**Antwoorden les 10: Difie, Hellman en Merkle**

**Opgave 1**

Een eenvoudige boodschap zou kunnen zijn :"hallo buurvrouw"

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| h | a | l | l | o | b | u | u | r | v | r | o | u | w |

Om de boodschap te vercijferen moet Alice de getallen eerst omzetten in getallen met gebruik van de ASCII-tabel. Dankzij haar computer kan zij gebruik maken van een eenvoudig werkblad om zich niet al teveel rekenwerk op de hals te halen:

In Excel vindt ze de functie CODE(tekst), die de letters omzet in getallen volgens de ASCII-tabel.
In de volgende regel vermenigvuldigt ze de regel met 35 en stuurt de code naar Bob:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 104 | 97 | 108 | 108 | 111 | 98 | 117 | 117 | 114 | 118 | 114 | 111 | 117 | 119 |
| 3640 | 3395 | 3780 | 3780 | 3885 | 3430 | 4095 | 4095 | 3990 | 4130 | 3990 | 3885 | 4095 | 4165 |

Bob vermenigvuldigt de hele rij met 42 en stuurt het resultaat terug:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 152880 | 142590 | 158760 | 158760 | 163170 | 144060 | 171990 | 171990 | 167580 | 173460 | 167580 | 163170 | 171990 | 174930 |

Alice deelt de hele rij nu door 35 en stuurt het weer terug naar Bob.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4368 | 4074 | 4536 | 4536 | 4662 | 4116 | 4914 | 4914 | 4788 | 4956 | 4788 | 4662 | 4914 | 4998 |

Bob deelt de hele rij door 42 en vindt de boodschap in ASCII-code:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 104 | 97 | 108 | 108 | 111 | 98 | 117 | 117 | 114 | 118 | 114 | 111 | 117 | 119 |

Met de functie TEKEN(getal) vindt Bob de klare tekst.
Samengevat ziet het er als volgt uit:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| h | a | l | l | o | b | u | u | r | v | r | o | u | w |
| 104 | 97 | 108 | 108 | 111 | 98 | 117 | 117 | 114 | 118 | 114 | 111 | 117 | 119 |
| 3640 | 3395 | 3780 | 3780 | 3885 | 3430 | 4095 | 4095 | 3990 | 4130 | 3990 | 3885 | 4095 | 4165 |
| 152880 | 142590 | 158760 | 158760 | 163170 | 144060 | 171990 | 171990 | 167580 | 173460 | 167580 | 163170 | 171990 | 174930 |
| 4368 | 4074 | 4536 | 4536 | 4662 | 4116 | 4914 | 4914 | 4788 | 4956 | 4788 | 4662 | 4914 | 4998 |
| 104 | 97 | 108 | 108 | 111 | 98 | 117 | 117 | 114 | 118 | 114 | 111 | 117 | 119 |
| h | a | l | l | o | b | u | u | r | v | r | o | u | w |

**Opdracht 2**Als Eve alle berichten weet te onderscheppen is het niet zo ingewikkeld. Door het antwoord van Bob te delen door de boodschap van Alice vindt zij eenvoudig dat Bob de getallen met 42 vermenigvuldigd heeft. Als ze de reactie van Alice deelt door 42 ontsleutelt ze net zo makkelijk als Bob de boodschap. Ook is het dan niet meer zo moeilijk om de sleutel van Alice te berekenen. Dit is namelijk de boodschap van Alice gedeeld door de boodschap in ASCII. Zo is bijvoorbeeld **152880/3640=42** en zo is **3640/104=35**.
Als Eve alleen de oorspronkelijke boodschap van Alice ziet dan kan ze daar de frequentieanalyse op loslaten of op zoek gaan naar de grootste gemene deler van al deze getallen. Ze zal dan in de meeste gevallen snel het getal 35 of een veelvoud daarvan vinden.

|  |  |  |
| --- | --- | --- |
| Grootste getal | Kleinste getal  | Verschil  |
| 3640 | 3395  | 245  |
| 3395 | 245x13 | 210 |
| 245 | 210 | 35 |
| 210 | 35x6 | 0 |

Het vinden van de grootste gemene deler gaat volgens het [algoritme van Euclides](http://nl.wikipedia.org/wiki/Algoritme). Dit heeft als uitgangspunt dat een deler van twee getallen ook een deler is van het verschil tussen die getallen. Door verder te rekenen met de kleinste getallen vind je snel de grootste gemene deler. Zie het voorbeeld hiernaast. De GGD van 3640 en 3395 blijkt 35 te zijn. We hebben de tabel iets ingekort door ineens 13x het getal 245 van 3395 af te trekken. Voor de uitvoering van het algoritme bestaan verscheidene comuterprogramma-tjes die je snel het antwoord geven. In pseudo-code ziet dit algoritme er als volgt uit:

**function** ggd(a,b)

 **if** a = b **return** a

 **else if** a < b **return** ggd(a, b-a)

 **else return** ggd(a-b, b)

**end**

**Opgave 3**Toelichting: Excel kent de zogenaamde REST-functie , wat een andere naam is voor de modulo-functie.
235/23 = 10 rest 5. Dat wil zeggen dat de klok modulo 23 tienmaal is rondgegaan en nu opnieuw 5 aanwijst.
Om het aantal rondjes te berekenen maken we gebruik van de functie GEHEEL(getal). Op de plaats van het getal voeren we de deling 235/23 uit.

|  |  |  |
| --- | --- | --- |
| REST(235;23) | REST(402;51) | REST(75;18) |
| 5 | 45 | 3 |
| 10 | 7  | 4  |

**Opgave 4**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| grondtal | deler  | Alice kiest  | Alice verstuurt naar Bob  | Bob kiest  | Bob verstuurt naar Alice  | Het geheime getal  |
| 43 | 79  | 7  | 59  | 11  | 60  | 68  |
| 17 | 127 | 10 | 9 | 6 | 76 | 73 |
| 85 | 211 | 12 | 193 | 13 | 158 | 125 |
| 64 | 149 | 18 | 80 | 22 | 31 | 107 |

De berekeningen van het werkblad zijn hieronder afgedrukt:
