

Übungsblatt 12

Aufgabe 63

mündlich

Zeigen Sie, dass ein Public-Key-Kryptosystem nicht komplexitätstheoretisch sicher sein kann.

Aufgabe 64

mündlich

Ein RSA-Exponent $e \in \mathbb{Z}_{\varphi(n)}^*$ heie schwach, wenn fur alle $x \in \mathbb{Z}_n$ gilt: $x^e \equiv_n x$. Zeigen Sie, dass fur jeden RSA-Modul $n = pq$ genau $\varphi(n)/\text{kgV}(p-1, q-1) \geq 2$ schwache RSA-Exponenten existieren. Wie konnen diese erkannt bzw. wie kann ihre Verwendung ausgeschlossen werden?

Aufgabe 65

mndlich

Zwei RSA-Exponenten $e_1, e_2 \in \mathbb{Z}_{\varphi(n)}^*$ heien quivalent, wenn fur alle $x \in \mathbb{Z}_n$ gilt: $x^{e_1} \equiv_n x^{e_2}$.

- Zeigen Sie, dass zwei RSA-Exponenten e_1 und e_2 genau dann quivalent sind, wenn $e_1 \equiv_v e_2$ gilt, wobei $v = \text{kgV}(p-1, q-1)$ ist.
- Folgern Sie, dass der Entschlsselungsexponent d aus e auch ber die Kongruenz $ed \equiv_v 1$ bestimmt werden kann.

Aufgabe 66

mndlich

Ein RSA-Klartext $x \in \mathbb{Z}_n$ heie Fixpunkt fur den RSA-Exponenten e , wenn $x^e \equiv_n x$ ist. Bestimmen Sie die Anzahl der Fixpunkte in Abhangigkeit von e und n .

Aufgabe 67

mndlich

Sei A ein effizienter Algorithmus, der einen zufallig gewhlten RSA-Kryptotext $y \in \mathbb{Z}_n$ mit Wahrscheinlichkeit $\epsilon > 0$ dechiffriert. Transformieren Sie A in einen effizienten probabilistischen Algorithmus B , der jeden RSA-Kryptotext $y \in \mathbb{Z}_n$ bei Eingabe von y und einer Unrzahl 0^n mit Wahrscheinlichkeit $\geq 1 - 2^{-n}$ dechiffriert.

Aufgabe 68

mndlich

Der RSA-Kryptotext $y = 855$ wurde mit dem Schlssel $(e, n) = (17, 3233)$ erzeugt und liefert folgende Bits $b_i = \text{klartext-parity}(2^{ie}y \bmod n)$ fur $i = 1, \dots, 12$: 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1. Bestimmen Sie den zugehrigen Klartext.

Aufgabe 69

mndlich

Berechnen Sie fur $n = 221$ und $v = 4224 = 2^7 \cdot 33 = 2^m u$ die Mengen $A = \{a \in \mathbb{Z}_n^* \mid a^u \equiv_n 1\}$ und $B_t = \{a \in \mathbb{Z}_n^* \mid a^{2^t u} \equiv_n -1\}$ fur $t \geq 0$.

Aufgabe 70

10 Punkte

- Verschlsseln Sie den Klartext $x = 444$ mit dem ffentlichen RSA-Schlssel $(613, 989)$.
- Der Kryptotext $y = 444$ wurde mit dem RSA-Schlssel $k = (613, 989)$ erzeugt. Bestimmen Sie den zugehrigen Klartext.
- Faktorisieren Sie die Zahl $n = 9382619383$ mit dem Verfahren der Differenz der Quadrate.
- Faktorisieren Sie die Zahl $n = 4386607$ bei Kenntnis von $\varphi(n) = 4382136$.