Computergebruik: Maple **12 december 2002**

Eindopdrachten

Opdracht 1.
Gebruik MAPLE om een publieke sleutel voor het RSA-cryptosysteem te maken:
Genereer twee (verschillende) priemgetallen p en q van 20 decimale cijfers, bereken hun product $n := pq$ en kies e tussen 1 en $\varphi(n) = (p-1)(q-1)$ zo dat $\mathrm{ggd}(e, \varphi(n)) = 1$.
Maak je publieke sleutel (n, e) openbaar, door hem per e-mail naar `souvi@sci.kun.nl` te sturen.
De publieke sleutels zullen op de web-pagina

`http://www-math.sci.kun.nl/~souvi/maple/maple.html`

gepubliceerd worden.

Opdracht 2.
Schrijf MAPLE-functies voor de volgende taken:

(i) Gegeven n, zet een leesbare tekst om in een rij getallen tussen 0 en n.

(ii) Versleutel een getal m tussen 0 en n volgens RSA gegeven een publieke sleutel (n, e).

(iii) Bereken voor p, q en e de decryptie-sleutel d voor RSA.

(iv) Ontsleutel een met je publieke sleutel (n, e) gecodeerd getal b tussen 0 en n met behulp van d.

(v) Zet een rij getallen tussen 0 en n om in leesbare tekst.

Stuur de programma's per e-mail naar `souvi@sci.kun.nl`.

Opdracht 3.
Stuur elk van je medestudenten een met zijn/haar openbare sleutel versleuteld bericht en stuur een afschrift naar alle anderen en naar mij. Maak openlijk duidelijk aan wie de boodschap eigenlijk gericht was.
Van de bij jou binnenkomende berichten ontsleutel je de berichten die aan jou gericht waren. Probeer door RSA te kraken ook de andere berichten te lezen.

Een paar handige MAPLE-functies:
Opdracht 1: `isprime, nextprime, rand, gcd, igcd`
Opdracht 2:
(i)+(v): `with, StringTools, Ord, Char, convert/base, Explode, Implode, map`
(ii)+(iv): `mod, &^`
(iii): `igcdex`
Opdracht 3: `ifactor`