RUHR UNIVERSITÄT BOCHUM RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Ilya Ozerov, Elena Kirshanova

Hausübungen zur Vorlesung

Kryptanalyse

SS 2014

Blatt Solution to the HW10 Ex.2 / 14 July, 2014

Exercise 1 (10 Punkte)**:**
Using the Pohlig-Hellmann method, solve the dlog problem $\beta = \alpha^x \mod p$ for

$$(\alpha, \beta, p) = (2, 39183497, 41022299).$$

Provide all the intermediate steps of the algorithm: show the vector $(a_1, \dots a_k)$ that you use as an input to the CRT to determine x. Also, provide the values for $\alpha_i = \alpha^{\frac{p-1}{p_i^{e_i}}}$ and $\beta_i = \beta^{\frac{p-1}{p_i^{e_i}}}$, where $p - 1 = \prod_i^k p_i^{e_i}$.

Solution

First, we notice that the order of multiplicative group of $\mathbb{F}_p$ factors as

$$N = \#\mathbb{F}_p^* = p - 1 = 41022298 = 2 \cdot 29^5.$$

For each prime factor of the form $q_i^{e_i}$, we compute $\alpha_i = \alpha^{N/q_i^{e_i}} \mod p$ and $\beta_i = \beta^{N/q_i^{e_i}} \mod p$, which gives us elements α_i with prime power order $q_i^{e_i}$. In our case,

$$\alpha_1 = \alpha^{41022298/2} = 41022298 \qquad \beta_1 = \beta^{41022298/2} = 1$$
$$\alpha_2 = \alpha^{41022298/29^5} = 4 \qquad \beta_2 = \beta^{41022298/29^5} = 11844727.$$

Thus, we reduce the dlog problem to computing the dlog in the prime power groups: $\alpha_i^{y_i} = \beta_i$, where each dlog is considered module $q_i^{e_i}$ (the first one $\mod 2$, the second $\mod 29^5$. Obviously, $y_1 = 0$, since we've obtained $\beta_1 = 1$. To solve the second dlog $4^{y_2} = 11844727 \mod 29^5$, we simply express y_2 as $y_2 = y_{2,0} + y_{2,1} \cdot 29 + y_{2,2} \cdot 29^2 + y_{2,3} \cdot 29^3 + y_{2,4} \cdot 29^4$ and try to determine all $y_{2,i}$ successively solving the dlog in the group of order 29 for instances:

$$(\alpha^{29^4})^{y_{2,i}} = (\beta + \alpha^{-y_{0,1} - \dots - y_{0,i} \cdot 29^{i-1}})^{29^{4-i}}.$$

In out example, $y_2 = 7 + 8 \cdot 29 + 26 \cdot 29^2 + 18 \cdot 29^3 18 \cdot 29^4 = 13192165 \mod p$.
to reconstruct the original dlog, we use CRT and solve for x

$$x = 0 \mod 2,$$
$$x = 13192165 \mod 29^5,$$

from where we obtain $x = 33703314 \mod N$ and check that this is indeed the answer.