KRIPTOGRAFIJA
Zadaća 3.131

Filip Nikšić

22. travnja 2007.

1. Dešifrirajte šifrat:

```
SOAAO TOADE PSMED OAOIS VKNIR DKIST REJON OSAAD
GCUSA EPMGL DBRDD NMCVA NAOND NEIOA ACEEI AVERI
JIVEI JSAOJ TUIOA IAIOG AOEIE LIJKA IIDJS TVSJZ
TNOJV BNMIJ EOENL AEKLT AILAU AJIOE RITME TIMEJ
C
```

ako je poznato da je dobiven stupčanom transpozicijom iz otvorenog teksta na hrvatskom jeziku, te da je broj stupaca između 4 i 16.

Rj. Uočimo prvo da šifrat ima 161 znak. Kako je $161 = 7 \cdot 23$, zaključujemo da je broj stupaca 7. (Dakle, nema potrebe za analiziranjem odnosa suglasnika i samoglasnika.)

Ispišimo tekst u 7 stupaca i za svaki (uređeni) par stupaca pogledajmo koliko se od 23 bigrama koji nastanu njihovim spajanjem nalazi među 36 najfrekventnijih bigrama hrvatskog jezika. Podatci su dani u tablici:

	1	2	3	4	5	6	7
1		6	3	3	4	5	2
2	11		3	3	3	1	5
3	3	3		6	11	1	4
4	7	3	6		1	5	7
5	4	6	6	2		12	2
6	4	6	3	10	8		3
7	1	11	1	4	6	6	

1	2	3	4	5	6	7
S	I	P	A	I	T	L
O	R	M	A	O	V	T
A	D	G	C	A	S	A
A	K	L	E	I	J	I
O	I	D	E	A	Z	L
T	S	B	I	I	T	A
O	T	R	A	O	N	U
A	R	D	V	G	O	A
D	E	D	E	A	J	J
E	J	N	R	O	V	I
P	O	M	I	E	B	O
S	N	C	J	I	N	E
M	O	V	I	E	M	R
E	S	A	V	L	I	I
D	A	N	E	I	J	T
O	A	A	I	J	E	M
A	D	O	J	K	O	E
O	G	N	S	A	E	T
I	C	D	A	I	N	I
S	U	N	O	I	L	M
V	S	E	J	D	A	E
K	A	I	T	J	E	J
N	E	O	U	S	K	C

U tablici uočavamo brojeve 10, 11, 12. Pretpostavljamo da zajedno stoje stupci 2 1, 7 2, 6 4, 3 5 i 5 6. To nam već daje dva dijela ključa: 721 i 3564. Ostaje upitno jesu li zajedno 1 3, ili možda 4 7. To sad već lako možemo uočiti u stupcima desno, a možemo se voditi i time što u tablici na mjestu (4,7) stoji 7, a na mjestu (1,3) stoji 3.

Dakle, traženi ključ je 3564721, a otvoreni tekst glasi:

```
pitalismovatrogascadalijeikadazeliobitiastronautodgova
radajejednovrijemebioopcinjensvemiromalivisenijetadaje
imaookojedanaestgodinaicinilomusedajesvijetjakoskucen
```

Pitali smo vatrogasca da li je ikada želio biti astronaut. Odgovara da je jedno vrijeme bio opčinjen Svemirom, ali više nije. Tada je imao oko jedanaest godina i činilo mu se da je svijet jako skučen.

2. Dešifrirajte sljedeća dva šifrata:

```
DAXFK EOV
NCFHG MNR
```

ako je poznato da su dobiveni istim ključem po pravilu

$$y_i \equiv x_i + k_i \pmod{26}.$$

Oba teksta počinju jednim od slova `d`, `i`, `n`, `o`, `p`, `s`.

Rj. Označimo li šifrate s y i y', otvorene tekstove s x i x', a ključ s k, onda iz

$$y_i = x_i + k_i$$
$$y'_i = x'_i + k_i$$

zaključujemo da vrijedi

$$y'_i - y_i = x'_i - x_i.$$

Budući da je $y'_1 - y_1 = \texttt{N} - \texttt{D} = 10$, zaključujemo da postoje dvije mogućnosti za x_1 i x'_1: `d`, `n`, i `i`, `s`.

Ukoliko se odlučimo za `d` i `n`, sve mogućnosti za x_2 su `a`, `e`, `i`, `j`, `l`, `n`, `o`, `r`, `u`, `v`, `z`. Kako je $y'_2 - y_2 = \texttt{C} - \texttt{A} = 2$, odgovarajuće mogućnosti za x'_2 su: `c`, `g`, `k`, `l`, `n`, `p`, `q`, `t`, `w`, `x`, `b`. Dakle, ovu opciju možemo odbaciti.

Imamo, dakle, $(x_1, x'_1, k_1) = (\texttt{i}, \texttt{s}, \texttt{v})$. Najzgodnije je sada gledati koje bi moglo biti drugo slovo ključa. Kandidati su: `a`, `e`, `i`, `j`, `l`, `o`, `r`, `u`. Odgovarajući kandidati za x_1 su `a`, `w`, `s`, `r`, `p`, `m`, `j`, `g`. U rječniku pronalazimo daleko najviše riječi za $(x_2, x'_2, k_2) = (\texttt{s}, \texttt{u}, \texttt{i})$ pa nastavljamo u tom smjeru.

Kandidati za x_3 su `c`, `e`, `h`, `i`, `j`, `k`, `l`, `m`, `p`, `t`, `u`. Odgovarajući kandidati za x'_3 su `k`, `m`, `p`, `q`, `r`, `s`, `t`, `u`, `x`, `b`, `c`, a odgovarajući kandidati za k_3 su `v`, `t`, `q`, `p`, `o`, `n`, `m`, `l`, `i`, `e`, `d`. Tu opet većinu kombinacija možemo eliminirati, a najizglednija opcija je $(x_3, x'_3, k_3) = (\texttt{k}, \texttt{s}, \texttt{n})$.

Pogledajmo što dosad imamo za početak od x, x', k: `isk`, `sus`, `vin`. Rječnik sad kaže da bi ključ mogao počinjati s `vina` ili `vino`. Brzo otkrivamo da nam opcija `vino` za početke od x i x' daje `iskr`, `sust`.

Sad već postaje sasvim trivijalno. Vidimo da x vuće na `iskre`, što povlači da x' počinje sa `susta`, a k s `vinog`. Dalje možemo i pogoditi: x je `iskrenos`, x' je `sustavno`, a k je `vinograd`. Vidimo da se sve slaže.

Rješenje, uz ključ `vinograd`:

```
iskre nos
susta vno
```

Valja još napomenuti da sam pri rješavanju koristio EH Rječnik WS autora Zorana Cindorija baziranog na rječniku dr. sc. Gorana Igalyja. Relevantni URL-ovi:

```
http://www.inet.hr/~zcindori/rjecnik/
http://web.math.hr/~igaly/EHrjecnik.htm
```