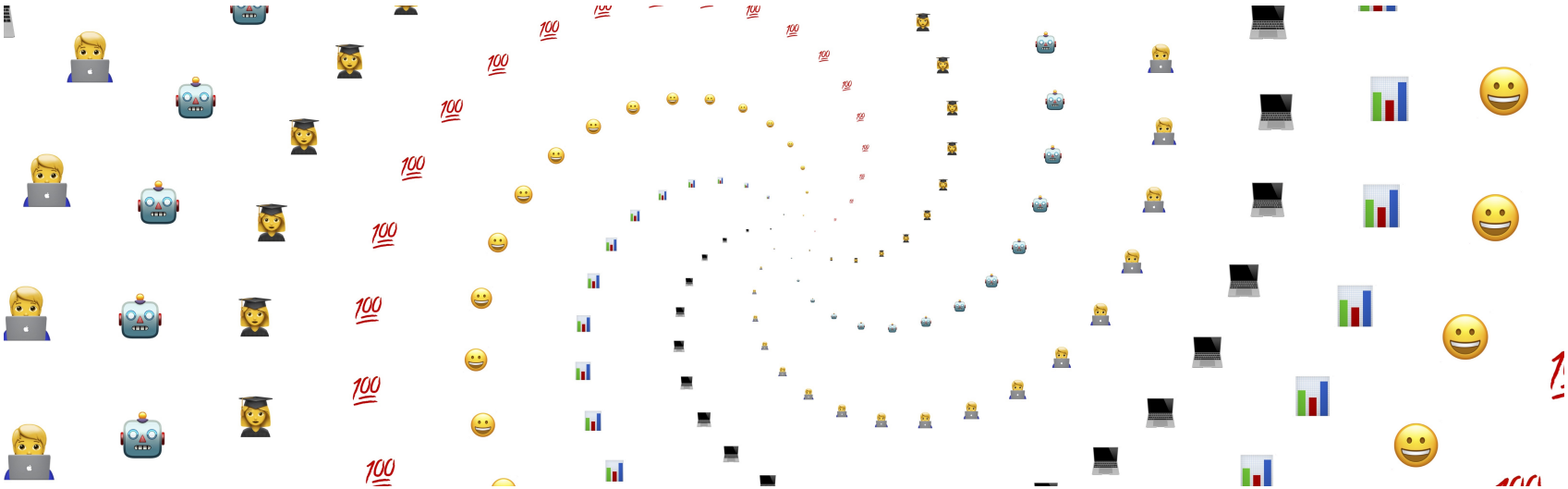
Kryptologie

Kasiski-Test

Cyril Wendl

Fachschaft Informatik
Kantonsschule im Lee



Wiederholung: 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...
```

- Vorteil gegenüber Caesar?

Wiederholung: Vigenère

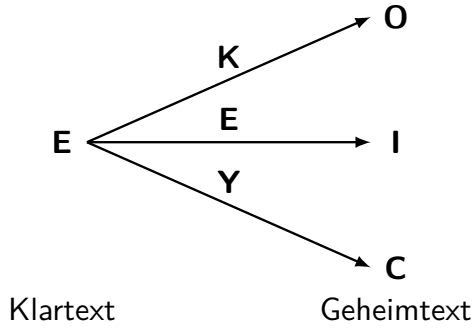
```
  Klartext: JEM|AND|MUS|STE|JOS|EFK|VER|LE...
Schlüssel: KEY|KEY|KEY|KEY|KEY|KEY|KEY|KE...
Geheimtext: TIK|KRB|WYQ|CXC|TSQ|OJI|FIP|VI...
```

- Vorteil gegenüber Caesar?

Wiederholung: 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...
```

- Vorteil gegenüber Caesar?
  Verteilung der Buchstabenhäufigkeiten



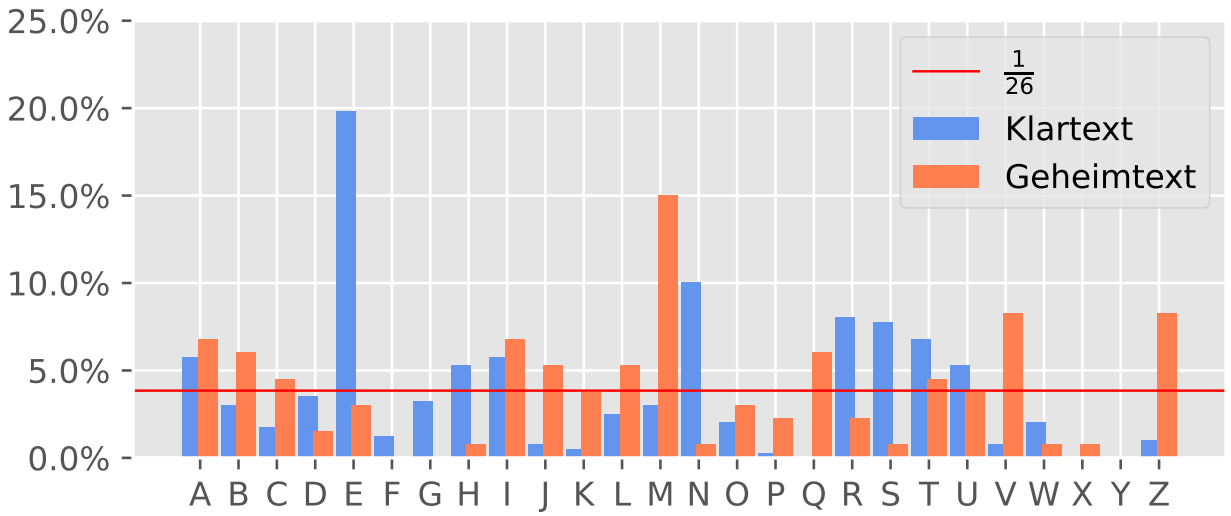
- Knackbar falls Schlüssellänge bekannt?

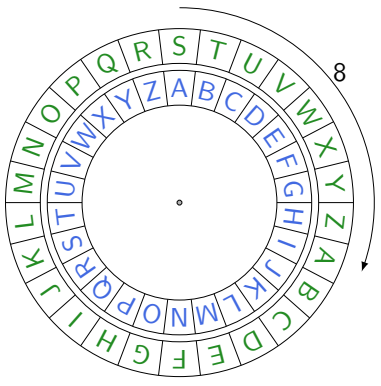
Wiederholung

Angriff auf Vigenère bei bekannter 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?)



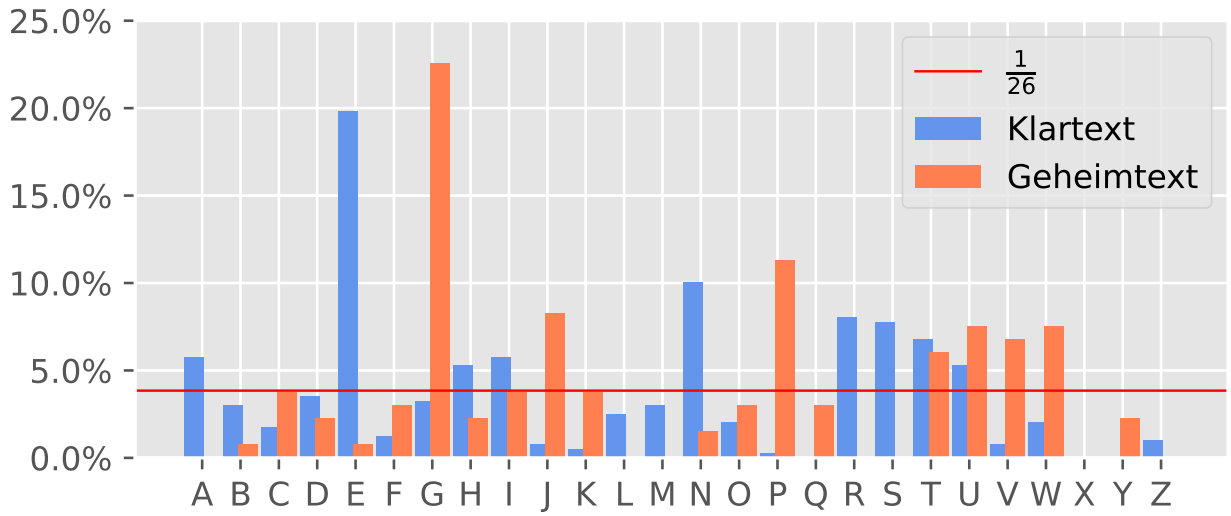


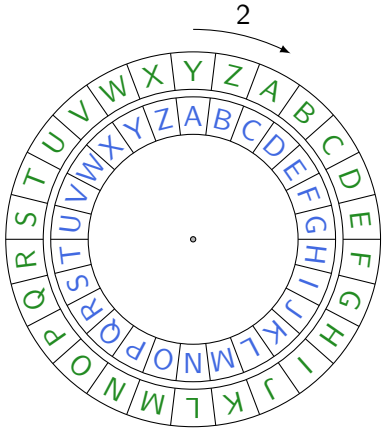
Wiederholung

Angriff auf Vigenère bei bekannter 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?)



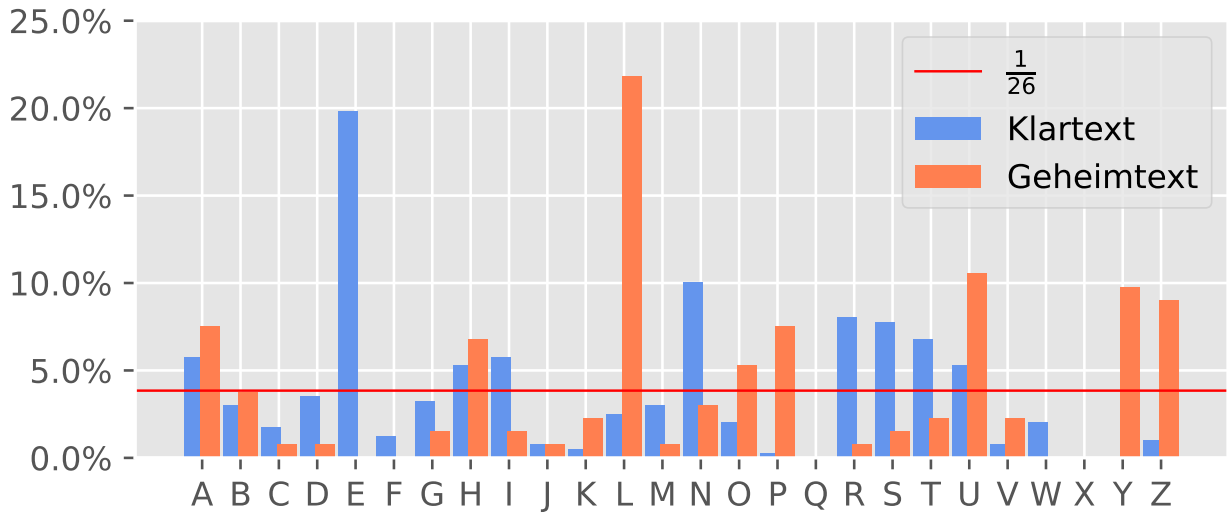


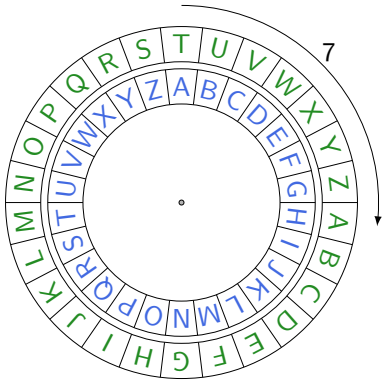
Wiederholung

Angriff auf Vigenère bei bekannter 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?)

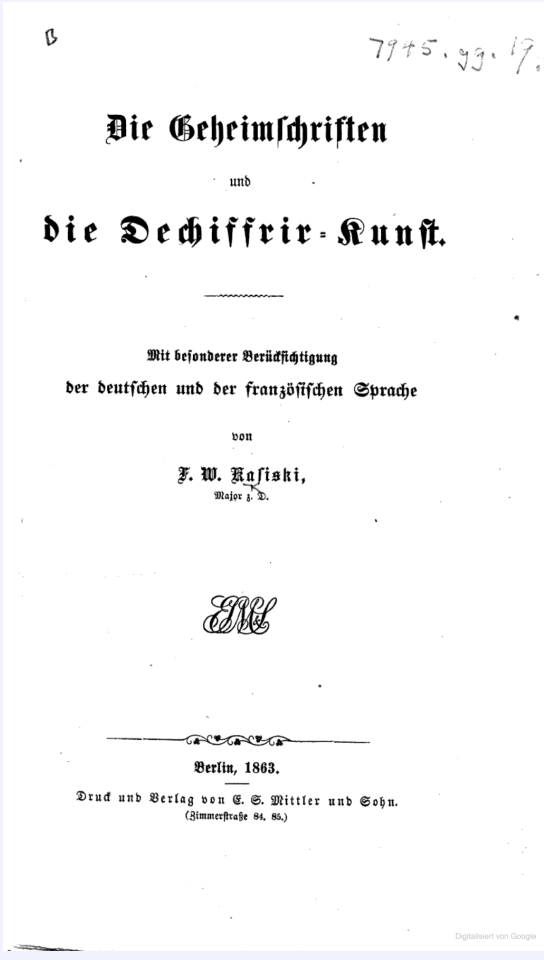




Was, wenn die Schlüssellänge unbekannt ist?

Kasiski-Test

Friedrich Kasiski



B

7945. gg. 17.

Die Geheimschriften

und

die Dechiffrir-Kunst.

Mit besonderer Berücksichtigung

der deutschen und der französischen Sprache

von

F. W. Kasiski,

Major z. D.

Berlin, 1863.

Druck und Verlag von E. S. Mittler und Sohn.

(Zimmerstraße 84. 85.)

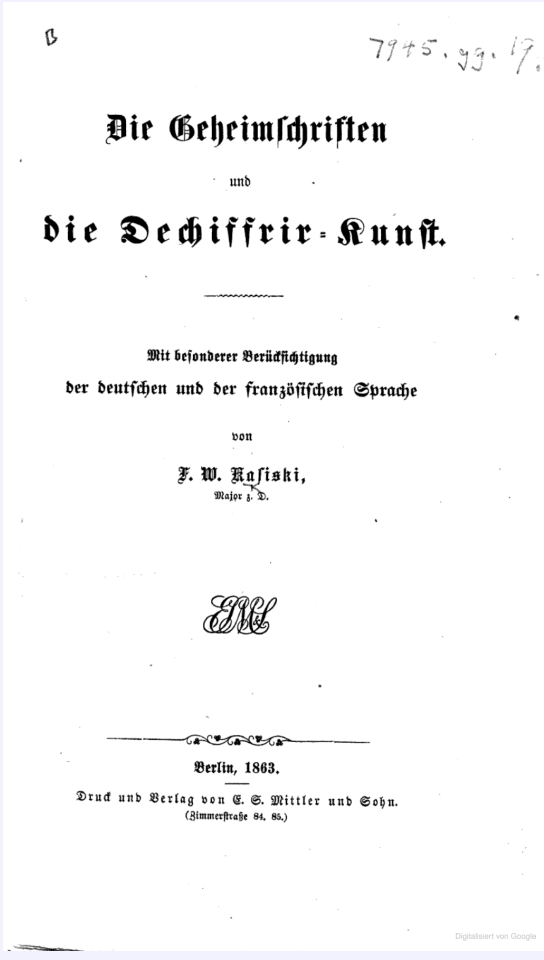
Digitalisiert von Google

Quelle (Kein Bild von Kasiski vorhanden)

- Kasiski-Test ist benannt nach dem preussischen Infanteriemajor **Friedrich Kasiski** (1805–1868).

Kasiski-Test

Friedrich Kasiski



B

7945. gg. 17.

Die Geheimschriften

und

die Dechiffrir-Kunst.

Mit besonderer Berücksichtigung

der deutschen und der französischen Sprache

von

F. W. Kasiski,

Major z. D.

Berlin, 1863.

Druck und Verlag von E. S. Mittler und Sohn.

(Zimmerstraße 84. 85.)

Digitalisiert von Google

Quelle (Kein Bild von Kasiski vorhanden)

- Kasiski-Test ist benannt nach dem preussischen Infanteriemajor **Friedrich Kasiski** (1805–1868).
- Nutzte die Tatsache, dass gewisse Bigramme / Trigramme häufiger vorkommen als andere

Häufigkeiten Bi- und Trigramme

Buchstabe	Relative Häufigkeit (%)
E	17.40
N	9.78
I	7.55
S	7.27
R	7.00
...	...

(a) Buchstabenhäufigkeit

Häufigkeiten Bi- und Trigramme

Buchstabe	Relative Häufigkeit (%)
E	17.40
N	9.78
I	7.55
S	7.27
R	7.00
...	...

(a) Buchstabenhäufigkeit

Bigramm	Relative Häufigkeit (%)
ER	3.94
EN	3.07
CH	2.73
DE	2.41
EI	2.29
...	...

(b) Bigrammhäufigkeit

Häufigkeiten Bi- und Trigramme

Buchstabe	Relative Häufigkeit (%)
E	17.40
N	9.78
I	7.55
S	7.27
R	7.00
...	...

(a) Buchstabenhäufigkeit

Bigramm	Relative Häufigkeit (%)
ER	3.94
EN	3.07
CH	2.73
DE	2.41
EI	2.29
...	...

(b) Bigrammhäufigkeit

Trigramm	Relative Häufigkeit (%)
DER	1.44
SCH	1.21
ICH	1.08
DIE	0.98
UND	0.95
...	...

(c) Trigrammhäufigkeit

Angriff auf Vigenère: Unbekannte Schlüssellänge

Kasiski-Test

MEINKLEINERREIMSCHEINTKEINERZUSEIN

Angriff auf Vigenère: Unbekannte Schlüssellänge

Kasiski-Test

```
MEINKLEINERREIMSCHEINTKEINERZUSEIN
CODECODECODECODECODECODECODECODECO
```

Angriff auf Vigenère: Unbekannte Schlüssellänge

Kasiski-Test

```
MEINKLEINERREIMSCHEINTKEINERZUSEIN
CODECODECODECODECODECODECODECODECO
OSLRMZHMPSUVGWPWEVHMPHNIKBHVBIVIKB
```

Angriff auf Vigenère: Unbekannte Schlüssellänge

Kasiski-Test

```
MEINKLEINERREIMSCHEINTKEINERZUSEIN
CODECODECODECODECODECODECODECODECO
OSLRMZHMPSUVGWPWEVHMPHNIKBHVBIVIKB
  2     7            19     24     32
```

- „HMP“ und „IKB“ kommen je zweimal im Geheimtext vor

Angriff auf Vigenère: Unbekannte Schlüssellänge

Kasiski-Test

```
MEINKLEINERREIMSCHEINTKEINERZUSEIN
CODECODECODECODECODECODECODECODECO
OSLRMZHMPSUVGWPWEVHMPHNIKBHVBIVIKB
  2     7           19    24      32
```

- „HMP“ und „IKB“ kommen je zweimal im Geheimtext vor

Angriff auf Vigenère: Unbekannte Schlüssellänge

Kasiski-Test

```
MEINKLEINERREIMSCHEINTKEINERZUSEIN
CODECODECODECODECODECODECODECODECO
OSLRMZHMPSUVGWPWEVHMPHNIKBHVBIVIKB
  2     7           19     24       32
```

- „HMP“ und „IKB“ kommen je zweimal im Geheimtext vor
  - HMP: Positionen 7 und 19. $\rightarrow$ 19-7 $= 12 = \mathbf{2} \times \mathbf{2} \times 3$

Angriff auf Vigenère: Unbekannte Schlüssellänge

Kasiski-Test

```
MEINKLEINERREIMSCHEINTKEINERZUSEIN
CODECODECODECODECODECODECODECODECO
OSLRMZHMPSUVGWPWEVHMPHNIKBHVBIVIKB
  2     7            19     24     32
```

- „HMP“ und „IKB“ kommen je zweimal im Geheimtext vor
  - HMP: Positionen 7 und 19. $\rightarrow$ 19-7 $= 12 = \mathbf{2} \times \mathbf{2} \times 3$
  - IKB: Positionen 24 und 32. $\rightarrow$ 32-24 $= 8 = \mathbf{2} \times \mathbf{2} \times 2$

Angriff auf Vigenère: Unbekannte Schlüssellänge

Kasiski-Test

```
MEINKLEINERREIMSCHEINTKEINERZUSEIN
CODECODECODECODECODECODECODECODECO
OSLRMZHMPSUVGWPWEVHMPHNIKBHVBIVIKB
  2     7           19    24      32
```

- „HMP“ und „IKB“ kommen je zweimal im Geheimtext vor
  - HMP: Positionen 7 und 19. $\rightarrow$ 19-7 $= 12 = \mathbf{2} \times \mathbf{2} \times 3$
  - IKB: Positionen 24 und 32. $\rightarrow$ 32-24 $= 8 = \mathbf{2} \times \mathbf{2} \times 2$
  - **Könnte die Schlüssellänge auch 12 sein?**

Angriff auf Vigenère: Unbekannte Schlüssellänge

Kasiski-Test

```
MEINKLEINERREIMSCHEINTKEINERZUSEIN
ABCDEFGHIJKLABCDEFGHIJKLABCDEFGHIJ??
OSLRMZHMPSUVGWPWEVHMPHNIKBHVBIVIKB
  2     7             19     24        32
```

- „HMP“ und „IKB“ kommen je zweimal im Geheimtext vor
  - HMP: Positionen 7 und 19. $\rightarrow$ 19-7 $= 12 = \mathbf{2} \times \mathbf{2} \times 3$
  - IKB: Positionen 24 und 32. $\rightarrow$ 32-24 $= 8 = \mathbf{2} \times \mathbf{2} \times 2$
  - **Könnte die Schlüssellänge auch 12 sein?**

Angriff auf Vigenère: Unbekannte Schlüssellänge

Kasiski-Test

```
MEINKLEINERREIMSCHEINTKEINERZUSEIN
ABCDEFGHIJKLABCDEFGHIJKLABCDEFGHIJ??
OSLRMZHMPSUVGWPWEVHMPHNIKBHVBIVIKB
  2      7             19      24          32
```

- „HMP“ und „IKB“ kommen je zweimal im Geheimtext vor
  - `HMP`: Positionen 7 und 19. $\rightarrow$ 19-7 $= 12 = \mathbf{2} \times \mathbf{2} \times 3$
  - `IKB`: Positionen 24 und 32. $\rightarrow$ 32-24 $= 8 = \mathbf{2} \times \mathbf{2} \times 2$
  - **Könnte die Schlüssellänge auch 12 sein?** Nein, denn dann würden die beiden `IKB` nicht auf den selben Schlüsselteil fallen!

Angriff auf Vigenère: Unbekannte Schlüssellänge

Kasiski-Test

```
MEINKLEINERREIMSCHEINTKEINERZUSEIN
CODECODECODECODECODECODECODECODECO
OSLRMZHMPSUVGWPWEVHMPHNIKBHVBIVIKB
  2     7           19     24      32
```

- „HMP“ und „IKB“ kommen je zweimal im Geheimtext vor
  - `HMP`: Positionen 7 und 19. $\rightarrow$ 19-7 $= 12 = \mathbf{2} \times \mathbf{2} \times 3$
  - `IKB`: Positionen 24 und 32. $\rightarrow$ 32-24 $= 8 = \mathbf{2} \times \mathbf{2} \times 2$
  - **Könnte die Schlüssellänge auch 12 sein?** Nein, denn dann würden die beiden `IKB` nicht auf den selben Schlüsselteil fallen!
  - Distanz zwischen Positionen = Vielfaches der Schlüssellänge?

Angriff auf Vigenère: Unbekannte Schlüssellänge

Kasiski-Test

```
MEINKLEINERREIMSCHEINTKEINERZUSEIN
CODECODECODECODECODECODECODECODECO
OSLRMZHMPSUVGWPWEVHMPHNIKBHVBIVIKB
  2     7           19     24       32
```

- „HMP“ und „IKB“ kommen je zweimal im Geheimtext vor
  - HMP: Positionen 7 und 19. $\rightarrow$ 19-7 $= 12 = \mathbf{2} \times \mathbf{2} \times 3$

$$\underbrace{\mathbf{7}}_{\text{Position 1 HMP}} + \underbrace{\mathbf{4}}_{\text{Codewort-Länge!}} \times \underbrace{\mathbf{3}}_{\text{Anzahl Codewörter}} = \underbrace{\mathbf{19}}_{\text{Position 2 HMP}}$$

  - IKB: Positionen 24 und 32. $\rightarrow$ 32-24 $= 8 = \mathbf{2} \times \mathbf{2} \times 2$
  - **Könnte die Schlüssellänge auch 12 sein?** Nein, denn dann würden die beiden IKB nicht auf den selben Schlüsselteil fallen!
  - Distanz zwischen Positionen = Vielfaches der Schlüssellänge?

Angriff auf Vigenère: Unbekannte Schlüssellänge

Kasiski-Test

```
MEINKLEINERREIMSCHEINTKEINERZUSEIN
CODECODECODECODECODECODECODECODECO
OSLRMZHMPSUVGWPWEVHMPHNIKBHVBIVIKB
  2     7           19    24      32
```

- „HMP“ und „IKB“ kommen je zweimal im Geheimtext vor
  - HMP: Positionen 7 und 19. $\rightarrow$ 19-7 $= 12 = \mathbf{2} \times \mathbf{2} \times 3$

$$\underbrace{\mathbf{7}}_{\text{Position 1 HMP}} + \underbrace{\mathbf{4}}_{\text{Codewort-Länge!}} \times \underbrace{\mathbf{3}}_{\text{Anzahl Codewörter}} = \underbrace{\mathbf{19}}_{\text{Position 2 HMP}}$$

  - IKB: Positionen 24 und 32. $\rightarrow$ 32-24 $= 8 = \mathbf{2} \times \mathbf{2} \times 2$

$$\underbrace{\mathbf{24}}_{\text{Position 1 IKB}} + \underbrace{\mathbf{4}}_{\text{Codewort-Länge!}} \times \underbrace{\mathbf{2}}_{\text{Anzahl Codewörter}} = \underbrace{\mathbf{32}}_{\text{Position 2 IKB}}$$

  - **Könnte die Schlüssellänge auch 12 sein?** Nein, denn dann würden die beiden IKB nicht auf den selben Schlüsselteil fallen!
  - Distanz zwischen Positionen = Vielfaches der Schlüssellänge?

Auftrag

Skript

- Aufgabe 1.17 (**von Hand**, Tipps genau lesen!)
- Aufgabe 1.18 (**mit Online-Tool**)
- Aufgabe 1.19
- Challenge: Anhang A lesen, Aufgaben Moodle