

Trabalho 1

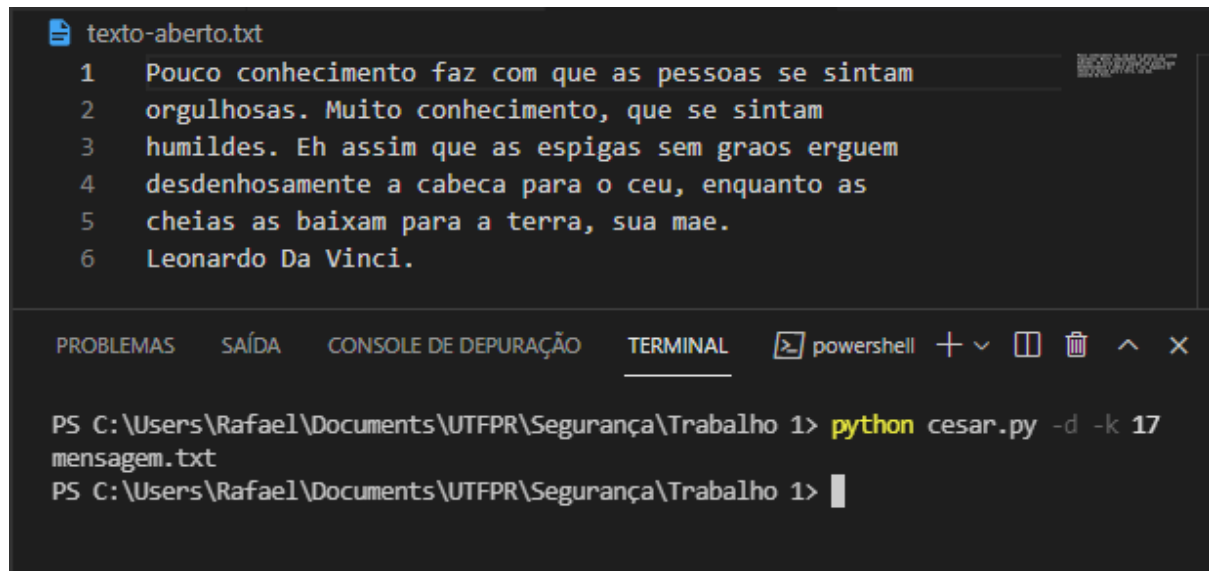
Rafael Lammel Marinheiro
05/10/2021

A. Faça a criptoanálise da mensagem cifrada com o cifrador de César e mostre a chave usada. Qual é o texto criptografado?

R.: Utilizando o script de criptoanálise na mensagem fornecida do trabalho é possível notar que a letra 'r' é o símbolo que mais aparece dentro da mensagem (considerando apenas os símbolos que são criptografados, como diz o enunciado da questão):

Símbolo	Freq. (%)
r	14.49
v	12.56
9	11.59
5	8.21
4	5.8
z	5.8
3	5.8
B	5.31
t	5.31
A	3.86
8	3.86
y	3.38
7	1.93
6	1.93
x	1.93
u	1.93
2	0.97
s	0.97
g	0.48
w	0.48
G	0.48
d	0.48
V	0.48
E	0.48
c	0.48
U	0.48
m	0.48

De acordo com a própria proposta do trabalho, é comum nos textos que a letra 'a' seja a letra mais utilizada do alfabeto. Apesar de estarmos considerando números na criptografia também, essa dedução ainda pode ser bem aplicada. Sendo assim, foi verificado que a distância entre a letra que mais apareceu na mensagem cifrada ('r') para o 'a' é de 17. Aplicando a cifra de César para descriptografar, com chave 17, temos a mensagem descriptografada:



The screenshot shows a code editor with a file named 'texto-aberto.txt' containing the following text:

```
1 Pouco conhecimento faz com que as pessoas se sintam
2 orgulhosas. Muito conhecimento, que se sintam
3 humildes. Eh assim que as espigas sem graos erguem
4 desdenhosamente a cabeça para o ceu, enquanto as
5 cheias as baixam para a terra, sua mae.
6 Leonardo Da Vinci.
```

Below the editor is a terminal window with the following commands and output:

```
PS C:\Users\Rafael\Documents\UTFPR\Segurança\Trabalho 1> python cesar.py -d -k 17
mensagem.txt
PS C:\Users\Rafael\Documents\UTFPR\Segurança\Trabalho 1>
```

Chave: 17

Texto:

*Pouco conhecimento faz com que as pessoas se sintam
orgulhosas. Muito conhecimento, que se sintam
humildes. Eh assim que as espigas sem graos erguem
desdenhosamente a cabeça para o ceu, enquanto as
cheias as baixam para a terra, sua mae.
Leonardo Da Vinci.*

B. O algoritmo de Vernam é vulnerável à análise de frequências? Justifique.

R.: Não. Como no algoritmo de Vernam utilizamos uma chave aleatória do mesmo tamanho ou de tamanho maior que a mensagem original, cada caractere é criptografado com uma chave diferente, ao invés de criptografamos o texto inteiro com a mesma chave. Isso faz com que uma letra no texto original seja mapeada para uma letra aleatória, ou seja, a mesma letra na mensagem original pode ser representada por letras diferentes na mensagem criptografada, tornando praticamente impossível o uso de um analisador de frequência na mensagem cifrada.

B-I. Como será feita a geração da chave?

R.: Para cada criptografia será gerada uma chave aleatória com o mesmo número de símbolos que a mensagem original (desconsiderando os símbolos que não entram na criptografia). Essa chave é então salva em um arquivo **.dat** que o usuário pode utilizar depois para descriptografar a mensagem.

B-II. É possível usar o algoritmo de Vernam para cifrar uma base de dados? Justifique.

R.: Sim, porém não seria eficiente, pois a chave precisa ter o mesmo tamanho que os dados que estão sendo encriptados. Dessa forma, a quantidade de dados a serem guardados dobra de tamanho.

C. O algoritmo RC4 é vulnerável à análise de frequências? Justifique.

R.: Não. O algoritmo RC4 transforma as letras da mensagem original em uma letra aleatória na mensagem final, ou seja, a mesma letra no texto original pode ser criptografada para uma letra diferente na mensagem criptografada.