

Kryptographie

Blatt 12, 01.07.05, Abgabe 08.07.05

Sei $N \in \mathbb{N}$ mit $\text{ggT}(\lambda(N), N) = 1$. $g \in \mathbb{Z}_{N^2}^*$ habe Ordnung αN , $1 \leq \alpha \leq \lambda(N)$. Für $m \in \mathbb{Z}_{N^2}$ mit $m \equiv 1 \pmod{N}$ sei $L(u) = \frac{m-1}{N} \pmod{N}$.

Aufgabe 1. Zeige für $r, m \in \mathbb{Z}_N$ und $c := g^{m+Nr}$, dass $m = L(c^\alpha)/L(g^\alpha)$.

Hinweis: $g^\alpha = 1 + vN \pmod{N^2}$ mit $\text{ggT}(v, N) = 1$.

Aufgabe 2. Sei $N = p \cdot q$ RSA Modul, $p - 1 = \alpha p_2$, $g \in \mathbb{Z}_{N^2}^*$ habe die Ordnung αN .

Die Nachricht $m \in \mathbb{Z}_p \cong [0, p[$ werde verschlüsselt zu $c = g^m r^N$ mit $r \in_R \langle g \rangle$.

Zeige : $m = L(c^\alpha)/L(g^\alpha) \pmod{p}$.

Welche Vorsichtsmaßnahmen erfordert dieses Kryptoschema ?

Aufgabe 3. Sei p prim, $g \in \mathbb{Z}_{p^2}^*$ habe Ordnung $p\alpha$, $1 \leq \alpha \leq p - 1$, $\alpha | p - 1$.

Zu $u \in \mathbb{Z}_{p^2}$ mit $u \equiv 1 \pmod{p}$ sei $L_p(u) = \frac{u-1}{p} \pmod{p}$.

Die Nachricht $m \in \mathbb{Z}_p \cong [0, p[$ werde verschlüsselt zu $c := g^m r^p$ mit $r \in_R \mathbb{Z}_p^*$.

Zeige: $m = L_p(c^\alpha)/L_p(g^\alpha) \pmod{p}$.

Ist das Kryptoschema sicher ?