Université de Bordeaux — **Comp. Number Theory – N1MA9W11**
Master 2 MATH — 2014–2015

Final Exam. 2013 December 17th, 14h00 – 17h00.

Handwritten lecture notes are allowed as well as the course typescript. You may compose in either English or French.

Exercise (Introduction)

The RSA cryptosystem uses two distinct primes p, q, their product $N = pq$ and two integers d, e such that $de \equiv 1 \pmod{\varphi(N)}$, where $\varphi(N) = (p-1)(q-1)$ is Euler's totient. We call N the *RSA modulus*, e (resp. d) is the *encryption* (resp. *decryption*) exponent. The pair (N, e) is the *public key*, and is used to encrypt messages (or check signatures); the *secret key* d allows to decrypt them (or to sign a message): a *message* is an element $m \in \mathbb{Z}/N\mathbb{Z}$, the encrypted text is $c := m^e$; knowing the secret key d, we can decrypt it as $c^d = m$.

In practice p and q have roughly 1024 bit, to prevent outsiders from factoring N.

1) Prove that $m^{de} = m$ for all $m \in \mathbb{Z}/N\mathbb{Z}$. [*Also for non-invertible m!*]

2) Given two large primes p, q, $N = pq$, $\varphi(N) = (p-1)(q-1)$ and e chosen uniformly at random in $\mathbb{Z}/\varphi(N)\mathbb{Z}$:

a) how to compute d, and at what cost ?

b) what is the cost of encryption ?

3) Conversely, given d, e and N:

a) prove that the following algorithm recovers p and q: let $k = de - 1 =: 2^r t$ with t odd and $r > 0$; choose $g \in \mathbb{Z}/N\mathbb{Z}$ uniformly at random and compute the least $i \leqslant r$ such that $g^{t2^i} = 1$; either $\gcd(g^{t2^{i-1}} - 1, N)$ is p or q and we win; or we choose another g. [*This is a rough description, which does not work as stated in some corner cases. Fill in the details.*]

b) what is its (randomized) complexity?

Exercise (Wiener's attack)

You may use freely the following two facts:

Fact. (Hardy & Wright, Theorem 184) Let $x \in \mathbb{R}$ and p, q two integers such that $|p/q - x| < 1/(2q^2)$, then p/q is a convergent in the continued fraction of x.

Fact. Assume $0 \leqslant a < b$. Euclid's algorithm produces the $O(\log b)$ convergents of the rational number a/b in time $O(\log b)^2$.

We shall prove:

Theorem 1 (Wiener). *Let $N = pq$ with $q < p < 2q$ two primes of the same binary size, and let $0 < d \leqslant \frac{1}{3}N^{1/4}$. Given $0 \leqslant e < \varphi(N)$ such that $de \equiv 1 \pmod{\varphi(N)}$, one can efficiently recover d.*

1) Why would choosing a "small" d be advantageous in the RSA context ?

2) Let k (unknown) such that $de = 1 + k\varphi(N)$. Prove successively that
a) $0 \leqslant k \leqslant d$,
b) $N - \varphi(N) < 3\sqrt{N}$,
c) and finally, for $k \neq 0$,

$$\left|\frac{e}{N} - \frac{k}{d}\right| \leqslant \frac{3k}{d\sqrt{N}} < \frac{1}{3d^2}.$$

3) As a consequence, describe an algorithm finding (k, d) quickly, given (e, N). What is its complexity ?

4) How can choosing $e \gg \varphi(N)$ prevent the attack (even when d remains "small") without harming too much the process of encryption / decryption ?

Problem (Coppersmith's attack on short messages)

Theorem 2 (Coppersmith)**.** *Let $N > 0$ be an integer and $f \in \mathbb{Z}[x]$ be a monic polynomial of degree d. Set $B = N^{\frac{1}{d}-\varepsilon}$, for some $\varepsilon > 0$. Then one can efficiently find all integers $|x_0| < B$ such that $f(x_0) \equiv 0 \pmod{N}$.*

The running time is dominated by the time it takes to run LLL on a lattice of dimension $O(w)$, $w := \max(1/\varepsilon, \log_2 N)$, given by $O(w)$ generators whose coordinates are bounded by N.

Fact. The LLL algorithm run on a lattice Λ of dimension n produces $v \in \Lambda \setminus \{0\}$ such that $\|v\|_2 \leqslant 2^{(n-1)/2} d(\Lambda)^{1/n}$, in polynomial time.

1) Why is the theorem useless if N is prime or, more generally, easy to factor?

2) Let $h \in \mathbb{Z}[x]$ of degree d and $B > 0$ an integer such that

$$\|h(xB)\|_2 < \frac{N}{\sqrt{d+1}}.$$

Prove that if $|x_0| < B$ satisfies $h(x_0) \equiv 0 \pmod{N}$, then $h(x_0) = 0$ in $\mathbb{Z}$.

3) Let $m > 0$ be an integer, to be chosen later and let $g_{u,v} := N^{m-v} x^u f^v$.
a) Prove that $f(x_0) \equiv 0 \pmod{N}$ implies that $g_{u,v}(x_0) \equiv 0 \pmod{N^m}$ for all $0 \leqslant v \leqslant m$ and $0 \leqslant u$.
b) Prove that the lattice generated by the $g_{u,v}(xB)$, for $0 \leqslant u < d$, $0 \leqslant v \leqslant m$, has dimension $n := d(m+1)$ and determinant $\Delta = B^{n(n-1)/2} N^{nm/2}$.
c) Prove that for m large enough, there is an integer linear combination h of the $g_{u,v}$, $0 \leqslant u < d$, $0 \leqslant v \leqslant m$ satisfying $\|h(xB)\|_2 < N^m/\sqrt{n+1}$.
d) Choose m wisely and prove Coppersmith's theorem.

4) We attack an RSA implementation with *small* encryption exponent, say $e = 3$. Given a cyphertext $c \in \mathbb{Z}/N\mathbb{Z}$ associated to an unknown *short* message $\overline{m} \in \mathbb{Z}/N\mathbb{Z}$, such that its canonical representative in $\mathbb{Z}$ satisfies $0 \leqslant m < N^{(1/e)-\varepsilon}$ for some $\varepsilon > 0$. Explain how to use Coppersmith's theorem to recover a preimage m such that $m^e = c \pmod{N}$.