Home assignment 3 — Cryptography. UAM 2010-2011

Deadline: May 5th

Name:

Exercises

1) Solve the equation $x^{2011} \equiv 1234 \pmod{1625}$. Note: It is not admitted to try all classes modulo 1625 with the computer.

2) Consider a RSA cryptosystem with an encryption key $k \not\equiv \pm 1 \pmod{n}$, $n = pq$. Can the encrypting and the decrypting function coincide, i.e. $e_k(e_k(m)) = m$, $\forall m \in \mathcal{M}$? In the affirmative provide and example and in the negative provide a proof.

3) Find all bases for which 15 is a pseudoprime to the base a.

4) Given $n = p_1 p_2 \cdots p_r$ with p_i distinct primes, $r > 1$, prove that if n is a Carmichael number then $p_i - 1$ divides $n - 1$ for every $1 \le i \le r$. Hint: Use primitive roots modulo p_i. Note: Recall that a Carmichael number n is a pseudoprime to every base coprime to n.

5) Describe the calculations to decide if $n = 1 + 367 \cdot 10^3$ is prime using Pocklington primality test.
