

# Exercises on Modulo Arithmetic and RSA

Víctor Alcázar      Kosmas Palios      Albert Ribes

April 3, 2017

Note: This is a correction of our previous submission.

## Exercise 2

We first compute  $x = b^c \bmod \phi(p)$

Then we compute  $a^x \bmod p$ .

Why is this correct? Simply because for every  $p, a$ , as Euler tells us that  $a^{\phi(p)} = 1 \bmod p$ , we have the following  $a^k = a^{k + \phi(p) * l} \bmod p$ .

This takes polynomial time, as modular exponentiation can be computed in polynomial time, with use of repeated squaring.