TMA4155 — Exercise 12

Kristian Gjøsteen

2006-11-14

NB! This exercise will be in the auditorium F2.

Task 1 — Diffie-Hellman

*Find two other students to do parts **b.** and **c.** of this exercise with.*

In this task we shall work with the prime $p = 47$. Note that $p = 2 \cdot 23 + 1$, and that $q = 23$ is prime. Let $g = 4$.

a. Prove that g has order q without computing $g^q \bmod p$.

b. Alice and Bob uses the Diffie-Hellman protocol to agree on a shared secret using the parameters p, q, g, while Eve eavesdrops on their communication. In groups of three, pretend to be Alice, Bob and Eve. Eve must find the shared secret.

c. Alice and Bob uses the Diffie-Hellman protocol to agree on a shared secret using the parameters p, q, g, sending all their messages by way of Eve. Alice encrypts a number in $\{1, 2, \ldots, 46\}$ by adding the shared secret to it modulo 47, and sends the ciphertext to Bob. Bob decrypts. In groups of three, pretend to be Alice, Bob and Eve. Eve must make sure that Bob ends up with the number 12.

Task 2 — Discrete Logarithms

Let $p = 271$ be a prime. Compute the discrete logarithm of 74 to the base 6 using Pohlig-Hellman.