RUHR UNIVERSITÄT BOCHUM

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

**Präsenzübungen zur Vorlesung**

# Kryptanalyse

**SS 2014**

Blatt 7 / 23 June 2014

**Exercise 1:**
Let $N_1, \ldots, N_5$ be pairwise prime RSA-modules and $m < N_i$ be a message. Provide an efficient algorithm to solve the following system:

$$\begin{aligned} c_1 &= m^3 \bmod N_1 \\ c_2 &= m^3 \bmod N_2 \\ c_3 &= m^5 \bmod N_3 \\ c_4 &= m^5 \bmod N_4 \\ c_5 &= m^5 \bmod N_5 \end{aligned}$$

Can you solve it without the last equation?

**Exercise 2:**
Let $M$ have an unknown divisor $b$ and $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree $n$. Assume you have an access to an algorithm $\mathcal{A}$ that on input $M$ and $f(x)$ outputs a root $x_0$ of $f(x) \bmod b$ that is *not* a root of $f(x) \bmod M$, that is,

$$f(x_0) = 0 \bmod b \text{ and } f(x_0) \neq 0 \bmod M.$$

Show how to find a non-trivial factor of $M$ in time polynomial in $n$ and $\log M$.

**Exercise 3:**
This exercise deals with the problem of finding a solution for a bivariate system of equations. Consider RSA with related messages. Assume Eve has intercepted two RSA-ciphertexts encrypted with public exponent $e = 3$: $c_1 = m_1^3 \bmod N$, $c_2 = m_2^3 \bmod N$. To apply Coppersmith's attack, she considers the following system of equations with two unknowns $x_1, x_2$ that correspond to the solution $(m_1, m_2)$:

$$\begin{aligned} f_1(x_1) &= x_1^3 - c_1 \bmod N \\ f_2(x_2) &= x_2^3 - c_2 \bmod N \\ p(x_1, x_2) &= 0 \bmod N. \end{aligned}$$

**Case 1.** Assume Eve has an explicit relation between $m_1$ and $m_1$:

$$p(m_1, m_2) : m_2 = a \cdot m_1 + b,$$

for some known $a$ and $b$. Reduce the problem to a univariate system with two equations.
**Case 2.** Now assume we the relation is given by

$$p(m_1, m_2) = m_2^2 + m_1 m_2 + 4 = 0 \bmod N.$$

In order to help Eve to solve this system, proceed as follows:

1. Using the Sylvester matrix, compute the resultant $r(x_2)$ of $p(x_1, x_2)$ and $f_1(x_1)$ with regard to $x_1$.

2. The obtained resultant has a common root with $f_2(x_2)$. Find $\gcd(r(x_2), f_2(x_2)) \bmod N$. What does it tell you about $m_2$?

3. Using the above, construct two polynomials in only one unknown. Can you now determine $m_1$?