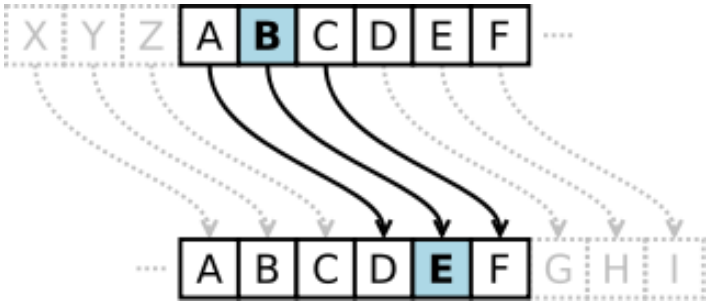
Cifra de César

Programação em Python

A Cifra

Descrição

Em criptografia, a Cifra de César, também conhecida como cifra de troca, código de César ou troca de César, é uma das mais simples e conhecidas técnicas de criptografia. É um tipo de cifra de substituição na qual cada letra do texto é substituída por outra, que se apresenta no alfabeto abaixo dela um número fixo de vezes. Por exemplo, com uma troca de três posições, A seria substituído por D, B se tornaria E, e assim por diante. O nome do método é em homenagem a Júlio César, que o usou para se comunicar com os seus generais.



Uso

A transformação pode ser representada alinhando-se dois alfabetos; o alfabeto cifrado é o alfabeto normal rotacionado à direita ou esquerda por um número de posições. Por exemplo, aqui está uma cifra de César usando uma rotação à esquerda de três posições (o parâmetro de troca, três neste caso, é usado como chave)

```
Normal:   abcdefghijklmnopqrstuvwxyz
Cifrado:  defghijklmnopqrstuvwxyzabc
```

Para criptografar uma mensagem, deve-se simplesmente observar cada letra da mensagem na linha "Normal" e escrever a letra correspondente na linha "Cifrado". Para descriptografar, deve-se fazer o contrário.

```
Normal:   a ligeira raposa marrom saltou sobre o cachorro cansado
Cifrado:  d oljhlud udsrvd pduurp vdowrx vreuh r fdfkruur fdqvdgr
```

Quebrando a Cifra de Cesar

A cifra de César pode ser facilmente decifrada mesmo em um cenário que se tenha apenas o texto cifrado.

Sabendo que a cifra consiste apenas na movimentação de letras de um alfabeto, sabe-se que ela se limita a 26 possíveis chaves.

Rotação ou troca	Possível texto
0	exeuyi eksve
1	dwdtxh djrud
2	cvcsw gciqtc
3	bubrvf bhpsb
4	Ataque agora
5	zszptd zfnqz
6	yryosc yempy
...	
23	hahxbl hnvyh
24	gzgwak gmuxg
25	fyfvzj fltwf

Encontrando todas as soluções possíveis há duas maneiras de encontrar a chave certa.

Manualmente

A pessoa que aplicou a força bruta pode manualmente observar as saídas para cada uma das 26 chaves e selecionar a que mais faz sentido.

Automaticamente

Sabendo palavras que podem estar presentes na mensagem original (ou o idioma dela) é possível criar um dicionário do idioma.

Desta maneira, para cada solução possível deve ser contabilizado o número de palavras contidas no dicionário presentes na mensagem obtida.

A solução com maior número de palavras do dicionário presentes, deve ser a que pertence ao idioma.

Atividade

A atividade da M1 será um algoritmo força bruta capaz de quebrar a Cifra de César automaticamente.

Para isso, devem ser utilizados os arquivos **fantasia.txt** e **lagrimas.txt** como mensagens a serem lidas, e o arquivo **dicionariopt.txt** como dicionário do idioma.

Para facilitar, não serão utilizados acentos nas palavras.

O dicionariocompletopt.txt possui todas as palavras da língua portuguesa. Para quem quiser um desafio a mais, pode fazer um algoritmo para o processo de codificar qualquer mensagem (CUIDADO com os acentos)