Übungsblatt 13

Abgabe für die mündlichen Aufgaben bis 21. 07. 2020

Aufgabe 77 ***mündlich***

Zeigen Sie, dass ein RSA-Kryptotext $y \in \mathbb{Z}_n$ dasselbe Jacobi-Symbol wie der zugehörige Klartext $x \in \mathbb{Z}_n$ hat.

Aufgabe 78 ***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 $\log_{p,\alpha} \beta$, 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 $p \equiv_8 5$ das Legendre-Symbol $(\frac{2}{p}) = -1$ 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 $L_0(\beta) = L_0(p - \beta)$ gilt.

Aufgabe 79 ***mündlich***

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

(a) Berechnen Sie den Kryptotext y zum Klartext $x = 32767$.

(b) Bestimmen Sie die vier möglichen Klartexte zum Kryptotext y.

Aufgabe 80 ***mündlich***

Sei p eine ungerade Primzahl und sei $\mathrm{ggT}(a,p) = 1$.

(a) Sei $i \geq 2$ und $b^2 \equiv_{p^{i-1}} a$. Zeigen Sie, dass es genau ein $x \in \mathbb{Z}_{p^i}$ gibt mit $x^2 \equiv_{p^i} a$ und $x \equiv_{p^{i-1}} b$. Geben Sie ein effizientes Verfahren zur Berechnung von x an.

(b) Berechnen Sie mit Ihrem Verfahren ausgehend von $6^2 \equiv_{19} 17$ die Quadratwurzeln von 17 modulo 19^2 und modulo 19^3.

(c) Zeigen Sie für jedes $i \geq 1$, dass die Kongruenz $x^2 \equiv_{p^i} a$ entweder 0 oder 2 Lösungen hat.

Aufgabe 81 ***mündlich***

Wir betrachten das ElGamal-System über der Gruppe $\mathbb{F}_{27}^*$, wobei wir zur Konstruktion des Körpers $\mathbb{F}_{27}$ das irreduzible Polynom $m(x) = x^3 + 2x^2 + 1$ benutzen. Angenommen, wir wählen als Erzeuger das Element $\alpha = x$ und als privaten Schlüssel $a = 11$. Wie lässt sich damit der Kryptotext

$$y = (K,H)(P,X)(N,K)(H,R)(T,F)(V,Y)(E,H)(F,A)(T,W)(J,D)(U,J)$$

entschlüsseln, wenn wir die 26 Zeichen $A,\dots,Z$ der Reihe nach mit den Körperelementen $1, 2, x, x+1, x+2, 2x, \dots, 2x^2+2x+2$ kodieren?