

Übungsblatt 12

Abgabe für die mündlichen Aufgaben bis 14. 07. 2020 und für die schriftliche Aufgabe bis 21. 07. 2020

Aufgabe 66

mündlich

- (a) Bestimmen Sie den kleinsten Erzeuger von \mathbb{Z}_{97}^* .
- (b) Bestimmen Sie die Anzahl aller Erzeuger von $\mathbb{Z}_{1041817}^*$.

Aufgabe 67

mündlich

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

Aufgabe 68

mündlich

Überlegen Sie, wie sich die Berechnung von $\text{RSA}_{(d,n)}^{-1}$ bei Kenntnis der Primfaktoren p und q von n mithilfe des chinesischen Restsatzes beschleunigen lässt.

Aufgabe 69

mündlich

Angenommen, Bob, Bert, and Bernd verwenden denselben RSA-Chiffrierexponenten $e = 3$, aber paarweise teilerfremde Modulzahlen n_1, n_2, n_3 . Wie kann ein Angreifer den Klartext x berechnen, falls Alice x an alle drei Empfänger sendet?

Aufgabe 70

mündlich

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

- (a) Zeigen Sie, dass für jeden RSA-Modul $n = pq$ genau $\varphi(n)/k \geq 2$ schwache RSA-Exponenten existieren, wobei $k = \text{kgV}(p-1, q-1)$ ist. Wie können diese erkannt bzw. wie kann ihre Verwendung ausgeschlossen werden?
- (b) Zeigen Sie, dass zwei RSA-Exponenten e_1 und e_2 genau dann äquivalent sind, wenn $e_1 \equiv_k e_2$ gilt.
- (c) Folgern Sie, dass die Exponenten aller RSA-Schlüssel (e, n) und (d, n) modulo k reduziert werden können, ohne deren Funktionalität zu beeinträchtigen.

Aufgabe 71

mündlich

Ein RSA-Klartext $x \in \mathbb{Z}_n$ heißt *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 72

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^m mit Wahrscheinlichkeit $\geq 1 - 2^{-m}$ dechiffriert.

Aufgabe 73

mündlich

Berechnen Sie für $n = 221$ und $v = 4224$ die exakte Erfolgswahrscheinlichkeit von $\text{RSA-Factorize}(n, v)$ sowie den Wert der im Skript hergeleiteten oberen Schranke $\sigma(n)/(n-1)$ für $\text{Pr}[\text{RSA-Factorize}(n, v) = ?]$.

Aufgabe 74

mündlich

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

Aufgabe 75

mündlich

Seien p, q ungerade Primzahlen, $k = \text{kgV}(p-1, q-1)$ und $n = pq$.

- (a) Zeigen Sie für alle $a \in \mathbb{Z}_n^*$ die Gleichheit $\text{ord}_n(a) = \text{kgV}(\text{ord}_p(a), \text{ord}_q(a))$.
- (b) Zeigen Sie, dass es ein Element $a \in \mathbb{Z}_n^*$ mit $\text{ord}_n(a) = k$ gibt.
- (c) Sei nun $\text{ggT}(p-1, q-1) = 2$ und $p, q > 3$. Angenommen, wir haben ein Orakel, das für eine feste Basis $a \in \mathbb{Z}_n^*$ mit $\text{ord}_n(a) = \varphi(n)/2$ den diskreten Logarithmus in \mathbb{Z}_n^* berechnet. Das Orakel gibt also für beliebige Anfragen $b \in \langle a \rangle$ den diskreten Logarithmus $x = \log_{n,a} b$ mit $0 \leq x \leq \varphi(n)/2 - 1$ zurück (der Wert $\varphi(n)/2$ bleibt dabei geheim).
Zeigen Sie, dass das Orakel bei Eingabe $b = a^n \bmod n$ den Wert $x = n - \varphi(n)$ zurückgibt.
- (d) Geben Sie einen effizienten Algorithmus an, der n unter Benutzung des Orakels aus (c) faktorisiert.

Aufgabe 76

10 Punkte

- (a) Verschlüsseln Sie den Klartext $x = 444$ mit dem öffentlichen RSA-Schlüssel $(e, n) = (613, 989)$.
- (b) Der Kryptotext $y = 444$ wurde mit dem öffentlichen RSA-Schlüssel $(e, n) = (613, 989)$ erzeugt. Bestimmen Sie den zugehörigen privaten RSA-Schlüssel (d, n) und den Klartext $x = \text{RSA}_{(d,n)}^{-1}(y)$.
- (c) Faktorisieren Sie die Zahl $n = 9382619383$ mit dem Verfahren der Differenz der Quadrate.
- (d) Faktorisieren Sie die Zahl $n = 4386607$ bei Kenntnis von $\varphi(n) = 4382136$.