WISKUNNEND WISKE

DE SCHRANDERE SCHATBEWAKERS

De schatkamer van het kasteel van Jef Blaaskop op het eiland Amoras wordt beschermd door 10 schatbewakers. Enkel Jef Blaaskop kent de code van de kluis. Hij is echter heel lui en wil dat de bewakers de kluis voor hem kunnen openen. Om de schat toch zo goed mogelijk te beveiligen, vraagt hij de hulp van professor Barabas. Hij moet een code ontwikkelen zodat eender welke 3 schatbewakers samen de kluis kunnen openen, maar geen enkele twee dat samen kunnen. Hoe lost professor Barabas dit op? Hoe kan je dit veralgemenen naar de situatie met *n* schatbewakers zodanig dat elke *m* de kluis kunnen openen, maar elke *m-1* dat niet kunnen?

OPDRACHT 3: HOE LOST PROFESSOR BARABAS DIT OP? EN BEWIJS DIT.

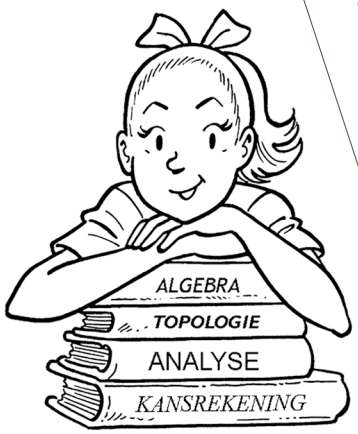
Waar wiskundigen vandaag hun hoofd over breken.

Tegenwoordig zijn het niet alleen schatten die beschermd moeten worden maar eveneens topsecret informatie. Cryptografie is de tak van de wiskunde die methoden onderzoekt om informatie te beschermen. Wiskundigen zoeken naar algoritmen om boodschappen te coderen, zodat deze veilig zijn voor transport (briefwisseling, e-mail) en nadien opnieuw gedecodeerd kunnen worden door de ontvanger. Zelfs Julius Caesar gaf een gecodeerde versie van informatie mee aan zijn boodschappers. Zo veranderde hij elke letter door de letter die zich 3 plaatsen verderop in het alfabet bevindt, d.w.z. A → D, B → E, ..., X → A, Y → B, Z → C. De persoon voor wie de informatie bestemd was, kon de gecodeerde boodschap opnieuw decoderen door de codeersleutel omgekeerd toe te passen.

In de cryptografie noemt men de boodschap die men wilt coderen **klare tekst** (plaintext) en de gecodeerde versie noemt men **cijfertekst** (ciphertext). De manier van coderen waarbij dezelfde sleutel gebruikt wordt zowel voor het coderen als het decoderen noemen we **Private Key** cryptografie, de ontvanger moet in bezit zijn van de sleutel om de cijfertekst te kunnen decoderen. Het probleem bij deze vorm van cryptografie is dat wanneer je van een bepaald woord het corresponderende codewoord kent, je de sleutel kan achterhalen en deze kan gebruiken om andere cijfertekst te ontcijferen. Daarom werd er in 1975 een nieuw soort cryptografie geïntroduceerd door Whitfield Diffie en Martin Hellman, namelijk **Public Key** cryptografie. Public Key cryptografie maakt gebruik van 2 sleutels, een publieke sleutel om de klare tekst te coderen en een private sleutel om de cijfertekst te decoderen. Dit wil zeggen dat iedereen die beschikt over de publieke sleutel de informatie kan coderen maar niet kan decoderen. Daarom noemt men deze vorm van cryptografie ook asymmetrisch, aangezien de sleutel voor decryptie niet louter de omgekeerde sleutel is voor encryptie.

De bekendste vorm van Public Key cryptografie is de **RSA**-code. Deze code werd in 1977 door 2 computerwetenschappers, Rivest en Shamir, en een wiskundige, Adleman, ontwikkeld. Vandaar ook de naam RSA. De procedure voor encryptie en decryptie zijn beiden gebaseerd op de ontbinding in priemfactoren. De RSA-code werkt vandaag de dag uitstekend omdat de ontbinding van grote getallen in priemfactoren nog altijd een heel moeilijk probleem is, zelfs voor computers. Om de goede werking van RSA te tonen, publiceerde Martin Gardner in 1977 een uitdaging voor de lezers in de wetenschapskrant *The Scientific American*. Hij gaf hen een getal van 129 cijfers en vroeg de lezer om dit getal in twee priemgetallen op te splitsen. Slechts in 1994, 17 jaren later, gaf een team van 600 vrijwilligers het correcte antwoord. In de hedendaagse RSA-codes worden nog veel grotere getallen gebruikt en dus is het bijna onmogelijk de code te kraken.

De enige vijand van RSA is de kwantumcomputer. Deze computers worden gebouwd op basis van kwantummechanica. Dit zijn uiterst snelle computers die grote getallen zonder problemen in heel korte tijd kunnen factoriseren. Wanneer deze computer eenmaal zal bestaan, wordt RSA nutteloos. Jammer genoeg (of gelukkig voor de RSA-code) bestaat deze computer op dit ogenblik enkel in theorie of in kleine testmodellen. Toch staan wetenschappers al klaar met alternatieven die RSA in de toekomst kunnen vervangen.



Vrije Universiteit Brussel