Lösungen vom 30.4.2018

7.) für Vigenère-Chiffre:

beide Schlüssel gleichlang ⇒ entspricht einer einzelnen Vigenère-Verschlüsselung derselben Länge.
Schlüssel verschieden lang: Es tritt erst nach $kgV(l_1, l_2)$ vielen Buchstaben eine Wiederholung ein.

10.) for alle Schlüssel k do
Berechne $m = D(c, k)$
Bestimme relative Häufigkeiten h_i der Buchstaben in m. Vergleiche mit W'keiten p_i im Deutschen
Verwende eine der Formeln

$$\sum_{i=1}^{n} (p_i - h_i)^2 \quad , \quad \sum_{i=1}^{n} |p_i - h_i| \rightarrow \min$$

$$\sum_{i=1}^{n} p_i \cdot h_i \rightarrow \max$$

um wahrscheinlichsten deutschen Text zu bestimmen. Des Weiteren kann Analyse der Bigramm-Häufigkeiten helfen.

11.) PANAMAKANAL enthält 5×A und 2×N (nur Häufigkeiten ≥ 2 sind relevant); ergibt:

$$\tilde{IC} = \frac{5}{11} \cdot \frac{4}{10} + \frac{2}{11} \cdot \frac{1}{10} = \frac{22}{110} = \frac{1}{5} = 20\%$$

TEPRYMEXQFY enthält 2×E, 2×Y:

$$\tilde{IC} = \frac{2}{11} \cdot \frac{1}{10} + \frac{2}{11} \cdot \frac{1}{10} = \frac{4}{110} = \frac{2}{55} \approx 3{,}6\%$$

12.) Playfair:

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

MO|RG|EN|IN|AL|LE|RF|RU|EH|DI|EB|UR|GA|NG|RE|IF|EN
LA YF GL SG MO UL AM VK FI IS OG KV FB WN FK EG GL

Vigenère:

MORGENINALLERFRUEHDIEBURGANGREIFEN
+ KRYPTOKRYPTOKRYPTOKRYPTOKRYPTOKRYP
WFPVXBSEYAESBWPJXVNZCQMFQRLVKSSWCC

13.) XSD liegen im Abstand 15 voneinander
AWER liegen im Abstand 20 voneinander
⇒ Vermutete Schlüssellänge ist $ggT(15,20) = 5$

14.) 1. Experiment $E(X) = \sum_{i<j} \frac{1}{26} = \binom{n}{2} \cdot \frac{1}{26}$

2. Experiment $E(X) = \sum_{i<j} 0{,}07 = \binom{n}{2} \cdot 0{,}07$

Setze $E(X)=1$ im 1. Exp: $n \approx 7{,}7$

Setze $E(X)=1$ im 2. Exp: $n \approx 5.9$

15.) RUNDERHUNDINDEX
+ BADBADBADBADBADBAD
SUQEEUIUQEIQEE

$ggT(6,9)=3$

← 6 →
← 9 →

17.) Shannon-Entropie: $-0,2 \cdot \log_2 0,2 - 0,4 \cdot \log_2 0,4 - 0,1 \cdot \log_2 0,1$
$- 0,3 \cdot \log_2 0,3 = 1,85$

Koinz. index: $0,2^2 + 0,4^2 + 0,1^2 + 0,3^2 = 0,3$

Renyi-Entropie: $-\log_2(0,3) = 1,74$

19.) Koinz. index: $\left(\frac{1}{8}\right)^2 + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{4}\right)^2 + \left(\frac{1}{8}\right)^2 = \frac{11}{32} \approx 0,344$

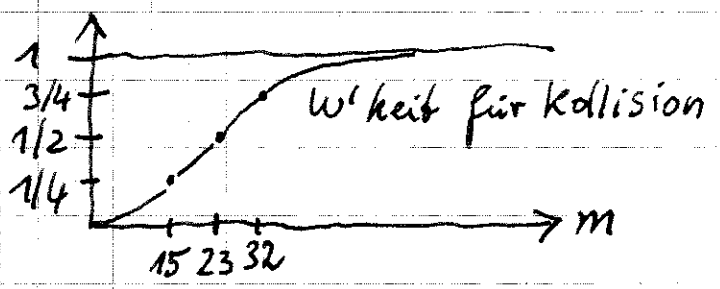
Shannon-Entropie: $-2 \cdot \frac{1}{8} \cdot \log_2\left(\frac{1}{8}\right) - \frac{1}{2} \log_2\left(\frac{1}{2}\right) - \frac{1}{4} \cdot \log_2\left(\frac{1}{4}\right)$
$= \frac{1}{4} \cdot 3 + \frac{1}{2} + \frac{1}{4} \cdot 2 = \frac{7}{4} = 1,75$

21.) $H(\text{Zwergen-Lotto}) = \log_2 \binom{7}{3} \approx 5,13$

23.) Um 1. bzw. 3. Quartil zu berechnen, die Approximationsformel $e^{-(m-0,5)^2/2n}$ auf 3/4 bzw. 1/4 setzen. Man erhält:

$m \approx 0,5 + 0,759 \cdot \sqrt{n}$ (1. Quartil), bei $n = 365$, $m = 15$

$m \approx 0,5 + 1,665 \cdot \sqrt{n}$ (3. Quartil), bei $n = 365$, $m \approx 32,3$



26.) $2^{80} \cdot 10^{-10}$ s = 3,8 Mio Jahre

27.) $-0,5 \cdot \log_2 0,5 - 0,48 \cdot \log_2 0,48 - 0,02 \cdot \log_2 0,02 \approx 1,12$ bit

Information bei Zwilling ist $-\log_2 0,02 \approx 5,6$ bit

28.) E E H E O Z C N D N R
S S E N C E H U W D
G C H N H I E N U E

$\widetilde{IC}$ von 1. Zeile: $\frac{3}{11}\cdot\frac{2}{10}+\frac{2}{11}\cdot\frac{1}{10}=\frac{8}{110}\approx 7{,}3\ \%$

$\widetilde{IC}$ von 2. Zeile: $\frac{2}{10}\cdot\frac{1}{9}+\frac{2}{10}\cdot\frac{1}{9}=\frac{4}{90}\approx 4{,}44\%$

$\widetilde{IC}$ von 3. Zeile: $3\cdot\frac{2}{10}\cdot\frac{1}{9}=\frac{6}{90}\approx 6{,}67\%$

29.) $$\sum_{i=1}^{n}\left(p_i-\frac{1}{n}\right)^2=\sum_{i=1}^{n}\left(p_i^2-\frac{2}{n}p_i+\frac{1}{n^2}\right)$$

$$=\underbrace{\sum_{i=1}^{n}p_i^2}_{=IC(P)}-\frac{2}{n}\underbrace{\sum_{i=1}^{n}p_i}_{=1}+\underbrace{\sum_{i=1}^{n}\frac{1}{n^2}}_{=1/n}=IC(P)-\frac{1}{n}$$

30.) Bei Verschiebung um 3 Buchstaben erhält man:

B L O F D W X W C R P U F L Y B E
− B L O F D W X W C R P U F L
? ? ? E S I S T G U T S O W E I T

Vermutet man ALL für die ersten 3 Buchstaben, so ergibt sich, dass das Schlüsselwort BAD war.

31.) $\widetilde{IC}\approx\frac{1}{m}\cdot 7{,}6\%+\frac{m-1}{m}\cdot 3{,}85\%$, m Schlüssellänge

Nach m auflösen:

$$m\approx\frac{3{,}75}{\widetilde{IC}-3{,}85}$$ ($\widetilde{IC}$ in Prozent einsetzen)