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. Installieren Sie `sagemath` auf Ihrem Rechner und benutzen Sie es dort, oder benutzen Sie `https://sagecell.sagemath.org`, um die folgenden Aufgaben zu lösen:

(1) Berechnen Sie $111111^{11} \bmod 100001$
(2) Berechnen Sie den größten gemeinsamen Teiler ggT(44511,444666).
(3) Finden Sie die kleinste fünfstellige Primzahl.
(4) Finden Sie alle $n \in \{1, 2, \ldots, 1002\}$ mit $n^2 \bmod 1003 = 17$.
(5) Wieviele verschiedene Werte hat $n^2 \bmod 91$ für $n \in \mathbb{N}$?
(6) Wieviele verschiedene Werte hat $2^n \bmod 91$ für $n \in \mathbb{N}$?

Aufgabe 2: (Multiplizieren geht schnell, Faktorisieren kann dauern...)
(a) Berechnen Sie 11111111111111111111111111111 · 1111111111111111111111111111111
(29 Einsen und 31 Einsen) und
1111111111111111111111111111111111111111 · 11111111111111111111111111111111111111111
(41 Einsen und 43 Einsen)

(b) Finden Sie die Primfaktorzerlegung der folgenden Zahl (egal wie):

1524157875323883675049535156256668194788340189977090382099957323531120560885224538947063 7

Aufgabe 3: (Known plaintext-Angriff auf Vigenérecode)
Seien die Buchstaben a,b,c,d, ...,z repräsentiert durch $0, 1, 2, \ldots, 25$. Das Wort m =techfakstudierende wurde mit dem Vigenérecode mit einem Schlüssel k zu EEOIIAVSFVGIPRQOGE verschlüsselt. Das Wort m' wurde leichtsinnigerweise mit demselben Schlüssel k als c'=TNFFOLTGQOWEDYEUHMP verschlüsselt. Wie lauetet 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 enthalten keine 6 als Ziffer.
(d) Fast alle natürlichen Zahlen enthalten alle Ziffern 0,1,2,3,4,5,6,7,8,9.

Abgabe bis Mittwoch 22.4.2026 bis 12:00 Uhr per Email an die Tutorin.
Bitte auf jeder Abgabe das Tutorium angeben!

Lisa Henetmayr Mi 12 Uhr in S0-115 lhenetmayr+krypto@techfak.de
Lisa Henetmayr Mi 16 Uhr in U2-147 lhenetmayr+krypto@techfak.de