Cäsar-Verschlüsselung

Aufgaben:

1. *Eine Nachricht von Julius Cäsar an seine Truppen könnte gelautet haben: CPITKHH!*
   Lösung: ANGRIFF!
2. *…*
3. *...*
4. *Jedes Verschlüsselungsverfahren benötigt einen Schlüssel, der nur dem Sender und dem Empfänger bekannt sein darf. Was ist bei der Cäsar-Verschlüsselung der Schlüssel?*
   Lösung: Die Einstellung der Scheibe (also auf welchen Buchstaben wird das A abgebildet) stellt den Schlüssel (das Geheimnis dar).
5. *Während einer langweiligen Unterrichtsstunde beschließt du spontan einer Klassenkameradin eine geheime, verschlüsselte Nachricht zu schicken. Warum ist dies mit der Cäsar-Verschlüsselung nicht möglich?*

   Lösung: Das Problem ist, dass man noch keinen Schlüssel vereinbart hat. Möchte man dies während der Stunde machen, dann muss der Schlüssel durch die Klasse geschickt werden und kann daher von anderen mitgelesen werden (unsicherer Kanal).
   Bem: bei symmetrischen Verfahren ist dies grundsätzlich nicht möglich. Der Schlüssel muss vorher über einen sicheren Kanal ausgetauscht werden (die Bank schickt z.B. den PIN per Post).

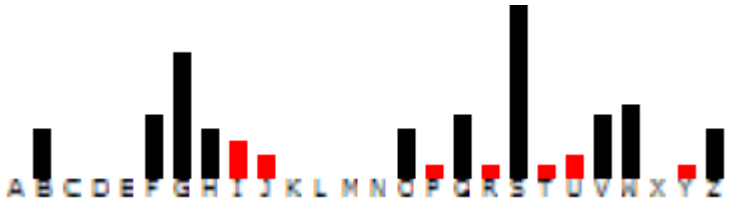
Brechen der Verschlüsselung

Geheime Nachricht:

```
RWS QOSGOF-JSFGQVZISGGSZIBU WGH YSWB UIHSG
JSFTOVFSB, GWS ZOSGGH GWQV ZSWQVH PFSQVSB.
```

Aufgaben:

6. *Finde heraus, welche Nachricht in diesem Kryptotext steckt. Beschreibe, wie du bei dem Brechen vorgegangen bist.*
   Lösung: DIE CAESAR-VERSCHLUESSELUNG IST KEIN GUTES VERFAHREN, SIE LAESST SICH LEICHT BRECHEN.
   Die Nachricht ist um 14 Buchstaben verschoben.
7. *Untersuche, wie oft welcher Buchstabe im Kryptotext vorkommt. Erkläre, wie diese Information beim Brechen der Verschlüsselung benutzt werden kann.*
   Lösung:



S ist am häufigsten. Dies muss das E sein.

Bild der Kopfzeile: „Skytale.png“ von Luringen (ownwork) via Wikimedia Commons [CC BY-SA 3.0] (Abgerufen: 03.2017)
Bild „Häufigkeitsverteilung“, Schaller. Erstellt mit Cryptool-Online, URL: http://www.cryptool-online.org/ (Abgerufen: 11.2016)