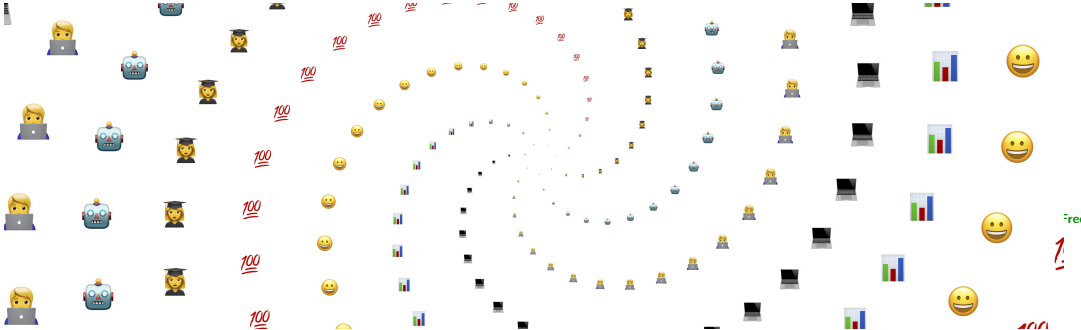
Kryptologie

Vigenère-Chiffre

Cyril Blum

Fachschaft Informatik
Kantonsschule im Lee



Vigenère

Von Caesar...

```
  Klartext: JEMANDMUSSTEJOSEFKVERLEUMDETHA...
Schlüssel: GGGGGGGGGGGGGGGGGGGGGGGGGGGGGG...
Geheimtext: PKSGTJSAYYZKPUYKLQBKXRKASJKZNG...
```

Vigenère

...zu Vigenère

```
  Klartext: JEM|AND|MUS|STE|JOS|EFK|VER|LE...
 Schlüssel: KEY|KEY|KEY|KEY|KEY|KEY|KEY|KE...
Geheimtext: TIK|KRB|WYQ|CXC|TSQ|OJI|FIP|VI...
```



Vigenère

```
  Klartext: JEM|AND|MUS|STE|JOS|EFK|VER|LE...
 Schlüssel: KEY|KEY|KEY|KEY|KEY|KEY|KEY|KE...
Geheimtext: TIK|KRB|WYQ|CXC|TSQ|OJI|FIP|VI...
```

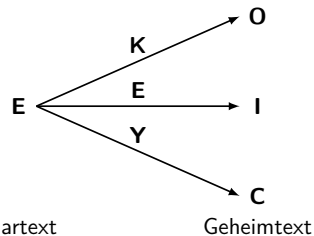
- B=Verschiebung um 1 Position, C=Verschiebung um 2 Positionen, usw.
- Galt über 300 Jahre lang als sicher!



Vigenère

```
  Klartext: JEM|AND|MUS|STE|JOS|EFK|VER|LE...
Schlüssel: KEY|KEY|KEY|KEY|KEY|KEY|KEY|KE...
Geheimtext: TIK|KRB|WYQ|CXC|TSQ|OJI|FIP|VI...
```

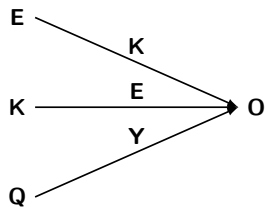
- B=Verschiebung um 1 Position, C=Verschiebung um 2 Positionen, usw.
- Galt über 300 Jahre lang als sicher!



Vigenère

```
  Klartext: JEM|AND|MUS|STE|JOS|EFK|VER|LE...
Schlüssel: KEY|KEY|KEY|KEY|KEY|KEY|KEY|KE...
Geheimtext: TIK|KRB|WYQ|CXC|TSQ|OJI|FIP|VI...
```

- B=Verschiebung um 1 Position, C=Verschiebung um 2 Positionen, usw.
- Galt über 300 Jahre lang als sicher!



Blaise de Vigenère

Blaise de Vigenère



- Vigenère-Verschlüsselung nach dem französischen Diplomat und Kryptograf Blaise de Vigenère (1523–1596).

Quelle

Blaise de Vigenère

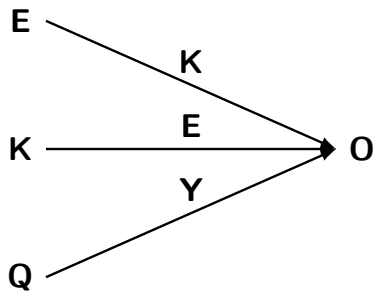
Blaise de Vigenère



- Vigenère-Verschlüsselung nach dem französischen Diplomat und Kryptograf Blaise de Vigenère (1523–1596).
- Galt über 300 Jahre lang (bis ca. 1863) als unbrechbar!

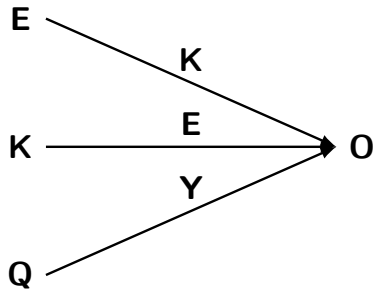
Quelle

Vigenère



Klartext Geheimtext

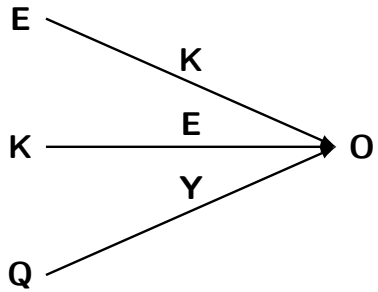
Vigenère



Klartext Geheimtext

$$h_{Geheimtext}(O) = \frac{h_{Klartext}(E) + h_{Klartext}(K) + h_{Klartext}(Q)}{3}$$

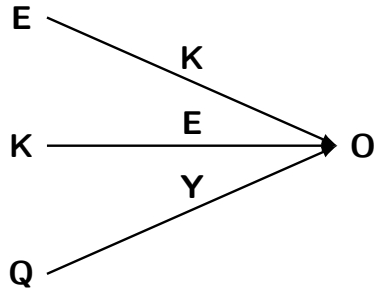
Vigenère



Klartext Geheimtext

$$h_{Geheimtext}(O) = \frac{h_{Klartext}(E) + h_{Klartext}(K) + h_{Klartext}(Q)}{3}$$
$$= \frac{17.7\% + 1.4\% + 0.01\%}{3} = 6.4\%$$

Vigenère



Klartext Geheimtext

$$h_{Geheimtext}(O) = \frac{h_{Klartext}(E) + h_{Klartext}(K) + h_{Klartext}(Q)}{3}$$
$$= \frac{17.7\% + 1.4\% + 0.01\%}{3} = 6.4\%$$

→ Die Häufigkeiten der Buchstaben entsprechen nun nicht mehr direkt einer Häufigkeit eines anderen Buchstabens im Originaltext!

Verschlüsselungs- / Entschlüsselungs-Methode

Wie kann man diesen Text verschlüsseln?

NIEMANDKANNDASLESEN
REDREDREDREDREDREDR

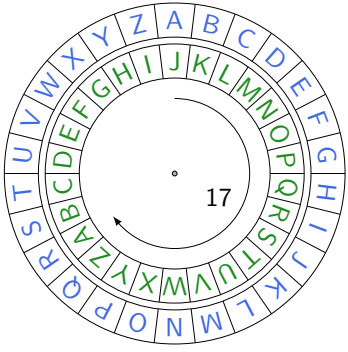


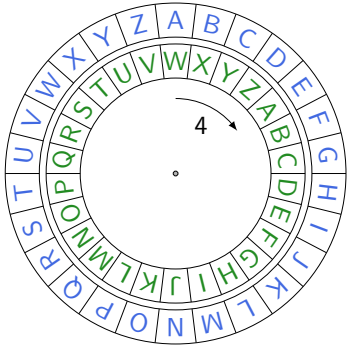
Verschlüsselungs- / Entschlüsselungs-Methode

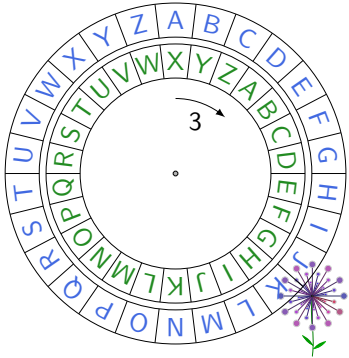
Wie kann man diesen Text verschlüsseln?

NIEMANDKANNDASLESEN
REDREDREDREDREDREDR

Mit 3 Caesar-Scheiben:







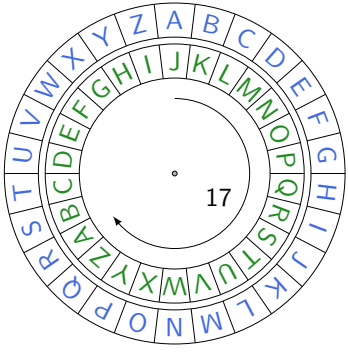
EMHDEQUODERGRWOVWHE

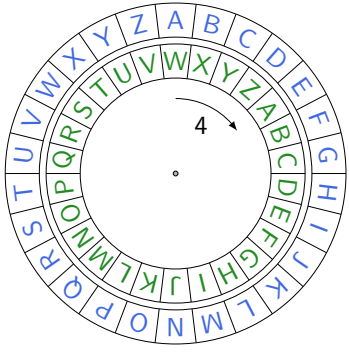
Verschlüsselungs- / Entschlüsselungs-Methode

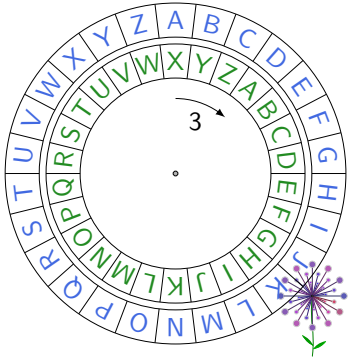
Wie kann man diesen Text verschlüsseln?

NIEMANDKANNDASLESEN
REDREDREDREDREDREDR

Mit 3 Caesar-Scheiben:







EMHDEQUODERGRWOVWHE

Schlüsselbuchstabe

Klartextbuchstabe	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

NIEMANDKANNDASLESEN
REDREDREDREDREDREDR
EMHDEQUODERGRWOVWHE

Schlüsselbuchstabe

Klartextbuchstabe	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

NIEMANDKANNDASLESEN
REDREDREDREDREDREDR
EMHDEQUODERGRWOVWHE

Schlüsselbuchstabe

Klartextbuchstabe	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

NIEMANDKANNDASLESEN	
REDREDREDREDREDREDR	
EMHDEQUODERGRWOVWHE	

Auftrag

Skript

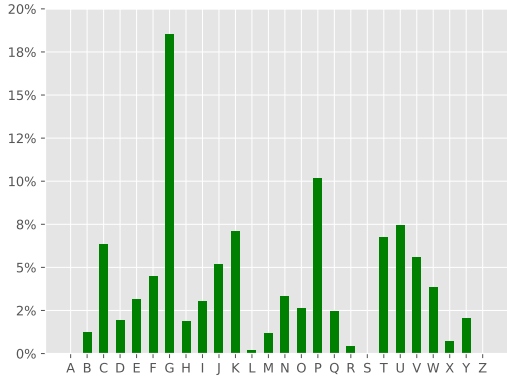
- Ver- und Entschlüsselung:

  2.1 - 2.3

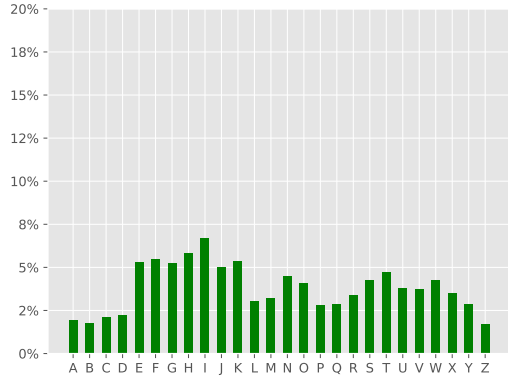
- Schnelle: Lernkontrolle auf Moodle (erste Aufgabe)



Angriff auf Vigenère: Bekannte Schlüssellänge



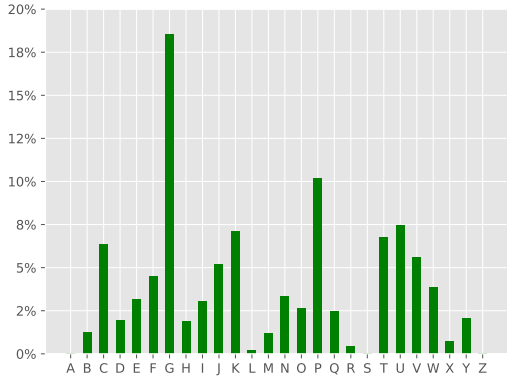
(a) Caesar



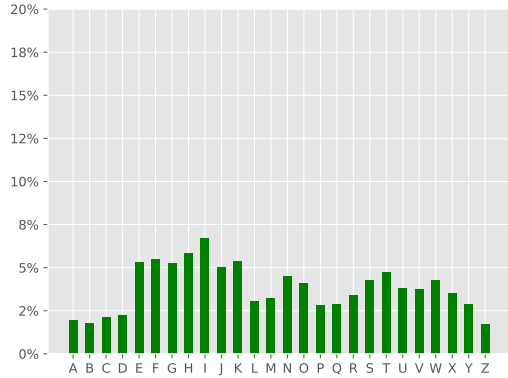
(b) Vigenère

FreeFlower

Angriff auf Vigenère: Bekannte Schlüssellänge



(a) Caesar

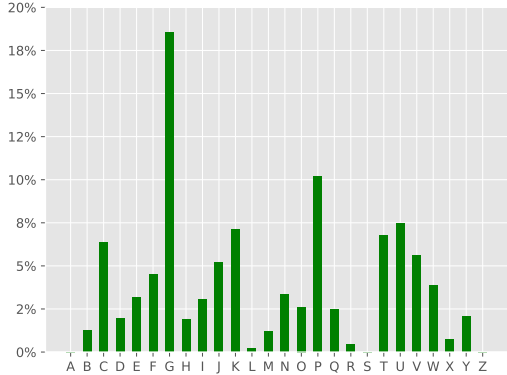


(b) Vigenère

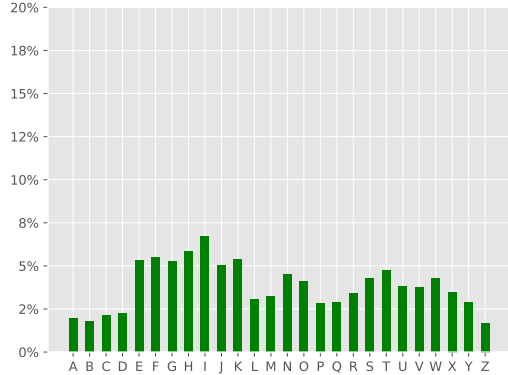
Frage: Weshalb sehen die beiden Diagramme so unterschiedlich aus?

FreeFlower

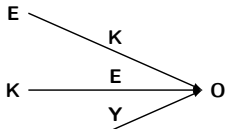
Angriff auf Vigenère: Bekannte Schlüssellänge



(a) Caesar

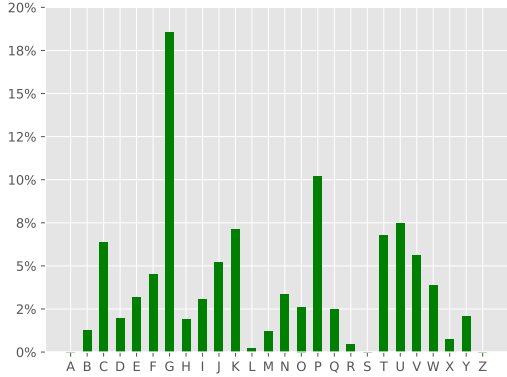


(b) Vigenère

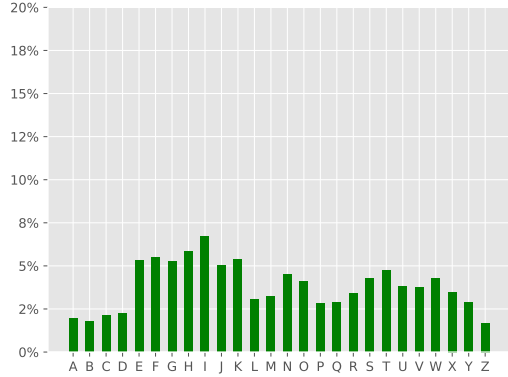




Angriff auf Vigenère: Bekannte Schlüssellänge



(a) Caesar



(b) Vigenère

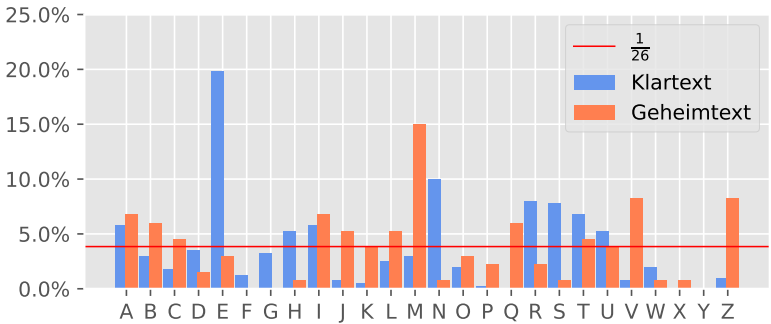
Frage: Würde die Buchstabenverteilung auch so aussehen, wenn man in der rechten Grafik statt allen Buchstaben nur jeder dritte Buchstabe (z.B. alle grünen Buchstaben) betrachten würde?

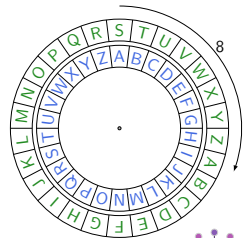
RGT IPK UWZ AVL BQZ MHR DGY TGB UFL BJH JGU LGU VQO VGK IUZ MTL BYH ADA AGZ

Angriff auf Vigenère: Bekannte Schlüssellänge

RGT IPK UWZ AVL RQZ MHR DGY TGB UFL BJH JGU LGU VQO VGK IUZ MTL BYH ADA AGZ
OGA IPO JVA MYB ZFL MTL QPL AOV ZIL VUC MTO IHA MVZ EKL MKU PWU LWJ ACN BGL
ZGZ EC. . .

→ Häufigster Buchstaben in Gruppe 1: M (🔑 Schlüssel?)



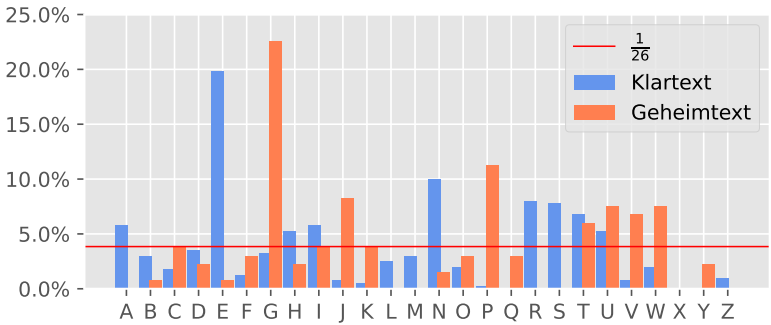


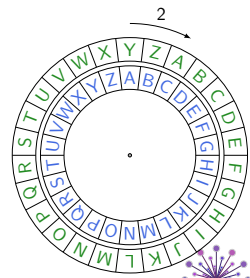
FreeFlower

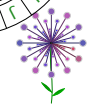
Angriff auf Vigenère: Bekannte Schlüssellänge

RGT IPK UWZ AVL RQZ MHR DGY TGB UFL BJH JGU LGU VQO VGK IUZ MTL BYH ADA AGZ
OGA IPO JVA MYB ZFL MTL QPL AOV ZIL VUC MTO IHA MVZ EKL MKU PWU LWJ ACN BGL
ZGZ EC. . .

→ Häufigster Buchstaben in Gruppe 2: G (🔑 Schlüssel?)





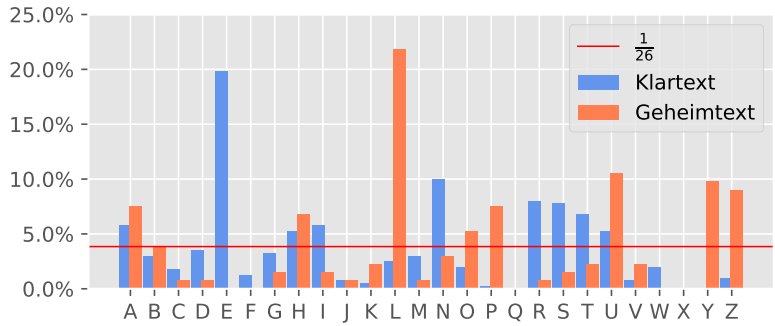


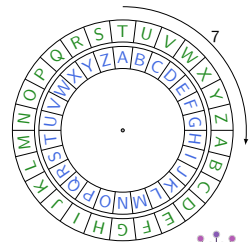
FreeFlower

Angriff auf Vigenère: Bekannte Schlüssellänge

RGT IPK UWZ AVL RQZ MHR DGY TGB UFL BJH JGU LGU VQO VGK IUZ MTL BYH ADA AGZ
OGA IPO JVA MYB ZFL MTL QPL AOV ZIL VUC MTO IHA MVZ EKL MKU PWU LWJ ACN BGL
ZGZ EC. . .

→ Häufigster Buchstaben in Gruppe 3: L (🔑 Schlüssel?)





FreeFlower

Auftrag

Skript

- Aufgaben 2.4-2.5

