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

TU Chemnitz
Wintersemester 2006/2007
29.11.2006

Datenschutz und Datensicherheit / Systemsicherheit

7. Übung

1. Aufgabe:

   Wann existiert eine Lösung x für die Gleichung $ax \equiv b \pmod{m}$?

2. Aufgabe:

   Demonstrieren Sie die Methode der Vorlesung für schnelles Potenzieren bei x^{43}.

   Welche Laufzeit hat das Verfahren?

3. Aufgabe:

   a) Überzeugen Sie sich, daß $\mathbb{Z}_{10}^*$ unter Multiplikation abgeschlossen ist.

   Erinnerung: $\mathbb{Z}_n^*$ ist die Menge der zur n teilerfremden Zahlen, die kleiner als n sind. Unter Multiplikation abgeschlossen sein heißt in diesem Fall, daß das Produkt modulo 10 von je zwei Zahlen aus $\mathbb{Z}_{10}^*$ wieder in $\mathbb{Z}_{10}^*$ liegt.

   b) Beweisen Sie, daß $\mathbb{Z}_n^*$ unter Multiplikation abgeschlossen ist.

4. Aufgabe:

   Die Eulersche φ-Funktion ist definiert als $\varphi(n) = |\mathbb{Z}_n^*|$ an. Berechnen Sie $\varphi(n)$ für $n = 8, 9, 10$ und 11.

5. Aufgabe:

   Zeigen oder widerlegen Sie:

   a) Wenn g ein Generator von $\mathbb{Z}_m^*$ ist, so gilt $g^{\varphi(m)} \equiv 1 \pmod{m}$.

   b) $g^a \equiv g^{a \bmod \varphi(m)} \pmod{m}$.

   c) Falls $\mathrm{ggT}(a, n) = 1$, dann gilt

   $$\{0, 1, \ldots, n-1\} = \{(a \cdot 0) \bmod n, (a \cdot 1) \bmod n, \ldots, (a \cdot (n-1)) \bmod n\}.$$

   d) Wenn g Generator von $\mathbb{Z}_m^*$ ist und $\mathrm{ggT}(a, \varphi(m)) = 1$, dann ist $g^a \bmod m$ auch ein Generator von $\mathbb{Z}_m^*$.

   e) Wenn $\mathbb{Z}_m^*$ einen Generator hat, dann hat $\mathbb{Z}_m^*$ genau $\varphi(\varphi(m))$ Generatoren.

6. Aufgabe:

   a) Ein Generator von $\mathbb{Z}_{18}^*$ ist 5. Finden Sie die restlichen Generatoren.

   b) Ein Generator von $\mathbb{Z}_{7}^*$ ist 3. Finden Sie die restlichen Generatoren.

   c) Besitzt die $\mathbb{Z}_{8}^*$ einen Generator?

7. Aufgabe:

   a) Führen Sie das Diffie-Hellman-Verfahren zur Vereinbarung eines gemeinsamen Schlüssels durch. Benutzen Sie $p = 61$ und $g = 2$.

   b) Welche Konsequenz hat es, wenn für g kein Generator gewählt wird?