Gegeven

	m	e
Marleen	3403	1111
Cindy	3551	1763

Marleen krijgt volgende boodschap toegestuurd:
2199 1698 3095 3333 2588 2426 378 3190
Ontcijfer deze boodschap.

Oplossing:

Om te ontcijferen hebben we de privé sleutel van Marleen nodig.
De privé sleutel van Marleen bestaat uit d en m.
m is reeds gekend => d berekenen.
Om d te berekenen, heb je de priemgetallen p en q waarmee m berekend werd. Deze priemgetallen bepaal je met de functie factor(m). Vervolgens bepaal je het getal K=(p-1)*(q-1).
Om d te bepalen, heb je de functie gcdext(e, K) nodig deze functie geeft als resultaat gcdext(e,K)=1= d.e+j.K (belangrijk de getallen e en K in de juiste volgorde ingeven)

```
>pC:=53; qC:=67; mC:=pC*qC, KC:=(pC-1)*(qC-1)

  3551
  3432

>eC:=1763; {ggd, dC, jC}:=gcdext(eC, (pC-1)*(qC-1)); ggd, dC, jC

  1
  1643
  -844

>pM:=41; qM:=83; mM:=pM*qM, KM:=(pM-1)*(qM-1)

  3403
  3280

>eM:=1111; {ggd, dM, jM}:=gcdext(eM, (pM-1)*(qM-1)); ggd, dM, jM

  1
  -1609
  545
  d is negatief om een positieve d te bekomen d+K

>dM:=dM+KM

  1671
```

```
>v:=[2199,  1698,  3095,  3333,  2588,  2426,  378,  3190];
```

```
  Zorg ervoor dat de m en d van Marleen in Maxima gekend zijn. Modulo
  rekenen doe je in Maxima.
```

```
> Md::=dM; Mm::=mM;
>boodschap=[]; for i=1 to cols(v) hulp::= v[i]; boodschap:=boodschap|mxmget(&mod(hulp^Md, Mm)); end; boodschap
```

```
  [111,  112,  103,  97,  118,  101,  32,  49]
```

```
  We zetten nu de bekomen ascii waarden om naar letters. Als hier een
  waarde staat dit niet ligt tussen 0 en 255, ben je fout bezig.
```

```
>tekst=""; for i=1 to cols(v)  tekst:=tekst|char(boodschap[i]); end; tekst
```

```
  opgave 1
```

Marleen stuurt naar Cindy een gehandtekende vercijferde boodschap. Wat ontvangt Marleen als de oorspronkelijke boodschap CD-ROM is?

.

```
>tekst="CD-ROM";
```

```
  Tekst omzetten naar Ascii
```

```
> v:=[]; for i=1 to strlen(tekst) v:=v|ascii(substring(tekst,i,i)); end; v
```

```
  [67,  68,  45,  82,  79,  77]
```

```
  Marleen plaatst haar handtekening= maakt gebruik van haar privé
  sleutel
```

```
>   Md::=dM; Mm::=mM;
>boodschap=[]; for i=1 to cols(v) hulp::= v[i]; boodschap:=boodschap|mxmget(&mod(hulp^Md, Mm)); end; boodschap
```

```
  [2243,  2621,  2710,  82,  2979,  3244]
```

```
  Marleen gebruikt de openbare sleutel van Cindy zodat Cindy de enige
  is die deze boodschap kan ontcijferen.
```

```
> Me::=1763; Mm::=3551;
>verzonden=[]; for i=1 to cols(boodschap) hulp::= boodschap[i]; verzonden:=verzonden|mxmget("mod(hulp^Me, Mm)"); end; verzonden
```

```
  [587,  1182,  2182,  1097,  1792,  2587]
```

Maak zelf een sleutel aan.
Geef m, e en d . Maak hierbij gebruik van het 600ste priemgetal en het priemgetal dat net groter is dan 3456.

```
  Laat bv alle priemgetallen kleiner dan 10000 genereren. Steek deze in
  een vector. Het 600ste element in deze vector is het 600ste
  priemgetal.
>v:=primes(10000); p:=v[600]
  4409
> q:=mxmget(&prev_prime(3456)) // mxmget is hier nodig omdat &prev_prime(3456) wordt geïnterpreteerd als een String
  3449
  m is het product van p en q
>m:=p*q, K:=(p-1)*(q-1)
  15206641
  15198784
  Keuze van e: e<K en ggd(e,k)=1
>e:=mxmget(&prev_prime(1519800))
  1519789
>gcd(e,K)
  1
  bepalen van d (zie opgave a hoe je d berekent)
> {ggd, d, j}:=gcdext(e, K); ggd, d, j
  1
  5525285
  -552496
  de gevonden d=5525285>0
```