Wolfgang K. Seiler
Tel. 2515

A5, C201

15. Februar 2013

1. Übungsblatt Kryptologie

Aufgabe 1: *(3 Punkte)*

Bei der Übertragung einer geheimen Nachricht werden typischerweise drei Kodierungsschritte ausgeführt:

1. Bei der *Quellenkodierung* wird die Nachricht für das Übertragungsmedium aufbereitet; beispielsweise können Buchstaben durch ihre ASCII-Codes ersetzt werden. Bei längeren Texten werden hier auch noch Komprimierungsverfahren angewendet.
2. Die *Kanalkodierung* sichert die Nachrich durch fehlerekennende oder fehlerkorrigierende Codes gegen Übertragungsfehler.
3. Durch kryptographische Verschlüsselung wird die Nachricht gegen Abhören geschützt.

In welcher Reihenfolge sollte man diese drei Schritte anwenden, um die Nachricht optimal zu sichern?

Aufgabe 2: *(8 Punkte)*

Jedes der folgenden Kryptogramme verschlüsselt ein deutsches Wort mit einer Caesar-Chiffre. Versuchen Sie, zu entschlüsseln!

a) `xgas` *b)* `xql` *c)* `old` *d)* `ma` *e)* `qh`

Aufgabe 3: *(6 Punkte)*

Das folgende Kryptogramm wurde durch monoalphabetische Subsdtitution erzeugt.

```
amxhq flmkh gitin qkbnn ygbst nntbq tygdi aostm
pitkr niygt msdlv tbqvt iqtmy fchsq tmdtq ztufd
ztdqm kbtmr tptsq sdl
```

Sie vermuten, daß es mit dem Wort *Kryptographie* beginnt. Rekonstruieren Sie, soweit möglich, den Klartext und den Schlüssel, d.h. die angewandte Permutation des Alphabets!

Aufgabe 4: *(3 Punkte)*

Mafia-Boss Bernardo Provenzano verschlüsselte „A“ durch die Zahl „4“ und so weiter bis zur Zahl „29“ für „Z“ und schrieb diese Zahlen dann ohne Zwischenraum hintereinander. Entschlüsseln Sie die Nachricht 64211222415242312746182115818178 !

Abgabe bis zum Freitag, dem 22. Februar 2013, um 11.55 Uhr