**T-79.159 Cryptography and Data Security** **Spring 2004**
**Tutorial 5**
**Thursday 4.3.2004 14.15, room T3.**
**Markku-Juhani O. Saarinen** `<mjos@tcs.hut.fi>`

These exercises may require refreshing your basic number theory skills. Consult your textbooks (e.g. Cormen, Leiserson, Rivest, *Introduction to Algorithms*) or the web.

`http://www.math.umbc.edu/~campbell/NumbThy/Class/BasicNumbThy.html` may be helpful too.

1. Compute the exact value of $2^{123456789} \mod 10007$. What is the algorithm and its complexity ?

2. Compute the inverse of $2 \mod 10007$, i.e. a number $x$ satisfying $2x \equiv 1 \mod 10007$. What is the algorithm and its complexity ?

3. Consider RSA encryption. Is it possible to derive the the secret factors $p$ and $q$ from the public modulus $n$ and the secret key $d$ alone ? Here we use the standard definitions: $n = pq$, Encryption $C \equiv M^e \mod n$, decryption $M \equiv C^d \mod n$, $ed \equiv 1 \mod \phi(n)$.