3.1 Grundlagen der Kryptographie

Verschlüsselungstechniken ermöglichen einem Sender das Verbergen von Daten, sodass ein Eindringling keine Information aus den abgefangenen Daten herauslesen kann. Der Empfänger muss in der Lage sein, die Originaldaten aus den verschlüsselten Daten wiederherzustellen.

Alle Verschlüsselungsalgorithmen haben gemein, dass dabei *etwas* durch *etwas anderes* ersetzt wird: Beispielsweise wird ein Teil eines **Klartextes** genommen und dann der entsprechende **Chiffretext** berechnet, aus dem die verschlüsselte Nachricht besteht. Ein Vertreter der *klassischen Verschlüsselung* ist die *monoalphabetische Substitution*[1]: Dabei kann jeder Buchstabe jeden anderen Buchstaben ersetzen, solange jeder Buchstabe einen eindeutigen Ersatzbuchstaben besitzt, und umgekehrt. Abbildung 1 zeigt eine mögliche Substitutionsregel, um Klartext zu verschlüsseln.

```
Buchstabe im 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
Buchstabe im Chiffretext: m n b v c x z a s d f g h j k l p o i u y t r e w q
```

Abbildung 1: Eine monoalphabetische Substitution

Die Klartextnachricht `ich liebe Sicherheit` wird nun zu `sba pscbc isbacoacsu`.

Die *modernen Verschlüsselungstechniken* werden in *symmetrische* und *asymmetrische Schlüssel* unterteilt. Bei *symmetrischen Schlüsseln* verwenden die Teilnehmer denselben Schlüssel (Private-Key) und sind geheim. In *asymmetrischen* Systemen (Public-Key Systeme) wird ein Schlüsselpaar eingesetzt: Einer dieser Schlüssel ist öffentlich bekannt (Public-Key). Der andere Schlüssel ist nur dem Besitzer bekannt (Private-Key).

[1] Siehe: Monoalphabetische Substitution – Wikipedia

