Activiteit 16

Geheimen delen—Protocollen die informatie verbergen

Samenvatting

Cryptografische technieken stellen ons in staat om informatie te delen met andere mensen, met behoud van privacy op een verrassend hoog niveau. Deze activiteit illustreert een situatie waarin informatie wordt gedeeld en toch niets daarvan wordt onthuld: een groep leerlingen berekent hun gemiddelde leeftijd zonder dat ze aan iemand hoeven te vertellen wat hun leeftijd is.

Vaardigheden

- Een gemiddelde berekenen.
- Willekeurige getallen.
- Samenwerken.

Leeftijd

7 jaar en ouder

Materialen

Voor elke groep leerlingen:

- een notitieblok
- een pen.

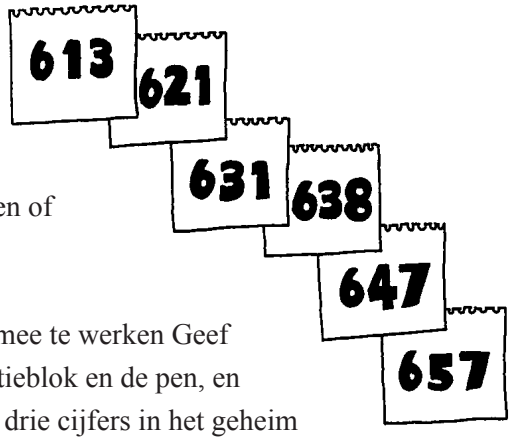
Geheimen delen

Introductie

Bij deze activiteit vinden we de gemiddelde leeftijd van een groep leerlingen zonder dat iemand zijn leeftijd onthult. Als alternatief zou je het gemiddelde inkomen (zakgeld) van de leerlingen in de groep, of een dergelijk persoonlijk detail kunnen uitzoeken. De berekening van deze statistieken werkt bijzonder goed met volwassenen, omdat oudere mensen gevoeliger voor details zoals leeftijd en inkomen kunnen zijn. Je hebt minstens drie leerlingen in de groep nodig.

Discussie

Leg uit aan de groep dat je wil uitvinden wat hun gemiddelde leeftijd is zonder dat iemand tegen iemand anders zegt hoe oud hij is.
Vraag suggesties hoe je dat zou kunnen doen en of het wel mogelijk is.



Maak groepjes van zes tot tien leerlingen om mee te werken Geef aan de eerste leerling van elk groepje een notitieblok en de pen, en vraag of ze een willekeurig gekozen getal van drie cijfers in het geheim opschrijven op het bovenste vel papier. In dit voorbeeld is 613 gekozen als het willekeurige getal.

Laat elke eerste leerling het eerste blaadje afscheuren, zijn/haar leeftijd optellen bij het willekeurige getal en de uitkomst opschrijven op het tweede blaadje van het notitieblok. In dit voorbeeld is de eerste leerling 8 jaar, dus op het tweede blaadje staat 621. Ze moeten het afgescheurde blaadje bij zich houden (en aan niemand laten zien.)

Het notitieblok wordt dan doorgegeven aan de tweede leerling die zijn leeftijd erbij optelt, het blaadje afscheurt en het totaal opschrijft op het volgende blaadje. In het voorbeeld is de tweede leerling 10 jaar. Ga zo door met dit proces van het bovenste blaadje afscheuren en de leeftijd optellen bij het getal totdat alle leerlingen aan de beurt zijn geweest.

Dan krijgt de eerste leerling het notitieblok. Laat die leerling het originele willekeurige getal aftrekken van het getal op het notitieblok. In dit voorbeeld deden vijf leerlingen mee en als je van het laatste getal, 657, het originele getal, 613, aftrekt, is de uitkomst 44. Dat getal is de som van de leeftijden van de leerlingen en het gemiddelde kan worden berekend door het te delen door het aantal leerlingen; dus de gemiddelde leeftijd van de groep uit ons voorbeeld is 8.8.

Wijs de leerlingen er op dat zolang iedereen zijn stukje papier vernietigt, niemand de leeftijd van een persoon kan weten, tenzij twee mensen besluiten om samen te werken.

Variaties en uitbreidingen

Dit systeem kan worden aangepast om een geheime stemming mogelijk te maken door elke persoon een op te laten tellen als ze ja stemmen, en nul als ze nee stemmen. Natuurlijk, als iemand meer dan één optelt (of minder dan nul), dan zou de stemming oneerlijk zijn, maar ze zouden het risico lopen argwaan te wekken als iedereen ja gestemd had, omdat het aantal ja stemmen meer dan het aantal mensen zou zijn.

Waar gaat dit over?

Computers slaan veel persoonlijke informatie over ons op: ons banksaldo, onze sociale netwerken, hoeveel belasting we betalen, hoe lang we een rijbewijs hebben, onze betalingsgeschiedenis, examenresultaten, medische dossiers, en ga zo maar door. Privacy is erg belangrijk! Maar we moeten in staat zijn om een deel van deze informatie te delen met andere mensen.
Bijvoorbeeld, bij het betalen voor goederen in een winkel met een creditcard, moet de winkel kunnen controleren of we daarmee kunnen betalen.
Vaak eindigen we met het verstrekken van meer informatie dan echt nodig is. Bijvoorbeeld, als we elektronisch betalen in een winkel, ziet de winkel onze bank, ons rekeningnummer en onze naam. Verder ziet de bank waar we onze boodschappen hebben gedaan. Banken kunnen een profiel van iemand creëren door het monitoren van dingen zoals waar mensen benzine kopen of boodschappen, hoeveel ze uitgeven elke dag aan deze items, en wanneer deze plaatsen worden bezocht. Als we contant hadden betaald dan was niets van deze informatie onthuld. De meeste mensen maken zich niet zo veel zorgen, dat deze informatie wordt gedeeld, maar er is de mogelijkheid van misbruik, zowel voor gerichte marketing (bijvoorbeeld het verzenden van reisadvertenties aan

mensen die veel geld besteden aan vliegtickets), discriminatie (zoals het aanbieden van een betere service aan iemand wiens bank meestal alleen vermogende klanten heeft), of zelfs chantage (zoals dreigen met de onthulling van details van een beschamende transactie). En verder kunnen mensen de manier waarop ze winkelen veranderen als ze denken dat iemand hen kan monitoren.

Dit verlies van privacy wordt vrij algemeen aanvaard, maar er bestaan cryptografische protocollen, waarmee we elektronische financiële transacties kunnen doen met het zelfde niveau van privacy als transacties met contant geld. Het is misschien moeilijk te geloven dat geld kan worden overgemaakt van je bankrekening naar de rekening van de winkel zonder dat iemand weet waar het geld vandaan kwam of naar toe gaat. Deze activiteit maakt een dergelijke transactie een beetje meer plausibel: in beide situaties is sprake van een beperkt delen van informatie, en dit kan mogelijk worden gemaakt door een slim protocol.

Verder lezen

Een goed artikel dat deze punten benadrukt is geschreven door David Chaum, met de provocerende titel “Security without identification: transaction systems to make Big Brother obsolete.” Het artikel is goed leesbaar, en geeft eenvoudige voorbeelden van protocollen om informatie te verbergen, met inbegrip van hoe transacties volledig privé kunnen worden gemaakt bij het gebruik van ‘elektronisch geld”. Het artikel kun je vinden in Communications of the ACM, Oktober 1985, bijvoorbeeld hier www.cs.ru.nl/~jhh/pub/secsem/chaum1985bigbrother.pdf

Het Nederlandse boekje Verborgen boodschappen, een inleiding in de cryptografie http://www.epsilon-uitgaven.nl/Z35.php is aanmerkelijk toegankelijker.