Implementation of RSA

Jean-Sébastien Coron

University of Luxembourg

1 Big integer library

The following exercise 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 Square and multiply

Implement the square and multiply algorithm.

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. In Sage, you can use the random_prime() function.
2. Implement the RSA encryption function, the RSA decryption function, and check that decryption works.
3. Implement the textbook RSA signature scheme, and check that signature verification works.