Wolfgang K. Seiler
Tel. 2515

A5, C201

14. September 2016

1. Übungsblatt Kryptologie

Aufgabe 1: *(2 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: *(4 Punkte)*

a) Wie viele Buchstaben bekannten Klartexts brauchen Sie, um ein Caesar-verschlüsseltes Kryptogramm zu entschlüsseln?

b) Geben Sie eine begründete Schätzung für die Anzahl der Klartextbuchstaben, die Sie zur Entschlüsselung einer beliebigen monoalphabetischen Substitution brauchen!

c) Ab wie vielen Buchstaben Klartext können Sie bei einer beliebigen monoalphabetischen Substitution sicher sein, daß Sie die Permutation angeben können?

Aufgabe 3: *(6 Punkte)*

Jedes der folgenden Kryptogramme verschlüsselt ein deutsches Wort mit einer Caesar-Chiffre. Welche dieser Kryptogramme können Sie eindeutig entschlüsseln?

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

Aufgabe 4: *(6 Punkte)*

Das folgende Kryptogramm wurde durch monoalphabetische Substitution 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 auf das Alphabet angewandte Permutation!

Aufgabe 5: *(2 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 Dienstag, dem 20. September 2016, um 15.25 Uhr