RUHR UNIVERSITÄT BOCHUM RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Ilya Ozerov, Elena Kirshanova

Präsenzübungen zur Vorlesung

Kryptanalyse

SS 2014

Blatt 7 / 02 June 2014

Lattices

Exercise 1:
Prove Theorem 50 for the non-homogeneous linear system

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b \bmod N.$$

Wiener's attack

Exercise 2:
What is the bound on secret RSA-key d in Wiener's attack when N is a prodcut of *three* equal size distinct primes? Does this make the attack more/less effective?

Coppersmith's method

Exercise 3:
Let $c = m^3 \bmod N$ and $c' = (m + r)^3 \bmod N$ be two RSA-ciphertexts for message m with *known* padding r. Provide an efficient algorithm to recover m using c, c', r and N.

Exercise 4:
Consider a monic polynomial of degree 2

$$f(x) = x^2 + ax + b$$

with $f(x_0) = 0 \bmod M$ and $|x_0| < X$. Using the proof of Theorem 59 provide a more tight estimation for X s.t. the Coppersmith's method finds x_0 in polynomial in $\log M$ time. Use $m = 3$.