HOE BEWAAR JE SAMEN EEN GEHEIM

KOEN DE NAEGHEL

SAMENVATTING. Dit artikel gaat over hoe een groep mensen samen een waardevol document of een grote som geld in een kluis kunnen bewaren, en wel op zo'n manier dat de kluis pas open kan indien voldoende sleutelhouders samenwerken. We laten zien hoe een meetkundige eigenschap van veeltermfuncties leidt tot een elegante, praktische en veilige methode van gegevensversleuteling, naar een methode van Shamir uit 1979 [5]. In onze tekst sluiten de gevallen met een klein aantal sleutelhouders aan bij de leerstof van de tweede graad (rechte, parabool). De algemene behandeling hoort thuis in de derde graad (telproblemen, lineaire stelsels) met een knipoog naar uitbreidingsleerstof en wiskunde aan het hoger onderwijs (modulair rekenen).

Geheimen bewaren en veilig communiceren: het is van alle tijden. Sinds de komst van het internet en het elektronische betaalverkeer is de beveiliging van gegevens dan ook steeds belangrijker geworden. Het is bijna vanzelfsprekend dat men, voor het ontwikkelen van een moeilijk te kraken code, beroep doet op de wiskunde. Verrassend is echter hoe sommige deelgebieden van de wiskunde die op het eerste zicht niets te maken hebben met coderen van gegevens, toch aanleiding kunnen geven tot een goed codeermechanisme, zonder dat de daarvoor gebruikte wiskunde ons petje te boven gaat. Een bekend voorbeeld daarvan is getaltheorie, waar de studie van priemgetallen aanleiding gaf tot het versleutelsysteem RSA, genoemd naar Rivest, Shamir en Adleman die ze in 1978 hebben bedacht [1]. Hierbij is de achterliggende gedachte dat zelfs de meest geavanceerde computeralgoritmen bijzonder veel tijd nodig hebben om een natuurlijk getal dat voldoende groot is te ontbinden in priemfactoren, terwijl het omgekeerde probleem, namelijk het vermenigvuldigen van grote priemgetallen, relatief gezien heel weinig computertijd kost. De afgelopen jaren hebben heel wat leerlingen uit de derde graad een onderzoeksopdracht over RSA gemaakt, een indicatie dat de wiskunde die nodig is om RSA te begrijpen best haalbaar is.

Dit artikel gaat over een ander, minder bekend beveiligingsprobleem, namelijk hoe een groep mensen die elkaar onderling wantrouwen toch samen een geheim kunnen bewaren. In de eerste paragraaf buigen we ons over zo'n concrete probleemstelling, dat gaat over een ouderwetse kluis met meerdere sloten. Met onze oplossing laten we zien waarom deze methode, zelfs voor een bescheiden aantal groepsleden, in de praktijk onhaalbaar wordt. In de tweede paragraaf gooien we het over een ander boeg. Daar pikken we het idee op om een geheime code in stukjes op te delen, om ze daarna over de groep mensen te verdelen. De methode die wij zullen uitwerken, werd in 1979 bedacht door Shamir (de "S" in RSA), zie [5, 3]. Datzelfde jaar vond ook Blakley, onafhankelijk van Shamir, zo'n werkwijze [2]. In een derde en laatste paragraaf gaan we na hoe veilig deze manier van coderen is.

Datum: 25 februari 2016. De auteur is Luc Van den Broeck erkentelijk voor het kritisch nalezen van dit artikel.

1. Een kluis met meerdere sleutels

Een voor de hand liggende manier om samen een waardevol document te bewaren, is om het in een kluis te stoppen en aan elk lid van de groep een sleutel te geven. Maar wat als er wantrouwen heerst en men wil dat de kluis enkel kan geopend worden als een meerderheid van de groep aanwezig is? In zijn boek uit 1968 [4] stelt Chung Laung Liu voor om de kluis te voorzien van meerdere sloten. Eén van zijn oefeningen hebben we als volgt vertaald.

Probleem 1. *Elf ministers willen een staatsgeheim in een kluis bewaren, die enkel kan geopend worden wanneer er minstens zes van de elf ministers aanwezig zijn. Ze voorzien de kluisdeur van een aantal verschillende sloten, zodat ze enkel open kan als in elk slot de juiste sleutel steekt. Van elke sleutel maken ze meerdere kopieën, en elke minister draagt een aantal sleutels bij zich. Volgens het rekenhof is het aantal sloten op de kluis zo klein mogelijk.*

(a) *Hoeveel sloten heeft de kluis?*
(b) *Hoeveel sleutels draagt elke minister bij zich?*

Een essentieel onderdeel van probleemoplossend denken is de vaardigheid om voor een probleem een passende zoekstrategie te bedenken. Het loont dan ook de moeite om dit probleem aan leerlingen of studenten voor te leggen, met de vraag: wat kan je helpen om de oplossing te vinden? Meestal komt de klas er zelf op om eerst een kleiner geval te onderzoeken.

Noem n het totaal aantal ministers en k het aantal ministers dat minstens aanwezig moet zijn om de kluis te openen (waarbij $1 \leq k \leq n$). We zullen eerst het probleem oplossen voor $k = 2$ en $n = 3$. Dat geval is aanzienlijk eenvoudiger, en kan zelfs aan de eerste graad worden voorgelegd.

1.1. Het geval $k = 2$ en $n = 3$.

Noem de drie ministers A, B en C. We moeten ervoor zorgen dat (1) één minister de kluis niet kan openen en (2) elke groep van twee ministers de kluis wel kan openmaken. Minister A kan de kluis niet openen, zodat hij minstens één sleutel mist, bijvoorbeeld de sleutel van het eerste slot. Als ministers A en B samenwerken, dan kunnen ze de kluis wel openen, zodat we zeker weten dat minister B de sleutel van het eerste slot wel heeft. Om dezelfde reden kan ook minister C het eerste slot openen. Kortom, bij elke minister hoort minstens één slot waarvan hij de sleutel niet heeft, en elke andere minister heeft die missende sleutel(s) wel. Daaruit mogen we besluiten dat de kluis minstens drie sloten heeft. Onderstaande Tabel 1 toont aan dat een kluis met precies drie sloten kan voldoen. Elke minister heeft dan twee sleutels bij zich.

ministers	heeft niet sleutel	heeft wel sleutels
A	1	$2, 3$
B	2	$1, 3$
C	3	$1, 2$

Tabel 1 Een oplossing van Probleem 1 voor $(k, n) = (2, 3)$

1.2. **Het geval $k = 3$ en $n = 5$.** Dit opstapje is haalbaar voor leerlingen uit de tweede graad, omdat de redenering die daarvoor nodig is geen formules vereist die ze nog niet gezien hebben. De uitkomst is dat de kluis tien sloten heeft en dat elke minister zes sleutels bij zich draagt. Tabel 2 toont een mogelijke oplossing.

ministers	heeft niet sleutels	heeft wel sleutels
A	$1, 2, 3, 4$	$5, 6, 7, 8, 9, 10$
B	$1, 5, 6, 7$	$2, 3, 4, 8, 9, 10$
C	$2, 5, 8, 9$	$1, 3, 4, 6, 7, 10$
D	$3, 6, 8, 10$	$1, 2, 4, 5, 7, 9$
E	$4, 7, 9, 10$	$1, 2, 3, 5, 6, 8$

Tabel 2 Een oplossing van Probleem 1 voor $(k, n) = (3, 5)$

1.3. **Een algemene oplossing van Probleem 1.** De oplossing van het oorspronkelijke probleem waarbij $(k, n) = (6, 11)$ is eerder voorbehouden voor leerlingen uit de derde graad, omdat er een formule uit het leerstofonderdeel telproblemen voor nodig is. Onze redenering gaat als volgt.

We moeten ervoor zorgen dat (1) elke groep van vijf ministers de kluis niet kan openen en (2) elke groep van zes ministers dat wel kan.

Beschouw een willekeurige verzameling van vijf ministers. Wegens voorwaarde (1) is er minstens één slot dat door geen enkele van die vijf ministers kan geopend worden. Mocht een ander groepje van vijf ministers hetzelfde slot ook niet kunnen openen, dan zou er een groepje van zes ministers kunnen gevormd worden dat de kluis niet kan openen, zodat aan voorwaarde (2) niet voldaan zou zijn. Kortom, bij elk groepje van vijf hoort minstens één missende sleutel, en twee verschillende groepjes van vijf hebben geen missende sleutel(s) gemeen. Daaruit volgt dat het aantal sloten op de kluis minstens gelijk moet zijn aan het aantal verschillende groepjes van vijf ministers. Dat wordt het aantal combinaties van 5 uit 11 genoemd, en is gelijk aan

$$C_{11}^5 = \frac{11!}{5!(11-5)!} = \frac{11 \cdot 10 \cdot 9 \cdot 8 \cdot 7}{5 \cdot 4 \cdot 3 \cdot 2} = 11 \cdot 3 \cdot 2 \cdot 7 = 462.$$

Om het aantal sleutels per minister te bepalen, beschouwen we een welbepaalde minister A en een groep van vijf andere ministers. Wegens voorwaarde (1) heeft die groep minstens één missende sleutel. Wil aan voorwaarde (2) voldaan zijn, dan moet minister A samen met die vijf de kluis kunnen openen. Anders gezegd, minister A heeft minstens de missende sleutels van alle groepjes van vijf waartoe A niet behoort. Dat aantal is gelijk aan $C_{10}^5 = 252$.

We hebben dus aangetoond dat de kluis minstens 462 sloten telt. Om in te zien dat 462 sloten ook volstaan, sommen we eerst alle groepjes van vijf ministers op, zeg $V_1, V_2, \ldots, V_{462}$. Een minister krijgt de sleutel van slot i als en slechts als hij niet tot het groepje V_i behoort. Zo is voldaan aan voorwaarde (1). Om na te gaan of er ook voorwaarde (2) geldt, nemen we een willekeurig groepje van zes ministers. Behoort minister X tot dat groepje, dan weten we dat de vijf anderen samen maar één sleutel missen, die X in zijn bezit heeft, zodat die zes samen toegang hebben tot de kluis. De oplossing op vraag (a) is dus

462, en onze redenering hierboven leidt ertoe dat elke minister precies 252 sleutels bij zich draagt, wat dus het antwoord op vraag (b) is.

Leerlingen die Probleem 1 met elf ministers hebben opgelost, kunnen met enkele vervolgvragen nog wat verder worden uitgedaagd. De uitgewerkte oplossingen worden overgelaten aan de lezer.

Probleem 1 (vervolg).

(c) *Hoeveel ministers kunnen een welbepaald slot openmaken?*
(d) *Hoeveel sleutels hebben twee ministers gemeen?*

Onze oplossing van Probleem 1 laat zich veralgemenen voor willekeurige waarden van n en k (waarbij $1 \leq k \leq n$): er zijn C_n^{k-1} sloten nodig en elke minister moet C_{n-1}^{k-1} sleutels bij zich hebben. Een welbepaald slot kan dan door $n-k+1$ ministers worden opengemaakt en twee ministers hebben C_{n-2}^{k-1} sleutels gemeen. Om dat laatste resultaat te bereiken, kan de formule van Stifel-Pascal worden aangewend.

In het bovenstaande Probleem 1 met elf ministers zou het erg onpraktisch zijn om elke minister 252 sleutels te laten dragen. Ook al vervangen we de klassieke sloten door elektronische versies waar een code moet worden ingetikt, dan nog blijft de methode om een kluis met meerdere sloten te voorzien, eerder omslachtig. In de volgende paragraaf pakken we het dan ook op een andere manier aan.

2. Een geheime code in stukjes verdelen

In 1979 bedacht Adi Shamir een praktische manier om een groep van n mensen, die elkaar onderling wantrouwen, een geheim te laten bewaren [5]. Zijn idee was om met een geheime code $c \in \mathbb{N}$ een aantal getallen $c_1, c_2, \ldots, c_n \in \mathbb{N}$ te associëren zodat

(1) kennis van $k-1$ of minder getallen c_i het onmogelijk maken om de geheime code c te achterhalen, en
(2) kennis van k of meer getallen c_i het mogelijk maken om het getal c te bepalen.

Zo'n plan wordt in het Engels een *threshold scheme* genoemd, wat wij hier vrij zullen vertalen als een *drempelplan*: zodra iemand uit de groep de kennisdrempel van k getallen overschrijdt, kan die persoon de geheime code c vinden.

De grote vraag is natuurlijk *hoe* we met het geheim getal c zo'n getallen c_i kunnen associëren. Hieronder zullen we het elegante drempelplan van Shamir bespreken voor $(k, n) = (3, 8)$. Daarna geven we aan hoe dit kan veralgemeend worden voor andere waarden van n en $k \leq n$.

Probleem 2. *Een rijke weduwnaar bewaart zijn geld in een kluis met één elektronisch slot, dat kan geopend worden door een natuurlijk getal in te toetsen. De man heeft acht kinderen, en wil dat zijn kluis enkel open kan wanneer er minstens drie van de acht kinderen samenwerken. Hoe kan de man zijn geheime code doorgeven?*

Drempelplan van Shamir. Noem $C \in \mathbb{N}$ de geheime combinatie. Eerst kiest de weduwnaar een geheime veelterm van graad twee waarvan de coëfficiënten natuurlijke getallen zijn en waarbij de constante term gelijk is aan c:

$$V(x) = ax^2 + bx + c \quad \text{met } a, b \in \mathbb{N} \text{ en } a \neq 0.$$

Daarna berekent hij het getal $c_1 = V(1)$ dat hij aan zijn eerste kind geeft, het getal $c_2 = V(2)$ dat hij aan zijn tweede kind geeft, enzovoort. Ten slotte zegt hij aan zijn kinderen dat de geheime combinatie c hoort bij het snijpunt $(0, c)$ van de y-as met de parabool die door de punten met coördinaten $(1, c_1)$, $(2, c_2)$ etc. gaat. Dat er minstens drie kinderen nodig zijn om de veelterm $V(x)$ en dus de code c te bepalen, volgt uit de volgende meetkundige eigenschap: drie verschillende punten op een parabool leggen die parabool uniek vast, maar twee of minder punten doen dat niet. We illusteren dit met een concreet voorbeeld uit [7].

Stel bijvoorbeeld dat de kinderen de getallen c_i uit Tabel 3 kregen.

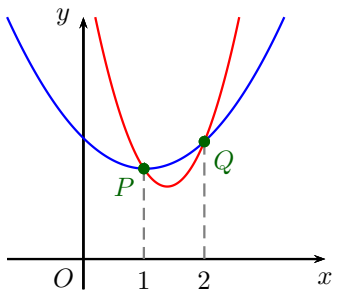
kind	heeft getal
A	$c_1 = 1494$
B	$c_2 = 1942$
C	$c_3 = 2578$
D	$c_4 = 3402$
E	$c_5 = 4414$
F	$c_6 = 5614$
G	$c_7 = 7002$
H	$c_8 = 8578$

Tabel 3 Een drempelplan voor $(k, n) = (3, 8)$

Spannen bijvoorbeeld enkel de kinderen A en B samen, dan kunnen ze proberen om de tweedegraadsveelterm $V(x) = ax^2 + bx + c$ te achterhalen door hun kennis $V(1) = 1494$ en $V(2) = 1942$ te vertalen in een lineair stelsel:

$$\begin{cases} a + b + c = 1494 \\ 4a + 2b + c = 1942 \end{cases} \quad \Rightarrow \quad \begin{cases} a = r - 523 \\ b = 2017 - 3r \\ c = 2r \end{cases} \quad (r \in \mathbb{R}).$$

Zo vinden ze meerdere mogelijkheden voor de veelterm $V(x)$. Zonder een andere broer of zus zullen de kinderen A en B de geheime code c niet kunnen achterhalen. De achterliggende, meetkundige reden is dat er meerdere parabolen zijn die door de punten $P(1, 1494)$ en $Q(2, 1942)$ gaan, zie Figuur 1.



Figuur 1 Door de punten P en Q gaat meer dan een parabool.

Werken bijvoorbeeld de kinderen C, E en H samen, dan verkrijgen ze het stelsel

$$(*) \qquad \begin{cases} 9a + 3b + c = 2578 \\ 25a + 5b + c = 4414 \\ 64a + 8b + c = 8578. \end{cases}$$

Met wat rekenwerk vinden ze een unieke oplossing voor dit stelsel, en bepalen zo de tweedegraadsveelterm $V(x) = 94\,x^2 + 166x + 1234$. De geheime combinatie is dus $c = 1234$. Een ander drietal kinderen zal dezelfde oplossing vinden.

Leerlingen die vertrouwd zijn met determinanten, kunnen het lineair stelsel $(*)$ ook oplossen door de regel van Cramer toe te passen. De coëfficiëntenmatrix $A = \left(\begin{smallmatrix} 9 & 3 & 1 \\ 25 & 5 & 1 \\ 64 & 8 & 1 \end{smallmatrix}\right)$ is, op de volgorde van de kolommen na, een Vandermonde-matrix. Nu is de determinant van een Vandermonde-matrix van orde $m \geq 2$ te schrijven als

$$\begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{m-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{m-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_m & x_m^2 & \dots & x_n^{m-1} \end{vmatrix} = \prod_{1 \leq i < j \leq m} (x_j - x_i),$$

een formule die met behulp van inductie kan worden bewezen. Hieruit volgt dat de determinant van de coëfficiëntenmatrix van het lineair stelsel $(*)$ gelijk is aan

$$\det A = \begin{vmatrix} 3^2 & 3 & 1 \\ 5^2 & 5 & 1 \\ 8^2 & 8 & 1 \end{vmatrix} = - \begin{vmatrix} 1 & 3 & 3^2 \\ 1 & 5 & 5^2 \\ 1 & 8 & 8^2 \end{vmatrix} = -(5-3)(8-3)(8-5) = -30,$$

en die is verschillend van nul precies omdat de punten met coördinaten $(3, c_3)$, $(5, c_5)$ en $(8, c_8)$ alle verschillende x-waarden hebben. De regel van Cramer impliceert dan dat het lineair stelsel $(*)$ een unieke oplossing heeft, met als geheime code

$$c = \frac{\begin{vmatrix} 9 & 3 & 2578 \\ 25 & 5 & 4414 \\ 64 & 8 & 8578 \end{vmatrix}}{\begin{vmatrix} 9 & 3 & 1 \\ 25 & 5 & 1 \\ 64 & 8 & 1 \end{vmatrix}} = \frac{-37020}{-30} = 1234.$$

Dat alle 3×3-stelsels dezelfde oplossing hebben, volgt uit het feit dat de maker van de code voor elke kind dezelfde tweedegraadsfunctie heeft gebruikt.

Deze redenering laat zien hoe de theorie van lineaire stelsels en determinanten verklaart dat een parabool volledig bepaald is van zodra we drie verschillende verschillende punten kennen die op de parabool liggen. Bovendien veralgemeend deze werkwijze zich tot een bewijs van de volgende meetkundige eigenschap.

Elke veeltermfunctie f van graad $k-1$ is volledig bepaald door k verschillende punten die op de grafiek van f liggen, maar is niet bepaald door $k-1$ of minder punten die op de grafiek van f liggen.

Een expliciet voorschrift van die veeltermfunctie f wordt een *interpolatieformule* genoemd, meest bekend zijn die van Lagrange en die van Newton. Voor een bewijs van deze eigenschap met bijbehorende interpolatieformules verwijzen we naar [6, §5.2 en §5.3]. De eigenschap garandeert ons dat het drempelplan van Shamir ook werkt voor andere waarden van n en k (waarbij $1 \leq k \leq n$).

3. Modulair rekenen zorgt voor meer veiligheid

Om na te gaan hoe veilig het drempelplan van Shamir is, hernemen we Probleem 2 en het drempelplan uit Tabel 3 hierboven. Zelfs als kind A zelfzuchtig blijft en met niemand wil samenwerken, kan het toch wat informatie over de geheime code c ontrafelen. De kennis dat $V(1) = 1494$ leidt immers tot het verband $c = 1494 - a - b$, en omdat de onbekenden a, b, c natuurlijke getallen zijn met $a \neq 0$, volgt hieruit dat $c \in \{0, 1, 2, \ldots, 1493\}$. Zo worden de op het eerste zicht oneindig veel mogelijkheden voor c teruggebracht tot 1494 mogelijkheden. In zekere zin is kind A zelfs bevoordeeld ten opzichte van de anderen: zo kan kind H enkel besluiten dat $c \in \{0, 1, 2, \ldots, 8514\}$.

Beslist kind A om samen te werken met B, dan kunnen ze het aantal mogelijkheden voor de geheime code c nog verder reduceren. Hun stelsel is dan equivalent met

$$\begin{cases} a + b + c = 1494 \\ 4a + 2b + c = 1942 \end{cases} \quad \Leftrightarrow \quad \begin{cases} a = r - 523 \\ b = 2017 - 3r \\ c = 2r \end{cases} \quad \text{waarbij } r \in \{523, 524, \ldots, 672\}.$$

Kinderen A en B weten dus dat $c \in \{1046, 1048, 1050, \ldots, 1344\}$ waarmee nog 150 mogelijkheden voor c overblijven.

Dat veiligheidsprobleem wordt verholpen door het zogenaamd *modulair rekenen*. Daarvoor kiest de weduwnaar een priemgetal p, waarvan de grootte de veiligheid van Shamir's drempelplan zal weerspiegelen. Bij wijze van voorbeeld kiezen we $p = 9973$, het grootste priemgetal dat vier cijfers heeft. Rekenen modulo p komt erop neer dat bij het optellen en vermenigvuldigen van gehele getallen het eindresultaat x vervangen wordt door de rest r bij deling van x door p. In dat proces schrijven we dan $x = r \bmod p$. Zo is bijvoorbeeld (voor $p = 9973$)

$$9972 + 1 = 9973 = 0 \bmod p, \quad -5000 = 4973 \bmod p \quad \text{en} \quad 100^2 = 10\,000 = 27 \bmod p.$$

De verzameling van alle mogelijke resten bij deling door p wordt genoteerd als $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$. In deze verzameling zijn de optelling en vermenigvuldiging modulo p inwendig. Het feit dat p een priemgetal is, zorgt ervoor dat elk element in $\mathbb{Z}_p$ een inverse voor de vermenigvuldiging modulo p heeft. Zo is bijvoorbeeld (voor $p = 9973$)

$$2^{-1} = 4987 \bmod p \quad \text{want} \quad 2 \cdot 4987 = 9974 = 1 \bmod p, \text{ en}$$
$$2016^{-1} = 5872 \bmod p \quad \text{want} \quad 2016 \cdot 5872 = 11\,837\,952 = 1 \bmod p.$$

Daarom zegt men dat de verzameling $\mathbb{Z}_p$, voorzien van de optelling en vermenigvuldiging modulo p, een veld is. Oplossen van lineaire stelsels over $\mathbb{Z}_p$ kan op dezelfde manier kan gebeuren als over $\mathbb{R}$, wat we in de derde graad gewoon zijn. Er kan dus gebruik gemaakt worden van rijherleiden, inverse matrices, determinanten en de regel van Cramer [6, §4.7]. Ook hier kunnen de berekeningen met behulp van een computeralgebrapakket worden uitgevoerd.

Dankzij het modulair rekenen kunnen zelfzuchtige kinderen hun kansen niet langer beduidend verhogen door informatie bij elkaar te sprokkelen. Werkt bijvoorbeeld kind A alleen, dan kan het uit $c = 1494 - a - b$ niet afleiden dat $c < 1494$. Zo geldt voor $a = 7436$, $b = 2016$ en $c = 2015$ ook dat $1494 - a - b = c \bmod p$. Op die manier heeft kind A nog steeds $p = 9973$ mogelijkheden voor c. Samenwerken met kind B zal enkel opleveren dat $c \neq 1046 \bmod p$, zodat er nog steeds 9972 mogelijkheden overblijven.

We sluiten deze tekst af met een oefening op het drempelplan van Shamir en modulair rekenen. Om je het plezier van het zoeken te gunnen, zullen we het eindantwoord niet expliciet vermelden. We geven wel mee dat het kwadraat van de geheime code een getal is waarin elk cijfer tweemaal voorkomt, zodat je jouw oplossing toch kan controleren.

Oefening. *De koning bewaart een staatsgeheim in een kluis, die enkel kan geopend worden wanneer er minstens zes van zijn elf ministers aanwezig zijn. Hij voorziet de kluis van één viercijferige code en geeft elke minister een natuurlijk getal c_i. Er is bekend dat de geheime code gelijk is aan de constante term van de vijfdegraadsveelterm met coëfficiënten in $\mathbb{Z}_{9973}$ waarvoor de waarde in $i \in \{1, 2, \ldots, 11\}$ gelijk is aan $c_i \bmod 9973$. Door een slordigheid komen de getallen hieronder in het staatsblad terecht. Kun jij de geheime code vinden?*

$$c_2 = 6158, \quad c_5 = 6378, \quad c_6 = 1999, \quad c_9 = 3095, \quad c_{10} = 9173 \quad \text{en} \quad c_{11} = 8237.$$

Referenties

[1] L. Adleman, R. Rivest, A. Shamir, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM, vol. 21, no. 2, p. 120-126, 1978.

[2] G.R. Blackley, *Safeguarding cryptographic keys*, Proc. AFIPS 1979 NCC, Vol. 48, p. 313-317, 1979.

[3] E. Brown, *Saints and scoundrels and two theorems that are really the same*, The college mathematics journal, Vol. 46, no. 5, p. 326-334, 2015.

[4] C.L. Liu, *Introduction to combinatorical mathematics*, McGraw-Hill, New-York, 1968.

[5] A. Shamir, *How to share a secret*, Communications of the ACM, vol. 22, no. 11, p. 612-613, 1979.

[6] B.L. Van der Waerden, *Algebra Volume 1*, Springer-Verlag, New Tork, 1991.

[7] Website https://en.wikipedia.org/wiki/Secret_sharing, geraadpleegd 25 februari 2016.

Koen De Naeghel, Onze-Lieve-Vrouwecollege, Collegestraat 24, 8310 Brugge.
E-mail address: koendenaeghel@hotmail.com