Cryptography I, homework sheet 3

Due: 07 October 2011, 10:45

Attention: one-line answers using a computer algebra system do *not* count. But it is a good moment to familiarize yourself with some system(s) so that you know how to solve similar problems for real life examples and to verify your answers. You may use a computer algebra system to compute subresults, such as factorizations, modular reduction, multiplication, squaring but not for modular inverses.

1. The integer $p = 1009$ is prime. You are the eavesdropper and know that Alice and Bob use the Diffie-Hellman key-exchange in a cyclic subgroup of $(\mathbb{Z}/p, +)$ with generator $g = 123$. You observe $h_a = 234$ and $h_b = 456$. What is the shared key of Alice and Bob?

2. Write the table for multiplication in $\mathbb{Z}/9\mathbb{Z}$.

3. Find integers n and m so that

$$124n + 162m = 6.$$

4. Give all elements in $(\mathbb{Z}/12)^\times$.

5. Give all elements in $(\mathbb{Z}/21)^\times$.

6. Let $(M, \circ)$ be a monoid. Prove that the set $M^\times$ of invertible elements in M forms a group.