

Wintersemester 2013/14

Elementare Zahlentheorie**Präsenzübungen 6****Aufgabe 1:** Was spricht gegen die Verwendung von

- 13979
- 36863

als RSA-Module (außer der Tatsache, dass sie für praktische Zwecke zu klein sind)?

Aufgabe 2: Wieviele Rechenoperationen erfordert eine RSA-Verschlüsselung mit Verschlüsselungsexponent $s = 2^{16} + 1$?**Aufgabe 3:** Zeigen Sie: n ist genau dann eine Primzahl, falls $\varphi(n) = n - 1$.**Aufgabe 4:** Zeigen Sie: 91 ist ein Fermat'sche Pseudoprimzahl zur Basis 3.