Activiteit 18

Kid Krypto—Publieke sleutel encryptie

Samenvatting

Encryptie is de sleutel tot informatie veiligheid. En de sleutel tot moderne encryptie is, dat een zender door alleen publieke informatie te gebruiken zijn boodschap zo kan versleutelen dat het alleen kan worden ontsloten (privé natuurlijk) door de beoogde ontvanger. Het is alsof iedereen een hangslot koopt, zijn naam er op schrijft en ze allemaal op dezelfde tafel leggen voor de anderen om te gebruiken. Ze houden de sleutel natuurlijk-de hangsloten zijn van het soort die je gewoon dicht klikt. Als ik jou een veilig bericht wil sturen, stop ik het in een doos, pak je hangslot, sluit de doos en stuur die naar jou. Zelfs als de doos in verkeerde handen valt, kan niemand anders het ontgrendelen. Met deze opzet is er geen noodzaak tot enige voorafgaande communicatie om geheime codes te regelen. Deze activiteit laat zien hoe dit digitaal kan worden gedaan. En in de digitale wereld, in plaats van je hangslot oppakken en gebruiken, kopieer je het en gebruik je de kopie en laat je de originele slot op de tafel liggen. Als ik een kopie van het fysieke hangslot zou moeten maken, kan ik dat alleen doen door het uit elkaar te halen. Daarbij zou ik onvermijdelijk zien hoe het werkte. Maar in de digitale wereld kunnen we regelen dat mensen sloten kopiëren zonder dat ze de sleutel kunnen ontdekken! Klinkt dat onmogelijk? Lees verder.

Vaardigheden

- Puzzels oplossen.
- Geheime codes.

Leeftijd

11 jaar en ouder

Materialen

De leerlingen worden verdeeld in groepen van ongeveer 4 en in die groepen vormen ze twee subgroepen. Elke subgroep krijgt een kopie van de twee kaarten op het werkblad Kid Krypto Kaarten. Dus voor elke groep leerlingen is nodig:

- twee kopieën van het werkblad Kid Krypto Kaarten.

Je hebt ook nodig:

een overhead projector transparant of projectie van Kid Krypto Coderen, en iets om op het diagram notities te kunnen maken.

Kid Krypto

Introductie

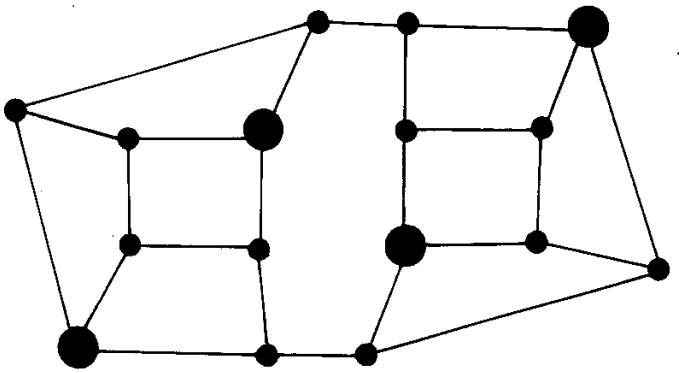
Dit is technisch de meest uitdagende activiteit in dit boek. Het vereist zorgvuldig werken en aanhoudende concentratie om het met succes te voltooien. Leerlingen moeten al het voorbeeld van een-weg functies hebben onderzocht in activiteit 14, Toeristenstad, en het is handig als ze de andere activiteiten in dit deel (Activiteit 16, Geheimen delen, en activiteit 17, De Peruviaanse toss) hebben afgerond. De activiteit maakt ook gebruik van ideeën die aan bod zijn gekomen in Activiteit 1, Tel de punten en Activiteit 5, Twintig keer raden.

Amy is van plan om Bill een geheim bericht te sturen. Normaal gesproken zouden we denken aan geheime boodschappen als een zin of paragraaf, maar in de volgende oefening zal Amy slechts één teken sturen - in feite zal ze een getal sturen, dat een teken vertegenwoordigt. Dit lijkt wel erg simpel, maar bedenk dat ze een hele reeks van dergelijke 'berichten' zou kunnen sturen om een zin te maken, en het werk zou gedaan kunnen worden door een computer. We zullen zien hoe Amy's getal te verstoppen in een versleuteld bericht met Bill's publieke slot zo dat als iemand het bericht onderschept, die niet in staat zal zijn om het te decoderen. Alleen Bill kan dat doen, want alleen hij heeft de sleutel tot het slot.

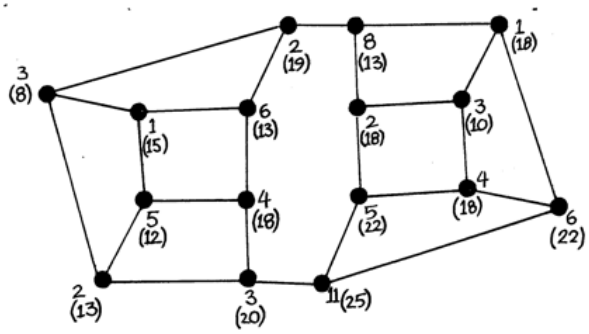
We zullen de berichten versleutelen door kaarten te gebruiken. Geen schatkaarten waar een X de schat markeert, maar straatkaarten zoals die van Toeristenstad (Activiteit 14), waar de lijnen de straten zijn en de stippen de kruispunten. Elke kaart heeft een publieke versie (het slot) en een privé versie (de sleutel).

Discussie

Op het werkblad Kid Krypto Coderen staat Bill's publieke kaart. Het is geen geheim: Bill legt het op de tafel (of een website) voor iedereen zichtbaar; hij geeft het aan iedereen die hem een bericht wil sturen. Amy heeft een kopie; net als iedere ander. Het figuur hieronder toont Bill's privé kaart. Het is hetzelfde als zijn publieke kaart behalve dat sommige kruispunten groter zijn. Hij houdt die versie van zijn kaart geheim.



Deze activiteit kun je het beste klassikaal doen of in ieder geval klassikaal starten, omdat het gaat om een behoorlijke hoeveelheid werk. Hoewel het niet moeilijk is, moet dit nauwkeurig worden gedaan, want fouten veroorzaken een hoop problemen. Het is belangrijk dat de leerlingen beseffen hoe vreemd het is dat deze vorm van encryptie op alle berichten kan worden toegepast (het lijkt onmogelijk) - Deze motivatie hebben leerlingen nodig om zich te concentreren voor deze activiteit. Een argument dat wij zeer motiverend voor leerlingen vonden is, dat met deze methode zij geheime notities kunnen sturen in de klas, en zelfs als hun leraar weet hoe het briefje werd gecodeerd, zal de leerkracht niet in staat zijn om het te decoderen.



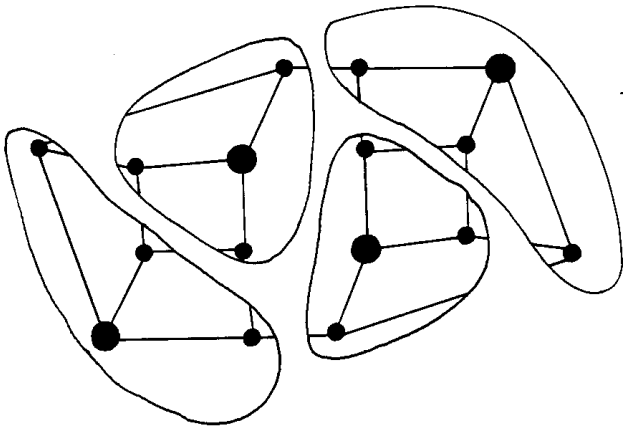
Toon Bill's publieke kaart (Kid Krypto Coderen werkblad). Bepaal welk getal Amy gaat sturen. Plaats dan willekeurige getallen op elke kruising op de kaart, zodat de willekeurige getallen samen opgeteld het getal zijn dat Amy wil verzenden. Deze afbeelding geeft

een voorbeeld van dergelijke getallen als de bovenste getallen (zonder haakjes) bij elke kruising. Hier heeft Amy gekozen om het getal 66 te sturen, zodat de getallen zonder haakjes samen opgeteld 66 zijn. Indien nodig, kun je negatieve getallen gebruikt om het totaal tot de gewenste waarde te maken.

Nu moet Amy berekenen wat ze naar Bill stuurt. Als ze de kaart met de getallen stuurt kan iedereen die de kaart in handen krijgt de getallen optellen en de boodschap begrijpen. In plaats daarvan moet Amy een kruispunt kiezen en naar dit kruispunt én de drie aansluitende kruispunten kijken (dus een totaal van 4 kruispunten) en alle getallen van deze 4 kruispunten bij elkaar optellen. Ze schrijft dit getal bij het kruispunt tussen haakjes of met een andere kleur pen. Bijvoorbeeld het meest rechtse kruispunt op de voorbeeldkaart is verbonden met 3 andere kruispunten met de getallen 1, 4, 11 en zelf heeft het getal 6. Dus dit is een totaal van 22. Herhaal dit voor alle kruispunten op de kaart. Je zou uit moeten komen op alle getallen die tussen haakjes staan.

Amy kan nu de kaart met alleen de getallen die tussen haakjes staan naar Bill sturen. Gum de oorspronkelijke getallen uit of maak een nieuwe kaart met alleen de nieuwe getallen. Laat de leerlingen ontdekken of ze uit kunnen vinden wat het originele bericht was. Dat zal ze niet lukken.

Alleen iemand met Bill's privé sleutel kan het bericht van Amy ontcijferen. Markeer op het gecodeerde bericht de kruispunten die op de sleutelkaart van Bill met een grotere stip zijn getekend. Om de boodschap te decoderen kijkt Bill alleen naar de geheime gemarkeerde kruispunten en telt de getallen bij deze kruispunten op. In het voorbeeld zijn deze kruispunten gemarkeerd met 13, 13, 22 en 18 en de som daarvan is 66. Amy's originele bericht.



Hoe werkt dit? De kaart van Bill is niet zo maar een kaart. Stel je voor dat Bill een gemarkeerd kruispunt zou kiezen en een lijn zou trekken om de kruispunten die op 1 straat afstand staan en dit herhaalt voor ieder gemarkeerd kruispunt. Dit leidt tot een indeling van de kaart in niet-overlappende delen, zoals hiernaast wordt geïllustreerd. Laat deze delen zien aan de leerlingen door de lijnen op de kaart te tekenen. De groep van kruispunten in ieder deel is exact de som van het gemarkeerde kruispunt, dus de som van de 4 gemarkeerde kruispunten op het gecodeerde bericht zal precies de som zijn van alle

originele getallen op de originele kaart, zodat dat het originele bericht van Amy is!

Poeh! Dat is een hoop werk voor het sturen van één letter. Dat klopt het is een hoop werk om een letter gecodeerd te sturen - encryptie is niet iets makkelijks. Maar kijk eens wat we bereikt hebben: complete geheimhouding met het gebruik van een publieke sleutel, waarin geen vooraf gemaakte afspraken nodig zijn tussen de boodschappers. Je zou je publieke sleutel kunnen publiceren op een website en iedereen zou je een geheime boodschap kunnen sturen, maar alleen diegenen die ook de privé sleutel hebben, zouden het bericht kunnen ontcijferen. En in het dagelijks leven worden de berekeningen gedaan door software (meestal ingebouwd in je webbrowser), dus alleen de computer moet heel hard werken.

Misschien is het leuk voor de leerlingen te weten dat ze nu tot een selecte groep behoren die echt met de hand en hoofd met publieke sleutel encryptie hebben gewerkt - computer-wetenschappers beschouwen dit als een onmogelijke taak en nog minder mensen hebben dit ooit gedaan!

En wat nu, als er afgeluisterd wordt? Bill's kaart is hetzelfde als de kaarten in de Toeristenstad activiteit (activiteit 14), waar de gemarkeerde kruispunten een minimale manier van IJscowagens plaatsen om alle straathoeken te kunnen bedienen waarbij niemand meer dan 1 straat hoeft te lopen. We zagen in Toeristenstad dat het makkelijk voor Bill is om zo'n kaart te maken door te beginnen met de stukken in zijn privé kaart en juist heel moeilijk is voor iemand anders om de minimale manier te vinden om ijscowagens te plaatsen behalve met de brute-kracht-methode. De brute-kracht-methode is om iedere mogelijk situatie met 1 wagen af te gaan, dan iedere mogelijke situatie met 2 wagens en zo voort tot je bij een oplossing komt. Niemand weet of er een betere methode is voor een algemene kaart - en al heel veel mensen hebben dit proberen te vinden.

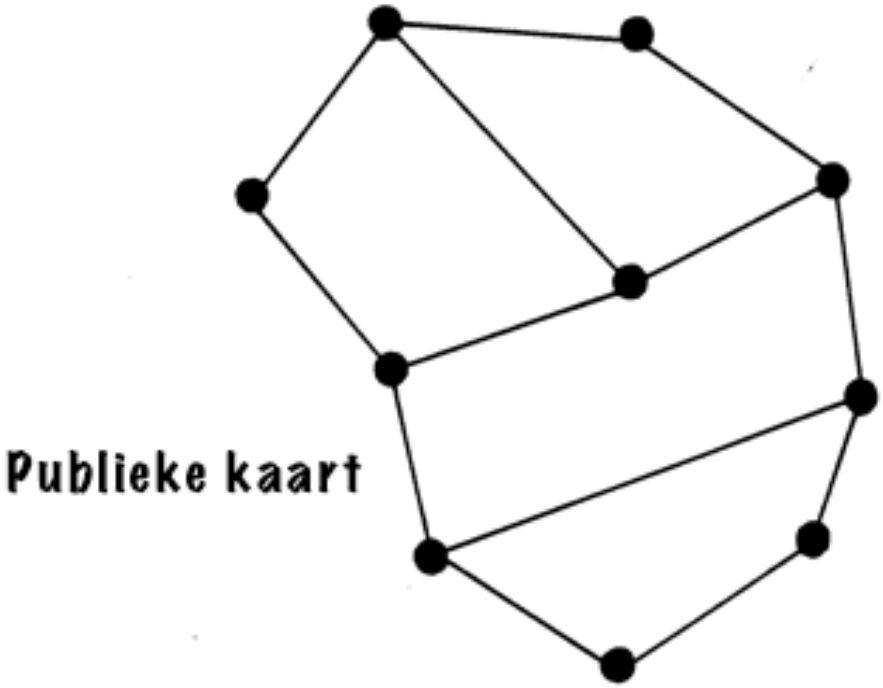
En als je aanneemt dat Bill begint met een heel ingewikkelde kaart, met bijvoorbeeld 50 of zelfs 100 kruispunten, dan lijkt het erop dat niemand de code zou kunnen kraken - zelfs de slimste wiskundigen hebben dit geprobeerd en zijn hier niet in geslaagd. (Maar er is een addertje onder het gras: zie bij "Waar gaat dit allemaal over?")

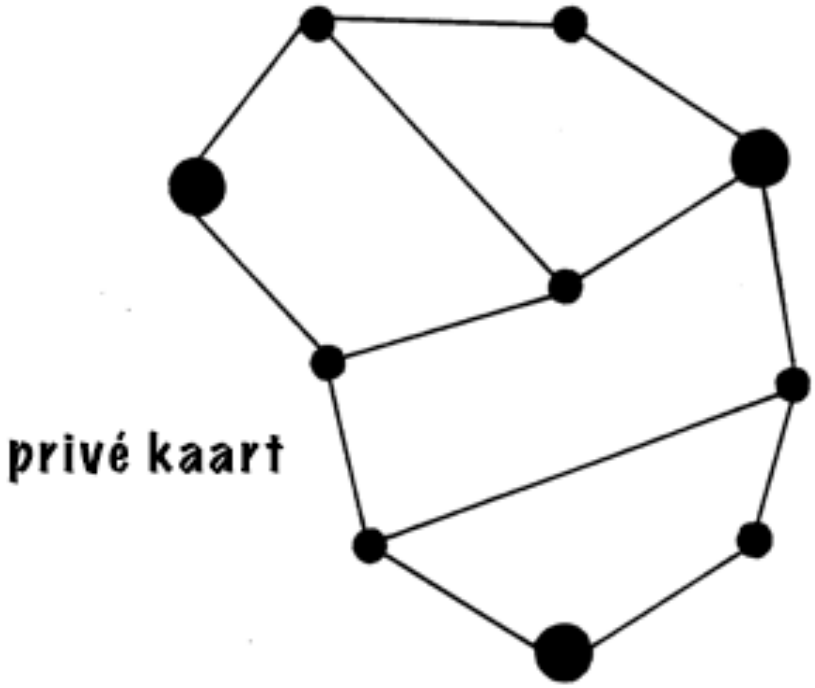
Nu de hele klas het voorbeeld gezien heeft, deel je de klas in een even aantal groepen, bijvoorbeeld 4. Geef de helft van de groepen de publieke kaart van de Kid Krypto Kaarten. Deze groepen kiezen een "bericht" (ieder heel getal), coderen dit met de publieke sleutel en geven het gecodeerde bericht aan de andere groep. De andere groep kan proberen dit te ontcijferen, het is onwaarschijnlijk dat ze hierin slagen totdat ze de privé kaart krijgen (of ontdekken!). Geef ze uiteindelijk de privé kaart en kijk of ze het bericht nu kunnen ontcijferen.

Nu kan ieder groepje haar eigen kaart maken, waarbij ze de privé versie geheim houden en de publieke versie aan de andere groep geven of het via het digibord publiek maken. Het principe voor het ontwerpen van de kaarten is precies hetzelfde als beschreven in de activiteit Toeristenstad en extra wegen kunnen toegevoegd worden om de oplossing nog beter te verbergen. Zorg er wel voor dat je geen extra straten toevoegt aan de "speciale" kruispunten. Dat zou een kruispunt creëren waarbij twee ijscowagen in een sprong gehaald kunnen worden, dat is prima voor de Toeristenstadsituatie, maar geeft problemen met encryptie. Omdat nu de "speciale" kruispunten nu niet meer de kaart verdelen in niet-overlappende delen zoals geïllustreerd werd in de privé kaart, en dat is essentieel voor de encryptie truc om te werken.

Werkblad Activiteit: Kid Krypto Kaarten

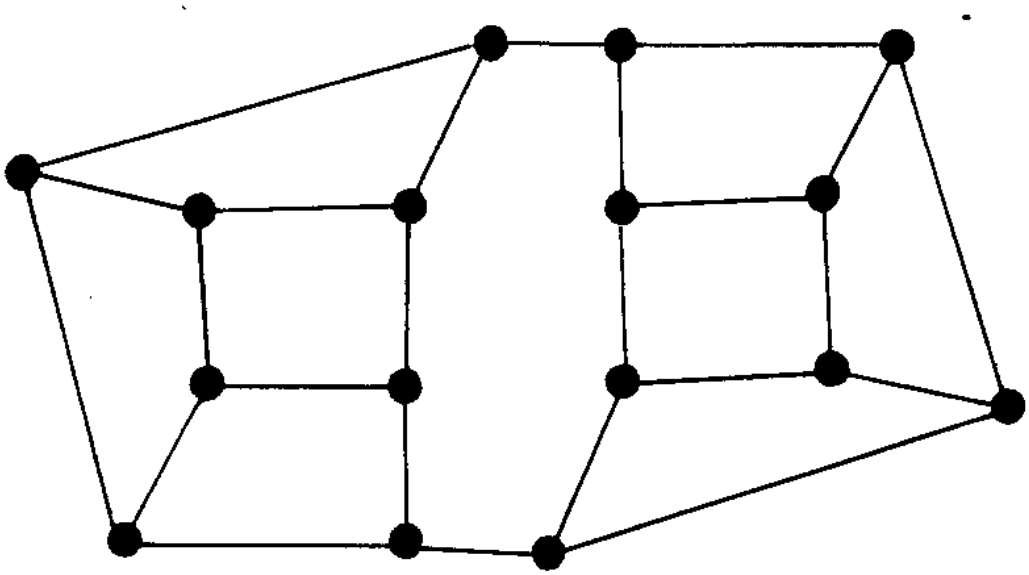
Gebruik deze kaarten zoals beschreven in de tekst om berichten te versleutelen en te ontcijferen.





Werkblad Activiteit: Kid Krypto Coderen

Laat deze kaart aan de klas zien en gebruik het om te laten zien hoe je een bericht codeert.



Waar gaat dit allemaal over?

Het is belangrijk dat we via computernetwerken berichten kunnen versturen die alleen door de beoogde ontvanger kunnen worden gelezen, dat niemand -hoe slim of rijk ze ook zijn- in staat is om het bericht te begrijpen als ze het onderscheppen. Er zijn heel wat manieren hiervoor die ervan uitgaan dat zender en ontvanger allebei beschikken over een geheime code om hun berichten te versleutelen en ontcijferen. Het bijzondere van public-key encryptie ia dat Amy veilig een bericht aan Bill kan sturen zonder vooraf zo'n geheime code af te spreken. Amy kan gewoon op een open toegankelijke plaats, een webpagina bijvoorbeeld, het slot vinden dat ze moet gebruiken voor de versleuteling van het bericht.

Cryptografie gaat over meer dan geheime berichten, een andere toepassing is authenticatie, het vaststellen of iemand wel is die hij of zij zegt te zijn. Hoe weet Amy dat een bericht echt van Bill komt en niet van een bedrieger die zich voordoet als Bill? Bijvoorbeeld als er email binnenkomt met "Liefste, ik zit hier vast zonder geld. Maak alsjeblieft even € 100 over naar mijn bankrekening NL12IBAN0003456789. Liefs, Bill"? Hoe weet ze dat het echt Bill is die geld van haar nodig heeft? Sommige cryptosystemen kunnen ook voor dit probleem worden ingezet. Vergelijkbaar met hoe Amy een bericht aan Bill kan sturen door zijn publieke sleutel te gebruiken, kan Bill een bericht aanmaken dat alleen hij kan aanmaken door gebruik te maken van zijn privé sleutel. Als het Amy lukt om het bericht te ontcijferen met Bill's publieke sleutel weet ze zeker dat het van hem afkomstig is. Iedereen die het bericht onderschept kan op dezelfde manier de inhoud ontcijferen. Als Bill wil dat alleen Amy het bericht kan lezen moet hij het nogmaals versleutelen met Amy's publieke sleutel. Deze dubbele versleuteling op basis van de dezelfde publieke en privé sleutels zorgt ervoor dat Amy en Bob veilig met elkaar kunnen communiceren in de zekerheid dat ze ook echt met elkaar praten.

Op dit moment kunnen we toegeven dat de methode zoals gebruikt bij deze activiteit weliswaar lijkt op de in de praktijk gebruikte krachtige versleuteling, maar toch niet veilig is, zelfs niet als er met een grote kaart gewerkt wordt.

Hoewel er geen effectieve manier bekend is om een minimaal aantal ijsco-karretjes om een willekeurige kaart te plaatsen, waarmee de methode in principe veilig is, blijkt er compleet andere manier te zijn om de code te lijf te gaan. Die nadere manier zal de meeste scholieren ontgaan, maar het is toch goed te weten dat het bestaat. Je zou kunnen zeggen dat de besproken aanpak veilig is voor scholieren onderling maar niet veilig als er wiskundigen in de buurt zijn. Sla de volgende paragraaf gerust over als je wiskundige interesse bescheiden is.

Nummer de kruispunten op de kaart 1, 2, 3, … Noem de originele getallen die aan de kruispunten zijn toegevoegd b1, b2, b3, ..., en de nummers die uiteindelijk worden verzonden t1, t2, t3, ... Veronderstel dat kruispunt 1 is verbonden met kruispunten 2, 3 en 4. Dan is het doorgezonden getal voor dat kruispunt
t1 = b1+b2+b3+b4 .

Op dezelfde manier kunnen vergelijken worden opgesteld voor elk ander kruispunt, er zijn zo evenveel vergelijken als onbekende b1, b2, b3, ... Een luistervink die de kaart kent en de getallen t1, t2, t3, ... die verzonden worden kan het stelsel van deze vergelijkingen oplossen met een computerprogramma. En wanneer je zo de onbekende b1, b2, b3, ..., hebt bepaald, hoef je ze alleen nog maar op te tellen om het geheime getal terug te vinden, de geheime kaart voor ontcijfering is helemaal niet nodig. De tijd die de computer nodig heeft om het stelsel vergelijkingen op te lossen groeit als een derde macht van het aantal kruispunten, en de methode staat bekend als Gauss eliminatie. Maar omdat in de vergelijkingen maar een beperkt aantal kruispunten worden beschouwd, waarmee alle andere kruispunten met een factor 0 worden meegenomen, bestaan er efficiëntere technieken. Vergelijk dit met de aanpak met brute kracht, waarmee we alle mogelijkheden langs gaan, die voor zover we weten het beste is wat we kunnen doen met de ontsleutelingskaart.

We hopen dat je je niet in de maling voelt genomen. De manier waarop publieke sleutel encryptie in de praktijk werkt is vrijwel identiek aan wat wij hebben gedaan, alleen wordt er voor versleutelen een andere methode gebruikt die we niet makkelijk met pen en papier kunnen laten zien. De oorspronkelijke methode voor publieke sleutel encryptie, en nog altijd een van de meest veilige, is gebaseerd op het feit dat het heel moeilijk is om grote getallen te ontbinden in factoren.
Wat zijn de factoren van het 100-cijferige getal 9.412.343.607.359.262.946.971.172.136.294.514.357.528.981.378.983.082.541.347.532.211.942.640.121.301.590.698.634.089.611.468.911.681? Probeer het niet te lang!
Het zijn 86.759.222.313.428.390.812.218.077.095.850.708.048.977 en 108.488.104.853.637.470.612.961.399.842.972.948.409.834.611.525.790.577.216.753. Er zijn geen andere factoren, want dit zijn twee priemgetallen. Het vinden ervan is een zware klus, een supercomputer heeft er maanden voor nodig.

In een realistisch encryptie systeem kan Bill het 100-cijferige getal als publieke sleutel gebruiken en de twee priemfactoren als zijn privé sleutels. Het vinden van zulke sleutels is niet al te moeilijk: alles wat je nodig hebt zijn twee grote priemgetallen. Zoek twee priemgetallen die groot genoeg zijn (dat is te doen), vermenigvuldig ze en je hebt je publieke sleutel. Het vermenigvuldigen van grote getallen is voor een computer niet zo moeilijk. Maar niemand kan uit de publieke sleutel je privé sleutel afleiden, tenzij ze

maanden de beschikking hebben over een supercomputer. En mocht dat je zorgen baren dan neem je een publieke sleutel van 200 cijfers i.p.v. 100, dan is de supercomputer jaren zoet. Het belangrijkste is dat het kraken van de sleutel duurder is dan de waarde van de informatie die erdoor ontsloten wordt. Op dit moment is het gebruikelijk om voor een veilige internetverbinding gebruik te maken van 512-bit sleutels, dat komt overeen met een getal van ongeveer 155 cijfers.

We hebben nog niet uitgelegd hoe je met een publieke sleutel gebaseerd op een priemgetal een bericht kunt coderen, zodat het alleen te ontcijferen valt met de privé sleutel. De eerlijkheid gebied te zeggen dat dat ook net wat ingewikkelder is dan we het boven hebben uitgelegd. De methode werkt niet direct met de twee priemfactoren maar met andere getallen die daarmee gemaakt kunnen worden. Maar de essentie is hetzelfde: als je grote getallen in hun priemfactoren kunt ontbinden kun je de code kraken. We laten de details van de echte methode hier achterwege; we hebben al hard genoeg ons best gedaan om het idee erachter te begrijpen.

Hoe veilig is zo'n systeem gebaseerd op priemgetallen? Nou, het ontbinden van grote getallen in priemfactoren houdt de knapste wiskundigen al eeuwen bezig. En, hoewel er methodes zijn gevonden die veel beter zijn dan met domme kracht alle getallen te proberen, is er nog niemand die een snel algoritme (snel als in polynomiale tijd) heeft gevonden. Evenmin heeft iemand bewezen dat zo'n algoritme niet kan bestaan, Daarmee lijkt de methode niet alleen goed genoeg voor op school maar ook goed genoeg voor wiskundigen. Maar we moeten ons bewust blijven dat ooit iemand een methode ontdekt om de boodschap te ontcijferen zonder gebruik te maken van ontbinden in priemfactoren (zoals de behandelde techniek gekraakt kon worden zonder naar de kaart te kijken). Voorlopig lijkt het OK om te vertrouwen dat dat niet gebeurt.

Een ander punt om je bij dit soort systemen zorgen te maken is wanneer er maar een paar mogelijke berichten zijn. Een afluisteraar zou al die berichten kunnen coderen met de publieke sleutel en heeft daarna een tabel waarin hij het bericht kan opzoeken. De methode van Amy omzeilt dit probleem doordat er vele manieren zijn om hetzelfde bericht te versleutelen, afhankelijk van de getallen die gekozen werden om op te tellen bij de code. In de praktijk zijn cryptografische systemen zo ontworpen dat er zoveel mogelijke berichten zijn dat je zelfs niet wil beginnen om ze allemaal uit te proberen, ook al heb je de hulp van supercomputer(s).

Het is onbekend of er een snelle methode bestaat om een getal in zijn priemfactoren te ontbinden. Niemand heeft er een kunnen bedenken en evenmin heeft iemand bewezen dat zoiets helemaal niet kan. Als zo'n snelle methode opduikt zullen veel communicatiesystemen ineens onveilig blijken. In deel IV bespraken we NP-volledige problemen die geza-

menlijk standhouden op opgelost worden: als een zo'n NP-volledig probleem oplosbaar is (dat wil zeggen, een snelle methode bestaat die altijd werkt om het op te lossen) dan zijn alle NP-volledige problemen opgelost. Juist omdat heel veel onderzoekers zonder succes geprobeerd hebben NP-volledige problemen op te lossen, zouden dergelijke problemen ook een goede basis zijn voor het ontwerpen van een cryptosysteem. Helaas, daar komen weer andere problemen bij kijken, en daarom zijn de huidige cryptosystemen gedwongen te vertrouwen op problemen die mogelijk veel makkelijker te kraken zijn (zoals priemfactorisatie). De antwoorden op dit soort vragen zijn miljoenen euro's waard en worden beschouwd als vitaal voor de nationale veiligheid. Cryptografie is mede daarom een levendige tak van informatica onderzoek.

Verder lezen

Harel's boek Algorithmics behandelt publieke sleutel cryptografie en legt uit hoe grote priemgetallen gebruikt worden om een veilig publieke sleutel systeem te maken. Het standaard wetenschappelijke boek over cryptografie is *Cryptography and data security* van Dorothy Denning terwijl *Applied cryptography* van Bruce Schneier een meer praktisch boek is. Dewdney's Turing Omnibus beschrijft een ander systeem voor publieke sleutel cryptografie.