Mathematisches Institut
der Universität München
Prof. Dr. O. Forster

WS 2011/12
7. Nov. 2011

Einführung in die Kryptographie

Übungsblatt 1

Aufgabe 1

Der folgende Geheimtext wurde aus einem deutschen Klartext durch einen Caesar-Shift $\sigma_d : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$, $x \mapsto x + d$, gewonnen.

```
ZJOSPLZZMHJOUBTTLYGDLPKYLPZPLILU
```

Man entschlüssele den Geheimtext und bestimme d.

Aufgabe 2

a) Für jeden Caesar-Shift $\sigma_d : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$, $x \mapsto x + d$, bestimme man die Ordnung, d.h. die kleinste ganze Zahl $r \geqslant 1$, so dass

$$\sigma_d^r = \underbrace{\sigma_d \circ \sigma_d \circ \ldots \circ \sigma_d}_{r\text{-mal}} = \mathrm{id}_{\mathbb{Z}_{26}}.$$

b) Man bestimme alle bijektiven Abbildungen der Gstalt

$$\varphi_{ab} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}, \qquad x \mapsto ax + b,$$

der Ordnung 2 (dann gilt $\varphi_{ab}^{-1} = \varphi_{ab}$).

Aufgabe 3

Das Zielalphabet $\mathfrak{B}$ einer monoalphabetischen Verschlüsselung $\sigma : \{\mathtt{A}, \mathtt{B}, ..., \mathtt{Z}\} \to \mathfrak{B}$ bestehe aus folgenden 26 Zeichen:

```
0123456789()[]{}/\+-*^#$!?
```

Der folgende Geheimtext entstand aus einem deutschen Klartext durch Verschlüsselung mittels σ.

```
\0/]1**}44^/0/4$8}029*0-)98/!082^*{^{1/{80--}2?0/4
{/^44092\70)/^?{0\}00/4{02!09?02
```

Man finde den Klartext, wobei bekannt sei, dass er das Wort `KOMMISSAR` enthält.

---

b.w.

Aufgabe 4 (CBC-Modus monoalphabetischer Verschlüsselungen)

Sei $\mathfrak{A} = \{A, B, \ldots, Z\} \cong \mathbb{Z}_{26}$ und $\sigma : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ eine Permutation. Der CBC-Modus der monoalphabetischen Verschlüsselung, die durch σ gegeben wird, ist wie folgt definiert: Sei

$$x = (x_1, x_2, \ldots, x_N) \in \mathbb{Z}_{26}^N$$

der Klartext und $y_0 \in \mathbb{Z}_{26}$ ein beliebig vorgegebenes Element. Dann ist der verschlüsselte Text $y = (y_1, \ldots, y_N)$ definiert durch

$$y_i := \sigma(x_i + y_{i-1}) \quad \text{für } i = 1, \ldots, N.$$

Hier bezeichnet + die Addition modulo 26.

(*Bemerkung.* Die Buchstaben CBC stehen für *cipher block chaining*.)

a) Man verschlüssele den Text `AAAAAAAAAAAAAAAAAAAAAAAAA` im CBC-Modus zu $\sigma = \sigma_d$ mit $d = 5, 6, 13$ und $y_0 = 3$.

b) Man zeige: Ist $\sigma = \sigma_d$ ein Caesar-Shift, so lässt sich die Entschlüsselung des CBC-Modus zu σ_d auf die Entschlüsselung eines gewöhnlichen Caesar-Shifts zurückführen.

c) Man entschlüssele den Geheimtext

`IPBRENKHRWDPHGXOXTXYHUCYHURENTCU`

der mit dem CBC-Modus eines Caesar-Shifts erzeugt worden ist.
