Übungsblatt 13

Abgabe der schriftlichen Lösungen am 8. 2. 2018 bis 13.10 Uhr

Aufgabe 62 ***mündlich, rechenintensiv***

Betrachten Sie folgendes Zufallsexperiment:

> Ein probabilistischer Primzahltest T (mit einseitiger Fehlerwahrscheinlichkeit ε im Fall einer zusammengesetzten Eingabe) wird auf eine zufällig gewählte ungerade Binärzahl $n \in [2^l, 2^{l+1} - 1]$ angewandt.

Bestimmen Sie näherungsweise die Wahrscheinlichkeiten der beiden Ereignisse »n ist prim« (Ereignis A) und »$T(n)$ gibt prim aus« (Ereignis B). Wie groß sind die bedingten Wahrscheinlichkeiten $\Pr\left[\overline{A}|B\right]$, $\Pr\left[B|\overline{A}\right]$ und $\Pr\left[B|A\right]$ im Fall $\varepsilon = 2^{-m}$, $m = 1, 2, 5, 10, 20, 30, 50, 100$? Interpretieren Sie diese Zahlen.

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 ein 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 ***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 $\varphi(n) = 4382136$.