Lattice Reduction Techniques To Attack RSA

David Wong

University of Bordeaux

March 2015

RSA ?

(e, N) is the **public key**, (d, N) is the **private key**.

(e, N) is the **public key**, (d, N) is the **private key**.

To **encrypt** a message m, with $m < N$ we just do :

$$c = m^e \pmod N$$

(e, N) is the **public key**, (d, N) is the **private key**.

To **encrypt** a message m, with $m < N$ we just do :

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

And to **decrypt** :

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

To generate these keys, we first generate **two primes** p and q such that :

$$N = p \times q$$

To generate these keys, we first generate **two primes** p and q such that :

$$N = p \times q$$

Use p and q to generate the pair **private key/public key** (d, e).

ATTACKS ?

On the implementation or on the mathematics.

On the implementation or on the mathematics.

Model :

- Recover the plaintext $m^e = c \pmod{N}$
- Recover the private key d

On the implementation or on the mathematics.

Model :

- Recover the plaintext $m^e = c \pmod{N}$
- Recover the private key d

Relaxed model :

On the implementation or on the mathematics.

Model :

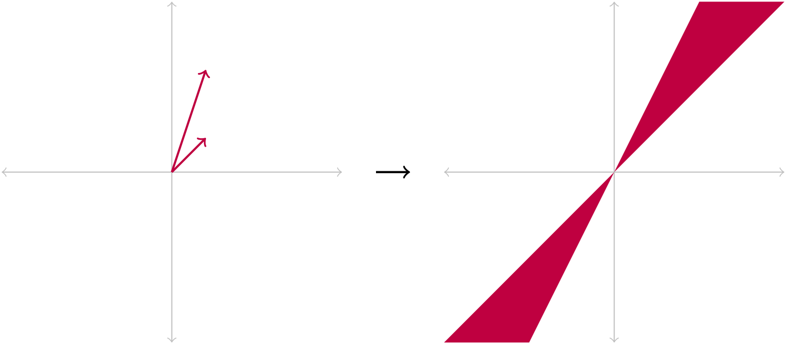
- Recover the plaintext $m^e = c \pmod{N}$
- Recover the private key d

Relaxed model :

- We know a part of the message
- We know an approximation of one of the prime
- The private exponent is too small

LATTICE ?

A bit like a **vector space**.



COPPERSMITH ?

BONEH-DURFEE ?