Anne Keune
Vrije Universiteit, Faculteit der Exacte Wetenschappen,
Divisie Wiskunde en Informatica,
De Boelelaan 1081, 1081 HV Amsterdam
anne@cs.vu.nl

Boekbespreking In code, a mathematical journey

Sarah versus RSA

Sarah Flannery, dochter van een Iers wiskundige, baarde opzien door een nieuw cryptografisch systeem te ontwikkelen dat het meest gebruikte systeem RSA leek te kunnen vervangen. Hoe zij deze codering heeft gevonden en wat daarna kwam heeft zij, met haar vader als co-auteur, in een boek samengevat. Anne Keune, student informatica aan de Vrije Universiteit Amsterdam bespreekt het boek.

Met de opkomst van het internet is de behoefte om data beveiligd te kunnen versturen de afgelopen jaren enorm vergroot. Niet alleen voor bedrijven is dit van groot belang. Ook door het individu wordt een grote waarde gehecht aan het behoud van zijn of haar privacy.

Het principe van codering is echter al duizenden jaren oud. Zo werden door Julius Caesar, met het drie plaatsen verschuiven van het alfabet, al teksten gecodeerd. Aangezien het ontcijferen van een dergelijke code niet moeilijk is, volstaat deze manier inmiddels al lang niet meer. In het algemeen is men op zoek naar een gemakkelijk uitrekenbare functie waarbij het, zonder de juiste gegevens, zeer moeilijk of het liefst onmogelijk is de inverse van deze functie te vinden. Een dergelijke functie wordt ook wel een 'one-way' functie genoemd. Met andere woorden: de codering moet gemakkelijk uitvoerbaar zijn in tegenstelling tot de decodering die, zonder de juiste gegevens, een onmogelijke opgave moet zijn.

In Code, A Mathematical Journey, geschreven door Sarah Flannery in samenwerking met haar vader David Flannery, gaat over het project *Cryptography — A New Algorithm Versus RSA* waardoor de 16-jarige Sarah verscheidene vermeldenswaardige titels en prijzen, zoals *Ireland's Young Scientist of the year 1999* en de *Intel Excellence Award*, in ontvangst mocht nemen. Het boek gaat echter vooral over de weg hier naar toe en wat hier achteraf nog allemaal bij kwam kijken. Zoals de titel van haar project al impliceert, introduceerde Sarah, zij het met behulp van enkele anderen, een nieuw coderingsalgoritme, oftewel een nieuwe 'one-way' functie. Deze werd met name door snelheidsvoordelen door veel mensen als briljant beoordeeld.

In Code

"There is a blackboard in our kitchen." Zo begint Sarah Flannery haar boek en tevens vindt daar haar eerste kennismaking met de wiskunde plaats. Opgegroeid met een schoolbord in de keuken en met een docent wiskunde als vader is Sarah van jongs af aan spelenderwijs met wiskunde bezig geweest.Een groot gedeelte van het eerste hoofdstuk is opgebouwd uit kleine wiskundige puzzeltjes en vraagstukjes. Deze manier van schrijven geeft een leuke indruk van de manier waarop Sarah en haar familie zich thuis altijd met de wiskunde hebben bezig gehouden. Ook blijkt hieruit dat Sarah ontzettend enthousiast is over de wiskunde en over alles wat ze hierover thuis op het schoolbord heeft geleerd.

Het tweede hoofdstuk gaat hier op door, maar de gestelde vragen neigen steeds meer naar de getaltheorie en cryptografie. De meeste van

deze vragen zijn afkomstig uit de avondlessen wiskunde, met de naam *Mathematical Excursions*, die Sarah bij haar vader volgde. Deze dienen als opstap naar hoe Sarah tot het beginnen van haar eerste project is gekomen. Hoewel het meerdere keren in het boek aan mensen zonder wiskundige aanleg wordt afgeraden de hoofdstukken drie en vier te lezen, zou ik toch sterk willen adviseren dit wél te doen.

Omdat dit boek populair wetenschappelijk is en dus voor een groter publiek toegankelijk moet zijn, is het helaas zo dat er niet meer wiskunde behandeld wordt dan enkele eigenschappen van de modulorekening. Er zit een goede opbouw in de hoofdstukken die leidt tot genoeg wiskundige kennis om het RSA-algoritme, verder beschreven in hoofdstuk vijf, stapje voor stapje te begrijpen.

Dat dit boek voor groter publiek is geschreven blijkt ook uit de vier pagina's die nodig zijn voor de uitleg van de functienotatie in hoofdstuk drie. Voor de geïnteresseerde lezer staan er achter in het boek vier appendices. Twee met oplossingen van opgegeven puzzels en problemen en twee waarin dieper wordt ingegaan op de wiskundige aspecten nodig voor verder inzicht in de cryptografie. Ook deze zijn zeer duidelijk en systematisch geschreven; alleen jammer dat er steeds wordt aangenomen dat de lezer geen behoefte heeft aan het daadwerkelijke bewijs van gegeven stellingen.

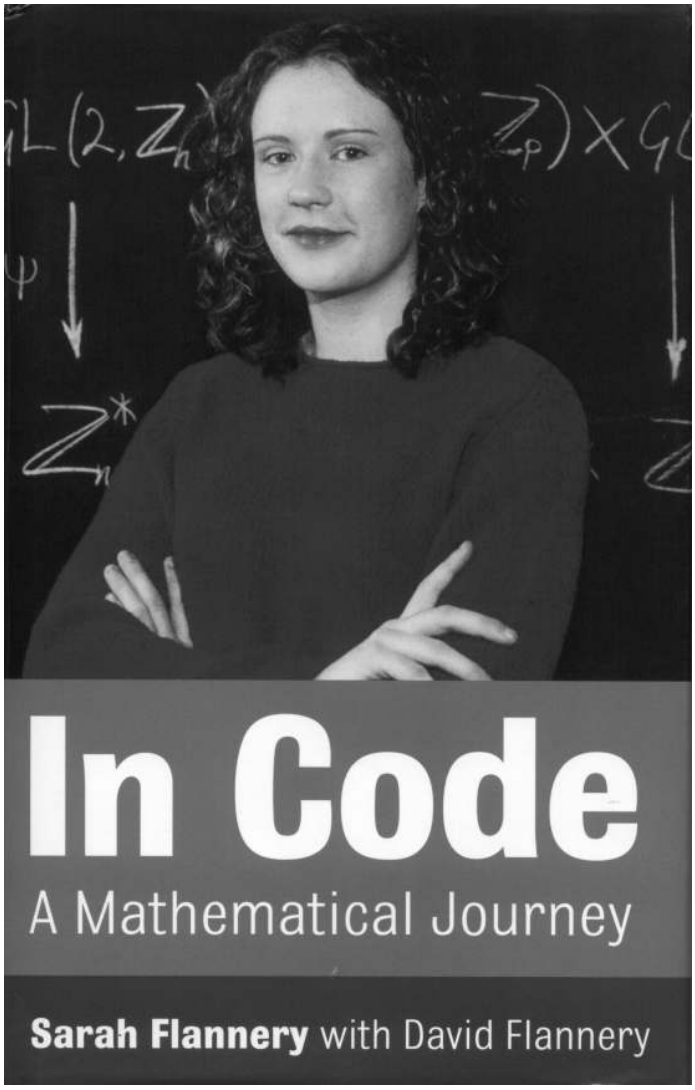
Een nieuw algoritme

Ondanks de titel *In Code, A Mathematical Journey* is dit niet het boek dat ik zou willen aanraden aan mensen die zich wat verder in de cryptografie willen verdiepen. Het boek geeft, naast het leuke verhaal, wel een goede algemene indruk van wat cryptografie inhoudt, maar cryptografie is duidelijk niet de essentie van het boek. Het boek is vooral erg leuk en interessant om te lezen als je benieuwd bent naar de persoonlijke ontwikkelingen van de schrijfster en naar alles wat er komt kijken bij (maar vooral na) het uitvinden van een nieuw coderingsalgoritme. Sarah's nieuwe coderingsalgoritme is gebaseerd op de ideeën van Michael Purser, oprichter van Baltimore Technologies. Omdat ze hierbij gebruik maakt van bepaalde technieken uit de matrixrekening, heeft Sarah haar coderingsalgoritme het Cayley-Purser algoritme genoemd. Doordat Sarah's algoritme enkel multiplicatie en geen exponentiële berekeningen bevat, kan dit algoritme twintig keer zo snel worden uitgevoerd als het momenteel meest gehanteerde RSA-algoritme. Dit zorgde voor nogal wat opschudding over de gehele wereld. Mede door verschillende lovende publicaties in verscheidene kranten werd Sarah op elke denkbare gelegenheid over de gehele wereld uitgenodigd haar ideeën te komen vertellen. Dit alles zonder dat de veiligheid van het algoritme bewezen werd. En inderdaad, tot ieders teleurstelling, werd het tegendeel bewezen: het algoritme was niet waterdicht.

Patent

Erg verbaasd was ik over de discussies die er ontstonden over de vraag of Sarah wel of geen patent moest aanvragen. Deze ontstonden, omdat Sarah's nieuwe ideeën direkt in het bedrijfsleven toepasbaar zijn en daar schuilt natuurlijk het grote geld. Samen met haar ouders had ze al tijdens het maken van haar project besloten geen patent aan te vragen. Dit omdat, voornamelijk in de opvatting van haar vader, wiskundige ideeën gratis met iedereen gedeeld zouden moeten worden en een wiskundig idee niet iets is wat je zou moeten kunnen bezitten. Toen Sarah's coderingsalgoritme echter door de pers en menig ander als briljant werd beschreven, brandde de discussie los. Over de gehele wereld vond men het belangrijk zijn of haar mening hierover te geven.

In het boek staan een handvol van deze reacties — gevonden op het internet — variërend van "God Bless this kid for not patenting her discovery" tot "Make money Sarah! Patent it! Don't throw away millions of dollars!!!!". Maar Sarah heeft naar mijn mening juist gehandeld en zich niet laten afleiden door wat de pers en individuen over haar schreven. Zelfs toen ze een aanbod kreeg om voor Pepsi reklame te maken, heeft ze dit afgewezen. Meewerken aan dergelijke reclame zou kunnen suggereren dat je intelligent wordt van het drinken van Pepsi, of dat je zelf niets liever dan Pepsi drinkt.



Natuurlijk hebben haar ouders een grote invloed gehad bij het maken van dit soort beslissingen. Toch vind ik het erg nobel van haar dat ze zich niet heeft laten afleiden van haar uiteindelijke doel.

Ondanks het feit dat het algoritme niet waterdicht was, wist Sarah toch met haar project en een toegevoegd verslag over de aanval op haar algoritme de *EU Young Scientist competition* te winnen en tevens een *Honorary Award* in ontvangst te nemen.

Ik vind het jammer dat in het boek niet het gehele Cayley-Purser algoritme staat beschreven, noch de aanval hierop. De reden die hiervoor wordt gegeven is dat de technische aard het voor opname in het boek ongeschikt maakte. Geïnteresseerden kunnen het algoritme vinden op de website http://www.cayley-purser.ie.

Sarah Flannery with David Flannery, ***In Code, A Mathematical Journey****, Profile Books, februari 2001, paperback; prijs ƒ 24.-, ISBN 1861972717.*