# Digitalni podpis, kitajski izrek o ostankih, RSA

1. Alenka ima javni ključ $(n, e)$ in zasebni ključ $(n, d)$ za RSA. Radi bi, da nam podpiše sporočilo $m$, a sporočila ne želimo razkriti. Zato podtaknemo v podpis neko drugo sporočilo $m' \equiv k \cdot m \pmod{n}$. Privzamemo lahko, da je sporočilo $m$ tuje z $n$ (sicer znamo $n$ razcepiti in lahko sami podpišemo karkoli).

   (a) Kako moramo izbrati $k$, da bomo iz podpisa sporočila $m'$ ($s' \equiv m'^d \pmod{n}$) lahko izračunali podpis sporočila $m$ ($s \equiv m^d \pmod{n}$) ne da bi uporabili zasebni ključ $d$?

   (b) Naj bo $n = 85$, $e = 11$ in $m = 42$. Poiščite $k$ in sporočilo $m'$ kot v točki (a).

2. Prababica noče povedati, koliko je stara. Povedala je, da je bilo pred enim letom število njenih let deljivo s tri, čez dve leti bo deljivo s pet in čez štiri leta bo deljivo s sedem. Koliko je stara?

3. Napad na majhen eksponent RSA. Naj bodo $n_1, n_2, n_3$ paroma tuji moduli za kriptosistem RSA in $e = 3$. Naj bo $y_i = x^e \pmod{n_i}$ za $i = 1, 2, 3$, torej isto sporočilo zašifriramo s tremi različnimi javnimi ključi. Poiščite $x$. Ilistrirajte napad na primeru $n_1 = 55$, $n_2 = 391$, $n_3 = 1189$ in $c_1 = 6$, $c_2 = 105$, $c_3 = 1148$.

4. Naj bo $p$ liho praštevilo in $a$ naravno število. Koliko rešitev ima enačba

$$x^a \equiv 1 \pmod{p}?$$

5. Poiščite vse rešitve enačbe

   (a) $x^7 \equiv x \pmod{19}$,

   (b) $x^7 \equiv x \pmod{23}$.

6. Nezakrita sporočila pri kriptosistemu RSA. Naj bo $(n = p \cdot q, e)$ javni ključ za RSA. Koliko besedil iz $\mathbb{Z}_n$ se pri šifriranju s ključem $(n, e)$ ne spremeni? Koliko je to za $n = 85$ in $e = 33$?

7. Naj bo $p = 19$, $q = 23$ in $n = p \cdot q = 437$. Poiščite sporočilo, različno od $0, 1, -1$, ki se pri šifriranju z javnim ključem $(437, 7)$ za RSA ne bo spremenilo.