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

TU Chemnitz
Wintersemester 2006/2007
08.12.2006

Datenschutz und Datensicherheit / Systemsicherheit

8. Übung

1. Aufgabe:

   Zeigen Sie:

   a) Für zwei verschiedene Primzahlen p und q gilt $\varphi(p \cdot q) = (p-1) \cdot (q-1)$.

   b) Für eine Primzahlpotenz p^k gilt $\varphi(p^k) = p^k - p^{k-1}$.

   c) Für zwei teilerfremde Zahlen a und b gilt $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

   Geben Sie eine Formel für $\varphi(m)$ an, wenn die Primfaktorzerlegung von m bekannt ist.

2. Aufgabe:

   a) Nehmen Sie an, daß B eine verschlüsselte Nachricht von A erhalten möchte. Dazu veröffentlicht B die Zahlen $p = 17$ und $g = 3$. Was muß B noch veröffentlichen, damit A ihm eine Nachricht per ElGamal-Verschlüsselungsverfahren schicken kann?

   b) Verschlüsseln Sie (anstelle von A) die Nachricht $m = 7$.

   c) Entschlüsseln Sie (anstelle von B) die Nachricht $(4, 11)$.

   d) Wieso sollte die Zahl z bei jeder neuen Nachrichtenübermittlung geändert werden?

   e) Funktioniert die Nachrichtenübermittlung mit ElGamal auch dann, wenn g kein Generator der Menge $\mathbb{Z}_p^*$ ist? Welche Gefahr besteht in diesem Fall?

   f) Was ist zu beachten, wenn keine Primzahl p, sondern ein beliebiges m als Modul gewählt wird?