Übungen zur Vorlesung **Blatt 3**
Elliptische Kurven und Kryptographie 4.05.2015

PD Dr. K. Halupczok
Dipl.–Math. A. Juhas SoSe 2015

Abgabetermin: Montag, 11. Mai 2015, bis 12:15 Uhr in die Briefkästen

Aufgabe 1:

Wir betrachten $(\mathbb{Z}_m^*, \cdot, 1)$ und sei m so gewählt, dass $\mathbb{Z}_m^* = \langle \underline{b} \rangle$ mit $\underline{b} \in \mathbb{Z}_m^*$. Der diskrete Logarithmus ist durch die Abbildung

$$\log_b : \begin{cases} \mathbb{Z}_m^* & \longrightarrow & \mathbb{Z}_{\varphi(m)} \\ b^k \bmod m & \longmapsto & k \bmod \varphi(m) \end{cases}$$

definiert. Zeigen Sie

(a) $\log_b$ ist wohldefiniert.
(b) $\log_b$ erfüllt die Funktionalgleichung $\log_b(\underline{xy}) = \log_b(\underline{x}) + \log_b(\underline{y})$ mit $\underline{x}$, $\underline{y} \in \mathbb{Z}_m^*$.
(c) $\log_b$ ist bijektiv.

Finden Sie einen Erzeuger $\underline{b}$ von $\mathbb{Z}_{23}^*$ und berechnen Sie $\log_b(\underline{13})$.

Aufgabe 2:

Gegeben sei ein RSA-Verfahren mit $n = 22499$, $e = 1291$.

(a) Kodieren Sie den Text „SEI␣EPSILON␣" wie im Skript zum RSA–Verfahren beschrieben.
(b) Finden Sie ein $d \in \mathbb{N}$ mit
$$de \equiv 1 \bmod \varphi(n).$$
(c) Dekodieren Sie den Text „JI.FTJ" wie im Skript zum RSA–Verfahren beschrieben.

(Bemerkung: Sie dürfen für die Ver– und Entschlüsselung einen PC zur Hilfe nehmen.)

Aufgabe 3:

(a) Begründen Sie, warum $n = 32399$ (abgesehen davon, dass n klein ist) eine schlechte Wahl für einen RSA–Modul ist. Welche n sind somit generell ungeeignet?
(b) Gegeben sei ein RSA–Verfahren mit Parametern $n = 2047$, $e \equiv 1 \bmod 88$. Begründen Sie, warum $d = e$ eine schlechte Wahl für einen privaten Schlüssel d ist. (Zwei Gründe, einer davon schwerwiegend.)

Aufgabe 4:

(a) Finden Sie für $p = 53$ und $q = 13$ eine Restklasse $\underline{x} \in \mathbb{Z}_p^*$ mit $\operatorname{ord}(\underline{x}) = q$.
(b) Der geheime Schlüssel von Alice ist $a = 9$. Berechnen Sie ihren öffentlichen DSA-Schlüssel.
(c) Berechnen Sie mit Alices geheimen Schlüssel eine Signatur zur Nachricht m mit Hashwert 8. Verwenden Sie dabei die Zufallszahl $\tilde{a} = 4$ und überprüfen Sie die Gültigkeit der Signatur.