Universiteit van Stellenbosch

Toegepaste Wiskunde 314

Tutoriaal 7: Donderdag 22 April 2004

MEMORANDUM

(1) $74\,183^{6\,149} \equiv 79\,809 \pmod{81\,403}$.

(2) (a) Die getal $n = 27\,449$ is wel priem.

(b) i. $\alpha = 17\,261$ is nie 'n generator van $(\mathbb{Z}_{27\,449}\backslash\{0\}, \times)$ nie — die orde daarvan is $13\,724$.

ii. $\alpha = 17\,264$ is wel 'n generator van $(\mathbb{Z}_{27\,449}\backslash\{0\}, \times)$ — die orde daarvan is $27\,448$.

(c) Die kriptoteks is byvoorbeeld $y_0 = (15\,537, 3\,701)$, $y_1 = (17\,348, 12\,531)$, $y_2 = (21\,724, 22\,852)$, $y_3 = (16\,263, 9\,243)$ en $y_4 = (11\,039, 15\,479)$ indien die maskers $k_0 = 457$, $k_1 = 1\,965$, $k_2 = 3\,167$, $k_3 = 17$ en $k_4 = 905$ onderskeidelik met 'n bloklengte–protokol van 4 syfers (2 karakters) gebruik word.

(3) Die skoonteks is `follow`.

(4) Die eerste lys in Shanks se algoritme word gegee deur ((0, 1), (1, 267), (2, 355), (3, 614), (4, 56), (5, 276), (6, 312), (7, 140), (8, 690), (9, 780), (10, 350), (11, 502), (12, 727), (13, 875), (14, 32), (15, 1206), (16, 353), (17, 80), (18, 569), (19, 271), (20, 200), (21, 811), (22, 66), (23, 500), (24, 193), (25, 165), (26, 27), (27, 1094), (28, 1024), (29, 679), (30, 289), (31, 114), (32, 1086), (33, 111), (34, 285))

Die tweede Lys in Shanks se algoritme word gegee deur ((0, 616), (1, 979), (2, 49), (3, 1148), (4, 1213), (5, 814), (6, 27), (7, 982), (8, 294), (9, 773), (10, 1163), (11, 1215), (12, 162), (13, 1000), (14, 541), (15, 969), (16, 863), (17, 1175), (18, 972), (19, 1108), (20, 800), (21, 922), (22, 286), (23, 935), (24, 940), (25, 533), (26, 1131), (27, 640), (28, 493), (29, 718), (30, 748), (31, 752), (32, 671), (33, 171), (34, 512))

Die enigste elemente uit die twee lyste met gemeenskaplike tweede inskrywings is (26, 27) en (6, 27). Dus is die diskrete logaritme $a = 35 \times 26 + 6 = 916$

Die skoonteks is `kipling`.