# Introduction to Cryptography: Homework 8

**November 17, 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, November 29, 17:00 sharp!

**Grading:** You can score a total of 100 points for the hand-in assignments. To get full points, please **explain all answers clearly and verify computations, e.g., concerning inverses**.

## Exercises:

1. **Brightspace quiz.** Make the Brightspace quiz on groups, "Practicing with groups". Go to Activities -> Quizzes. [You can attempt the quiz as often as you would like/need.]
2. **Subgroups.** Consider the group $(\mathbb{Z}/37\mathbb{Z})^*$.
   (a) Compute $\#(\mathbb{Z}/37\mathbb{Z})^*$.
   (b) Let $A = \{0, 1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36\}$. Is $A$ a subgroup of $(\mathbb{Z}/37\mathbb{Z})^*$?
   (c) Let $B = \{1, 5, 14, 17, 25\}$. Is $B$ a subgroup of $(\mathbb{Z}/37\mathbb{Z})^*$?
   (d) Let $C = \{10, 11, 27, 36\}$. Is $C$ a subgroup of $(\mathbb{Z}/37\mathbb{Z})^*$?
   (e) Let $D = \{1, 7, 9, 10, 12, 16, 26, 33, 34\}$. Is $D$ a subgroup of $(\mathbb{Z}/37\mathbb{Z})^*$?
   (f) Consider the prime-order subgroups of $(\mathbb{Z}/37\mathbb{Z})^*$. What possible orders do they have?
3. **Euclidean algorithm.**
   (a) Compute $\gcd(5, 23)$ using the Euclidean algorithm.
   (b) Compute integers $x, y$ such that $5x + 23y = \gcd(5, 23)$.
   (c) Take the equation from (b) and take both sides modulo 23. What remains?
   (d) What can you say about the multiplicative inverse of 5 modulo 23?
   (e) Solve the equation $5z + 3 \equiv 17 \pmod{23}$ for $z$.
   (f) Compute integers $a, b$ such that $5a + 23b = 17$.
4. **Modular inverses.** We consider the group $(\mathbb{Z}/31\mathbb{Z})^*$.
   (a) What is the inverse of 2 modulo 31? Verify your answer.
   (b) Compute the inverse of 13 modulo 31 using Fermat's Little Theorem and Square-and-Multiply. Verify your answer.
   (c) What is the inverse of 26 modulo 31? Verify your answer. [Use (a) and (b).]

# Hand in assignment:

1. **(60 points) Orders of elements and modular exponentiation.** Consider the integer 1061. Consider the groups $\mathbb{Z}/1061\mathbb{Z} = (\mathbb{Z}/1061\mathbb{Z}, +)$ and $(\mathbb{Z}/1061\mathbb{Z})^* = (\mathbb{Z}/1061\mathbb{Z}) \setminus \{0\}, \times))$.

   (a) Is 1061 a prime number? 2 pt

   (b) Let $a$ be an element in $\mathbb{Z}/1061\mathbb{Z}$. What values can the order of $a$ attain? 6 pt

   (c) Let $g$ be an element in $(\mathbb{Z}/1061\mathbb{Z})^*$. What values can the order of $g$ attain? 20 pt

   (d) What is the multiplicative order of 112 modulo 1061? [Hint: Start small.] 24 pt

   (e) Show how $112^{38481}$ modulo 1061 can be computed very efficiently using (c). 10 pt

2. **(40 points) Modular groups.** Consider the set $\mathbb{Z}/23\mathbb{Z}$. We consider the group $(\mathbb{Z}/23\mathbb{Z} \setminus \{0\}, \times)$.

   (a) List all elements of the cyclic subgroup generated by 6, i.e., $\langle 6 \rangle$. 20 pt

   (b) What is the order of 6 in $((\mathbb{Z}/23\mathbb{Z}) \setminus \{0\}, \times)$? 4 pt

   (c) What is the inverse of 6 in $((\mathbb{Z}/23\mathbb{Z}) \setminus \{0\}, \times)$? 8 pt

   (d) Find the smallest positive $x$ such that $6^x = 3 \pmod{23}$. This $x$ is called the discrete logarithm $\mathrm{dlog}_6(3)$ in $((\mathbb{Z}/23\mathbb{Z}) \setminus \{0\}, \times)$. 8 pt