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

einfuehrung_kryptologie.odp	3.1 MiB	15.10.2019 14:13
einfuehrung_kryptologie.pdf	935.6 KiB	15.10.2019 14:13