Wiskunnend Wiske 2012

Opdracht 3, Wico Campus Sint-Hubertus, Neerpelt, 6Wis

Oplossing

Voor het algemene geval met n schatbewakers zodanig dat elke m schatbewakers de kluis kunnen openen, maar elke $m-1$ dat niet kunnen, stellen we deze oplossingsmethode voor.

Zij C de code waarmee de kluis geopend kan worden. Maak nu een veelterm van de $(m-1)$'ste graad, met als constante term C. Bepaal nu n verschillende koppels getallen, die punten van de grafiek van de veelterm voorstellen. Geef nu elke persoon 1 van deze koppels (geen 2 personen krijgen hetzelfde koppel). Bovendien wordt aan iedereen de informatie gegeven dat ze over een punt van een veelterm van graad $m-1$ beschikken, waarvan de constante term de code vertegenwoordigt. Natuurlijk geven we niemand het koppel $(0, C)$

Daar elke veelterm van de k'de graad uniek bepaald wordt door k+1 punten, maar volledig onbepaald is met minder punten, zijn er op zijn minst m punten nodig om de vergelijking van de geconstrueerde veelterm van graad $m-1$ te achterhalen. Elke m personen beschikken samen over net genoeg gegevens om deze vergelijking te berekenen.

Eens dit gebeurd is, weten de m schatbewakers dus wat de constante term is, en bijgevolg ook wat de code is.

Hieronder volgt een uitgewerkt voorbeeld voor n=10 en m=3 (de situatie waarvan sprake was in de opgave). We nemen als code 314.

We kiezen als veelterm: $f(x) = 188x^2 - 487x + 314$

Deze bevat het triviale punt $P_0(0{,}314)$, die we aan niemand geven, maar de volgende punten geven we wel:
$P_1(1{,}15)$; $P_2(2{,}92)$; $P_3(3{,}545)$; $P_4(4{,}1374)$; $P_5(5{,}2579)$; $P_6(6{,}4160)$; $P_7(7{,}6117)$; $P_8(8{,}8450)$; $P_9(9{,}11159)$ en $P_{10}(10{,}14244)$

Als nu bv. persoon 3, 4 en 9 samenwerken, dan zijn de punten $P_3(3{,}545)$, $P_4(4{,}1374)$ en $P_9(9{,}11159)$ bekend.

Een algemene veelterm van de 2de graad wordt gegeven door $f(x) = ax^2 + bx + c$

Vullen we hier achtereenvolgens de punten P_3, P_4 *en* P_9 in, dan krijgen we het volgende 3x3-stelsel van Cramer:

$$\begin{aligned} 9a + 3b + c &= 545 \\ 16a + 4b + c &= 1374 \\ 81a + 9b + c &= 11159 \end{aligned}$$

We kunnen dit stelsel eenvoudig oplossen met behulp van de substitutiemethode of de combinatiemethode , of we kunnen hem in matrixvorm door ons grafisch rekentoestel laten rij-reduceren:

$$\begin{vmatrix} 9 & 3 & 1 & 545 \\ 16 & 4 & 1 & 1374 \\ 81 & 9 & 1 & 11159 \end{vmatrix} \overset{RREF}{\Longrightarrow} \begin{vmatrix} 1 & 0 & 0 & 188 \\ 0 & 1 & 0 & -487 \\ 0 & 0 & 1 & 314 \end{vmatrix}$$

Dan kunnen we meteen aflezen: $a = 188, b = -487\ en\ c = 314$ en dus $f(x) = 188x^2 - 487x + 314$

Bijgevolg weten de 3 schatbewakers dat de code 314 is.

Deze methode levert dus een heel snelle, eenvoudige en veilige manier op om het bericht te ontcijferen.

We merken nog even terzijde op dat de functie ook snel kan bepaald worden met behulp van Lagrange-interpolatie, maar dit zou ons te ver leiden. ■