Dr. Dirk Frettlöh 4.4.2022

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 57401^{17} 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 71 für $n = 1, 2, \ldots, 70$?
(6) Wieviele verschiedene Werte hat 2^n mod 71 für $n = 1, 2, \ldots, 70$?

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

$$1111111111111111111111111111111111111111111 \cdot 11111111111111111111111111111111111111111$$

(b) Finden Sie die Primfaktorzerlegung der folgenden Zahl:

$$12345679012345679012345679012345679012433198765432098765432098765432098765432105611$$

Aufgabe 3: (Known plaintext-Angriff auf One-Time-Pad)
Seien die Buchstaben a,b,c,d, ...,z repräsentiert durch $0, 1, 2, \ldots, 25$. Das Wort m =turing wurde mit dem One-Time-Pad-Verfahren (siehe Vorlesung) mit einem Schlüssel k zu XHZOZG verschlüsselt. Das Wort m' wurde leichtsinnigerweise mit demselben Schlüssel k als c'=WUISUR 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 Zweierpotenzen.
(b) Fast alle natürlichen Zahlen enthalten eine 7 als Ziffer.
(c) Fast alle natürlichen Zahlen sind nicht durch drei teilbar.
(d) Fast alle natürlichen Zahlen enthalten alle Ziffern 0,1,2,3,4,5,6,7,8,9.

Abgabe bis Montag 11.4.2022 bis 14 Uhr per Email an den Tutor.
Bitte auf jeder Abgabe das Tutorium angeben!

Jan-Philipp Brünger jbruenger@techfak.de
Simon Hahm shahm+krypto@techfak.de
Tim Lakämper tlakaemper+krypto@techfak.de