Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Vigenere – picoCTF

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Vigenere – Guilherme Gonsales de Sá |
| **N° Revisão** | 1 |
| **Data de publicação** | 18/05/2025 |
| **Link** | <https://play.picoctf.org/practice/challenge/316?category=2&difficulty=2&page=1> |

|  |  |  |
| --- | --- | --- |
| **Redação** | Guilherme Gonsales de Sá | Estudante |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 17/05/2025 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Médio |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | Criptografia |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

[Contextualização 3](#_heading=h.gjdgxs)

[Conceitos e variações 3](#_heading=h.30j0zll)

[Desenvolvimento 5](#_heading=h.1fob9te)

[Can you decrypt the message? 5](#_heading=h.3znysh7)

[Conclusão 6](#_heading=h.1t3h5sf)

[Referências 7](#_heading=h.4d34og8)

Scripts 7

**Contextualização**

O ctf ‘Vigenere’, como o nome diz, trata sobre a cifra de criptografia clássica popularizada por Blaise de Vigenère, conhecida como Cifra de Vigenère. Embora seja um conceito simples dentro de criptografia, é interessante explorar os conceitos de tal cifra, assim como variações da mesma, para que possa-se integra-la em outras cifras mais complexas como uma camada adicional de proteção.

**Conceitos e variações**

Para compreender a cifra de Vigenère, é necessário compreender primeiro a cifra de César.

A cifra de César é um tipo de criptografia reversível, baseada em substituição simples de um caractere por outro. Por exemplo, consideremos um alfabeto que contenha [a, b, c, ... x, y, z]. Agora, consideremos a mensagem não encriptada ‘*ola leitor’*. Aplicando a cifra de césar com um shift 0 (ou seja, deslocamento de 0 posições), tem-se: a=a, b=b, c=c,...,z=z.

Dessa forma, observa-se que nossa mensagem continua idêntica. Aplicando um shift 1, tem-se: a=b, b=c, c=d, ..., z=a. Dessa forma, a mensagem encriptada via cifra de césar com shift 1 é: *‘pmb mfjups’*.

Considerando shift 2, teríamos: a=c, b=d, c=e, ..., z=b.

Considerando shift 3, teríamos: a=d, b=e, c=f, ... , z=c.

Tal padrão se mantém até shift 25, onde a=z, ..., z=y. No entanto, ao saber qual foi o deslocamento utilizado para apenas uma letra, é possível descriptografar toda a mensagem encriptada com um simples programa, ou até mesmo de forma manual.

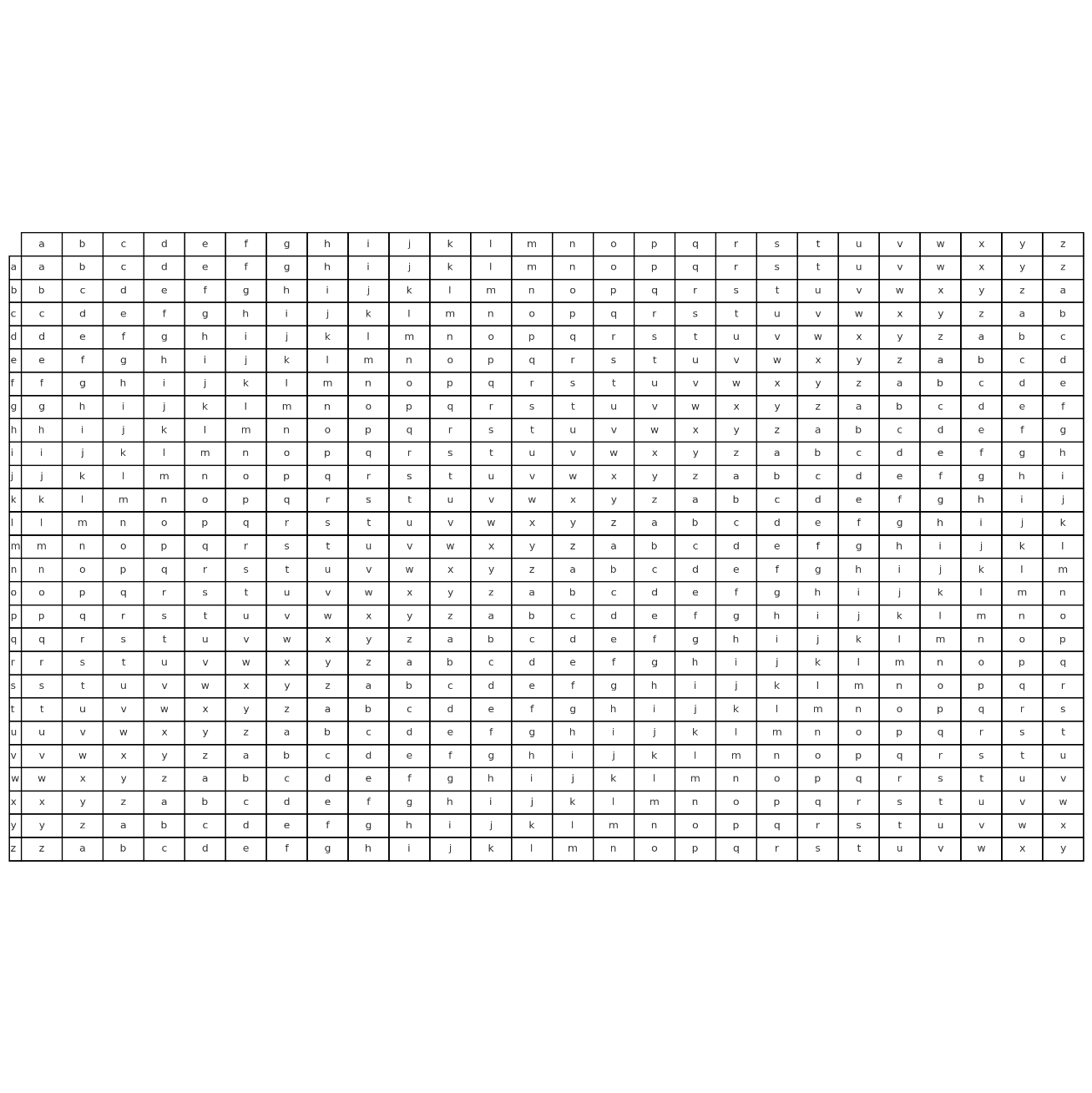
De forma genérica, pode-se descrever o comportamento da cifra de césar como:

Onde: C caractere cifrado, P é o caractere original e K é o shift/rot/deslocamento.

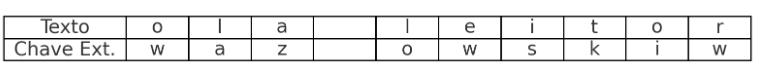
Para decriptação de tal cifra, pode-se apenas substituir K por -K, tal como:

Existe um caso específico da cifra de césar, conhecido como *rot13.* O *rot13* é uma cifra extremamente difundida, e ela é o caso em que o shift da cifra de césar é 13. Esse é um caso interessante, pois ao considerar o alfabeto [a, b, c, ..., z], o shift 13 é o inverso de si próprio, ou seja, shift 13 = shift -13. Tal cifra pode ser usada para verificações/encriptações rápidas de mensagens.

Tratando-se da cifra de Vigenère, pode-se entender a mesma como uma concatenação de várias cifras de César de acordo com uma chave. Para a encriptação, considerando o mesmo alfabeto utilizado anteriormente, necessita-se da *Tabula Recta* (ou *grade de Vigenère*).Ela é uma tabela de dimensões NxN, onde N é o tamanho do alfabeto utilizado (no caso, 26), e os shifts serão dados pelo número da linha, iniciando-se no índice 0. Isso significa que, caso nosso caractere da chave seja ‘a’, o caractere de mesma posição na mensagem a ser encriptada será ele próprio, pois terá shift 0. Caso o caractere da chave seja ‘b’, o caractere de mesma posição na mensagem será encriptado com shift 1, e assim sucessivamente.



Sendo assim , encriptemos a mensagem ‘ola leitor’, utilizando a cifra de Vigenère, com a chave ‘wazowski’. A chave será utilizada de forma circular, ou seja, se a chave acabar antes de parear com o tamanho da mensagem original, ela começa a se repetir. Desconsiderando o espaço, a mensagem ‘ola leitor’, lendo-se ‘olaleitor’, tem 9 caracteres. A chave ‘wazowski’, por sua vez, tem 8 caracteres, e ficará ‘wazowskiw’ pareando com o tamanho da mensagem.



Dessa forma, utilizando da *Tabula Recta*, a mensagem encriptada é: *klz zaadwn*.

De forma genérica, considerando o alfabeto dado *a priori,* pode-se compreender a cifra de Vigenère como:

Onde: Ci é o caractere de posição i cifrado, Pi é caractere de índice i a ser cifrado e Ki representa o shift a ser utilizado de acordo com o caractere de índice i na chave.

Para decriptação, pode-se compreender o algoritmo como:

Para os casos acima, tanto para a cifra de césar como para a cifra de vigenère, considerou-se o alfabeto [a, b, c, ..., z]. No entanto, é possível alterar o alfabeto utilizado para tornar tais cifras mais fortes. Pode-se considerar, por exemplo, um alfabeto alfanumérico [0, 1, 2, ..., a, b, c, ..., z], ou um alfabeto alfanumérico com letras maiúsculas e minúsculas [0, 1, 2, ..., A, B, C, ..., Z, a, b, c, ..., z], dentre outras alfabetos (incluindo caracteres especiais, incluindo toda a tabela ASCII, alfabetos customizados, etc...). Sendo assim, pode-se generalizar as cifras para um alfabeto de n elementos. Dessa forma, tem-se a cifra de césar, genericamente, como:

Onde n é o número de elementos no alfabeto. Para decriptação, tem-se:

Com a cifra de Vigenère, tem-se para encriptação:

Para a decriptação, tem-se:

No caso de *rot13*, pode-se considerar equivalente qualquer cifra *rot(n/2)*, dado que n seja um número par.

**Desenvolvimento**

**Can you decryptt this message?**

Ao iniciar o exercício, uma mensagem cifrada nos é fornecida.



Pelo nome do ctf, supõe-se que a cifra utilizada é a cifra de Vigenère. Sendo assim, podemos utilizar um site para fazer a decriptação da mensagem ou criar um script. Utilizando o site <https://www.dcode.fr/vigenere-cipher>, coloquemos a mensagem encriptada e a chave fornecida: *CYLAB*.



Ao acionar ‘decrypt’, recebemos a resposta:

****

Concluindo, dessa forma, o exercício proposto.

**Conclusão**

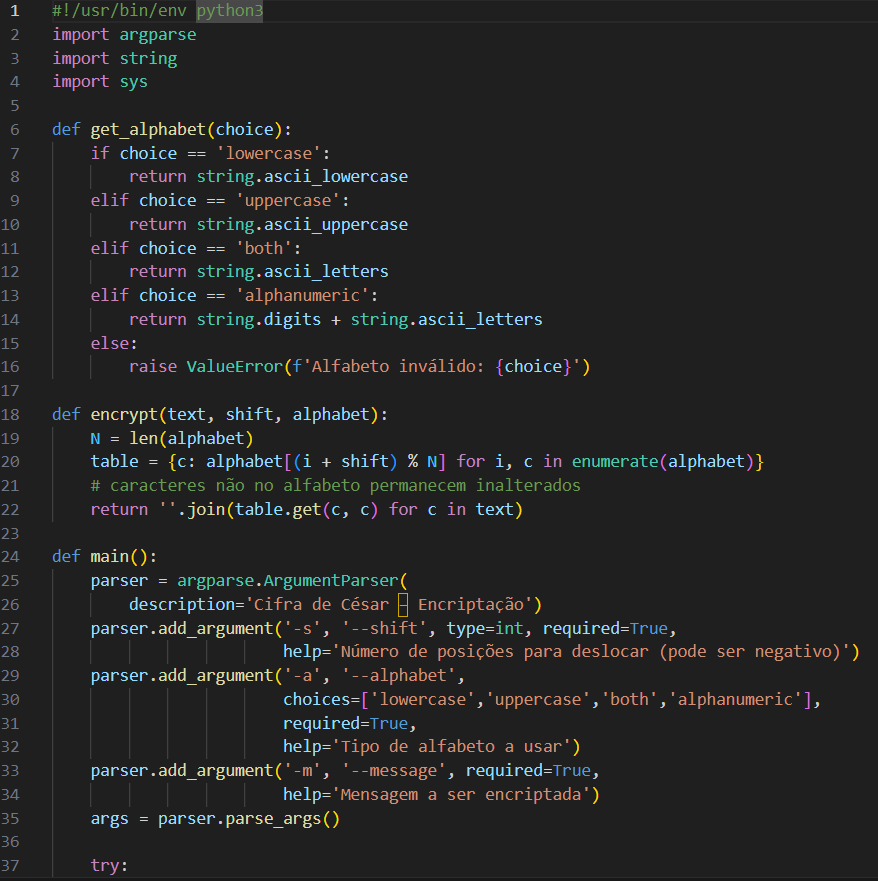
Apesar da prática ser simples, o CTF abrange alguns conceitos basais de criptografia clássica, que podem ser usados juntamente com métodos mais modernos de criptografia para uma encriptação mais robusta. Sendo assim, conclui-se que é, de fato, um bom CTF para iniciantes que pretendem se aprofundar na área de criptografia, embora a prática pudesse ser um pouco mais complexa combinando várias camadas de cifras e/ou utilizando a cifra de Vigenère com outros métodos de encriptação mais modernos.

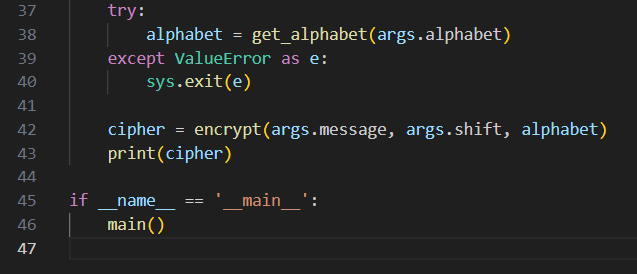
**Referências**

<https://pt.wikipedia.org/wiki/Cifra_de_Vigen%C3%A8re>

**Scripts**

1 – encriptação por cifra de César



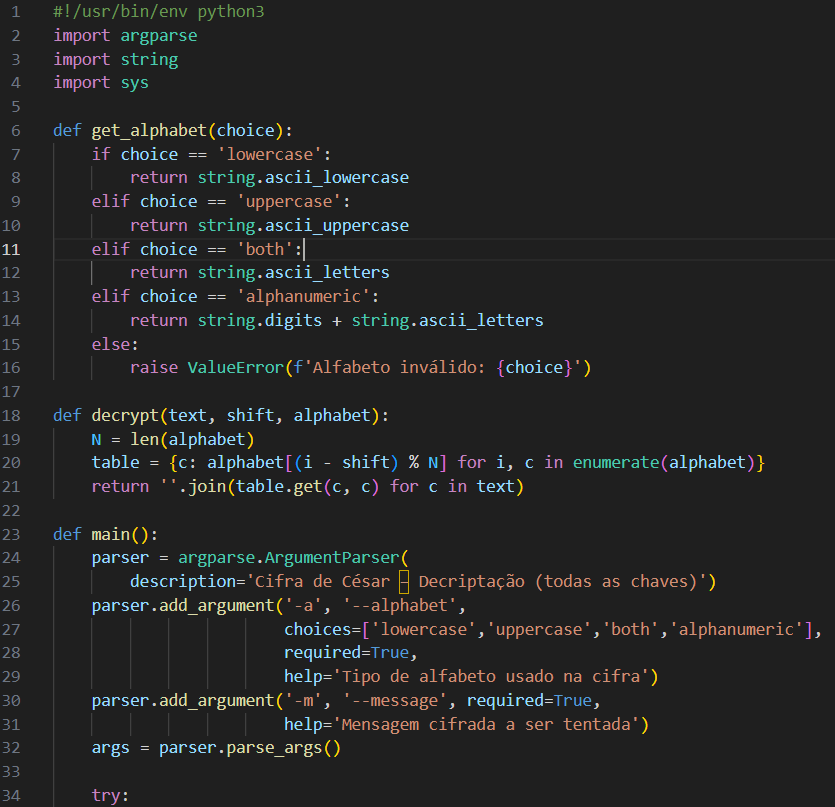


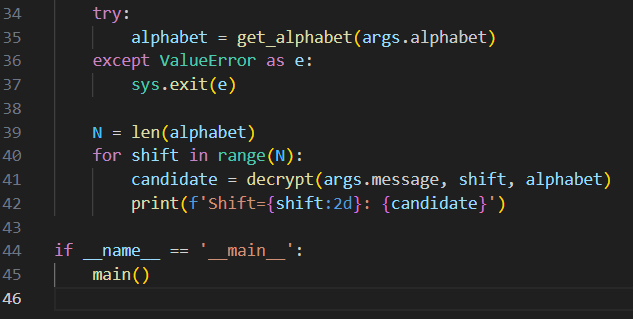
Exemplo de chamada:



Onde -a indica o alfabeto, -s indica o número de shifts e -m indica a mensagem a ser encriptada

2 – Decriptação de cifra de César





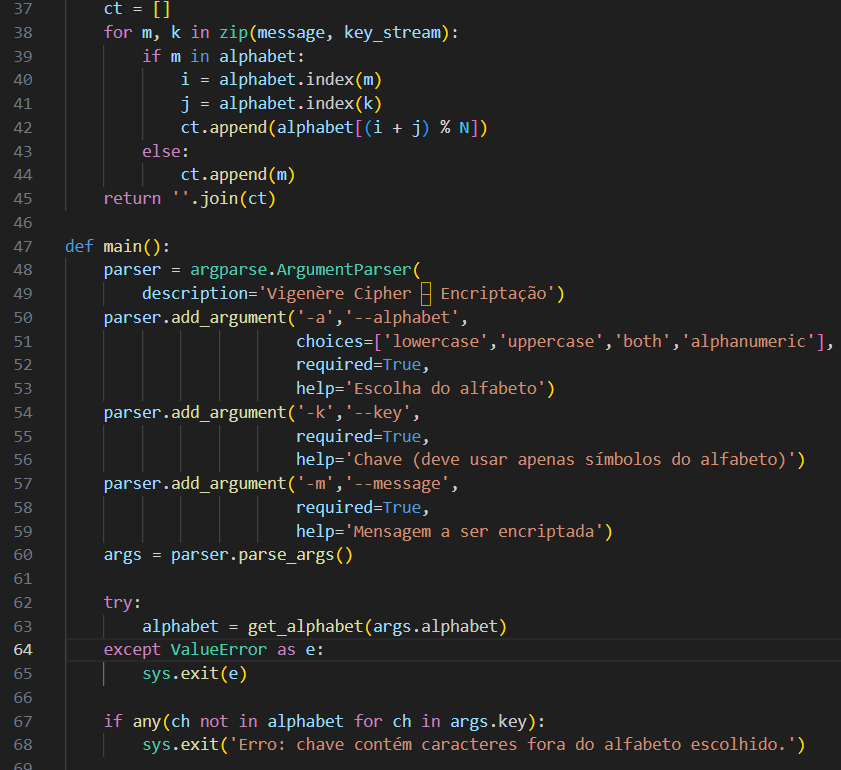
Exemplo de chamada:

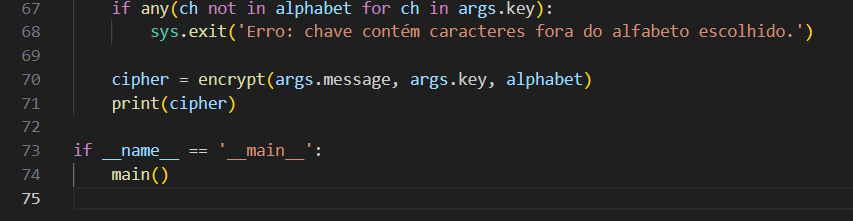


Onde -a indica o alfabeto e -m indica a mensagem encriptada

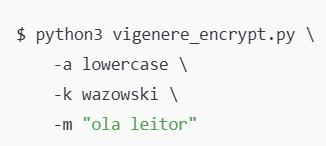
3 – Encriptação por cifra de Vigenère





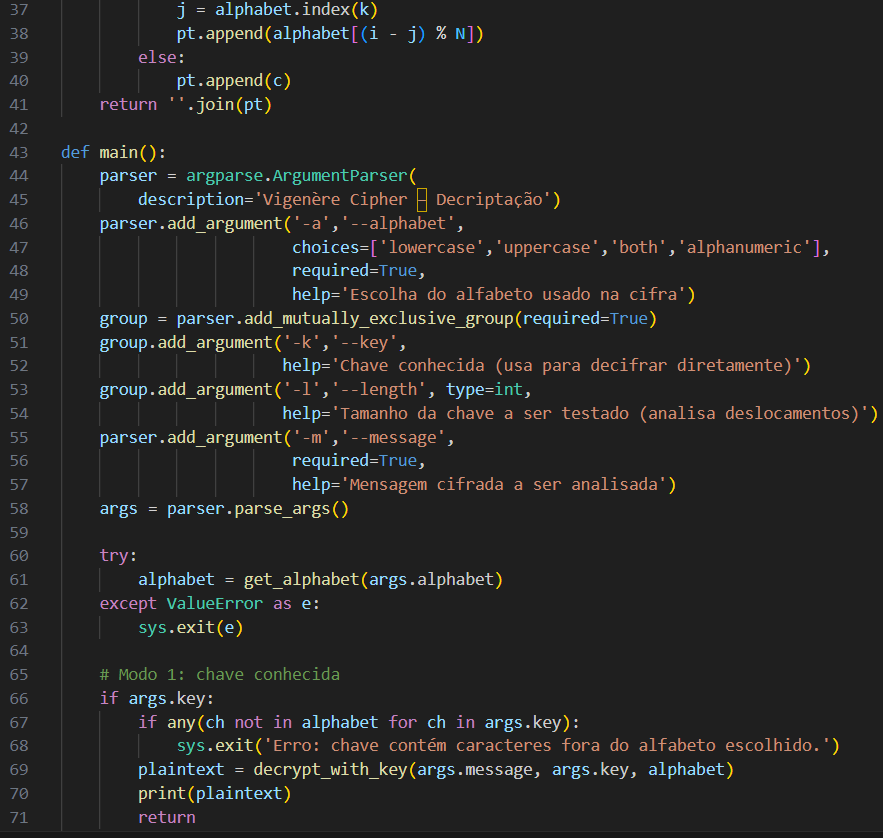
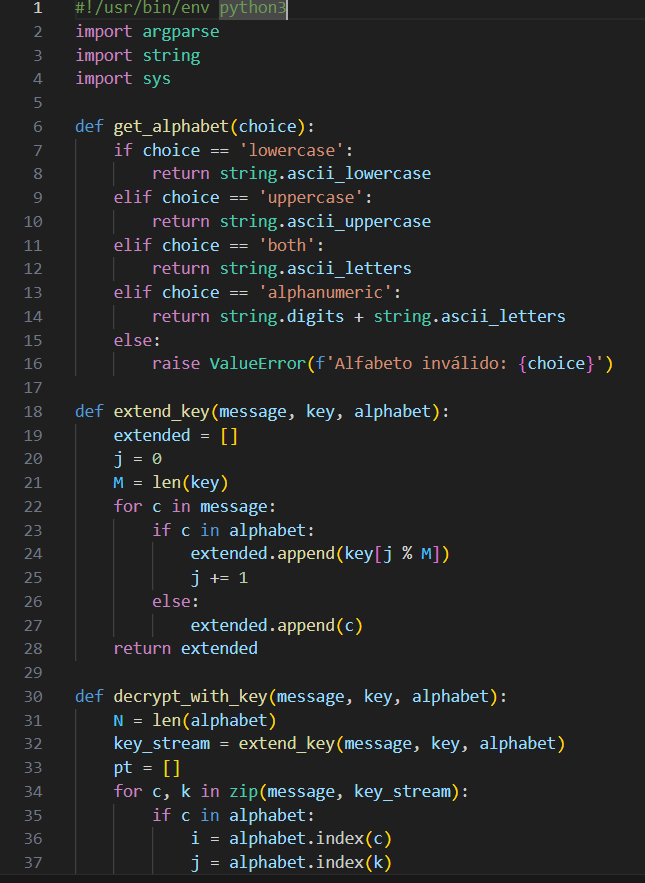


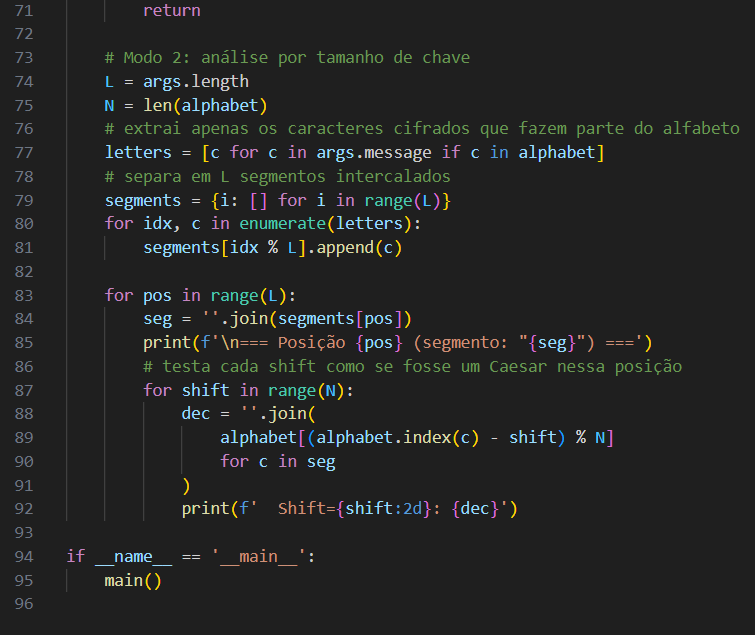
Exemplo de chamada:



Onde -a é o alfabeto, -k é a chave utilizada e -m é a mensagem a ser encriptada

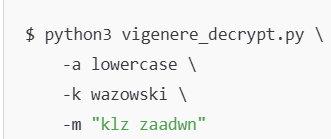
4 – Decriptação de cifra de Vigenère





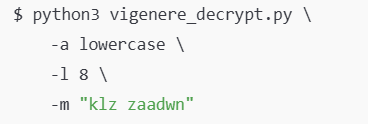
Exemplo de chamada:

Modo 1: chave conhecida



Onde -a é o alfabeto, -k é a chave conhecida e -m é a mensagem encriptada

Modo 2: chave desconhecida



Onde -a é o alfabeto, -l indica o tamanho de chave a ser testado e -m indica a mensagem encriptada.