Universiteit van Stellenbosch

Toegepaste Wiskunde 314

Tutoriaal 8: Donderdag 29 April 2004

(1) Gestel 'n sesde persoon, Persoon F, moet tot die RSA–gebruikersgroep in Tabel 4-4 op bladsy 143 van die klasnotas toegevoeg word. Genereer, met behulp van die program **Mathematica**, geldige sleutelgetalle p, q, n, e en d vir Persoon F, sodat die publieke getalle, n en e, uit net soveel desimale bestaan as dié van Persone A–E. [Wenk: Die **Mathematica**–opdrag `Prime[m]` lewer die m–de priemgetal; die opdrag `GCD[e,n]` lewer, met behulp van die Euklidiese Algoritme, die grootste gemene deler van e en n; en die opdrag `PowerMod[e,-1,n]` lewer, met behulp van die Gewysigde Euklidiese Algoritme, die multiplikatiewe inverse $e^{-1} \pmod{n}$.]

(2) Probleem 7(a) op bladsy 155 van die klasnotas (gebruik 'n bloklengte protokol van 5 karakters, oftewel 10 desimale syfers).

(3) Die getal $n = 762\,029$ bestaan uit die produk van twee priemgetalle. Gebruik Pollard se Algoritme met gladheidsgrens $B = 13$ om n te faktoriseer. Gebruik die opdrag `FactorInteger[n]` in **Mathematica** om die korrektheid van jou antwoord te toets.

(4) Gebruik die **Mathematica**–opdragte `FactorInteger[n]` en `PowerMod[e,-1,n]` om Probleem 6 op bladsy 155 van die klasnotas te doen.

(5) Probleem 8(c) op bladsy 155 van die klasnotas.

(6) Probleem 10(a) op bladsy 156 van die klasnotas.

(7) Probleme 11(a)–(b) op bladsy 156 van die klasnotas.

(8) Konstrueer binêre (n, M, d)–kodes met die volgende parameters of verduidelik waarom so 'n kode nie bestaan nie:

(a) $(6, 2, 6)$

(b) $(3, 8, 1)$

(c) $(4, 8, 2)$

(d) $(5, 4, 3)$

(e) $(5, 3, 4)$

(f) $(8, 30, 3)$