Übungsblatt 14

Abgabe der schriftlichen Lösungen am 15. 2. 2018 bis 13.10 Uhr

Aufgabe 68 ***mündlich***

Sei A ein effizienter Algorithmus, der einen zufällig gewählten RSA-Kryptotext $y \in \mathbb{Z}_n$ mit Wahrscheinlichkeit $\epsilon > 0$ dechiffriert (d.h. A ist effizient im Average-Case für eine feste Erfolgswahrscheinlichkeit). 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 (d.h. B ist u.a. effizient im Worst-Case für jede Erfolgswahrscheinlichkeit).

Aufgabe 69 ***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 70 ***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 71 ***mündlich***

Seien p und q ungerade Primzahlen und $n = pq$.

(a) Zeigen Sie, dass $\text{ord}_n(\alpha) = \text{kgV}(\text{ord}_p(\alpha), \text{ord}_q(\alpha))$ für alle $\alpha \in \mathbb{Z}_n^*$.

(b) Zeigen Sie, dass es ein $\alpha \in \mathbb{Z}_n^*$ gibt mit $\text{ord}_n(\alpha) = \frac{\varphi(n)}{\text{ggT}(p-1, q-1)}$

(c) Sei nun $\text{ggT}(p-1, q-1) = 2$ und $p, q > 3$. Angenommen, wir haben ein Orakel, das für ein $\alpha \in Z_n^*$ mit $\text{ord}_n(\alpha) = \varphi(n)/2$ den diskreten Logarithmus in der Untergruppe $[\alpha]$ berechnet. Das Orakel berechnet also für beliebige $\beta \in [\alpha]$ den diskreten Logarithmus $a = \log_{n,\alpha} \beta$ mit $0 \leq a \leq \varphi(n)/2 - 1$. (Der Wert $\varphi(n)/2$ bleibt dabei geheim.)

Zeigen Sie, dass für das vom Orakel bei Eingabe $\beta = \alpha^n$ berechnete a gilt: $n - a = \varphi(n)$.

(d) Geben Sie einen effizienten Algorithmus an, der n unter Benutzung des Orakels aus (c) faktorisiert.

Aufgabe 72 ***mündlich***

Sei p prim mit $p \equiv_8 5$, und sei a ein quadratischer Rest modulo p. Weiterhin bezeichne $L_i(\beta)$ für $\beta \in \mathbb{Z}_p^*$ das Bit mit Wertigkeit 2^i in der Binärdarstellung von $\log_{n,\alpha} \beta$, wobei α ein Erzeuger von $\mathbb{Z}_p^*$ ist. Zeigen Sie:

(a) $a^{(p-1)/4} \equiv_p \pm 1$.

(b) Wenn $a^{(p-1)/4} \equiv_p 1$, dann ist $a^{(p+3)/8} \bmod p$ eine Quadratwurzel von a modulo p.

(c) Wenn $a^{(p-1)/4} \equiv_p -1$, dann ist $2^{-1}(4a)^{(p+3)/8} \bmod p$ eine Quadratwurzel von a modulo p.

Hinweis: Verwenden Sie die Tatsache, dass im Fall $p \equiv_8 5$ $(\frac{2}{p}) = -1$ ist.

(d) Bei Kenntnis von α kann $L_1(\beta)$ effizient berechnet werden.

Hinweis: Machen Sie davon Gebrauch, dass im Fall $p \equiv_8 5$ Quadratwurzeln modulo p effizient berechnet werden können und für alle $\beta \in \mathbb{Z}_p^*$ die Gleichheit $L_0(\beta) = L_1(p - \beta)$ gilt.

Aufgabe 73 ***10 Punkte***

Betrachten Sie das Rabin-System mit dem Schlüssel $p = 199$, $q = 211$, $n = pq$ und $e = 1357$.

(a) Berechnen Sie den Kryptotext y des Klartextes $x = 32767$.

(b) Bestimmen Sie die vier möglichen Entschlüsselungen von y.