

## 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 ein 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 die 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. Verschlüssele 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
trgklizexlgxiruzexuvvveuzex
trgklizexreuczebzexgfikrcjKyviv
rivknfwrkzfejKyvVeczxykvevu
```

reuKyvIvjzjkretvGfikrcjriv  
cftrkvurknfibjfwrik(Jkrklvjreu  
Grzekzexj)kyiflxyflkkyvnficurj  
nvccrjdrepfkyviglscztcftrkzfej  
(YzjkfiztCftrkzfejCzsirizvjreu  
GfjkFwwztvj)Kfvriegfzekjpflyrmv  
kfjlttvjjwlcceptivrkvreudrzekrzer  
wzvcusvknvvekyivvgfikrcjKyvsrkkcv  
svknvvekyvwrkzfejdrpgcrpzekfkyv  
jkfipczevrkjfdvgfzek

### Arbeitsauftrag

- Entschlüssele 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 jlixv vlpif  
ozniz utkhf mDulu iUAkk smktq ipxlq  
xOvqu Gtmre Buurt mBpkv Lvlsq 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

```
yxBr1 nkkpr vFtej leqmi uDCEA goivG  
smorH GxiAx mzJml Izwkr uxvuy zvqcq  
hiypr nkrde BzkCz lixzi uwqqt sjlDA  
xhlvz qyXsm ktkrH vmEjv lmKDK AGyzG  
kgrhq qymjl qyXeB qAonm mjPqx qlwiG  
lhlqZ GkgrA msFyy Izpkf ljzqz 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]

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

Permanent link:  
<https://wiki.qg-moessingen.de/faecher:informatik:oberstufe:kryptographie:einfuehrung:start?rev=1645459825>

Last update: 21.02.2022 17:10

