Lösungen, am 23.4.2018 behandelt

0.) ce soir sous P à cent sous six
soupé Sans-Souci

Großes G, kleines a = G grand, a petit
J'ai grand appetit

1.) ES GESCHEHEN NOCH ZEICHEN UND WUNDER

2.)

Mögliche Cäsar-Shifts:

N R J
O S K
P T L
Q U M
R V N
S W O
T X P
U Y Q
V Z R
W A S ← wahrscheinlichster Satzanfang
X B T
Y C U
Z D V
A E W
B F X
C G Y
D H Z
E I A ← auch denkbar: Eiapopeia...
F J B
G K C
H L D
I M E ← auch denkbar: Im Eimer ...
J N F
K O G ← auch denkbar: Kognitionswissenschaft...
L P H
M Q I

Sobald ein 4. Buchstabe hinzukommt, sollte es eindeutig werden.

3.) ANKOMME FREITAG DEN DREIZEH

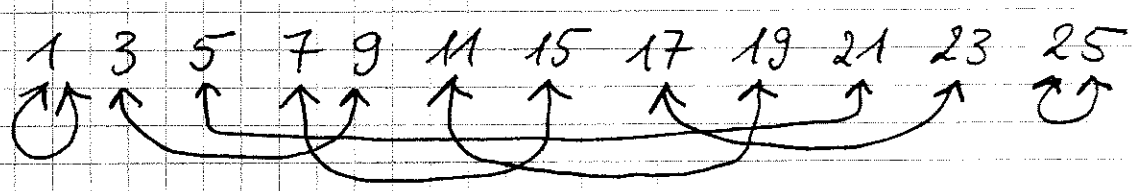
4.) Falls $\pi(x)=x$ unzulässig, so sei d_n die Anzahl der fixpunktfreien Permutationen in S_n.
Man kann eine Rekursionsformel für d_n aufstellen:

$$d_n = (n-1)\cdot(d_{n-1} + d_{n-2})$$

Asymptotisch ergibt sich, dass $d_n \approx \frac{1}{e}\cdot n!$

Falls zusätzlich aus $\pi(x)=y$ folgt $\pi(y)=x$, so gibt es $25\cdot 23\cdot 21\cdot 19\cdot 17\cdot 15\cdot 13\cdot 11\cdot 9\cdot 7\cdot 5\cdot 3$ Möglichkeiten.

5.) a muss teilerfremd zu 26 sein. Diese a's sind: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25
Daher gibt es $12\cdot 26 = 312$ zulässige Schlüssel.
Genau diese a's besitzen multiplikative Inverse:



Beispiel: $3\cdot 9 = 27 \equiv 1 \pmod{26}$

6.) $C \equiv 3x + 5$

$C - 5 \equiv 3x$

$9 \cdot (C-5) \equiv x$

$x \equiv 9 \cdot C - 45 \equiv 9 \cdot C + 7$

} alles (mod 26)

7.) $C_2 = a_2 \cdot C_1 + b_2 = a_2 \cdot (a_1 \cdot x + b_1) + b_2 = (a_1 a_2)x + (a_2 b_1 + b_2)$

Dies ist ebenfalls eine affine Chiffre!

8.) 2 Gleichungen (modulo 26):

(1) $a \cdot 8 + b = 15$

(2) $a \cdot 5 + b = 16$

(1)-(2): $3a = -1$

$a = (-1) \cdot 9 = -9 = 17$

$\Rightarrow b = 16 - 5 \cdot 17 = 16 - 17 = -3 = 23$

9.) $\binom{5}{3} \cdot 3! \cdot 26^3 = 5 \cdot 4 \cdot 3 \cdot 26^3 = 1054560$

16.)

A	B	C	D
3	1	2	4
5	6		7
	8		9
	0		

} die Zahlen 0,...,9 zufällig verteilt.

18.) Setze $2^{n/7} \stackrel{!}{=} 2^{80}$, $\frac{n}{7} = 80$, $n = 560$

Mindestschlüssellänge ≥ 560

20.) Modulo 30: $\varphi(30) \cdot 30 = \varphi(2) \cdot \varphi(3) \cdot \varphi(5) \cdot 30$

$= 1 \cdot 2 \cdot 4 \cdot 30 = 240$ Schlüssel

Modulo 29: $\varphi(29) \cdot 29 = 28 \cdot 29 = 812$ Schlüssel

22.) Anzahl Schlüssel $= 26 \cdot 25 \cdot 24 \cdot 23 \cdot 22 = 7893600 \hat{=} 23$ Bit

Schlüssel in Deutsch $= 5 \cdot 2$ Bit $= 10$ Bit