

Elektronický podpis pomocí RSA

1 Označení parametrů RSA

- modulus $n = pq$ pro p, q různá prvočísla
- veřejný exponent e takový, že $e, \varphi(n)$ jsou nesoudělná. ($\varphi()$ je Eulerova funkce).
- soukromý exponent $d \equiv e^{-1} \pmod{\varphi(n)}$

2 Podepsání zprávy

Podpis je vždy vázaný ke konkrétní zprávě a nedá se "zkopírovat" ke zprávě jiné – to odpovídá tomu, že se při podepisování i ověřování podpisu počítá se zprávou. Podpisem zprávy M je pak

$$S = M^d \pmod{n}$$

Zejména si povšimněte, že zprávu dokáže podepsat pouze vlastník soukromého exponentu d .

Příklad 1. *Nechť RSA parametry jsou $n = 91 = 7 \cdot 13$, $e = 5$, $d = 29$. Podepište zprávu $M = 7$.*

Řešení. *Podpisem je $S = M^d = 7^{29} \equiv 63 \pmod{n}$.*

3 Ověření podpisu

Vzpomeňte si, že u šifrování se nejdříve zpráva umocňovala na e a pak se $C = M^e$ umocňovalo na d . U podepisování je pořadí exponentů opačné. Při

ověřování podpisu se tedy kontroluje, zda

$$S^e \equiv M \pmod{n}.$$

Pokud kongruence platí, je S podpisem zprávy M . Všimněte si, že k ověření podpisu stačí znalost veřejného klíče – může to tedy udělat kdokoli.

Příklad 2. *Ověřte podpis $S = 63$ zprávy $M = 7$ z předchozího příkladu.*

Řešení. *Platí, že $S^e = 63^5 \equiv 7 \pmod{91}$. Tedy $S = 63$ je podpisem zprávy $M = 7$.*

Příklad 3. *Ověřte, zda je $S_2 = 24$ podpisem zprávy $M_2 = 62$.*

Řešení. *$(S_2)^e = 24^5 \equiv 33 \not\equiv 62 \pmod{91}$. Tedy $S_2 = 24$ není podpisem zprávy $M_2 = 62$.*