# Vigenère-Kodierung: Entziffern von Vigenère

## Manuelles Entziffern mit der Kasiski-Methode

Für den Beispieltext sind Schlüsselwort, Klar- und Geheimtext bekannt. Obwohl dieser Text kurz ist, kann man erkennen, wie Rückschlüsse auf die Länge des Schlüsselwortes gezogen werden können.

Schlüsselwort KREIS

K R E I S K R E I S K R E I S K ~~R E~~ I S K R E I ~~S K~~ R E I S K R E I S K R E I S K R E
O Z R M Y O Y I Q E C T L Z A P ~~K M~~ A L O Z R M ~~K M~~ Y V Q X D U M M Y O Y I Q E S J X
E I N E G E H E I M S C H R I F ~~T I~~ S T E I N E ~~S C~~ H R I F T D I E G E H E I M I S T

1. Textbrücken
   a. Betrachte die unterstrichenen Stellen (Abschnitt 1, Abschnitt 2). Was haben sie gemeinsam?
   b. Der Text enthält auch eine Stelle (~~Abschnitt 3~~) mit einer Durchstreichung. Beschreibe eine Gemeinsamkeit und einen Unterschied zu den unterstrichenen Stellen.
   c. Leite die Bedeutung der folgenden Fachbegriffe ab.

      Eine Brücke im verschlüsselten Text besteht aus zwei _____ Textabschnitten.

      Bei einer echten Brücke sind beide Textabschnitte mit _____ Schlüsselbuchstaben verschlüsselt.

      Bei unechten Brücken _____
2. Länge des Schlüsselwortes
   a. Ermittle den Abstand der Brücken, also den Abstand der jeweils ersten Zeichen innerhalb derselben Brücke.
      - Brückenlänge zu Abschnitt 1:
      - Brückenlänge zu Abschnitt 2:
      - Brückenlänge zu Abschnitt 3:
   b. Vergleiche die beiden Brückenlängen mit der Länge des Schlüsselwortes:

      Die Länge des Schlüsselwortes ist ein _____ der Länge jeder _____ Brücke.
   c. Formuliere diese Vorgehensweise zur Ermittlung der Schlüssellänge allgemein.
3. Gruppenarbeit (3 Personen): Ermittelt gemeinsam die Länge des Schlüsselwortes des verschlüsselten Textes.

   Für Schnelle: Auf dem Tauschlaufwerk liegt eine Datei **`vigenere.py`**. Verwende die dort definierten Funktionen um das Schlüsselwort zu ermitteln und dann den Text zu entschlüsseln. Der Text ist in der Variable **`geheimtext`** in der Datei enthalten.

   Zusatz: Das Schlüsselwort ist ein Name aus einem Roman von Alexandre Dumas. Aus welchem? Finde heraus, welche Bedeutung der Inhalt des Textes im Rahmen dieses Romans hat.

# Vigenère-Kodierung: Entziffern von Vigenère

Zu entschlüsseln ist der folgende Geheimtext. Er wurde mit dem Vigenère-Verfahren chiffriert, leider ist irgendwie das Schlüsselwort abhanden gekommen. Die Teilung des Textes in Fünferblöcke ist nur der besseren Zählbarkeit geschuldet und steht in keinem Zusammenhang zum Inhalt.

**LMWTL JHAPA XRHHA AYFGE EMHJH IHGHX XEAYD AJSPA**
**VWLBG WMWHN TEMKF HRJYS UTRKP QUEIB IOLNR BRWPA**
**EMMCH LHXFW UDVXX WOETK EXLEQ BIKDU PAWGO LGXRE**
**DSFGE ZPEAX VYUIS YIFZE EWIFX MRBRW QSPAA WUWVX**
**KWQDR GIAQW NGHRX EAMOJ DESMI FGEEZ IYHNJ TIJWI**

**TBQTO IPDEM IDVXX WOETK EXLSP AINHR FXRVX NTIVA**
**YAGXV TRTFV LSITR GIJKO OXROL RQWIJ ERHVL BHGYB**
**GZHRT XLWLM UTPLX NTWIF QIACI VHMST PDPUF LIAQH**
**NEFWV DHMDW QDCXV KRNRG HAHWB KXWHR STLJH NQBIW**
**LNRII JVOAT RVLEN GHWUE EBGZW EGWMW EENFX WQDRK**

**IFJLV LGZHN GXPWJ RNYIF JEFXP DVCUT JLZEE WIFDU**
**SWMWJ EUXME KAYMY FJEVG KWVCU PSJHN QHGZV CUKIA**
**EEAPM JRFGW MFJES KHAHE FNRKX NGXVL UARZP AFHJT**
**IJHWR GROLR FXLWQ WHXVV HNQTW KIRRF HWVIR OSJXN**
**FXVWQ AHZIF OEFXR VLEFB WLHIA UIVDU RKPAF HRKQS**

**QGREH WUTRE IYUAS BIMQD RKQMV SQNVU KDNLI AQEBW**
**IJDNQ XVWPI GMIDE EUHFW QWRKH WQ**