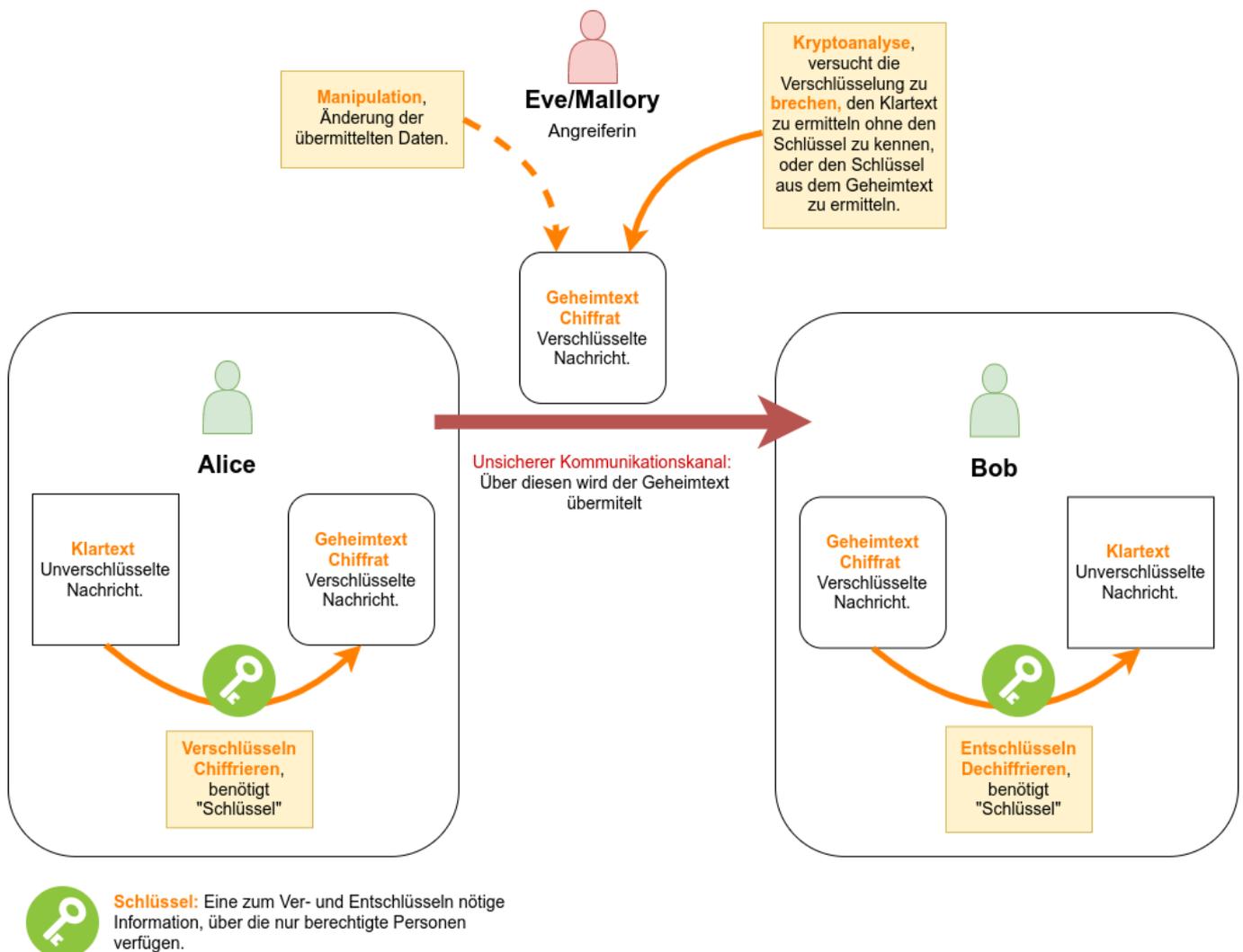


Schlüssels verschlüsselt und damit in einen **Geheimtext** umgewandelt. Dieser Geheimtext lässt sich nur von einer Person zurück in den Klartext **entschlüsseln**, die ihrerseits über einen passenden **Schlüssel** verfügt.

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.

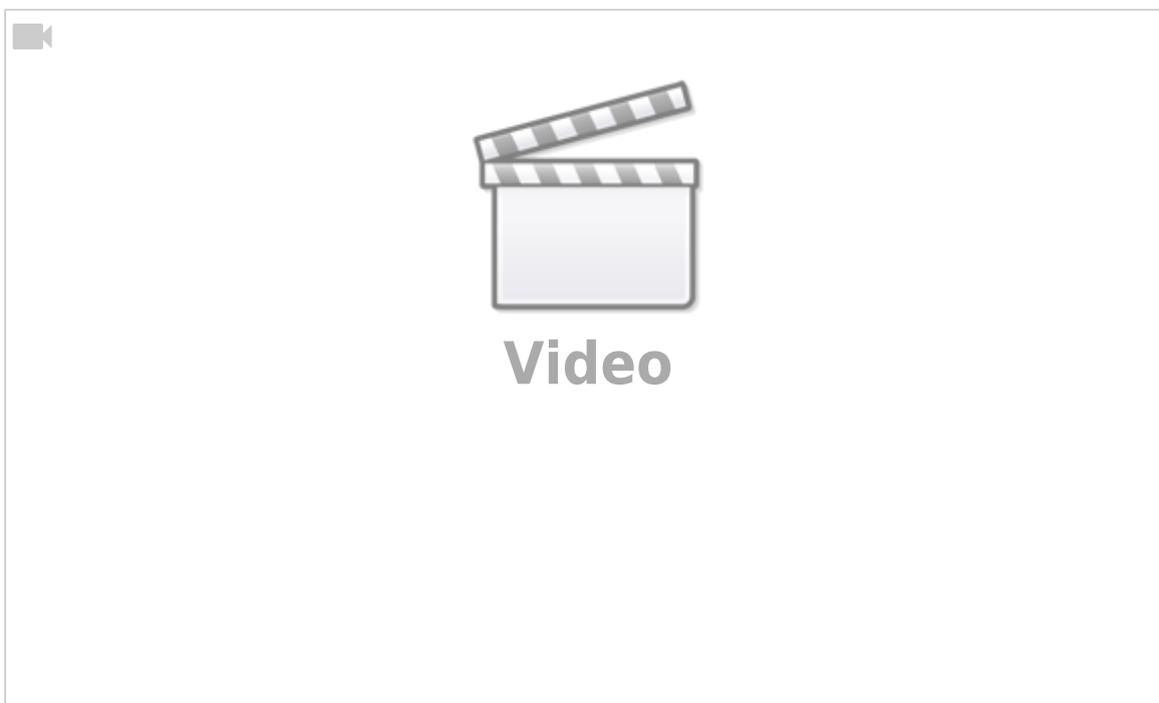


(A2)

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.

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=VeH0KnZtjY>



(A3)

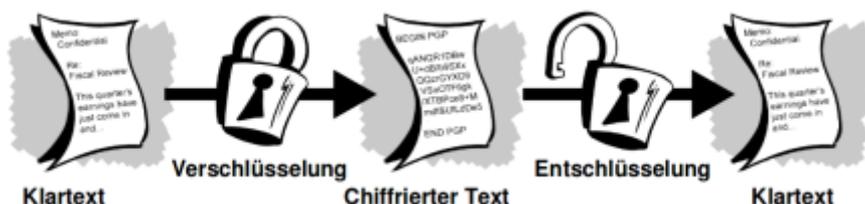
- (A)** Die Cäsar-Chiffre ist ein monoalphabetisches Substitutionsverfahren. Erkläre den Begriff.
- (B)** Grenze Substitutions- von Transpositionsverfahren ab.
- (C)** Nenne den Schlüssel, den Sender und Empfänger bei der Cäsar Chiffre kennen müssen.
- (D)** Monoalphabetische Chiffren sind für die Kryptoanalyse keine Herausforderung - sie können leicht durch eine **Häufigkeitsanalyse** geknackt werden. Beschreibe dieses Verfahren.
- (E)** 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
pfkaExoovpibqwqbkklzeibybkab
SbotxkaqbPfbpqbekabojxdfpzebk
Tbiqxyibekbkadbdbkueyboybexkabik
Exoovpbeopzeibzeqrkasboprzebk
afbBkqtfzhirkdpbfkbojxdfpzebk
CaefdhhbfqbkwrsboefkabokAxebo
sbopzetbfdbkpfbfexrzea fbtxeob
Dbpze fzeqbtfbpbfbkBiqbokwrQlab
hxjbkpltfbafbQxqpxzebaxppExoov
bfkwxrybobofpqXrßboabjybslowrdbk
pfbfeobkPlekAraibvtlbpkro
dbeqXkExoovpbicqbjDbyroqpxd
tfoafej slk0rybrpExdofaabj
TfiaueqborkaPzeiueppbiybtxeoboabo
WxrybobopzeribEldtxoqpa fbBfkixarkd
fkaxpFkqbokxqueyboyoxzeqBopq
gbqwqbocaeoqbobqtxpueybopbfkb
EbohrkcqafbBufpqbkwabodbebfjkb
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 unerkant bleibt, wird Verschlüsselung (= **Kryptographie**) genannt.

Verschlüsseln von Klartext ergibt ein unleserliches Zeichengewirr, das dann Verschlüsselungstext oder *Chifftrat*, 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.

1)

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

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

Permanent link:
<https://info-bw.de/faecher:informatik:oberstufe:kryptographie:einfuehrung:substitution:start?rev=1645464055>

Last update: **21.02.2022 17:20**

