Určení délky klíče šifrovaného textu

Index koincidence

- Pravděpodobnost, že se u dvou textů v daném jazyce vyskytnou stejná písmena na stejném místě v textu.
- Zkratka: IK

Index koincidence

- Vzorec:

$$IK = \frac{\sum_{i="A"}^{"Z"} f_i(f_i - 1)}{N(N-1)}$$

- f_i - počet znaku i v textu
- IK – index koincidence
- N – celkový počet znaků v textu

zdroj: materiály k cvičení Mgr. Radim Janča

Index koincidence

- Tabulka pro vybrané jazyky

čeština	0.06027
angličtina	0.06689
dánština	0.07073
finština	0.07380
francouzština	0.07460
holandština	0.07981
němčina	0.07667

Index koincidence

- 1. text je zašifrován jednoduchou záměnou písmen

  - výpočet indexu koincidence
  - určení jazyka zašifrovaného textu

Index koincidence

- 2. test zašifrován periodickým klíčem
  - rozdělení ŠT do bloků
  - výpočet IK pro jednotlivé bloky
  - průměr IK pro každou možnost rozdělení
  - určení délky klíče a jazyka textu

Příklad

Určete délku klíče českého textu:

EFCWV SFXWQ JBTWB SDINZ AVDWW APWAA CZMKF SEPWX SRLGC
JTWDC PKEEO FSPSB ZVSWZ CSCTM KRLGM CDMEY AVHGK QPVFC WFSJY
NEERC CPMAD SYOQK XLDQW CKRSX TDECU SAVAJ CRVWB INISN GJTQX
OYSZM JEAUR OKIDW HBUDS BJENW HKUHU MUECC QPZSN BJLGZ XKNAU
RJRWQ ERTJS ZLRWN DLZAV OWINW ERDSV CESBY ZFKVI NDIHP DJTWZ
ZTDAB DCUHY DCMKY KEYUR DZPKR PICAM VUECM CVJSU MGIDG ZPZSV
IORQF BPZSZ CDXMN DMADY HZLDY KFUVY ZFNSI DBDQJ GTXGF AVDSM
SDXMA XTHWW HFELY BKOZV OGYHM BRLMJ JPHDM IRKRO XTDNP PKIDY
NNIDY SFZSN IYEVJ DLHWW VFFWL TDKJU ILLGZ XKINS RPPAX PSLWC
YOZGS QCEVI QSWNC IPLWU CNMCR TIEGU OXDAI BYOMB OWCFY BVSAM
OAECQ TIYUR ZPTJG ZIYDI JTGCW

Zdroj: www.karlin.mff.cuni.cz/~tuma/nciphers/nciphers3.**pdf**

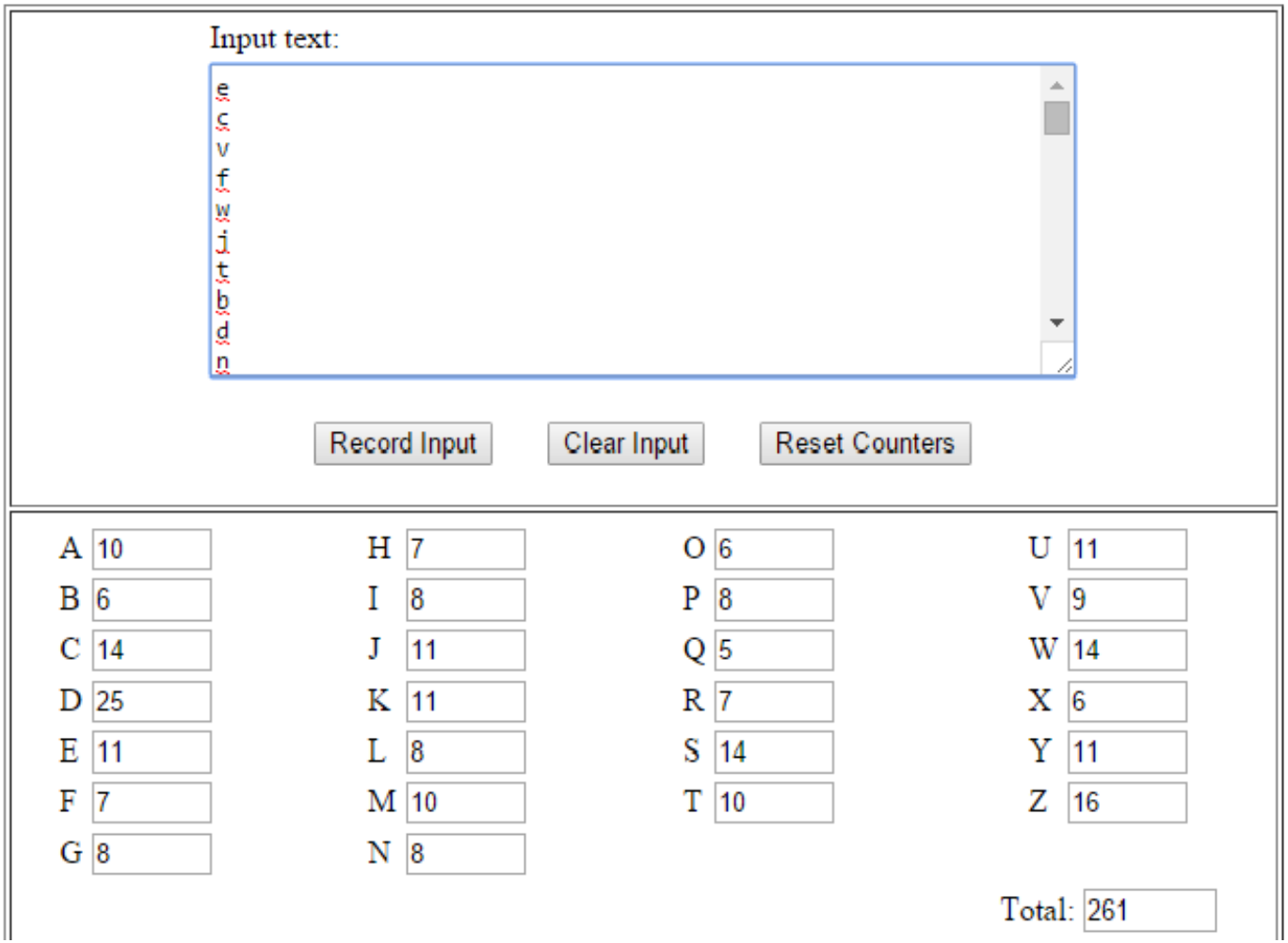
- Pomocí výpočtů testujeme možné délky klíče od 1 (zašifrování jednoduchou záměnou písmen) dokud nenajdeme použitou délku klíče

Délka klíče 1

H3 =SUMA(D3:D28)/(B30*(B30-1))

	A	B	C	D	E	F	G	H	I	J
1	původní									
2	znak	výskyt		mezivýpočet				index koincidence		
3	a	20		380		(B3*(B3-1))		0,039877		
4	b	16		240						
5	c	30		870						
6	d	34		1122						
7	e	21		420						
8	f	16		240						
9	g	15		210						
10	h	12		132						
11	i	24		552						
12	j	19		342						
13	k	19		342						
14	l	15		210						
15	m	21		420						
16	n	19		342						
17	o	14		182						
18	p	20		380						
19	q	12		132						
20	r	20		380						
21	s	32		992						
22	t	16		240						
23	u	16		240						
24	v	20		380						
25	w	29		812						
26	x	14		182						
27	y	21		420						
28	z	25		600						
29										
30	počet znak	520								
31										

Frequency Counter



Zdroj:https://www.mtholyoke.edu/courses/quenell/s2003/ma139/js/count.html

Délka klíče 2 – liché znaky

F3 =SUMA(D3:D28)/(B30*(B30-1))

	A	B	C	D	E	F	G	H	I
1	pro dvě - první								
2	znak	výskyt		mezivýpočet		index koincidence			
3	a	10		90		0,041173			
4	b	6		30					
5	c	14		182					
6	d	25		600					
7	e	11		110					
8	f	7		42					
9	g	8		56					
10	h	7		42					
11	i	8		56					
12	j	11		110					
13	k	11		110					
14	l	8		56					
15	m	10		90					
16	n	8		56					
17	o	6		30					
18	p	8		56					
19	q	5		20					
20	r	7		42					
21	s	14		182					
22	t	10		90					
23	u	11		110					
24	v	9		72					
25	w	14		182					
26	x	6		30					
27	y	11		110					
28	z	16		240					
29									
30	počet znaků	261							
31									

Délka klíče 2 – sudé znaky

F3 | =SUMA(D3:D28)/(B30*(B30-1))

Pole názvů

	A	B	C	D	E	F	G	H	I	J
1	pro dvě – druhá									
2	znak	výskyt		mezivýpočet		index koincidence				
3	a	10		90		0,039115				
4	b	10		90						
5	c	16		240						
6	d	9		72						
7	e	10		90						
8	f	9		72						
9	g	7		42						
10	h	5		20						
11	i	16		240						
12	j	8		56						
13	k	8		56						
14	l	7		42						
15	m	11		110						
16	n	11		110						
17	o	8		56						
18	p	13		156						
19	q	7		42						
20	r	13		156						
21	s	18		306						
22	t	6		30						
23	u	5		20						
24	v	11		110						
25	w	15		210						
26	x	8		56						
27	y	10		90						
28	z	9		72						
29										
30	počet znak	260								
31										

Souhrn pro délku klíče 1 až 5

H7 =SUMA(B7:F7)/5

	A	B	C	D	E	F	G	H	I	J	K
1	delka klice										
2		první	druha	treti	ctvrta	pata		průměr			
3	jedna	0,03988						0,03988		cílová hodnota = 0,06	
4	dve	0,04117	0,03911					0,04014			
5	tri	0,04345	0,04033	0,0371				0,04029			
6	ctyri	0,04122	0,03948	0,04329	0,04342			0,04185			
7	pet	0,1125	0,04593	0,0463	0,06572	0,05022		0,06414			
8											

Děkuji za pozornost ☺