RUHR UNIVERSITÄT BOCHUM

RUB

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

Präsenzübungen zur Vorlesung

Kryptanalyse I

SS 2015

Blatt 1 / 16 April 2014

Aufgabe 1:
Show that

1. $\phi(pq) = (p-1)(q-1)$, if $\text{ggT}(p,q) = 1$
2. $\phi(p^k) = p^k \cdot (1 - \frac{1}{p})$ for prime p, $k \in \mathbb{N}$.

Aufgabe 2:
Let $N = pq$ be an RSA modulus and $l(N) = \text{LCM}(p-1, q-1)$ (LCM = Least Common Multiple/ kleinstes gemeinsames Vielfaches). Prove that for a public key e one can compute the corresponding secret key as

$$e \cdot d = 1 \bmod l(N).$$

Aufgabe 3:
Prove the generalized version of the Chinese Remainder Theorem: let $m_1, \ldots m_k$ be pairwise relatively prime integers (i.e. $\gcd(m_i, m_j) = 1$ for all $i \neq j$). Show that the following system of simultaneous congruences has exactly one solution x modulo $N = m_1 \cdot \ldots \cdot m_k$

$$\begin{cases} x = a_1 \bmod m_1 \\ x = a_2 \bmod m_2 \\ \quad \vdots \\ x = a_k \bmod m_k. \end{cases}$$

Aufgabe 4:
Let

$$\begin{aligned} \text{RSA}_e : \mathbb{Z}_N^* &\to \mathbb{Z}_N^* \\ x &\mapsto x^e \end{aligned}$$

Show that

$$|\{x \in \mathbb{Z}_N^* | \text{RSA}_e(x) = x\}| = \gcd(e-1, p-1) \cdot \gcd(e-1, q-1).$$

Hint: Show that $|\{x \in \mathbb{Z}_N^* | x^k = 1\}| = \gcd(k, p-1)$ for prime p.