Kryptography Sheet 3A

hhu Düsseldorf
Winter term 23/24

Hand in: until monday 06.11.2023, before the lecture starts

Website: `http://reh.math.uni-duesseldorf.de/~khalupczok/krypto/`

Exercise 1: The order of a power in a cyclic group

Let G be a finite cyclic group with generator $a \in G$.

Show that $\operatorname{ord}(a^j) = \dfrac{\operatorname{ord}(a)}{(j, \operatorname{ord}(a))}$ holds for all $j \in \mathbb{Z}$.

Use this to calculate the order of $\underline{5}^{11}$ in the subgroup $H = \langle \underline{5} \rangle$ of the group $G = \mathbb{Z}_{5963}^{\times}$.

Exercise 2: Calculation of $\varphi(N)$ and factorizing N

Let $p \neq q$ be primes and $N = pq$. Show:
The primes p and q are exactly the roots of the quadratic polynomial

$$T^2 - (N + 1 - \varphi(N))T + N.$$

Thus anyone who knows $\varphi(N)$, can factorize N. (In other words: the calculation of $\varphi(N)$ is as difficult as factorizing N.)
Use this to calculate the prime factors of $N = 542029$ with

$$\varphi(N) = 540540.$$

$*$ Do you know a paper-algorithm for taking square roots in $\mathbb{N}$? Has in a short running time in general?