Universiteit van Stellenbosch

Toegepaste Wiskunde 314

Tutoriaal 7: Donderdag 22 April 2004

(1) (a) Doen probleem 1(b) op bladsy 154 van die klasnotas.

(b) Toets die korrektheid van jou antwoord deur middel van die program **EnDeCrypt**. [Wenk: Klik op "Tools" op die **EnDeCrypt** hoofspyskaart, en daarna op "Modular calculator".]

(c) Toets die korrektheid van jou antwoord deur middel van die **Mathematica**–opdrag `PowerMod[`a, b, n`]`, wat die modulêre magsverheffing $a^b \pmod{n}$ bereken.

(2) (a) Gebruik die **Mathematica**–opdrag `PrimeQ[`n`]` om te bepaal of $n = 27\,449$ priem is.

(b) Gebruik die **Mathematica**–opdrag `MultiplicativeOrder[`α, n`]` om te bepaal of die volgende waardes van α generators in die groep $(\mathbb{Z}_{27\,449}\backslash\{0\}, \times)$ is:

i. $\alpha = 17\,261$

ii. $\alpha = 17\,264$

(c) Doen probleem 2(b) op bladsy 154 van die klasnotas, maar gebruik die grondtal $\alpha_j = 17\,264$ in plaas van die gegewe grontal, $\alpha_j = 17\,261$. Gebruik 'n maksimale bloklengte–protokol.

(3) Die kriptoteks (28053244, 9841039), (22577741, 1427551) is met behulp van die ElGamal–sisteem gevorm, en is aan Persoon B in Tabel 4-1 op bladsy 134 van die klasnotas gerig. 'n Bloklengte–protokol van 6 syfers (3 karakters) is gebruik. Wat is die ooreenstemmende skoonteks? [Wenk: Die geheime sleutelgetal van Persoon B is $a = 247$.]

(4) (a) Gebruik die **Mathematica**–opdragte `Table[`$A(i), \{i, a, b\}$`]`, `PowerMod[`a, b, n`]`, `Extract[`A, B`]` en `Intersection[`A, B`]` om die diskrete logaritme

$$a = \log_{619} 616 \pmod{1223}$$

volgens Shanks se algoritme te bereken (soos in die klas gedemonstreer).

(b) Gebruik die **Mathematica**–opdrag `MultiplicativeOrder[`α, n, β`]` om die korrektheid van jou antwoord in (a) te toets.

(c) Doen probleem 4(a) op bladsy 155 van die klasnotas.