Domácí úlohy 3.

odevzdat do 15.3. 10:40

Pro úlohy 2a), 3a) doporučuji použít kalkulačku nebo si udělat jednoduchý počítačový program. Úlohy 2b), 3b) lze řešit v ruce.

1. (4 bodů) Uvažujte binární operaci $x + y = 0 * (x * y)$ definovanou na eliptické křivce (viz přednáška). Popište, jak vypadá $-x$. Návod: pro který bod u platí $0 * u = 0$? Řešení popište neformálně pomocí obrázku.

2. (8 bodů) Uvažujte Diffie-Hellmanův kryptosystém s parametrem $\mathbb{Z}_p^* = \langle a \rangle$. Nepřítel zachytil čísla x, y. Jaké je heslo?

(a) $p = 43$, $a = 3$, $x = 22$, $y = 23$.
(b) $p = 2^{31} - 1$, $a = 7$, $x = 2$, $y = 343$.

3. (8 bodů) Uvažujte El Gamalův kryptosystém s veřejným klíčem $\mathbb{Z}_p^* = \langle a \rangle$, b. Nepřítel zachytil dvojici (c_1, c_2). Jaká je tajná zpráva?

(a) $p = 43$, $a = 3$, $b = 12$, $(c_1, c_2) = (4, 4)$.
(b) $p = 2^{31} - 1$, $a = 7$, $b = 2$, $(c_1, c_2) = (1, 3)$.