Dr. Dirk Frettlöh 5.4.2023

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, oder benutzen Sie `https://sagecell.sagemath.org`, um die folgenden Aufgaben zu lösen:

(1) Berechnen Sie $54321^{123456} \bmod 654321$
(2) Berechnen Sie den größten gemeinsamen Teiler ggT(123123, 456456).
(3) Finden Sie die kleinste sechsstellige Quadratzahl.
(4) Finden Sie alle $n \in \{1, 2, \ldots, 1000\}$ mit $n^2 \bmod 1001 = 23$.
(5) Wieviele verschiedene Werte hat $n^2 \bmod 61$ für $n = 1, 2, \ldots, 60$?
(6) Wieviele verschiedene Werte hat $2^n \bmod 61$ für $n = 1, 2, \ldots, 60$?

Aufgabe 2: (Multiplizieren geht schnell, Faktorisieren kann dauern...)
(a) Berechnen Sie das folgende Produkt (43 Siebenen und 41 Siebenen)

$$7777777777777777777777777777777777777777777 \cdot 77777777777777777777777777777777777777$$

(b) Finden Sie die Primfaktorzerlegung der folgenden Zahl:

60493827160493827160493827160493827160493840183950617283950617283950617283950617283951219

Aufgabe 3: (Known plaintext-Angriff auf Vigenère)
Seien die Buchstaben a,b,c,d, ...,z repräsentiert durch $0, 1, 2, \ldots, 25$. Das Wort m =leibniz wurde mit dem Vigenère-Verfahren (siehe Vorlesung) mit einem Schlüssel k zu CWISFIQ verschlüsselt. Das Wort m' wurde leichtsinnigerweise mit demselben Schlüssel k als c'=CSGISNXW 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 nicht durch drei teilbar.
(b) Fast alle natürlichen Zahlen sind keine Zweierpotenzen.
(c) Fast alle natürlichen Zahlen sind Quadratzahlen.
(d) Fast alle natürlichen Zahlen enthalten eine 7 als Ziffer.

Abgabe bis Dienstag 11.4.2023 bis 23:59 Uhr per Email an den Tutor.
Bitte auf jeder Abgabe das Tutorium angeben!

Jakob Niermann janiermann+krypto@techfak.de
Tim Lakämper tlakaemper+krypto@techfak.de