TP 3: implementation of RSA

Jean-Sébastien Coron

Université du Luxembourg

1 Big integer library

The following exercises can be done using

1. Python
2. The Sage library, available at `http://www.sagemath.org/`
3. The GMP library, using C or C++

The prefered solution is to use the Sage library.

2 Fermat test

1. Implement the Fermat test of primality with small integers.
2. Write a function to generate random k-bit prime numbers.

3 RSA

1. Write the key-generation function function of RSA. The function should generate two random primes p and q of size $k/2$ bits.
2. Implement the RSA encryption function
3. Implement the RSA decryption function
4. Check that decryption works