

Quebrando a cifra de Deslocamento Simples

A cifra de deslocamento simples é uma cifra de substituição mono-alfabética, quer isto dizer que cada letra do alfabeto contida na mensagem original será substituída sempre pela mesma letra do alfabeto. Por exemplo, numa cifra de Júlio César, todos os “a”s da mensagem original serão substituídos por “d”s, na mensagem cifrada.

É então possível, dado um, ou mais, textos cifrados, montar o seguinte ataque.

- Dada a frequência relativa das letras na língua em que se escreveram essas mensagens.
 1. Para todos os valores possíveis da chave, calcular a frequência relativa das letras nos textos assim decifradas.
 2. Comparar as duas tabelas de frequências relativas das letras, a da língua de base utilizada e a das várias tentativas.
 3. Calcular o valor do χ -quadrado entre a lista de frequências da mensagem (fr) e a lista das frequências esperadas para o Português ($frPT$), o qual é dado pela expressão $\sum_{i=0}^{n-1} \frac{(fr_i - frPT_i)^2}{frPT_i}$. O menor valor encontrado dá-nos o melhor ajuste entre as duas tabelas de frequências, e portanto o melhor candidato à chave da cifra.

Dada a seguinte tabela para as frequências relativas das letras do alfabeto na língua Portuguesa (considerando somente as letras entre 'a' e 'z'):

```
tabelaPT :: [Float]
tabelaPT = [14.811279, 1.051562, 3.691005, 5.094306, 12.775915, 0.980317, 1.210767,
            1.463604, 5.898956, 0.371862, 0.005934, 3.058580, 4.665052, 4.909355,
            10.633738, 2.429875, 1.226371, 6.736397, 7.917757, 4.174107, 4.473234,
            1.705391, 0.005142, 0.215266, 0.027841, 0.466387]
```

Implemente em Haskell as seguintes funções:

1. `freqRel :: String → [Float]`

que dado um texto (“string”), devolve a lista das frequências relativas, para esse texto, das letras do alfabeto.

2. `chiQuadrado :: [Float] → [Float] → Float`

que calcula o valor do χ -quadrado para duas listas de valores reais.

3. `desloca :: Int → [a] → [a]`

que desloca todos os valores de uma dada lista n posições para a esquerda.

4. `quebra :: String → (String, Int)`

que quebra a cifra de deslocamento simples, dando como resultado o texto decifrado, assim como o valor da chave de encriptação.