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 12345^{54321} mod 654321
(2) Berechnen Sie den größten gemeinsamen Teiler ggT(111 111,111 111 111).
(3) Finden Sie die kleinste fünfstellige Primzahl.
(4) Finden Sie alle $n \in \{1, 2, \ldots, 1000\}$ mit n^2 mod $1001 = 23$.
(5) Wieviele verschiedene Werte hat n^2 mod 61 für $n = 1, 2, \ldots, 60$?
(6) Wieviele verschiedene Werte hat 2^n mod 61 für $n = 1, 2, \ldots, 60$?

Aufgabe 2: (Multiplizieren geht schnell, Faktorisieren kann dauern...)
(a) Berechnen Sie das folgende Produkt (43 Einsen und 47 Einsen)

1111111111111111111111111111111111111111111·11111111111111111111111111111111111111111111111

(b) Finden Sie die Primfaktorzerlegung der folgenden Zahl:

152415787532388367504953515625666819478834018997709038209995732353112056088522453894706 37

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 =mnebel wurde mit dem One-Time-Pad-Verfahren (siehe Vorlesung) mit einem Schlüssel k zu GOYOXF verschlüsselt. Das Wort m' wurde leichtsinnigerweise mit demselben Schlüssel k als c'=JLLREF 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 ungerade.
(b) Fast alle natürlichen Zahlen sind ungleich 3 modulo 1000.
(c) Fast alle natürlichen Zahlen sind keine Quadratzahlen.
(d) Fast alle natürlichen Zahlen enthalten eine 3 als Ziffer.

Abgabe bis Mittwoch 21.4.2021 bis 14 Uhr per Email an den Tutor.
Bitte auf jeder Abgabe das Tutorium angeben!

Jan-Philipp Brünger jbruenger@techfak.de
Leonard Ellinghaus lellinghaus+krypto@techfak.de
Kallias Stoupas kstoupas+krypto@techfak.de