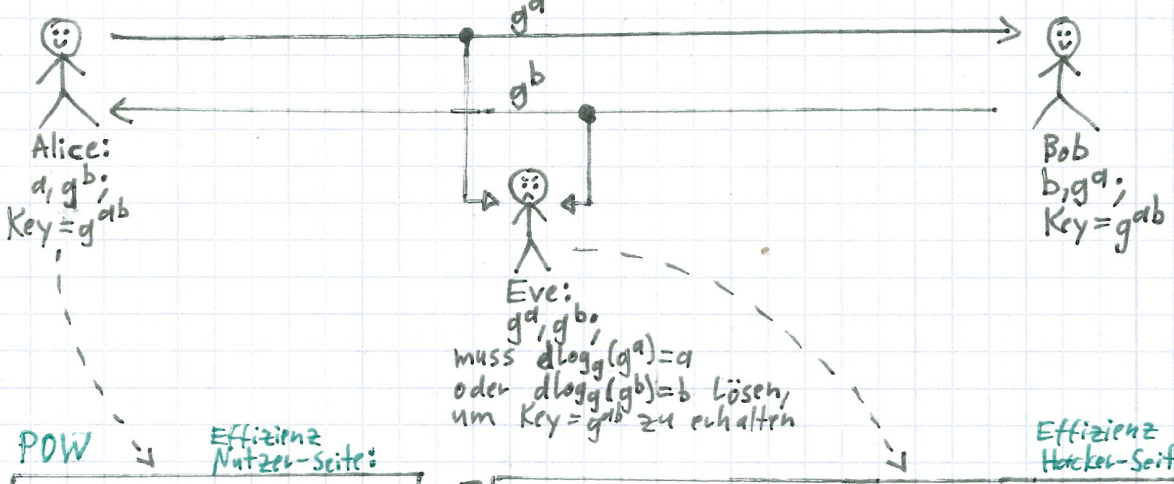
Eigenes „Gesamtbild" CRYPTO 1 – Diskr. Log. (I) + (II)

1.5.22, 5.5.22 & 7.5.22 & 15/16.5.22

Diffie-Hellman-Schlüsselaustausch zw. Alice & Bob:



POW — Effizienz Nutzer-Seite:

Wie berechnet Alice g^a und $(g^b)^a$ effizient?:

Square and Multiply:

$g^1 \xrightarrow{\wedge 2} g^{10} \xrightarrow{\wedge 2} g^{100} \rightarrow \dots$

z.B. $g^{18} = g^{10010} = g^{10000} \cdot g^{10}$

Register 1	Register 2
1	$\wedge 2 \; \wedge 2 \; \wedge \dots$
x	wenn ne 1

$\Rightarrow O(\log(g^a))$ Platz$^{(?)}$
$\Rightarrow O(\log(a))$ Zeit

(VL Diskr. Log II): ⇒ weiterhin: „knacke" dlog

1b.) Indexkalkül/Index Calculus [1.] Wähle ein B.

[2.] Bestimme Zahlen $f_1, \dots, f_t$ sodass
g^{f_i} B-glatt (d.h. alle Primteiler $\leq B$),
Faktorbasis $f_b = \{p_1, \dots, p_t\} = \{p \mid p \in \mathbb{P}, p \leq B\}$.
$g^{f_i} = p_1^{e_{i1}} \cdot \dots \cdot p_t^{e_{it}}$
$\Rightarrow f_i = e_1 \cdot dlog_g(p_1) + \dots + e_t \cdot dlog_g(p_t)$
→ LGS mit r Glgen & t Unbestimmten
→ Lösg. liefert $dlog_g(p_i)$, $1 \leq i \leq t$.
→ LGS ist mod $p-1$: $\frac{p-1}{2} \in \mathbb{P}$, sonst eher Silver.-P.-H.

[3.] Suche ein f, sodass $h \cdot g^f$ B-glatt:
$h \cdot g^f = p_1^{e_1} \cdot \dots \cdot p_t^{e_t} \Rightarrow dlog_g(h) + f = e_1 \cdot dlog_g(p_1) + \dots$
$\Rightarrow dlog_g(h) = -f + \sum_{i=1}^{t} e_i \cdot dlog_g(p_i)$ ■

↳ ⊕ schneller ⊖ Eb finden nur für $\mathbb{Z}_p^*$ mach bar, n. E.ll.K.

(VL Diskr. Log. II):
Spare Platz bei Pollard-ρ mit „Floyd's Trick" (dafür etwas mehr Zeit nötig):
$x_0 = y_0 = g^{a_0} \cdot h^{b_0}$; merke x_i, y_i und ihre Darstellg.
$x_i = f(x_{i-1})$; $y_i = f(f(y_{i-1}))$
Sobald $x_k = y_k \Leftrightarrow g^{a_k} \cdot h^{b_k} = g^{\alpha_k} \cdot h^{\beta_k}$
$\Rightarrow g^{a_k - \alpha_k} = h^{\beta_k - b_k} = (g^x)^{\beta_k - b_k}$
$\Rightarrow x = \frac{a_k - \alpha_k}{\beta_k - b_k}$ ■ Eine Kollision existiert bei $y_i = x_{2i} \Leftrightarrow i \equiv 2i \Leftrightarrow i \equiv 0 \pmod{T}$

!

Effizienz Hacker-Seite: DLP

Wie berechnet Eve $x = dlog_g(g^x)$, gegeben $h = g^x$, effizient?:

1.) Silver-Pohlig-Hellman-Reduktion: $G = \{g^0, \dots, g^{n-1}\}$ zyklisch.

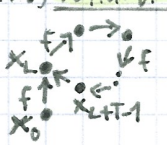
[1] $ord(G) = a \cdot b$ mit $ggT(a,b) = 1$
und DLP ist „leicht" in Ordnung a und b:
- Finde „leicht" x_a, x_b: $(g^b)^{x_a} = h^b$ (Ord. a), $(g^a)^{x_b} = h^a$ (Ord. b)
- Finde mit Euklid u, v: $ua + vb = ggT(a,b) = 1$
- Ergebnis: $x = u \cdot a \cdot x_b + v \cdot b \cdot x_a$
- Beweis: $g^x = (g^{ax_b})^u \cdot (g^{bx_a})^v = h^{au+bv} = h$ ■

[2] $ord(G) = p^e$ mit $p \in \mathbb{P}$ und $e > 1$
und DLP ist „leicht" in Ordnung p:
Idee: Reduziere rekursiv von Ord. p^e auf p^{e-1}:
- $h = g^x$
- $h = g^{x_0 + x_1 p + x_2 p^2 + \dots}$
- $h^{p^{e-1}} = (g^{x_0 + x_1 p + \dots})^{p^{e-1}}$ (schreibe x zur Basis p)
- $h^{p^{e-1}} = (g^{p^{e-1} x_0}) \cdot g^{p^{e-1} \cdot p \cdot (x_1 + x_2 p + \dots)}$
- $h^{p^{e-1}} = (g^{p^{e-1} x_0}) \cdot 1$ (da Ordnung p^e)
- $ord(\langle g^{p^{e-1}} \rangle) = p$, also x_0 „leicht" bestimmbar
- Neues Problem: $h = g^{x_0} \cdot (g^p)^{x_1 + x_2 p + \dots}$
  $h \cdot g^{-x_0} = (g^p)^{x_1 + x_2 p + \dots}$
  → DLP in $\langle g^p \rangle$ der Ordnung p^{e-1} ■

⇒ Bleibt das DLP in ($\mathbb{Z}$ykl.) Gruppen mit Primzahlordnung:

2a.) Babystep-Giantstep-Algo/Shanks' Algo: (beliebige zykl. Grp.)
($|G| > 1 = n$)
Giant Steps: $g^0, g^N, g^{2N}, \dots, g^{(N-1)N}$ $(N = \lceil \sqrt{n} \rceil)$
Baby Steps: $h, hg, hg^2, \dots$
Irgendwann muss Kollision: $g^{uN} = hg^{-v}$
$\Rightarrow x = dlog_g(h) = uN + v$ ■

2b.) Pollard-ρ („Rho"):



$f(x) = \begin{cases} xh, & x \in G_1 \\ x^2, & x \in G_2 \\ xg, & x \in G_3 \end{cases} \Rightarrow x_i = g^{u_i} \cdot h^{v_i}$

$x_L = x_{L+T} \Rightarrow g^{u_L} \cdot h^{v_L} = g^{u_{L+T}} \cdot h^{v_{L+T}}$
$\Rightarrow g^{u_L - u_{L+T}} = h^{v_{L+T} - v_L} = (g^x)^{v_{L+T} - v_L} \Rightarrow x = \frac{u_L - u_{L+T}}{v_{L+T} - v_L}$ ■

⇒ Beide basieren auf dem Geburtstagsparadoxon ($\sqrt{|G|}$) und sind besser als naives Brute-Force, aber dennoch für große Gruppen n. durchf.bar!