

# Cryptografie

*Deze lesbrief is afkomstig van [www.rekenmeemetabc.nl](http://www.rekenmeemetabc.nl). Op deze site staat nog veel meer informatie, over het onderwerp van deze lesbrief en andere wiskundige onderwerpen. Ook zijn hier puzzels en wedstrijden te vinden.*



Cryptografie draait om het beveiligen van berichten tegen mogelijke vijanden van buiten. Hierbij hoef je niet direct aan oorlogssituaties te denken: ook bij het versturen van bijvoorbeeld creditcardgegevens over internet is cryptografie onmisbaar. Cryptografie wordt gebruikt voor het beveiligen van een bericht zodat een buitenstaander er geen informatie uit kan halen, maar ook om te controleren dat het bericht bij de juiste ontvanger aankomt. Het blijkt dat je hiervoor dezelfde technieken kunt gebruiken.

## Geheime sleutels

Bij de simpelste vorm van cryptografie hebben zender en ontvanger beide beschikking over dezelfde geheime sleutel. De zender codeert het bericht met deze sleutel en de ontvanger decodeert het bericht. Een buitenstaander die de sleutel niet kent, kan ook het bericht niet ontcijferen.

*Opgave 1:* Codeer het bericht MORGEN ZONNIG EN WARM met de volgende sleutel: verschuif de eerste letter 1 naar voren in het alfabet, de tweede letter 2, de derde letter 3, de vierde letter weer 1, enzovoorts.

*Opgave 2:* Denk je dat het verstandig is om heel veel tekst te versturen met dezelfde sleutel?

In de praktijk wordt de boodschap vaak eerst omgezet in nullen en enen. Die noemen we bits. Een sleutel kan dan bijvoorbeeld zijn: verander de bits (d.w.z. als het een nul was, wordt het een één en andersom) nummer 1, 3, 4, 6, 7, 9 en 11.

*Opgave 3:* Decodeer met deze sleutel het bericht 00111010011.

Soms is de zender niet genteresseerd in het geheimhouden van de boodschap, maar alleen in het controleren of de boodschap bij de juiste persoon is aangekomen. Ook dit kan als beide personen dezelfde geheime sleutel kennen. Met het (niet-gecodeerde) bericht stuurt de zender nu nog een extra berichtje mee, dat wel gecodeerd is.

*Opgave 4:* Bedenk een manier waarop de ontvanger hiermee kan aantonen dat hij inderdaad de persoon met de sleutel is.

## Publieke sleutels

Het grote probleem met de vorige methode is: hoe zorg je dat beide partijen dezelfde sleutel hebben terwijl de rest van de wereld deze sleutel niet heeft? Zeker bij communicatie over internet is dat een probleem, omdat de zender en ontvanger dan niet gemakkelijk elkaar de sleutel kunnen influisteren. Dit probleem is op te lossen door cryptografie met publieke sleutels te doen. Dit is wel wat ingewikkelder.

Stel ik codeer een geheime boodschap, namelijk een getal kleiner dan 91, op de volgende manier: ik doe het getal tot de macht 29 en neem vervolgens de rest bij deling door 91. Hier komt 72 uit.

*Opgave 5:* Bedenk een methode om te achterhalen wat mijn geheime boodschap was (voer het niet echt uit). Is dit een snelle methode?

De manier waarop ik mijn geheime boodschap codeer, is nu aan iedereen bekend. Dit noemen we een publieke sleutel. Toch is het heel moeilijk om te achterhalen wat mijn geheime boodschap is. Je kunt je voorstellen als de getallen nog wat groter zijn, dat het zelfs met een computer niet meer te doen is. Natuurlijk is het wel de bedoeling dat de ontvanger mijn boodschap kan ontcijferen. Daarom heeft hij nog een geheime sleutel, namelijk 5.

*Opgave 6:* Doe 72 tot de macht 5 en neem de rest bij deling door 91. Het getal dat hier uit komt, is mijn geheime boodschap.

**Tip:** Steeds 91 aftrekken om uiteindelijk op de rest uit te komen, is een hoop werk. Deel in plaats daarvan op je rekenmachine het getal door 91. Schrijf het getal op dat voor de komma staat. Ga nu weer terug naar het oorspronkelijke getal en trek hiervan af 91 keer het getal wat je opgeschreven hebt. Dat geeft de rest bij deling door 91.

*Opgave 7:* Controleer dat als je de geheime boodschap codeert zoals hierboven beschreven, dat je dan inderdaad op 72 uit komt.

**Tip:** Als de getallen te groot worden voor je rekenmachine, kun je het ook in stapjes doen. Je weet dat tot de macht 29 doen hetzelfde is als: eerst tot de macht 9, dan dat tot de macht 3, en de uitkomst nog twee keer vermenigvuldigen met het oorspronkelijke getal. Na elke stap mag je al de rest nemen bij deling door 91. Hierdoor blijven de getallen klein genoeg om mee te werken.

*Opgave 8:* Kan een buitenstaander op deze manier ook de geheime boodschap achterhalen? Kost dit hem veel tijd?

*Opgave 9:* Is het bij deze methode nodig dat twee mensen dezelfde geheime sleutel kennen, zoals bij de vorige methode?

In de praktijk zijn de getallen die gebruikt worden veel groter. De ontvanger berekent

de geheime en publieke sleutel en brengt de publieke sleutel naar buiten. De zender codeert zijn bericht met deze publieke sleutel en stuurt het naar de ontvanger. Zonder de geheime sleutel kost het terugvinden van de geheime boodschap veel te veel tijd, dus in de praktijk is het onmogelijk voor iedereen behalve de ontvanger om het geheime bericht te achterhalen.

*Opgave 10:* Kun je deze techniek ook toepassen om te controleren of een boodschap bij de juiste persoon is aangekomen?

*Opgave 11:* Codeer en decodeer zelf een bericht, waarbij de publieke sleutel is: tot de macht 113 en dan de rest bij deling door 143. De geheime sleutel die hierbij hoort is 17.

Deze methode van cryptografie heet RSA en is uitgevonden in 1977. Varianten hierop worden nog steeds overal toegepast, bijvoorbeeld op internet en bij de communicatie tussen pinautomaten en banken.