

$p = 449$. Hledáme číslo $a \in \mathbb{Z}_{449}$ tž. $a^2 \equiv 2 \pmod{449}$, $449-1 = 2^6 \cdot 7 \implies q = 7, e = 6$.

1. zvolíme $z_0 = 3 \implies z_0^{\frac{p-1}{2}} = 3^{224} \equiv -1 \pmod{449} \implies z = 3^7 \pmod{449} = 391$

2. $y = 391, r = 6, b = 2^7 \pmod{449} = 128, x = 2^4 = 16$

3. hledáme $m \in \mathbb{N}_0$, zkoušením zjistíme, že $m = 5$, protože $b^{2^5} = 128^{32} \equiv 1 \pmod{449}$

4. $t = 391^{2^{6-5-1}} = 391, y = 391^2 \pmod{449} = 221, r = 5, x = 391 \cdot 16 \pmod{449} = 419, b = 128 \cdot 221 \pmod{449} = 1$

5. $b = 1 \implies m = 0 \implies$ výsledek je $a = x = 419$. ($419^2 \pmod{449} = 2$)