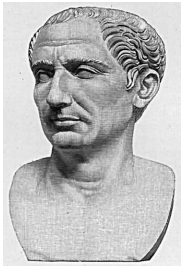

Cäsar-Verschlüsselung

Nach der Überlieferung des römischen Schriftstellers Sueton verwendete Julius Cäsar ein Verschlüsselungsverfahren, um seinen Feldherrn im Krieg Nachrichten zu schicken. Er verschob dazu alle Buchstaben im Alphabet, um zwei Zeichen. Aus A wurde C, aus B wurde D, aus C wurde E usw. Am Ende des Alphabets fing er wieder vorne an. Aus X wurde Z, aus Y wurde A und aus Z ein B.

Chiffrier-Scheibe

Leon Battista Alberti vereinfachte das Verfahren im 15. Jahrhundert durch die Entwicklung der Chiffrierscheibe. Schneide für die Herstellung einer die beiden Kreise mit den Buchstaben aus. Bohre in die Mitte je ein Loch und hefte die beiden Scheiben mit einer Musterbeutelklammer zusammen.

Aufgaben:

1. *Eine Nachricht von Julius Cäsar an seine Truppen könnte gelautet haben: CPITKHH!*
   Stelle die Scheibe so ein, dass auf der inneren Scheibe das C auf der Position des A auf der äußeren Scheibe steht. Auf der inneren Scheibe stehen die Buchstaben des verschlüsselten Textes (Kryptotext), auf der äußeren kannst du den entschlüsselten Text ablesen (Klartext).
2. *Vereinbare mit einem Freund/einer Freundin, welchen Buchstaben ihr beim Verschlüsseln aus A machen wollt. Schreibt euch gegenseitig eine kurze Nachricht. Verschlüsselt diese gemäß der Cäsar-Verschlüsselung mit eurer vereinbarten Verschiebung.*
3. *Entschlüssele die Nachricht des anderen und vergleicht mit dem Originaltext.*
4. *Jedes Verschlüsselungsverfahren benötigt einen Schlüssel, der nur dem Sender und dem Empfänger bekannt sein darf. Was ist bei der Cäsar-Verschlüsselung der Schlüssel?*
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?*

Brechen der Verschlüsselung

Wenn verschlüsselte Nachrichten verschickt werden, gibt es auch immer jemand, der diese Nachricht trotz Verschlüsselung lesen will. Man spricht vom „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.*
7. *Untersuche, wie oft welcher Buchstabe im Kryptotext vorkommt. Erkläre, wie diese Information beim Brechen der Verschlüsselung benutzt werden kann.*
8. *(*) Entwirf ein verbessertes Verschlüsselungsverfahren, das nicht so leicht zu brechen ist.*

(Abgerufen: 03.2017)