TU/e is digitale notaris te slim af

TU/e-wiskundigen maken twee dezelfde 'vingerafdrukken'.

door **Martijn Hover**

EINDHOVEN – De boekenkast van TU/e-wiskundige dr. Benne de Weger kweekt geen vertrouwen in de mens. Titels als 'Hacker's Guide' ('Gids voor Hackers'), 'The Art of Deception' ('De kunst der misleiding') en 'The Spam Kings' drukken je met de neus vooral op onze bedrieglijke kant.

De Weger is dan ook cryptograaf, geheimschriftdeskundige. Het zijn mensen als hij die er voor zorgen dat er bij het versturen en verhandelen van computerbestanden niet al te veel mis kan gaan.

Zijn onderzoeksgroep publiceerde onlangs in het prestigieuze tijdschrift The Economist een artikel waarin zij op het eerste oog aankondigt te hebben voorspeld wie de nieuwe president wordt van de VS. Dat staat in een computerdocument waaraan een zogenaamde 'hashfunctie' is toegevoegd. Een hash is een soort samenvatting van het bestand die een getal oplevert dat kenmerkend is voor dat bestand. „Noem het maar een soort vingerafdruk", aldus De Weger. Het document waarin de nieuwe president wordt voorspeld, zou dus uniek moeten zijn.

Drie jaar geleden toonde de Chinese wiskundige Wang echter aan dat het mogelijk is twee verschillende documenten met dezelfde 'vingerafdruk' te maken.

„Dat was maar een zeer beperkte doorbraak", aldus De Weger. Hij en zijn collega prof. Arjen Lenstra (thans werkzaam bij de Technische Universiteit in Lausanne) gaven student Marc Stevens – inmiddels vertrokken naar het Centrum voor Wiskunde en Informatica in Amsterdam – opdracht om uit te zoeken of de methode-Wang kon worden uitgebreid.

De student slaagde wonderwel in zijn opdracht. Stevens is erin geslaagd om een manier te vinden waarmee meerdere, verschillende documenten van dezelfde hash kunnen worden voorzien.

Zijn methode is losgelaten op twaalf documenten met twaalf verschillende namen van presidentskandidaten, die dus allemaal dezelfde digitale 'vingerafdruk' hebben. „De hash werkt als een soort digitale notaris", legt De Weger uit. „De hashfunctie doet veronderstellen dat het een uniek document is. Het is alsof je een envelop met daarin de voorspelling bij de notaris hebt achtergelaten die hem pas op de dag van de verkiezingen mag openen om te zien of je gelijk had." Stevens fopte de digitale notaris door niet één, maar twaalf voorspellingen van een identieke 'vingerafdruk' te voorzien. Het is dus gewoon een kwestie van het openen van de juiste 'envelop' op de verkiezingsdag.

Eenvoudig was dat niet, vooral omdat voor zo'n klus een enorme rekenkracht vereist is. In eerste instantie kostte het een netwerk van vierduizend aan elkaar gekoppelde pc's een halfjaar om één 'botsing' van twee hashfuncties voort te brengen. Toen deden de onderzoekers echter een opmerkelijke ontdekking: een spelletjescomputer als een Playstation beschikt wegens de hoge grafische eisen die de spelletjes stellen, over veel meer rekenkracht dan een normale pc. „Één Playstation heeft, omgebouwd tot rekenmachine, de kracht van dertig pc's", aldus De Weger. Door de hashfunctie nog iets slimmer te maken, kon de rekentijd verder worden teruggebracht. Toch heeft het speelgoed voor het berekenen van een identieke hash voor de twaalf bestanden met presidentkandidaten nog altijd drie weken onafgebroken staan rekenen.

Mede door het werk van De Weger en zijn collega's loopt momenteel in de VS een open competitie om een betere versleuteling te vinden.

Het onderzoek is terug te vinden op de site www.win.tue.nl/hashclasg/Nostradamus.