Prof. Dr. A. Goerdt
M. Auerbach, A. Lanka

TU Chemnitz
Wintersemester 2006/2007
15.12.2006

Datenschutz und Datensicherheit / Systemsicherheit

9. Übung

1. Aufgabe:

   a) Zeigen Sie: Für alle $a \in \mathbb{Z}_n^*$ gilt $a \cdot \mathbb{Z}_n^* = \mathbb{Z}_n^*$, d.h. für $\mathbb{Z}_n^* = \{r_1, \ldots, r_{\varphi(n)}\}$ gilt

   $$\{r_1, \ldots, r_{\varphi(n)}\} = \{(a \cdot r_1) \bmod n, \ldots, (a \cdot r_{\varphi(n)}) \bmod n\}.$$

   b) Folgern Sie aus a) den Satz von Euler/Fermat

   „Wenn a und n teilerfremd sind, dann ist $a^{\varphi(n)} \equiv 1 \pmod{n}$“.

   Hinweis: Multiplizieren Sie alle Elemente aus $\mathbb{Z}_n^*$ miteinander.

2. Aufgabe:

   Demonstrieren Sie das RSA-Verfahren mit den Primzahlen $p = 5$ und $q = 11$.

   a) Berechnen Sie einen geheimen Schlüssel d und ermitteln Sie den zugehörigen öffentlichen Schlüssel e.
   b) Entschlüsseln Sie damit die Nachricht $c = 41$.
   c) Verschlüsseln Sie die Nachricht $m = 12$.

3. Aufgabe:

   Wir wollen RSA modifizieren und statt der beiden Primzahlen p und q nun drei verschiedene Primzahlen p_1, p_2, p_3 einsetzen ($n = p_1 \cdot p_2 \cdot p_3$). Beweisen Sie, daß das modifizierte Verfahren noch immer korrekt ist.

   Zeigen Sie zunächst $m^{e \cdot d} \equiv m \pmod{p_i}$ (eine Unterscheidung $p_i \mid m$ und $p_i \nmid m$ ist hilfreich) und folgern Sie aus diesen drei Kongruenzen $m^{e \cdot d} \equiv m \pmod{n}$.