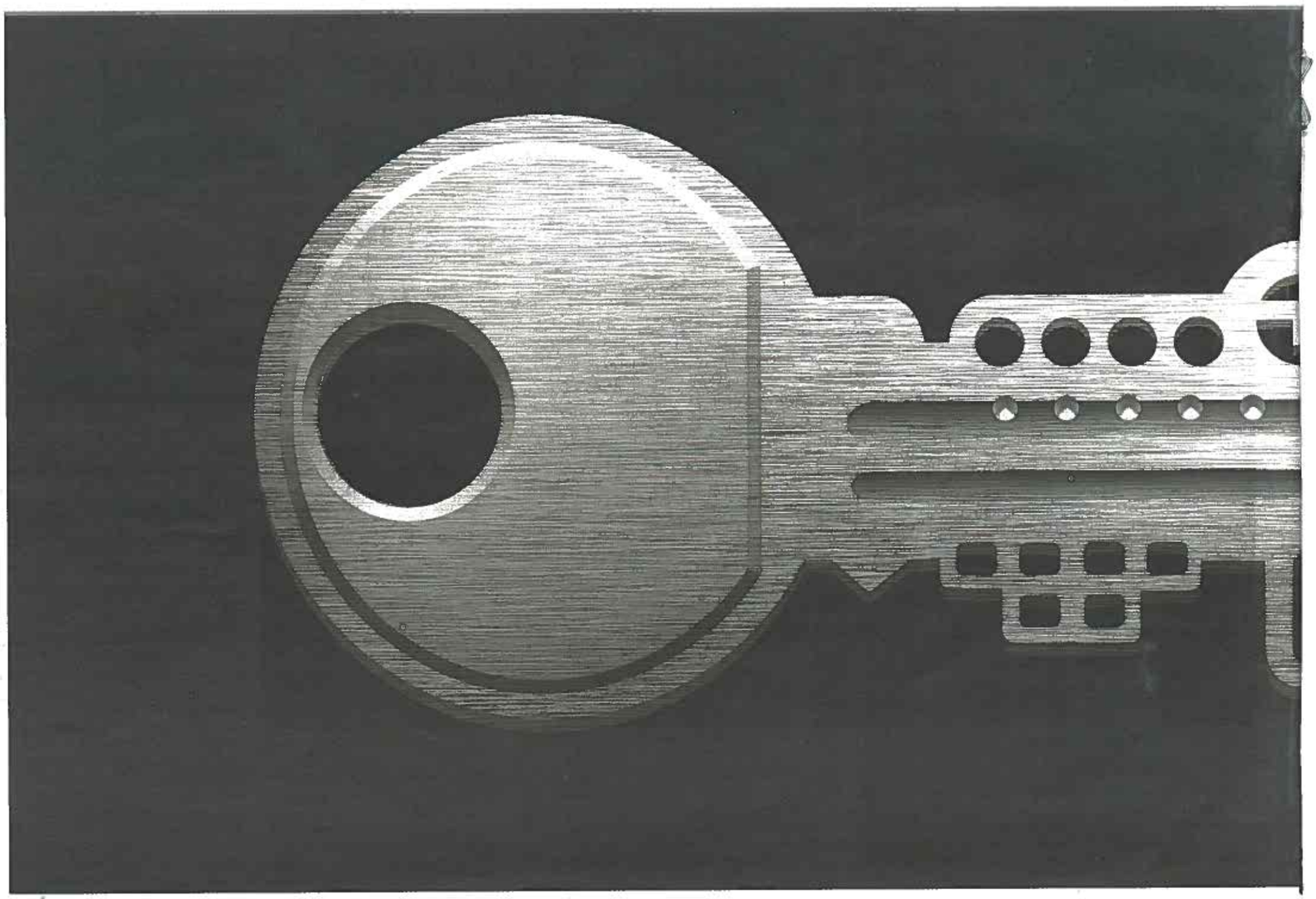
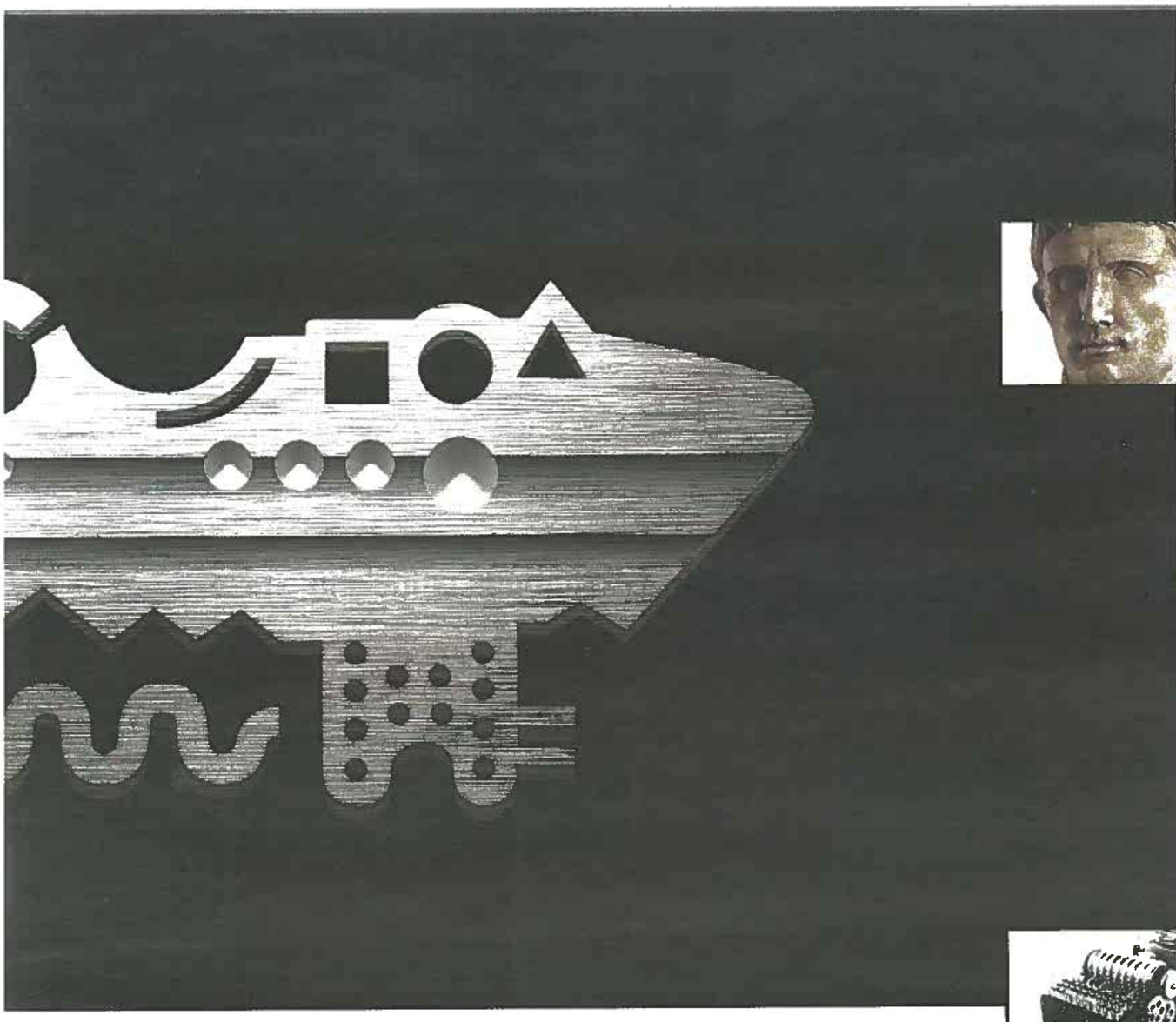


Geheime

Twintig eeuwen. Zo lang duurt het om een goed versleuteld wachtwoord van tien tekens te kraken. Justitie had dus geluk dat misbruikverdachte Robert M. zelf zijn wachtwoord vrijgaf. Onbekend is of hij toegang gaf tot álle foto's en films. Want geheime bestanden kunnen onzichtbaar worden gemaakt. En dat is niet eens zo moeilijk.

door **Monique Prins**
beeld **Mark Reijntjens**

Geheimschrift, ofwel cryptografie, roept direct beelden op van spionnen, detectives en oorlogen. Maar ook in het dagelijks leven is cryptografie alom aanwezig: bij mobiele telefoongesprekken, internetbankieren, elektronisch stemmen, belastingaangifte en patiëntendossiers. Cryptografie zorgt ervoor dat bestanden alleen toegankelijk worden voor degene die de juiste sleutel heeft om een bestand te openen. Het beveiligen van informatie is kinderlijk eenvoudig. Dat is een prettig idee voor iedereen die graag online winkelt en bankiert. Vervelend is dat ook criminelen hun gegevens zo makkelijk kunnen versleutelen.
Robert M. verborg zijn kinderpornobestanden via het programma Truecrypt, dat gratis is te downloaden. Hoe werkt zo'n encryptie-programma precies? Encryptie is een soort geheimschrift, waarbij een bestand (tekst, film, foto) flink door de war wordt gegooid zodat het helemaal onleesbaar wordt. Voor het terugrekenen is een wachtwoord of sleutel nodig. Dat is ook weer een getal dat bij het rekenproces wordt gebruikt.
Truecrypt heeft een goede naam, zegt cryptograaf Benne de Weger van de Technische Universiteit Eindhoven. Truecrypt maakt gebruik van het programma AES dat volop wordt gebruikt door de Amerikaanse overheid. „Het is nog nooit gelukt om dit programma te kraken", zegt De Weger. „En dat zegt wel wat, want er worden veelvuldig pogingen gedaan om de sleutel te vinden. Truecrypt gebruikt verschillende lagen van sleutels. Er is een sleutel om de juiste sleutel te vinden om toegang te krijgen tot versleutelde informatie. Zo bouw je verschillende beveiligde lagen in." Het is onduidelijk of het wachtwoord dat Robert M. gaf toegang verschafte tot álle informatie. Er kunnen (foto)bestanden op zijn computer staan die versleuteld blijven. Sterker nog: zijn computer kan bestanden hebben die niet eens herkenbaar zijn als bestanden. En het is lastig zoeken naar iets waarvan je niet weet of het bestaat.
De Weger: „Geheime bestanden zien eruit als willekeurige nullen en enen, als een soort ruis die niet herkenbaar is als een bestand." Als er veel geheugen in gebruik is, kan dit wijzen op geheime bestanden. Maar het geheugen kan ook écht worden opgeslokt door ruis.
De politie moet op zoek naar mogelijke sporen in het geheugen van de computervan Robert M., zegt universitair hoofddocent wiskunde Wieb Bosma. „Truecrypt doet net alsof het geheime mapje er niet is. Maar ergens op zijn computer staan mogelijk resten van het programma dat hij heeft gebruikt om bestanden te versleutelen. Dat kan een ingang bieden. Ik begrijp dat de politie zich voor het hoofd sloeg dat ze zijn computer had afgesloten om mee naar het bureau te kunnen nemen. Als ze dat niet hadden gedaan, konden ze misschien zijn wachtwoord en alle bestanden waar hij net naar had gekeken al eerder opsporen. Een pijnlijke constatering."
De zwakste schakel van cryptografische technieken is de mens.
„Kies een sterk wachtwoord. Liefst met hoofdletters, cijfers en leestekens. Iemand die jouw bestand wil kraken zal als eerste op zoek gaan naar namen van vriendinnetjes, honden en verjaardagen. Die moet je dus niet gebruiken. Deel je wachtwoord niet met te veel mensen, zoals bij WikiLeaks is gebeurd. Soms wel een miljoen mensen hadden toegang tot de vertrouwelijke informatie die naar WikiLeaks is gelekt. Er hoeft maar één rotte appel tussen te zitten en het gaat mis."
Er zijn veel misverstanden over een goed wachtwoord, zegt Bosma. „Veel mensen die online bankieren, denken dat ze hun wachtwoord op elk moment weer opnieuw bij de bank kunnen opvragen. Maar dat kan niet. Dat zou betekenen dat bij de bank jouw



sleutels

Kraken van versleutelde gegevens

- **Woordenboek-aanval**
  Een wachtwoord dat bestaat uit een normaal woord kan worden gekraakt door op een bestand alle woorden uit het woordenboek, eventueel in combinatie met cijfers, los te laten. Door het (voor een supercomputer) geringe aantal mogelijkheden kost dit relatief weinig tijd. Het kan binnen enkele uren tot dagen zijn gekraakt.
- **Brute kracht-aanval**
  Als een wachtwoord bestaat uit hoofdletters, kleine letters, symbolen, cijfers en leestekens is het raden van alle mogelijkheden nagenoeg onmogelijk. Met elk extra teken wordt het aantal mogelijkheden honderd keer zo groot. Een supercomputer kan een wachtwoord van acht tekens binnen twaalf weken kraken. Bij tien tekens zijn maar liefst twintig eeuwen nodig.
- **Verouderde cryptografie**
  Geheimschrift van tien tot twintig jaar geleden was geschreven voor computers met veel minder rekenvermogen dan huidige computers. Met een moderne supercomputer is een aanval eenvoudig te winnen.

wachtwoord wordt opgeslagen en dat verzwakt het systeem. De bank kan hooguit jouw oude wachtwoord weggooien en zeggen dat je een nieuw mag kiezen. Ten onrechte wordt er vanuit gegaan dat er een achterdeurtje zit in een versleuteld systeem. Maar het doel voor goede beveiliging is juist dat er geen achterdeur meer is."

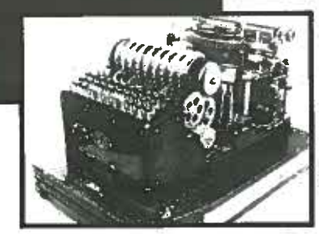
Extra hindernis voor politie en justitie is dat zij – in tegenstelling tot criminelen – rekening moeten houden met de wet. Hoogleraar regulering van technologie Bert-Jaap Koops deed onderzoek naar het spanningsveld tussen beveiliging, privacy en opsporing. Na zaken met omvangrijke misbruik als Robert M. en Benno L. klinkt ook in Nederland af en toe de roep om verdachten te dwingen hun wachtwoorden vrij te geven. Maar dat kan zomaar niet, zegt Koops. „Een verdachte hoeft volgens het Nederlandse recht niet mee te werken aan zijn eigen veroordeling. Ook familieleden kun je daar niet toe dwingen. In Engeland of Frankrijk mag justitie het wachtwoord wél opeisen. Op weigering staat twee tot drie jaar cel."

Er zitten haken en ogen aan deze dwang. „Een verdachte kan zeggen dat er helemaal geen geheime bestanden zijn. En hij kan zeggen dat hij het wachtwoord is vergeten. Dat is lastig straffen."

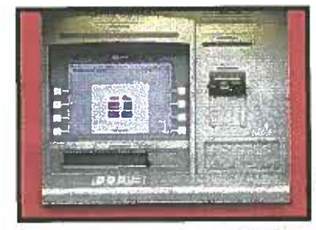
Zeker onder invloed van de PVV wordt vaker geopperd dat veiligheid zwaarder moet wegen dan privacy. Koops: „Privacy is een grondrecht. Als er veel bewijs is van een misdrijf, mag er tijdelijk inbreuk op worden gemaakt. Maar je kunt je recht op privacy nooit verspelen. Ook Robert M. niet."

Geheimschrift

- De geschiedenis van het geheimschrift of **cryptologie** gaat in ieder geval terug tot de oude Grieken.
- Een van de oudste bekende geheimschriften was in gebruik bij **Julius Caesar** (100 - 44 v. Chr.). De Romeinse politicus codeerde zijn berichten door letters drie posities op te schuiven in het alfabet. De 'a' werd een 'd', de 'b' een 'e', enzovoort.
- De sleutel van de Caesarcode was eenvoudig te ontcijferen, in tegenstelling tot het **Vigenèrecijfer** dat in 1553 werd uitgevonden. Hierbij worden letters vervangen aan de hand van een sleutelwoord en verschillende alfabetische reeksen. Het duurde drie eeuwen voordat wiskundigen de code kraakten.
- Met de opkomst van de massacommunicatie in de tweede helft van de 19e eeuw (elektrische telegraaf, radio) werd geheimschrift populair op grote schaal.
- De Eerste Wereldoorlog versnelde de ontwikkeling van **versleutelapparaten**. Deze rotormachines verhaspelden teksten niet volgens één vast patroon, waardoor het aantal mogelijkheden enorm toenam. De code kraken werd daardoor bijzonder moeilijk.
- De meest bekende machine is de in 1920 ontwikkelde **Enigma** (Grieks voor 'raadsel'), mede bedacht door de Nederlander Hugo Koch. Het apparaat raakte beroemd omdat de nazi's het gebruikten tijdens de Tweede Wereldoorlog. De Britten wisten de codes echter te breken, met behulp van voorlopers van de computer. Daardoor beschikten zij over strategische informatie, die beslissend is geweest voor het verdere verloop van de Tweede Wereldoorlog.



- Een eenvoudige vorm van cryptografie bestaat uit het spreken van een **vreemde taal**. Zo gebruikten de Verenigde Staten Navajo, een indianentaal, in de oorlog tegen Japan. Ze hadden daarvoor een team van Navajo's opgeleid die de radioboodschappen in hun eigen taal doorgaven.
- Na 1945 werden verbeterde rotormachines gebruikt. Met de komst van de **computer** werd het mogelijk de versleuteling zeer snel uit te voeren en met een groot aantal mogelijke sleutels. De rotormachines verloren daardoor hun functie.
- **Internet** heeft het belang van het versleutelen van informatie doen toenemen, om te voorkomen dat criminelen er met geld en gegevens van burgers vandoor gaan.



- Cryptologie wordt tegenwoordig veel voor **vreedzame doelen** gebruikt, zoals bij pinnen, telefoneren en internetbankieren.
- Criminelen gebruiken ook graag versleuteling. Zo codeerde de 'Unabomber', die tussen 1978 en 1995 zestien aanslagen pleegde in de VS, zijn aantekeningen.
- Vooralsnog is **kwantum-encryptie** gegarandeerd veilig: elke poging tot afluisteren is meteen zichtbaar voor zender en ontvanger, zodat die maatregelen kunnen nemen.