Alunos: Lorenzo Martins Lazzarin – 200022610;

Ayrton Jorge Nassif - 200048805

O código feito é uma implementação da cifra de Vigenère para criptografia e descriptografia de mensagens de texto. Além disso, o código apresenta uma função para realizar um ataque de recuperação de senha, que utiliza duas mensagens cifradas para tentar determinar a chave utilizada na criptografia.

A cifra de Vigenère é um método de criptografia que utiliza uma tabela de substituição para cifrar mensagens de texto. A ideia básica é utilizar uma palavra-chave para cifrar cada letra da mensagem, de modo que a letra cifrada seja determinada pela linha e coluna correspondente à letra da palavra-chave e da mensagem.

O código começa definindo constantes que serão utilizadas ao longo do código. Constantes essas como o alfabeto, ou a frequência das letras, tanto português, como inglês. São definidos duas constantes, “msg_teste1”, que corresponde ao desafio 1, e a “msg_teste2”, que corresponde ao desafio 2, que recebem os textos a serem atacados, e recuperadas as chaves.

Em seguida, são definidas as funções cripto(), e descrypto(), que recebem como parâmetros uma mensagem de texto e uma palavra-chave, e retornam a mensagem cifrada e decifrada, respectivamente, conforme diz a cifra de Vigenerè. Em seguida, é dado a função keyStream(), que é responsável por concatenar a chave até chegar ao tamanho da mensagem, já que a regra pede que seja do mesmo tamanho ou maior.

Em seguida, temos a função descryptoMsgSemChave(), que é responsável por pegar o texto cifrado, retirar os caracteres especiais, tirar os espaços em brancos, deixar todos os caracteres em minúsculos, e atribuir esse novo texto a outras funções, como por exemplo tamanhoChave().

Como o nome já diz, a função tamanhoChave() é responsável por obter o tamanho da chave. Ele obtém o tamanho por meio de um dicionário, que contém o resultado do MDC como chave e a ocorrência de cada letra como valor.

Logo acima da função “tamanhoChave()”, temos a função “frequenciaOcorrencias()”, que recebe a mensagem sem caracteres especiais, e é responsável por mover o texto para a esquerda, como diz a cifra de vigenerè. Com isso, ele irá analisar as ocorrências com que as letras são iguais, e gravar essas ocorrências em um dicionário, que possui o deslocamento como chave, e a ocorrência como valor. Ele só irá armazenar no dicionário, caso a letra da mensagem, seja igual a essa mesma letra, porém deslocada para a esquerda.

Logo após, temos a função “descobrindoPorcentagemLetra()”, que recebe a mensagem sem caracteres especiais, e o tamanho da chave, que já foi dado na função “tamanhoChave()”. A função “descobrindoPorcentagemLetra()” irá criar uma lista de listas, que irá receber letras de cada posição delimitada pela chave. Ou seja, se a chave tem tamanho = 5, teremos 5 subistas. Após a função criar essas listas, ele irá analisar cada letra dessas sublistas, descobrir sua porcentagem dentro de cada sublista, salvando assim esse resultado em uma lista com a mesma estrutura, porém, ordenada alfabeticamente.

Seguindo, temos a função “descobrindoLetra()”, que irá receber a porcentagem das letras, dada na função anterior, junto com o tamanho da chave. Essa função irá analisar a porcentagem de cada letra salva dentro da lista, e multiplicar cada letra do alfabeto de porcentagens, definido no início do código, e que foi passado pelo professor. O resultado das somas dessa multiplicação será guardado dentro de outra lista, ordenadas pelo deslocamento do das porcentagens que encontramos. Com isso, tem-se o deslocamento com a maior soma de porcentagem, de acordo com o alfabeto passado pelo professor. Com isso, ele procura a letra do alfabeto que corresponde ao deslocamento.

Tendo a possível chave, temos a função “descriptoDesafio()”, que irá receber a mensagem codificada, e com a chave descoberta, irá descriptografar a mensagem, percorrendo o texto e movendo conforme a chave, pulando os caracteres especiais, e os espaços.

Por fim, temos as chamadas de função, que são chamadas de acordo com o usuário. Vários “input()” irão guiar o usuário para qual opção ele quer, seja criptografar uma mensagem, descriptografar passando uma chave, ou atacar uma mensagem criptografada, recuperando a chave original, e usando-a para obter e mensagem original.