Cvičení 5. 4. 2013 – řešení

Příklad 2. Faktorizujte číslo $N = 6557$, víte-li, že je součinem dvou prvočísel p, q splňujících $|p - q| < 10$ (jde to bez kalkulačky!).

Řešení: Budeme předpokládat $q = p + k$ pro $k = 0, 2, 4, 6, 8$ (prvočíla p, q jsou evidentě obě lichá) a řešit kvadratickou rovnici $p(p + k) = 6557$.

Pokud $k = 0$, tak $p^2 = 6657$. Ale my víme, že $80^2 = 6400 < 6557 < 6561 = 81^2$ (tohle se dá ještě tipnout a vynásobit písemně).

Pokud $k = 2$, potřebujeme $p(p+2) = 6557$, což po doplnění na čtverec dává $(p + 1)^2 = p + 2p + 1 = 6558$, což už víme, že není čtverec.

Pokud $k = 4$, potřebujeme $p(p + 4) = 6557$. Tedy $p^2 + 4p + 4 = 6561 = 81^1$, tedy $p + 2 = 81$ funguje (a nutně $q = 83$).

Celý postup výše je ekvivalentní tomu, že zkoušíme napsat 6557 ve tvaru $a^2 - b^2 = (a + b)(a - b)$ pro malé b, tj. zjišťujeme, zda $6557 + b^2$ není náhodou čtverec pro $b = 0, 1, 2, 3, 5$. Pro $b = 2$ máme $6557 + 4 = 6561 = 81^2$. Zapsáno takhle je to takzvaná Fermatova faktorizace.

Příklad 3. Jsme útočníci na RSA, známe $n = 851, e = 7$, ale nikoli tajný exponent d.

Zachytili jsme zašifrovanou zprávu $C = 42$ od Alice. Rádi bychom si přečetli, co Alice psala. Přesvědčili jsme ji proto, aby dešifrovala (tj. umocnila na d-tou modulo n) nevinně se tvářící zprávu $M = 270 \equiv 2^e C \pmod{n}$ a sdělila nám výsledek $V = 603$. Jak teď dešifrujeme C?

Řešení: Protože platí $2^{ed} \equiv 2 \pmod{n}$, tak platí $V \equiv M^d \equiv 2C^d \pmod{n}$. Modulo n je $2^{-1} \equiv 426$, tedy hledaná zpráva je $426 \cdot V \equiv 727$.

Příklad 4. Tři malá prasátka mají každé svůj privátní klíč (d_1, N_1), (d_2, N_2) a (d_3, N_3) a všechna používají veřejný exponent $e = 3$. Červená Karkulka poslala každému prasátku identickou pozvánku M na narozeninovou oslavu zašifrovanou pomocí jeho veřejného klíče, tj. zprávy mají tvar $C_1 = M^e \pmod{N_1}$, $C_2 = M^e \pmod{N_2}$, $C_3 = M^e \pmod{N_3}$.

Velký zlý vlk všechny tři zašifrované zprávy zachytil a zná veřejné klíče. Poraďte mu, jak z C_1, C_2, C_3 získat M.

Řešení: Vlk snadno může ověřit, že čísla N_1, N_2, N_3 jsou nesoudělná – spustí na každou z jejich dvojic Euklidův algoritmus a pokud dostane výsledek větší než jedna, už z něj vypadne faktorizace nějakého N_i.

Aby posílání zprávy mělo smysl, musí být $M < N_1, N_2, N_3$, takže $0 \leq M^3 < N_1 N_2 N_3$. Číslo M^3 pak lze snadno dopočítat z Čínské zbytkové věty a sady rovnic:

$$\begin{aligned} M^3 &\equiv C_1 \pmod{N_1} \\ M^3 &\equiv C_2 \pmod{N_2} \\ M^3 &\equiv C_3 \pmod{N_3}. \end{aligned}$$

Vlk tedy určil M^3 v $\mathbb{Z}$. Nyní mu stačí spočítat běžnou třetí odmocninu z M^3, aby dostal M.

Proti tomuto útoku existují dvě obrany: Větší e a padding.