Discrete logarithm

(exercises)

Application of discrete models

1. Write a function that calculates the order of a given $\overline{a} \in \mathbb{Z}_p^*$ (where p is a prime number).
2. Calculate the power $\overline{a}^n$ from $\overline{a} \in \mathbb{Z}_p$ and $n \in \mathbb{N}$ using *fast exponentiation.* The function expects three parameters: a, n and p, all integers.
3. Find all generators of $\mathbb{Z}_p^*$ for a given prime number p.
4. Calculate the discrete logarithm of $\overline{a} \in \mathbb{Z}_p^*$ to the base $\overline{g}$, where $\overline{g}$ is a generator of $\mathbb{Z}_p^*$, using a) simple search; b) the baby-step giant-step algorithm.
5. Simulate the Diffie–Hellman key exchange, i.e. write a program that executes both participants' steps, calculates the common secret in both ways, and checks if they match. (The prime number p and the generator $\overline{g} \in \mathbb{Z}_p^*$ are adjustable parameters. Try it with $p = 23$ and $\overline{g} = \overline{5}$.)
6. Break the Diffie–Hellman key exchange (if possible), i.e. write a function that tries to calculate the common secret from the publicly visible data, using discrete logarithm.