

Einführung in die Kryptologie

Die Skytale

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



1)



(A1)

(A) Recherchiere zur **Skytale** und notiere den historischen Kontext.

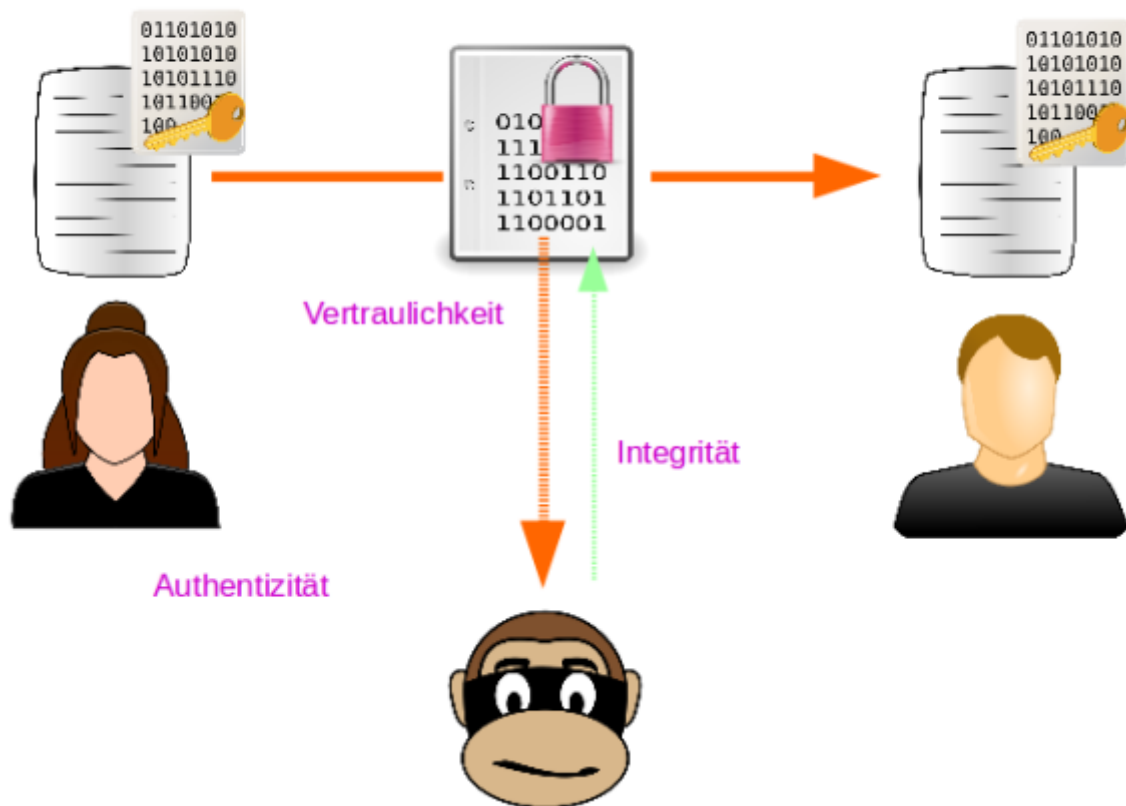
(B) Beschreibe das Verschlüsselungsverfahren: Was muss der Absender tun, um eine Nachricht zu **verschlüsseln**, was muss der Empfänger tun, um die Nachricht zu **entschlüsseln**? Nenne den **Schlüssel**, den Sender und Empfänger kennen müssen.

(C) Bewerte die Sicherheit des Verfahrens.

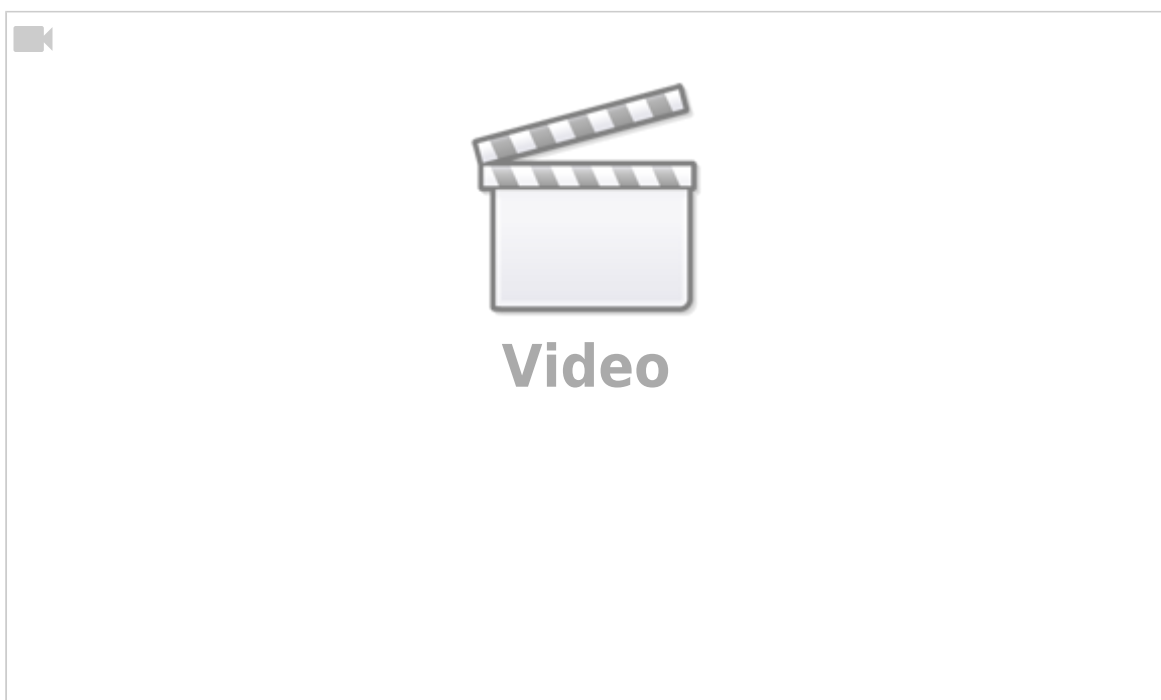
(D) Wie könnte die Verschlüsselung sicherer gemacht werden? Mache Vorschläge.

Grundbegriffe

Grundproblem und Ziele der Kryptographie



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  
xipTxfpbfkafbCueoplodbpbfbkbo  
kfzeqjxdfpzebkQxkqbMbqrkfxIfivp  
PzetbpqborkaabobkBebjxkkbpSboklk  
AropibvueybodbybkAfbAropibvp  
pfkaExoovpibqwbklzeibybkb  
SbotxkaqbPfbpqbebkabojxdfpzebk  
Tbiqxyibekbkadbdbkueyboybexkabik  
Exoovpbeopzeibzeqrkasboprzebk  
afbBkqtfzhirkdpbfkbojxdfpzebk  
CaefdhhbfqbkwsboefkabokAxebo  
sbopzetbfdbkpfbfexrzeaftxeob  
DbpzeqzeqbtfbpbfbkbiqbokwrQlab  
hxjbkpltfbafbQxqpxzebaxppExoov  
bfkWxrybobofpqXrßboabjybslowrdbk  
pfbfeobkPlekAraibvtlbpkro  
dbeqXkExoovpbicqbjDbyroqpqxd  
tfoafejslkOrybrpExdofaabj  
TfiaueqborkaPzeiueppbiybtxeoboabo  
WxrybobopzeribEldtxoqpafbBfkixarkd  
fkaxpFkqbokxqueyboyoxzeqBopq  
gbqwbocaeeoqbobqtxpueybopbfkb  
EbohrkcqafbBufpqbkwabodbebfjbk  
jxdfpzebkMxoxiibitbiqrkapbfkb  
bfdbkbkCaefdhhbfqbkxipWxrybobo
```

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



- 1)
Bildquelle: <https://commons.wikimedia.org/wiki/File:Skytale.png>, Lizenz: Creative Commons Attribution-Share Alike 3.0 Unported

