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

Präsenzübungen zur Vorlesung

Kryptanalyse

SS 2014

Blatt 1 / 14. April 2014

AUFGABE 1:

Sei G eine multiplikative Gruppe mit neutralem Element 1. Sei $a \in G$ beliebig. Zeigen Sie, dass $\langle a \rangle = \{a, a^2, \ldots, a^{\mathrm{ord}(a)}\}$ eine multiplikative Gruppe ist.

AUFGABE 2:

Sei p prim und $k \in \mathbb{N}$. Zeigen Sie, dass $\phi(p^k) = p^k \cdot (1 - \frac{1}{p})$.

AUFGABE 3:

Zeigen Sie den verallgemeinerten Chinesischen Restsatz: Seien $m_1, m_2, \ldots, m_n$ teilerfremde natürliche Zahlen. Dann existiert genau eine Lösung $x \bmod m_1 \cdot m_2 \cdot \ldots \cdot m_n$ des Gleichungssystems

$$\left| \begin{array}{c} x = a_1 \bmod m_1 \\ x = a_2 \bmod m_2 \\ \vdots \\ x = a_n \bmod m_n \end{array} \right| .$$

AUFGABE 4:

Alice feiert eine Party und möchte eine Einladung an Bob, Berta und Birte verschicken. Diese besitzen paarweise teilerfremde RSA-Moduln N_1, N_2, N_3. Außerdem benutzen alle drei den öffentlichen Schlüssel $e = 3$. Die von Alice verschickte Nachricht m soll ein gültiger Klartext für alle Moduln sein, d.h. $m < \min\{N_1, N_2, N_3\}$. Die arme Eve ist nicht zur Party eingeladen, würde aber liebend gerne wissen, wann und wo die Feier stattfindet. Helfen Sie Eve und zeigen Sie, wie man m effizient berechnen kann.

Eine abelsche Gruppe $(G, \cdot)$ hat folgende Eigenschaften:

1) Abgeschlossenheit: Für alle $a, b \in G$ gilt $a \cdot b \in G$.
2) Assoziativität: Für alle $a, b, c \in G$ gilt $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3) Kommutativität: Für alle $a, b \in G$ gilt $a \cdot b = b \cdot a$.
4) Neutrales Element: Es gibt ein eindeutiges $e \in G$ mit $a \cdot e = a$ für alle $a \in G$.
5) Inverses Element: Für jedes $a \in G$ gibt es ein eindeutiges $a^{-1} \in G$ mit $a \cdot a^{-1} = e$.