Wolfgang K. Seiler
Tel. 2515

B6, B4.08

18. Februar 2025

1. Übungsblatt Kryptologie

Aufgabe 1:

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 Nachricht 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:

Man spricht heute von einer Caesar-Chiffre, wenn die Buchstaben A–Z des Alphabets um einen festen Betrag zyklisch verschoden werden, für drei etwa als A $\to$ D, B $\to$ E, ..., X $\to$ A, Y $\to$ B, Z $\to$ C.

a) Wie viele Buchstaben bekannten Klartexts brauchen Sie mindestens, um ein Caesarverschlüsseltes Kryptogramm eindeutig zu entschlüsseln?

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

```
xgas    xql    old    ma    qh
```

c) Mafia-Boss Bernardo Provenzano verschlüsselte „A“ durch die Zahl „4“, „B“ durch „5“ und so weiter bis zur Zahl „29“ für „Z“ und schrieb diese Zahlen dann ohne Zwischenraum hintereinander. Entschlüsseln Sie seine Nachricht 64211222415242312746182115818178 !

Aufgabe 3:

a) Das folgende Kryptogramm wurde erzeugt, indem die 26 Buchstaben des Alphabets einer festen Permutation unterworfen wurden:

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

Sie vermuten, daß es sich um deutschen Klartext handelt, der mit dem Wort *Kryptographie* beginnt und daß die Permutation konstruiert wurde, indem man den ersten Buchstaben des Alphabets die Buchstaben eines Schlüsselworts (nach Streichung von Dubletten) zuordnet und danach die sonstigen Buchstaben in alphabetischer Reihenfolge. Rekonstruieren Sie, soweit möglich, den Klartext und die Permutation!

b) Ab wie vielen Buchstaben bekanntem Klartexts können Sie bei einer solchen Chiffre sicher sein, daß Sie die Permutation eindeutig bestimmen können?

c) Wie wirkt sich die Spezifikation der Permutation durch ein Schlüsselwort auf die Sicherheit aus?

Abgabe und Besprechung am Mittwoch, dem 25. Februar 2025, um 15.30 Uhr