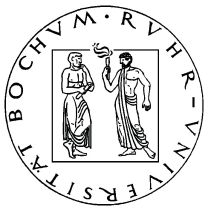
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann, Alexander Meurer



Hausübungen zur Vorlesung

Kryptanalyse

WS 2009/2010

Blatt 1 / 16. Oktober 2009 / Abgabe bis spätestens 28. Oktober 2009, 10 Uhr, entweder vor der Übung oder in NA 5/74

AUFGABE 1 (4 Punkte)**:**
Sei $N = pq$ mit $p \neq q$ prim. Zeigen Sie, dass $\text{ord}(\mathbb{Z}_N^*) = (p-1)(q-1)$.

AUFGABE 2 (6 Punkte)**:**

(a) Sei $N \in \mathbb{N}$ und $x \in \mathbb{Z}_N^*$ mit $\text{ord}(x) = k \in \mathbb{N}$. Zeigen Sie , dass mit $a, b \in \mathbb{Z}$ gilt:

$$x^a \equiv x^b \pmod{N} \Leftrightarrow a \equiv b \pmod{k}.$$

(b) Seien $a, b \in \mathbb{Z}$ mit $a \equiv b \pmod{\varphi(N)}$. Zeigen Sie, dass dann für alle $x \in \mathbb{Z}_N^*$ gilt:

$$x^a \equiv x^b \pmod{N}.$$

(c) Berechnen Sie $5^{2222211} \pmod{19}$.

(d) Bestimmen Sie das Inverse zu $5^{2222225} \pmod{19}$.

AUFGABE 3 (4 Punkte)**:**
Sei G eine zyklische Gruppe. Zeigen Sie, dass es $\varphi(\text{ord}(G))$ viele Generatoren in G gibt.

AUFGABE 4 (6 Punkte)**:**
Zeigen Sie den verallgemeinerten Chinesischen Restsatz:
Seien $m_1, m_2, \ldots, m_n$ teilerfremde natürliche Zahlen. Es existiert genau eine Lösung $x \bmod m_1 m_2 \ldots m_n$ des Gleichungssystems

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