L3 1. Verschlüsselung und Datensicherheit

1.1 Verschlüsselungsklassen

Einfache Verschlüsselungsverfahren gab es schon vor Tausenden von Jahren. Bereits im alten Ägypten wurde Kryptografie (Wissenschaft der Verschlüsselung von Informationen) eingesetzt, indem Texte in hieroglyphische Schriftsysteme übertragen wurden, die von der üblichen Darstellungsform abwichen. Im Laufe der Zeit wurde eine Vielzahl verschiedener Verschlüsselungsverfahren entwickelt, die über die Zeit immer weiter verfeinert wurden.

Grundsätzlich unterscheidet die Kryptographie zwei grundlegende Verschlüsselungsklassen: die **Transposition** und die **Substitution**.

Die Verschlüsselungsmethoden beider Verschlüsselungsklassen zählen zu den symmetrischen Verschlüsselungsverfahren. Wesentliches Merkmal dieser Verfahren ist, dass der verwendete Schlüssel sowohl dem Sender einer Nachricht als auch dem Empfänger einer Nachricht bekannt sein muss.

Daraus ergibt sich ein wesentlicher Nachteil dieser Verfahren. Der Schlüssel muss dem Empfänger der Nachricht über einen „sicheren Kanal“ übertragen werden, den es ohne Verschlüsselung aber nicht gibt. Die Geheimhaltung des Schlüssels ist somit nicht gewährleistet.

Als ein weiterer Kritikpunkt muss angeführt werden, dass die Anzahl möglicher Schlüssel äußerst gering ist. Einen effektiven Schutz vor Angriff kann auch aus diesem Grund nicht sichergestellt werden.

1.1.1 Transposition

Bei der Transposition werden die Zeichen eines zu verschlüsselnden Textes umsortiert. Jedes Zeichen bleibt unverändert erhalten. Lediglich die Stelle, an der das Zeichen steht, wird geändert.

„Gartenzaun“-Transposition

Hier werden die Buchstaben des zu verschlüsselnden Textes abwechselnd in zwei oder mehr Zeilen geschrieben. Der verwendete Schlüssel gibt die Anzahl der verwendeten Zeilen an.

Bei einem Schlüssel 3 wird der erste Buchstabe am Anfang der ersten Zeile, der zweite in der zweiten Zeile, der dritte in der dritten Zeile, der vierte wieder in der ersten Zeile geschrieben. Abschließend werden die Zeichenketten der verschiedenen Zeilen hintereinander geschrieben.

Für den Text `'DiesIstEineGeheimeBotschaft'` ergibt sich bei einem Schlüssel 4 folgende Verschlüsselung (Chiffre):

```
D   I   I   E   M   T   A
 I   S   N   H   E   S   F
  E   T   E   E   B   C   T
   S   E   G   I   O   H
```

➔ Chiffre: `DIIEMTAISNHESFETEEBCTSEGIOH`

Zur Entschlüsselung des Textes muss dieser in vier Teile aufgeteilt in vier Zeilen geschrieben und von oben nach unten gelesen werden.

1.1.2 Substitution

Bei der Substitution wird jedes Zeichen eines zu verschlüsselnden Textes durch ein anderes Zeichen ersetzt.

Caesar-Verschlüsselung

Bei der Caesar-Verschlüsselung wird jeder Buchstabe des zu verschlüsselnden Textes um eine bestimmte Zahl im Alphabet weitergeschoben. Die Anzahl der verschobenen Zeichen gibt den verwendeten Schlüssel an.

Für den Text 'DiesIstEineGeheimeBotschaft' ergibt sich bei einem Schlüssel 4 folgende Verschlüsselung (Chiffre):

```
Klartext: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Geheim:   E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
```

Chiffre: ➔ HmiwMwxImriKilimqiFsxwejx

Zur Entschlüsselung des Textes wird der geheime Schlüssel verwendet und alle Buchstaben im Geheimtext werden um diese Anzahl im Alphabet zurückverschoben.

Im digitalen Zeitalter spielen diese Verschlüsselungsmethoden keine Rolle mehr. Mit dem Aufkommen der ersten Computer entstand eine immer größere Nachfrage nach Datenverschlüsselung. Die nun als Wissenschaft betriebene Kryptographie lieferte zahlreiche Forschungsergebnisse, die einen höheren Sicherheitsstandard versprachen.