Computação: Criptografia

Marcos Santana | marcos_br_santana@outlook.com

Tutorial 1

Certo dia, Maria verificando seu e-mail, encontra uma mensagem estranha, que parecia estar criptografada. A mensagem se encontra abaixo:

```
Ofrjx Hqjwp Thedlss, (5275-5213), mvythkv go wkdowkdsmk tipe Ljvkarmpn
Exsfobcsdi, Thedlss makzmdmc, go 5209, wo gxzomu vnvxajenu pq uyep hoh cvqnqkwc
bpitbpixrpbtcit cu pimw fg Mhyhkhf f fg Gsvkxk. Iwwe ylshjhv jsywj qu
igsvuy mtmbzqkw f vjpwncrlx ykxboa gsqs fewi teve p txh, qemw yfwij, irl noxywsxkny
tsifx f igsvuy ubujhecqwdujysei, wo swzybdkxdo hfrut fg kyzaju fc
oxqoxrkbsk mtmbzqki. P Rwbcrcdcn qh Ovomdbsmkv dqg Ovodbyxsmc Nwprwnnab (MIII)
xvd xpd ercerfragnpnb nyhmpjh ijxxj yarwlryrx go vhx twowbqxw, pq uyep xpd wixe
go qnsmf vixe bozbocoxdk kwzzmvbm f xpd wixe go qnsmf hzwaf bozbocoxdk p hfrut
tatigdbpvctixrd. Iwwe ylshjhv f lxvdvnwcn lxwqnlrmj gsqs b wjlwf fc pdr kpylpah.
Thedlss irl wo lrnwcrbcj f alvypjv rznyt fynat. Hoh f qemw lxwqnlrmx ujqfx
"mycikwma fg Thedlss". P thedlss, bupkhkl fg kqzct vjpwncrlx, yljlilb iwwi
rsqi go vxd qxvnwjpnv.
```

Sem saber o que a mensagem dizia, ela decide pedir ajuda ao seu professor de Álgebra, que confirma sua suspeita. Ele diz que poderia ser um tipo de criptografia conhecida como "Cifra de César", que é muito antiga e fácil de ser quebrada. No entanto, ele também diz que não poderia ajuda-lá, pois não tinha conhecimentos de programação para criar um algorítimo que decifrasse a mensagem.

Maria curiosa para descobrir o que a mensagem dizia, decide fazer uma pesquisa na internet sobre a "Cifra de César". Ela vê então que essa criptografia consiste em trocar uma letra do alfabeto por outra, seguindo uma ordem lógica. Quando a chave é 3, troca-se A por D, B por E, C por F e assim por diante. A imagem abaixo mostra um mecanismo utilizado por Júlio César.

Figura 1: Cifra de César

Após entender como funcionava a criptografia, Maria procurou saber mais sobre algorítimos. Porém, ela nunca havia tido nenhum contato com tal área. Logo ela descobre que precisaria escolher uma linguagem de programação e de uma IDE compatível com essa para poder escrever seu algorítimo.

1. Há uma vasta gama de linguagens de programação, cada uma tem vantagens e desvantagens, que a tornam mais viáveis ou não para determinados algorítimos. O que é uma linguagem de programação? Cite cinco.

2. IDE ou Ambiente de Desenvolvimento Integrado, é uma ferramenta que pessoas utilizam para desenvolvimentos de software. Cada IDE é compatível apenas com algumas Linguagens de Programação. Como funciona uma IDE? Encontre algumas compatíveis com a linguagem C++.

3. Após entender como funciona as Linguagens de Programação e IDE, Maria decide que irá escrever seu algoritimo em C++, e encontra duas IDE completíveis com a linguagem. Essas são o Visual Studio: `https://www.visualstudio.com/pt-br/vs/community/` e o Code Blocks: `http://www.codeblocks.org/`. Pesquise mais sobre as duas IDE, pergunte para colegas e outras pessoas mais experientes de seu curso, veja prós e contras e analise qual será a melhor opção para você.

Após muita pesquisa, Maria decide qual IDE é melhor para ela, então o baixa e instala. Chega a hora de escrever o algoritimo, mas Maria não sabe nem por onde começar, Então ela tem a ideia de procurar por um algorítimo de Cifra de César em linguagem C++ na internet, até que ela encontra um repositório no GitHub que poderia ajuda-lá. O repositório que ela encontrou foi esse: `https://github.com/zerocool-br/cifradecesar`.

4. Leia o arquivo README.md do repositório e tente entender o que cada função faz. Em seguida, baixe o código, e tente o compilar e executar no seu IDE, depois, tente descriptografar a mensagem.

   Dica: pesquise sobre as bibliotecas usadas no programa e por suas principais funções, depois tente fazer programas simples com elas.

Maria tenta descriptografar a mensagem utilizando várias chaves, mas sem exito. No entanto, ela vai notando que Caracteres especias como acentos, colchetes e virgulas devem ser ignorados ou substituídos por um equivalente. Após várias tentativas, ela começa notar também alguns padrões. Algumas chaves conseguem descriptografar algumas palavras, porém outras são apenas descriptografadas com outras chaves. No entanto, o programa que ela está usando, trabalha apenas com uma chave *Estática*, todavia, a mensagem parece estar criptografada com o que aparenta ser uma chave *Dinâmica*!

5. Assim como Maria, faça o teste com várias chaves, até chegar na mesma conclusão. O que quer dizer que a mensagem foi criptografada com uma chave *Estática*? E com uma chave *Dinâmica*? Dê exemplos.

6. Agora que você entendeu como funciona a criptografia na mensagem, faça alterações no programa e tente descriptografar a mensagem. O que ela diz?

   Dica: utilize a função strlen.

Referências

[1] Cifra de César. Disponível em: https://pt.wikipedia.org/wiki/Cifra_de_C%C3%A9sar. Acesso em 13 de Abril de 2017

[2] Caesar Cipher. Disponível em: http://www.dcode.fr/caesar-cipher. Acesso em 13 de Abril de 2017