Humboldt-Universität zu Berlin
Prof. Dr. Johannes Köbler

Übungsblatt 8

Besprechung der mündlichen Aufgaben am 15. 12. 2022
Abgabe der schriftlichen Lösungen bis 3. 1. 2023, 23:59 Uhr

Aufgabe 45 Sei E die elliptische Kurve $y^2 = x^3 - x$ über $\mathbb{Z}_{71}$. ***mündlich***

(a) Bestimmen Sie die Anzahl der Punkte von E.

(b) Bestimmen Sie alle Punkte der Ordnung 1, 2, 3 und 4, sowie einen Punkt maximaler Ordnung in E. Ist E zyklisch?

Aufgabe 46 ***mündlich***
Sei E eine elliptische Kurve und f eine Funktion $\{0,1\}^{t+n} \to E$. Betrachten Sie für $N = 2^n \in \mathbb{N}$. folgende Hashfunktion $h : \bigcup_{l=1}^{N} \{0,1\}^{l(t+n)} \to E$: Für einen Text $x \in \{0,1\}^*$ seien $x_0, \ldots, x_{l-1}$ die t-Bitblöcke, dann gilt:

$$h(x) = \sum_{i=0}^{l-1} f(x_i \mathrm{bin}_n(i)),$$

wobei $\mathrm{bin}_n(i)$ die Binärdarstellung von i mit genau n Bits ist.

(a) Sei $h(x)$ der Hashwert einer Nachricht $x \in \{0,1\}^l$. Wie bestimmen Sie für $x' \in \{0,1\}^l$ den Wert $h(x \oplus x')$ effizient, wenn x' höchstens $\frac{l}{2}$ Einsen enthält?

(b) Welches Eigenschaft von h wäre ohne das Suffix $\mathrm{bin}_n(i)$ (unabhängig von f) verletzt?

(c) Warum sollten für f keine $i \in \{0, \ldots, N-2\}, P \in E$ existieren, sodass für alle $x \in \{0,1\}^t$ gilt: $f(x\mathrm{bin}_n(i)) - f(x\mathrm{bin}_n(i+1)) = P$?

(d) Warum ist für $k \in \{0,1\}^t$ die Funktion h_k mit $h_k(x) = h(kx)$ nicht als MAC geeignet?

(e) Falls das Problem, bei gegebenen $P, Q \in E$ mit $Q = kP$ die Zahl k zu finden (diskretes Logarithmusproblem) für E schwer ist, eignet sich dann h'_k mit $h'_k(x) = kh(x)$ als MAC?

Hinweis: Betrachten Sie drei Nachrichten $x_1x_2, x'_1x_2, x_1x'_2$ mit je 2 Blöcken.

Aufgabe 47 Sei E die elliptische Kurve $y^2 = x^3 + x + 26$ über $\mathbb{Z}_{127}$. ***mündlich***

(a) Bestimmen Sie die NAF-Darstellung der Zahl 87.

(b) Bestimmen Sie mit Hilfe des Algorithmus DoubleAddSub das Vielfache $87P$ des Punktes $P = (2, 6)$ auf der elliptischen Kurve E.

Aufgabe 48 ***mündlich***

Bestimmen Sie die Anzahl l_i aller natürlichen Zahlen, die eine NAF-Darstellung der Form $(c_{i-1}, \ldots, c_0)$ mit $c_{i-1} = 1$ haben. Zeigen Sie hierzu folgende Rekursion und finden Sie eine explizite Formel für l_i.

$$l_i = \begin{cases} 1, & i \leq 2, \\ 2(l_1 + \cdots + l_{i-2}) + 1, & i \geq 3. \end{cases}$$

Aufgabe 49 Sei $(G, \circ, e)$ eine endliche Gruppe der Ordnung n. ***mündlich***

(a) Zeigen Sie, dass G genau dann zyklisch ist, wenn G isomorph zu $(\mathbb{Z}_n, +, 0)$ ist.

(b) Zeigen Sie, dass das Produkt zweier zyklischer Gruppen der Ordnungen n_1 und n_2 genau dann zyklisch ist, wenn $\mathrm{ggT}(n_1, n_2) = 1$ ist.

(c) Folgern Sie, dass $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ im Fall $n_1 | n_2$ genau dann zyklisch ist, wenn $n_1 = 1$ ist.

(d) Bestimmen Sie die Ordnung $\mathrm{ord}(a) = \min\{k \geq 1 \mid ka \equiv_m 0\}$ von a in $\mathbb{Z}_m$.

(e) Sei $a \in \mathbb{Z}_m^*$ ein Element der Ordnung $\mathrm{ord}(a) = k$. Welche Ordnung hat dann die Potenz a^i in $\mathbb{Z}_m^*$?

Aufgabe 50 ***mündlich***

Ein Text x soll mit dem RSA-Verfahren sowohl verschlüsselt als auch signiert werden. Beschreiben Sie, worauf hierbei zu achten ist, damit die Nachricht nicht abgefangen und unbemerkt mit der Signatur eines Angreifers versehen werden kann.

Aufgabe 51 ***10 Punkte***

Sei E_q die elliptische Kurve $y^2 + y = x^3$ über $\mathbb{F}_q$ $(q = 2^n)$.

(a) Sei $P = (x, y) \in E_q$. Bestimmen Sie die Koordinaten von $-P$ und von $2P$.

(b) Bestimmen Sie die Ordnung aller Punkte P von E_{16}. (*Hinweis:* Berechnen Sie die Koordinaten von $4P$.)

(c) Bestimmen Sie die Anzahl der Punkte von E_4 und von E_{16}. (*Hinweis:* Zeigen Sie $\#E_{16} = \#E_4$ und benutzen Sie den Satz von Hasse.)