

Universidade Tecnológica Federal do Paraná (UTFPR)
Departamento Acadêmico de Informática (DAINF)
Introdução à Criptografia
Professor: Rodrigo Minetto (rodrigo.minetto@gmail.com)

Lista de exercícios

1) Implemente a cifra de César e recupere o significado do arquivo “misterio.txt”, em anexo ao material da aula, que foi deslocado três casas para frente. Os caracteres especiais para “**espaço**” e “**nova linha**” não foram codificados. O código utilizado para criptografar é:

```
...
int alphabet_size = 26;
int shift = ?; /*deslocamento!*/
char ch;
...
code = ((ch - 'a') + shift) % alphabet_size + 'a';
```

2) Descubra o significado do arquivo “carta.txt”, em anexo ao material da aula, que foi criptografado de um texto em português com uma cifra de substituição monoalfabética. Se achar necessário, desenvolva para auxiliá-lo um programa que conta a frequência dos símbolos. O importante neste exercício não é decifrar todo o conteúdo da carta sem erros, mas sim discutir como você conseguiu achar algum significado. Precisamente, liste as informações que o levaram a fazer as substituições.

A título de curiosidade, os textos das cartas foram escritos por lideranças de facções criminosas e contém um suposto plano para execução de um promotor de justiça. As cartas foram interceptadas pela polícia no ano passado.

Para auxiliá-lo considere as seguintes frequências de letras para textos em português

a	b	c	...
0.1463,	0.0104,	0.0388,	0.0499,
0.1257,	0.0102,	0.0130,	0.0128,
0.0618,	0.0040,	0.0002,	0.0278,
0.0474,	0.0505,	0.1073,	0.0252,
0.0120,	0.0653,	0.0781,	0.0434,
0.0463,	0.0167,	0.0001,	0.0021,
0.0001,	0.0047		

