

**Alle Angaben ohne Gewähr. Keine Garantie auf Vollständigkeit oder Richtigkeit.**

<b>1</b>	<b>Einführung</b>	<b>2</b>
1.1	Ausgangspunkte für Angriffe . . . . .	2
1.2	Angriffsarten . . . . .	2
1.3	Historische Verschlüsselungsverfahren . . . . .	2

## 1 Einführung

### 1.1 Ausgangspunkte für Angriffe

Angriffe können nach den zur Verfügung stehenden Informationen unterteilt werden:

- **Ciphertext-Only-Attack:** Nur das *Chiffre*, also die verschlüsselte Nachricht, ist bekannt
- **Known-Plaintext-Attack:** Es gibt bekannte Klartext-Chiffre-Paare. Hilfreich sind bekannte Anfangs- und Endphrasen, die in mehreren Nachrichten vorkommen.
- **Chosen-Plaintext-Attack:** Es besteht die Möglichkeit, beliebige Texte zu verschlüsseln und somit Klartext-Chiffre-Paare zu erzeugen.

### 1.2 Angriffsarten

- Brute-Force (z.B. alle Schlüssel ausprobieren)
- Statistische Methoden (z.B. Häufigkeitsanalysen von Buchstaben)
- Strukturelle Angriffe (z.B. Lineare Kryptoanalyse)

### 1.3 Historische Verschlüsselungsverfahren

Historisch wurden zur Verschlüsselung zwei grundlegende Operationen verwendet:

- **Substitution**
- **Permutation**

Alleine sind beide Verfahren meistens nicht sicher, jedoch verwenden moderne Verschlüsselungsverfahren eine Kombination beider Operationen.