Implementação de cifradores simétricos

O objetivo desta atividade prática é compreender melhor o funcionamento dos algoritmos de cifragem simétrica mais simples.

O cifrador de César

Produzir uma implementação do cifrador de César. Ele deve funcionar da seguinte forma:

Para cifrar:

```
cesar -c -k 5 < texto-aberto.txt > texto-cifrado.txt
```

Para decifrar:

```
cesar -d -k 5 < texto-cifrado.txt > texto-aberto.txt
```

Opções:

- -c : cifrar
- -d : decifrar
- -k *n* : valor da chave a ser usada

A rotação de caracteres deve ser feita **somente** sobre os caracteres [A-Za-z0-9]. Caracteres acentuados devem ser tratados sem acento.

Análise de frequências

A análise de frequências é uma técnica simples de criptanálise que consiste em identificar os caracteres do texto cifrado usando a frequência de uso dos caracteres na língua em que se supõe que a mensagem esteja escrita. O algoritmo de César é um cifrador de substituição simples e portanto vulnerável a essa técnica.

Considerando a tabela de frequências de caracteres em português informada abaixo (obtida deste site), escreva um programa para fazer a criptanálise de uma mensagem cifrada com o cifrador de César.

Letra	Freq.%	Letra	Freq.%	Letra	Freq.%	Letra	Freq.%	Letra	Freq.%
A	14.63	B	1.04	C	3.88	D	4.99	E	12.57
F	1.02	G	1.30	H	1.28	I	6.18	J	0.40
K	0.02	L	2.78	M	4.74	N	5.05	O	10.73
P	2.52	Q	1.20	R	6.53	S	7.81	T	4.34
U	4.63	V	1.67	W	0.01	X	0.21	Y	0.01
Z	0.47								

A mensagem a ser analisada é:

```
g5Bt5 t54yvtz3v4A5 wrG t53 7Bv r9 6v995r9 9v 9z4Ar3
58xB2y59r9. dBzA5 t54yvtz3v4A5, 7Bv 9v 9z4Ar3
yB3z2uv9. Vy r99z3 7Bv r9 v96zxr9 9v3 x8r59 v8xBv3
uv9uv4y59r3v4Av r trsvtr 6r8r 5 tvB, v47Br4A5 r9
tyvzr9 r9 srzEr3 6r8r r Av88r, 9Br 3rv.
```

```
cv54r8u5 Ur mz4tz.
```

O cifrador RC4

O RC4 é um algoritmo de cifragem simétrica por fluxo, proposto por Rivest em 1987. Além de ser eficiente e robusto, ele possui uma implementação bastante simples e didática. Esse cifrador está disponível em linha de comando através do pacote `openssl` (em Linux):

Exemplos de operações simples (`man enc` ou `man openssl` para exemplos mais complexos):

```
openssl rc4 -in input.txt -out output.rc4
```

Para decodificar um arquivo:

```
openssl rc4 -d -in input.txt -out output.rc4
```

Atividade: aplicar o cifrador RC4 ao texto da atividade anterior e efetuar a análise de frequências do arquivo de saída. Comparar a distribuição de frequências da entrada com a da saída.

O cifrador de Vernam

Escrever um programa cifrador de Vernam que funcione da seguinte forma:

```
vernam -c chave.dat < texto-aberto.txt > texto-cifrado.txt
```

Questões para refletir:

- Como será feita a geração da chave?
- Como você pode testar seu cifrador?
- O algoritmo de Vernam é vulnerável à análise de frequências?

From:
https://wiki.inf.ufpr.br/maziero/ - **Prof. Carlos Maziero**

Permanent link:
https://wiki.inf.ufpr.br/maziero/doku.php?id=sas:cifradores

Last update: **2014/04/25 16:01**