Cryptography, exercise sheet 3 for 21 Sep 2021

We will work through these exercises on wonder.me; you can find the URL for the room in the Canvas announcement and in Zulip chat under the topic "Wonder session" in the "general" stream. These are exercises to challenge your understanding of the lectures you have watched already, namely lectures I – IX about ECC and lectures I – VII about DLP. These are not for homework.

You can call one of us over by choosing "invite to circle". Please note, though, that if we are in another circle busy talking we will not come right away and invitations expire quickly. So pick one of us who is in the TA corner, thus not occupied.

1. The elliptic curve
$$y^2 = x^3 + x + 3 \text{ over } \mathbb{F}_{43}$$
has 47 points. The point $P = (19, 42)$ has order 47. The point $Q = (28, 15)$ is a multiple of P. Use the BSGS method to compute the discrete logarithm $a = \log_P(Q)$ of Q with base P.
Verify your result.

2. Discuss how you can document the work you did in exercise 1 so that one can grade it. Also remember to check that you verified your result. This is also important for the grading (and for you to get confirmation).

3. Show the steps to compute $5P + 7Q$ using double-scalar multiplication. How many additions and doublings do you need?

4. Use the schoolbook version of Pollard rho and Floyd's cycle-finding algorithm to solve the DLP from exercise 1 using starting point $S_0 = F_0 = W_0 = 5Q$ and the step function from dlp-4.pdf, last page.
Note, the slides have been updated to fix a typo on that slide (W is the variable that the first argument gets assigned to.

5. Discuss how you can document the work you did in exercise 4 so that one can grade it.

6. This exercise is about the running example in dlp-6.pdf, i.e., $p = 1000003$, $E : y^2 = x^3 - x$ over $\mathbb{F}_p$ with $1000004 = 2^2 \cdot 53^2 \cdot 89$ points. $P = (101384, 614510)$ is a point of order $2 \cdot 53^2 \cdot 89$ and $Q = aP = (670366, 740819)$? is the target.

   In this exercise you will compute a_1, a_2, a_3, a_4 and solve the DLP.

   (a) Compute $a_2 \equiv a \bmod 2$ by solving the DLP in the order-2 subgroup.

   (b) Use the BSGS algorithm to solve the 2 DLPs in the order-53 subgroup to get a_2 and a_3. Make sure to update Q before solving the second one – and do not overwrite your original Q.

   (c) Solve the DLP in the size-89 subgroup. Feel free to use a for loop in Sage to solve this

   (d) Use the Chinese remainder theorem to compute a. Test your solution.

7. Let point P have order 411672 and point Q be a multiple of P. Explain how to compute the DLP of Q base P using the Pohlig-Hellman attack and estimate the number of steps needed.

8. Test your understanding of the Pohlig–Hellman method by explaining it to a fellow student or one of the TAs.