

4. Übung zur Vorlesung Kryptographie

Achtung: Wenn Sie programmieren und die Chiffretexte unten als Input verwenden möchten, brauchen Sie sie nicht abzutippen. Sie stehen in einer .txt-Datei an den bekannten beiden Orten im Web.

Aufgabe 14: Kryptanalyse einer affinen Chiffre (5 Punkte)

Der folgende Chiffretext wurde mit einer affinen Chiffre verschlüsselt. Entschlüsseln Sie ihn und beschreiben Sie möglichst genau, welche Schritte Sie dabei vorgenommen haben.

```
KQEREJEBPCPPCJCRKIEACUZBKRVPKRBCIBQCARBJCVFCUP
KRIOFKPACUZQEPBKRXPEIEABDKPBCPFCDCCAFIEABDKP
BCPFEQPKAZBKRHAIBKAPCCIBURCCDKDCCJCIDFUIXPAFF
ERBICZDFKABICBBENEFUCUPJCVKABPCYDCCDPKBCOCPERK
IVKSCPICBRKIJPKABI
```

Aufgabe 15: Kryptanalyse einer Vigenère-Chiffre (10 Punkte)

Der folgende Chiffretext wurde mit einer Vigenère-Chiffre verschlüsselt. Entschlüsseln Sie ihn und beschreiben Sie möglichst genau, welche Schritte Sie dabei vorgenommen haben.

```
KCCPKBGUFDPHQTYAVINRRTMVGRKDNBVFDETDGILTXRGUD
DKOTFMBPVGEGLTGCKQRACQCWDNAWCRXIZAKFTLEWRPTYC
QKYVXCHKFTPONCQQRHJVAJUWETMCMSPKQDYHJVDAHCTRL
SVSKCGCZQQDZXGSFRLSWCWSJTBHAFSIASPRJAHKJRJUMV
GKMITZHFPDISPZLVLGWTFPLKKEBDPGCEBSHCTJRWXBAPS
PEZQNRWXCVCYCGAONWDDKACKAWBBIKFTIOVKCGGHJVLNHI
FFSQESVYCLACNVRWBBIREPBBVFEXOSCDYGZWPFDTKFQIY
CWHJVLNHIQIBTKHJVNP IST
```

Aufgabe 16: Enigma / Stromchiffre (5 Punkte)

Die folgende Stromchiffre enthält Ideen aus der Enigma-Maschine (siehe z.B. auch <http://www.ugrad.cs.jhu.edu/~russell/classes/enigma/>).

Sei π eine feste Permutation von \mathbb{Z}_{26} . Der Schlüssel K ist ein Element aus \mathbb{Z}_{26} . Für $i \geq 1$ wird ein Schlüsselstrom-Element z_i als $z_i = (K + i - 1) \bmod 26$ definiert. Ver- und Entschlüsselung benutzen die Permutationen π und π^{-1} auf folgende Weise:

$$\begin{aligned} e_z(x) &= \pi(x) + z \bmod 26 \\ d_z(y) &= \pi^{-1}(y - z \bmod 26). \end{aligned}$$

Wir nehmen an, dass es sich bei π um die folgende Permutation handelt:

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
$\pi(x)$	23	13	24	0	7	15	14	6	25	16	22	1	19	18	5	11	17	2	21	12	20	4	10	9	3	8

Entschlüsseln Sie mit Hilfe von Brute Force folgenden Chiffretext:

```
WRTCNRLLSAFARWKXFTXCZRHNHYPDTZUUKMPLUSOXNEUDOKLXRMCBKGRCURR
```

und beschreiben Sie möglichst genau, welche Schritte Sie dabei vorgenommen haben.