

6. cvičení - domácí úloha

Zadáno 31. března 2009

Odevzdat do 13. dubna 2009

1. Zvol si dvě oblíbená prvočísla (přiměřeně velká - aspoň 1 z nich ať je aspoň dvouciferné). Najdi pro ně vhodný veřejný a tajný klíč pro RSA.

2. Nechtě jsou p, q dvě různá lichá prvočísla. Jak ze znalosti $N = pq$ a $\varphi(N)$ můžeme spočítat p a q ? (Bonusová otázka, kterou není potřeba řešit: Jak můžeme p, q zjistit, známe-li N a $\text{nsn}(p - 1, q - 1)$?)

K započítání domácí úlohy stačí (správně) vyřešit aspoň částečně oba příklady.