Cifra Deslocamento Simples

A cifra de Júlio César (100ac-44ac) é um cifra de substituição mono-alfabética simples, definida pelo deslocamento das letras da mensagem original, ao que se sabe esse deslocamento era de três posições para a direita, quando se consideram as suas posições relativas no alfabeto usado na mensagem.

Temos então que as várias letras do texto a cifrar vão ser substituídas por outras letras, três posições mais à direita, considerando-se o mesmo alfabeto de base para os textos em claro e para os textos cifrados. Sempre que neste processo de deslocameno se ultrapasse o fim do alfabeto retoma-se o cálculo das posições no início do alfabeto.

O processo de desencriptar é simétrico deste processo.

Considere o seguinte alfabeto e a sua respectiva codificação:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
w	x	y	z	à	á	â	ã	ç	è	é	ê	ì	í	ò	ó	ô	õ	ù	ú	ü	
22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	

Por exemplo, a mensagem “acifradejúliocésar” é tranformada em “dfliudghmbolrfívdu”

a	c	i	f	r	a	d	e	j	ú	l	i	o	c	é	s	a	r
0	2	8	5	17	0	3	4	9	41	11	8	14	2	32	18	0	17
3	5	11	8	20	3	6	7	12	1	14	11	17	5	35	21	3	20
d	f	l	i	u	d	g	h	m	b	o	l	r	f	í	v	d	u

Formalmente tem-se:

Definição 1 (Cifra Deslocamento) *Sejam* $\mathcal{M} = \mathcal{C} = (\mathbb{Z}_{43})^*$ *e* $\mathcal{K} = \mathbb{Z}_{43}$. *Define-se então:*

$$e_K(x) = (x + K) \bmod 43$$

e

$$d_K(y) = (y - K) \bmod 43$$

para todo o $x, y \in \mathbb{Z}_{43}$

sendo que o operador “x mod y” nos dá o resto da divisão inteira de x por y.

Implemente em Haskell as seguintes funções:

1. Para a conversão entre as letras do alfabeto e a sua codificação.

```
letrasParaInt :: Char → Int
intParaLetras :: Int → Char
```

2. Implementação da cifra de deslocamento simples com chave $n \in \mathbb{Z}_{43}$.

```
cifra :: Int → Char → Char
```

3. Implementação do decifrar de um carácter da mensagem, dada a chave $n \in \mathbb{Z}_{43}$.

   `decifra :: Int → Char → Char`

4. O processo de encriptar uma mensagem.

   `encriptar :: Int → String → String`

5. O processo de desencriptar uma mensagem.

   `desencriptar :: Int → String → String`