Leibniz Gemeinschaft

IPN
Leibniz-Institut für die Pädagogik der Naturwissenschaften und Mathematik

Security of the Caesar cipher

Security of the Caesar cipher

How could an attacker receive the plaintext from the cipher, without knowing the key.

Security of the Caesar cipher

- We know, that during encryption one of 26 keys was used.
- If you decrypt the ciphertext with the correct key, you receive the plaintext.

Try every key

If you encrypt a cipher with every possible key, the plaintext is one of the results.

Improvements

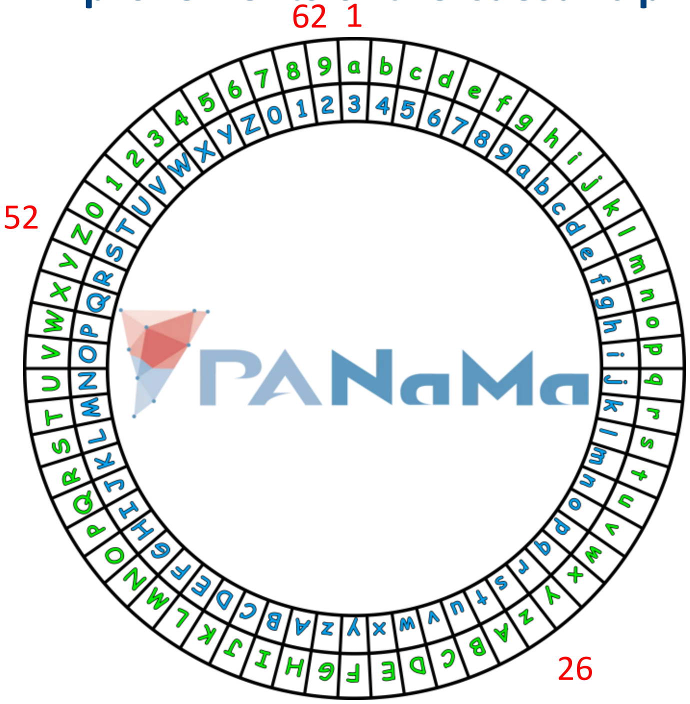
- **Problem**:

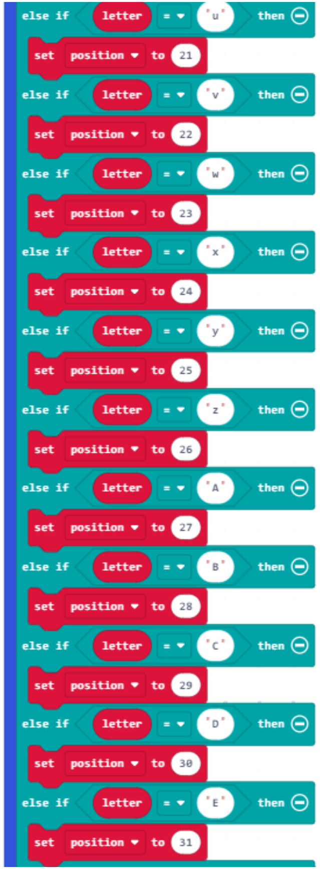
  You can try every key in no time.

- **Solution**:

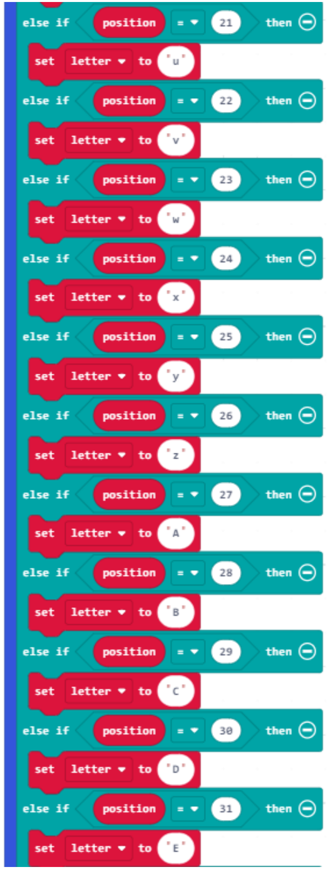
  Change the procedure in a way, that it is possiple to use more different keys.

Improvements of the Caesar cipher



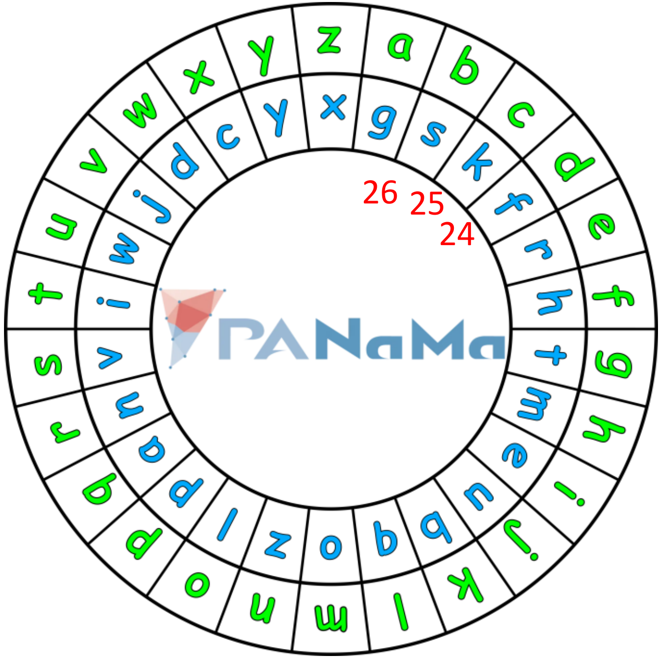


```
else if letter = "u" then
    set position to 21
else if letter = "v" then
    set position to 22
else if letter = "w" then
    set position to 23
else if letter = "x" then
    set position to 24
else if letter = "y" then
    set position to 25
else if letter = "z" then
    set position to 26
else if letter = "A" then
    set position to 27
else if letter = "B" then
    set position to 28
else if letter = "C" then
    set position to 29
else if letter = "D" then
    set position to 30
else if letter = "E" then
    set position to 31
```

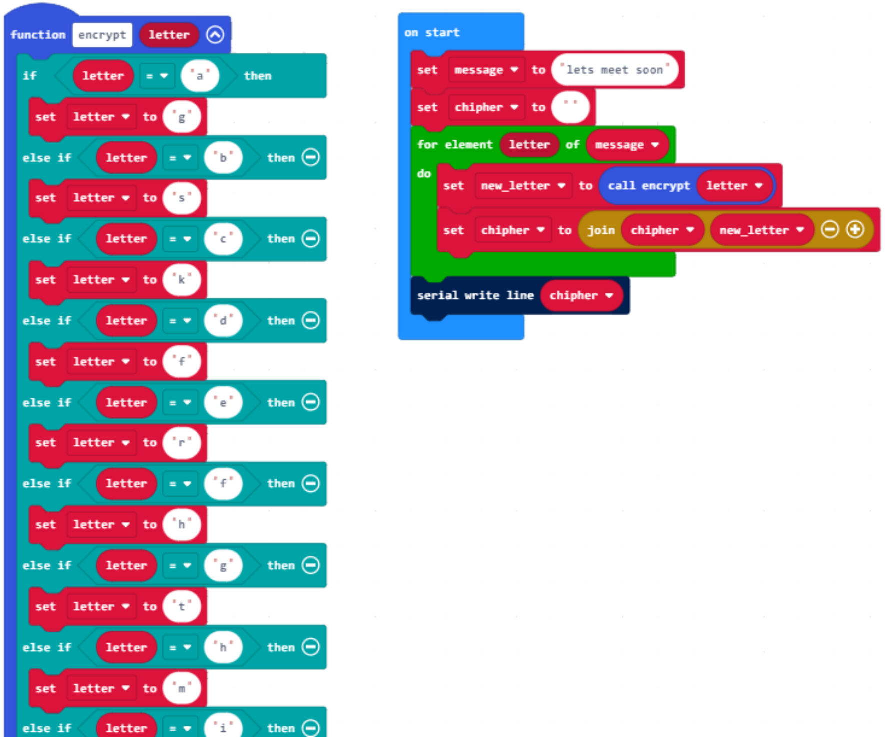


```
else if position = 21 then
    set letter to "u"
else if position = 22 then
    set letter to "v"
else if position = 23 then
    set letter to "w"
else if position = 24 then
    set letter to "x"
else if position = 25 then
    set letter to "y"
else if position = 26 then
    set letter to "z"
else if position = 27 then
    set letter to "A"
else if position = 28 then
    set letter to "B"
else if position = 29 then
    set letter to "C"
else if position = 30 then
    set letter to "D"
else if position = 31 then
    set letter to "E"
```

Improvements of the Caesar cipher



26 * 25 * 24 * 23 * … * 2 * 1 =
403.291.461.126.605.635.584.000.000



```
function encrypt letter
  if letter = "a" then
    set letter to "g"
  else if letter = "b" then
    set letter to "s"
  else if letter = "c" then
    set letter to "k"
  else if letter = "d" then
    set letter to "f"
  else if letter = "e" then
    set letter to "r"
  else if letter = "f" then
    set letter to "h"
  else if letter = "g" then
    set letter to "t"
  else if letter = "h" then
    set letter to "m"
  else if letter = "i" then
```

```
on start
  set message to "lets meet soon"
  set chipher to ""
  for element letter of message
  do
    set new_letter to call encrypt letter
    set chipher to join chipher new_letter
  serial write line chipher
```

Number of possible keys

- Alphabet with 26 characters:

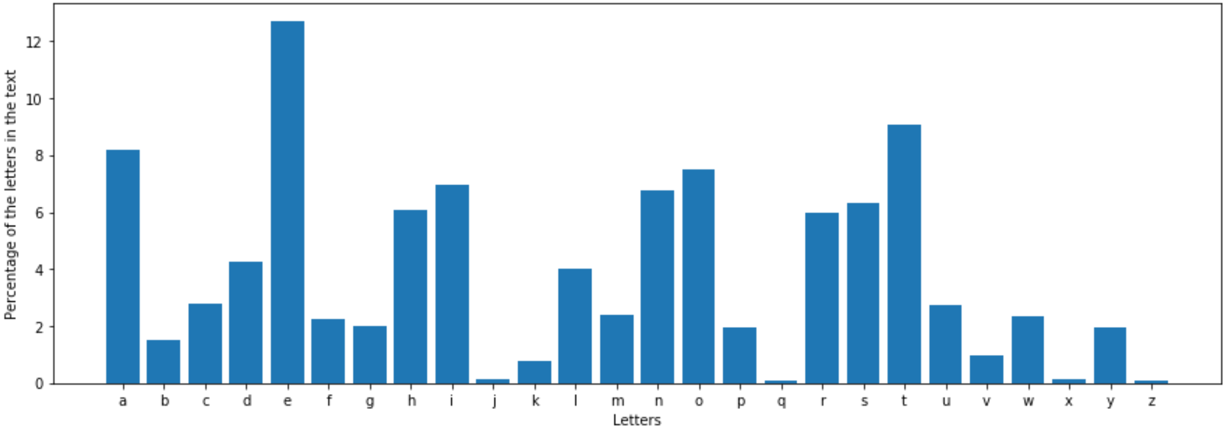
  403.291.461.126.605.635.584.000.000 (403 Quadrillion)

- Not secure!

Security of the Caesar cipher

In every language different letters occur in different frequencies.

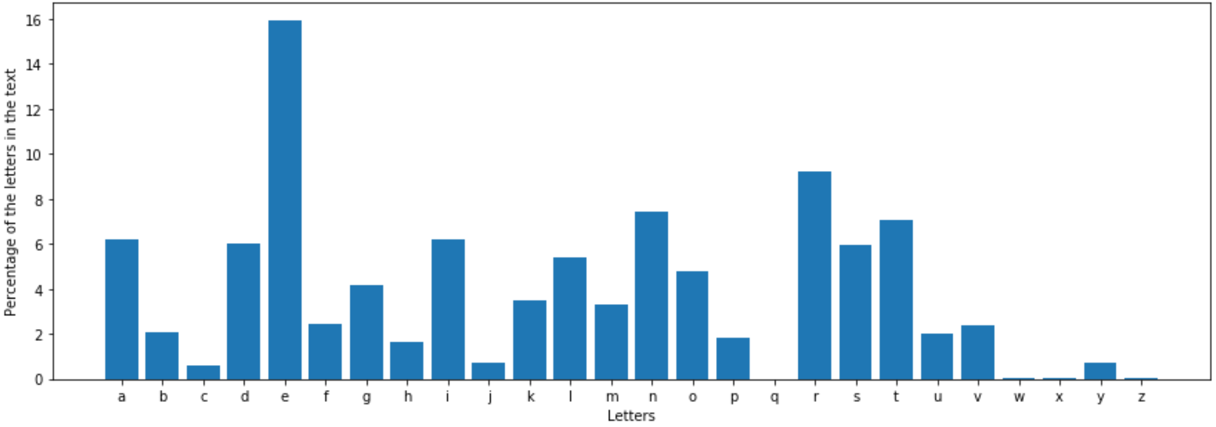
English



Security of the Caesar cipher

In every language different letters occur in different frequencies.

Dansk



Frequency analysis

- In English ***e*** is the most frequent letter.
- The most frequent letter in the plaintext: ***e***
- The most frequent letter in the ciphertext?

  The letter that you get when you encrypt the letter ***e.***

Frequency analysis

- In English ***t*** is the second most frequent letter.
- The second most frequent letter in the plaintext: ***t***
- The second most frequent letter in the ciphertext?

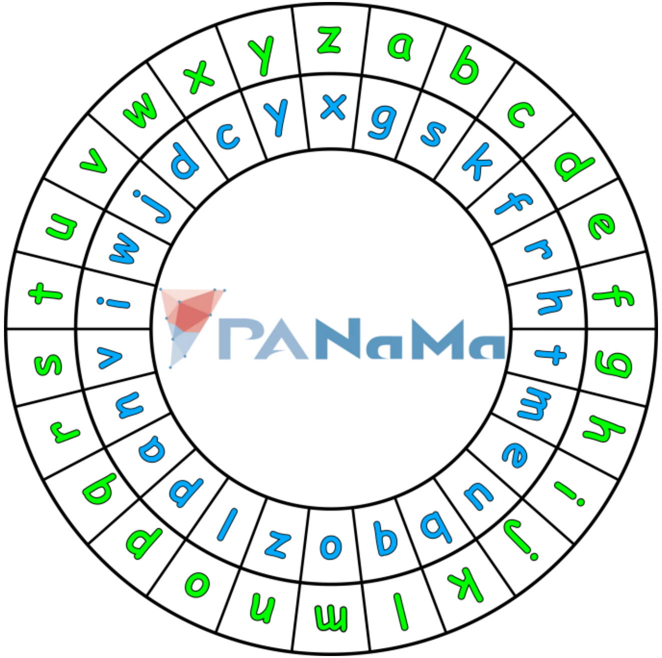
  The letter that you get when you encrypt the letter ***t.***

Frequency analysis

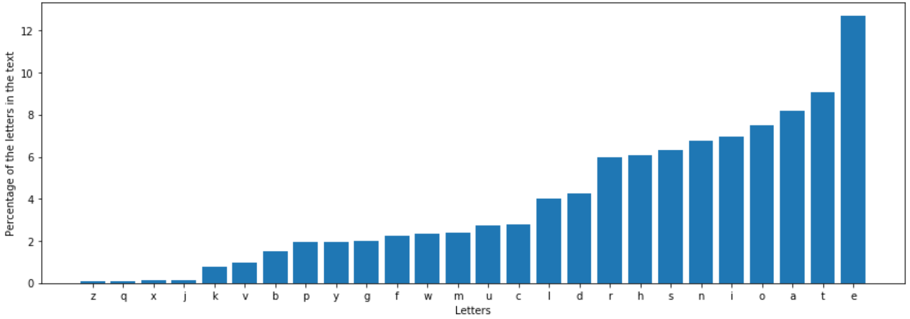
- If the message has a certain length, you can count the how often a certain letter occurs.

- How often a letter appears in the ciphertext provides information about which letter it corresponds to in the plaintext.

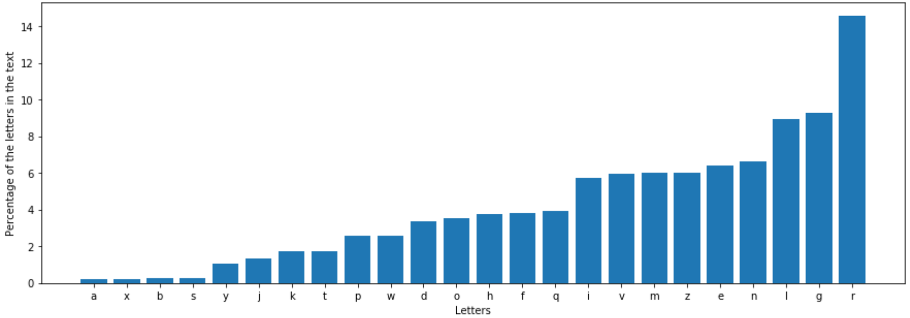
Frequency analysis


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
x g s k f r h t m e u b q o z l p a n v i w j d c y
PANaMa

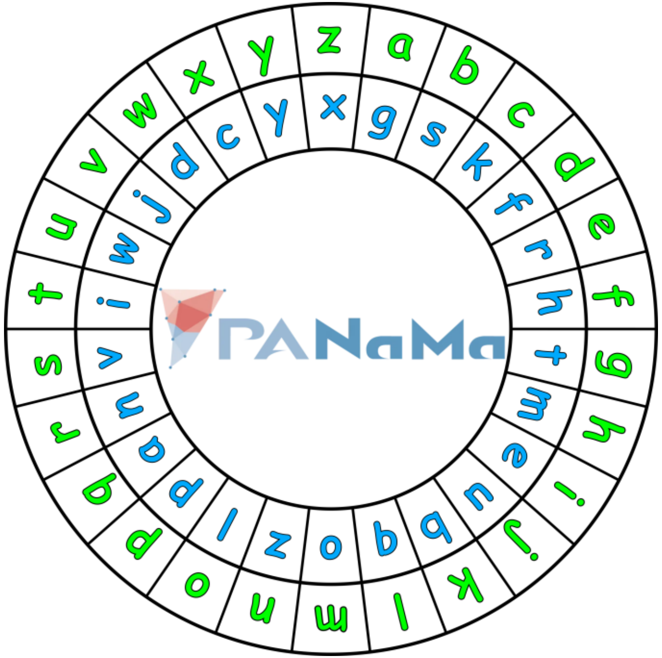
Random English text



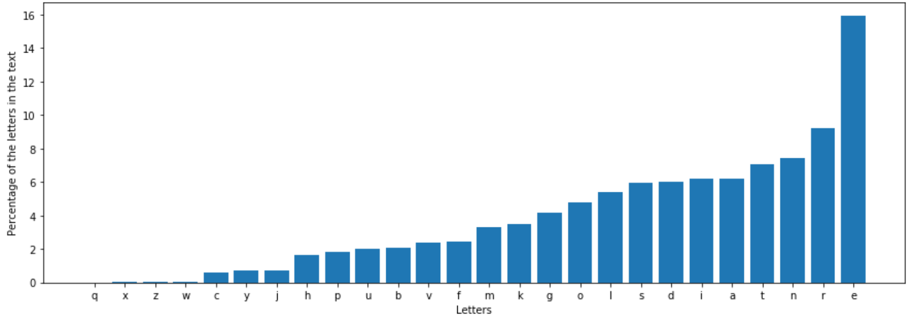
Cipher



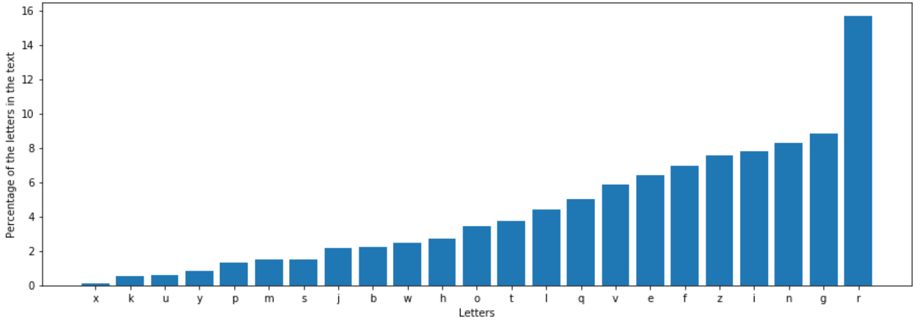
Frequency analysis


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
x g s k f r h t m e n q b o z l p a u v i w j d c y
PANaMa

Random Danish text



Cipher



Improvements of the Caesar cipher

- Problem:

  A certain plaintext letter is replaced by the same ciphertext letter.

- Solution:

  Not only does the letter dictate what it is replaced by, but also at which position of the text it appears.

The Vigenère cipher

- Origin of name: Blaise de **Vigenère** (1523 –1596)
- Improvement of the Caesar cipher
- More possible **keys**
- Protection against **frequency analysis**
- Was first broken systematically around 1850.

The Vigenère cipher

- Letters are shifted by different values
- A key doesn‘t consist of a number, but of several numbers, or:
- (to be able to better remember the key) of a **keyword**.

Example

- Message: „movementexpected“
- Key: „hallo“

message:	m	o	v	e	m	e	n	t	e	x	p	e	c	t	e	d
key:																

Example

- Message: „movementexpected“
- Key: „hallo“

message:	m	o	v	e	m	e	n	t	e	x	p	e	c	t	e	d
key:	h	a	l	l	o											

Example

- Message: „movementexpected“
- Key: „hallo“

message:	m	o	v	e	m	e	n	t	e	x	p	e	c	t	e	d
key:	h	a	l	l	o	h	a	l	l	o						

Example

- Message: „movementexpected“
- Key: „hallo“

message:	m	o	v	e	m	e	n	t	e	x	p	e	c	t	e	d
key:	h	a	l	l	o	h	a	l	l	o	h	a	l	l	o	

Example

- Message: „movementexpected“
- Key: „hallo“

message:	m	o	v	e	m	e	n	t	e	x	p	e	c	t	e	d
key:	h	a	l	l	o	h	a	l	l	o	h	a	l	l	o	h

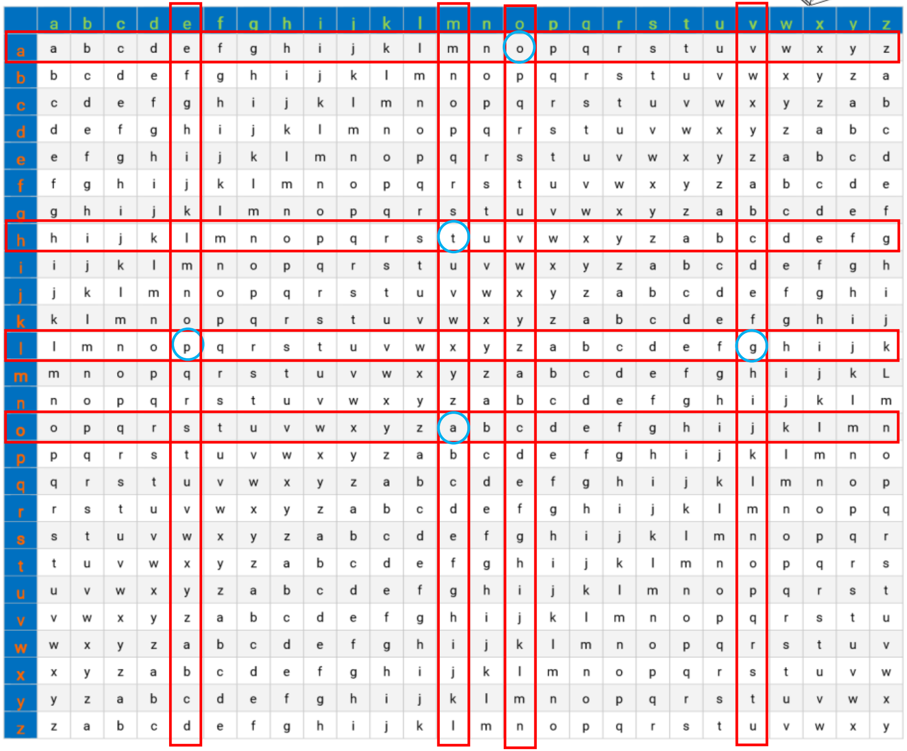
Example

The message letter is shifted by the keyword letter.

message:	m	o	v	e	m	e	n	t	e	x	p	e	c	t	e	d
key:	h	a	l	l	o	h	a	l	l	o	h	a	l	l	o	h
cipher:																

Encrypt with the Vigenère table

message:	m	o	v	e	m
key:	h	a	l	l	o
cipher:	t	o	g	p	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
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

Example

The message letter is shifted by the keyword letter.

message:	m	o	v	e	m	e	n	t	e	x	p	e	c	t	e	d
key:	h	a	l	l	o	h	a	l	l	o	h	a	l	l	o	h
cipher:	t	o	g	p	a	l	n	e	p	l	w	e	n	e	s	k

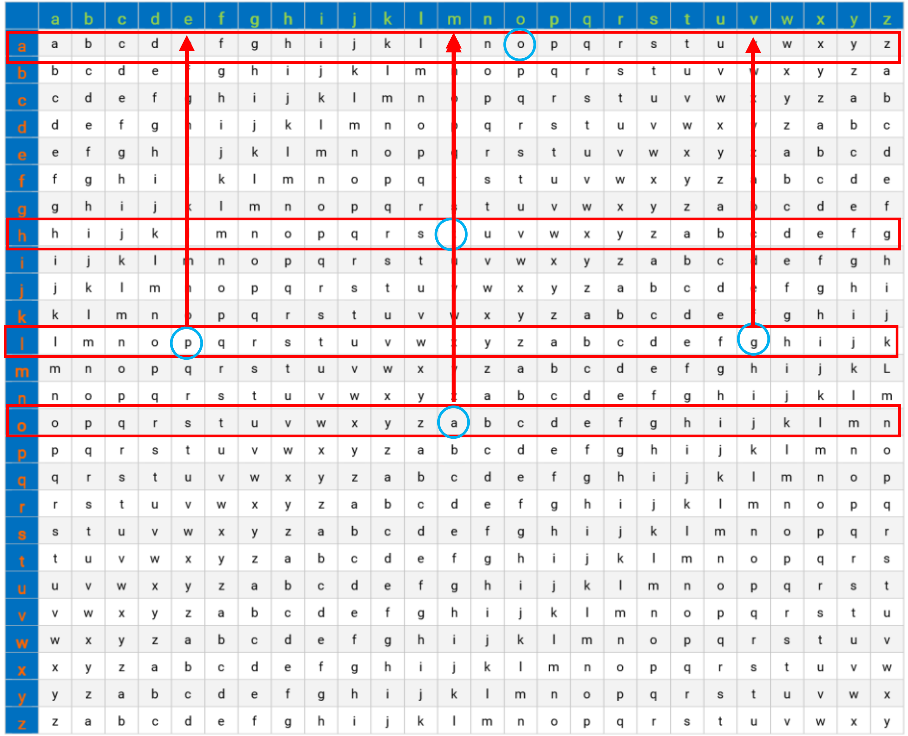
Example

The message letter is shifted back by the keyword letter.

message:																
key:	h	a	l	l	o	h	a	l	l	o	h	a	l	l	o	h
cipher:	t	o	g	p	a	l	n	e	p	l	w	e	n	e	s	k

Decrypt with the Vigenère table

message:	m	o	v	e	m
key:	h	a	l	l	o
cipher:	t	o	g	p	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
a	a	b	c	d	[illegible]	f	g	h	i	j	k	l	[illegible]	n	o	p	q	r	s	t	u	[illegible]	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	[illegible]	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	[illegible]	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

Example

The message letter is shifted back by the keyword letter.

message:	m	o	v	e	m	e	n	t	e	x	p	e	c	t	e	d
key:	h	a	l	l	o	h	a	l	l	o	h	a	l	l	o	h
cipher:	t	o	g	p	a	l	n	e	p	l	w	e	n	e	s	k

Security of the Vigenère cipher

- The key „**hallo**“ has 5 digits.
- All possible 5 digit keywords:

  $26 \cdot 26 \cdot 26 \cdot 26 \cdot 26 = 11.881.376$

- Key with 6 digits: 308.915.776
- Key with 8 digits: 208.827.064.576
- Key with 19 digits: better than „mixed up“ Caesar

Summary

- The Caesar cipher is very unsecure.
- There is only a limited amount of possible keys & a frequency analysis is possible.

Summary

- More keys: „mixed up“ Caesar
- Less vulnerable against frequency analysis: Vigenère cipher
- Under certain circumstances the Vigenère cipher is **100% secure**!