Christian Schindelhauer

Freiburg, Nov 19, 2008

Submission deadline: Nov. 24, 2008

Exercises

Algorithm theory

Winter term 2008/09

Exercise sheet 5

TASK 1 (1 point)**:**

For an RSA encryption choose $p = 13$ and $q = 17$.
Moreover, let $e = (131 + ((m - 309) \cdot 1105)) \bmod 221$ where m is your immatriculation number.

1. Compute the number d and specify the outputs of the algorithm *Extended-Euclid*. Furthermore, give the public and private key.

2. Generate a digital signature for the message $M = 72$. Use the Fast Exponentiation algorithm `power()` from the lectures. What does a recipient of the message have to check in order to verify the signature?

TASK 2 (0 points)**:**

We consider *Universal Hashing* for the Universe $U = \{0, ..., 10\}$ of size $N = 11$. For a Hash-table of size $m = 4$ the following Hash-function is randomly chosen:

$$h_{a,b}(x) = ((ax + b) mod\ N) mod\ m$$

with $a = 8$ and $b = 3$.

1. For the set $S = \{1, 5, 8, 9\}$ give the occupation of the Hash-table. How many collision do occur?

2. Find a „bad“ Hash-function $h_{a,b}$ for S, that means values for a and b such that at least 3 elements from S are hashed to the same bucket of the Hash-table.