Kryptologie

Varianten kryptographischer Verfahren

```
a7Hzq .#5r<
kÜ\as TâÆK$
ûj(Ö2 ñw%h:
Úk{4R f~`z8
¤˜Æ+Ô „&¢Dø
```

Substitution:

Buchstaben oder Buchstabengruppen werden duch andere ersetzt.

Monoalphabetische Substitution:

Jeder Buchstabe wird stets durch das gleiche Zeichen ersetzt.

Polyalphabetische Substitution:

Jeder Buchstabe wird, abhängig von seiner Position im Text, jedesmal durch ein anderes Zeichen ersetzt. (Wichtigstes Verfahren der klassischen Kryptographie bis in die 1960er-Jahre)

Monographische Substitution:

Je ein Buchstabe wird durch ein Zeichen ersetzt.

Polygraphische Substitution:

Jeweils ein oder mehrere Buchstaben werden durch mehrere Zeichen ersetzt.

Homophone Substitution:

Für einige Klartextbuchstaben oder -buchstabengruppen gibt es verschiedene Möglichkeiten, den Geheimtext zu wählen.
Zur Modellierung führt man am besten einen Wahrscheinlichkeitsraum Ω ein und betrachtet Verschlüsselungsfunktionen

$$f_k : \mathrm{M} \times \Omega \to \Sigma^*$$

Ein solches Verfahren nennt man auch **probabilistische Chiffrierung**.

Transposition:

Die Buchstaben des Klartexts werden permutiert (durcheinandergewürfelt).

Codebuch:

Zeichenfolgen unterschiedlicher Länge (z. B. ganze Wörter) werden durch andere anhand eines Verzeichnisses ersetzt.
Beispiel: Kompression - hier wird das Verzeichnis bei gängigen Verfahren dynamisch erzeugt.
Seit der Renaissance auch unter der Bezeichnung **Nomenklator** verwendet. Meist gebrauchte Verschlüsselungsmethode bis weit ins 20. Jahrhundert. Vor allem in der Diplomatie gebräuchlich.

Quellcodierung (überverschlüsselte Codierung)**:**

Vor Anwendung einer Chiffrierung wird der Klartext nach einem Codebuch umgewandelt.

Buch-Chiffre:

Die zu verschlüsselnden Wörter oder Buchstaben werden in einem bestimmten Buch gesucht. Als Geheimtext wird dann die Position des Wortes oder Buchstabens in dem Buch genommen, also z. B. Seitennummer, Zeilennummer, Nummer des Worts (+ gegbenenfalls Nummer des Buchstabens).

Blockchiffre:
Es wird stets eine bestimmte Anzahl von Buchstaben gemeinsam substituiert.

Stromchiffre:
Jeder Buchstabe wird einzeln chiffriert.

Produktchiffre:
Nacheinanderausführung von Transpositionen und Blocksubstitutionen im Wechsel.

Autor: Klaus Pommerening, 5. November 1999; letzte Änderung: 30. Januar 2008.