

# LU04.A03 - Vigenère Verschlüsselung

## Lernziele

- Ich kann Texte mit antiken Verfahren ver- und entschlüsseln.

## Rahmenbedingungen

- **Zeitbudget:** 10 Minuten
- **Sozialform:** Einzelarbeit
- **Hilfsmittel:** Dossier „SymmetrischVerschluesselung\_Theorie“
- **Erwartetes Ergebnis:** Schreiben Sie die beiden Lösungen übereinander direkt in den Auftrag hier im Moodle.

## Ausgangslage

Die ersten Verschlüsselungsverfahren wurden vor rund 2'000 Jahren erfunden und bestanden im Kern aus einem Textband und einem passenden Stock, der den Schlüssel darstellte. Neben diesem Skytale-Verfahren wurden auch andere Verfahren im Laufe der Zeit erfunden. Eines der bemerkenswertesten unter diesen frühen Methoden ist das Vigenère-Verschlüsselungsverfahren, benannt nach Blaise de Vigenère, einem Diplomaten aus dem 16. Jahrhundert. Es wurde als deutliche Verbesserung gegenüber den einfachen monoalphabetischen Verschlüsselungen der Zeit angesehen, weil es eine polyalphabetische Verschlüsselung nutzt, bei der der Klartext und der Schlüssel kombiniert werden, um den Chiffretext zu erzeugen. Dieses Verfahren war zu seiner Zeit revolutionär, da es eine Mehrschichtverschlüsselung bot, die wesentlich schwerer zu brechen war als seine Vorgänger und lange als unknackbar galt. Es ebnete den Weg für die Entwicklung komplexerer Verschlüsselungsmethoden, wie wir sie heute kennen.

## Arbeitsauftrag

Verschlüsseln Sie die nachfolgenden Nachrichten mit dem Vigenère-Verfahren schriftlich und nachvollziehbar.

- **1. Wort**
  - **Klartext:** Geheimnis
  - **Schlüssel:** Extrem
  - **Chiffretext:** ???
- **2. Wort**
  - **Klartext:** Verrat
  - **Schlüssel:** Leise
  - **Chiffretext:** ???

## Tabelle

	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

From:

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

Permanent link:

<https://wiki.bzz.ch/modul/m183/learningunits/lu04/aufgaben/03?rev=1752153328>

Last update: **2025/07/10 15:15**

