Exercises I

Note: We discuss solutions to the exercises together in the class on the **18th November 2024**.

Exercise 1. *Finite groups*

1. We consider the group $(G, \cdot, 1)$, where $G = (\mathbb{Z}/21\mathbb{Z})^\times$.
   i. What is the order $\mathsf{ord}(G)$ of the group? List its elements.
   ii. Compute the inverse of 11 in the group.
   iii. Compute (by hand!) 2^{2403} in the group.
   iv. Compute the subgroup $\langle 7 \rangle$ generated by 7.

2. We consider the group $(G, \cdot, 1)$, where $G = (\mathbb{Z}/23\mathbb{Z})^\times$.
   i. What is the order $\mathsf{ord}(G)$ of the group? List its elements.
   ii. Compute the subgroup $\langle 2 \rangle$ generated by 2.
   iii. Compute the subgroup $\langle 5 \rangle$ generated by 5.

Hint: Recall that for any group $(G, \cdot, 1)$, it holds $x^{\mathsf{ord}(G)} = 1$ for every $x \in G$.

Exercise 2. *Non-secure key exchange*

1. We consider the following key-exchange protocol between Alice and Bob.
   1. Alice samples uniformly at random k_A and r from $\{0,1\}^n$. They then send $s = k_A \oplus r$ to Bob.
   2. Bob samples uniformly at random t from $\{0,1\}^n$ and sends $u = s \oplus t$ to Alice.
   3. Alice computes $w = u \oplus r$ and sends w to Bob.
   4. Bob computes $k_B = w \oplus t$.

   i. Show that Alice and Bob share the same key, namely $k_A = k_B$.
   ii. Show that the protocol is not secure against an eavesdropping Eve!

Hint: Look at the set of messages sent between Alice and Bob and show that they contain enough information to compute the key.