Aufgabe: Bringt es einen grundsätzlichen Vorteil, wenn man einen Klartext zunächst affin verschlüsselt: $c = (k_1 \cdot a + k_2) \bmod 26$ und ihn danach ein zweites Mal affin verschlüsselt: $c' = (k_1' \cdot c + k_2') \bmod 26$?

Antwort: Nein, dies ist insgesamt immer noch eine einzelne affine Verschlüsselung, denn

$$c' = (k_1' \cdot (k_1 \cdot a + k_2) + k_2') \bmod 26$$

$$= (\underbrace{k_1' \cdot k_1}_{k_1''} \cdot a + \underbrace{k_1' \cdot k_2 + k_2'}_{k_2''}) \bmod 26$$

Aufgabe: In der letzten Vorlesung wurde die Vigenère-Chiffre erklärt.

Sei $a_0 a_1 a_2 \dots a_{n-1}$ der Klartext der Länge n.

Sei $k_0 k_1 k_2 \dots k_{m-1}$ der Schlüssel der Länge m.
(Im Allgemeinen: $m < n$)

Sei $c_0 c_1 c_2 \dots c_{n-1}$ die zugehörige Chiffre.

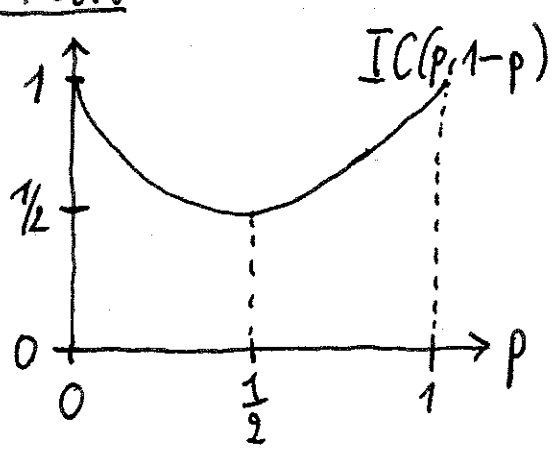
Gib eine mathematische Formel an,

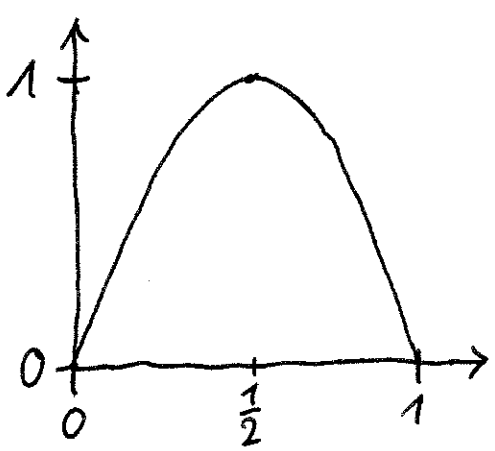
wobei $(A, B, \dots, Z) \triangleq (0, 1, \dots, 25)$

Lösung: $c_i = (a_i + k_{i \bmod m}) \bmod 26$, $i = 0, 1, \dots, n-1$.

Aufgabe: Der Koinzidenzindex für $n=2$ ist $p^2 + (1-p)^2 = IC(p, 1-p)$. Die Verteilung ist $(p, 1-p)$. Skizziere den Verlauf von $IC(p, 1-p)$ und von der Renyi-Entropie $-\log_2 IC(p, 1-p)$

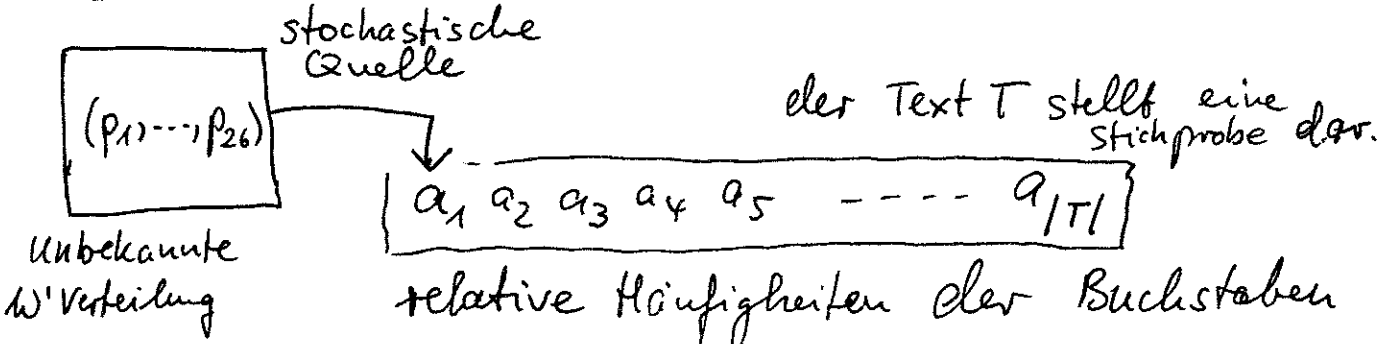
Antwort:





bzw. Schätzen,
Ermitteln des Koinzidenzindex eines Textes T

Modell:



relative Häufigkeiten der Buchstaben im Text ermitteln. Hieraus einen Schätzwert für $IC(p_1, \ldots, p_{26})$ ermitteln.

Erwartungstreue Schätzung:

$$\widehat{IC} = \sum_{a \in \Sigma} \frac{h(a)}{n} \cdot \frac{h(a)-1}{n-1}$$

wobei $n = |T|$, $h(a)$... Häufigkeit des Buchstabens a im Text T.

Σ zugrunde liegendes Alphabet, z.B.

$\Sigma = \{A, B, \ldots, Z\}$

Interpretation: Zunächst einen Buchstaben im gesamten Text unter Gleichverteilung auswählen: $\frac{h(a)}{n}$ ist die W'keit für Buchstaben a. Dann unter den verbleibenden Buchstaben einen zufällig auswählen. Dann ist $\frac{h(a)-1}{n-1}$ die W'heit, wieder den Buchstaben a ~~zu~~ zu erhalten.

Aufgabe: Schätzen des IC-Werts von

MORGENFRUEHANGREIFEN

Textlänge $n = 20$

Buchstaben, die (≥ 2)-mal vorkommen:

R ... 3	ergibt Summand	$\frac{3}{20} \cdot \frac{2}{19}$	$= 1{,}58\,\%$
G ... 2		$\frac{2}{20} \cdot \frac{1}{19}$	$= 0{,}53\,\%$
E ... 4		$\frac{4}{20} \cdot \frac{3}{19}$	$= 3{,}16\,\%$
N ... 3		$\frac{3}{20} \cdot \frac{2}{19}$	$= 1{,}58\,\%$
F ... 2		$\frac{2}{20} \cdot \frac{1}{19}$	$= 0{,}53\,\%$

$\widetilde{IC} = 7{,}38\,\%$

ES GESCHEHEN NOCH ZEICHEN UND WUNDER

Textlänge $n = 31$

E ... 7	ergibt	$\frac{7}{31} \cdot \frac{6}{30}$	$= 4{,}52\,\%$
N ... 5		$\frac{5}{31} \cdot \frac{4}{30}$	$= 2{,}15\,\%$
H ... 4		$\frac{4}{31} \cdot \frac{3}{30}$	$= 1{,}29\,\%$
C ... 3		$\frac{3}{31} \cdot \frac{2}{30}$	$= 0{,}65\,\%$
U ... 2		$\frac{2}{31} \cdot \frac{1}{30}$	$= 0{,}22\,\%$
S ... 2		$\frac{2}{31} \cdot \frac{1}{30}$	$= 0{,}22\,\%$

$\widetilde{IC} = 9{,}05\,\%$

Zufallsfolge von Buchstaben, Gleichverteilung:

ZLXDH KYQRE AIJIT DQDXM IXMDT UEVRO H

(n=30)

e. gibt: $\widehat{IC} = 0,039 = 3,9\%$

(hierbei: 1 Buchstabe, der 4x vorkommt,
2 Buchstaben, die 3x vorkommen,
5 Buchstaben, die 2x vorkommen)

bei Vigenère-Verschlüsselung

Ermitteln der Schlüsselwortlänge nach der

Friedman-Methode:

Durchlaufe in einer Schleife alle potenziellen Schlüsselwortlängen $m = 1, 2, 3, 4, \ldots$

Gruppiere die Chiffre $c_0 c_1 c_2 c_3 \ldots$ in m Teilfolgen:

1. Teilfolge: $c_0 \; c_m \; c_{2m} \; c_{3m} \ldots \rightarrow \widetilde{IC}_1$
2. Teilfolge: $c_1 \; c_{m+1} \; c_{2m+1} \; c_{3m+1} \ldots \rightarrow \widetilde{IC}_2$
⋮
m. Teilfolge: $c_{m-1} \; c_{2m-1} \; c_{3m-1} \; c_{4m-1} \ldots \rightarrow \widetilde{IC}_m$

Ermittle für jede der Teilfolgen eine Koinzidenzindex-Schätzung.

Sofern m nicht die richtige Schlüsselwortlänge ist, so entsprechen die $\widetilde{IC}$-Werte eher derjenigen einer Gleichverteilung, also $\widetilde{IC} \approx 4\%$.

Beispiel:

M	O	R	G	E	N	F	R	U	E	H	A	N	G	R	E	I	F	E	N
D	E	A	T	H	D	E	A	T	H	D	E	A	T	H	D	E	A	T	H
P	S	R	Z	L	Q	J	R	N	L	K	E	N	Z	Y	H	M	F	X	U

Falsche Schlüssellängen-Vermutung $m = 4$

P L N N M → $\widetilde{IC} = \frac{2}{5} \cdot \frac{1}{4} = 0{,}1$

S Q L Z F → $\widetilde{IC} = 0$

R J K Y X → $\widetilde{IC} = 0$

Z R E H U → $\widetilde{IC} = 0$

Mittlerer $\widetilde{IC}$-Wert = $0{,}025 = 2{,}5\%$

Richtige Schlüssellänge $m = 5$:

P Q K H → $\widetilde{IC} = 0$

S J E M → $\widetilde{IC} = 0$

R R N F → $\widetilde{IC} = \frac{2}{4} \cdot \frac{1}{3} = 0{,}167$

Z N Z X → $\widetilde{IC} = 0{,}167$

L L Y U → $\widetilde{IC} = 0{,}167$

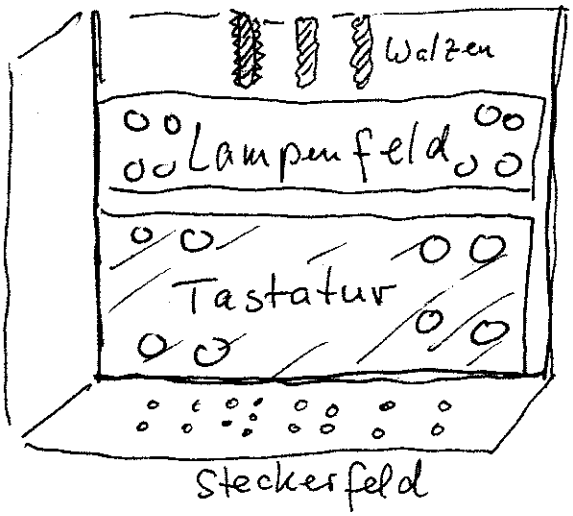
Mittlerer $\widetilde{IC}$-Wert = $0{,}1$ $= 10\%$

Angenommen, die richtige Schlüsselwortlänge wurde (mittels Kasiski oder Friedman) ermittelt.

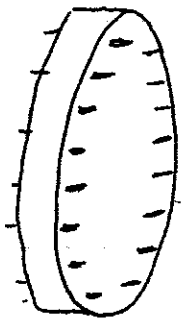
Nun muss für jede Teilfolge der richtige Shift gemäß Cäsar-Chiffrierung bestimmt werden. Hierzu alle 26-Cäsar-Schlüssel überprüfen, welcher eine größte Ähnlichkeit mit der deutschen Sprache hat.

Die Enigma-Verschlüsselungsmaschine

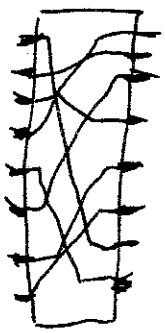
(Enigma: (griechisch) Rätsel, Geheimnis)



Jede Walze realisiert auf elektrischem Weg eine Permutation $\{A,\dots,Z\} \to \{A,\dots,Z\}$



← 26 Stifte, ebenso auf der Rückseite



interne Verdrahtung

Ein Bestandteil des Schlüssel besteht darin, 3 aus 5 vorhandenen Walzen auszuwählen und in einer bestimmten Reihfolge in das Gerät einzulegen, z.B. 524.

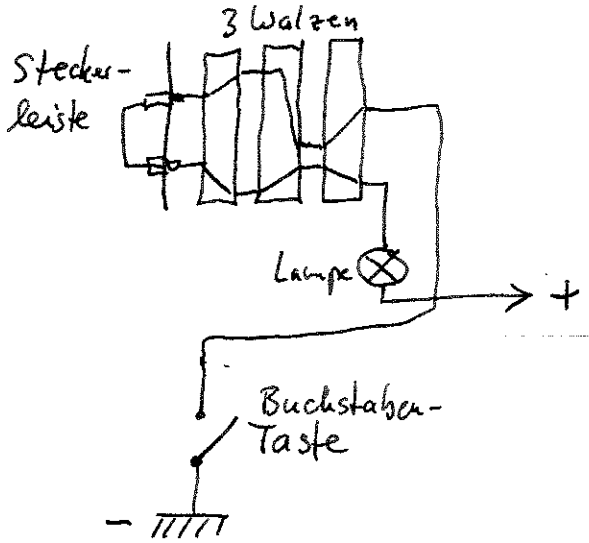
Dies ergibt $\binom{5}{3} \cdot 3! = 60$ Möglichkeiten

Die 3 Walzen werden in eine Anfangsposition gedreht, die ebenfalls Bestandteil des Schlüssels ist. Anzahl Möglichkeiten = $26^3 = 17\,576$

Insgesamt: $60 \cdot 17\,576 = 1\,054\,560$

Durch die Stecker kann eine weitere Permutation realisiert werden.

Elektrischer Stromverlauf:



Nach jedem Tastendruck

drehen sich die Walzen

weiter.

Enigma