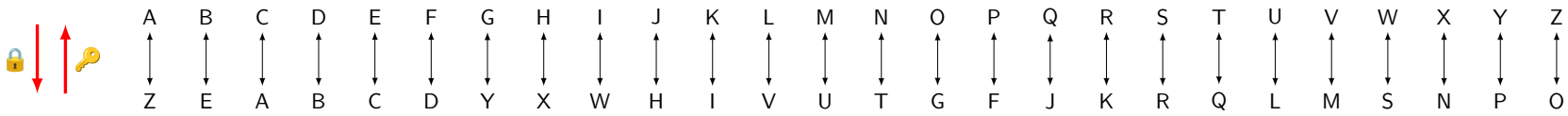
Häufigkeitsverteilung



$\rightarrow$ **Wie knacken wir so etwas?**

Häufigkeitsverteilung

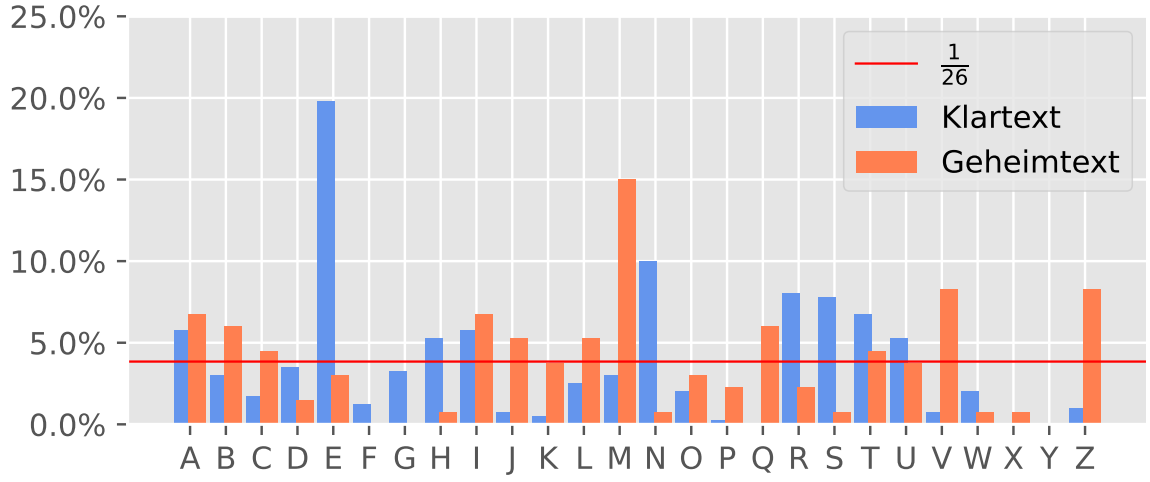
E	17,74 %
N	10,01 %
I	7,60 %
R	6,98 %
S	6,88 %
A	6,43 %
T	5,94 %
H	5,22 %
D	5,12 %

U	4,27 %
L	3,49 %
C	3,26 %
M	2,75 %
G	2,69 %
O	2,39 %
B	1,85 %
W	1,73 %
F	1,56 %

K	1,40 %
Z	1,10 %
P	0,64 %
V	0,64 %
J	0,23 %
Y	0,04 %
X	0,02 %
Q	0,01 %

$h_{\square}(T)$

$=$ Häufigkeit von Buchstabe $\square$ in Text T.



Häufigkeitsanalyse

Problem: Alle **monoalphabetischen** Kryptosysteme lassen sich mit einfacher Häufigkeitsanalyse knacken

E	17,74 %
N	10,01 %
I	7,60 %
R	6,98 %
S	6,88 %
A	6,43 %
T	5,94 %
H	5,22 %
D	5,12 %

U	4,27 %
L	3,49 %
C	3,26 %
M	2,75 %
G	2,69 %
O	2,39 %
B	1,85 %
W	1,73 %
F	1,56 %

K	1,40 %
Z	1,10 %
P	0,64 %
V	0,64 %
J	0,23 %
Y	0,04 %
X	0,02 %
Q	0,01 %

ER	3,89 %
EN	3,74 %
CH	2,97 %
TE	2,21 %
ND	2,11 %
DE	2,06 %

EIN	1,14 %
ICH	1,12 %
DER	0,92 %
SCH	0,84 %
UND	0,81 %
DIE	0,74 %

```
MUMMUXJUQYMHQOUSUTUQNGWTJQVHUMXQUXQJSUVYPPUM
----------------------------------------
```

U kommt 10-mal vor, M kommt 6-mal vor, Q kommt 6-mal vor

Häufigkeitsanalyse

Problem: Alle **monoalphabetischen** Kryptosysteme lassen sich mit einfacher Häufigkeitsanalyse knacken

E	17,74 %
N	10,01 %
I	7,60 %
R	6,98 %
S	6,88 %
A	6,43 %
T	5,94 %
H	5,22 %
D	5,12 %

U	4,27 %
L	3,49 %
C	3,26 %
M	2,75 %
G	2,69 %
O	2,39 %
B	1,85 %
W	1,73 %
F	1,56 %

K	1,40 %
Z	1,10 %
P	0,64 %
V	0,64 %
J	0,23 %
Y	0,04 %
X	0,02 %
Q	0,01 %

ER	3,89 %
EN	3,74 %
CH	2,97 %
TE	2,21 %
ND	2,11 %
DE	2,06 %

EIN	1,14 %
ICH	1,12 %
DER	0,92 %
SCH	0,84 %
UND	0,81 %
DIE	0,74 %

```
MUMMUXJUQYMHQOUSUTUQNGWTJQVHUMXQUXQJSUVYPPUM
NENNE--EI-N-I-E-E-EI-----I--EN-IE-I--E----EN
```

U=E, M=N, Q=I?

Häufigkeitsanalyse

Problem: Alle **monoalphabetischen** Kryptosysteme lassen sich mit einfacher Häufigkeitsanalyse knacken

E	17,74 %
N	10,01 %
I	7,60 %
R	6,98 %
S	6,88 %
A	6,43 %
T	5,94 %
H	5,22 %
D	5,12 %

U	4,27 %
L	3,49 %
C	3,26 %
M	2,75 %
G	2,69 %
O	2,39 %
B	1,85 %
W	1,73 %
F	1,56 %

K	1,40 %
Z	1,10 %
P	0,64 %
V	0,64 %
J	0,23 %
Y	0,04 %
X	0,02 %
Q	0,01 %

ER	3,89 %
EN	3,74 %
CH	2,97 %
TE	2,21 %
ND	2,11 %
DE	2,06 %

EIN	1,14 %
ICH	1,12 %
DER	0,92 %
SCH	0,84 %
UND	0,81 %
DIE	0,74 %

```
MUMMUXJUQYMHQOUSUTUQNGWTJQVHUMXQUXQJSUVYPPUM
NENNED-EI-N-I-E-E-EI-----I--ENDIEDI--E----EN
```

Wir fahren nun mit Trigrammen weiter: „Die“?

Häufigkeitsanalyse

Problem: Alle **monoalphabetischen** Kryptosysteme lassen sich mit einfacher Häufigkeitsanalyse knacken

E	17,74 %
N	10,01 %
I	7,60 %
R	6,98 %
S	6,88 %
A	6,43 %
T	5,94 %
H	5,22 %
D	5,12 %

U	4,27 %
L	3,49 %
C	3,26 %
M	2,75 %
G	2,69 %
O	2,39 %
B	1,85 %
W	1,73 %
F	1,56 %

K	1,40 %
Z	1,10 %
P	0,64 %
V	0,64 %
J	0,23 %
Y	0,04 %
X	0,02 %
Q	0,01 %

ER	3,89 %
EN	3,74 %
CH	2,97 %
TE	2,21 %
ND	2,11 %
DE	2,06 %

EIN	1,14 %
ICH	1,12 %
DER	0,92 %
SCH	0,84 %
UND	0,81 %
DIE	0,74 %

```
MUMMUXJUQYMHQOUSUTUQNGWTJQVHUMXQUXQJSUVYPPUM
NENNEDREI-N-I-E-E-EI----RI--ENDIEDIR-E----EN
```

„D-EI“=„Drei“?

Häufigkeitsanalyse

Problem: Alle **monoalphabetischen** Kryptosysteme lassen sich mit einfacher Häufigkeitsanalyse knacken

E	17,74 %
N	10,01 %
I	7,60 %
R	6,98 %
S	6,88 %
A	6,43 %
T	5,94 %
H	5,22 %
D	5,12 %

U	4,27 %
L	3,49 %
C	3,26 %
M	2,75 %
G	2,69 %
O	2,39 %
B	1,85 %
W	1,73 %
F	1,56 %

K	1,40 %
Z	1,10 %
P	0,64 %
V	0,64 %
J	0,23 %
Y	0,04 %
X	0,02 %
Q	0,01 %

ER	3,89 %
EN	3,74 %
CH	2,97 %
TE	2,21 %
ND	2,11 %
DE	2,06 %

EIN	1,14 %
ICH	1,12 %
DER	0,92 %
SCH	0,84 %
UND	0,81 %
DIE	0,74 %

```
MUMMU|XJUQ|YMHQOUSUTUQNGWTJQVHUM|XQU|XQJ|SUVYPPUM
NENNE|DREI|-N-I-E-E-EI----RI--EN|DIE|DIR|-E----EN
```

Man beginnt einzelne Wörter zu erkennen...

Häufigkeitsanalyse

Problem: Alle **monoalphabetischen** Kryptosysteme lassen sich mit einfacher Häufigkeitsanalyse knacken

E	17,74 %
N	10,01 %
I	7,60 %
R	6,98 %
S	6,88 %
A	6,43 %
T	5,94 %
H	5,22 %
D	5,12 %

U	4,27 %
L	3,49 %
C	3,26 %
M	2,75 %
G	2,69 %
O	2,39 %
B	1,85 %
W	1,73 %
F	1,56 %

K	1,40 %
Z	1,10 %
P	0,64 %
V	0,64 %
J	0,23 %
Y	0,04 %
X	0,02 %
Q	0,01 %

ER	3,89 %
EN	3,74 %
CH	2,97 %
TE	2,21 %
ND	2,11 %
DE	2,06 %

EIN	1,14 %
ICH	1,12 %
DER	0,92 %
SCH	0,84 %
UND	0,81 %
DIE	0,74 %

MUMMU|XJUQ|YMHQOU|SUTUQNGWTJQVHUM|XQU|XQJ|SUVYPPUM

NENNE|DREI|ANTIKE|GEHEIMSCHRIFTEN|DIE|DIR|GEFALLEN

😊

Auftrag

Skript

- 1.9
- Challenge: 1.10, 1.11

Mono- und Polyalphabetische Kryptosysteme

- **Monoalphabetisch**: Jeder Buchstabe wird immer durch denselben Buchstaben erstetzt, unabhängig von seiner Position im Klartext. **Nachteil**: Einfache Entschlüsselung durch Häufigkeitsanalyse

Mono- und Polyalphabetische Kryptosysteme

- **Monoalphabetisch**: Jeder Buchstabe wird immer durch denselben Buchstaben erstetzt, unabhängig von seiner Position im Klartext. **Nachteil**: Einfache Entschlüsselung durch Häufigkeitsanalyse
- **Polyalphabetisch**: Jeder Buchstabe kann durch unterschiedliche Buchstaben ersetzt werden