Domácí úkol 4

Příklad 4.1 Čtvrtý domácí úkol se skládá ze dvou částí, implementační a detektivní.

Implementační část

Vaším prvním úkolem je implementovat šifrovací a dešifrovací funkce pro Caesarovu a Vigènerovu šifru. Pokud tyto šifry neznáte nebo si nejste jisti implementačními detaily, doporučujeme přečíst si odpovídající popis na Wikipedii[1].

Tedy budete implementovat následující čtyři funkce:

```
caesarEncrypt :: Int -> String -> String
caesarDecrypt :: Int -> String -> String
vigenereEncrypt :: String -> String -> String
vigenereDecrypt :: String -> String -> String
```

Kde

- `caesarEncrypt key plainText` je výsledek zašifrování řetězce `plainText` Caesarovou šifrou s klíčem `key`,
- `caesarDecrypt key cipherText` je výsledek dešifrování řetězce `cipherText`, který byl zašifrovaný Caesarovou šifrou s klíčem `key`,
- `vigenereEncrypt key plainText` je výsledek zašifrování řetězce `plainText` Vigènerovou šifrou s klíčem `key`,
- `vigenereDecrypt key cipherText` je výsledek dešifrování řetězce `cipherText`, který byl zašifrovaný Vigènerovou šifrou s klíčem `key`.

Můžete předpokládat, že vstupem pro všechny tyto funkce budou řetězce skládající se jen z malých písmen anglické abecedy (bez diakritiky a mezer). Stejně tak výstupem všech těchto funkcí má být řetězec skládající se jen z malých písmen anglické abecedy. Například:

```
> caesarEncrypt 5 "ahoj"
"fmto"
> caesarEncrypt 1 "abcdefghijklmnopqrstuvwxyz"
"bcdefghijklmnopqrstuvwxyza"
> vigenereEncrypt "heslo" "ahojsvete"
"hlgugcilp"
> vigenereEncrypt "abcd" "aaaaaaaaaaaa"
"abcdabcdabcd"
```

Při implementaci se vám možná budou hodit funkce `chr` a `ord` z modulu `Data.Char`.

[1] https://cs.wikipedia.org/wiki/Caesarova_%C5%A1ifra
https://cs.wikipedia.org/wiki/Vigen%C3%A8rova_%C5%A1ifra

Detektivní část

Dostali jste od Boba dvě zašifrované zprávy, jednu zašifrovanou Caesarovou šifrou, druhou Vigenèrovou šifrou. Bohužel ale nevíte, jakým klíčem byly tyto zprávy zašifrovány. Za pomoci funkcí implementovaných v první části a interpretu jazyka Haskell zkuste tyto zprávy dešifrovat, pokud víte, že

- text zprávy zašifrované Caesarovou šifrou obsahuje slovo „ahoj“,
- text zprávy zašifrované Vigenèrovou šifrou obsahuje slovo „jmeno“,
- Bobova žena se jmenuje „Alice“, jeho děti se jmenují „Václav“ a „Andrea“, jeho pes se jmenuje „Brok“, jeho kočka se jmenuje „Micka“ a Bob není vůbec kreativní, takže jako klíč k Vigenèrově šifře určitě zvolil jedno z těchto jmen.

Od Boba jste dostali následující zprávy:

- pro Caesarovu šifru `"qxezjecuupzyijybziucfhyxbqielqsyktqzuksyjubujexejefhutcujk"`,
- pro Vigènerovu šifru `"ghkfafmnckqroonarghbmzpktmpgclargwavmpneemvmm"`.

Při dešifrování se vám možná bude hodit funkce `isInfixOf` z modulu `Data.List`.

Poznámky k odevzdání

Odevzdejte jeden `.hs` soubor do příslušné odevzdávárny. Kostru tohoto souboru najdete ve studijních materiálech.

Ve hlavičce souboru uveďte jméno, UČO a skupinu řešitele. V první části souboru implementujte všechny požadované funkce. Nezapomeňte váš zdrojový kód okomentovat. Ve druhé části jako komentář[2] uveďte dešifrované obě zprávy a popište, jak jste při jejich dešifrování postupovali (včetně použitých příkazů interpretu).

Za vaše řešení můžete dostat i desetinné body, pokud například implementujete jen část požadovaných funkcí.

[2] V Haskellu je komentář uvozen značkou --