ŠIFRA 13

zadání A – nápovědy B/C - vysvětlení

ZÁVOD PRAHOU
20. ŘÍJNA 2018

Zadání

Tato šifra nepoužívá písmeno CH!

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

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

Nápověda B

Vernam rika…

Nápověda C

Kobyliska strelnice

Vysvětlení

Vernamova šifra používá jednorázový, náhodně generovaný klíč o stejné délce jako zpráva, zarovnaná na násobek pěti znaků. Taková zpráva je bez klíče nerozluštitelná.

Zde ovšem klíč je, je potřeba jen zjistit, že první dva řádky jsou klíč a druhé dva řádky jsou zašifrovaná zpráva. Takže např. prvních 10 znaků:

```
šifra:  L R P W F    L E Q J M
klíč:   P M X I E    Y W Z U N
zpráva: V E R N A    M R I K A
```

Zašifrovaný text: VERNAMRIKADALSIMSTANOVISTEMJE**KOBYLISKASTRELNICE**