Publicatie : Sir Edmund addendum Volkskrant
Datum : 13 feb 2016 Pagina : 44
cm2 : 1.168 Advertentiewaarde : € 25.000,00
Regio : Nederland
Frequentie : wekelijks
Oplage : 262.229

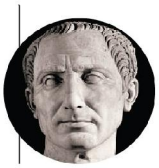
# WETENSCHAP

## INFORMATICA
## HOE BLIJVEN ONZE DATA VEILIG OPGEBORGEN?

1ste eeuw

**JULIUS CAESAR**
**Letterverwisseling**

Verschuift letters in een bevel een vast aantal plaatsen in het alfabet: ABBA wordt DEED



9de eeuw

**AL KINDI**
**Cryptoanalyse**

Gebruikt letterfrequenties om boodschap te decoderen

16de eeuw

**BLAISE DE VIGENÈRE**
**Multiverwisseling**

Geheim woord bepaalt via een tabel verschuivingen van elke letter in een boodschap

1835

**SAMUEL MORSE**
**Seinen**

Morsecode voor het elektronisch verzenden van berichten: ABBA wordt .--...-....-

Publicatie : Sir Edmund addendum Volkskrant
Datum : 13 feb 2016
cm2 : 1.168
Pagina : 44
Advertentiewaarde : € 25.000,00
Regio : Nederland
Frequentie : wekelijks
Oplage : 262.229

19de eeuw

**AUGUSTE KERCKHOFF**
**Standaardwerk**

*La Cryptographie Militaire*, de 'bijbel' voor makers en krakers

1940-45

**ALAN TURING**
**Computers**

Duitse Enigma-codes worden met elektronische rekenmachine gekraakt, deels Pools werk

1977

**RSA**
**Priemgetallen**

Versleuteling (Rivest, Shamir, Adleman) via openbare sleutels die uit moeilijk traceerbare priemgetallen zijn opgebouwd

1984

**CHARLES BENNETT EN GILLES BRASSARD**
**Quantumsleutels**

Eerste methode om met quantumtruc sleutels aan te maken

1993

**ARJAN EN HENDRIK LENSTRA**
**Cijferzeef**

Klassieke maar efficiënte wiskundige methodes om de priemfactoren in grote getallen te vinden

De geheimtalen waarmee we onze e-mail en onlinebankzaken versleutelen lijken niet lang meer veilig. Wat gaat de hackers van de toekomst dan wel weerstaan?

Door **Martijn van Calmthout** Foto **Rein Janssen**

# Sleutelen aan nieuwe sloten

De truc van een hangslot is dat het gemakkelijk dichtgaat en dan niet meer open. Zo simpel, zegt informaticus Harry Buhrman van het Centrum voor Wiskunde & Informatica en de Universiteit van Amsterdam, is het idee van cryptografie eigenlijk. 'Het gaat erom dat je voor het verhaspelen van een boodschap iets gebruikt dat eenvoudig is om te maken, maar verschrikkelijk moeilijk om uit elkaar te peuteren. Het liefst gewoon onmogelijk. Tenzij je de sleutel hebt of heel veel tijd.'

Buhrman, een vriendelijke bijna-vijftiger met een chaotische werkkamer vol papier, laptops en tennisballen, is komende maandag een van de gasten in het Kenniscafé in De Balie in Amsterdam, dat gaat over de kwetsbaarheid van onze geheimhouding. Hoe veilig, is de centrale vraag die informatici, cryptografen en hackers daar bespreken, zijn onze data eigenlijk opgeborgen?

Wat Buhrman betreft is de vraag zelfs nog specifieker: hoe zorg je dat data veilig opgeborgen blijven? Behalve hoogleraar aan de UvA en het CWI is hij ook directeur van het net opgerichte centrum QuSoft, dat software gaat ontwikkelen voor zogeheten quantumcomputers. Daarvan wordt binnen tien tot twintig jaar een ongekende rekenrevolutie verwacht. Wat nu nog onmogelijk ingewikkeld lijkt, bijvoorbeeld het vinden van een cryptografische sleutel uit talloze mogelijkheden, is tegen die tijd een kwestie van minuten. Met dank aan de quantumwetten rekenen quantumcomputers namelijk niet met enen óf nullen, maar met enen en nullen tegelijk. 'Die quantummachines gaan er komen, en we proberen nu te bedenken wat je ermee kunt', zegt Buhrman. Cryptografie is een veelgenoemd gebied.

**Binnenkort zijn daardoor**, althans in theorie, veelgebruikte cryptografische sloten op informatie bijna net zo makkelijk te openen als ze te sluiten waren. Weg veiligheid. En niet alleen die van staatsinlichtingen en militaire geheimen. Elke e-mail die we verzenden, elke keer dat we onze bankrekening checken, elk wachtwoord dat we aanmaken, elk boek dat we bij Amazon bestellen of elk jurkje bij Zalando: het wordt allemaal via versleutelde datacommunicatie afgehandeld. Zonder zou het een jungle zijn, daarbuiten in de digitale wereld.

En de zwartste nachtmerrie-scenario's liggen niet eens zo veel verderop in het dagelijkse bestaan. Als de cryptobeveiliging waarmee Microsoft zijn security updates verpakt breekbaar is, kan een slimme hacker een eigen achterdeurtje bouwen in vrijwel alle besturingssystemen ter wereld. 'Dan ben je God', zegt de Leids/Amsterdamse wiskundige Ronald Cramer.

**Wat mij betreft wordt er veel te gemakkelijk gedaan alsof quantum een toverstok is die alles kan kraken**

Cramer, een beer van een veertiger met een glimmende schedel, uitgesproken meningen en bewust geen smartphone, leidt aan hetzelfde CWI de cryptogroep, zeg maar de slotenmakers. De groep is onder meer vermaard om het werk aan systemen waarmee meerdere commerciële partijen kunnen bieden op rechten zonder dat ze elkaar in de kaarten kunnen kijken. Echt anoniem online stemmen en digitale handtekeningen zijn andere belangrijke toepassingen.

Cramer heeft zijn eigen opvatting over de voorspelde quantumrevolutie. 'Wat mij betreft wordt er veel te gemakkelijk gedaan alsof quantum een toverstok is die alles kan kraken. In werkelijkheid is een heel specifiek soort cryptosystemen kwetsbaar. Helaas zijn dat net die dingen die veel commercieel worden gebruikt. Maar er zijn alternatieven. Dat alles verloren zou zijn, is echt flauwekul.'

Ook in een wereld waar even- ➤

Publicatie : Sir Edmund addendum Volkskrant
Datum : 13 feb 2016 Pagina : 44
cm2 : 1.168 Advertentiewaarde : € 25.000,00
Regio : Nederland
Frequentie : wekelijks
Oplage : 262.229

1994

**PETER SHOR**
**Quantumrekenen**

Eerste algoritme dat via quantumvaagheid elke RSA-achtige code kan breken

2004

**IDQUANTIQUE**
**Quantumcrypto**

Eerste commerciële vorm van onafluisterbare quantumcommunicatie voor het versturen van sleutels

2015

**NSA**
**Post-quantum**

Aankondiging dat de Amerikaanse afluisterdienst zelf gaat overstappen op quantumbestendige cryptografie

20??

**QUANTUMCOMPUTERS**

Onder meer Delftse fysici sleutelen hard aan een bruikbare quantumprocessor, eerste serieuze systemen binnen tien jaar

## ALICE STUURT EEN MAILTJE NAAR BOB

Alice en Bob worden ze genoemd, de vaste hoofdpersonen in uitleg van cryptografische systemen.
Alice wil een geheime brief sturen aan Bob, die onderweg niet door derden te lezen is. Kan dat? Dat kan zeker. Ze stuurt Bob allereerst een verzoek om een slot. Bob stuurt een open hangslot naar Alice, die haar brief schrijft en die in een kistje stopt dat ze afsluit met Bobs slot. Ze stuurt dat kistje met brief op naar Bob, die het met zijn sleutel open maakt. Bob leest de brief.
Maar wat als Alice Bob wil mailen? In de digitale wereld speelt de wiskunde een reddende rol. Bijvoorbeeld via priemgetallen. Als Alice een bericht aan Bob wil sturen, zoekt ze zijn cryptocode op. Die openbare code heeft de vorm van een enorm getal, tot meer dan duizend cijfers lang. Speciale software op de computer van Alice versleutelt met die cryptocode haar bericht. De verzegelde boodschap gaat naar Bob. Zijn computer kent als enige de priemgetallen waarvan zijn cryptocode het product is. Die priemgetallen zijn nodig om de boodschap van Alice te ontwarren. Bob heeft de sleutel van het slot en kan dat. Een buitenstaander eigenlijk niet. Die kan alleen maar gissen naar Bobs priemgetallen.

► tueel quantumalgoritmen cryptosystemen aanvallen, hebben wiskundigen wel ideeën over geschikte vraagstukken van het asymmetrische type: wel makkelijk te maken, heel moeilijk uiteen te rafelen. Voorheen kwam de meeste klassieke moderne cryptografie uit de getaltheoretische hoek: schema's met priemgetallen, logaritmische functies, elliptische curves. Zulke schema's, de details doen er hier niet eens toe, hebben allemaal een vorm van periodiciteit, waardoor ze gevoelig zijn voor wat heet Shor's algoritme.

Die vondst uit 1994 van de Amerikaan Peter Shor gaat door het leven als de killer-app van het quantumkraken. Shor liet destijds in een wiskundig huzarenstukje zien dat met zijn aanpak het rekenwerk efficiënt blijft, ook als de te kraken getallen groter worden, waardoor het aantal mogelijkheden exponentieel oploopt. Dat kost sommige commerciële cryptosystemen op den duur de kop, zegt Buhrman.

Maar er is hoop. Inmiddels wordt nagedacht over fundamenteel ingewikkelder problemen als kortste afstanden tussen geheime punten in veeldimensionale puntenroosters, of rekensystemen waarin opzettelijke fouten worden geïntroduceerd die alleen met een geheime correctie gemakkelijk te vinden zijn. De betreffende wiskunde is zelf niet eens nieuw, zegt Cramer. Die stamt uit de jaren zeventig en tachtig, maar werd toen te ingewikkeld gevonden.

Wiskundig is van sommige cryptoschema's het gerede vermoeden dat ze niet sneller dan mogelijkheid voor mogelijkheid zijn na te rekenen. Zulke opgaven vergen bij een beetje omvang meer rekentijd dan het bestaan van het heelal. Meer dan zelfs een quantumcomputer aankan, is het idee.

Maar cryptografie, benadrukt Cramer, is meer dan mooie ideeën. 'Er zitten ook heel praktische kanten aan en in de praktijk is de eigenlijke crypto het veiligste element. Communicatie, afscherming, procedures: dat zijn vaak de kwetsbare schakels.'

**Sommige cryptoschema's zouden meer rekentijd vergen dan zelfs een quantumcomputer aankan**

Nederlandse wiskundigen spelen hoe dan ook en al van oudsher een prominente rol als luizen in de pels van de cryptografie, bijvoorbeeld voor het zogeheten public key protocol, waarbij een verzender van informatie het wiskundige equivalent van een open hangslot ophaalt bij de beoogde ontvanger, zijn boodschap ermee vergrendelt en verstuurt. De ontvanger is de enige met een sleutel die het slot openkrijgt.

**De broers Arjen** (voorheen Citi Bank en nu in Lausanne) en Hendrik Lenstra (Leiden) ontwikkelden in de jaren negentig de zogeheten *number field sieve*-methoden waarmee iets efficiënter naar de priemdelers in enorm grote cryptogetallen kan worden gezocht. Dat dwong de leveranciers van dat veelgebruikte RSA-cryptosysteem, dat op de praktische onvindbaarheid van zulke priemsleutels berust, steeds grotere publieke sleutels te gaan gebruiken: 256 cijfers werd 512 en tegenwoordig is dat al 1024 of nog meer, afhankelijk van de toepassing.

Zo gaat het in het vak eigenlijk altijd, zegt Cramer: 'Veiligheid is als een volumeknop die je nu en dan wat verder zult moeten opendraaien. Je kruipt dan wat verder naar rechts in de grafiek van toenemende moeilijkheid. Maar niet met een zover mogelijk.' ●

**KennisCafé De Kraakbare Wereld** maandag 15 februari, De Balie, Kleine-Gartmanplantsoen 10, Amsterdam. Met o.a. Harry Buhrman (CWI) en Tanja Lange (TU Eindhoven). Info: debalie.nl.