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 HW9 Ex.1 / 7 July, 2014

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

$$(\alpha, \beta, p) = (204667, 733106, 759377).$$

Solution
We use the following factor-base of B-smooth numbers for $B = 180$:
$B = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 1531\}$.
We set $k = \#B = 43$. Notice, that we also add the prime-factorization of $p-1 = 2^4 \cdot 31 \cdot 1531$ (that is why 1531 appears in the set B). Next, according to the index-calculus algorithm we look through the factorizations of α^r for random $r \in_R (0 \dots p-1)$ and hope to find enough B-smooth numbers among them. Once we find one $\alpha^r = \prod_{i=1}^{k} p_i^{e_i}$, we save an exponent vector $e = (e_1, \dots, e_k)$ and a corresponding number r into a k-dimensional vector R. In our case we need to find k linearly-independent over $\mathbb{Z}_{p-1}$ such exponent vectors. We write all these vectors we have found as the rows of the matrix E (note this matrix has rank k). The matrix is provided in a separate file. Our vector R is of the form

$R =$ [28028 596142 525101 177759 81579 538277 446427 636024 242588 361251 441382 590243 212201 16115 696587 469560 162467 597516 230367 464941 110241 135946 253378 146825 81947 164283 202601 2237 404440 18553 560826 57506 739513 469177 710083 101014 699227 453986 93946 498781 131302 589082 661362].

We find x_1, x_2, x_3, s.t. $E \cdot x_1 = R \mod 2^4, E \cdot x_2 = R \mod 31, E \cdot x_3 = R \mod 1531$. Using Chinese-Remainder Theorem, we reconstruct x and solve the equation $E \cdot X = R \mod (p-1)$. The entries of the output vector X are the discrete logarithms of our factor-base elements: $X = (\mathrm{dlog}_\alpha(2), \mathrm{dlog}_\alpha(3), \dots, \mathrm{dlog}_\alpha(1531))$, and is of the form:

$X =$ [34634 273553 264937 303889 714726 401525 475022 637226 311610 658013 602114 535824 281666 730904 285321 669498 220833 698802 30709 619396 528881 65637 510770 82137 681624 392823 449748 653086 549460 563903 222806 300014 464108 15352 554740 614979 587415 720519 175708 372519 354998 206876 398414].

Finally, we look for a random r_0 s.t. $\beta \cdot \alpha^{r_0}$ is B-smooth and, since we know all the dlogs of our B-smooth number $(\mathrm{dlog}_\alpha(p_i))$, we can compute $\mathrm{dlog}_\alpha(\beta) = -r_0 + \sum_{i=1}^{k} e_i \cdot \mathrm{dlog}_\alpha(p_i) \mod (p-1)$. We find $r_0 = 363394$ with $\beta \cdot \alpha^r = 2^5 \cdot 169$, from where

$$\mathrm{dlog}_{204667}(733106) = 836.$$