

Code-Break-Party



January 27th, 2020

Outline

Substitutions-Chiffren

- Cäsar Chiffre

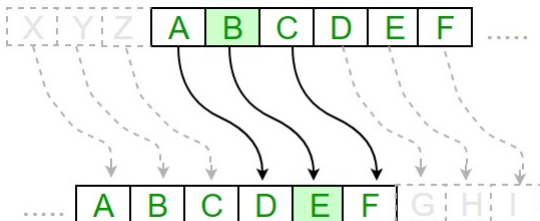
- Monoalphabetische Substitution

- Vigenère-Chiffre

Enigma

Cäsar Chiffre

- Klartext (plain text): ATTACKATDAWN
- Geheimtext (cipher text): DWWDFNDWGDZQ
- Schlüssel: 3 → um 3 Stellen nach rechts verschieben



Cäsar Kryptoanalyse

- Es gibt nur eine begrenzte Anzahl von Schlüsseln (nur 25 sinnvolle Verschiebungen)
- Brute-Force-Angriff → alle Kombinationen durchprobieren:

Schlüssel	Entschlüsselter Text
0	DWPDFNDWGDZQ
1	CVVCEMCVFCYP
2	BUUBDLBUEBXO
3	ATTACKATDAWN
⋮	⋮

Monoalphabetische Substitution (Kryptogram)

- Anstelle für jeden Buchstaben den gleichen Offset zu verwenden, werden unterschiedliche Buchstaben verschieden verschoben

- Substitutionstabelle:

Klartext Alphabet	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Geheimtext Alphabet	MOSKAUBCDEFGHIJLNPQRTVWXYZ

- Beispiel:

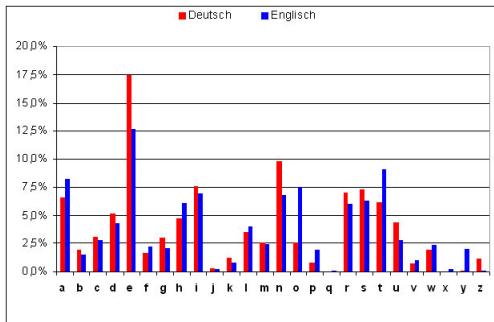
FL EE AT ONCE. WE ARE DISCOVERED.

wird zu

UGAA MR JISA. WA MPA KDQSJVAPAK.

Frequenzanalyse

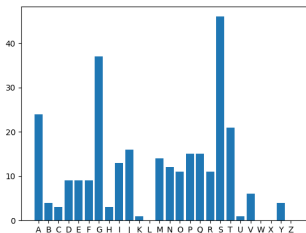
- Buchstaben kommen in natürlicher Sprache mit unterschiedlicher Häufigkeit vor
- Im Deutschen: E, I, N sind häufig, Q, X, Y sind selten



- Statistische Eigenschaften des Klartexts werden von einer Substitutionschiffre nicht verändert

Beispiel Frequenzanalyse

Tg stgsf Djia tf Ejnsg, nm dseqs stg Ajeetq. Gtiaq
tg stgsf csriaqsg, piafrqythsg Djia, vj sp gmia Fjnso
otsiaq rgn Vrofytkcsd uvg nsg Vmsgnsg asomeamsghsg,
rgn mria gtiaq tg stgso qojibsgsg, bmadsg Pmgnhores
jags Qtpias rgn Pqrsads, vj fmg ptia yrf Sppsg
atgpsqysg bjsggqs: gstg, nmp Djia vmo stgs
Ajeetqajsads, rgn nmp astppq, sp vmo psao
bjfcjoqmesd.

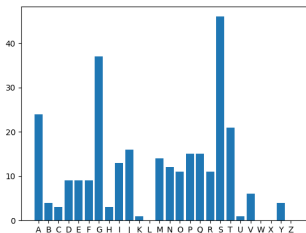


Ciphertext Alphabet

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Beispiel Frequenzanalyse

Tg etgef Djia tf Ejneg, nm deeqe etg Ajeetq. Gtiaq
 tg etgef ceriaqeg, piafrqytheg Djia, vj ep gmia Fjneoo
 oteiaq rgn Vrofytkced uvg neg Vmegneg aeomeamegheg,
 rgn mria gtiaq tg etgeo qojibegeg, bmadeg Pmgnhoree
 jage Qtpiae rgn Pqreade, vj fmg ptia yrf Epppeg
 atgpeqyeg bjeggqe: getg, nmp Djia vmo etge
 Ajeetqajeade, rgn nmp aetppq, ep vmo peao
 bjfcjoqmeed.



Ciphertext Alphabet

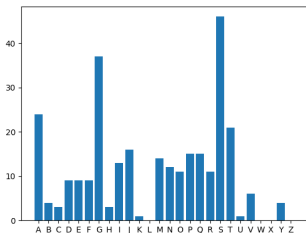
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Plaintext Alphabet

E

Beispiel Frequenzanalyse

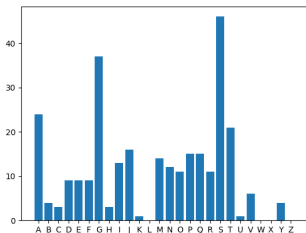
Tn etnef Djia tf Ejnen, nm deege etn Ajeetq. Ntiaq
 tn etnef ceriaqen, piafrqythen Djia, vj ep nmia Fjne
 oteiaq rnn Vrofytkced ujn nen Vmennen aeomeamenhen,
 rnn mria ntiaq tn etneo qojibenen, bmaden Pmnnhoree
 jane Qtpiae rnn Pqreade, vj fmn ptia yrf Eppen
 atnpeqyen bjennqe: netn, nmp Djia vmo etne
 Ajeetqajeade, rnn nmp aetppq, ep vmo peao
 bjfcjoqmeed.



Ciphertext Alphabet	ABCDEFGHIJKLMNOPQRSTUVWXYZ																									
Plaintext Alphabet	N													E												

Beispiel Frequenzanalyse

In einef Djia if Ejnen, nm deege ein Ajeeiq. Niiag
in einef ceriaqen, piafrqyihen Djia, vj ep nmia Fjne
oieiaq rnn Vrofyikced ujn nen Vmennen aeomeamenhen,
rnn mria niiag in eineo qojibenenen, bmaden Pmnnhoree
jane Qipiae rnn Pqreade, vj fmn piia yrf Eppen
ainpeqyen bjennqe: nein, nmp Djia vmo eine
Ajeeiqajeade, rnn nmp aeippq, ep vmo peao
bjfcjoqmeed.



Ciphertext Alphabet

ABCDEFGHIJKLMNOPQRSTUVWXYZ

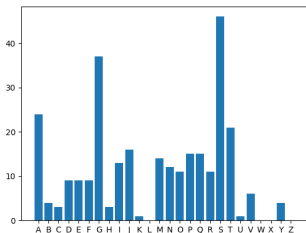
Plaintext Alphabet

N

EI

Beispiel Frequenzanalyse

In einem Djia im Ejnen, nm deege ein Ajeeiq. Niiag
in einem ceriaqen, piamrqyihen Djia, vj ep nmia Mjne
oieiaq rnn Vromyikced ujn nen Vmennen aeomeamenhen,
rnn mria niiag in eineo qojibenen, bmaden Pmnnhoree
jane Qipiae rnn Pqreade, vj mmn piia yrm Eppen
ainpeqyen bjennqe: nein, nmp Djia vmo eine
Ajeeiqajeade, rnn nmp aeippq, ep vmo peao
bjmcjoqmeed.



Ciphertext Alphabet

ABCDEFGHIJKLMNOPQRSTUVWXYZ

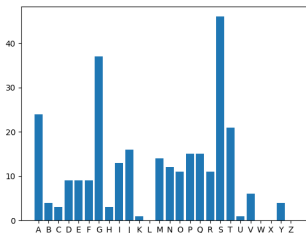
Plaintext Alphabet

MN

EI

Beispiel Frequenzanalyse

In einem Djia im Ejnen, na deege ein Ajeeiq. Niiag in einem ceriaqen, piamrqyihen Djia, vj ep naia Mjneooieiaq rnn Vromyikced ujn nen Vaennen aeoaeeaaenhen, rnn aria niiag in eineo qojibenen, baaden Pannhoree jane Qipiae rnn Pqreade, vj man piia yrm Eppen ainpeqyen bjennqe: nein, nap Djia vao eine Ajeeiqajeade, rnn nap aeippq, ep vao peao bjmcjoqaed.



Ciphertext Alphabet

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Plaintext Alphabet

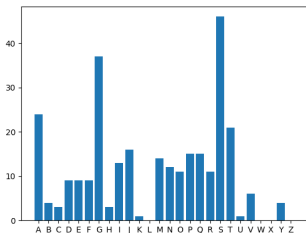
MN

A

EI

Beispiel Frequenzanalyse

In einem Djia im Ejden, da deege ein Ajeeiq. Niiag in einem ceuiaqen, piamuqyihen Djia, vj ep naia Mjdeo oieiaq und Vuomyikced ujn den Vaenden aeoaeaaenhen, und auia niiag in eineo qojibenen, baaden Pandhouee jane Qipiae und Pqueade, vj man piia yum Eppen ainpeqyen bjennqe: nein, dap Djia vao eine Ajeeiqajeade, und dap aeippq, ep vao peao bjmcjoqaed.



Ciphertext Alphabet

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Plaintext Alphabet

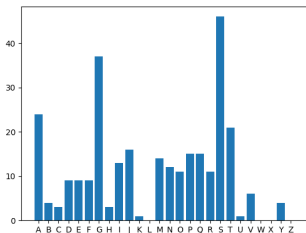
MN

AD

UEI

Beispiel Frequenzanalyse

In einem Djia im Ejden, da deege ein Ajeeiq. Niiag
in einem ceuiaqen, siamuqyihen Djia, vj es naia Mjdeo
oieiaq und Vuomyikced ujn den Vaenden aeoaeaaenhen,
und auia niiag in eineo qojibenen, baaden Sandhouee
jane Qisiae und Squeade, vj man siia yum Essen
ainseqyen bjennqe: nein, das Djia vao eine
Ajeeiqajeade, und das aeissq, es vao seao
bjmcjoqaed.



Ciphertext Alphabet

ABCDEFGHIJKLMNOPQRSTUVWXYZ

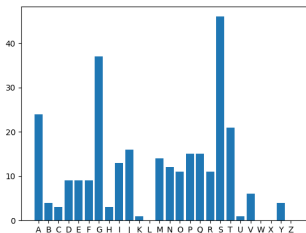
Plaintext Alphabet

MN

AD S UEI

Beispiel Frequenzanalyse

In einem Djia im Ejden, da deege ein Ajeeiq. Niiag in einem ceuiaqen, siamuqzihen Djia, vj es naia Mjdeo oieiaq und Vuomzikced ujn den Vaenden aeoaeaaenhen, und auia niiag in eineo qojibenen, baaden Sandhouee jane Qisiae und Squeade, vj man siia zum Essen ainseqzen bjennqe: nein, das Djia vao eine Ajeeiqajeade, und das aeissq, es vao seao bjmcjoqaed.



Ciphertext Alphabet

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Plaintext Alphabet

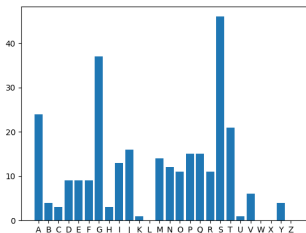
MN

AD S UEI

Z

Beispiel Frequenzanalyse

In einem Djia im Ejden, da deege ein Ajeeiq. Niiag
in einem ceuiaqen, siamuqzihen Djia, vj es naia Mjder
rieiaq und Vurmzikced ujn den Vaenden aeraeaaenhen,
und auia niiag in einer qrijibenen, baaden Sandhruee
jane Qisiae und Squeade, vj man siia zum Essen
ainseqzen bjennqe: nein, das Djia var eine
Ajeeiqajeade, und das aeissq, es var sear
bjmcjrqaed.



Ciphertext Alphabet

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Plaintext Alphabet

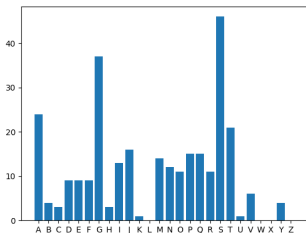
MN

ADRS UEI

Z

Beispiel Frequenzanalyse

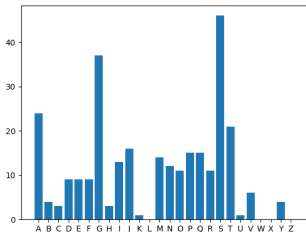
In einem Djih im Ejden, da deete ein Hjeeit. Niiht in einem ceuihten, sihmutzihen Djih, vj es naih Mjder rieiht und Vurmzikced ujn den Vaenden heraehaenhen, und auih niiht in einer trjibenen, bahden Sandhruee jhne Tisihe und Stuehde, vj man siih zum Essen hinsetzen bjennte: nein, das Djih var eine Hjeeithjehde, und das heisst, es var sehr bjmcjrtaeed.



Ciphertext Alphabet	ABCDEFGHIJKLMNOPQRSTUVWXYZ																									
Plaintext Alphabet	H		MN		ADRTSUEI																Z					

Beispiel Frequenzanalyse

In einem Doch im Eoden, da deete ein Hooeit. Nicht in einem ceuchten, schmutzigen Doch, vo es nach Moder riecht und Vurmzikced uon den Vaenden heraehaengen, und auch nicht in einer trockenen, kahden Sandgruee ohne Tische und Stuehde, vo man sich zum Essen hinsetzen koennte: nein, das Doch var eine Hooeithoehde, und das heisst, es var sehr komcortaeed.



Ciphertext Alphabet

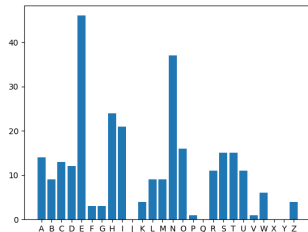
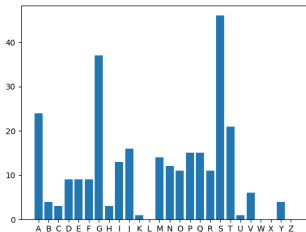
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Plaintext Alphabet

HK MNGCO ADRSTUEI Z

Beispiel Frequenzanalyse

In einem Loch im Boden, da lebte ein Hobbit. Nicht in einem feuchten, schmutzigen Loch, wo es nach Moder riecht und Wurmzipfel von den Waenden herabhaengen, und auch nicht in einer trockenen, kahlen Sandgrube ohne Tische und Stuehle, wo man sich zum Essen hinsetzen koennte: nein, das Loch war eine Hobbithoehle, und das heisst, es war sehr komfortabel.



Ciphertext Alphabet

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Plaintext Alphabet

HKFLBMNGCOP ADRSTUEIVW Z

Vigenère-Chiffre

- Poly-alphabetische Substitution
- Verwendet unterschiedliche Cäsar-Chiffren für aufeinanderfolgende Buchstaben
- Beispiel:

Schlüsselwort		B	A	Y	R	E	U	T	H
Cäsar mit Schlüssel		1	0	24	17	4	20	19	7

Verschlüsselung:

Klartext		ES	WAR	EINMAL	VOR	LANGER,	LANGER	ZEIT,	...
Schlüssel		BA	YRE	UTHBAY	REU	THBAYR,	EUTHBA	YREU,	...
Geheimtext		FS	URV	YBUNAJ	MSL	EHOGCI,	PUGNFR	XVMN,	...

→ Gleiche Buchstaben werden nicht immer gleich verschlüsselt

Tabula recta

	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

Vigenère Kryptoanalyse: Kasiski test

- Schwachstelle der Vigenère-Chiffre: wiederholender Schlüssel

Vigenère Kryptoanalyse: Kasiski test

- Schwachstelle der Vigenère-Chiffre: wiederholender Schlüssel
- Angenommen wir kennen die Schlüssellänge K :

Vigenère Kryptoanalyse: Kasiski test

- Schwachstelle der Vigenère-Chiffre: wiederholender Schlüssel
- Angenommen wir kennen die Schlüssellänge K :
 - Text in K Blöcke aufteilen (Beispiel: $K = 3$)
PPKAMJELQHPIAHLWYPKDDNBGPMJELQHPIAHZWUYJH...

Vigenère Kryptoanalyse: Kasiski test

- Schwachstelle der Vigenère-Chiffre: wiederholender Schlüssel
- Angenommen wir kennen die Schlüssellänge K :
 - Text in K Blöcke aufteilen (Beispiel: $K = 3$)

PPKAMJELQHPIAHLWYPKDDNBGPMJELQHPIAHZWUYJH...

Vigenère Kryptoanalyse: Kasiski test

- Schwachstelle der Vigenère-Chiffre: wiederholender Schlüssel
- Angenommen wir kennen die Schlüssellänge K :
 - Text in K Blöcke aufteilen (Beispiel: $K = 3$)
 PPKAMJELQHP~~IAHLWYPKDDNBGPMJELQHP~~IAHZWUYJH...
 - Auf jedem Block eigene Häufigkeitsanalyse:
 PAEHAWKNPEHAWJ | PMLPHYDBMLPHUH | KJQILPDGJQIZY

Vigenère Kryptoanalyse: Kasiski test

- Schwachstelle der Vigenère-Chiffre: wiederholender Schlüssel
- Angenommen wir kennen die Schlüssellänge K :
 - Text in K Blöcke aufteilen (Beispiel: $K = 3$)
PPKAMJELQHP₁IAHLWYPKDDNBGPMJELQHP₂IAHZWUYJH...
P₁AEHAWKNPEHAWJ | P₂MLPHYDBMLPHUH | K₃JQILPDGJQIZY
 - Auf jedem Block eigene Häufigkeitsanalyse:
- Problem: Wie findet man die Schlüssellänge?

Vigenère Kryptoanalyse: Kasiski test

- Schwachstelle der Vigenère-Chiffre: wiederholender Schlüssel
- Angenommen wir kennen die Schlüssellänge K :

- Text in K Blöcke aufteilen (Beispiel: $K = 3$)

PPKAMJELQHPIAHLWYPKDDNBGPMJELQHPIAHZWUYJH...

- Auf jedem Block eigene Häufigkeitsanalyse:

PAEHAWKNPEHAWJ | PMLPHYDBMLPHUH | KJQILPDGJQIZY

- Problem: Wie findet man die Schlüssellänge?

Kasiski Test:

PPKAMJELQHPIAHLWYPKDDNBGPMJELQHPIAHZWUYJH...

- Suche nach wiederholenden Buchstabengruppen (N -Gramme)

Vigenère Kryptoanalyse: Kasiski test

- Schwachstelle der Vigenère-Chiffre: wiederholender Schlüssel
- Angenommen wir kennen die Schlüssellänge K :

- Text in K Blöcke aufteilen (Beispiel: $K = 3$)

PPKAMJELQHPIAHLWYPKDDNBGPMJELQHPIAHZWUYJH...

- Auf jedem Block eigene Häufigkeitsanalyse:

PAEHAWKNPEHAWJ | PMLPHYDBMLPHUH | KJQILPDGJQIZY

- Problem: Wie findet man die Schlüssellänge?

Kasiski Test:

PPKAMJELQHPIAHLWYPKDDNBGPMJELQHPIAHZWUYJH...

- Suche nach wiederholenden Buchstabengruppen (N -Gramme)

Vigenère Kryptoanalyse: Kasiski test

- Schwachstelle der Vigenère-Chiffre: wiederholender Schlüssel
- Angenommen wir kennen die Schlüssellänge K :
 - Text in K Blöcke aufteilen (Beispiel: $K = 3$)
PPKAMJELQHPIAHLWYPKDDNBGPMJELQHPIAHZWUYJH...
 - Auf jedem Block eigene Häufigkeitsanalyse:
PAEHAWKNPEHAWJ | PMLPHYDBMLPHUH | KJQILPDGJQIZY
- Problem: Wie findet man die Schlüssellänge?

Kasiski Test:

PPKAMJELQHPIAHLWYPKDDNBGPMJELQHPIAHZWUYJH...

index = 4

index = 25

- Suche nach wiederholenden Buchstabengruppen (N -Gramme)
- Bestimme Abstand zwischen den Wiederholungen
(hier: $d = 25 - 4 = 21$)

Vigenère Kryptoanalyse: Kasiski test

- Schwachstelle der Vigenère-Chiffre: wiederholender Schlüssel
- Angenommen wir kennen die Schlüssellänge K :

- Text in K Blöcke aufteilen (Beispiel: $K = 3$)

PPKAMJELQHPIAHLWYPKDDNBGPMJELQHPIAHZWUYJH...

- Auf jedem Block eigene Häufigkeitsanalyse:

PAEHAWKNPEHAWJ | PMLPHYDBMLPHUH | KJQILPDGJQIZY

- Problem: Wie findet man die Schlüssellänge?

Kasiski Test:

PPKAMJELQHPIAHLWYPKDDNBGPMJELQHPIAHZWUYJH...

index = 4

index = 25

- Suche nach wiederholenden Buchstabengruppen (N -Gramme)
 - Bestimme Abstand zwischen den Wiederholungen
(hier: $d = 25 - 4 = 21$)
 - Schlüssellänge Teiler des Abstands: $d = 3 \cdot 7 \rightarrow K = 3$ oder 7

Vigenère Kryptoanalyse: Friedman Test

- Statistischer Test zur Bestimmung der Schlüssellänge:

κ_p	Wahrscheinlichkeit, dass zwei zufällig gewählte Buchstaben eines Textes gleich sind
κ_r	Wahrscheinlichkeit, dass zwei Buchstaben eines zufälligen gleichverteilten Textes übereinstimmen

- Im Englischen (monocase, 26 Buchstaben)):

$$\kappa_p = 0.067 \quad \kappa_r = \frac{1}{26} = 0.0385$$

- Abschätzung der Schlüssellänge:

$$K \approx \frac{\kappa_p - \kappa_r}{\kappa_o - \kappa_r}$$

mit der beobachteten Koinzidenzrate

$$\kappa_o = \frac{\sum_{i=1}^{26} n_i(n_i - 1)}{N(N - 1)}$$

Friedman Test: Anwendung

YNCJHFUGVBAVFYXIZBSRJ CZGPBFCVTSUGGKWPWUHZCRFHYKFSOJCPGMMRBVUJFBWMWRJWEJIZGGLZGLHTUOFWQFCCXIUCOGTESSLKRFSLNTCME
IKCOAJISAMGVBLBSKVWNSUSJZWFKLAYYSFMTFYLAJFHZXWRGBNXXOKYFZFSGIYONBSXDWKMRDKMMVPWMYVFUEFZATXHRIKXNKKSLLOKLRBVP
FEHWWBVOJMMFIYAFJTGKYYOLMMVDSLXZBYMMVFWSGISCLAYYOLFTIBAGLVEMTQCMDTDZBDXFMSKGTJHWIMRRLKTURWGGCOUDTYWCXUKHZKZFK
MKFFSGTKVWKIRMQXYBBGPNEUZHBNQJEJRRKHSKCOTDZRGNGKSVBKZGZHZCRWOJIQGFJSOUDNJVSEQSSLXQCWFZYIWKPNKVS LN XVKHRVKZXWVOY
XXRBVTLVGZXSTSLPTICSWXUWNXWSVBSRKGHIREVBVNKCGDYYSGGJCSKLYIONXQVRTRFERLAFKVS LRRRWTQCHZXIZTXXWVBUX

- Rateversuch: Schlüssellänge $K = 4$

Friedman Test: Anwendung

YNCJHFUGVB AVFYXIZBSRJ CZGPBFCVTSUGGKWP WUHZCRFHYKF SOJCPGMMRBVUJFBWMWRJWEJIZGGLZGLHTUOFWQFCCXIUCOGTESSLKRFSLNTCME
IKCOAJISAMGVBLBSKVWNSUSJZWFKLAYYSFMTFYLAJFHZXWRGBNXXKOKYFZFSGIYONBSXDWKMRDKMMVPWMYVFUEFZATXHRIKXNKKSLLOKLD RBVP
FEHWWBVOJMMFIYAFJTGKYYOLMMVDSLXZBYMMVFWSGISCLAYYOLF TIBAGLVEMTQCMDTDZBDXFMSKGTJHWIMRRLKTURWGGCOUDTYWCXUKHZXKZFK
MKFFSGTKVWKIRMQXYBBGPNEUZHBNQJEJRRKHSKCOTDZRGNGKSVBKZGZHZCRWOJIQGFJSOUDNJVSEQSSXLQCWFZYYWKP NKVSLNXVKHRVKZXWVOY
XXRBVTLVGZXSTSLPTICSWUWNXWXS VBSRKGHIREVB NKC GDYYSGGJCSKLYIONXQV RTRFERLAFKVS LRRRWTQCHZXIZTXXWVBUX

- Rateversuch: Schlüssellänge $K = 4$
- Teile Text in 4 Blöcke auf

Friedman Test: Anwendung

YNCJHFUGVBVAVFYXIZBSRJ CZGPBFCVTSUGGKWPWUHZCRFHYKFSOJCPGMMRBVUJFBWMWRJWEJIZGGLZGLHTUOFWQFCXXIUOCGTESSLKRFSLNTCME
IKCOAJISAMGVBLSKVWNSUSJZWFKLAYSFMTFYLAJFHZXWRGBNKKOYFZFSGIYONBSXDWKMRDKMMVPWMYVFUEFZATXHRIKXNKKSLLOKLRBVP
FEHWWBVOJMMFIYAFJTGKYYOLMMVDSLXZBYMMVFWSGISCLAYYOLF TIBAGLVEMTQCMDTDZBDXFMSKGTJHWIMRRLKTURWGGCOUDTYWCXUKHZZKZFK
MKFFSGTKVWKIRMQXYBBGPNEUZHBNQJEJRRKHSKOTDZRGNGKSVBKZGZHCWOWJIQGFJSOUDNJVSEQSSSLXQCWFZYYWKPKNVSLNXVKHRVKZXWVOY
XXRBVTLVGZXSTSLPTICSWXUWNXWXSVBRSKGHIRVBVNKCGDYSGGJCSKLYIONXQVTRFRERLAFKVS LRRRWTCQCHZIZTXWVBUX

YHVFZJPVGPZHSRJMZZ
TWCCEKLMCIGBWSFYMLHR
XYSOXMMWFZHXSORFWJIJ
YMSBVGLOILDTBMTILRCT
XZFFTKQBEBEKCZGBZRIJ
DSSCYPSPVWVXGTTWNSRI
BGSCYXTRKRTZTV

NFBYBCBTGWCYOGBFWEGG
UQXOSRNEOSVSNJKYTAZG
KFGNDRMMUARNLKBEBMYT
YMLYFIALBVQTD SJMKWOY
UXKFKIXGUNJHORKKHWS
NELWYNLKKVXTZSIXXVKR
NDGSIQRLVRQXXB

CUAXSZFSKURKJMVBRJGL
OFIGSF TIAABKSZLSFJXB
OZIBWDVYETIKLLVHVMAG
OVXMWSYFAECDXKHRTGUW
KKMSVRYPZORSTGSZZOGO
JQXFWKNNHZORLXLCUWGBG
KYGKOVFASRCIXU

JGVIRGCUWHFFCMUWJILH
FCUTLSCKJMLVUWAFYFVN
KFYSKKPVFXKKIDPWOFK
LDZMSCYTGMZFGWRUGDC
HZKGWMBNHQRKDNVGCJFU
VSQZKVRXRYBVSPSWXSHV
CYJLNREFLWHZWX

$$\kappa_o = 0.0425$$

$$\kappa_o = 0.0404$$

$$\kappa_o = 0.0405$$

$$\kappa_o = 0.0432$$

- Rateversuch: Schlüssellänge $K = 4$
- Teile Text in 4 Blöcke auf
- Bestimme Koinzidenzindex für jeden Block

Friedman Test: Anwendung

YNCJHFUGVBVAVFYXIZBSRJ CZGPBFCVTSUGGKWPWUHZCRFHYKF SOJCPGMMRBVUJFBWMWRJWEJIZGGLZGLHTUOFWQFC CXIU COGTESSLRKFS LNTCME
IKCOAJISAMGVBLSKVWNSUSJZWFKLAYYSFMTFYLAJFHZZWRGBNXXKOKYFZFSGIYONBSXDWKMRDKMVPWMYVFUEFZATXHR IKXNKKSL LIOKLDRBVP
FEHWWBVOJMMFIYAFJTGKYYOLMMVDSLXZBYMMVFWSGISCLAYYOLF TIBAGLVEMTQCMDTDZBDXFMSKGTJHWIMRRLKTURWGGCOUDTYWCXUKHZZKZFK
MKFFSGTKVWKIRMQXYBBGPNEUZHBNQJEJRKH SKCOTDZRGNGKSVBKZGZHZCRWOJIQGFJSOUDNJVSEQSS LXQCWFZYYWKPKNVSLNXVKHRVKZXWVOY
XXRBVTLVGZXSTSLPTICSWXUWNXWXS VBSRKGHIRBVBKCGDYSGGJCSKLYIONXQVTRFRERLAFKVS LRRRWTTQCHZIXTZXXWVBUX

YHVFZJPVGPZHSRJM WZZ
TWCC EKL MCIGBWSFYMLHR
XYSOXMMWFZHXSORFWJIJ
YMSBVGLOILDTBMTILRCT
XZFFTKQBEBEK CZGBZRIJ
DSSCYP SVVXVGTWNSRI
BGSCYXTRKRTZTV

NFBYBCBTGW CYOGBFWEWG
UQXOSRNEOSVSNJKYTAZG
KFGNDRMMUARNLKBEBMYT
YMLYFIALBVQ TDSJMKWOY
UXKFKIXGUNJHORKKHQWS
NELWYNLKKVXTZSIXXVKR
NDGSIQRLVRQXXB

CUAXSZFSKURKJMVBRJGL
OFIGSFTIAABKSZLSFJXB
OZIBWDVYETIKLLVHVMAG
OVXMWSYFAECDXKHRTGUW
KKMSVRYPZORSTGSZZOGO
JQXFWKNHZORLXLCUWGBG
KYGKOVFASRCIXU

JGVIRGCUWHFFCMUWJILH
FCUTLSCKJMLVUWAFYFVN
KFYSKKPVFXKKIDPWOFFK
LDZMSCYTGMMZFGWRUGDC
HZKGWMBNHQRKDNVGCJFU
VSQZKVXRXBYVSPSWXSHV
CYJLNREFLWHZWX

$$\kappa_o = 0.0425$$

$$\kappa_o = 0.0404$$

$$\kappa_o = 0.0405$$

$$\kappa_o = 0.0432$$

- Rateversuch: Schlüssellänge $K = 4$
 - Teile Text in 4 Blöcke auf
 - Bestimme Koinzidenzindex für jeden Block
- Erinnerung:

$$\kappa_p = 0.067 \text{ (englisch)}, \quad \kappa_r = 0.0385 \text{ (zufällig)}$$

Friedman Test: Anwendung

YNCJHFUGVBVFXIZBSRJZGPFVCVTUGGKWPWUHZCRFHYKFSOJCPGMMRBVUJFBWMWRJWEJIZGGLZGLHTUOFWQFCCXIUCOGTESSLKRFSLNTCME
 IKCOAJISAMGVBLBSKVWNSUSJZWFKLAYYSFMTFYLAJFHZZXWRGBNXKOKYFZFSGIYONBSXDWMKRDKMMVPWMYVFUEFZATXHRKXNKKSLLOKLRBVP
 FEHWBVOJMMFIYAFJTGKYYOLMMVDSLXZBYMMVFWSGISCLAYYOLFRTIBAGLVEMTQCMDTDZBDXFMSKGTJHWIMRRLKTURWGGCOUDTYWCXUKHZXKZFK
 MKFFSGTKVWKIRMQXYBBGPNEUZHBNQOEJRRKHSKCOTDZRGNGKSVBKZGZHZCRWOJIQGFJSOUDNJVSEQSSLXQCWFZYYWKPKNVSLNXVKHRVKZXWVOY
 XXRBVTLVGZXSTSLPTICSWXUWNXWXSVBRSKGHIRBVBKCGDYSGGJCSKLYIONXQVTRFRERLAFKVSLLRRRWTQCHZIXIZTXWVBUX

YFAIJBWSZYJMJWJ
 LTQITKNIJGSSWYT
 JWXFISMMYFHNLD
 BMFYMXMGAFGTTXG
 IKGDXXMGKXPHEHT
 NBHOFDEXZPLHXXT
 XPWXBHBDGLXRALT
 XXX

NUVZCFUPCKCRFRI
 ZUFUERTKIVKUFYF
 FRKZYXRVVZRKIRE
 VFJYVZVIYTLQDFT
 MTGTUKKTIYNBJSD
 GKZJJNQYNNRWXL
 STXWSINYJYQFFRQ
 IW

CGFBZCGWRFPBBJZ
 GOCCSFCCSBVSKSY
 HGOFODDPFAIKOBH
 OITODBFSYIVCZMJ
 RUCYKZFKRBENRKG
 KZCISJSCYKXVVRV
 TIUXRRKYCIVEKRC
 ZV

JVYSGVGUFSGVWVG
 LFCOSSMOALWJLFL
 ZBKSNWKWUTKSKVW
 JYGLSYWCOBEMBSH
 RROWHFFVMBUORCR
 SGRQOVSWVVKOBG
 SCWSKBCSSORRVRH
 TB

HBXRPKTHHOMUMEG
 HWXGLEAMBNZAMA
 XNYGBKMMEXLLPW
 MAKMLSLAMDDKW
 LWUCZKSWQZQKOG
 VZWGUSLFKSKZYVZ
 LSNVGVGGKNTLSWZ
 XU

$$\kappa_o = 0.0523$$

$$\kappa_o = 0.0496$$

$$\kappa_o = 0.0517$$

$$\kappa_o = 0.0601$$

$$\kappa_o = 0.0511$$

- Rateversuch: Schlüssellänge $K = 5$
 - Teile Text in 5 Blöcke auf
 - Bestimme Koinzidenzindex für jeden Block
- Erinnerung:

$$\kappa_p = 0.067 \text{ (englisch)}, \quad \kappa_r = 0.0385 \text{ (zufällig)}$$

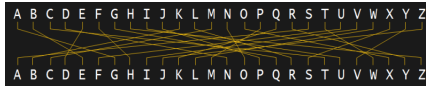
Enigma

- Von den Deutschen im 2. Weltkrieg zur Verschlüsselung verwendet
- Von den Alliierten gebrochen (ohne Wissen der Deutschen)



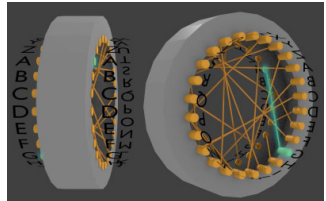
Enigma Funktionsweise

- Grundlage: Substitutionschiffre



- Rotoren ändern die Substitution nach jedem Buchstaben

initial position	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
	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
	G	E	T	N	D	H	Q	Z	U	P	B	R	C	O	X	M	K	Y	A	F	I	L	S	V	J	
first turn	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
	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
	J	G	E	T	N	D	H	Q	Z	U	P	B	R	C	O	X	M	K	Y	A	F	I	L	S	V	
second turn	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
	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
	V	J	G	E	T	N	D	H	Q	Z	U	P	B	R	C	O	X	M	K	Y	A	F	I	L	S	
third turn	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
	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
	S	V	J	G	E	T	N	D	H	Q	Z	U	P	B	R	C	O	X	M	K	Y	A	F	I	L	



- Anfangsposition der Rotoren entspricht dem Schlüssel



Enigma Funktionsweise

- Aus den Anfangspositionen der Rotoren erhält man

$$26 \cdot 26 \cdot 26 = 17\,576$$

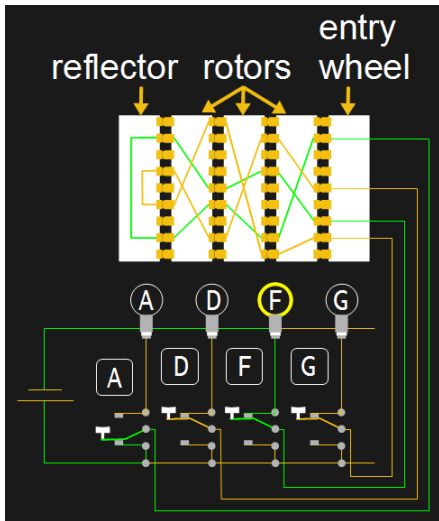
mögliche Verschlüsselungen für einen Buchstaben

- Es gibt mehrere mögliche Rotoren (numeriert mit I bis VII) von denen 3 Stück (in beliebiger Reihenfolge) ausgewählt werden

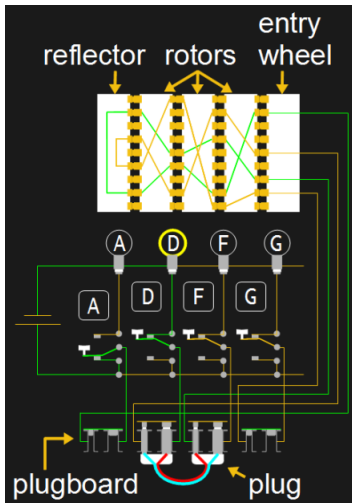
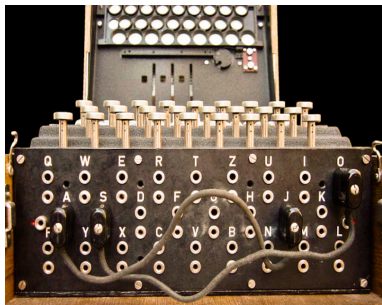
$$\rightarrow 8 \cdot 7 \cdot 6 = 336 \text{ Möglichkeiten}$$

Insgesamt: $17\,576 \cdot 336 = 5\,905\,376$ Möglichkeiten

Enigma: Innerer Aufbau



Enigma: Steckerbrett



→ bis zu 158 962 555 217 826 360 000 Möglichkeiten

- Verwende Python3 Implementation `pyenigma`
- Crib attack (Teil des Klartexts ist bekannt)
- Brute force ohne Steckerbrett

Die folgende Nachricht wurde abgefangen. Wir wissen, dass irgendwo in der Nachricht der Wetterbericht steht. Heute hat es geregnet.

Der Rest der Nachricht enthält den letzten Voucher.

OXSTMZLWDZYSCHIZOUFKTLRYHWNDPBNOQLBVWLQMUT
WPYBHFICHBCFABQBPUZKHSWGAJAPJRETCRABZLFJT

More topics

- Book cipher
- known plaintext attack
- key reuse attack (for one-time-pad)

<https://www.cryptool.org/en/cto-ciphers/caesar>