Übungsblatt 12

Aufgabe 63 ***mündlich***

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

Aufgabe 64 ***mündlich***

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

Aufgabe 65 ***mündlich***

Zwei RSA-Exponenten $e_1, e_2 \in \mathbb{Z}^*_{\varphi(n)}$ heißen äquivalent, wenn für alle $x \in \mathbb{Z}_n$ gilt: $x^{e_1} \equiv_n x^{e_2}$.

(a) Zeigen Sie, dass zwei RSA-Exponenten e_1 und e_2 genau dann äquivalent sind, wenn $e_1 \equiv_v e_2$ gilt, wobei $v = \operatorname{kgV}(p-1, q-1)$ ist.

(b) Folgern Sie, dass der Entschlüsselungsexponent d aus e auch über die Kongruenz $ed \equiv_v 1$ bestimmt werden kann.

Aufgabe 66 ***mündlich***

Ein RSA-Klartext $x \in \mathbb{Z}_n$ heiße Fixpunkt für den RSA-Exponenten e, wenn $x^e \equiv_n x$ ist. Bestimmen Sie die Anzahl der Fixpunkte in Abhängigkeit von e und n.

Aufgabe 67 ***mündlich***

Sei A ein effizienter Algorithmus, der einen zufällig gewählten 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 Unärzahl 0^n mit Wahrscheinlichkeit $\geq 1 - 2^{-n}$ dechiffriert.

Aufgabe 68 ***mündlich***

Der RSA-Kryptotext $y = 855$ wurde mit dem Schlüssel $(e, n) = (17, 3233)$ erzeugt und liefert folgende Bits $b_i = \text{klartext-parity}(2^{ie} y \bmod n)$ für $i = 1, \ldots, 12$: $0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1$. Bestimmen Sie den zugehörigen Klartext.

Aufgabe 69 ***mündlich***

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

Aufgabe 70 ***10 Punkte***

(a) Verschlüsseln Sie den Klartext $x = 444$ mit dem öffentlichen RSA-Schlüssel $(613, 989)$.

(b) Der Kryptotext $y = 444$ wurde mit dem RSA-Schlüssel $k = (613, 989)$ erzeugt. Bestimmen Sie den zugehörigen Klartext.

(c) Faktorisieren Sie die Zahl $n = 9382619383$ mit dem Verfahren der Differenz der Quadrate.

(d) Faktorisieren Sie die Zahl $n = 4386607$ bei Kenntnis von $\varphi(n) = 4382136$.