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^{11} mod 100001
(2) Berechnen Sie den größten gemeinsamen Teiler ggT(123123,456456).
(3) Finden Sie die kleinste vierstellige Primzahl.
(4) Finden Sie alle $n \in \{1, 2, \ldots, 1002\}$ mit $n^2 \bmod 1003 = 19$.
(5) Wieviele verschiedene Werte hat n^2 mod 61 für $n \in \mathbb{N}$?
(6) Wieviele verschiedene Werte hat 2^n mod 61 für $n \in \mathbb{N}$?

Aufgabe 2: (Multiplizieren geht schnell, Faktorisieren kann dauern...)
(a) Berechnen Sie $11111111111111111111111111111 \cdot 11111111111111111111111111111$
(29 Einsen und 31 Einsen) und
$1111111111111111111111111111111111111111 \cdot 1111111111111111111111111111111111111111111$
(41 Einsen und 43 Einsen)

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

$$123456790123456790123456790200209876543209876543209876549 21$$

$$12345679012345679012345679012345679012433198765432098765432098765432098765432105611$$

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 sind nicht durch 1000 teilbar.
(d) Fast alle natürlichen Zahlen enthalten alle Ziffern 0,1,2,3,4,5,6,7,8,9.

Abgabe bis Dienstag 16.4.2024 bis 23:59 Uhr per Email an den Tutor.
Bitte auf jeder Abgabe das Tutorium angeben!

Jakob Niermann	Mi 16 Uhr in T2-233	janiermann+krypto@techfak.de
Enrico di Gaspero	Do 16 Uhr in U2-216	edigaspero+krypto@techfak.de
Lisa Henetmayr	Fr 10 Uhr in X-E0-205	lhenetmayr+krypto@techfak.de
Richard Freidhof	Fr 12 Uhr in T2-141	rfreidhof+krypto@techfak.de