

LU05a - Verschlüsselung: Einführung

Der Wunsch geheime Nachrichten zu versenden, ist fast so alt wie die ersten Schriftzeichen. Schon im alten Ägypten wurden unübliche Zeichen als eine erste Form der Verschlüsselung verwendet.

siehe auch <https://www.cryptool.org/de/education/history>

Begriffe



Quelle: `cdn-ehmjb.nitrocdn.com/XEndFMRoHReLIVFeSuZyEacZMuUWEMvU/assets/static/optimized/rev-31a3d27/wp-content/uploads/2020/09/2.png`

Kryptologie

Die Wissenschaft die sich mit dem Verschlüsseln und Entschlüsseln von Informationen beschäftigt. Sie umfasst die Teilgebiete:

- Kryptografie: Verschlüsseln von Informationen
- Kryptoanalyse: Verschlüsselte Informationen entziffern

Steganografie

Die geheimen Informationen werden in unscheinbaren Daten (z.B. Bilder, Musik) versteckt.

Schlüssel

Bei den meisten Verschlüsselungsverfahren wird ein Schlüssel eingesetzt. Dieser Schlüssel ist eine Zahl oder ein Wort, welche als Grundlage für die Verschiebung und Ersetzung der Zeichen dient.

Klartext

Der unverschlüsselte Text einer Nachricht.

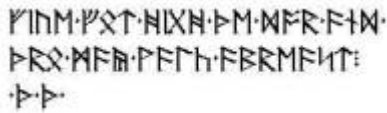
Chiffretext

Der verschlüsselte Text.

Verschlüsselungsverfahren

Substitution

Bei einem Substitutionsverfahren wird ein Buchstabe durch andere Buchstaben oder Symbole ersetzt. Im Buch „Der Hobbit“ finden sich diese Runen:



Der Autor hat die englischen Buchstaben durch Bildzeichen ersetzt (Substitution).

Transposition

Bei einem Transpositionsverfahren wird die Reihenfolge der Buchstaben scheinbar willkürlich verändert.

Klartext: „Hallo Universum“

Chiffretext: „RUHSNAUILMVLEO“

[m114-A0G](#)



Marcel Suter

From:
<https://wiki.bzz.ch/> - **BZZ - Modulwiki**

Permanent link:
<https://wiki.bzz.ch/modul/m114/learningunits/lu05/verschluesselungeinfuehrung>

Last update: **2024/03/28 14:07**

