 04.03.2022

# Tutorial zu Kryptografie & Kryptoanalyse

Sie lernen klassische Verschlüsselungsverfahren kennen und einordnen:
- Caesar
- Substitution
- Vigenère
- One Time Pad

Ebenfalls machen Sie Bekanntschaft mit Methoden der Kryptoanalyse:
- Brute-Force
- Häufigkeitsverteilung
- Friedman-Test

**Merkstoff ist grau markiert.** Sie sollten die vorgestellten Verfahren und ihre Schwächen kennen.

Im Text gibt es **Aufgaben**. Beantworten Sie diese schriftlich. Wenn Sie die Fragen beantworten können, haben Sie das Thema verstanden. Die Antworten werden später verglichen.

---

## Caesar-Verfahren

### Kryptoanalyse des Caesar-Verfahrens

Informieren Sie sich, wenn notwendig, noch einmal über das **Caesar-Verfahren.**

**Eine Analysemethode** für monoalphabethische Verschlüsselung nennt sich „**Brute-Force**“ (rohe Gewalt). Es werden **alle möglichen Schlüssel ausprobiert**, bis ein sinnvoller Klartext herauskommt.

**I. Nennen Sie die Anzahl der möglichen Schlüssel beim Caesar-Verfahren.**

**Substitutions-Verfahren** (→ nicht verwechseln mit der Substitution als Verschlüsselungs**typ**!! **)**

Irgendwann haben Caesars Nachfahren herausgefunden, dass das Verfahren nicht sicher ist. Wird aber die Anzahl der möglichen Schlüssel erhöht, dann würde die Kryptoanalyse durch Brute -Force erschwert werden. Dies gelingt mit dem Substitutionsverfahren.

Beim **Substitutionsverfahren** wird jeder Buchstabe des Klartextes durch einen beliebigen Buchstaben aus dem Geheimtext ersetzt („substituieren“= „ersetzen“). Es werden nicht mehr alle Buchstaben um gleich viele Stellen verschoben wie beim Caesar-Verfahren.

Damit man sich den Schlüssel gut merken kann, geht man so vor:
Die Buchstaben des Klartextalphabetes werden der Reihe nach aufgeschrieben. Darunter wird zuerst das Schlüsselwort (im Beispiel: „KRYPTO“) geschrieben und dann kommen der Reihe nach alle bisher im Schlüsselwort nicht benutzten Buchstaben des Alphabetes. Vorsicht: kein Buchstabe darf zweimal vorkommen!

Beispiel mit Schlüsselwort „**KRYPTO**“ Damit wird aus dem Klartext „**hallo**“ der Geheimtext „**BKFFI**“.

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

**II. Welchen Schlüssel müssten Sie bei diesem Verfahren eingeben, damit trotz vermeintlicher Verschlüsselung keine Verschlüsselung stattfindet?**
**Ordnen Sie das Substitutionsverfahren in die Systematik der Verschlüsselungsverfahren ein.**

 04.03.2022

## Kryptoanalyse des Substitutionsverfahrens

Das Substitutionsverfahren scheint sicher zu sein, gibt es doch theoretisch **$26! = 4 \cdot 10^{26}$** mögliche Schlüssel. Eine **Brute-Force-Analyse** dauert lange, ist aber mit heutiger Computertechnik in angemessener Zeit machbar.

Die Krypto-Analytiker haben aber noch eine andere Methode gefunden.

Die **Häufigkeitsanalyse** beruht darauf, dass **bestimmte Buchstaben einer Sprache häufiger als andere Vorkommen** und dies bei der Zuordnung von Klartext- zum Verschlüsselungsalphabet hilfreich ist. **Monoalphabetische** Verfahren sind **mit der Häufigkeitsanalyse zu knacken**.

Man kann so vorgehen:

- Man zählt wie häufig die einzelnen Buchstaben auftreten.
- Der Buchstabe, der am häufigsten auftritt, ist wahrscheinlich ein ‚e' (ausser der Text stammt aus dem Roman „**Anton Voyls Fortgang**" von Georges Perec, darin kommt kein einziges ‚e' vor…).
- Kommt ein Wort mit nur 2 Buchstaben vor, bei dem der erste Buchstabe wahrscheinlich ein ‚e' ist, so ist der 2. Buchstabe vermutlich ein ‚r'. Begründung: ‚er' ist ein häufiges Bigramm (Buchstabenpaar).
- Es können auch Häufigkeitsdaten von Trigrammen benutzt werden. Trigramme sind Folgen von 3 Buchstaben. (sch, ein, die, der, wer...)
- Hat man ein paar Buchstaben erraten ist es einfach aus dem Kontext noch weitere Buchstaben zu erraten.
- **Das Zählen der Buchstaben mit einem Computer → Word: Suchen und ersetzen→ a ersetzen durch a. usw.**

**III. Begründen Sie, warum der mittels Analyse zu entschlüsselnde Text nicht zu kurz sein darf.**

*** Zusatzaufgabe: Entschlüsseln Sie diesen Text mittels Häufigkeitsanalyse.**

### Symbolbasierte Verschlüsselungen – Ein Beispiel ist der Freimaurerkode

Informieren Sie sich hier über den **Freimaurerkode**.

**IV. Ordnen Sie den Freimaurercode in unsere Systematik ein.**

### Das Vigenére-Verfahren

Nachdem die Krypto-Analytiker das Substitutionsverfahren mittels Häufigkeitsanalyse geknackt hatten, waren die Verschlüsselungsspezialisten wieder gefragt.
Es musste eine neue Idee her, die Buchstabenhäufigkeit musste verschleiert werden.

Bei der **polyalphabetischen Verschlüsselung** ist einem Klartextbuchstaben nicht eineindeutig ein Geheimtextbuchstabe zugeordnet. („poly" = „viel") Ziel ist die Verschleierung der Buchstabenhäufigkeit.

Das bekannteste **polyalphabetische Verschlüsselungsverfahren heißt Vigenére-Verfahren**:

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | d | i | e | s | i | s | t | d | e | r | k | l | a | r | t | e | x | t |
| + | k | e | y | k | e | y | k | e | y | k | e | y | k | e | y | k | e | y |
| | O | N | D | D | N | R | E | I | D | C | P | K | L | W | S | P | C | S |

d → O, I  e → D, P

Vorgehen:
Der Schlüssel (hier „**key**") wird wiederholt unter den Klartext geschrieben.
Dann werden die Buchstaben des Klartextes und die Buchstaben des Schlüssels addiert.
Bsp: ‚**d**' (4. Buchstabe) + ‚**k**' (11. Buchstabe) = ‚**O**' (15. Buchstabe). Ist das Ergebnis größer als 26. wird vom Ergebnis 26 abgezogen und dann der Buchstabe zugeordnet. ‚**t**' (20. Buchstabe) + ‚**y**' (25. Buchst.) = ‚**S**' (45-26=19. Buchst.).
Eine verschlüsselte Nachricht wird wieder entschlüsselt, indem der Schlüssel vom Geheimtext subtrahiert wird.

**V. Verschlüsseln Sie mit dem Codewort INFOGK den Text BUDENZAUBER.**
**VI. Entschlüsseln Sie mit dem Codewort KLAUSUR den Geheimtext L B G Z E W S F Y.**

 04.03.2022

## Kryptoanalyse des Vigenère-Verfahrens

**VII. Ordnen Sie das Vigenère-Verfahren in unsere Systematik ein.**

Das Vigenére-Verfahren wurde auch als „Le chiffre indéchiffrable“ bezeichnet, weil es ohne Kenntnis des Schlüssels fast nicht zu knacken ist.

**VIII. Begründen Sie, wieso die Häufigkeitsanalyse bei Vigenére nicht funktioniert.**

Wie das Verfahren doch zu knacken ist, erfahren Sie im Video.

**IX. Erläutern Sie grob, wie ist das Knacken einer Nachricht auch bei einer polyalphabetischen Verschlüsselung möglich ist.**

## Das One-Time-Pad

Beim **One-Time-Pad** benutzt man ein **polyalphabetisches Verfahren**, bei dem der **Schlüssel mindestens so lang ist wie der Klartext**. Es ist ein **sicheres Verfahren**.

Informieren Sie sich über das **One-Time-Pad**.
**X. Notieren Sie Vor- und Nachteile der Verwendung eines One-Time-Pad-Verfahrens.**

Im praktischen Einsatz hat das One-Time-Pad aber einige gewaltige Nachteile:

- Man darf den Schlüssel nur einmal zum Verschlüsseln eines Textes benutzen. Wenn man ihn mehrfach benutzt, liefert man dem Angreifer Möglichkeiten zu einem erfolgreichen Angriff.
- Man kann sich den Schlüssel nicht merken. Er muss auf einem Medium festgehalten werden und auf sicherem Weg zwischen den Kommunikationspartnern überbracht werden.

Trotz dieser Nachteile wurde und wird das One-Time-Pad immer wieder benutzt.
So soll der "heiße Draht" zwischen dem amerikanischen und dem russischen Präsidenten durch ein Einmalschlüssel-Verfahren geschützt sein.

**XI. Ordnen Sie das One-Time-Pad in unsere Systematik ein.**