FTK3, WS 2023/24
4. Übungsblatt für den 24.11.2023

1. In den beiligenden Textfiles findest du Vorschläge für DSA Domain Parameter. Finde den einzigen Vorschlag, der alle Anforderungen erfüllt, und erkläre für jeden anderen Vorschlag, wo jeweils das Problem liegt.

2. Du erhältst von Alice die DSA-Signatur (r_1, s_1) der Nachricht m_1 mit dem Hashwert h_1 und die DSA-Signatur (r_2, s_2) der Nachricht m_2 mit dem Hashwert h_2. Alices DSA-Parameter und Public Key sind (p, ω, g, A), als Hashfunktion wurde SHA-256 verwendet. Alle Parameter finden sich im beiligenden Textfile.

   (a) Berechne Alices Private Key.
   (b) Prüfe, ob der berechnete Private Key zum Public Key passt.

3. Du wählst als Schnorr-Parameter eine Hashfunktion deiner Wahl, die Gruppe $\mathbb{Z}_p^*$ mit $p = 6277$ und $g = 2004$ mit der Ordnung $\omega = 523$ in $\mathbb{Z}_p^*$. Als Private Key wählst du $\alpha = 213$.

   (a) Berechne deinen Public Key.
   (b) Berechne mit deinem Private Key eine Signatur für die Nachricht `"Hello World"`.
   (c) Prüfe mit deinem Public Key die Signatur.

4. Gegeben ist die elliptische Kurve ε: $y^2 = x^3 - 4x + 4$ über $\mathbb{R}$.

   (a) Sind $(-2, 2)$ und $(-1, 7)$ Punkte auf ε?
   (b) Berechne – wenn möglich – die y-Koordinate von $(8, y)$ und von $(-8, y)$.

5. Gegeben ist die elliptische Kurve ε: $y^2 = x^3 + 2x + 4$ über $\mathbb{R}$ und die Punkte P und Q auf ε. Berechne $P + Q$ und überprüfe, ob das Ergebnis ein Punkt auf der Kurve ist.

   (a) $P = (-1, 1)$, $Q = (2, 4)$
   (b) $P = (-1, 1)$, $Q = (-1, 1)$
   (c) $P = (-1, 1)$, $Q = (-1, -1)$

6. Gegeben ist die elliptische Kurve ε: $y^2 = x^3 - 8x + 8$ über $\mathbb{R}$ und die Punkte $P = (1, 1)$, $Q = (-2, -4)$ und $R = (\frac{34}{9}, -\frac{152}{27})$ auf ε. Berechne

   (a) $(P + Q) + R$
   (b) $P + (Q + R)$

7. Bestimme die endliche Ordnung von $P = (1, 2)$ auf der elliptischen Kurve ε: $y^2 = x^3 + x + 2$ über $\mathbb{R}$.

8. Finde ein Tool zum Zeichnen von elliptischen Kurven über $\mathbb{R}$ und zeichne alle Kurven dieses Übungszettels.