Aufgabenblatt 2
Sicherheit digitaler Systeme

Institut: Berliner Hochschule für Technik
Dozent: Prof. Dr. Christian Forler
Url: `https://lms.bht-berlin.de/`
Email: `cforler(at)bht-berlin.de`
Wintersemester 23/24

Aufgabe 1 Schlüssellänge
Momentan besitzt das soziale Netzwerk Facebook ungefähr 1 Mrd. ($\approx 2^{30}$) Mitglieder. Gehen sie davon aus, dass die Hälfte der Nutzer jeweils ein Programm auf ihrem Rechner besitzt, das innerhalb von 15 Minuten 2^{39} Schleifen durchläuft schafft.

a) Berechnen Sie, wie viele Durchläufe ein Programm auf einem einzelne Rechner innerhalb von 1 Stunde, 1 Tag, 1 Woche, 1 Monat und 1 Jahr schafft.

b) Berechnen Sie die Werte aus Aufgabe a) für den Fall, dass alle Facebook-Nutzer mit solch einem Rechner/Programm parallel arbeiten.

c) Unter einem "Brute-Force"-Angriff auf ein Verschlüsselungsverfahren versteht man das vollständige Ausprobieren aller möglichen Schlüssel. Angenommen pro Schleifendurchlauf kann ein Schlüssel getestet werden. Berechnen Sie, welche maximale Schlüssellänge innerhalb von 1 Stunde, 1 Tag, 1 Woche, 1 Monat und 1 Jahr geknackt werden kann für folgende Szenarien:

   - ein Facebook-Nutzer lässt das Programm laufen.
   - die Hälfte aller Facebook-Nutzer lassen das Programm parallel laufen.

d) Es gilt wieder, ein Schlüssel kann in einem Schleifendurchlauf getestet werden. Wie lange braucht **ein Nutzer**, um eine Chiffre mit Schlüssellänge 56, 80 bzw. 128 Bit zu knacken?

Aufgabe 2 One-Time-Pad (OTP) **(8 Punkte)**

Eve hat zwei Chiffretexte (C1 und C2) die mit dem gleichen OTP-Schlüssel chiffriert wurden abgefangen. Eve hat schon die bitweise XOR-Differenz der beiden Chiffretexte als Dezimalzahlen berechnet.

$C1 \oplus C2 =$
`[17, 4, 1, 26, 0, 24, 23, 23, 10, 1, 28, 19, 19, 15, 20, 30, 6, 11, 4, 8, 17, 29, 23, 1, 24, 23, 28, 17, 20, 18, 9, 27, 17, 13, 13, 10, 13, 18, 7, 4, 22, 23, 10, 22, 13, 27, 8, 5, 28, 1, 23, 26, 19, 12, 6, 0, 8, 7, 2, 15, 0, 3, 7, 0, 9, 7, 29, 19, 19, 3, 2, 29, 27, 8, 11, 7, 0, 6, 17, 26, 10, 26, 31, 26]`

Rekonstruieren Sie die beiden Klartext-Nachrichten. Beachten Sie, dass die 26 Buchstaben des Alphabets für die Berechnung der XOR-Differenz jeweils durch 5 Bit codiert wurden, d.h. $A = 00001, B = 00010, C = 00011, ..., Z = 11010$.

(Hinweise: Eve weiß aus zuverlässiger Quelle, dass in einem der Klartexte das Wort `Kryptographie` *vorkommt. Weiter weiß sie, dass die Zeichenfolge* `Sicherheit` *in dem anderen Klartext zweimal vorkommt.)*

Aufgabe 3 Substitutionschiffre **(8 Punkte)**

Die folgenden beiden Kryptogramme sind mit einer Substitutionschiffre chriffriert worden: für beide wurde der gleiche Schlüssel verwendet.

Erstes Kryptogramm:

```
GPSBO NLPZB RPJIN LPRZE KNLPR ZFKHJ RPBPZ CHKSY PWYIL ZPCPZ ZYZR
BJPBB NLHOP BBPHB TOPZY BNLHO PBBPH Z
```

Zweites Kryptogramm:

```
PBRBY QKLSQ RSHRP XPZJK BHPXP ZZRNL YQPRH QRSKZ BHPXP ZBIZJ PSZQP
RHQRS KZBHR PXPZA PQIPL ZYBRZ JPBRB YRFFP SPYQK BQKLZ BRZZR ZJPSH
RPXPP BRBYK XPSRF FPSKO NLPYQ KBGPS ZOZEY RFQKL ZBRZZ
```

a) Ermittle (z.B. durch Zählen oder mit einem kleinen Computerprogramm) die relative Häufigkeiten der einzelnen Buchstaben in diesen Kryptogrammen. Welches ist der häufigste, welches der zweit- bzw. dritthäufigste Buchstabe.

b) Entschlüssle die beiden Kryptogramme. Als Hinweis sei verraten, dass eines von ihnen mit dem Klartext-Fragment “Versuchen” beginnt.

Buchstabe	Häufigkeit	Buchstabe	Häufigkeit
A	6.51%	N	9.78%
B	1.89%	O	2.51%
C	3.06%	P	0.79%
D	5.08%	Q	0.02%
E	17.40%	R	7.00%
F	1.66%	S	7.27%
G	3.01%	T	6.15%
H	4.76%	U	4.35%
I	7.55%	V	0.67%
J	0.27%	W	1.89%
K	1.21%	X	0.03%
L	3.44%	Y	0.04%
M	2.53%	Z	1.13%

Tabelle 1: Relative Buchstabenhäufigkeiten in der deutschen Sprache (Quelle: Beutelspacher, Kryptologie, S. 18).