Boekbespreking

Na het grote succes van zijn boek over de Laatste Stelling van Fermat heeft de Britse fysicus, auteur en programmamaker Simon Singh opnieuw een gooi naar de bestsellerlijsten gedaan met *Code: de wedloop tussen makers en brekers van geheime codes en cijferschrift*. Ook dit boek geeft een historisch opgezet, zeer leesbaar overzicht over een vakgebied dat door zijn technische karakter slechts voor experts toegankelijk lijkt te zijn. Singh slaagt er echter in ook de leek te boeien met een relaas vol spannende, intrigerende, en soms zelfs bloedstollende episodes. Zo als bijvoorbeeld het verhaal van Maria Stuart, die haar hoofd verloor (letterlijk!) doordat haar nicht en aartsrivale Elisabeth I de inhoud ontcijferde van een compromitterend bericht dat Maria in code verstuurd had. En natuurlijk komt ook het verhaal van het kraken van de Enigma, de vercijfermachine waarmee de Duitse marine gedurende de Tweede Wereldoorlog zijn berichten versleutelde, uitgebreid aan de orde.

Meer dan de helft van de bijna vijfhonderd bladzijden is gewijd aan de 'klassieke' cryptologie, dat wil zeggen de cryptologie van voor het computertijdperk. De wiskunde speelde daarbij slechts een bescheiden rol. Dat werd anders toen in de jaren zeventig van de vorige eeuw *openbare sleutelsystemen* hun intrede deden. Het door Rivest, Shamir en Adleman bedachte systeem RSA berust op stellingen van Euclides, Fermat en Euler, en daarmee werd de getallentheorie in één klap van een speeltuin voor wereldvreemde, theoretische wiskundigen tot een booming business waarin miljoenen te verdienen zijn. RSA is nog steeds niet gekraakt, en het ziet ernaar uit dat de toepassingen ervan, bijvoorbeeld bij email en elektronisch betalen over het internet, nog lang niet zijn uitgeput.
Singhs gevoel voor anekdotiek en saillante details komt goed tot zijn recht als hij de wederwaardigheden beschrijft van de initiatoren van deze ontwikkelingen en en passant ook nog vermeldt hoe de revolutionaire ideeën rond publieke sleutels al jaren eerder door de Britse wiskundige en cryptoloog James Ellis op papier waren gezet. Maar Ellis werkte voor de Britse geheime dienst en mocht zijn vondst dus niet openbaar maken. In 1973 trad Clifford Cocks, een briljante jonge wiskundige, die in 1968 deel had uitgemaakt van de Britse ploeg bij de Internationale Wiskunde Olympiade in Rusland, in dienst van dezelfde organisatie. Nadat hij kennis had genomen van het memorandum van Ellis verzon hij, naar hij zelf zegt in een half uurtje, een getallentheoretische realisatie van Ellis algemene idee die niets anders was dan het systeem dat Rivest, Shamir en Adleman vier jaar later zouden publiceren. Uiteraard wisten de laatstgenoemden niets van de ontdekking van Cocks; pas in 1997 mochten Cocks en zijn collega's bekendmaken dat zij dezelfde ideeën al eerder ontwikkeld hadden. Ellis was toen al overleden. De betrokkenen zijn er overigens laconiek over: als je voor een geheime dienst werkt, moet je niet op publieke erkenning rekenen.

Zijn opleiding als fysicus kon Singh natuurlijk niet verloochenen: hij moest wel een hoofdstuk wijden aan de meest raadselachtige, maar tegelijkertijd ook uitermate speculatieve nieuwe ontwikkeling op dit terrein: de quantumcryptografie. Als de verwachting dat met quantumtechnieken praktisch werkende cryptosystemen gerealiseerd kunnen worden uitkomen, worden daarmee nieuwe, onkraakbare codes mogelijk, terwijl allerlei andere, tot nu toe veilig geachte systemen zoals RSA, de vuilnisbak in kunnen. De sceptische lezer zal het eerst allemaal willen zien voordat hij het gelooft, maar wie weet...

Code: de wedloop tussen makers en brekers van geheime codes en cijferschrift is een spannend en goed gedocumenteerd boek over een fascinerend vakgebied. Veel historisch materiaal, maar de moderne, wiskundige cryptologie komt er toch een beetje bekaaid af: wel RSA, maar weinig of niets over andere systemen of over digitale handtekeningen en identificatieprotocollen. De *Nieuwe Wiskrant*-lezer die ook een abonnement op *Pythagoras* heeft, zal in de 37e jaargang (1996/1997) op dit gebied meer aan zijn trekken zijn gekomen. Toch aanbevolen!

Jan van de Craats

Titel:	*Code: de wedloop tussen makers en brekers van geheime codes en cijferschrift*, vertaald door Mea Flothuis
Auteur:	Simon Singh
Uitg.:	De Arbeiderspers, Amsterdam, 1999
ISBN:	90-295-3743-4
Prijs:	*f* 59,90