4 - Discrete-Log Ro-Pollarda

Friday, 21 June 2024 15:17

Mamy a, b. Chcemy x: $a^x = b$.

Optymalizacja pamięci w Baby-Step-Giant-Step:

Generujemy dużo liczb postaci $a^{\alpha_i} \cdot b^{\beta_i}$.

Jeśli $a^{\alpha_i} \cdot b^{\beta_i} = a^{\alpha_j} \cdot b^{\beta_j}$ to $a^{\alpha_i - \alpha_j} = b^{\beta_j - \beta_i}$

Więc znajdując $\beta^* = (\beta_j - \beta_i)^{-1} \pmod{|G|}$

$a^{\beta^*(\alpha_i - \alpha_j)} = b$.

Losujemy α_0, β_0. $(\alpha_{n+1}, \beta_{n+1}) = f(\alpha_n, \beta_n)$

f musi zależeć wyłącznie od $\alpha_n \cdot \beta_n$. Wtedy ciąg się zapętla i można zrobić żółwia i zająca.

Standardowe f:

- Mała stała $k \sim 20$
- $h: G \to [k]$ (hasz)
- Losowe $x_1, \dots, x_k, y_1, \dots, y_k$
- dla pary (α, β): $j = h(a^\alpha \cdot b^\beta)$

$f(\alpha, \beta) = (\alpha + x_j, \beta + y_j)$