Universiteit van Stellenbosch

Toegepaste Wiskunde 314

Tutoriaal 8: Donderdag 29 April 2004

MEMORANDUM

(1) Die RSA–gebruikersmodulusse in Tabel 4-4 het almal 'n lengte van 16 desimale syfers. Dus is die priemfaktore van elk van hierdie modulusse waarskynlik 8 desimale syfers lank. Eksperimentering in Mathematica lewer byvoorbeeld die volgende priemgetalle van hierdie lengtes: $p = \texttt{Prime[2000000]} = 32\ 452\ 843$ en $q = \texttt{Prime[5000000]} = 86\ 028\ 121$. Die produk, $n = 2\ 791\ 857\ 104\ 398\ 003$, van hierdie twee prieme het wel die verlangde lengte, en $\phi(n) = 2\ 791\ 856\ 985\ 917\ 040$. Die getal $d = 5\ 561$ is byvoorbeeld relatief priem tot $\phi(n)$, in welke geval $e \equiv d^{-1} \equiv 2\ 750\ 689\ 520\ 920\ 601 \pmod{\phi(n)}$ wel ook die verlangde lengte van 16 desimale het.

(2) Die kriptoteks is $y^{(0)} = 745\ 722\ 170\ 417\ 676$ en $y^{(1)} = 401\ 146\ 017\ 567\ 004$.

(3) Neem $n = 762\ 029$ en $B = 13$, soos voorgestel, en kies byvoorbeeld $a = 320$. Dan word die volgende resultate met behulp van Pollard se Algoritme verkry:

q	$\lfloor \ln n / \ln q \rfloor$	a
2	19	542 294
3	12	293 252
5	8	522 059
7	6	139 515
11	5	64 460
13	5	384 989

Met hierdie afvoer word die nie–triviale faktor $\text{ggd}(384\ 988, n) = 883$ van n verkry. Die **Mathematica**–opdrag `FactorInteger[762029]` lewer `{{863, 1}, {883, 1}}` as afvoer, wat die korrektheid van die faktorisering bevestig, aangesien $n = 863 \times 883$.

(4) (a) Vir Persoon A: $p = 15\ 485\ 863$, $q = 179\ 424\ 673$ en $d = 6\ 617$

(b) Vir Persoon B: $p = 86\ 028\ 121$, $q = 104\ 395\ 301$ en $d = 1\ 043$

(c) Vir Persoon C: $p = 49\ 979\ 687$, $q = 141\ 650\ 939$ en $d = 3\ 821$

(d) Vir Persoon D: $p = 32\ 452\ 843$, $q = 160\ 481\ 183$ en $d = 2\ 389$

(e) Vir Persoon E: $p = 67\ 867\ 967$, $q = 122\ 949\ 823$ en $d = 5\ 915$

(5) Die boodskap `AANVAL` is aan Persoon C gerig.

(6) Persoon A vorm die volgende kenteks, deur sy/haar eie sleutelgetalle te gebruik:

$$\begin{aligned} k_{E,x^{(0)}} &\equiv 33\ 532\ 075\ 550\ 261 \pmod{2\ 778\ 545\ 904\ 897\ 799} \\ k_{E,x^{(1)}} &\equiv 2\ 047\ 816\ 057\ 907\ 577 \pmod{2\ 778\ 545\ 904\ 897\ 799} \end{aligned}$$

Daarná vorm A die volgende kriptotekste, deur van Persoon E se publieke sleutelgetalle gebruik:

$$\begin{aligned} y^{(0)} &\equiv 624\ 759\ 770\ 901\ 116 \pmod{8\ 344\ 354\ 530\ 019\ 841} \\ y^{(1)} &\equiv 1\ 170\ 993\ 872\ 230\ 238 \pmod{8\ 344\ 354\ 530\ 019\ 841} \end{aligned}$$

(7) (a) Die boodskap is eg; die ooreenstemmende skoonteks is `TRUE`.

(b) Die boodskap is deur Persoon C vervals; die ooreenstemmende skoonteks is `LIAR`.