E: p, g, A, B

$B^{a} = K$

$A^{b} = K$

$a = ?$

$b = ?$

$g^{a} = A \pmod{p}$

PLD

$g^{b} = B \pmod{p}$

$b = ?$

PLD

Kryptosystem ElGamala (ElGamal)

$\mathcal{P} = \mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ $\quad$ p - duża liczba pierwsza

$\mathcal{C} = \mathbb{Z}_p^* \times \mathbb{Z}_p^* = \{(x,y) : x, y \in \mathbb{Z}_p^*\}$

$\mathcal{K} = \{(p, g, x, \alpha) : g^x \equiv \alpha \pmod{p}\}$

generator w $\mathbb{Z}_p^*$ $\iff$ $\{g^x : x \in \mathbb{N}\} = \mathbb{Z}_p^*$

(p, g, x, α)

Klucz publiczny: $(p, g, \alpha) = K$

Klucz prywatny: $x = (p, g, x)$

$(p, g, \alpha) = K$

A

$m \in P$

losuje $k \in \mathbb{Z}_{p-1}^*$

$\hat{m} = e_K(m, k) \longrightarrow (y_1, y_2)$

B (p, g, x, α)

$\boxed{g^x = \alpha}$ $(\mathbb{Z}_p)$

$m = d_K(y_1, y_2) = y_2 (y_1^x)^{-1}$

odwrotność w $\mathbb{Z}_p^*$ (RAE)

$$e_K(m, k) = (y_1, y_2), \quad y_1 = g^k \mod p$$
$$y_2 = m\alpha^k \mod p$$

B: $y_2 = m(g^x)^k = \boxed{m g^{xk}}$

$$y_1 = g^k \quad | ()^x$$
$$y_1^x = g^{kx} \quad | ()^{-1}$$
$$y_1^{-x} = (g^{kx})^{-1}$$

$$d_K(y_1, y_2) = y_2 \cdot (y_1^x)^{-1} =$$
$$= m\cancel{g^{xk}} \cdot (\cancel{g^{xk}})^{-1} = m$$

RSA $\quad n = pq$

$\sqrt{n}$

$\sqrt{113} \approx 10, \dots$

$2, 3, 5, 7$

$n \to \sqrt{n}$

$n = 2^{1000}$

$\sqrt{n} = 2^{500}$

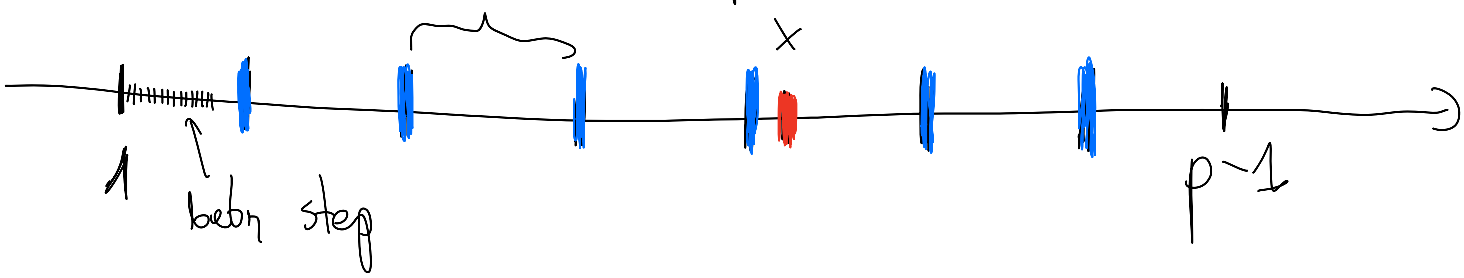
PLD $\quad \mathbb{Z}_p$

$g^x = a \qquad x = ?$

$x \in \{1, 2, \dots, p-1\} \qquad p \sim 2^{1000}$

Algorytm Shanksa (baby step - giant step)

giant step $= \sqrt{p}$



$g^x = a \pmod{p} \qquad x \in ?$

D - słownik (Python)

$m \leftarrow \lceil \sqrt{p} \rceil$

for $j = 0..\boxed{m-1}$

$\quad D[g^{jm}] = j \qquad (g^m)^j$

for $i = 0..\boxed{m-1}$

$\quad$ if ag^{-i} in D $\qquad x$

złożoność czasowa $\to O(\sqrt{p})$

return $\boxed{mD[ag^{-i}] + i}$

złożoność pamięciowa $O(\sqrt{p})$

$$ag^{-i} = g^{jm} \quad | \cdot g^{i}$$

$$a = g^{\boxed{jm+i}}$$

x

meet in the middle

Metoda ρ Pollarda

rho

Alg. Pohliga-Hellmana

Metoda rachunku indeksowego

$\mathbb{Z}_p \rightsquigarrow (G, \cdot)$ ← grupa

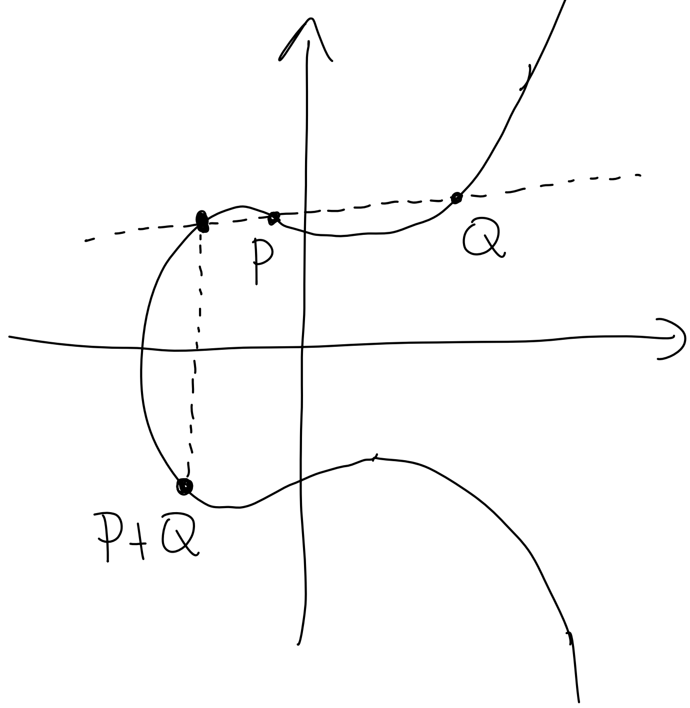
$g^x = a \longrightarrow \boxed{g^x = a}$

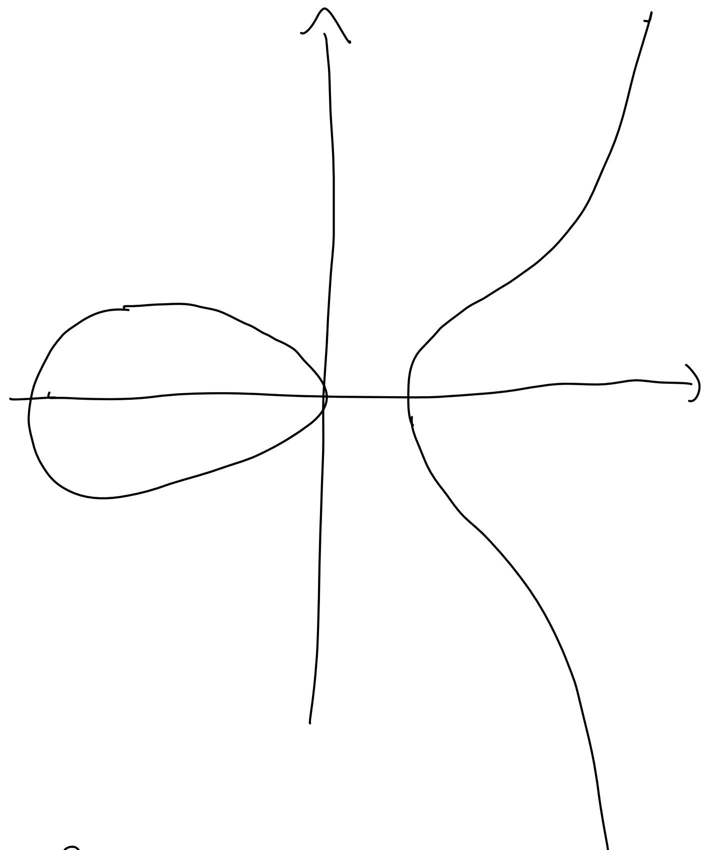
Kryptosystemy oparte o krzywe eliptyczne

(80')

$y^2 = x^3 + ax + b$, $a, b \in \mathbb{R}$

$\{(x,y) : \quad \} = \mathcal{E}$





$P+Q$ $(\mathcal{E}, +)$ tworzy grupę