Kryptologie

Übung, LVA 405.321
C. Fuchs

11. Übungsblatt, SS 2022

01.07.2022

1. Zeige mit Hilfe des Fermat-Tests, dass $2047 = 2^{11} - 1$ zusammengesetzt ist.

2. Implementiere den Miller-Rabin-Test und bestimme damit die kleinste 512-bit Primzahl.

3. Eine Fermat-Zahl ist eine Zahl der Form $F_n = 2^{2^n} + 1$. $F_0, \ldots, F_4$ sind Primzahlen und es wurde (vor langer Zeit) vermutet, dass alle F_n prim sind. Heutzutage geht man davon aus, dass alle F_n für $n \geq 5$ zusammengesetzt sind. Benutze den Miller-Rabin-Test um zu zeigen, dass F_5 zusammengesetzt ist.

4. Teste mit dem AKS-Test, ob 7919 eine Primzahl ist.