Discrete Mathematics
Notes Number theory

Moshe Rosenfeld

Hanoi 2011
moishe@u.washington.edu

1 Factoring Challenge

The following Key was intercepted during an exchange session on the internet:

Key = 5149655201481666288393234062791472595154099713623307834218536374878103610851426544234449973390985027568730853699423276912721013674109248474046130789

I happen to posses an **oracle** that can extract square roots mod this key.

If you send me an integer, if it is a quadratic residue mod Key, I will send you its' square root mod Key.

Note that it is very easy to verify that Key is a composite number.

Your mission is to factor this integer.