DL systems over finite fields IV

Example for index calculus attack

Tanja Lange

Eindhoven University of Technology

2MMC10 – Cryptology

Schoolbook version stage 1

Define factor base $\mathcal{F} = \{p_i | p_i \text{ prime }, p_i < B\}$ for some bound B.
Let $f = |\mathcal{F}|$.

Repeat the following until $f + 4$ relations are collected.

1. Pick random integer j.
2. Compute g^j in $\mathbf{F}_p$. Consider result as integer $b \in [0, p-1]$.
3. Check whether b factors over the factor base, i.e. whether

$$b = \prod_{i=1}^{f} p_i^{e_i} \text{ for } p_i \in \mathcal{F}, e_i \in \mathbf{N}$$

   If so, $j = \sum e_i \log_g(p_i)$. Store relation $(e_1, e_2, \ldots, e_f, j)$

Put the relations in a matrix. Note, inhomogenous system.
Use linear algebra to compute a solution to the system modulo $\text{ord}(g)$.
Output result $(a_1, a_2, \ldots, a_f)$.

If system under determined, collect more relations.

Example stage 1, part I

Example: $\mathbf{F}_{107}$ with $g = 2, h = 99$.
Define factor base $\mathcal{F} = \{p_i | p_i \text{ prime }, p_i < B\}$ for some bound B.
Let $f = |\mathcal{F}|$.

Repeat the following until $f + 4$ relations are collected.

1. Pick random integer j.
2. Compute g^j in $\mathbf{F}_p$. Consider result as integer $b \in [0, p-1]$.
3. Check whether b factors over the factor base, i.e. whether

$$b = \prod_{i=1}^{f} p_i^{e_i} \text{ for } p_i \in \mathcal{F}, e_i \in \mathbf{N}$$

If so, $j = \sum e_i \log_g(p_i)$. Store relation $(e_1, e_2, \ldots, e_f, j)$

Example stage 1, part I

Example: $\mathbf{F}_{107}$ with $g = 2, h = 99$.
Define factor base $\mathcal{F} = \{p_i | p_i \text{ prime }, p_i < B\}$ for some bound B.
Let $f = |\mathcal{F}|$.
$\mathcal{F} = \{2, 3, 5, 7\}., f = 4$

Repeat the following until $f + 4$ relations are collected.

1. Pick random integer j.
2. Compute g^j in $\mathbf{F}_p$. Consider result as integer $b \in [0, p-1]$.
3. Check whether b factors over the factor base, i.e. whether

$$b = \prod_{i=1}^{f} p_i^{e_i} \text{ for } p_i \in \mathcal{F}, e_i \in \mathbf{N}$$

If so, $j = \sum e_i \log_g(p_i)$. Store relation $(e_1, e_2, \ldots, e_f, j)$

Example stage 1, part I

Example: $\mathbf{F}_{107}$ with $g = 2, h = 99$.
Define factor base $\mathcal{F} = \{p_i | p_i \text{ prime }, p_i < B\}$ for some bound B.
Let $f = |\mathcal{F}|$.
$\mathcal{F} = \{2, 3, 5, 7\}., f = 4$

Repeat the following until $f + 4$ relations are collected.

1. Pick random integer j.
2. Compute g^j in $\mathbf{F}_p$. Consider result as integer $b \in [0, p-1]$.
3. Check whether b factors over the factor base, i.e. whether

$$b = \prod_{i=1}^{f} p_i^{e_i} \text{ for } p_i \in \mathcal{F}, e_i \in \mathbf{N}$$

   If so, $j = \sum e_i \log_g(p_i)$. Store relation $(e_1, e_2, \ldots, e_f, j)$

$g^{23} = 22 = 2 \cdot 11$

Example stage 1, part I

Example: $\mathbf{F}_{107}$ with $g = 2, h = 99$.
Define factor base $\mathcal{F} = \{p_i | p_i \text{ prime }, p_i < B\}$ for some bound B.
Let $f = |\mathcal{F}|$.
$\mathcal{F} = \{2, 3, 5, 7\}., f = 4$

Repeat the following until $f + 4$ relations are collected.

1. Pick random integer j.
2. Compute g^j in $\mathbf{F}_p$. Consider result as integer $b \in [0, p-1]$.
3. Check whether b factors over the factor base, i.e. whether

$$b = \prod_{i=1}^{f} p_i^{e_i} \text{ for } p_i \in \mathcal{F}, e_i \in \mathbf{N}$$

If so, $j = \sum e_i \log_g(p_i)$. Store relation $(e_1, e_2, \ldots, e_f, j)$

$g^{23} = 22 = 2 \cdot 11$ not $\mathcal{F}$-smooth.

Example stage 1, part I

Example: $\mathbf{F}_{107}$ with $g = 2, h = 99$.
Define factor base $\mathcal{F} = \{p_i | p_i \text{ prime }, p_i < B\}$ for some bound B.
Let $f = |\mathcal{F}|$.
$\mathcal{F} = \{2, 3, 5, 7\}., f = 4$

Repeat the following until $f + 4$ relations are collected.

1. Pick random integer j.
2. Compute g^j in $\mathbf{F}_p$. Consider result as integer $b \in [0, p-1]$.
3. Check whether b factors over the factor base, i.e. whether

$$b = \prod_{i=1}^{f} p_i^{e_i} \text{ for } p_i \in \mathcal{F}, e_i \in \mathbf{N}$$

If so, $j = \sum e_i \log_g(p_i)$. Store relation $(e_1, e_2, \ldots, e_f, j)$

$g^{23} = 22 = 2 \cdot 11$ not $\mathcal{F}$-smooth.
$g^{12} = 30 = 2 \cdot 3 \cdot 5$

Example stage 1, part I

Example: $\mathbf{F}_{107}$ with $g = 2, h = 99$.
Define factor base $\mathcal{F} = \{p_i | p_i \text{ prime }, p_i < B\}$ for some bound B.
Let $f = |\mathcal{F}|$.
$\mathcal{F} = \{2, 3, 5, 7\}., f = 4$

Repeat the following until $f + 4$ relations are collected.

1. Pick random integer j.
2. Compute g^j in $\mathbf{F}_p$. Consider result as integer $b \in [0, p-1]$.
3. Check whether b factors over the factor base, i.e. whether

$$b = \prod_{i=1}^{f} p_i^{e_i} \text{ for } p_i \in \mathcal{F}, e_i \in \mathbf{N}$$

If so, $j = \sum e_i \log_g(p_i)$. Store relation $(e_1, e_2, \ldots, e_f, j)$

$g^{23} = 22 = 2 \cdot 11$ not $\mathcal{F}$-smooth.
$g^{12} = 30 = 2 \cdot 3 \cdot 5$ we got a relation. $(1, 1, 1, 0, 12)$

Example stage 1, part I

Example: $\mathbf{F}_{107}$ with $g = 2, h = 99$.
Define factor base $\mathcal{F} = \{p_i | p_i \text{ prime }, p_i < B\}$ for some bound B.
Let $f = |\mathcal{F}|$.
$\mathcal{F} = \{2, 3, 5, 7\}., f = 4$

Repeat the following until $f + 4$ relations are collected.

1. Pick random integer j.
2. Compute g^j in $\mathbf{F}_p$. Consider result as integer $b \in [0, p-1]$.
3. Check whether b factors over the factor base, i.e. whether

$$b = \prod_{i=1}^{f} p_i^{e_i} \text{ for } p_i \in \mathcal{F}, e_i \in \mathbf{N}$$

   If so, $j = \sum e_i \log_g(p_i)$. Store relation $(e_1, e_2, \ldots, e_f, j)$

$g^{23} = 22 = 2 \cdot 11$ not $\mathcal{F}$-smooth.
$g^{12} = 30 = 2 \cdot 3 \cdot 5$ we got a relation. $(1, 1, 1, 0, 12)$
$g^{82} = 90 = 2 \cdot 3'^2 \cdot 5$ another relation. $(1, 2, 1, 0, 82)$

Example stage 1, part I

Example: $\mathbf{F}_{107}$ with $g = 2, h = 99$.
Define factor base $\mathcal{F} = \{p_i | p_i \text{ prime }, p_i < B\}$ for some bound B.
Let $f = |\mathcal{F}|$.
$\mathcal{F} = \{2, 3, 5, 7\}., f = 4$

Repeat the following until $f + 4$ relations are collected.

1. Pick random integer j.
2. Compute g^j in $\mathbf{F}_p$. Consider result as integer $b \in [0, p-1]$.
3. Check whether b factors over the factor base, i.e. whether

$$b = \prod_{i=1}^{f} p_i^{e_i} \text{ for } p_i \in \mathcal{F}, e_i \in \mathbf{N}$$

   If so, $j = \sum e_i \log_g(p_i)$. Store relation $(e_1, e_2, \ldots, e_f, j)$

$g^{23} = 22 = 2 \cdot 11$ not $\mathcal{F}$-smooth.
$g^{12} = 30 = 2 \cdot 3 \cdot 5$ we got a relation. $(1, 1, 1, 0, 12)$
$g^{82} = 90 = 2 \cdot 3'^2 \cdot 5$ another relation. $(1, 2, 1, 0, 82)$
$g^7 = 21 = 3 \cdot 7$

Example stage 1, part I

Example: $\mathbf{F}_{107}$ with $g = 2, h = 99$.
Define factor base $\mathcal{F} = \{p_i | p_i \text{ prime }, p_i < B\}$ for some bound B.
Let $f = |\mathcal{F}|$.
$\mathcal{F} = \{2, 3, 5, 7\}., f = 4$

Repeat the following until $f + 4$ relations are collected.

1. Pick random integer j.
2. Compute g^j in $\mathbf{F}_p$. Consider result as integer $b \in [0, p-1]$.
3. Check whether b factors over the factor base, i.e. whether

$$b = \prod_{i=1}^{f} p_i^{e_i} \text{ for } p_i \in \mathcal{F}, e_i \in \mathbf{N}$$

If so, $j = \sum e_i \log_g(p_i)$. Store relation $(e_1, e_2, \ldots, e_f, j)$

$g^{23} = 22 = 2 \cdot 11$ not $\mathcal{F}$-smooth.
$g^{12} = 30 = 2 \cdot 3 \cdot 5$ we got a relation. $(1, 1, 1, 0, 12)$
$g^{82} = 90 = 2 \cdot 3'^2 \cdot 5$ another relation. $(1, 2, 1, 0, 82)$
$g^{7} = 21 = 3 \cdot 7$ we got a relation. $(0, 1, 0, 1, 7)$

Example stage 1, part I

Example: $\mathbf{F}_{107}$ with $g = 2, h = 99$.
Define factor base $\mathcal{F} = \{p_i | p_i \text{ prime }, p_i < B\}$ for some bound B.
Let $f = |\mathcal{F}|$.
$\mathcal{F} = \{2, 3, 5, 7\}., f = 4$

Repeat the following until $f + 4$ relations are collected.

1. Pick random integer j.
2. Compute g^j in $\mathbf{F}_p$. Consider result as integer $b \in [0, p-1]$.
3. Check whether b factors over the factor base, i.e. whether

$$b = \prod_{i=1}^{f} p_i^{e_i} \text{ for } p_i \in \mathcal{F}, e_i \in \mathbf{N}$$

If so, $j = \sum e_i \log_g(p_i)$. Store relation $(e_1, e_2, \ldots, e_f, j)$

$g^{23} = 22 = 2 \cdot 11$ not $\mathcal{F}$-smooth.
$g^{12} = 30 = 2 \cdot 3 \cdot 5$ we got a relation. $(1, 1, 1, 0, 12)$
$g^{82} = 90 = 2 \cdot 3'^2 \cdot 5$ another relation. $(1, 2, 1, 0, 82)$
$g^7 = 21 = 3 \cdot 7$ we got a relation. $(0, 1, 0, 1, 7)$

Let's be optimistic (we also have $g = 2$, so may have enough relations).

Example stage 1, part II

Relations:
$(1, 0, 0, 0, 1)$ from $g^1 = 2$
$(1, 1, 1, 0, 12)$ from $g^{12} = 30 = 2 \cdot 3 \cdot 5$
$(1, 2, 1, 0, 82)$ from $g^{82} = 90 = 2 \cdot 3'^2 \cdot 5$
$(0, 1, 0, 1, 7)$ from $g^7 = 21 = 3 \cdot 7$

Put the relations in a matrix. Note, inhomogenous system.
Use linear algebra to compute a solution to the system modulo $\mathrm{ord}(g)$.
Output result $(a_1, a_2, \ldots, a_f)$.

Example stage 1, part II

Relations:
$(1, 0, 0, 0, 1)$ from $g^1 = 2$
$(1, 1, 1, 0, 12)$ from $g^{12} = 30 = 2 \cdot 3 \cdot 5$
$(1, 2, 1, 0, 82)$ from $g^{82} = 90 = 2 \cdot 3'^2 \cdot 5$
$(0, 1, 0, 1, 7)$ from $g^7 = 21 = 3 \cdot 7$

Put the relations in a matrix. Note, inhomogenous system.
Use linear algebra to compute a solution to the system modulo $\mathrm{ord}(g)$.
Output result $(a_1, a_2, \ldots, a_f)$.

$$\left(\begin{array}{cccc|r} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 12 \\ 1 & 2 & 1 & 0 & 82 \\ 0 & 1 & 0 & 1 & 7 \end{array}\right)$$

Example stage 1, part II

Relations:
$(1,0,0,0,1)$ from $g^1 = 2$
$(1,1,1,0,12)$ from $g^{12} = 30 = 2 \cdot 3 \cdot 5$
$(1,2,1,0,82)$ from $g^{82} = 90 = 2 \cdot 3'^2 \cdot 5$
$(0,1,0,1,7)$ from $g^7 = 21 = 3 \cdot 7$

Put the relations in a matrix. Note, inhomogenous system.
Use linear algebra to compute a solution to the system modulo $\mathrm{ord}(g)$.
Output result $(a_1, a_2, \ldots, a_f)$.

$$\left(\begin{array}{cccc|r} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 12 \\ 1 & 2 & 1 & 0 & 82 \\ 0 & 1 & 0 & 1 & 7 \end{array}\right) \sim \left(\begin{array}{cccc|r} 1 & 0 & 0 & 0 & 1 \\ & & & & \\ & & & & \\ & & & & \end{array}\right)$$

Example stage 1, part II

Relations:
$(1, 0, 0, 0, 1)$ from $g^1 = 2$
$(1, 1, 1, 0, 12)$ from $g^{12} = 30 = 2 \cdot 3 \cdot 5$
$(1, 2, 1, 0, 82)$ from $g^{82} = 90 = 2 \cdot 3'^2 \cdot 5$
$(0, 1, 0, 1, 7)$ from $g^7 = 21 = 3 \cdot 7$

Put the relations in a matrix. Note, inhomogenous system.
Use linear algebra to compute a solution to the system modulo $\mathrm{ord}(g)$.
Output result $(a_1, a_2, \ldots, a_f)$.

$$\left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 12 \\ 1 & 2 & 1 & 0 & 82 \\ 0 & 1 & 0 & 1 & 7 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 70 \\ & & & & \\ & & & & \end{array}\right)$$

Example stage 1, part II

Relations:
$(1, 0, 0, 0, 1)$ from $g^1 = 2$
$(1, 1, 1, 0, 12)$ from $g^{12} = 30 = 2 \cdot 3 \cdot 5$
$(1, 2, 1, 0, 82)$ from $g^{82} = 90 = 2 \cdot 3'^2 \cdot 5$
$(0, 1, 0, 1, 7)$ from $g^7 = 21 = 3 \cdot 7$

Put the relations in a matrix. Note, inhomogenous system.
Use linear algebra to compute a solution to the system modulo $\mathrm{ord}(g)$.
Output result $(a_1, a_2, \ldots, a_f)$.

$$\left(\begin{array}{cccc|r} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 12 \\ 1 & 2 & 1 & 0 & 82 \\ 0 & 1 & 0 & 1 & 7 \end{array}\right) \sim \left(\begin{array}{cccc|r} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 70 \\ 0 & 0 & 1 & 0 & 47 \\ & & & & \end{array}\right)$$

Example stage 1, part II

Relations:
$(1, 0, 0, 0, 1)$ from $g^1 = 2$
$(1, 1, 1, 0, 12)$ from $g^{12} = 30 = 2 \cdot 3 \cdot 5$
$(1, 2, 1, 0, 82)$ from $g^{82} = 90 = 2 \cdot 3'^2 \cdot 5$
$(0, 1, 0, 1, 7)$ from $g^7 = 21 = 3 \cdot 7$

Put the relations in a matrix. Note, inhomogenous system.
Use linear algebra to compute a solution to the system modulo $\mathrm{ord}(g)$.
Output result $(a_1, a_2, \ldots, a_f)$.

$$\left(\begin{array}{cccc|r} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 12 \\ 1 & 2 & 1 & 0 & 82 \\ 0 & 1 & 0 & 1 & 7 \end{array}\right) \sim \left(\begin{array}{cccc|r} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 70 \\ 0 & 0 & 1 & 0 & 47 \\ 0 & 0 & 0 & 1 & 43 \end{array}\right)$$

Example stage 1, part II

Relations:
$(1,0,0,0,1)$ from $g^1 = 2$
$(1,1,1,0,12)$ from $g^{12} = 30 = 2 \cdot 3 \cdot 5$
$(1,2,1,0,82)$ from $g^{82} = 90 = 2 \cdot 3'^2 \cdot 5$
$(0,1,0,1,7)$ from $g^7 = 21 = 3 \cdot 7$

Put the relations in a matrix. Note, inhomogenous system.
Use linear algebra to compute a solution to the system modulo $\mathrm{ord}(g)$.
Output result $(a_1, a_2, \ldots, a_f)$.

$$\left(\begin{array}{cccc|r} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 12 \\ 1 & 2 & 1 & 0 & 82 \\ 0 & 1 & 0 & 1 & 7 \end{array}\right) \sim \left(\begin{array}{cccc|r} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 70 \\ 0 & 0 & 1 & 0 & 47 \\ 0 & 0 & 0 & 1 & 43 \end{array}\right)$$

Note: Computations are modulo $p - 1 = 106$

Example stage 1, part II

Relations:
$(1, 0, 0, 0, 1)$ from $g^1 = 2$
$(1, 1, 1, 0, 12)$ from $g^{12} = 30 = 2 \cdot 3 \cdot 5$
$(1, 2, 1, 0, 82)$ from $g^{82} = 90 = 2 \cdot 3'^2 \cdot 5$
$(0, 1, 0, 1, 7)$ from $g^7 = 21 = 3 \cdot 7$

Put the relations in a matrix. Note, inhomogenous system.
Use linear algebra to compute a solution to the system modulo $\mathrm{ord}(g)$.
Output result $(a_1, a_2, \ldots, a_f)$.

$$\left(\begin{array}{cccc|r} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 12 \\ 1 & 2 & 1 & 0 & 82 \\ 0 & 1 & 0 & 1 & 7 \end{array}\right) \sim \left(\begin{array}{cccc|r} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 70 \\ 0 & 0 & 1 & 0 & 47 \\ 0 & 0 & 0 & 1 & 43 \end{array}\right)$$

Note: Computations are modulo $p - 1 = 106$ which is not prime.
Here everything worked, else could have computed modulo 53, gotten $\bar{a}_i$, and then for each $1 \leq i \leq f$ checked whether $a_i = \bar{a}_i$ or $a_i = \bar{a}_i + 53$ is correct.

Example stage 1, part II

Relations:
$(1, 0, 0, 0, 1)$ from $g^1 = 2$
$(1, 1, 1, 0, 12)$ from $g^{12} = 30 = 2 \cdot 3 \cdot 5$
$(1, 2, 1, 0, 82)$ from $g^{82} = 90 = 2 \cdot 3'^2 \cdot 5$
$(0, 1, 0, 1, 7)$ from $g^7 = 21 = 3 \cdot 7$

Put the relations in a matrix. Note, inhomogenous system.
Use linear algebra to compute a solution to the system modulo $\mathrm{ord}(g)$.
Output result $(a_1, a_2, \ldots, a_f)$.

$$\left(\begin{array}{cccc|r} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 12 \\ 1 & 2 & 1 & 0 & 82 \\ 0 & 1 & 0 & 1 & 7 \end{array}\right) \sim \left(\begin{array}{cccc|r} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 70 \\ 0 & 0 & 1 & 0 & 47 \\ 0 & 0 & 0 & 1 & 43 \end{array}\right)$$

Note: Computations are modulo $p - 1 = 106$ which is not prime.
Here everything worked, else could have computed modulo 53, gotten $\bar{a}_i$, and then for each $1 \leq i \leq f$ checked whether $a_i = \bar{a}_i$ or $a_i = \bar{a}_i + 53$ is correct. In general work modulo largest divisor of $p - 1$ for which matrix is invertible, then search residue class of $\bar{a}_i$.

Schoolbook version stage 2

This part uses the target h.

Repeat the following until successful

1. Pick random integer k.
2. Compute $g^k h$ in $\mathbf{F}_p$. Consider result as integer $b \in [0, p-1]$.
3. Check whether b factors over the factor base, i.e. whether

$$b = \prod_{i=1}^{f} p_i^{e_i} \text{ for } p_i \in \mathcal{F}, e_i \in \mathbf{N}$$

If so, output $-k + \sum e_i a_i$ modulo $\operatorname{ord}(g)$.

- Many optimizations to improve smoothness chance for b in stage 1.
- Make structured choices of j to enable sieving.
- Many optimizations of number-field sieve for factoring carry over. Best index calculus attack for $\mathbf{F}_p$ also called number-field sieve and uses number fields and sieving.
- Asymptotic cost $L^{c+o(1)}$ for constant c where $L = \exp((\ln n)^{1/3}(\ln \ln n)^{2/3})$

Example stage 2

This part uses the target h.

Repeat the following until successful

1. Pick random integer k.
2. Compute $g^k h$ in $\mathbf{F}_p$. Consider result as integer $b \in [0, p-1]$.
3. Check whether b factors over the factor base, i.e. whether

$$b = \prod_{i=1}^{f} p_i^{e_i} \text{ for } p_i \in \mathcal{F}, e_i \in \mathbf{N}$$

   If so, output $-k + \sum e_i a_i$ modulo $\mathrm{ord}(g)$.

Example stage 2

This part uses the target h.

Repeat the following until successful

1. Pick random integer k.
2. Compute $g^k h$ in $\mathbf{F}_p$. Consider result as integer $b \in [0, p-1]$.
3. Check whether b factors over the factor base, i.e. whether

$$b = \prod_{i=1}^{f} p_i^{e_i} \text{ for } p_i \in \mathcal{F}, e_i \in \mathbf{N}$$

If so, output $-k + \sum e_i a_i$ modulo $\operatorname{ord}(g)$.

$h = 99 = 3^2 \cdot 11$,

Example stage 2

This part uses the target h.

Repeat the following until successful

1. Pick random integer k.
2. Compute $g^k h$ in $\mathbf{F}_p$. Consider result as integer $b \in [0, p-1]$.
3. Check whether b factors over the factor base, i.e. whether

$$b = \prod_{i=1}^{f} p_i^{e_i} \text{ for } p_i \in \mathcal{F}, e_i \in \mathbf{N}$$

If so, output $-k + \sum e_i a_i$ modulo $\mathrm{ord}(g)$.

$h = 99 = 3^2 \cdot 11$, this is not $\mathcal{F}$-smooth.

Example stage 2

This part uses the target h.

Repeat the following until successful

1. Pick random integer k.
2. Compute $g^k h$ in $\mathbf{F}_p$. Consider result as integer $b \in [0, p-1]$.
3. Check whether b factors over the factor base, i.e. whether

$$b = \prod_{i=1}^{f} p_i^{e_i} \text{ for } p_i \in \mathcal{F}, e_i \in \mathbf{N}$$

   If so, output $-k + \sum e_i a_i$ modulo $\mathrm{ord}(g)$.

$h = 99 = 3^2 \cdot 11$, this is not $\mathcal{F}$-smooth.

Try a few more powers of g, eventually find

Example stage 2

This part uses the target h.

Repeat the following until successful

1. Pick random integer k.
2. Compute $g^k h$ in $\mathbf{F}_p$. Consider result as integer $b \in [0, p-1]$.
3. Check whether b factors over the factor base, i.e. whether

$$b = \prod_{i=1}^{f} p_i^{e_i} \text{ for } p_i \in \mathcal{F}, e_i \in \mathbf{N}$$

If so, output $-k + \sum e_i a_i$ modulo $\mathrm{ord}(g)$.

$h = 99 = 3^2 \cdot 11$, this is not $\mathcal{F}$-smooth.
Try a few more powers of g, eventually find $g^{31} h = 98 = 2 \cdot 7^2$.

Example stage 2

This part uses the target h.

Repeat the following until successful

1. Pick random integer k.
2. Compute $g^k h$ in $\mathbf{F}_p$. Consider result as integer $b \in [0, p-1]$.
3. Check whether b factors over the factor base, i.e. whether

$$b = \prod_{i=1}^{f} p_i^{e_i} \text{ for } p_i \in \mathcal{F}, e_i \in \mathbf{N}$$

   If so, output $-k + \sum e_i a_i$ modulo $\text{ord}(g)$.

$h = 99 = 3^2 \cdot 11$, this is not $\mathcal{F}$-smooth.
Try a few more powers of g, eventually find $g^{31} h = 98 = 2 \cdot 7^2$.

$a \equiv 1 + 2 \cdot 43 - 31 \equiv 56 \bmod 106$.

Example stage 2

This part uses the target h.

Repeat the following until successful

1. Pick random integer k.
2. Compute $g^k h$ in $\mathbf{F}_p$. Consider result as integer $b \in [0, p-1]$.
3. Check whether b factors over the factor base, i.e. whether

$$b = \prod_{i=1}^{f} p_i^{e_i} \text{ for } p_i \in \mathcal{F}, e_i \in \mathbf{N}$$

If so, output $-k + \sum e_i a_i$ modulo $\mathrm{ord}(g)$.

$h = 99 = 3^2 \cdot 11$, this is not $\mathcal{F}$-smooth.
Try a few more powers of g, eventually find $g^{31} h = 98 = 2 \cdot 7^2$.

$a \equiv 1 + 2 \cdot 43 - 31 \equiv 56 \bmod 106$.

Always make sure to test: $g^{56} = 99 = h$.