

Übungen zur Vorlesung Kryptographie

Blatt 1

Aufgabe 1: (sagemath nutzen)

Die Aufgabe ist, das Computeralgebraprogramm `sagemath` nutzen zu lernen. Viele Übungsaufgaben in dieser Veranstaltung dürfen oder sollen mit dem Rechner gelöst werden. Deren Lösungen dürfen als `sagemath` oder `python`-Code abgegeben werden. `sagemath` ist auf den Techfak-Netboot-Rechnern installiert (also im GZI). Benutzen Sie diese, oder installieren Sie sich `sagemath` auf Ihrem Rechner, oder benutzen Sie <https://sagecell.sagemath.org>, um die folgenden Aufgaben zu lösen:

- (1) Berechnen Sie $111111^2 \bmod 100003$
- (2) Berechnen Sie den größten gemeinsamen Teiler $\text{ggT}(12345, 54321)$.
- (3) Finden Sie die kleinste vierstellige Primzahl.
- (4) Finden Sie alle $n \in \{1, 2, \dots, 1002\}$ mit $n^2 \bmod 1003 = 19$.
- (5) Wieviele verschiedene Werte hat $n^2 \bmod 101$ für $n = 1, 2, \dots, 100$?
- (6) Wieviele verschiedene Werte hat $2^n \bmod 101$ für $n = 1, 2, \dots, 100$?
- (7) Finden Sie die exakte Lösung $x \in \mathbb{R}$ von $x^3 + x = 1$.
- (8) Finden Sie die ersten 20 Dezimalstellen von $x \in \mathbb{R}$ mit $x^3 + x = 1$.

Aufgabe 2: (Multiplizieren geht schnell, Faktorisieren kann dauern...)

- (a) Berechnen Sie $11111111111111111111111111111111 \cdot 11111111111111111111111111111111$
(29 Einsen und 31 Einsen) und
 $111 \cdot 111$
(41 Einsen und 43 Einsen)
- (b) Finden Sie die Primfaktorzerlegung der folgenden Zahlen:

12345679012345679012345679020020987654320987654320987654921

12345679012345679012345679012345679012433198765432098765432098765432098765432105611

Aufgabe 3: (Known plaintext-Angriff auf Vigenèrecode)

Seien die Buchstaben a,b,c,d, ...,z repräsentiert durch 0, 1, 2, ..., 25. Das Wort $m = \text{techfakstudierende}$ wurde mit dem Vigenèrecode mit einem Schlüssel k zu $EEOIIAVSFVGI\text{PRQOGE}$ verschlüsselt. Das Wort m' wurde leichtsinnigerweise mit demselben Schlüssel k als $c' = \text{TNFFOLTGQOWEDYEUHMP}$ verschlüsselt. Wie lautet m' ? Wie lautet k ?

Aufgabe 4: (Fast alle)

Welche der folgenden Aussagen sind wahr, welche falsch? Begründen Sie Ihre Antwort durch eine Grenzwertberechnung!

- (a) Fast alle natürlichen Zahlen sind keine Zehnerpotenzen.
- (b) Fast alle natürlichen Zahlen enthalten eine 0 als Ziffer.
- (c) Fast alle natürlichen Zahlen sind nicht durch 1000 teilbar.
- (d) Fast alle natürlichen Zahlen enthalten alle Ziffern 0,1,2,3,4,5,6,7,8,9.