

Einführung in die Kryptologie

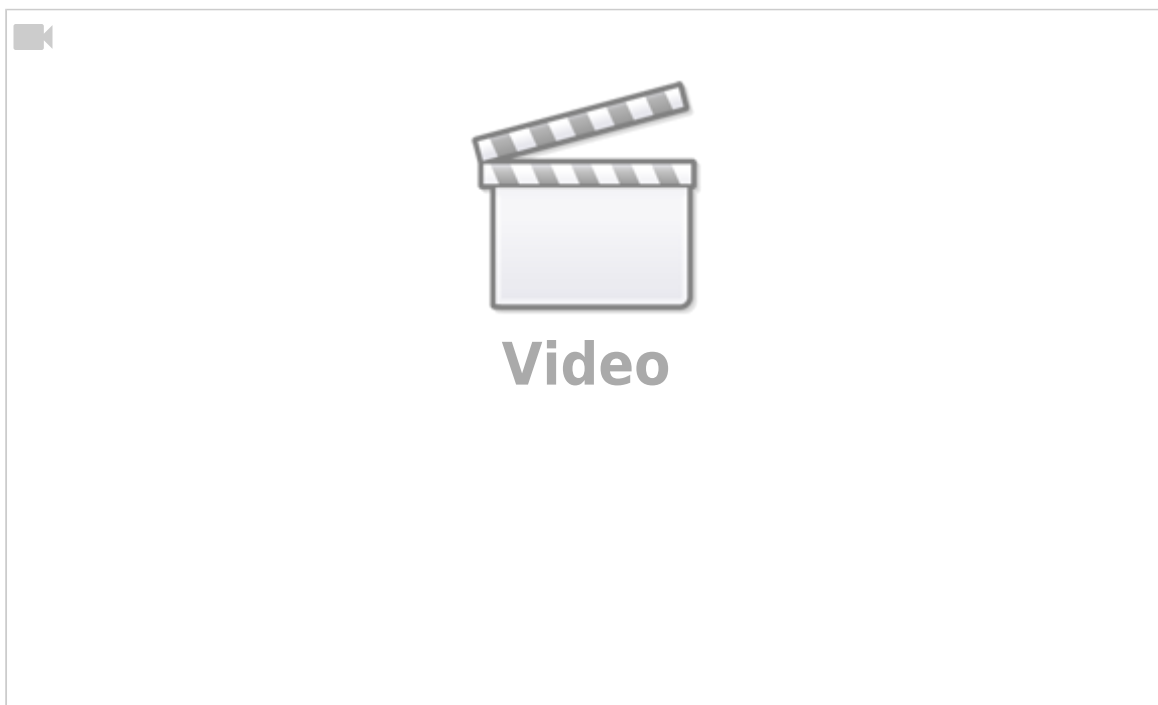
Schon vor 2500 Jahren wurden im militärischen Umfeld geheime Botschaften übermittelt, beispielsweise in Form der Skytale - die Verschlüsselung beruht auf einem **Transpositionsverfahren**.

Aufgaben

1. Recherchiere zur Skytale und notiere den historischen Kontext.
2. Beschreibe das Verschlüsselungsverfahren.
3. Nenne den Schlüssel, den Sender und Empfänger kennen müssen.
4. Bewerte die Sicherheit des Verfahrens.
5. Wie könnte die Verschlüsselung sicherer gemacht werden? Mache Vorschläge.



Jahrhunderte später vertraute Julius Cäsar keinem der Boten, die Nachrichten an seine Generäle überbrachten. Er ersetzte deshalb in seinen Nachrichten jedes A durch ein D, jedes B durch ein E usw. So verfuhr er mit dem ganzen Alphabet. Nur jemand, der die Regel des Vertauschens durch den drittnächsten Buchstaben kannte, konnte die Nachrichten entschlüsseln - er wandte das erste **Substitutionsverfahren** zur Verschlüsselung an.



<https://www.youtube.com/watch?v=VeH0KnZtljY>

Aufgaben

1. Die Cäsar-Chiffre ist ein monoalphabetisches Substitutionsverfahren. Erkläre den Begriff.
2. Grenze Substitutions- von Transpositionsverfahren ab.

3. Nenne den Schlüssel, den Sender und Empfänger kennen müssen.
4. Monoalphabetische Chiffren sind für die Kryptoanalyse keine Herausforderung - sie können leicht durch eine **Häufigkeitsanalyse** geknackt werden. Beschreibe dieses Verfahren.
5. Benutze die Informationen und Werkzeuge auf <https://www.cryptogram.org/resource-area/solve-a-cipher/> um den folgenden Geheimtext in Cäsar-Chiffre zu entschlüsseln:

```
ExoovtfoakxzeabjQlapbfkboBiqbok
xipTxfpbfkafbCueoplodpbfkbo
kfzeqjxdfpzebkQxkqbMbqrkfxIfivp
PzetbpqborkaabobkBebjxkkbpSboklk
AropibvueybodbybkAfbAropibvp
pfkaExoovpibqwqbkLzeibybkab
SbotxkaqbPfbpqbekabojxdfpzebk
Tbiqxyibekbkadbdbkueyboybexkabik
Exoovpbeopzeibzeqrkasboprzebk
afbBkqtfzhirkdpbfkbojxdfpzebk
CaeefdhbfqbkwsboefkabokAxebo
sbopzetbfdbkpfbfexrzeaftxeob
DbpzeqzbtfbpbfkbiqbokwrQlab
hxjBkpltfbafbQxqpxzebaxppExoov
bfkwxrybobofpqXrßboabjybslowrdbk
pfbfeobkPlekAraibvtlbpkro
dbeqXkExoovpbicqbjDbyroqppxd
tfoafejslk0rybrpExdofaabj
TfiaueqborkaPzeiueppbiybtxeoboabo
WxrybobopzeribEldtxoqpaafbBfkixarkd
fkaxpFkqbokxqueyboyoxzeqBopq
gbqwqbocaeoqbobqtxpueybopbfkb
EbohrkcqafbBupqbkwabodbefbjbk
jxdfpzebkMxoxiibitbiqrkapbfkb
bfdbkbbkCaeefdhbfqbkxipWxrybobo
```

Verschlüsselung und Entschlüsselung

Daten, die ohne besondere Entschlüsselungsmethoden gelesen werden können, werden *Klartext* genannt. Das Verfahren zum Chiffrieren von Klartext, so dass dessen Inhalt unerkannt bleibt, wird Verschlüsselung (= **Kryptographie**) genannt.

Verschlüsseln von Klartext ergibt ein unleserliches Zeichengewirr, das dann Verschlüsselungstext oder *Chiffre*, manchmal auch *Geheimtext* genannt wird. Mit der Verschlüsselung bleiben Informationen unbefugten Personen verborgen, selbst wenn ihnen die Daten im verschlüsselten Zustand vorliegen. Das Verfahren des Zurückführens von chiffriertem Text in den ursprünglichen Klartext wird als Entschlüsselung (= **Kryptoanalyse**) bezeichnet.



Aufgaben

1. Übernimm das Schema oben auf dieser Seite in dein Heft und ergänze an passender Stelle die kryptologischen Fachbegriffe, die du bis jetzt gelernt hast.
2. Erläutere die drei Ziele der Kryptographie (**Vertraulichkeit, Authentizität, Integrität**).
3. Bewerte die beiden dir bisher bekannten kryptographischen Verfahren im Hinblick auf die drei Ziele.

From:

<https://wiki.qg-moessingen.de/> - QG Wiki

Permanent link:

<https://wiki.qg-moessingen.de/faecher:informatik:oberstufe:kryptographie:einfuehrung:substitution:start?rev=1585232590>

Last update: **26.03.2020 15:23**

