Prof. C. P. Schnorr Sommersemester 2017

Kryptographie

Blatt 3, 10.05.2017, Abgabe 17.05.2017

Pollard's rho Algorithmus im Handbook of Applied Cryptography.

Aufgabe 1. Zerlege $n = 19909$ mit Pollard's rho Algorithmus 3.9.

Begründe Fakt 3.11 : Alg. 3.9 zerlegt $n \in \mathbb{N}$ mit $O(n^{1/4})$ Mult. in $\mathbb{Z}_n^*$.

Aufgabe 2. Zeige: Alg. 3.14 findet Primteiler p von $n \in \mathbb{N}$ mit B-glattem $p-1$ in $O(B \ln n / \ln B)$ Mult. in $\mathbb{Z}_n^*$. Wie gross ist der $O(1)$ -Faktor ?

Aufgabe 3. Zerlege $n = 4303$ mit Alg. 3.14 und $B = 3$. Es gilt $n = p \cdot q$ mit p ist 3-glatt.

Punktzahl 5 Punkte für Aufgabe 1, 2 und 7 Punkte für Aufgabe 3.