TP 1: the RSA algorithm

Jean-Sébastien Coron

Université du Luxembourg

1 Attack on variants of RSA

1.1 Secret modulus

Assume that Alice wants to keep her RSA modulus N secret to everybody except to Bob. Alice uses $e = 3$ as public exponent. To encrypt a message m, Bob computes $c = m^3 \mod N$ and sends c to Alice. Assume that Eve gets $c_1 = m_1^3 \mod N$ and $c_2 = m_2^3 \mod N$ and already knows m_1 and m_2; explain how Eve can recover N.

1.2 Common modulus

Assume that Alice and Bob want to share the same modulus N but use different public exponent. Alice uses $e_A = 3$ and Bob uses $e_B = 5$. Let d_A and d_B be the corresponding private exponents. Explain how Alice can recover d_B from d_A.

1.3 Common modulus, cont.

Assume that Alice and Bob want to share the same modulus N but use different public exponent. Alice uses $e_A = 3$ and Bob uses $e_B = 5$. Now Charlie wants to encrypt a message m for Alice and Bob. He sends:

$$c_A = m^3 \mod N$$

to Alice and

$$c_B = m^5 \mod N$$

to Bob. Explain how Eve can recover m from N, c_A and c_B.

1.4 Implementation

Download and install the NTL number theory library available at `www.shoup.net`. Check that the previous attacks work by implementing them with NTL.