Dr. Dirk Frettlöh 3.4.2019

Übungen zur Vorlesung Kryptographie

Blatt 1

Aufgabe 1: (One time pad knacken)
Seien die Buchstaben a,b,c,d, ...,z binär repräsentiert durch 00000, 00001, 00010, 00011, 00100, ... 11001. Finden Sie $k \in \{0,1\}^{20}$, so dass das One-Time-Pad-Verfahren (Bsp 1.4 im Skript, die Binärvariante mit XOR) den Klartext m=lisa als $c = f(k,m)$ =OLAF verschlüsselt.

Das Wort m' wurde leichtsinnigerweise mit demselben Schlüssel k als c'=PDDO verschlüsselt. Wie lauetet m'?

Aufgabe 2: (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 3 als Ziffer.
(c) Fast alle natürlichen Zahlen sind nicht durch 10 teilbar.
(d) Fast alle natürlichen Zahlen enthalten alle Ziffern 0,1,2,3,4,5,6,7,8,9.

Aufgabe 3: (Faktorisieren)
Zerlegen Sie diese Zahl in ihre beiden Primfaktoren:

12345679012345679012345679012345679012345679018786543209876543209876543209876543209876543209 88111

Alles ist erlaubt: Computer, googeln, Onlinetools....

Aufgabe 4: (ggT)
(a) Berechnen Sie den ggT (größter gemeinsamer Teiler) von 1003 und 1717. Finden Sie $a, b \in \mathbb{Z}$ mit $a \cdot 1003 + b \cdot 1717 = \text{ggT}(1003, 1717)$

(b) Berechnen Sie den ggT (größter gemeinsamer Teiler) von 377 und 610. Finden Sie $a, b \in \mathbb{Z}$ mit $a \cdot 377 + b \cdot 610 = \text{ggT}(377, 610)$

Alle Aufgaben dürfen auch mit dem Computer gelöst werden. Falls Sie Programmcode abgeben, beschreiben Sie auf jeden Fall auch, wie Sie vorgingen.

Abgabe: Mittwoch 10.4.2019 bis 14 Uhr in Postfach 2183 in V3, oder per Email an den Tutor.
Bitte auf jeder Abgabe das Tutorium angeben! (Di oder Do)

Philipp Braukmann pbraukmann@techfak.uni-bielefeld.de
Oliver Tautz otautz@techfak.uni-bielefeld.de