**De rol van wiskunde in de strijd tegen aliens**

*Een leger aliens is geland op onze planeet en plant een snelle invasie. Als opperbevelhebbers is het onze taak het mensenleger te doen zegevieren. Om de aliens te verslaan, moeten we weten waar ze zich precies bevinden en welke richting ze uitgaan. Natuurlijk kunnen we niet zomaar soldaten sturen naar de bezette regio’s: die worden meteen ontdekt en neergeschoten door de buitenaardse laserpistolen. Hoe kunnen we de Aarde redden van de ondergang?*

Al snel bedenken we een slim plan. We bevelen onze luchtmacht over het vijandelijke gebied te vliegen en duizenden *sensoren* te droppen. Sensoren zijn kleine toestelletjes (ongeveer zo groot als een muntstuk) die op batterijen werken en de bewegingen van de aliens kunnen registreren. Bovendien kunnen ze draadloos met elkaar communiceren. Wanneer de sensoren op de grond landen, vormen ze samen een groot netwerk: ze sturen hun informatie naar elkaar door totdat die bij ons aankomt. Met die gegevens kan ons leger de aliens in de pan hakken. Briljant!

**Jammer genoeg blijken de aliens toevallig experts te zijn in het onderscheppen van draadloze communicatie. Zo kunnen ze de informatie die naar ons wordt doorgestuurd aanpassen om ons op een verkeerd been te zetten en alsnog de wereld te veroveren. Om dat te vermijden, moeten we ons netwerk dus beveiligen. Maar hoe doen we dat? Gelukkig hebben we het bevel over wiskundigen die ons daarbij kunnen helpen. Zij leggen ons uit dat we zogenaamde *symmetrische encryptie* kunnen gebruiken. Het principe van symmetrische encryptie is eenvoudig: twee sensoren gebruiken eenzelfde geheime sleutel om hun boodschappen te coderen; alleen met die specifieke sleutel is het mogelijk hun berichten weer te ontcijferen. Dat klinkt perfect.

Er is echter een bijkomend probleem: nadat onze soldaten de sensoren hebben gedropt, kunnen ze er niet meer mee interageren. We moeten de sleutels voor encryptie dus op voorhand opslaan in de toestelletjes. Door onze beveiliging mogen twee sensoren enkel met elkaar communiceren als ze een gemeenschappelijke sleutel hebben. We moeten de sleutels dus zorgvuldig verdelen onder de sensoren. Er bestaat een moeilijk woord voor zo’n verdeelstrategie: een *sleutelpredistributie-schema* (afgekort SPS).

Ziezo, we hebben nu een duidelijke opdracht voor onze wiskundigen: bedenk een goed SPS. Daarmee kunnen we een veilig netwerk van sensoren maken, zodat we de aliens in de gaten kunnen houden. Al snel merken de wiskundigen op dat drie factoren belangrijk zijn bij het ontwerpen van een SPS. Ten eerste is er de *sleutelopslag*. Dat is het aantal sleutels dat elke sensor moet opslaan. Omdat sensoren erg klein zijn, is hun geheugen beperkt, dus we moeten proberen de sleutelopslag zo klein mogelijk te houden. Vervolgens is er de *connectiviteit* van het netwerk. Als een sensor geen buren heeft met gemeenschappelijke sleutels, dan kan hij zijn gegevens niet doorgeven. Om weinig kans te hebben op zulke nutteloze sensoren, moet de connectiviteit zo hoog mogelijk zijn. Dat wil zeggen dat zo veel mogelijk sensoren met elkaar moeten kunnen communiceren. Ten slotte willen we natuurlijk de *veiligheid* van het netwerk maximaliseren. Dat is belangrijk, omdat de aliens kunnen proberen sleutels te raden door de berichten van sensoren op te vangen.

Goed, laten we snel een SPS maken en die aliens verpletteren! Nu we al die dingen weten, moet dat een koud kunstje zijn, toch? Helaas, de wiskundigen sputteren weer tegen. Een wijsneus komt ons algauw uitleggen dat het allemaal niet zo eenvoudig is. Drie gemakkelijke voorbeelden moeten ons daarvan overtuigen.

Probeer eerst dezelfde sleutel in elke sensor op te slaan. Eén sleutel zorgt voor minimale sleutelopslag en laat elke sensor toe met alle andere sensoren te communiceren. Mooi zo. Maar als de aliens die ene sleutel raden, dan kunnen ze meteen alle berichten in het netwerk ontcijferen. Dit SPS is dus niet bepaald veilig.

Om de veiligheid te verbeteren, is het aangeraden het hergebruik van sleutels te beperken. Misschien kunnen we voor elk paar sensoren een unieke sleutel maken en die in beide toestellen opslaan? Op die manier hebben we nog steeds maximale connectiviteit. Bij het raden van één sleutel blijft de communicatie tussen alle andere sensoren veilig, omdat alle sleutels verschillend zijn. Ook de veiligheid is dus optimaal. Maar het nadeel van dit SPS schuilt in de sleutelopslag. In een netwerk met 1000 sensoren moet elk apparaat bijvoorbeeld 999 sleutels opslaan. Dat is veel te veel in de praktijk.

Een laatste poging: laten we in elke sensor slechts één unieke sleutel opslaan. Dan hebben we minimale sleutelopslag en maximale veiligheid. Oké, deze keer zien we het addertje onder het gras wel aankomen. Inderdaad, geen enkele sensor kan communiceren met andere sensoren. Compleet zinloos! Ook dit SPS is goed voor de prullenmand.

Uit pure wanhoop gooien we onze armen in de lucht. Het lijkt hopeloos. We zullen nooit de strijd tegen de aliens winnen, de mensheid is verloren! Smekend wenden we ons weer tot de wiskundigen. Wat moeten we nu doen? Een ander plan bedenken? Deze keer zijn we maar al te blij dat de wiskundigen ons geruststellen: we maken wel degelijk een kans. De laatste decennia hebben zij namelijk veel onderzoek gedaan naar SPSen. Ze bedachten een heleboel ingewikkelde manieren om sleutels te verdelen, gebaseerd op moeilijke wiskundige theorieën. Al die SPSen garanderen een beter evenwicht tussen sleutelopslag, connectiviteit en veiligheid. Dankzij die methoden kunnen we ons plan toch uitvoeren en de strijd aangaan met de aliens. Op naar de overwinning, met dank aan de wiskunde!

*Hoewel het belang van SPSen werd geïllustreerd met een spannende oorlog tegen aliens, zijn er nog ontelbare andere toepassingen. Sensoren worden vandaag al vaak ingezet in moeilijk bereikbare gebieden: ze meten de temperatuur in vulkaankraters, registreren voorbodes van aardbevingen in bergen, brengen de verspreiding van bosbranden in kaart, enzovoort. Het onderzoek naar SPSen is trouwens springlevend, aangezien wiskundigen tot vandaag niet voldoende begrijpen waarom sommige strategieën goed werken of beter zijn dan andere. Gezien de talloze toepassingen is het erg belangrijk verder te investeren in onderzoek. Kwestie dat we klaar zijn als die aliens toch komen…*