Alternative using discrete logarithms

October 14, 2021 12:17 PM

In Ben-Or Tiwari we need $p > m_i \le p_n^{d}$. $\boxed{29^{100}}$

Pick $p = q_1 q_2 \cdots q_n + 1$ where $q_i > d_i = \deg(f, x_i)$ and $\gcd(q_i, q_j) = 1$.

$\Rightarrow p \geq \prod (d_i + 1)$.

E.g. $n=5$, $d_i = \underline{30}$ $\quad p = 31 \cdot 33 \cdot 35 \cdot 37 \cdot 38 + 1$

$n = 10$, $d_i = 100$ $\quad p = 101 \cdot 103 \cdot 105 \cdot 107 \cdot 109 \cdot 113 \cdot 121 \cdot 131 \cdot 137 \cdot 104 + 1 = 3.25 \cdot 10^{20}$.

Find α a generator of $\mathbb{Z}_p^*$. (easy $p-1 = \prod q_i$) [easy]

Let $\omega_k = \boxed{\alpha^{(p-1)/q_k}}$ so $\text{order}(\omega_k) = q_k$.

Evaluate $v_j = f(\omega_1^j, \omega_2^j, \ldots, \omega_n^j)$ for $0 \le j \le 2T-1$ in $\mathbb{Z}_p$.

Compute $\lambda(z)$ and m_i the roots of $\lambda(z) \in \mathbb{Z}_p[z]$.

If $M_i = x_1^{d_1} x_2^{d_2} \cdots x_n^{d_n}$ then $\boxed{m_i = \omega_1^{d_1} \omega_2^{d_2} \cdots \omega_n^{d_n}} \in \mathbb{Z}_p$.

How given m_i do we find $d_1, d_2, \ldots, d_n$?

[Solve $\alpha^x = m_i$ in $\mathbb{Z}_p$ for $0 \le x < p-1$.]

Compute $x = \log_\alpha m_i$ a discrete logarithm using Pohlig-Hellman.

[This is tractable because $p-1$ has small prime factors]

$\Rightarrow x \equiv d_1 \log_\alpha \omega_1 + d_2 \log_\alpha \omega_2 + \cdots + d_n \log_\alpha \omega_n \pmod{p-1}$.

$\Rightarrow x \equiv d_1 \frac{p-1}{q_1} + d_2 \cdot \frac{p-1}{q_2} + \cdots + d_n \cdot \frac{p-1}{q_n}$

mod q_1

$\Rightarrow x \equiv d_1 \cdot \frac{p-1}{q_1} + d_2 \cdot 0 + \cdots + d_n \cdot 0 \mod q_1$

$\Rightarrow d_1 = x \cdot \left(\frac{p-1}{q_1}\right)^{-1} \mod q_1$ ✓ $\gcd(q_i, q_j) = 1$.

I know $M_1 = x_1^{d_1} x_2^{d_2} \cdots x_n^{d_n}$ ✓

Works because $p-1$ has no large prime factors and $m_i \neq m_j$.

Discrete $\log_\alpha x$ in Maple. with(numtheory);
mlog(x, α, p);