Oplossing extra oefening 2

Oplossing a

Bepalen van het priemgetal net kleiner dan je geboortedatum.
We vertrekken van de geboortedatum 3/04/1994.

```
>&prev_prime(3041994)

                                3041989
```

```
>tekst:=randomTekst(30)
  rbwdfmapcqfzvioxzmeksgvljujfae
```

Coderen

- Tekst omzetten naar cijfers

```
>cijferTekst:=naarCijfer(tekst)
  [17,  1,  22,  3,  5,  12,  0,  15,  2,  16,  5,  25,  21,  8,  14,
  23,  25,  12,  4,  10,  18,  6,  21,  11,  9,  20,  9,  5,  0,  4]
```

- Coderen met RSA. Benny stuurt naar Valerie=> Benny gebruikt de openbare sleutel van Valerie e = 2087 en m= = 7597

```
>codeer:=modRek(cijferTekst, 2087,7597)
  [7450,  1,  2532,  6110,  4782,  344,  0,  7555,  5588,  1574,  4782,
  554,  7374,  4087,  5058,  2295,  554,  344,  2074,  3167,  871,
  1762,  7374,  2192,  442,  3783,  442,  4782,  0,  2074]
```

Decoderen

- Decoderen met RSA. Valerie gebruikt haar privésleutel
  - ✓ Bepalen van de privésleutel

```
>factor(7597)
  [71,  107]
>p:=71; q:=107; K:=(p-1)*(q-1)
  7420
>{ggd, d, j}:=gcdext(2087,7420); ggd, d, j
  1
  1863
  -524
```

  - ✓ Decoderen

```
>decodeer:=modRek(codeer, d, 7597)
  [17,  1,  22,  3,  5,  12,  0,  15,  2,  16,  5,  25,  21,  8,  14,
  23,  25,  12,  4,  10,  18,  6,  21,  11,  9,  20,  9,  5,  0,  4]
```

- Cijfers omzetten naar bijhorende tekst

```
>boodschp:=naarTekst(decodeer)
  rbwdfmapcqfzvioxzmeksgvljujfae
```

Oplossing b

```
>codeer:=[7705, 2605, 1001, 4098, 5859]
  [7705,  2605,  1001,  4098,  5859]
```

Nagaan of de boodschap van Mark komt: RSA gebruiken met de openbare sleutel van Mark. Als je getallen uitkomt >=0 en <=26, heb je de zender gevonden. We hebben immers aan de letters a tot z de waarden 0 tot 26 gegeven. Wanneer je met Ascii waarden werkt, moet je getallen uitkomen >=0 en <=255

```
>oorsprMark:=modRek(codeer, 1097,7663)
  [3349,  3602,  5675,  3016,  1415]
```

=> Boodschap komt niet van Mark.

Nagaan of de boodschap van Benny komt: RSA gebruiken met de openbare sleutel van Benny.

```
>oorsprBenny:=modRek(codeer, 941,9047)
  [6676,  3649,  7294,  4961,  5630]
```

=> Boodschap komt niet van Benny

Nagaan of de boodschap van Lutgard komt: RSA gebruiken met de openbare sleutel van Lutgard.

```
>oorsprLut:=modRek(codeer, 1217,9167)
  [15,  23,  11,  8,  19]
```

=> Boodschap komt van Lutgard want allemaal getallen >=0 en <=25

We zetten de boodschap dan om naar tekst

```
>naarTekst(oorsprLut)
  pxlit
```

Verzonden boodschap pxlit

Oplossing c

Valerie:

Tekst omzetten naar cijfers

```
>cijferTekst:=naarCijfer("toegepasteinformatica")
```

```
[19,  14,  4,  6,  4,  15,  0,  18,  19,  4,  8,  13,  5,  14,  17,
12,  0,  19,  8,  2,  0]
```

Valerie plaatst haar handtekening: RSA toepassen met haar privésleutel. De privésleutel van Valerie hebben we in oefening 1 gevonden: d = 1863 en m = 7597.

```
>codeer:=modRek(cijferTekst, 1863,7597)
```

```
[6124,  330,  4760,  1247,  4760,  4619,  0,  7195,  6124,  4760,
6590,  278,  4740,  330,  5481,  6690,  0,  6124,  6590,  2954,  0]
```

Valerie naar Mark? RSA toepassen met de openbare sleutel van Mark. Zit 6001 hiertussen?

```
>oorsprMark:=modRek(codeer, 1097,7663)
```

```
[2148,  6944,  3186,  1274,  3186,  4472,  0,  587,  2148,  3186,
2506,  568,  6873,  6944,  7500,  7070,  0,  2148,  2506,  420,  0]
```

Valerie naar Benny? RSA toepassen met de openbare sleutel van Benny. Zit 6001 hiertussen?

```
>oorsprBenny:=modRek(codeer, 941,9047)
```

```
[6422,  2760,  4550,  8362,  4550,  3916,  0,  4143,  6422,  4550,
6001,  7206,  2448,  2760,  6428,  6532,  0,  6422,  6001,  2891,  0]
```

=> 6001 zit hiertussen en staat voor de letter i

Valerie naar Lutgard? RSA toepassen met de openbare sleutel van Lutgard. Zit 6001 hiertussen?

```
>oorsprLutgard:=modRek(codeer, 1217,9167)
```

```
[2838,  859,  3803,  624,  3803,  1978,  0,  1279,  2838,  3803,  2233,
888,  651,  859,  1743,  4431,  0,  2838,  2233,  2858,  0]
```

Valerie naar Steven? RSA toepassen met de openbare sleutel van Steven. Zit 6001 hiertussen?

```
>oorsprSteven:=modRek(codeer, 977,8249)
```

```
[5776,  6297,  6833,  987,  6833,  4919,  0,  7026,  5776,  6833,  539,
5289,  4804,  6297,  2155,  5955,  0,  5776,  539,  3499,  0]
```

Besluit: de boodschap is verstuurd naar Benny.

Het getal 0 staat hier overal tussen omdat we aan de letter a de waarde 0 gegeven hebben en 0^{exp}(mod m) = 0. Dit hadden we kunnen vermijden door niet te starten met 0 als codering voor a maar bvb van 2, en b de waarde 3, ….

Codering van de letter b gaat hetzelfde probleem geven immers 1^{exp}(mod m) = 1. Dit probleem wordt verholpen door niet te starten met beginwaarde 0 voor a, 1 voor b enz. maar met beginwaarde 2 voor a, 3 voor b enz.

Oplossing d

In EuMathT kan je met de ingebouwde functie primes(n) alle priemgetallen laten genereren < 10000. We steken dit in een vector en bepalen de lengte van deze vector.

```
>v:=primes(10000);
>len:=length(v)
  1229
```

We genereren 2 gehele getallen >=1 en <=1229 om random de plaats te bepalen in deze vector. Zo hebben we 2 priemgetallen p en q gegenereerd.

```
>p:=v[intrandom(1229)], q:=v[intrandom(1229)]
  6199
  1571
```

We bepalen m, K en kiezen willekeurig een getal e <K zodat ggd(e,k)=1

```
>m:=p*q
  9738629
>K:=(p-1)*(q-1)
  9730860
>e:=997331
  997331
>gcd(e,K)
  1
```

We bepalen d.

```
>{ggd,d,j}:=gcdext(e,K); ggd, d, j
  1
  -4492009
  460393
```

De d die we hier uitkomen is <0, we kunnen deze positief maken door K erbij op te tellen.

```
>d:=d+K
  5238851
```

Openbare sleutel e = 997331 en m = 9738629
Privésleutel d = 5238851 en m = 9738629