

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

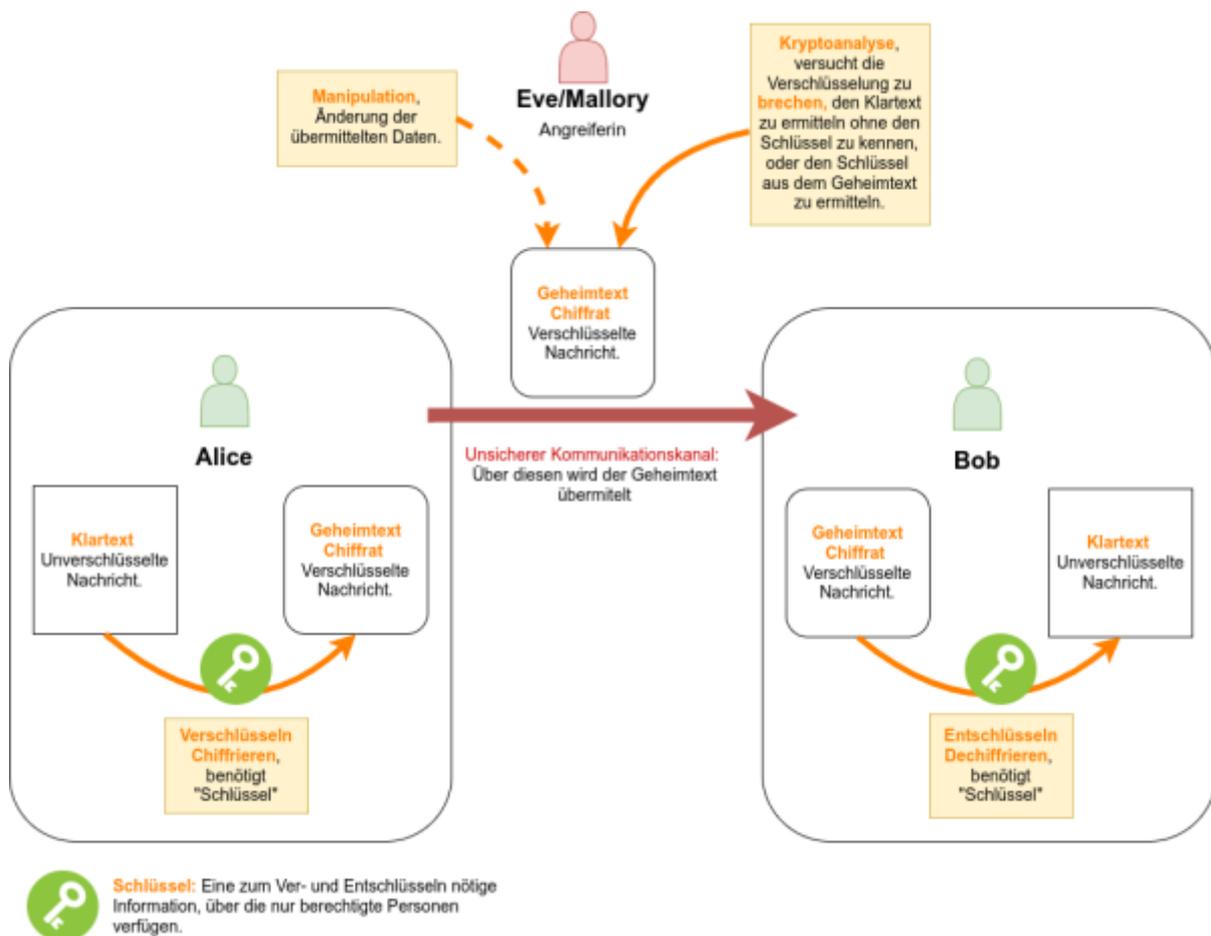
Die folgende Grafik ist eine Darstellung einer Miniwelt, welche die Situation zur Untersuchung verschlüsselter Kommunikation gut darstellt. Alice möchte mit Bob über einen unsicheren Kanal (z.B. das Internet) kommunizieren, ohne dass Eve (Eavesdropping, "abhören", manchmal auch Mallory) diese Kommunikation verstehen kann.

Die Nachricht liegt beim Sender zunächst als **Klartext** vor und wird von diesem mit Hilfe eines

Schlüssels verschlüsselt und damit in einen **Geheimtext** umgewandelt. Dieser Geheimtext lässt sich nur von einer Person zurück in den Klartext **entschlüsseln**, die ihrerseits über einen passenden **Schlüssel** verfügt.

Wenn Eve in den Besitz des Geheimtexts kommt, kann sie versuchen, durch **Kryptoanalyse** den Klartext - oder zunächst den Schlüssel - zu ermitteln. Außerdem könnte Sie versuchen, die übermittelten Informationen zu manipulieren.

Da Bob über den korrekten **Schlüssel** zur **Dechiffrierung** des **Geheimtexts** verfügt, kann er den Geheimtext entschlüsseln, um den Klartext zu erhalten. So kann er die Nachricht lesen, die Alice ihm geschickt hat.



(A2)

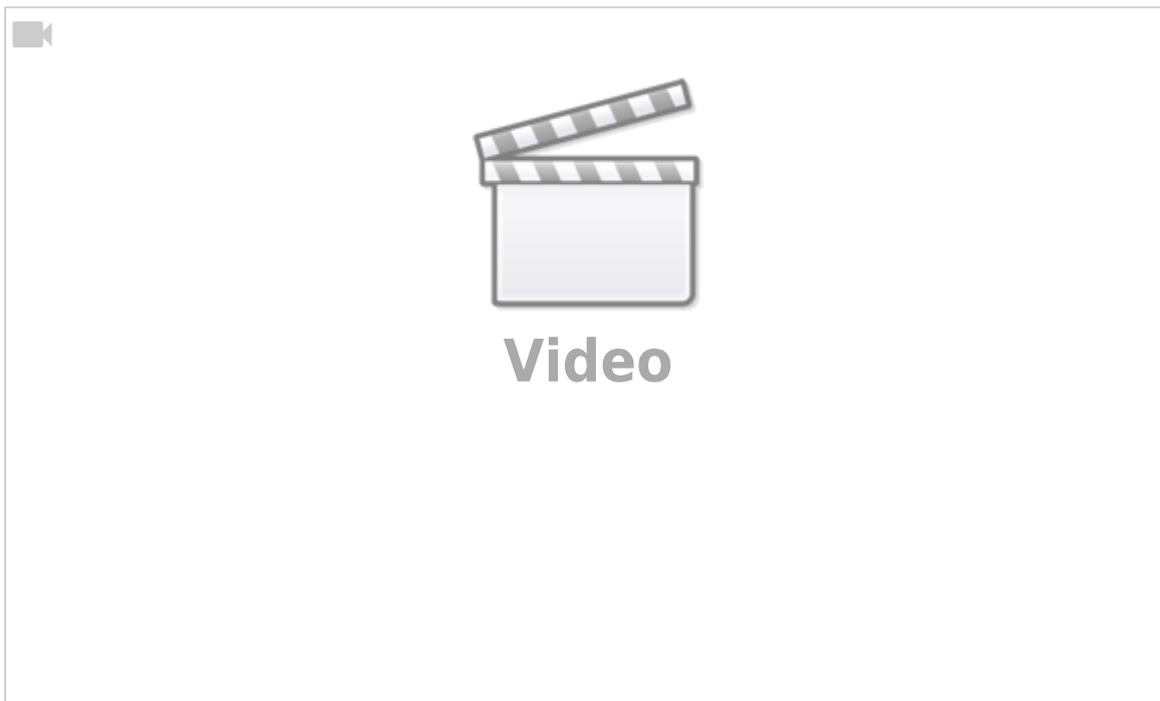
Analysiere die Grafik und erstelle einen Heftaufschrieb mit allen **Fachbegriffen**, denen du in der Grafik begegnest. Es reicht aus, eine Liste mit den Fachbegriffen und kurzen Erklärungen zu haben.



(A3)

Die Cäsar Verschlüsselung

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
xipTxfpbfkafbCueoplodbpbkbo
kfzeqjxdfpzebkQxkqbMbqrkfxIfivp
PzetbpqborkaabobkBebjxkkbpSboklk
AropibvueybodbybkAfbAropibvp
pfkaExoovpibqwqbkklzeibybkab
SbotxkaqbPfbpqbebkabojxdfpzebk
  
```


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

From:
<https://www.info-bw.de/> -

Permanent link:
<https://www.info-bw.de/faecher:informatik:oberstufe:kryptographie:einfuehrung:substitution:start?rev=1645463804>

Last update: **21.02.2022 17:16**

