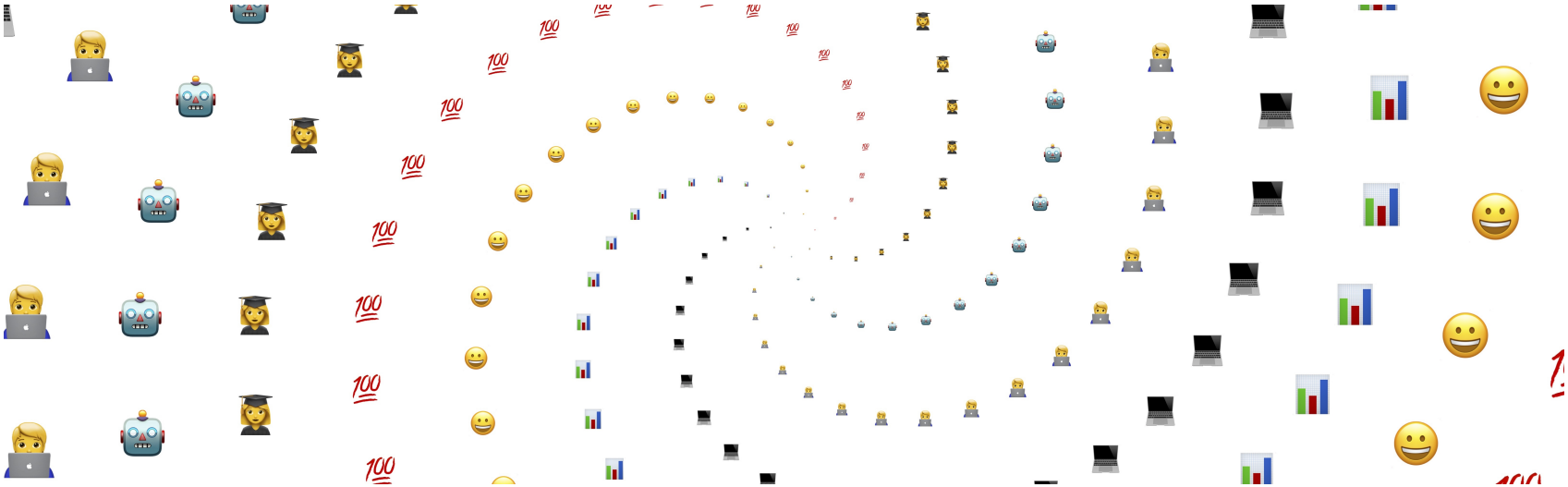
Kryptologie

Caesar-Verschlüsselung

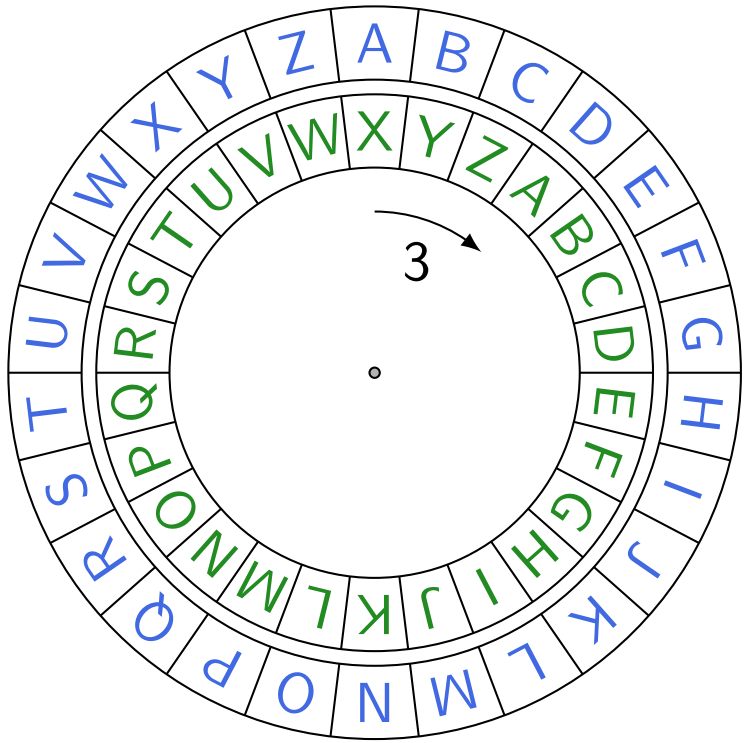
Cyril Wendl

Fachschaft Informatik
Kantonsschule im Lee



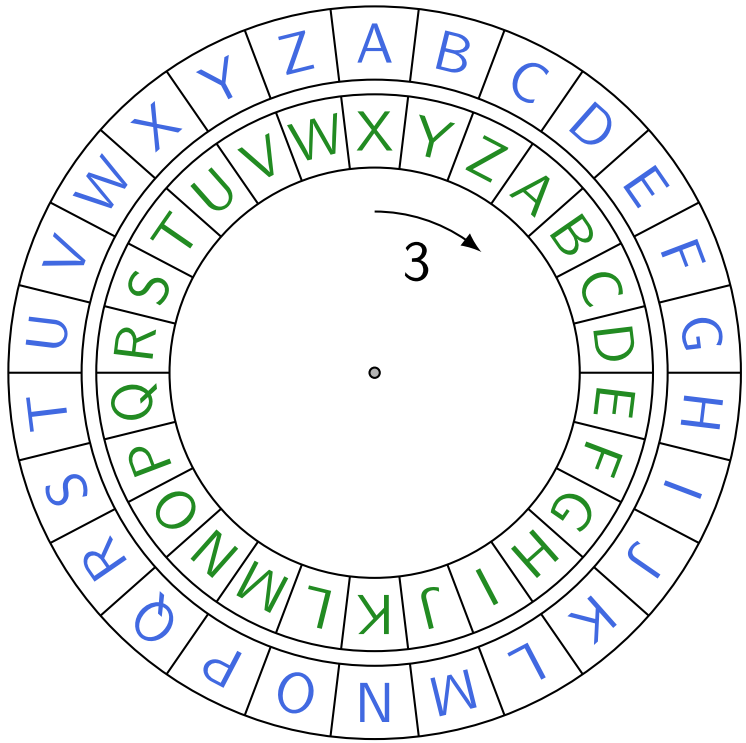
Caesar-Kryptosystem

- Zwei Drehscheiben:
  Klartext aussen,
  Geheimtext innen



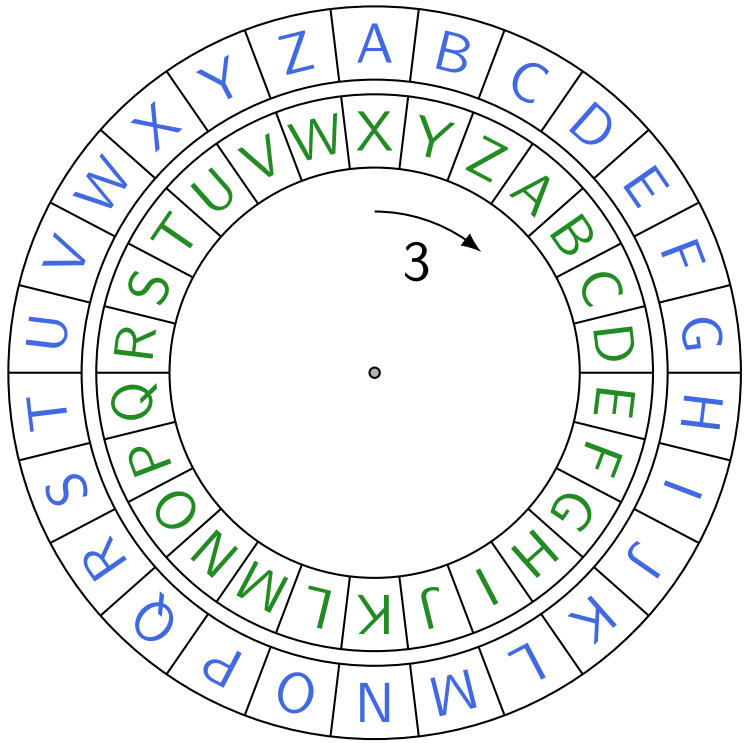
Caesar-Kryptosystem

- Zwei Drehscheiben: Klartext aussen, Geheimtext innen
- Schlüssel = Verschiebung der inneren gegenüber der ausseren Scheibe



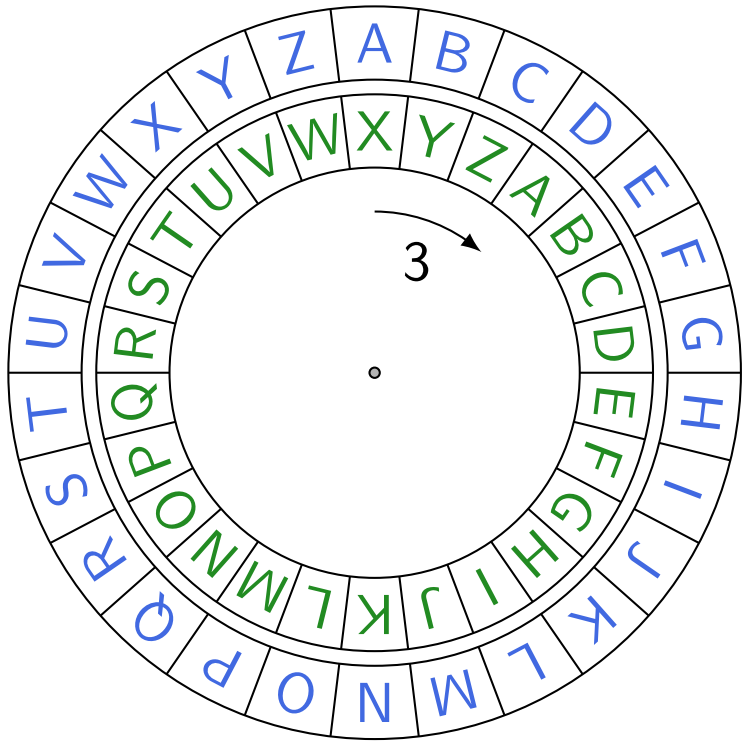
Caesar-Kryptosystem

- Zwei Drehscheiben:
  Klartext aussen,
  Geheimtext innen
- Schlüssel = Verschiebung
  der inneren gegenüber
  der ausseren Scheibe
- Z.B.: HALLO = KDOOR



Caesar-Kryptosystem

- Zwei Drehscheiben: Klartext aussen, Geheimtext innen
- Schlüssel = Verschiebung der inneren gegenüber der ausseren Scheibe
- Z.B.: HALLO = KDOOR
- Extrem unsichere Verschlüsselung: Nur 26 mögliche Schlüssel



Auftrag

Skript (auf Moodle)

- Aufgaben 1.5, 1.6

Angriff auf Caesar

Wie würden Sie folgenden Text knacken?

```
Geheimtext: PKSGTJSAYYZKPUYKLQBKXRKASJKZNG...
```

Angriff auf Caesar

Wie würden Sie folgenden Text knacken?

`Geheimtext: PKSGTJSAYYZKPUYKLQBKXRKASJKZNG...`

Häufigster Buchstabe im obigen Geheimtext: `K`
Häufigster Buchstabe im deutschen Alphabet: `E`

Angriff auf Caesar

Wie würden Sie folgenden Text knacken?

`Geheimtext: PKSGTJSAYYZKPUYKLQBKXRKASJKZNG...`

Häufigster Buchstabe im obigen Geheimtext: `K`
Häufigster Buchstabe im deutschen Alphabet: `E`

- `E`: Buchstabe mit Ordnung 4

Angriff auf Caesar

Wie würden Sie folgenden Text knacken?

`Geheimtext: PKSGTJSAYYZKPUYKLQBKXRKASJKZNG...`

Häufigster Buchstabe im obigen Geheimtext: `K`
Häufigster Buchstabe im deutschen Alphabet: `E`

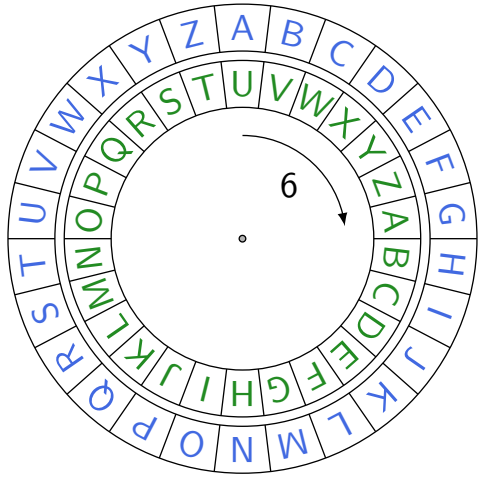
- `E`: Buchstabe mit Ordnung 4
- `K`: Buchstabe mit Ordnung 10

Angriff auf Caesar

Wie würden Sie folgenden Text knacken?

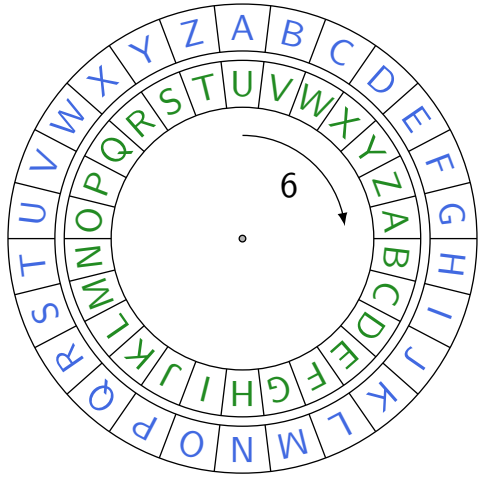
`Geheimtext: PKSGTJSAYYZKPUYKLQBKXRKASJKZNG...`

- `E`: Buchstabe mit Ordnung 4
- `K`: Buchstabe mit Ordnung 10
- Schlüssel = Verschiebung von $10 - 4 = 6$ = Buchstabe `G`



Angriff auf Caesar

Wie würden Sie folgenden Text knacken?




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

Angriff auf Caesar

Wie würden Sie folgenden Text knacken?

`NGKALOMYZKXHAINYZGHKOTJKAZYINKTZKDZKTOYZSKOYZKTYK...`

- Häufigster Buchstabe im deutschen Alphabet: `E` (= Buchstabe 5)

Angriff auf Caesar

Wie würden Sie folgenden Text knacken?

`NGKALOMYZKXHAINYZGHKOTJKAZYINKTZKDZKTOYZSKOYZKTYK...`

- Häufigster Buchstabe im deutschen Alphabet: `E` (= Buchstabe 5)
- Häufigster Buchstabe im obigen Geheimtext: `K` (= Buchstabe 11)

Angriff auf Caesar

Wie würden Sie folgenden Text knacken?

`NGKALOMYZKXHAINYZGHKOTJKAZYINKTZKDZKTOYZSKOYZKTYK...`

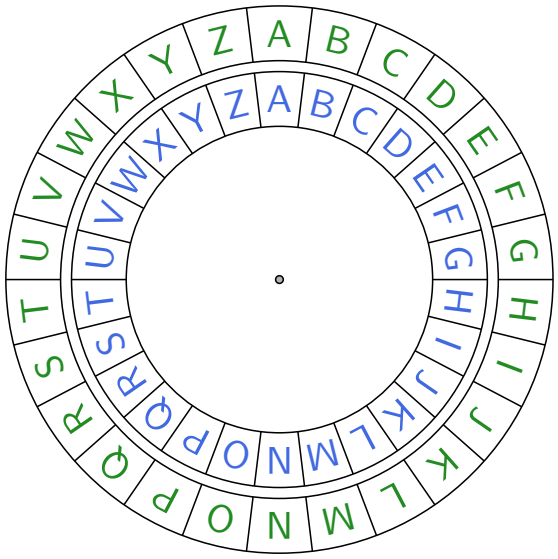
- Häufigster Buchstabe im deutschen Alphabet: `E` (= Buchstabe 5)
- Häufigster Buchstabe im obigen Geheimtext: `K` (= Buchstabe 11)
- Verschiebung von $11 - 5 = 6$

Angriff auf Caesar

Wie würden Sie folgenden Text knacken?

`NGKALOMYZKXHAINYZGHKOTJKAZYINKTZKDZKTOYZSKOYZKTYK...`

- Häufigster Buchstabe im deutschen Alphabet: `E` (= Buchstabe 5)
- Häufigster Buchstabe im obigen Geheimtext: `K` (= Buchstabe 11)
- Verschiebung von $11 - 5 = 6$
- Schlüssel $= 6$ (= Buchstabe `G`)

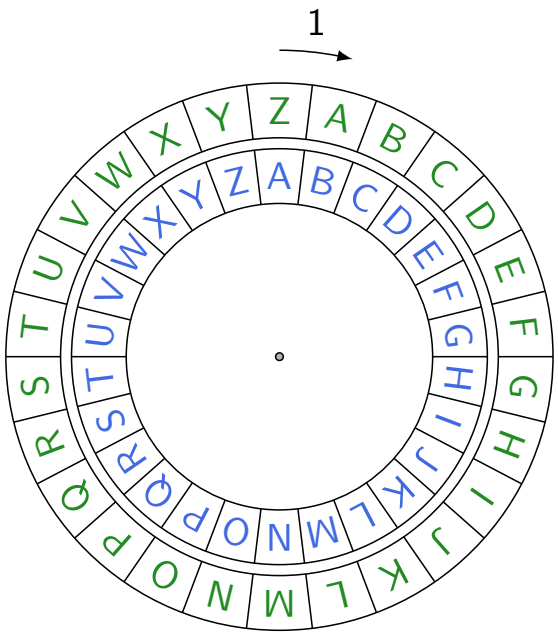


Angriff auf Caesar

Wie würden Sie folgenden Text knacken?

`NGKALOMYZKXHAINYZGHKOTJKAZYINKTZKDZKTOYZSKOYZKTYK...`

- Häufigster Buchstabe im deutschen Alphabet: `E` (= Buchstabe 5)
- Häufigster Buchstabe im obigen Geheimtext: `K` (= Buchstabe 11)
- Verschiebung von $11 - 5 = 6$
- Schlüssel $= 6$ (= Buchstabe `G`)

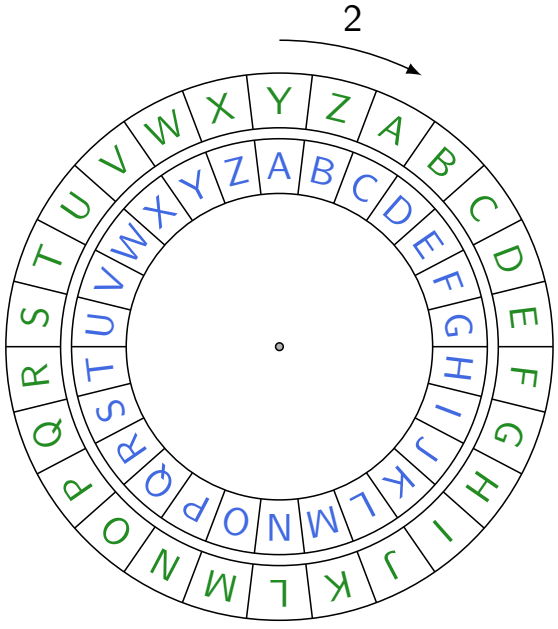


Angriff auf Caesar

Wie würden Sie folgenden Text knacken?

`NGKALOMYZKXHAINYZGHKOTJKAZYINKTZKDZKTOYZSKOYZKTYK...`

- Häufigster Buchstabe im deutschen Alphabet: `E` (= Buchstabe 5)
- Häufigster Buchstabe im obigen Geheimtext: `K` (= Buchstabe 11)
- Verschiebung von $11 - 5 = 6$
- Schlüssel $= 6$ (= Buchstabe `G`)

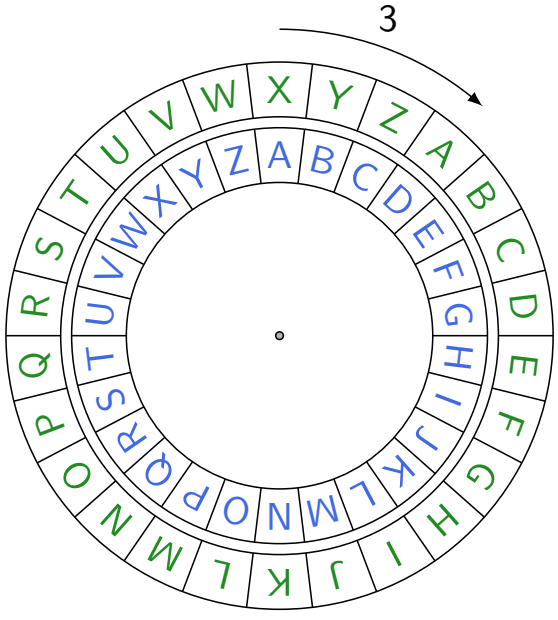


Angriff auf Caesar

Wie würden Sie folgenden Text knacken?

`NGKALOMYZKXHAINYZGHKOTJKAZYINKTZKDZKTOYZSKOYZKTYK...`

- Häufigster Buchstabe im deutschen Alphabet: `E` (= Buchstabe 5)
- Häufigster Buchstabe im obigen Geheimtext: `K` (= Buchstabe 11)
- Verschiebung von $11 - 5 = 6$
- Schlüssel $= 6$ (= Buchstabe `G`)

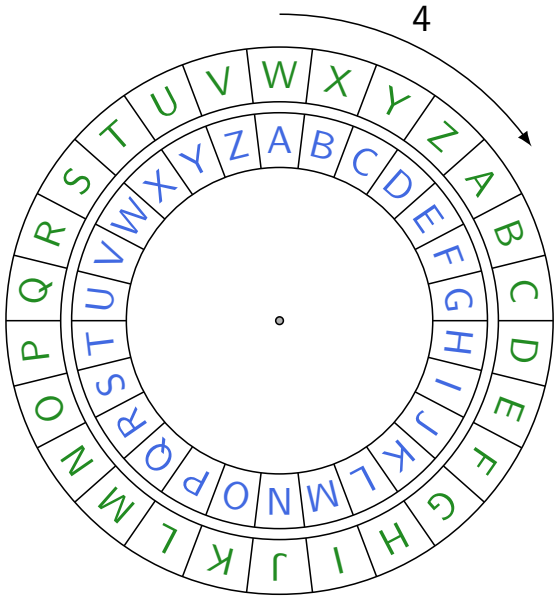


Angriff auf Caesar

Wie würden Sie folgenden Text knacken?

`NGKALOMYZKXHAINYZGHKOTJKAZYINKTZKDZKTOYZSKOYZKTYK...`

- Häufigster Buchstabe im deutschen Alphabet: `E` (= Buchstabe 5)
- Häufigster Buchstabe im obigen Geheimtext: `K` (= Buchstabe 11)
- Verschiebung von $11 - 5 = 6$
- Schlüssel $= 6$ (= Buchstabe `G`)

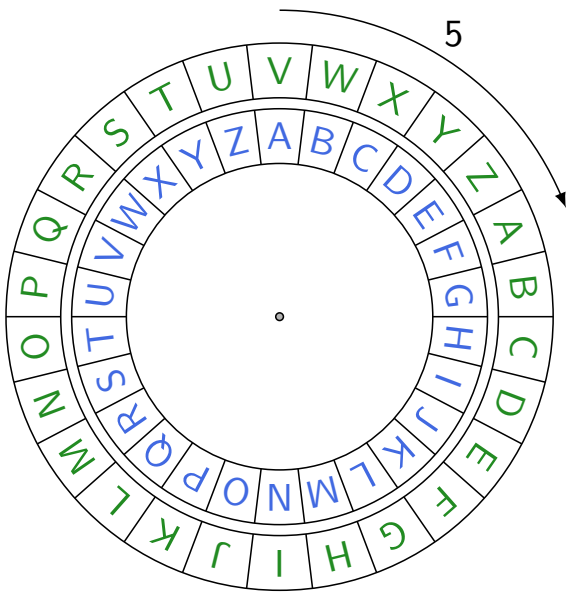


Angriff auf Caesar

Wie würden Sie folgenden Text knacken?

`NGKALOMYZKXHAINYZGHKOTJKAZYINKTZKDZKTOYZSKOYZKTYK...`

- Häufigster Buchstabe im deutschen Alphabet: `E` (= Buchstabe 5)
- Häufigster Buchstabe im obigen Geheimtext: `K` (= Buchstabe 11)
- Verschiebung von $11 - 5 = 6$
- Schlüssel $= 6$ (= Buchstabe `G`)

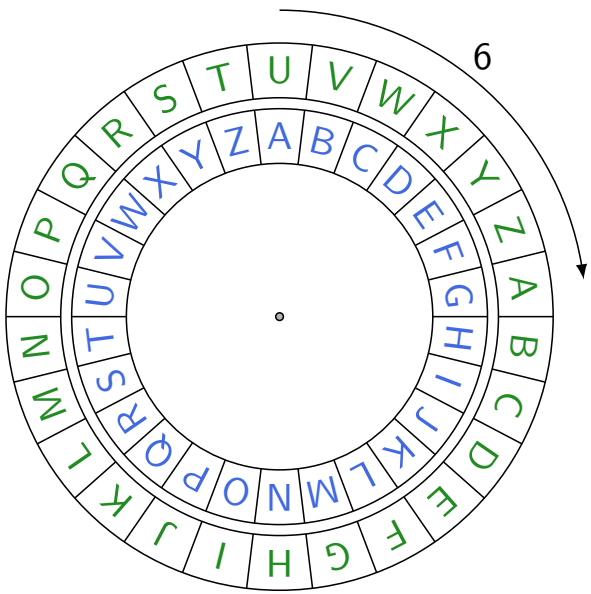


Angriff auf Caesar

Wie würden Sie folgenden Text knacken?

`NGKALOMYZKXHAINYZGHKOTJKAZYINKTZKDZKTOYZSKOYZKTYK...`

- Häufigster Buchstabe im deutschen Alphabet: `E` (= Buchstabe 5)
- Häufigster Buchstabe im obigen Geheimtext: `K` (= Buchstabe 11)
- Verschiebung von $11 - 5 = 6$
- Schlüssel $= 6$ (= Buchstabe `G`)



Auftrag:

- Erste 10 Zeichen des Texts knacken
- Challenge: Alles knacken (Schnelle)

Angriff auf Caesar

Wie würden Sie folgenden Text knacken?

`NGKALOMYZKXHAINYZGHKOTJKAZYINKTZKDZKTOYZSKOYZKTYK...`

- Häufigster Buchstabe im deutschen Alphabet: `E` (= Buchstabe 5)
- Häufigster Buchstabe im obigen Geheimtext: `K` (= Buchstabe 11)
- Verschiebung von $11 - 5 = 6$
- Schlüssel $= 6$ (= Buchstabe `G`)

Auftrag:

- Erste 10 Zeichen des Texts knacken
- Challenge: Alles knacken (Schnelle)

Wie könnte dieser Code trotzdem geknackt werden, wenn „E“ im Klartext selten oder gar nicht vorkommt?