

TP 5: implementation attacks against RSA

Jean-Sébastien Coron

Université du Luxembourg
www.jscoron.fr

1 Full RSA

Download and install the NTL number theory library available at www.shoup.net.
Implement the plain RSA encryption algorithm using NTL.

2 Implementation attack against RSA

To compute RSA decryption :

$$m = c^d \pmod{N}$$

we use the following square-and-multiply algorithm :

1. Write $d = d_k \dots d_0$ be the binary representation of d .
2. Let $z \leftarrow c \pmod{N}$
3. For $i = k - 1$ downto 0 do
 - (a) Let $z \leftarrow z^2 \pmod{N}$
 - (b) If $d_i = 1$ let $z \leftarrow z \cdot c \pmod{N}$
4. Output z

- 1) Implement RSA decryption with NTL using this algorithm.
- 2) Assume now that an attacker is given N and c as input, and is able to get the least significant bit of z after each step 3b. Show that the attacker can recover the private key d . Implement your attack to check that it works.