Universiteit van Stellenbosch

Toegepaste Wiskunde 314

Tutoriaaltoets 7: Donderdag 22 April 2004

MEMORANDUM

Tuttoets 7a.

Sien bladsy 135 van die klasnotas.

Tuttoets 7b.

Die volgende lyste kan met behulp van Shanks se algoritme opgestel word, waar $n = 2\,789$ en $m = \lceil \sqrt{n-1} \rceil = 53$:

Die lys $(j, \alpha^{mj}) \pmod{n}$:
((0, 1), (1, 619), (2, 1068), (3, 99), (4, 2712), (5, 2539), (6, 1434), (7, 744), (8, 351), (9, 2516), (10, 1142), (11, 1281), (12, 863), (13, 1498), (14, 1314), (15, 1767), (16, 485), (17, 1792), (18, 2015), (19, 602), (20, 1701), (21, 1466), (22, 1029), (23, 1059), (24, 106), (25, 1467), (26, 1648), (27, 2127), (28, 205), (29, 1390), (30, 1398), (31, 772), (32, 949), (33, 1741), (34, 1125), (35, 1914), (36, 2230), (37, 2604), (38, 2623), (39, 439), (40, 1208), (41, 300), (42, 1626), (43, 2454), (44, 1810), (45, 2001), (46, 303), (47, 694), (48, 80), (49, 2107), (50, 1770), (51, 2342), (52, 2207))

Die lys $(i, \beta\alpha^{-i}) \pmod{n}$:
((0, 2373), (1, 15), (2, 2232), (3, 1904), (4, 2184), (5, 2013), (6, 2227), (7, 1160), (8, 2479), (9, 1285), (10, 1556), (11, 2277), (12, 233), (13, 2318), (14, 198), (15, 2688), (16, 2263), (17, 381), (18, 355), (19, 2622), (20, 1367), (21, 1486), (22, 228), (23, 1574), (24, 493), (25, 1960), (26, 1592), (27, 1498), (28, 898), (29, 866), (30, 9), (31, 1897), (32, 2258), (33, 2426), (34, 650), (35, 1894), (36, 696), (37, 2603), (38, 771), (39, 2607), (40, 1924), (41, 2371), (42, 833), (43, 2350), (44, 1055), (45, 800), (46, 1902), (47, 213), (48, 2131), (49, 1378), (50, 2565), (51, 2368), (52, 2060))

Dit volg dus dat $a \equiv \log_{716} 2\,373 \equiv 53 \times 13 + 27 \equiv 716 \pmod{2\,789}$. Dekripsie met behulp van die ElGamal–sisteem en **EnDeCrypt** lewer dan die skoonteks `ok`.