# Kryptologie-Lexikon

Im Zusammenhang mit dem Thema Kryptologie hast du viele neue Begriffe kennengelernt. Damit du den Überblick nicht verlierst, soll hier ein kleines Lexikon entstehen.

**Aufgabe:** Teilt die Begriffe unter euch auf. Zu jedem Begriff schreiben ein bis zwei Schüler\*innen eine Definition und geben ggf. ein Beispiel an. Zwei andere Schüler\*innen sind jeweils für eine Überprüfung der Definition und ggf. Korrektur zuständig. Erstellt dazu ein Textdokument, an dem ihr kollaborativ arbeiten könnt.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kryptologie** | **Kryptographie** | **Kryptoanalyse** | **Vertraulich­keit** | **Klartext** |
| **Geheimtext / Chiffre** | **Schlüssel** | **Verschlüsseln / Chiffrieren** | **Entschlüsseln / Dechiffrieren** | **„Knacken“** |
| **Substitution** | **Monoalpha­betische Substitution** | **Homophone, monoalpha­betische Substitution** | **Polyalpha­betische Substitution** | **Transposition** |
| **Symmetrische Verschlüsselung** | **Asymmetrische Verschlüsselung** | **privater Schlüssel** | **öffentlicher Schlüssel** | **Authentifikation** |
| **Digitale Unterschrift / Signatur** | **Integrität** |  |  |  |

Dieses Werk ist lizenziert unter einer [Creative Commons Namensnennung - Nicht-kommerziell - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz](http://creativecommons.org/licenses/by-nc-sa/4.0/). Sie erlaubt Bearbeitungen und Weiterverteilung des Werks unter Nennung meines Namens und unter gleichen Bedingungen, jedoch keinerlei kommerzielle Nutzung.