

TP 02: l'algorithme RSA

Jean-Sébastien Coron

Université du Luxembourg

<http://www.eleves.ens.fr/home/coron/cours/cours.html>

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.

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