TMA4155 — Exercise 5

Kristian Gjøsteen

2006-09-28

Task 1 — RSA encryption

You want to strengthen your RSA encryption, but you do not want to have two different moduluses (because this leads to a much larger public key). So you decide to do as follows: First encrypt with the public key (n, e_1), then with the public key (n, e_2). Explain why this does not lead to increased security.

Task 2 — Euclid's algorithm

Use Euclid's algorithm to compute $\gcd(a, b)$ for:

a. $a = 153$, $b = 157$.

b. $a = 153$, $b = 187$.

c. $a = 10005$, $b = 1101$.

d. $a = 10005$, $b = 1103$.

Task 3 — Modular inverses

Use the extended Euklid's algorithm to find an inverse for a modulo n for:

a. $a = 153$, $n = 157$.

b. $a = 157$, $n = 153$.

c. $a = 1103$, $n = 10005$.

d. $a = 73$, $n = 1103$.

Task 4 — Primality testing

Compute 2^{560}, 5^{560} and 7^{560} modulo 561. What would the Fermat test say about 561 being prime?