Modern Cryptography Dec 3, 2019

Homework 9

Lecturer: Daniel Slamanig, TA: Karen Klein, Guillermo Perez Due: 23.59 CET, Dec 11, 2019

To get credit for this homework it must be submitted no later than Wednesday, December 11th via TUWEL. If you have not registered for the tutorial (192.063 Tutorial on Introduction to Modern Cryptography 2019W) on TUWEL, please do so. If you are unable to register for the course on TUWEL for some reason, submit your homework via email to via email to `michael.walter@ist.ac.at`, please use "MC19 Homework 9" as subject.

1. Groups
   - Let $N \in \mathbb{Z}_{>0}$ and let $G = \mathbb{Z}_N^*$. Prove that G is a group under the operation $a \cdot b := (a \cdot b) \bmod N$.
   - List the elements of $\mathbb{Z}_{17}^*$; What is its order?; What are the orders of 2 and 5?; Is $\mathbb{Z}_{17}^*$ cyclic?
   - Let $\mathbb{G}$ and $\mathbb{H}$ be groups. Show that $\mathbb{G} \times \mathbb{H}$ is a group (with $\times$ being the direct product).
2. Algorithmic aspects
   - Compute $101^{4800000002} \bmod 35$ (by hand).
   - Use the Extended Euclidean Algorithm (extGCD) to compute X, Y for $a = 2493$ and $b = 8709$. Illustrate all steps.
   - **[B.2 in book, 2nd edition]** Prove that the extGCD runs in time polynomial in the length of its inputs.