

LU05d - Vigenère

Dieses und weitere Verfahren zum Nachlesen und Ausprobieren

<https://www.cryptool.org/de/cryptool-online>

Dieses Verfahren wurde im 16. Jahrhundert von Blaise de Vigenère entwickelt und stellt eine Erweiterung der Caesar-Chiffre dar. Anhand eines Schlüssels wird für jeden Buchstaben festgelegt, um wie viele Stellen er im Alphabet verschoben wird. Dazu wird der Schlüssel immer wieder unter den Klartext notiert.

Klartext: DIESES VERFAHREN GALT DREIHUNDERT JAHRE LANG ALS NICHT KNACKBAR
Schlüssel: GEHEIM GEHEIMGEH EIMG EHEIMGEHEIM GEHEI MGEH EIM GEHEI MGEHEIMG

Nun beginnt man mit dem ersten Buchstaben im Klartext und im Schlüssel:

- Klartext: D
- Schlüssel: G

Der Schlüssel bestimmt, um wieviele Stellen der Buchstabe im Alphabet verschoben wird.

- Schlüssel: G = 6. Buchstabe im Alphabet nach dem Buchstaben **A**.
- Chiffre: D + 6 Stellen = J

Vigenère-Quadrat

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

Diese Tabelle ist ein Hilfsmittel zur schnelleren Verschlüsselung. Sie müssen nicht mehr die Positionen im Alphabet ermitteln bzw. berechnen. Stattdessen können Sie den Chiffre-Buchstaben direkt ablesen.

Die rot markierten Stellen zeigen die Anwendung: Der Buchstabe **K** im Klartext und der Buchstabe **N** im Schlüssel werden zum Buchstaben **X** im Chiffretext.

Verschlüsseln

Klartext: Ist das nicht toll
Schlüssel: Eim erE imerE imer

1. Wähle einen Buchstaben im Klartext (z.B. I) und den dazugehörigen Buchstaben im Schlüssel (z.B. E).

2. Suche die Spalte mit dem Buchstaben aus dem Klartext.
3. Suche die Zeile mit dem Buchstaben aus dem Schlüssel.
4. Im Schnittpunkt dieser Spalte und Zeile finden Sie den Chiffre-Buchstaben (z.B. M)

Chiffre: MAFHRWVUGYXBAPC

Entschlüsseln

Chiffre: WMCVWURMDWFXCOZHQDWCAZWQIFLRHF
Schlüssel: BildungszentrumBildungszentrum

1. Wähle einen Buchstaben im Schlüssel (z.B. B) und den dazugehörigen Buchstaben aus dem Chiffretext (z.B. W)
2. Suche die Zeile mit dem Buchstaben aus dem Schlüssel.
3. Suche innerhalb der Zeile die Spalte mit dem Buchstaben aus dem Chiffretext.
4. Der oberste Buchstabe in dieser Spalte ist der Klartext (z.B. V)

Klartext: VERSCHLUESSELUNGISTINTERESSANT

[m114-A0G](#)



Marcel Suter

From:

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

Permanent link:

<https://wiki.bzz.ch/modul/m114/learningunits/lu05/vigenere>

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

