

# TP 02: the RSA algorithm

Jean-Sébastien Coron

Université du Luxembourg

## 1 RSA light

Implement the plain RSA encryption algorithm with artificially small parameters. Implement the plain RSA signature algorithm with artificially small parameters.

## 2 Full RSA

Download and install the NTL number theory library available at [www.shoup.net](http://www.shoup.net).

Implement the plain RSA encryption algorithm and the plain RSA signature algorithm with large numbers.