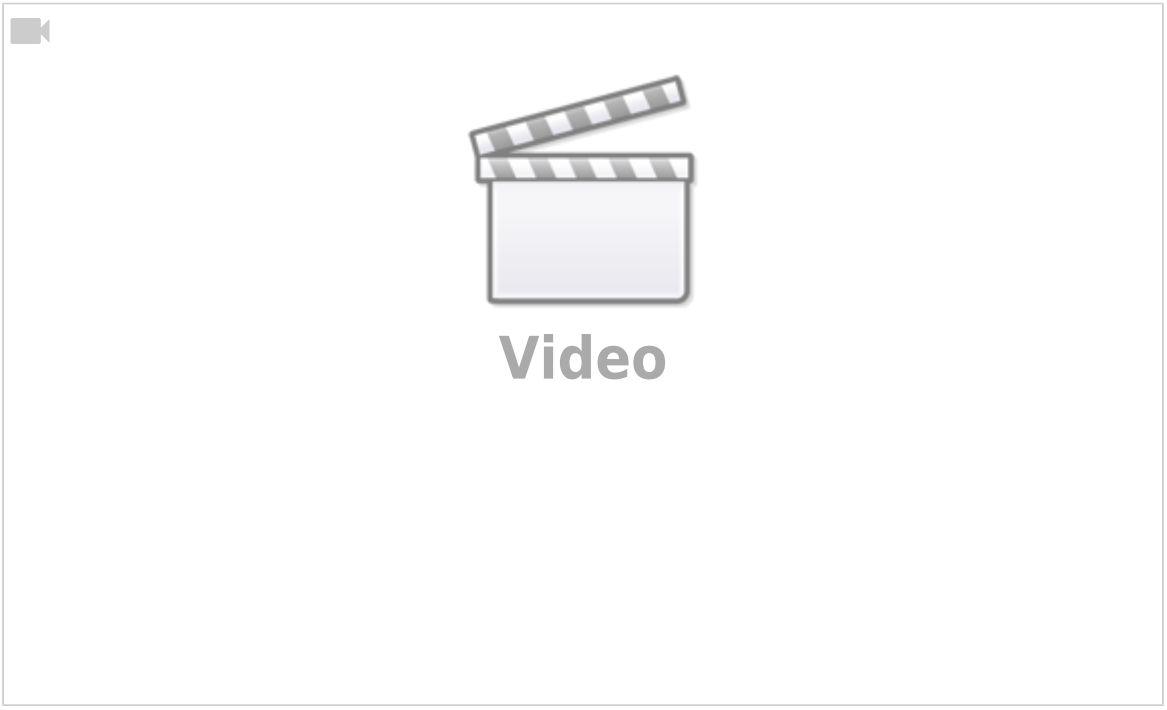
Einführung in die Kryptologie

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
 xipTxfpbfkafbCueoplodbpbfkbo
 kfzeqjxdfpzebkQxkqbMbqrkfxIfivp
 PzetbpqborkaabobkBebjxkkbpSboklk
 Aropibvueybodbybk AfbAropibvp
 pfkaExoovpibqwqbklzeibybkab
 SbotxkaqbPfbpqbebkabojxdfpzebk
 Tbiqxyibekbkadbdbkueyboybexkabik
 Exoovpbeopzeibzeqrkasboprzebk
 afbBkqtfzhirkdpbfkbojxdfpzebk
 CaeefdhbfqbkwrsboefkabokAxebo
 sbopzetbfdbkpfbfejxrzeafbtxeob
 DbpzefzeqbtfbpbfkbBiqbokwrQlab
 hxjbkpltfbafbQxqpxzebaxppExoov
 bfkWxrybobofpqXrßboabjybslowrdbk
 pfbfeobkPlekAraibvtlbpkro
 dbeqXkExoovpbicqbjDbyroqpqxd
 tfoafejslkOrybrpExdofaabj
 TfiaeueqborkaPzeiueppbiybtxeoboabo
 WxrybobopzeribEldtxoqpafbBfkixarkd
 fkaxpFkqbokxqueyboyoxzeqBopq
 gbqwqbocaeeoqbobqtxpueybopbfkb
 Ebohrkcqafb Bufpqbkwabodbebfjbk
 jxdfpzebkMxoxiibitbiqrkapbfkb
 bfdbkbkCaeefdhbfqbkxipWxrybobo
```

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 *Chiffrat*, 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.

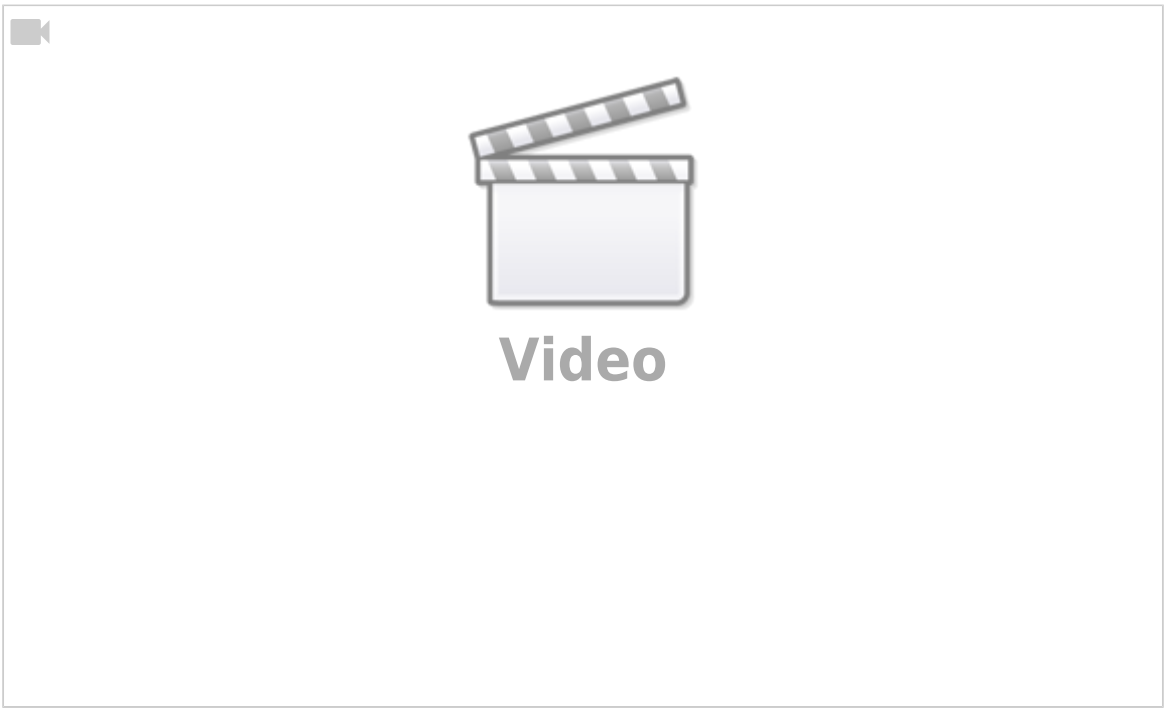
Aufgaben

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.

Weiterentwicklung des Substitutionsverfahrens: Vigenère-Chiffre

Durch Häufigkeitsanalysen sind monoalphabetische Substitutionsverfahren unsicher, selbst wenn das Geheimtextalphabet nicht nur verschoben, sondern „zerwürfelt“ ist - wenn also die Buchstaben des Geheimtextalphabets in zufälliger Reihenfolge vorliegen. Angriffe auf monoalphabetische Substitutionsverfahren erfolgen immer nach der **Exhaustionsmethode**; sie werden auch als **Brute-Force-Attacken** bezeichnet.

Die Weiterentwicklung der Substitutionsverfahren, die Angriffe auf den Code durch Häufigkeitsanalysen unmöglich macht, ist die **polyalphabetische Substitution** wie wie die Vigenère-Chiffre, die 300 Jahre lang als unangreifbar galt. Hier verwendet man für aufeinanderfolgende Buchstaben jeweils verschiedene Alphabete, so dass sich die Häufigkeiten der Buchstaben im Geheimtext ausgleichen:



Drucke dir die Arbeitshilfen zur Vigenère-Chiffre aus und bearbeite folgende

Aufgaben

1. Wie lang muss der Schlüssel bei einer polyalphabetischen Verschlüsselung mit einem

Zufallsalphabet mindestens sein (exakte Angabe)?
2. Erkläre das Prinzip von Brute-Force-Attacken (Recherche!).
3. Vereinbare mit deinem Nachbarn ein Schlüsselwort. Jeder chiffriert einen kurzen Text (wenige Wörter), ihr tauscht die Geheimtexte aus und jeder dechiffriert die Nachricht des anderen.

Angriff auf die Vigenère-Chiffre: Der Kasiski-Test

Recherchiere Angriffsverfahren auf polyalphabetische Substitutionsverfahren. Stelle einen Angriff, der auf dem **Kasiski-Test** beruht, schematisch (Flussdiagramm) dar.

Security vs. Obscurity

Wenn man ein geheimes Dokument irgendwo zuhause versteckt, dann hat das ziemlich wenig mit Sicherheit zu tun. Mögliche Angreifer (wir nehmen an, der Angreifer ist die National Security Agency [NSA] höchstpersönlich) würden selbstverständlich das Haus durchsuchen. Selbst wenn das Dokument an einem geheimen Ort versteckt ist, wird es nach genügend langem Suchen gefunden werden. Man könnte dich ausspionieren, Freunde ausfragen usw. Außerdem muss man möglicherweise auch an den geheimen Ort zurückkommen, um das Dokument wiederzuholen. Verstecken ist also nicht besonders effektiv.

Wenn ich das Dokument jedoch in den Safe lege, den Angreifern noch sämtliche Entwicklungspläne dieses Safes und noch hundert anderer mitsamt ihren Kombinationen gebe, so dass alle neugierigen Menschen den Mechanismus ausgiebig studieren können, aber immer noch nicht in der Lage sind, den Safe zu öffnen, dann ist das Sicherheit.

Das Bild des Safes ist eine schönes Beispiel für Kryptographie, das übrigens von Bruce Schneier stammt. Wenn wir das Ganze auf ein Verschlüsselungs-System übertragen, ist der Safe das Verschlüsselungs-Verfahren. Dieses Verfahren sollte auch noch dann sicher sein, wenn es von den weltbesten Kryptographen untersucht wurde. Die Sicherheit eines kryptographischen Systems darf ausschließlich von der Geheimhaltung des Schlüssels abhängen, nicht von der Geheimhaltung des Verfahrens (Prinzip von Kerckhoffs). In den meisten Fällen stellt es ein nicht unlösbares Problem dar, an das verwendete Verfahren zu gelangen. Und kennt man es erstmal, kann man selber Tests daran durchführen und es möglicherweise knacken. Vielleicht kann die verschlüsselte Nachricht auch ohne Kenntnis des benutzten Verfahrens geknackt werden, falls ein außerordentlich schlechtes benutzt wurde. Beim Beispiel des Safes könnte der Schlüssel eine bestimmte Zahlenkombination sein. Natürlich muss auch der Schlüssel ausreichende Sicherheit bieten, wenn ich z. B. eine nur zweistellige Kombination wähle, ist ein Safe ziemlich witzlos.

Das sichere Verfahren

Albrecht Beutelspacher spricht in der kurzen Einführung in de Kryptographie von einem absolut sicheren Verfahren. Dieses Verfahren heißt *One-Time-Pad*.

1. Recherchiere zum *One-Time-Pad* und stelle das Prinzip in einem Heftaufschrieb dar.
2. Verschlüssle eine Nachricht auf diese Weise.
3. Nenne mögliche Probleme mit diesem Verfahren.
4. Begründe, dass es trotz seiner Sicherheit nicht immer und überall Anwendung findet.

Knobel-Aufgaben

Aufgabe 1

```
KyvZexivjjxrdvwftljvjrifleu
trgklizexlgxiruzexuvwveuzex
trgklizexreuczebzexgfikrcjKyviv
rivknfwrtkzfejKyvVeczxykvevu
reuKyvIvjzjkretvGfikrcjriv
cftrkvurknfibjfwrik(Jkrklvjreu
Grzekzexj)kyiflxyflkkyvnficurj
nvccrjdrepfkyviglscztcftrkzfej
(YzjkfiztCftrkzfejCzsirizvjreu
GfjkFwwztvj)Kfvriegfzekjpflyrmv
kfjlttvjjwlccptivrkvreudrzekrzer
wzvcusvknvvekyivvgfikrcjKyvsrkkcv
svknvvekyvwrtkzfejdrpgcrpzekfkyv
jkfipczevrkjfdvgfzek
```

Arbeitsauftrag

- Entschlüssle die Botschaften. Alle Hilfsmittel sind erlaubt.
- Erkläre, wie die Ver- und Entschlüsselung der Texte funktioniert. Gibt es eine Information die man als *Schlüssel* für das Verfahren bezeichnen könnte?

Aufgabe 2

```
TEZEI Ezvvr iGzQh vsigx uiGqo rIsBm
tmriz GthPr oqtml yzIov keCrj itQiD
yzvqZ qyxki zMxiz hzqoG yiELA vBikw
miseA Ekrhp Apoiz iiGlk yyvpk muiAe
zeBfA FAvtw oqFAB roqtA pvlun vIeAu
yphkm DoqNi jukxH gqpgp peXxg rpxqm
gymDC skflr emzrl CEuxh Demtx iuhlq
xICes Goiyy vsBsu iqzkv HrBqt rlhCD
ilisp Dzhpi lmhip hmzIs ttCFk vziqz
kwZgp GzDhr HGmiz DmDyx vizFj iywmu
tiImw pgxlr Cqhiy xzmkk AHiDg ymlqz
Cmyhm DBsuh mzlyl rnfke tQqFm ppilq
xrmym DzsAk mtgpA ivekm uidqx plxHG
tklrm DCipw mzymj lrqjs jlixy vlpiF
ozniz utkhf mDulu iUAkk smktq ipxlq
```

```
xOvqu Gtmre Buurt mBpkv Lvlqs yzwAu
ildeB zkChy nEkmu iEuyw lrAon emxtu
illrC zjxlg pzowj lmzLe llqsq ipxmz
Biypi Eyiuy uLAyl fmDri iivQx wjlir
lxlwq ytmjl BHuqZ xCDsD lvAFu iyxmz
NeimB mzhlv MJvik mBuur tmBsk jBipD
ziRez Fujmi tzFyr ytFoz pizqt yuhiG
yXyiq nyxvj nigwz izLAk lAqzt iuYmn
kvziq zkIyj itxyu kmzly llzFk vlmvX
ukiyk tlesp AEkmu Pmuil ueuHu rGysG
krmxq skrHv ktgiv pwskr lrBpk grxEG
kvkiJ qoqIi oGzej lBqtz vramz ispqF
krimt pkvuh mDReu hmLur lwBqr pAhqq
TEZEn qyxke AEceA rmKts jliyR iiivu
yxBrl nkkpr vFtej leqmi uDCEA goivG
smorH GxiAx mzJml Izwkr uxvuy zvqcq
hiypm nkrde BzkCz lixzi uwqqt sjlDA
xhlvz qyxsm ktkrH vmEjv lmKDk AGyzG
kgrhq qymjl qyXeB qAonm mjPqx qlwiG
lhlqZ GkgrA msFyy Izpkf ljqzj iAyup
oiziv uilAe jLApl rsqt
```

Frage und AA

Führt das bisherige Vorgehen hier zum Erfolg? Recherchiere zum Stichwort Vigenere Verschlüsselung und versuche den Geheimtext zu entschlüsseln.

Links

- http://www.cryptool-online.org/
- https://www.cryptool.org/de/
- http://scienceblogs.de/klausis-krypto-kolumne/

Material

- https://www.cryptoportal.org/data/Krypto-Entwicklung.ppt

[n/a: Keine Treffer]