# Homework 13 in Cryptography I

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Steven Corroy

02.02.2010

**Exercise 34.**

Alice wants to tell Bob a secret $m$. She encrypts it with Bob's public RSA-key $(899, 11)$. The encrypted message which Alice sends to Bob is 468.

Find out, what the original message $m$ was.

**Exercise 35.**

Assume an RSA module $n := pq$ with two primes $p \neq q$ and a public key $e = d^{-1}$. The message $m \in \{1, \ldots, n-1\}$ is encrypted using the RSA-algorithm with $e$.

(a) Show that it is possible to compute the secret key $d$ if $m$ and $n$ are not coprime, i.e. if $p \mid m$ or $q \mid m$.

(b) Calculate the probability for $m$ and $n$ having common divisors.

(c) How large is the probability if $n$ has 1024 bits? The primes $p$ and $q$ are approximately of same size $(p, q \approx \sqrt{n})$.

**Exercise 36.** Assume a single message $m$ is encrypted with RSA twice: once with the public key $(n, e)$ and once with the public key $(n, f)$. The numbers $e$ and $f$ are relatively prime. Is it possible to decode the message with knowledge of the public parameters and the cryptograms?