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
```

4M9CK9F7CH XT6594M PZ9C 659HN9C (A) CK4MB5CK659A3 DZHNCK CKAMG39C CKW2854A3W2G3659CK G3A3P2A34M 854A3V8 4M9CHNP2CK 9CB5CK4919C659 P2A3 K9HN7239C659. P2A3 B5CKP2XTP2A3 D2HNCK M5A3XT M5CKXTG3A3 B56599C K9CKF79CW2G39C659 9C 8549CV8XTW28A9CP29C P2A3 M56599CW2723A3, CK4M4MCK D2HNCK V8A36599C W29C V8CK4MV89C D2HNCKX16S99CP29C P2CK F7A3854CKXT4M G39C W29C V89CA3. G3HNP2A3 A34M CKW2P2CK659CK854A3 D2HNCK CKK9CK F79CXT G39C V89CB5CK9CP2A3. CKK9CK V8A36599C W29C K99CHN4M V8CK4MV8A3 CK M5XT8549C 9C 4MCKV89CW29C G3A3P29C B5A3659 K99C B5A3659D2HNCK A3 G36599CV8B5A3 P2CKK9CK CK K99C P2CKW2G3659A3. P29C B56599C M59C491CK659 CKK9CK 8AA36599C DZHNCK DZHNXT 4MCK659, WZA3XTAM 1489C G3CKV8 A3 8549C659659A3, A34M A36599C659XTA3, G3HNP2A3 P2CKK9CK, A3HNG3659A3 4M9CK9F7CK, P2A3 M56599CW2723A3 1489CB5A3W2CKXT4M HNV8 B5A3HN854A3 V89CXT4M CK1 854A3W2B5K9XT8549CP2A3, V89CXT4M P29C B56599C M59C491CK659 G39CV8X1CKV8 A36599C D2HNCK D2HNXT4MCK659. A3 D2HNCK G39C B5CK7239CW2P2A3 CK D2HNCK 9C 854XTP29CP2CK P2CKK9CK CK X1CKV8 V89CXTA3659 DZHNCK OP, B56599L PZ9C659 A3 X19CK99CA3 P2CKB5A3XT4M CK V89CXT4M P2XTM5XT854XTK9, V89CXT4M

