1) Implementação

Tanto a Cifração quanto a Decifração Vigenere de mensagens estão implementadas na classe `VigenereCypher` do arquivo encrypt_decrypt.py

O código apresentado no arquivo encrypt_decrypt.py é uma implementação da Cifra de Vigenere. A classe VigenereCypher possui três métodos principais: mapping, encrypt e decrypt.

1. Método mapping: Este método cria e retorna uma matriz de mapeamento, onde cada linha representa um alfabeto rotacionado em uma posição.
2. Método encrypt: O método encrypt recebe como parâmetros a mensagem original, a chave, a matriz de mapeamento e o alfabeto. Ele cria uma variável chamada mensagem_cifrada, que armazenará a mensagem criptografada. Usando um loop while, o método percorre a mensagem original e verifica se cada caractere está no alfabeto. Se estiver, ele encontra a linha e a coluna correspondentes na matriz de mapeamento usando os valores ordinais dos caracteres e adiciona o caractere mapeado à mensagem_cifrada. Se não estiver no alfabeto, o caractere é adicionado diretamente à mensagem_cifrada. Ao final, a mensagem_cifrada e seu comprimento são retornados como uma tupla.
3. Método decrypt: O método decrypt é usado para decifrar a mensagem criptografada, revertendo o processo de criptografia. Ele recebe como parâmetros a mensagem_cifrada, a chave e o alfabeto. A variável mensagem_decifrada armazena a mensagem decifrada durante o processo. O método usa um loop while para percorrer a mensagem_cifrada e verifica se cada caractere está no alfabeto. Se estiver, ele calcula a coluna do caractere decifrado usando os valores ordinais dos caracteres e, em seguida, usa a função chr() para converter o valor ordinal na letra correspondente, que é adicionada à mensagem_decifrada. Se o caractere não estiver no alfabeto, ele é adicionado diretamente à mensagem_decifrada. Ao final, a mensagem_decifrada e seu comprimento são retornados como uma tupla.

Tamanho da Chave

O tamanho da chave é essencial para conseguirmos quebrar a criptografia Vegenere.

O processo para se encontrar possíveis tamanhos de chave está implementado no arquivo key_size.py e se tem como base o método de Kasiski, um método que visa encontrar possíveis tamanhos de chave utilizados em uma mensagem cifrada com a cifra de Vigenere. É baseado na análise de frequência de trigramas (conjuntos de três caracteres) ou n-gramas e na identificação de padrões repetidos.

1. A função **`key_size_probabilities`** é a função principal que reúne todos os recursos das outras funções utilizadas e realiza as seguintes etapas: Trata a mensagem cifrada, removendo caracteres não alfabéticos; obtém o histograma de trigramas; descarta os trigramas com frequência menor que o valor especificado; calcula os dvalues (diferenças entre ocorrências consecutivas) para os trigramas restantes; calcula o MDC para cada lista de dvalues e armazena a contagem de cada MDC em um dicionário chamado **`size_score`**; ordena o dicionário **`size_score`** em ordem decrescente de frequência e salva os resultados em um arquivo chamado "KeySize/SizeScore.txt", contendo possíveis tamanhos de chave e suas respectivas probabilidades.

Descoberta da Chave

Ao identificar o tamanho da chave, podemos dividir a mensagem cifrada em grupos e analisar a frequência relativa das letras. Comparando com frequências de diferentes idiomas, podemos determinar o idioma original e a chave, quebrando a criptografia.

No arquivo key_by_size.py, o código gera distribuições de cada grupo de caracteres cifrados pela mesma letra da chave, usando o tamanho da chave como parâmetro. Um arquivo é criado contendo as distribuições de frequência das letras de cada grupo e integrado ao arquivo dashboard_de_distribuicao.pbix, facilitando a análise de distribuição visualmente no Power BI.

app.py

Esse código é basicamente o script que integra todas as funcionalidades em um programa único de linha de comando.

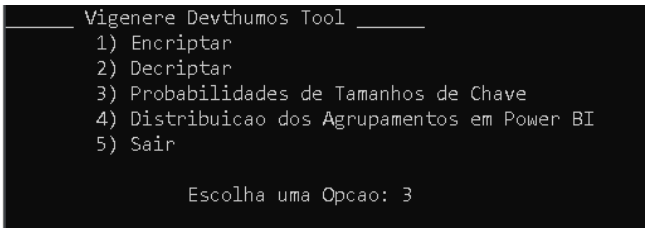
É recomendado a leitura do readme do repositório git para compreender melhor as instruções de utilização, mas de certa forma a execução é bem intuitiva e explicada pelo próprio programa.

2) Desafios

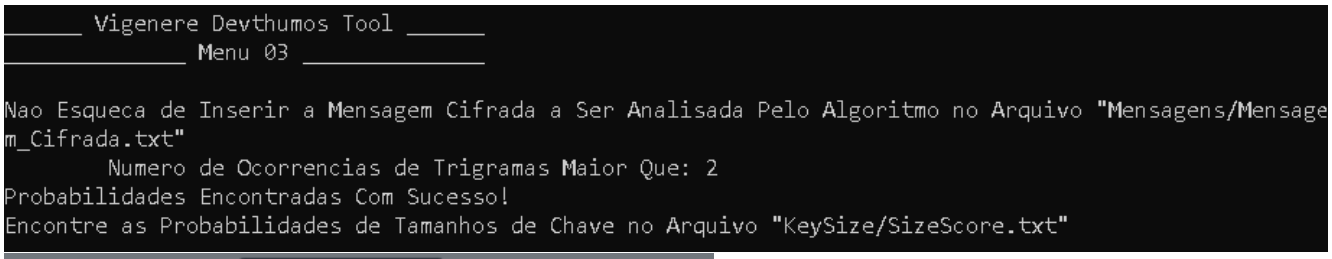
Os desafios são bastante similares quanto a forma de quebrar a criptografia

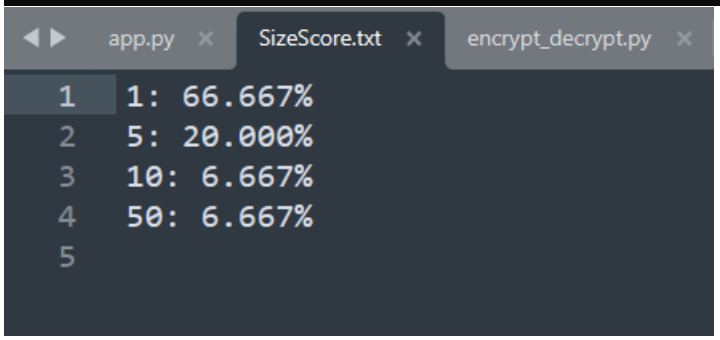
Desafio 1

O **primeiro passo** é descobrirmos possíveis tamanhos para a chave utilizada nessa cifra utilizando a opção 2 do programa principal app.py:



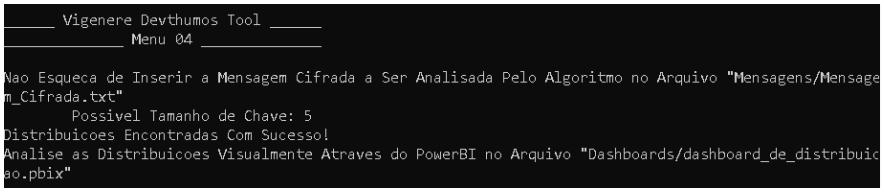
Filtramos quais trigramas serão utilizados para a o método de Kasisk através da escolha do parâmetro "maior que".





O **segundo passo** é escolhermos um possível tamanho de chave para começarmos a análise de distribuição. Nesse caso presumi que o Professor não escolheria uma chave de tamanho 1 e fui direto para o tamanho 5.

O **terceiro passo** é gerarmos distribuições de frequência de letras para compararmos com os dos idiomas inglês e português, assim como também descobrirmos a chave.

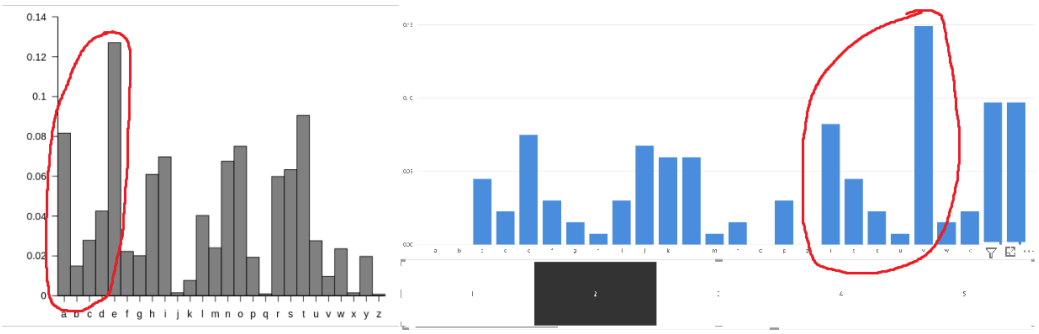


O **Quarto passo** é descobrir qual é o idioma. A criptografia Vegenere não está alterando a ordem ou tamanho das palavras, bem como não está afetando caracteres não alfabéticos. Dessa forma é bem intuitivo identificar o idioma de cada mensagem. A primeira mensagem é em inglês e a segunda mensagem é em português.

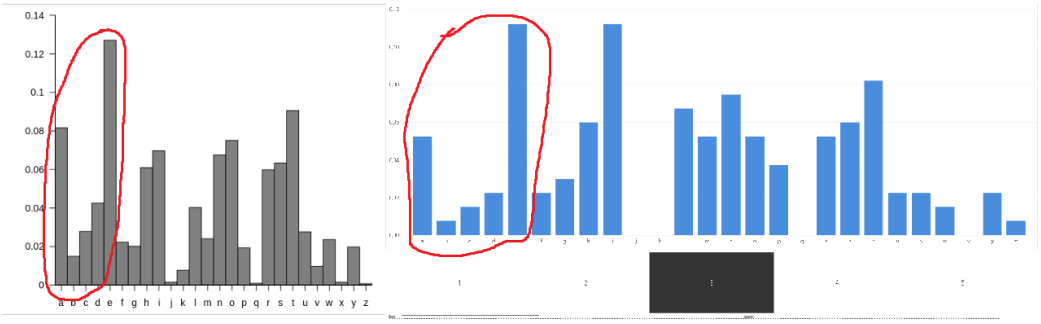
O **Quinto passo** é o penúltimo para decifrar a mensagem desafio 1 e consiste em comparar a distribuição de frequência de letras em inglês e descobrirmos a chave numérica de César, já que podemos trabalhar com cada grupo como se fosse esse tipo de Cifra.

- O primeiro caractere da Chave é “a”, é só analisarmos os picos de distribuição e encaixar na distribuição das letras em inglês

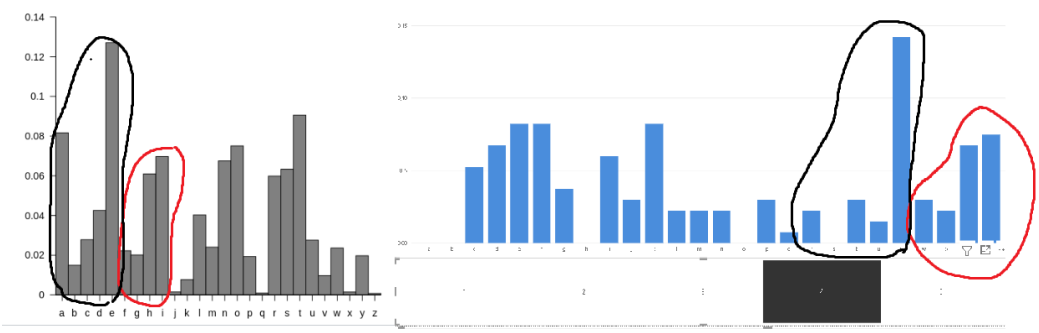
- O segundo caractere da Chave é “r”



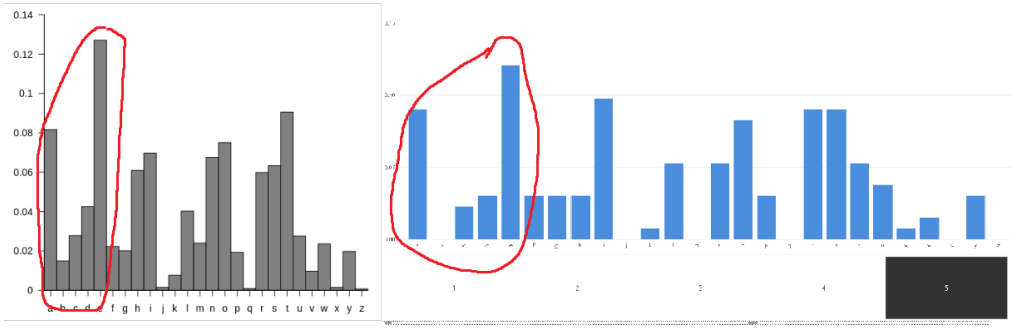
- O terceiro caractere da Chave é “a”



- O quarto caractere da Chave é “r”



- O quinto caractere da Chave é “a”



→ O sexto passo é decifrar a mensagem cifrada com a chave que encontramos

```
_____ Vigenere Devthumos Tool _____
       1) Encriptar
       2) Decriptar
       3) Probabilidades de Tamanhos de Chave
       4) Distribuicao dos Agrupamentos em Power BI
       5) Sair

              Escolha uma Opcao: 2



_____ Vigenere Devthumos Tool _____
_____________ Menu 02 _____________

Nao Esqueca de Inserir a Mensagem Cifrada a Ser Decifrada no Arquivo "Mensagens/Mensagem_Cifrada.txt"
       Chave: arara
Mensagem Decifrada Com Sucesso!
Encontre a Mensagem Decifrada no Arquivo "Mensagens/Mensagem_Decifrada.txt"
```

regulating the circulation. whenever i find myself growing grim about the mouth; whenever it is a damp, drizzly november in my soul; whenever i find myself involuntarily pausing before coffin warehouses, and bringing up the rear of every funeral i meet; and especially whenever my hypos get such an upper hand of me, that it requires a strong moral principle to prevent me from deliberately stepping into the street, and methodically knocking people's hats off--then, i account it high time to get to sea as soon as i can. this is my substitute for pistol and ball. with a philosophical flourish cato throws himself upon his sword; i quietly take to the ship. there is nothing surprising in this. if they but knew it, almost all men in their degree, some time or other, cherish very nearly the same feelings towards the ocean with me.

Com o desafio em português também não é diferente, os mesmos passos irão dar o mesmo resultado: A quebra da criptografia de Vegenere. Não consegui colocar de forma separada, pelo fato de ter dado 18 páginas, originalmente. Porém existe no diretório o PDF Mais_Detalhes_Ainda, que apresenta o código fonte com maior profundidade.

algum tempo hesitei se devia abrir estas memorias pelo principio ou pelo fim, isto e, se poria em primeiro lugar o meu nascimento ou a minha morte. suposto o uso vulgar seja comecar pelo nascimento, duas consideracoes me levaram a adotar diferente metodo: a primeira e que eu nao sou propriamente um autor defunto, mas um defunto autor, para quem a campa foi outro berco; a segunda e que o escrito ficaria assim mais galante e mais novo. moises, que tambem contou a sua morte, nao a pos no introito, mas no cabo: diferenca radical entre este livro e o pentateuco. dito isto, expirei as duas horas da tarde de uma sexta-feira do mes de agosto de 1869, na minha bela chacara de catumbi. tinha uns sessenta e quatro anos, rijos e prosperos, era solteiro, possuia cerca de trezentos contos e fui acompanhado ao cemiterio por onze amigos. onze amigos! verdade e que nao houve cartas nem anuncios. acresce que chovia — peneirava uma chuvinha miuda, triste e constante, tao constante e tao triste, que levou um daqueles fieis da ultima hora a intercalar esta engenhosa ideia no discurso que proferiu a beira de minha cova: — “vos, que o conhecestes, meus senhores, vos podeis dizer comigo que a natureza parece estar chorando a perda irreparavel de um dos mais belos caracteres que tem honrado a humanidade. este ar sombrio, estas gotas do ceu, aquelas nuvens escuras que cobrem o azul como um crepe funereo, tudo isso e a dor crua e ma que lhe roi a natureza as mais intimas entranhas; tudo isso e um sublime louvor ao nosso ilustre finado.” bom e fiel amigo! nao, nao me arrependo das vinte apolices que lhe deixei. e foi assim que cheguei a clausula dos meus dias; foi assim que me encaminhei para o undiscovered country de hamlet, sem as ânsias nem as duvidas do moco principe, mas pausado e tropego como quem se retira tarde do espetaculo. tarde e aborrecido. viramme ir umas nove ou dez pessoas, entre elas tres senhoras, minha irma sabina, casada com o cotrim, a filha, — um lirio do vale, — e... tenham paciencia! daqui a pouco lhes direi quem era a terceira senhora. contentem-se de saber que essa anonima, ainda que nao parenta, padeceu mais do que as parentas. e verdade, padeceu mais. nao digo que se carpisse, nao digo que se deixasse rolar pelo chao, convulsa. nem o meu obito era coisa altamente dramatica... um solteirao que expira aos sessenta e quatro anos, nao parece que reuna em si todos os elementos de uma tragedia. e dado que sim, o que menos convinha a essa anonima era aparenta-lo. de pe, a cabeceira da cama, com os olhos estupidos, a boca entreaberta, a triste senhora mal podia crer na minha extincao.