Introduction to Cryptography: Homework 13

December 16, 2021

Requirements about the delivery of this assignment:

- Submit a pdf-document via Brightspace;
- Make sure that you write both name and student number on all documents (not only in the file name).

Deadline: Monday, January 3, 17:00 sharp!

Grading: You can score a total of 100 points for the hand-in assignment. To get full points, please **explain all answers clearly**.

Exercises:

1. **Brightspace quiz.** Make the Brightspace quiz called "Terminology and definitions II". Go to activities -> Quizzes. [You can attempt the quiz as often as you would like/need.]

2. **Finding discrete logarithms.** The generic algorithms that can be used to solve the (elliptic-curve) discrete logarithm problem can also be applied to multiplicative groups. Since it is computationally less work and simpler to compute in modular groups, we let you solve the discrete log problem in modular groups rather than in elliptic-curve groups. Consider the group $((\mathbb{Z}/179\mathbb{Z})^*, \times)$ and its subgroup $\langle 3 \rangle$ of prime order 89.

   (a) Use the baby-step giant-step method to find x such that $3^x \equiv 89 \pmod{179}$. Pick $m = \lfloor \sqrt{89} \rfloor$ (see also Algorithm 7 and Example 14.2.2 in the lecture notes for inspiration). Copy, extend and fill the appropriate tables below in your answer.

   (b) Use Pollard's ρ algorithm to find x such that $3^x \equiv 89 \pmod{179}$. Make sure that you write down all intermediate steps, and not just the answer. Use the function

$$(a_{i+1}, b_{i+1}, c_{i+1}) = \begin{cases} (a_i \cdot g, b_i + 1, c_i) & \text{if } a_i \equiv 1 \pmod 3; \\ (a_i \cdot h, b_i, c_i + 1) & \text{if } a_i \equiv 2 \pmod 3; \\ (a_i^2, 2b_i, 2c_i) & \text{if } a_i \equiv 0 \pmod 3. \end{cases}$$

   and pick starting point $(3, 1, 0)$. (The function is not exactly the same as in Subsection 14.2.2 of the lecture notes, but the method works the same.) [Hint: It should take you less than fifteen steps to find the solution.]

i	0
3^i	

Table 1: Baby steps.

j	0
$89 \cdot 3^{-mj}$	

Table 2: Giant steps.

i	0
a_i	3
b_i	1
c_i	0

Table 3: Pollard's ρ algorithm.

Hand in assignments

1. **100 points) Finding discrete logarithms.** The generic algorithms that can be used to solve the (elliptic-curve) discrete logarithm problem can also be applied to multiplicative groups. Since it is computationally less work and simpler to compute in modular groups, we let you solve the discrete log problem in modular groups rather than in elliptic-curve groups. Consider the group $((\mathbb{Z}/179\mathbb{Z})^*, \times)$ and its subgroup $\langle 5 \rangle$ of prime order 89.

   (a) Use the baby-step giant-step method to find x such that $5^x \equiv 107 \pmod{179}$. Pick $m = \lfloor \sqrt{89} \rfloor$ (see also Algorithm 7 and Example 14.2.2 in the lecture notes for inspiration). Copy, extend and fill the appropriate tables below in your answer. 50 pt

   (b) Use Pollard's ρ algorithm to find x such that $5^x \equiv 107 \pmod{179}$. Make sure that you write down all intermediate steps, and not just the answer. Use the function 50 pt

$$(a_{i+1}, b_{i+1}, c_{i+1}) = \begin{cases} (a_i \cdot g, b_i + 1, c_i) & \text{if } a_i \equiv 1 \pmod 3; \\ (a_i \cdot h, b_i, c_i + 1) & \text{if } a_i \equiv 2 \pmod 3; \\ (a_i^2, 2b_i, 2c_i) & \text{if } a_i \equiv 0 \pmod 3. \end{cases}$$

   and pick starting point $(5, 1, 0)$. (The function is not exactly the same as in Subsection 14.2.2 of the lecture notes, but the method works the same.) [Hint: It should take you less than fifteen steps to find the solution.]

i	0
5^i	

Table 4: Baby steps.

j	0
$107 \cdot 5^{-mj}$	

Table 5: Giant steps.

i	0
a_i	3
b_i	1
c_i	0

Table 6: Pollard's ρ algorithm.