Problem obliczenia logarytmu dyskretnego.

Dane są 2 liczby α, β

$$\exists\ x : \alpha^x = \beta$$

$$x = \log_\alpha \beta$$

Niech teraz $\alpha, \beta \in \mathbb{Z}_p^*$

Zat, że $\exists\ x : \alpha^x \bmod p = \beta$

$x = \log_\alpha \beta \leftarrow$ logarytm dyskretny

Testowanie wszystkich x - nieefektywna metoda

Komputer kwantowy może to policzyć w czasie wielomianowym

1 Algorytm Shanks'a
Baby step, giant step

α - rzędu q w Z_p^* $(p = 2q+1)$

β - rzędu q

Chcemy policzyć $\log_\alpha \beta$

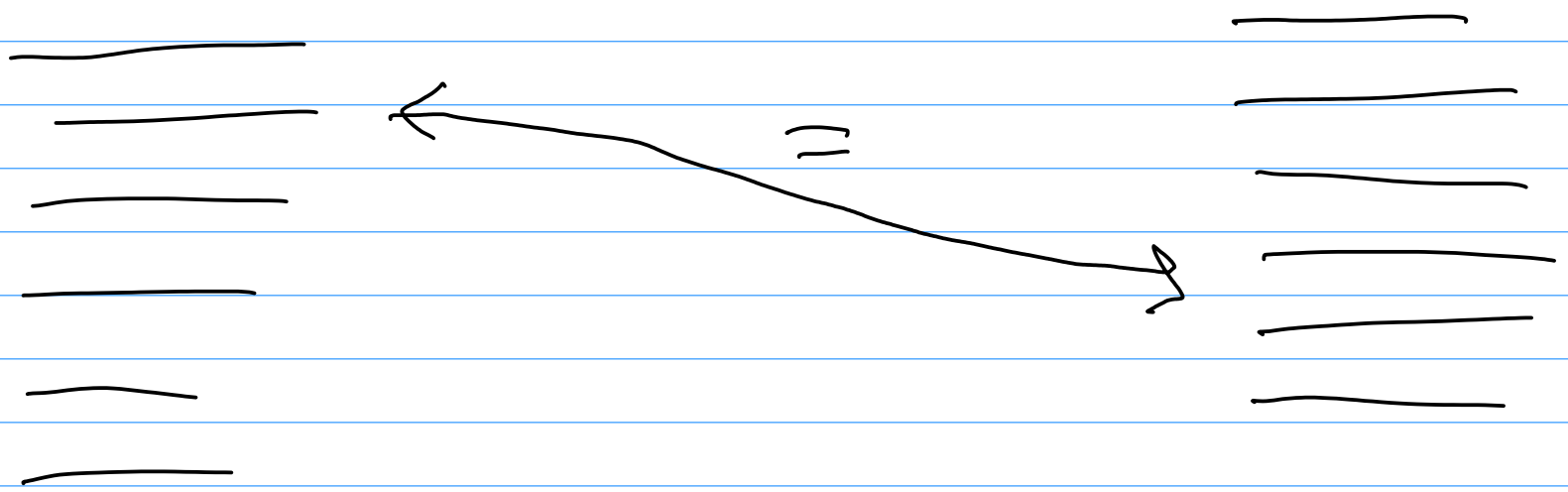
czyli $x : \alpha^x \bmod p = \beta$

$$x = x_1\lceil\sqrt{q}\rceil + x_0, 0 \le x_1, x_0 < \sqrt{q}$$

$$\alpha^{x_1\lceil\sqrt{q}\rceil + x_0} = \beta \iff \alpha^{x_1\lceil\sqrt{q}\rceil} = \beta\alpha^{-x_0}$$

Algorithm:

Pollia $\alpha^{x_1\lceil\sqrt{q}\rceil}$ pollia $\beta\alpha^{-x_0}$



Algorytm Pohliga - Hellmana

Może być użyty dla grup rzędu $q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}$

$p = 2 q_1^{t_1} \cdots q_s^{t_s} + 1$

2 redukcje:

R1: Jeśli umiemy policzyć $x : \alpha^x = \beta$ dla α, β rzędu q, to potrafimy też policzyć x', że $g^{x'} = y$ dla g rzędu q^t

Pokażę tę redukcję dla $t = 2$

Chcemy policzyć $x^{x'}$ i $q = y$

$x' = qx_1' + x_0'$ $\quad x' < q^2$

$x_1', x_0' < q$

Redukcja:

$\alpha = g^q \qquad \beta = y^q$

$g^{qx'} = y^q \qquad q^{qx'} = g^{q^2 x_1' + q x_0'} = q^{q x_0'}$

$\alpha^{x_0'} = \beta \qquad = \alpha^{x_0'}$

Umiemy policzyć x_0'

$$q^{q x_1' + x_0'} = y$$

$$q^{q x_1'} = y g^{-x_0'}$$

$$\alpha^{x_1'} = y g^{-x_0'}$$

umiemy policzyć x_1'

$$\Rightarrow x' = q x_1' + x_0'$$

R2: Jeżeli umiemy policzyć log dyskr w grupie rzędu $q_i^{t_i}$ dla $i = 1 - - 5$ to potrafimy policzyć log dyskr w grupie rzędu $q_1^{t_1} \cdot - - q_5^{t_5}$

$\alpha^x = \beta$ w grupie rzędu

$q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s} = m$

x jest jednoznacznie wyznaczone

przez układ reszt $(x_1, x_2, \ldots, x_s)$ gdzie

$x_i = x \bmod q_i^{t_i}$

$\alpha^{x \frac{m}{q_i^{t_i}}} = \alpha^{x q_1^{t_1} \cdots q_{i-1}^{t_{i-1}} q_{i+1}^{t_{i+1}} \cdots q_s^{t_s}}$

$= \beta^{\frac{m}{q_i^{t_i}}} = y$ $\quad \alpha^{\frac{m}{q_i^{t_i}}} = g$

rzędu $q_i^{t_i}$

$g^x = y$ w grupie rzędu $q_i^{t_i}$

$\Rightarrow g^{x_i} = y \Rightarrow$ umiemy wyliczyć x_i

Wyliczamy wszystkie x_i
i x uzyskujemy z układ rest
$x_{a_i} \dots, x_s$

Z punktu widzenia alg Pohliga-
Hellmana problem logarytm
dyskretnego jest najtrudniejszy
w grupach mod $p = 2 \cdot q + 1$

Liczby Sophie - Germain

Dla faktoryzacji alg $p-1$

dzięki najmniejszej efektywnej dla liczb $n = p \cdot q = (2p'+1)(2q'+1)$

Algorytm rachunku indeksu

2 fazy

faza I: (obliczamy $t : \alpha^t \underset{p}{=} \beta$)

$B = e^{\sqrt{\ln p \ln \ln p}}$

Wiele razy

losujemy x

Jeżeli $\alpha^x \bmod p$ nie rozkłada się

na czynniki $< B$ to zapamiętujemy x

Robimy to aż zbierzemy $B + C$ liczb x

$$\alpha^{x_i} \underset{p}{\equiv} p_1^{x_{i1}} p_2^{x_{i2}} \cdots p_k^{x_{ik}}$$

$$x_i \underset{p-1}{=} x_{i1} \log_\alpha p_1 + x_{i2} \log_\alpha p_2 + \cdots + x_{ik} \log_\alpha p_k$$

wiemy dane

Obliczamy $\log_\alpha p_1 \cdots \log_\alpha p_k$

Znajdujemy y: $\alpha^y \beta^{-1} = p_1^{y_1} \cdots p_k^{y_k}$

$\beta^{-1} = \alpha^{-t}$

$$y - t = y_1 \log_\alpha p_1 + \cdots + y_k \log_\alpha p_k$$

t — nasze obliczyć

RSA (Rivest, Shamir, Adleman) 1976

Alicja ma klucz jawny:

$n = p \cdot q = (2p'+1)(2q'+1)$, $e \perp 2p'q'$

i klucz tajny d : $de \equiv 1$

$2p'q' = NWD(p-1, q-1)$

Bob szyfruje m : $c = m^e \bmod n$

Alicja deszyfruje c : $c^d \equiv m^{ed} \equiv$

$m^{\triangle NWD(p-1, q-1)+1} \equiv m$

Bezpieczeństwo RSA opiera się na założeniu RSA, że dla danego c trudno jest policzyć m takie że

$$m^e = c$$

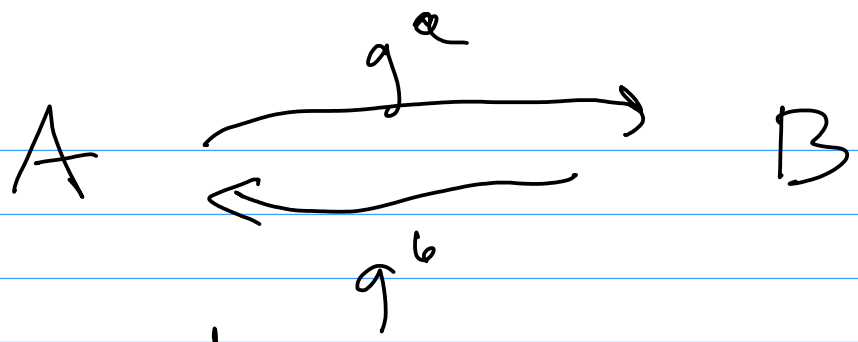
Uzgadnianie klucza - algorytm Diffiego - Hellmana

Na początku A i B uzgadniają p

$g \in Z_p^*$

A losuje a

B losuje b



$$K = g^{ab} = (g^b)^a = (g^a)^b$$

Obserwacja

p g g^a g^b i nie $\underline{\text{cyfrowy}}$ g^{ab}

Dane

Problem Diffiego - Hellmana.

Szyfrowanie Elgamala

Alicja ma klucz jawny $p, g, y = g^x$ klucz tajny jest x

Szyfrowanie m przez Boba:

Bob losuje r, $c = (g^r, y^r m)$

Alicja deszyfruje

$y^r = (g^r)^x = (g^x)^r$ $\quad m = y^r m / y^r$

Obserwacja p, g, g^x, g^r i nie wyliczyć g^{xr}