Laboratorul 6: Practică

Criptare si Decriptare

În criptografie, cifrul lui Cezar, numit și cifru cu deplasare, codul lui Cezar sau deplasarea lui Cezar, este una dintre cele mai simple și mai cunoscute tehnici de criptare. Este un tip de cifru al substituției, în care fiecare literă din textul inițial este înlocuită cu o literă care se află în alfabet la o distanță fixă față de cea înlocuită. De exemplu, cu o deplasare de cinci poziții în alfabetul limbii române, A este înlocuit cu D, Ă devine E și așa mai departe. Această metodă este numită așa după Iulius Cezar, care o folosea pentru a comunica cu generalii săi. Ideea este simplă: se ia un mesaj pe care dorim să îl criptăm și se deplasează toate literele ccu o anumită valoare între 0 și 26. De exemplu, dacă vrem să criptăm propoziția *"THIS IS A BIG SECRET"* cu deplasarea 5, va rezulta sirul "YMNX NX F GNL XJHWJY". În continuare vom implemeta o variantă a acestui cifru.

Codificarea unui mesaj

Criptarea șirurilor caracter cu caracter poate fi reprezentată de o cheie, folosind o listă de perechi. Fiecare pereche din listă indică pentru o literă care este codificarea ei. De exemplu un cifru pentru literele A-E poate fi dat de lista `[('A','C'), ('B','D'),('C','E'),('D','A'),('E','B')]`.

Exerciții

1. Putem roti o lista luând o parte de la început și adăugând-o la final:

```
Main> rotate 3 "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
"DEFGHIJKLMNOPQRSTUVWXYZABC"
```

Deschideți fișierul `lab6.hs` si completați funcția `rotate :: Int -> [Char] -> [Char]`. Pentru un număr `n`, `n > 0` și `n<lungimea listei`, funcția va roti lista cu n elemente. Funcția trebuie să arunce o eroare daca numărul n este negativ sau prea mare (hint: folosiți funcția `error`).

2. Observați funcția `prop_rotate`. Ce testează? Cum evită această funcție aruncarea erorii?
3. Folosind funcția `rotate`, scrieți o funcție `makeKey :: Int -> [(Char, Char)]` care intoarce cheia de criptare cu o anumită deplasare pentru lista de litere mari ale alfabetului englez.

```
Main> makeKey 5
[('A','F'),('B','G'),('C','H'),('D','I'),('E','J'),('F','K'),
('G','L'),('H','M'),('I','N'),('J','O'),('K','P'),('L','Q'),
('M','R'),('N','S'),('O','T'),('P','U'),('Q','V'),('R','W'),
('S','X'),('T','Y'),('U','Z'),('V','A'),('W','B'),('X','C'),
('Y','D'),('Z','E')]
```

4. Scrieți o funcție `lookUp :: Char -> [(Char, Char)] -> Char` care caută o pereche după prima componentă și întoarce a doua componentă a acesteia. Dacă nu există o pereche cu caracterul căutat pe prima poziție, funcția întoarce caracterul dat ca parametru.

```
Main> lookUp 'B' [('A', 'F'), ('B', 'G'), ('C', 'H')]
'G'
Main> lookUp '9' [('A', 'X'), ('B', 'Y'), ('C', 'Z')]
'9'
```

5. Scrieți o funcție `encipher :: Int -> Char -> Char` care criptează un caracter folosind cheia dată de o deplasare dată ca parametru.

```
Main> encipher 5 'C'
'H'
Main> encipher 7 'Q'
'X'
```

6. Pentru a fi criptat, textul trebuie să nu conțină semne de punctuație și să fie scris cu litere mari. Scrieți o funcție `normalize :: String -> String` care normalizează un șir, transformând literele mici în litere mari și eliminând toate caracterele care nu sunt litere sau cifre.

```
Main> normalize "July 4th!"
"JULY4TH"
```

7. Scrieți o funcție `encipherStr :: Int -> String -> String` care normalizează un șir și îl criptează folosind funcțiile definite anterior.

```
Main> encipherStr 5 "July 4th!"
"OZQD4YM"
```

Decodarea unui mesaj

8. Scrieți o funcție `reverseKey :: [(Char, Char)] -> [(Char, Char)]` pentru a inversa cheia de criptare, schimbând componentele din fiecare pereche între ele.

```
Main> reverseKey [('A', 'G'), ('B', 'H') , ('C', 'I')]
[('G', 'A'), ('H', 'B') , ('I', 'C')]
```

9. Scrieți funcțiile

```
decipher :: Int -> Char -> Char
decipherStr :: Int -> String -> String
```

pentru a decripta un caracter si un string folosind cheia generată de o deplasare dată. Funcția va lăsa nemodificate cifrele și spațiile, dar va șterge literele mici sau alte caractere.

```
Main> decipherStr 5 "OZQD4YM"
"JULY4TH"
```