Kryptographie **Blatt 4**

hhu Düsseldorf
WiSe 2023/24

Abgabe: bis Montag 13.11.2023, vor der Vorlesung

Vorlesungswebseite: `http://reh.math.uni-duesseldorf.de/~khalupczok/krypto/`

Aufgabe 1: Textkodierung beim RSA-Verfahren

Für eine RSA-Verschlüsselung sei der RSA-modul $n = 22499$ gegeben, für den $27^3 \leq n \leq 29^3$ gilt, sowie $n \leq 27^4$.
Klartexte im Klartext-Alphabet A $\mapsto 1, \ldots,$ Y $\mapsto 25$, Z $\mapsto 0$, Leerzeichen $\mapsto 26$, werden damit zu Blöcken aus je drei Zahlen von 0 bis 26 zusammengefasst, also z. B. „KLARTEXT “= 11, 12, 1/ 18, 20, 5/ 24, 20, 26. Jedem Block x_1, x_2, x_3 wird die Zahl $x = x_1 \cdot 27^2 + x_2 \cdot 27 + x_3$ zugeordnet, die beim RSA-Verfahren zu $v \equiv x^e \bmod n$ verschlüsselt wird. Die Zahl v wird dann durch $v = \tilde{v}_1 \cdot 27^3 + \tilde{v}_2 \cdot 27^2 + \tilde{v}_3 \cdot 27 + \tilde{v}_4$ beschrieben und so als Viererblock ins Alphabet Σ zurückkodiert. (a) Sei $e = 1291$. Verschlüsseln Sie damit die Klartextnachricht „NACHRICHT“ (b) Durch Hinzufügen zweier neuer Zeichen soll Σ zu Σ' erweitert werden, etwa mit den beiden Zeichen “,” und “.”. Mittels $v = v_1 \cdot 29^2 + v_2 \cdot 29 + v_3$, $0 \leq v_i < 29$, $i = 1, 2, 3$, kann der verschlüsselte Text dann wieder in Dreierblöcken im Alphabet Σ' dargestellt werden. Begründen Sie: Auch mit dieser Methode kann aus einem verschlüsselten Text eindeutig der Klartext wieder hergestellt werden. (c) Warum reicht es in Teil (b) nicht aus, das Alphabet mit einem einzigen Zeichen zu erweitern? (d) Verschlüsseln Sie wiederum den Klartext „NACHRICHT“ mit $e = 1291$ und dem erweiterten Geheimtext-Alphabet Σ' in (b).

Aufgabe 2: Rechenregeln des diskreten Logarithmus

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

$$\log_g : \begin{cases} \mathbb{Z}_m^\times \to \mathbb{Z}_{\varphi(m)} \\ g^k \bmod m \mapsto k \bmod \varphi(m) \end{cases}$$

definiert. Zeigen Sie: (a) $\log_g$ ist wohldefiniert. (b) $\log_g$ erfüllt die Funktionalgleichung $\log_g(xy) = \log_g(x) + \log_g(y)$ für alle $x, y \in \mathbb{Z}_m^\times$. (c) $\log_g$ ist bijektiv. (d) Sei m so gewählt, dass g, h Primitivwurzeln mod m sind. Zeigen Sie $\log_h(x) = \log_g(x) \cdot \log_h(g)$ für alle $x \in \mathbb{Z}_m^\times$.

Finden Sie einen Erzeuger g von $\mathbb{Z}_{23}^\times$ und berechnen Sie $\log_g(13)$.

Aufgabe 3: Modulares Wurzelziehen

(a) Sei $p \equiv 5$ (8) prim und $a \in \mathbb{Z}$. Zeigen Sie, dass $X^2 \equiv a \bmod p$ ein Lösungspaar $\pm x$ mit $x = 2^m a^n$ hat für geeignete $m, n \in \mathbb{N}_0$.

Berechnen Sie damit konkret das Lösungspaar von $X^2 \equiv 13 \bmod 653$.

(b) Berechnen Sie mit der Methode 6.10 der Vorlesung die Wurzeln von $x^2 \equiv 61 \bmod 73$.