NH 12-01-10 katern 1 pagina 08

Digitale beveiliging weer wat minder veilig

Wiskundigen ontbinden een getal van 232 cijfers in twee priemgetallen en vestigen een record

Een nieuw wereldrecord in het ontbinden van een groot getal in twee priemgetallen betekent dat de beveiligers van digitale informatie naar nóg grotere getallen moeten uitwijken.

Door BENNIE MOLS

ROTTERDAM, 12 JAN. Een groep wiskundigen is erin geslaagd een getal van 232 cijfers te ontbinden in zijn twee priemdelers, priemgetallen met elk 116 cijfers. Daarmee hebben zij een nieuw wereldrecord gevestigd. Deze wereldrecords – het vorige is van vijf jaar geleden met een getal van 200 cijfers – zijn belangrijk, omdat de beveiliging van bijvoorbeeld het elektronische betalingsverkeer gebaseerd is op cryptografische versleutelingen met zulke grote getallen die in twee priemgetallen te ontbinden zijn.

De internationale groep, waaronder wiskundigen van het Centrum Wiskunde en Informatica in Amsterdam (CWI), heeft een wetenschappelijke publicatie over de priemgetallenontbinding aangeboden aan het elektronische preprintarchief *Cryptology*.

Priemgetallen zijn getallen die alleen deelbaar zijn door 1 en zichzelf. Ze spelen een cruciale rol in de beveiliging van digitale informatie. Wie via een beveiligde website zijn bankzaken doet of een bestelling betaalt, maakt er automatisch gebruik van. Die beveiliging, de zogeheten RSA-cryptografie (vernoemd naar de bedenkers Rivest, Shamir en Adleman) gebruikt grote gehele getallen die het product zijn van twee priemgetallen.

Het getal 15 is een voorbeeld van een getal waarvan we snel zien dat het ontbonden kan worden in twee priemgetallen, want: $3 \times 5 = 15$. Hoe groter het getal, hoe moeilijker het wordt om te weten of een getal een product is van twee priemgetallen én om die twee 'priemdelers' te vinden. Niemand heeft nog een oplossing gevonden voor dit 'factorisatieprobleem'.

De onwaarschijnlijkheid om getallen van een paar honderd cijfers snel te ontbinden in twee grote priemdelers ligt aan de basis van RSA-cryptografie. De beveiligers nemen twee grote priemgetallen en vermenigvuldigen die met elkaar. Het grote getal is daarna de beveiligingssleutel die de boodschap codeert. Een kwaadwillende kan de code alleen kraken als hij beide grote priemdelers kent. En dat kan alleen door het grote getal te ontleden in de priemgetallen – met brute rekenkracht.

> Het kraken van creditkaartcodes kost nog duizend keer zo veel rekentijd

Om de betrouwbaarheid van digitale beveiligingen te testen en nieuwe standaarden te bepalen, proberen wiskundigen met razendsnelle computers steeds grotere getallen te ontbinden in priemdelers. In feite vermenigvuldigen ze steeds twee grote priemgetallen, tot ze hebben bevestigd of uitgesloten dat een bepaald getal een product is van twee priemgetallen. Voor het nieuwe wereldrecord zou een gewone personal computer 1.700 jaar moeten rekenen. Door het kraken te verdelen over honderden snelle computers gaf 'RSA-768' (de 232 decimale cijfers van het getal zijn digitaal weergegeven in 768 bits) in 2,5 jaar zijn twee priemdelers prijs.

Die gekraakte 768-bits-sleutel wordt vrijwel alleen nog gebruikt voor het versleutelen van niet al te gevoelige informatie, die maar een paar weken geheim hoeft te blijven. Voor kwaadwillenden is het nog steeds geen peulenschil om zulke informatie te ontcijferen. Zij moeten over minstens dezelfde rekenkracht beschikken als de wiskundigen hebben gebruikt.

Gevoelige informatie die lange tijd geheim moet blijven, bijvoorbeeld een creditcardcode, wordt beveiligd met sleutels van 1.024 bits (309 decimale cijfers). Die zijn nog niet gekraakt en voorlopig veilig. „Het kraken daarvan is nog duizendmaal rekenintensiever", zegt Herman te Riele van het CWI, die aan het kraken van RSA-768 meewerkte. „Tien jaar geleden lag het wereldrecord bij een sleutel van 512 bits en vijf jaar geleden bij 663 bits. Ruwweg heb je voor iedere 256 bits extra duizendmaal zo veel rekentijd nodig om de priemdelers te vinden. We verwachten dat we over tien jaar een sleutel van 1.024 bits kunnen kraken. Eigenlijk zou je sleutels van 768 bits al niet meer moeten gebruiken. En over tien jaar zou een sleutel van ten minste 1.280 bits standaard moeten zijn."