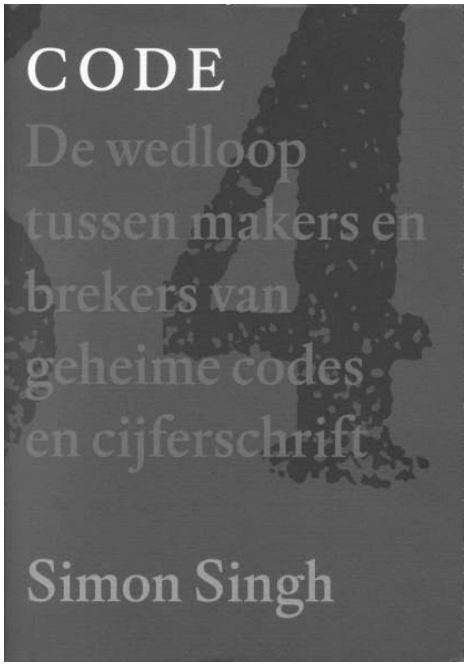
bruikbare geheimschriften bedacht waarvan bewezen kan worden dat ze zonder de sleutel onontcijferbaar zijn, met uitzondering van het 'eenmalig blokcijfer' dat echter bij elke nieuwe communicatie een nieuwe 'random' sleutel gebruikt, onafhankelijk van de vorige sleutel, hetgeen niet erg praktisch is. Overigens gaat het boek in het laatste hoofdstuk wel verder in op de theoretische mogelijkheid dat er echt bruikbare onbreekbare geheimschriften zullen komen (met behulp van de zogenaamde kwantum-cryptografie), maar ik vond dit hoofdstuk niet tot de beste en duidelijkste van het boek behoren.

*Code* gaat ook in op geheimschriften die nog steeds niet ontcijferd zijn, bijvoorbeeld het Beale geheimschrift dat de plek van een in de 19de eeuw begraven schat beschrijft in Virginia in de Verenigde Staten.

In het boek wordt ook een uitstapje gemaakt naar het ontcijferen van vreemde talen en alfabetten, bijvoorbeeld Egyptische hiërogliefen waarbij gebruik is gemaakt van cryptografische technieken. Maar er zijn ook talen die nog steeds niet ontcijferd zijn. Etruskisch bijvoorbeeld, alhoewel er tenminste duizend inscripties van zijn. Kortom, een veelzijdig en spannend boek dat ik zeer de moeite waard vind voor iedereen die in (de geschiedenis van) cryptografie geïnteresseerd is. De schrijver heeft in zijn boek een prijsvraag opgenomen bestaande uit tien te ontcijferen geheimschriften. Degene die als eerste alle tien — van makkelijk tot moeilijk oplopende — geheimschriften heeft ontcijferd kan £ 10.000,- verdienen! (Zie voor de prijsvraag ook de website http://www.4thestate.co.uk/cipherchallenge).

Mocht na lezing van dit boek Uw interesse geprikkeld zijn om meer over de wiskundige technieken te weet te komen die voor cryptografie gebruikt worden, dan kan ik U ook van harte het boek *Algebraic Aspects of Cryptography* van Neal Koblitz aanraden.

*Simon Singh,* ***Code, De wedloop tussen makers en brekers van geheime codes en cijferschrift***
*De Arbeiderspers, 1999, 460 p., prijs NLG 59,90. ISBN 90 295 3743 4*
*Nederlandse vertaling: Mea Flothuis*
*Oorspronkelijke titel* ***The Code Book, The Science of Secrecy from Ancient Egypt to Quantum Cryptography***
*Fourth Estate Limited, 1999, oorspronkelijke prijs £ 16,99*




**RSA**

Tweeduizend jaar lang werd het uitwisselen van decodeersleutels tussen zender en ontvanger als een van de zwakste plekken in een vercijferingssysteem gezien. Immers, degene die de sleutel onderschept kan het geheime bericht ontcijferen. Sinds de jaren '70 zijn er echter wiskundige manieren gevonden die hetzij het uitwisselen van geheime sleutels overbodig maken hetzij dit vrijwel zonder risico kunnen laten plaatsvinden. De zogenaamde public key-cryptografie waar RSA op gebaseerd is, maakt het uitwisselen van een geheime sleutel geheel overbodig: de zender maakt voor het verzenden gebruik van een publieke sleutel die de ontvanger gewoon kan publiceren. Alleen de ontvanger kan met zijn privésleutel, die hij wel geheim moet houden, het bericht decoderen. De publieke sleutel kan wel uit de geheime privé-sleutel worden afgeleid, maar het is vrijwel ondoenlijk om de geheime sleutel uit de publieke sleutel af te leiden. Dit kan dankzij het gebruik van een éénrichtingsfunctie; in het geval van RSA gebeurt dit door middel van grote priemgetallen: het is eenvoudig om twee grote priemgetallen met elkaar te vermenigvuldigen, maar met de huidige computers en algoritmes is het bijna onmogelijk om een gegeven groot getal (van enkele honderden cijfers lang) in een redelijke tijd te ontbinden in zijn priemfactoren.

**Diffie-Hellman**

Het Diffie-Hellman-algoritme maakt het mogelijk een geheime sleutel te coderen en via een openbaar kanaal te verzenden, zonder dat het voor een buitenstaander die het bericht onderschept, praktisch mogelijk is de geheime sleutel uit het gecodeerde bericht te ontcijferen. Ook dit algoritme is gebaseerd op het gebruik van een slimme éénrichtingsfunctie. Zonder op de wiskundige technieken in te gaan, kan het Diffie-Hellman-algoritme als volgt geïllustreerd worden. Stel, Alice wil een geheime sleutel naar haar vriend Bob sturen waarmee hij al haar toekomstige gecodeerde geheime berichten kan decoderen. De slimme truc die ze toepast om te voorkomen dat een buitenstaander de geheime sleutel te weten kan komen, gaat als volgt: Alice stopt de geheime sleutel in een metalen kistje en sluit dit af met een hangslot waarvan alleen zij de eveneens geheime sleutel heeft. Zij stuurt dit kistje naar Bob, en niemand die het kistje kan openmaken omdat alleen zij de sleutel van het hangslot heeft. Bob ontvangt het kistje en sluit het kistje *nogmaals* af met een *ander* hangslot, waar alleen hij de sleutel van heeft, naast het hangslot van Alice. Bob stuurt het kistje met de twee hangsloten terug naar Alice die haar eigen hangslot er van af haalt (alleen zij kan dat, omdat alleen zij de sleutel van haar eigen hangslot heeft). Vervolgens stuurt zij het kistje met alleen nog het hangslot van Bob er aan voor de tweede keer naar Bob. Bob haalt vervolgens zijn eigen hangslot er af, iets wat alleen hij kan, omdat alleen hij de sleutel van zijn eigen hangslot heeft. Nu kan Bob het kistje openmaken en kennis nemen van de geheime sleutel die door hem en Alice voor het ver- en ontcijferen van toekomstige geheime berichten gebruikt zal gaan worden. Deze illustratie toont aan dat het inderdaad mogelijk is een geheime sleutel via een openbaar kanaal te versturen, zonder dat zender en ontvanger elkaar zelfs maar hoeven te ontmoeten en zonder dat het voor een buitenstaander mogelijk is de geheime sleutel tijdens het transport te weten te komen.