

Universität Tübingen, WS 13/14

Bernd Borchert

Übungen Kryptologie

Blatt 7

Aufgabe 7.1.

Faktorisieren Sie 299 mit Probedivision.

Aufgabe 7.2.

Faktorisieren Sie 3859 mit der ggT Methode. Nehmen Sie dafür die Zahl $510510 = 2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 17$

Aufgabe 7.3.

Faktorisieren Sie 247 nach der Pollard-rho Methode. Wählen Sie einen zufälligen Startwert. Entspricht Ihre Pfadlänge ungefähr dem Geburtstagsparadoxon?

Aufgabe 7.4

Faktorisieren Sie 1271 nach der Fermat Methode.