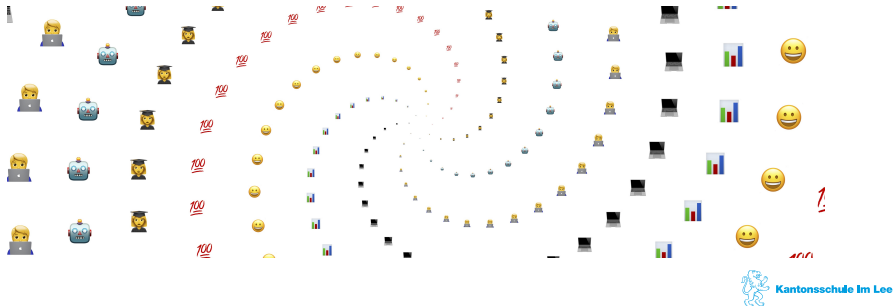


Kryptologie

Friedman'sche Charakteristik

Cyril Wendl

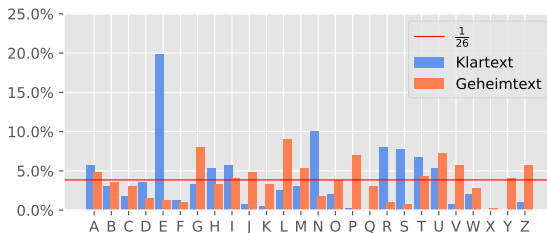
Fachschaft Informatik
Kantonsschule im Lee



Friedman'sche Charakteristik

Wie kann man die Schlüssellänge herausfinden, falls diese unbekannt ist?→ **Idee:**

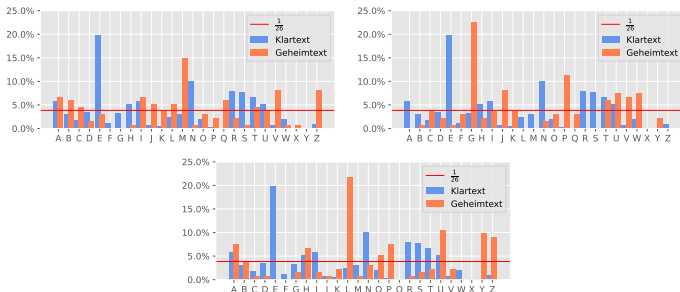
- ▶ Die Häufigkeit der Buchstaben in einem Vigenère-Geheimtext ist wegen der *polyalphabetischen* Verschlüsselung relativ *gleichmässig*...



Friedman'sche Charakteristik

Wie kann man die Schlüssellänge herausfinden, falls diese unbekannt ist?→ **Idee:**

► ...ausser wir schauen die Buchstaben in **Gruppen** an!

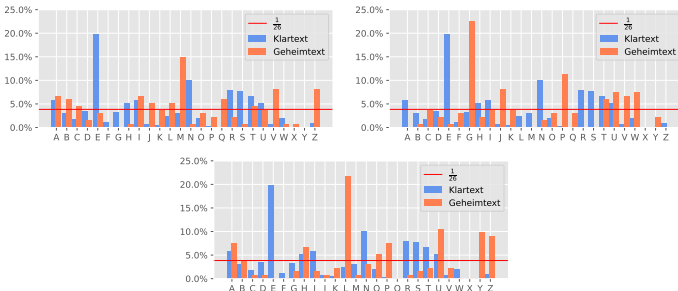


(Schrittgrösse=3)

Friedman'sche Charakteristik

Wie kann man die Schlüssellänge herausfinden, falls diese unbekannt ist?→ **Idee:**

- ...ausser wir schauen die Buchstaben in **Gruppen** an!



(Schrittgrösse=3)

- Aber wie wissen wir, wie viele Gruppen wir anschauen sollen?

Friedman-Test

William Friedman



William Friedman
([Quelle](#))

- ▶ Friedman-Test ist benannt nach dem russisch-amerikanischen Kryptologen **William Friedman** (1891–1969).



Friedman-Test

William Friedman



William Friedman
([Quelle](#))

- ▶ Friedman-Test ist benannt nach dem russisch-amerikanischen Kryptologen **William Friedman** (1891–1969).
- ▶ Gründete kurz vor Ausbruch des Zweiten Weltkrieges den Signals Intelligence Service (SIS), eine Geheimabteilung des US-Militärs zur Entzifferung feindlicher Codes und Geheimschriften.



Friedman-Test

William Friedman



William Friedman
([Quelle](#))

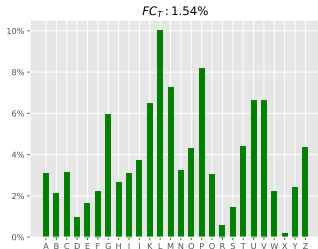
- ▶ Friedman-Test ist benannt nach dem russisch-amerikanischen Kryptologen **William Friedman** (1891–1969).
- ▶ Gründete kurz vor Ausbruch des Zweiten Weltkrieges den Signals Intelligence Service (SIS), eine Geheimabteilung des US-Militärs zur Entzifferung feindlicher Codes und Geheimschriften.
- ▶ Wie kann man **mit einer Zahl** die „Ungleichmässigkeit“ der Verteilung bestimmen?



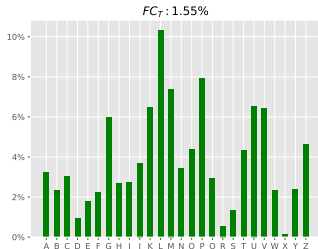
Friedman'sche Charakteristik

Schlüssellänge 2?

2 Gruppen: MU ZK JL QP AW JU MH YI IL LC ZA UP MR LZ HL SV CM
TZ BC UL GU PC IM PD QG TI PC QI LV GY MG UB UJ PN BM UZ MN AP
GY HN PK JL OT HB WS IV PW PK IH B



(a) Gruppe 1



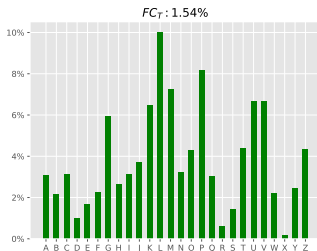
(b) Gruppe 2



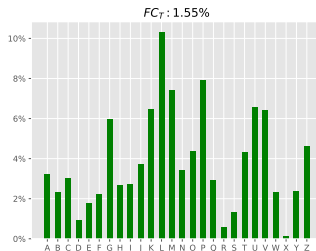
Friedman'sche Charakteristik

Schlüssellänge 2?

2 Gruppen: MU ZK JL QP AW JU MH YI IL LC ZA UP MR LZ HL SV CM
TZ BC UL GU PC IM PD QG TI PC QI LV GY MG UB UJ PN BM UZ MN AP
GY HN PK JL OT HB WS IV PW PK IH B



(a) Gruppe 1



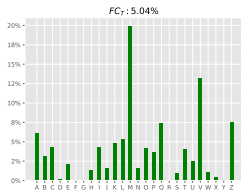
(b) Gruppe 2

Relativ gleichmässige Verteilung... 😐

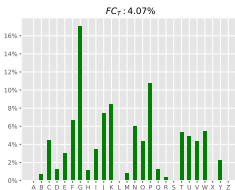
Friedman'sche Charakteristik

Schlüssellänge 3?

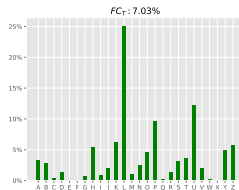
3 Gruppen: MUZ KJL QPA WJU MHY IIL LCZ AUP MRL ZHL SVC MTZ
BCU LGU PCI MPD QGT IPC QIL VGY MGU BUJ PNB MUZ MNA PGY HNP
KJL OTH BWS IVP WPK IHB



(a) Gruppe 1



(b) Gruppe 2

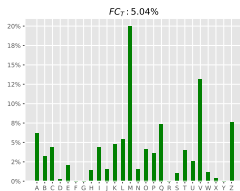


(c) Gruppe 3

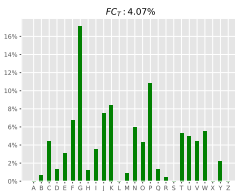
Friedman'sche Charakteristik

Schlüssellänge 3?

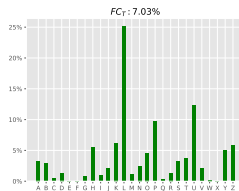
3 Gruppen: MUZ KJL QPA WJU MHY IIL LCZ AUP MRL ZHL SVC MTZ
BCU LGU PCI MPD QGT IPC QIL VGY MGU BUJ PNB MUZ MNA PGY HNP
KJL OTH BWS IVP WPK IHB



(a) Gruppe 1



(b) Gruppe 2



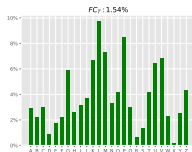
(c) Gruppe 3

Ungleiche Verteilung, grosser *peak*!... 😊

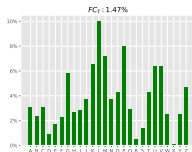
Friedman'sche Charakteristik

Schlüssellänge 4?

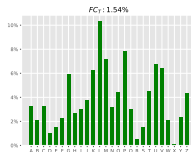
4 Gruppen: MUZK JLQP AWJU MHYI ILLC ZAUP MRLZ HLSV CMTZ
BCUL GUPC IMPD QGTI PCQI LVGY MGUB UJPN BMUZ MNAP GYHN
PKJL OTHB WSIV PWPK IHB



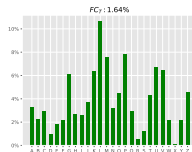
(a) Gruppe 1



(b) Gruppe 2



(c) Gruppe 3



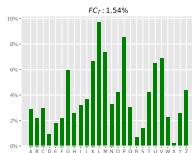
(d) Gruppe 4



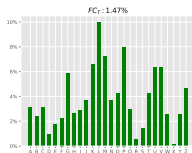
Friedman'sche Charakteristik

Schlüssellänge 4?

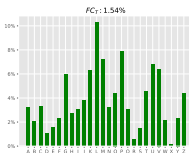
4 Gruppen: MUZK JLQP AWJU MHYI ILLC ZAUP MRLZ HLSV CMTZ
BCUL GUPC IMPD QGTI PCQI LVGY MGUB UJPN BMUZ MNAP GYHN
PKJL OTHB WSIV PWPK IHB



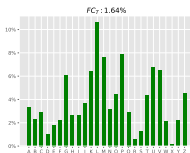
(a) Gruppe 1



(b) Gruppe 2



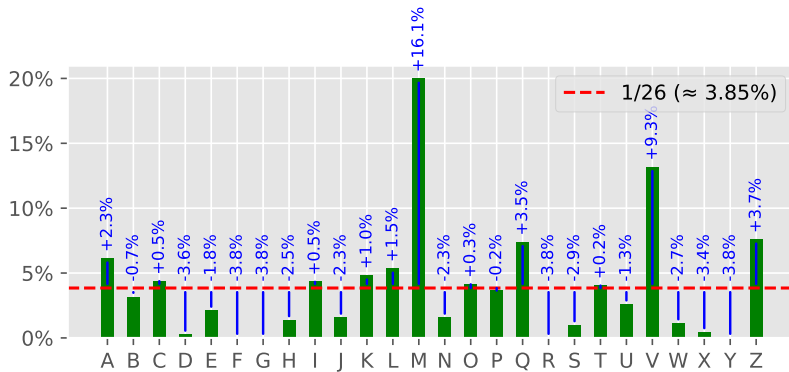
(c) Gruppe 3



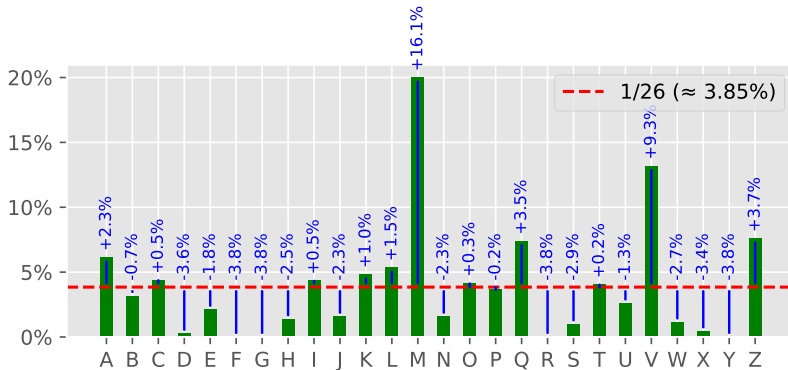
(d) Gruppe 4

Relativ gleichmässige Verteilung... 😐

Friedman'sche Charakteristik

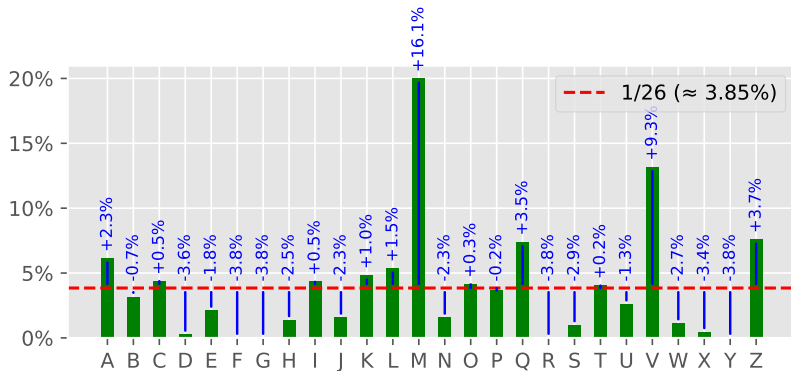


Friedman'sche Charakteristik



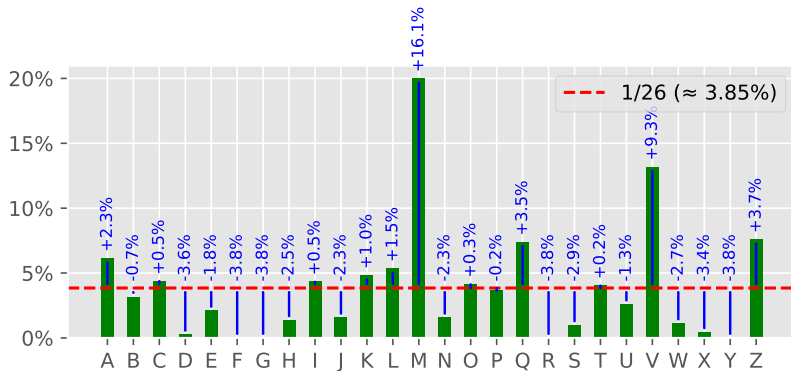
Kann man für die „(Un-)Gleichmässigkeit“ der Verteilung eine einzige Zahl finden?

Friedman'sche Charakteristik



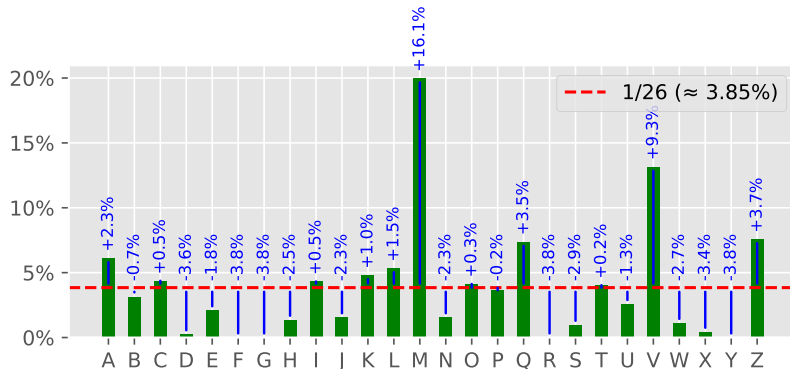
$$FC(T) = \left(h_A(T) - \frac{1}{26}\right)^2 + \left(h_B(T) - \frac{1}{26}\right)^2 + \dots + \left(h_Z(T) - \frac{1}{26}\right)^2$$

Friedman'sche Charakteristik



$$\begin{aligned} FC(T) &= \left(h_A(T) - \frac{1}{26}\right)^2 + \left(h_B(T) - \frac{1}{26}\right)^2 + \dots + \left(h_Z(T) - \frac{1}{26}\right)^2 \\ &= \sum_{\Delta \in \text{Alphabet}} \left(h_{\Delta}(T) - \frac{1}{26}\right)^2 \end{aligned}$$

Friedman'sche Charakteristik



$$\begin{aligned} FC(T) &= \left(h_A(T) - \frac{1}{26}\right)^2 + \left(h_B(T) - \frac{1}{26}\right)^2 + \dots + \left(h_Z(T) - \frac{1}{26}\right)^2 \\ &= \sum_{\Delta \in \text{Alphabet}} \left(h_{\Delta}(T) - \frac{1}{26}\right)^2 \end{aligned}$$

 $FC(T) \sim 0.0388$ für deutsche Texte

Angriff auf Vigenère: Beispiel

Friedman'sche Charakteristik + Häufigkeitsanalyse

MUZKJLQPAWJUMHYIILLCZAUPMRLZHL SVCMTZBCULGUPCIMPDQGTIP
CQILVGYMGUBUJPNBMUZMNAPGYHNP KJLOTHBWSIVPWPKIHB...



Angriff auf Vigenère: Beispiel

Friedman'sche Charakteristik + Häufigkeitsanalyse

MUZKJLQPAWJUMHYIILLCZAUPMRLZHLSVCMTZBCULGUPCIMPDQGTIP
CQILVGYMGUBUJPNBMUZMNAPGYHNPJKLOTHBWSIVPWPKIHB...

Brute force-Ansatz, um Wortlänge von Vigenère zu berechnen:

1. Alle möglichen Schlüsselwortlängen von 1 bis n ausprobieren
2. Buchstaben jeweils in Gruppen unterteilen



Angriff auf Vigenère: Beispiel

Friedman'sche Charakteristik + Häufigkeitsanalyse

MUZKJLQPAWJUMHYIILLCZAUPMRLZHL SVCMTZBCULGUPCIMP DQGTIP
CQILVGYMGUBUJPNBMUZMNAPGYHNPKJLOTHBWSIVPWPKIHB...

Brute force-Ansatz, um Wortlänge von Vigenère zu berechnen:

1. Alle möglichen Schlüsselwortlängen von 1 bis n ausprobieren
2. Buchstaben jeweils in Gruppen unterteilen
 - ▶ 2 Gruppen: MU ZK JL QP AW JU MH YI IL LC ZA UP MR LZ HL SV CM TZ BC
UL GU PC IM PD QG TI PC QI LV GY MG UB UJ PN BM UZ MN AP GY HN PK JL
OT HB WS IV PW PK IH B



Angriff auf Vigenère: Beispiel

Friedman'sche Charakteristik + Häufigkeitsanalyse

MUZKJLQPAWJUMHYIILLCZAUPMRLZHL SVCMTZBCULGUPCIMP DQGTIP
CQILVGYMGUBUJPNBMUZMNAPGYHNPKJLOTHBWSIVPWPKIHB...

Brute force-Ansatz, um Wortlänge von Vigenère zu berechnen:

1. Alle möglichen Schlüsselwortlängen von 1 bis n ausprobieren
2. Buchstaben jeweils in Gruppen unterteilen
 - ▶ 2 Gruppen: MU ZK JL QP AW JU MH YI IL LC ZA UP MR LZ HL SV CM TZ BC
UL GU PC IM PD QG TI PC QI LV GY MG UB UJ PN BM UZ MN AP GY HN PK JL
OT HB WS IV PW PK IH B
 - ▶ 3 Gruppen: MUZ KJL QPA WJU MHY IIL LCZ AUP MRL ZHL SVC MTZ BCU LGU
PCI MPD QGT IPC QIL VGY MGU BUJ PNB MUZ MNA PGY HNP KJL OTH BWS
IVP WPK IHB



Angriff auf Vigenère: Beispiel

Friedman'sche Charakteristik + Häufigkeitsanalyse

MUZKJLQPAWJUMHYIILLCZAUPMRLZHL SVCMTZBCULGUPCIMP DQGTIP
CQILVGYMGUBUJPNBMUZMNAPGYHNPKJLOTHBWSIVPWPKIHB...

Brute force-Ansatz, um Wortlänge von Vigenère zu berechnen:

1. Alle möglichen Schlüsselwortlängen von 1 bis n ausprobieren
2. Buchstaben jeweils in Gruppen unterteilen
 - ▶ 2 Gruppen: MU ZK JL QP AW JU MH YI IL LC ZA UP MR LZ HL SV CM TZ BC
UL GU PC IM PD QG TI PC QI LV GY MG UB UJ PN BM UZ MN AP GY HN PK JL
OT HB WS IV PW PK IH B
 - ▶ 3 Gruppen: MUZ KJL QPA WJU MHY IIL LCZ AUP MRL ZHL SVC MTZ BCU LGU
PCI MPD QGT IPC QIL VGY MGU BUJ PNB MUZ MNA PGY HNP KJL OTH BWS
IVP WPK IHB
 - ▶ 4 Gruppen: MUZK JLQP AWJU MHYI ILLC ZAUP MRLZ HLSV CMTZ BCUL GUPC
IMPD QGTI PCQI LVGY MGUB UJPN BMUZ MNAP GYHN PKJL OTHB WSIV PWPK
IHB



Angriff auf Vigenère: Beispiel

Friedman'sche Charakteristik + Häufigkeitsanalyse

MUZKJLQPAWJUMHYIILLCZAUPMRLZHL SVCMTZBCULGUPCIMPDQGTIP
CQILVGYMGUBUJPNBMUZMNAPGYHNPJKLOTHBWSIVPWPKIHB...

Brute force-Ansatz, um Wortlänge von Vigenère zu berechnen:

1. Alle möglichen Schlüsselwortlängen von 1 bis n ausprobieren
2. Buchstaben jeweils in Gruppen unterteilen
 - ▶ 2 Gruppen: MU ZK JL QP AW JU MH YI IL LC ZA UP MR LZ HL SV CM TZ BC
UL GU PC IM PD QG TI PC QI LV GY MG UB UJ PN BM UZ MN AP GY HN PK JL
OT HB WS IV PW PK IH B
 - ▶ 3 Gruppen: MUZ KJL QPA WJU MHY IIL LCZ AUP MRL ZHL SVC MTZ BCU LGU
PCI MPD QGT IPC QIL VGY MGU BUJ PNB MUZ MNA PGY HNP KJL OTH BWS
IVP WPK IHB
 - ▶ 4 Gruppen: MUZK JLQP AWJU MHYI ILLC ZAUP MRLZ HLSV CMTZ BCUL GUPC
IMPD QGTI PCQI LVGY MGUB UJPN BMUZ MNAP GYHN PKJL OTHB WSIV PWPK
IHB
 - ▶ ...



Angriff auf Vigenère: Beispiel

Friedman'sche Charakteristik + Häufigkeitsanalyse

MUZKJLQPAWJUMHYIILLCZAUPMRLZHL SVCMTZBCULGUPCIMP DQGTIP
CQILVGYMGUBUJPNBMUZMNA PGYHNPKJLOTHBWSIVPWPKIHB...

Brute force-Ansatz, um Wortlänge von Vigenère zu berechnen:

1. Alle möglichen Schlüsselwortlängen von 1 bis n ausprobieren
2. Buchstaben jeweils in Gruppen unterteilen
 - ▶ 2 Gruppen: MU ZK JL QP AW JU MH YI IL LC ZA UP MR LZ HL SV CM TZ BC
UL GU PC IM PD QG TI PC QI LV GY MG UB UJ PN BM UZ MN AP GY HN PK JL
OT HB WS IV PW PK IH B
 - ▶ 3 Gruppen: MUZ KJL QPA WJU MHY IIL LCZ AUP MRL ZHL SVC MTZ BCU LGU
PCI MPD QGT IPC QIL VGY MGU BUJ PNB MUZ MNA PGY HNP KJL OTH BWS
IVP WPK IHB
 - ▶ 4 Gruppen: MUZK JLQP AWJU MHYI ILLC ZAUP MRLZ HLSV CMTZ BCUL GUPC
IMPD QGTI PCQI LVGY MGUB UJPN BMUZ MNAP GYHN PKJL OTHB WSIV PWPK
IHB
 - ▶ ...
3. Durchschnittliche $FC(T)$ für alle Gruppen pro Schlüssellänge berechnen.



Angriff auf Vigenère: Beispiel

Friedman'sche Charakteristik + Häufigkeitsanalyse

MUZKJLQPAWJUMHYIILLCZAUPMRLZHL SVCMTZBCULGUPCIMP DQGTIP
CQILVGYMGUBUJPNBMUZMNAPGYHNP KJLOTHBWSIVPWP KIH B...

Brute force-Ansatz, um Wortlänge von Vigenère zu berechnen:

1. Alle möglichen Schlüsselwortlängen von 1 bis n ausprobieren
2. Buchstaben jeweils in Gruppen unterteilen
 - ▶ 2 Gruppen: MU ZK JL QP AW JU MH YI IL LC ZA UP MR LZ HL SV CM TZ BC
UL GU PC IM PD QG TI PC QI LV GY MG UB UJ PN BM UZ MN AP GY HN PK JL
OT HB WS IV PW PK IH B
 - ▶ 3 Gruppen: MUZ KJL QPA WJU MHY IIL LCZ AUP MRL ZHL SVC MTZ BCU LGU
PCI MPD QGT IPC QIL VGY MGU BUJ PNB MUZ MNA PGY HNP KJL OTH BWS
IVP WPK IHB
 - ▶ 4 Gruppen: MUZK JLQP AWJU MHYI ILLC ZAUP MRLZ HLSV CMTZ BCUL GUPC
IMPD QGTI PCQI LVGY MGUB UJPN BMUZ MNAP GYHN PKJL OTHB WSIV PWP K
IHB
 - ▶ ...
3. Durchschnittliche $FC(T)$ für alle Gruppen pro Schlüssellänge berechnen.
4. Wenn die richtige Schlüssellänge gewählt wurde, sollte $FC(T) \sim 0.0388$ sein.

Angriff auf Vigenère: Beispiel

Friedman'sche Charakteristik + Häufigkeitsanalyse

MUZKJLQPAWJUMHYIILLCZAUPMRLZHL SVCMTZBCULGUPCIMP DQGTIP
CQILVGYMGUBUJPNBMUZMNAPGYHNP KJLOTHBWSIVPWP KIH B...

Brute force-Ansatz, um Wortlänge von Vigenère zu berechnen:

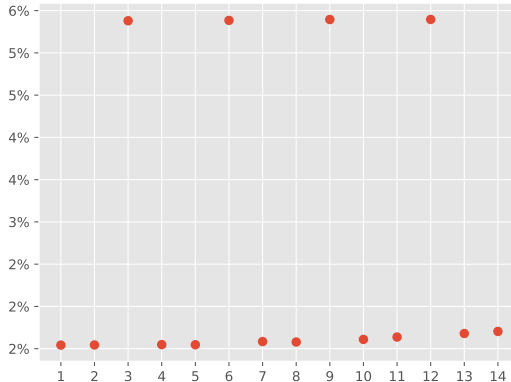
1. Alle möglichen Schlüsselwortlängen von 1 bis n ausprobieren
2. Buchstaben jeweils in Gruppen unterteilen
 - ▶ 2 Gruppen: MU ZK JL QP AW JU MH YI IL LC ZA UP MR LZ HL SV CM TZ BC
UL GU PC IM PD QG TI PC QI LV GY MG UB UJ PN BM UZ MN AP GY HN PK JL
OT HB WS IV PW PK IH B
 - ▶ 3 Gruppen: MUZ KJL QPA WJU MHY IIL LCZ AUP MRL ZHL SVC MTZ BCU LGU
PCI MPD QGT IPC QIL VGY MGU BUJ PNB MUZ MNA PGY HNP KJL OTH BWS
IVP WPK IHB
 - ▶ 4 Gruppen: MUZK JLQP AWJU MHYI ILLC ZAUP MRLZ HLSV CMTZ BCUL GUPC
IMPD QGTI PCQI LVGY MGUB UJPN BMUZ MNAP GYHN PKJL OTHB WSIV PWP K
IHB
 - ▶ ...
3. Durchschnittliche $FC(T)$ für alle Gruppen pro Schlüssellänge berechnen.
4. Wenn die richtige Schlüssellänge gewählt wurde, sollte $FC(T) \sim 0.0388$ sein.



Angriff auf Vigenère: Beispiel

Friedman'sche Charakteristik + Häufigkeitsanalyse

MUZKJLQPAWJUMHYIILLCZAUPMRLZHL SVCMTZBCULGUPCIMP DQGTIP
CQILVGYMGUBUJPNBMUZMNAPGYHNP KJLOTHBWSIVPWP KIH B...



→ Zeigt, wie ungleich die Buchstaben verteilt sind, wenn wir sie in 1, 2, 3, 4, ... Gruppen aufteilen.

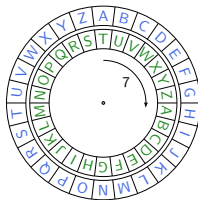
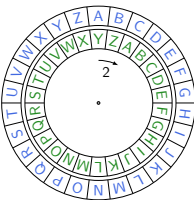
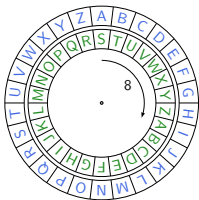
→ Hier sehen wir visuell, dass die Wortlänge 3 sein muss.

Angriff auf Vigenère: Beispiel

Friedman'sche Charakteristik + Häufigkeitsanalyse

MUZ KJL QPA WJU MHY IIL LCZ AUP MRL ZHL SVC MTZ BCU LGU PCI
MPD QGT IPC QIL VGY MGU BUJ PNB MUZ MNA PGY HNP KJL OTH BWS
IVP WPK IHB

→ Häufigster Buchstaben pro Gruppe: M, G, L



Auftrag

- ▶  Aufgaben 1.21 - 1.23
- ▶  Challenge: 1.24 - 1.26