Trabalho 2
Cifra de Vigenère

Introdução:

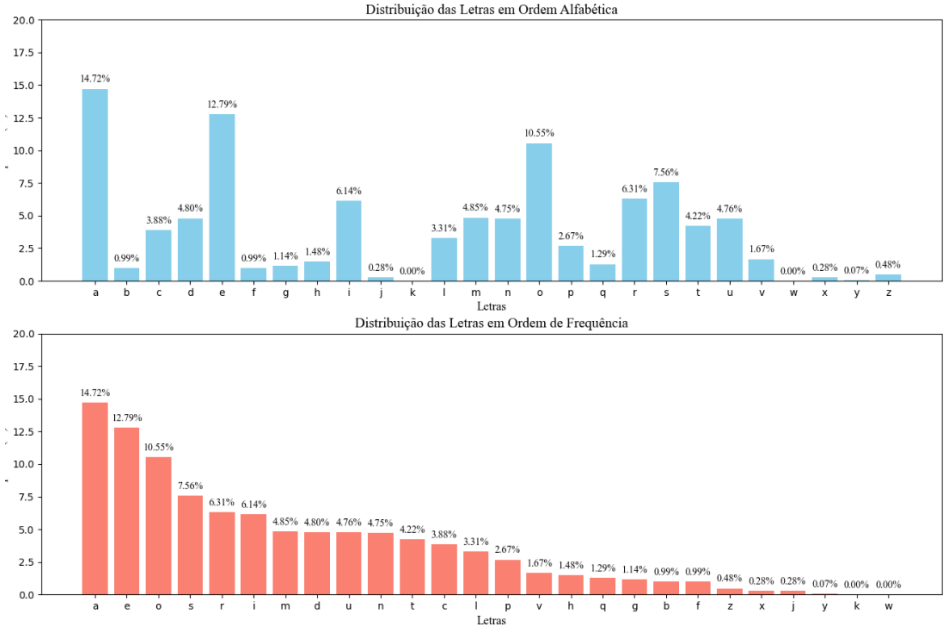
A criptografia é uma técnica milenar usada para proteger informações e assegurar uma comunicação segura entre indivíduos e instituições. Dentre os diversos métodos de criptografia, a cifra de Vigenère se destaca como uma das mais conhecidas. Ela utiliza uma chave para realizar um deslocamento das letras no alfabeto, codificando o texto original. Diferente da cifra de César, que usa um único deslocamento para todo o texto, a cifra de Vigenère é polialfabética, pois aplica deslocamentos variados ao longo do texto, tornando a criptografia mais resistente a ataques de frequência.

O objetivo deste trabalho é aplicar os conhecimentos sobre a cifra de Vigenère para decifrar um texto codificado. Ao realizar essa tarefa, será possível entender melhor os conceitos por trás dessa técnica e as estratégias usadas para superar a criptografia, que inicialmente parece segura.

Enunciado:

Vocês receberão um texto codificado utilizando a cifra de Vigenère. A chave utilizada para a cifra é uma palavra-chave.

- **Tarefa**:
  - A tarefa consiste em aplicar análise de frequência para atacar o texto cifrado. No entanto, como discutido em aula, a cifra de Vigenère é resistente a esse tipo de ataque direto.
  - Assim, o primeiro passo é determinar o tamanho da palavra-chave usada para cifrar o texto. Para determinar o tamanho da chave, duas abordagens são sugeridas: o Teste de Kasiski e o Índice de Coincidência. Neste caso, o valor-alvo do índice de coincidência é $I_c = 0{,}07797$.
  - Após determinar o tamanho da palavra-chave, aplique a análise de frequência nos segmentos do texto que foram codificados com o mesmo deslocamento. Para isso, utilize a distribuição de frequência fornecida no Material de Apoio.



- Desenvolver um relatório no formato de **artigo IEEE**, em colunas duplas, com no máximo duas páginas. A estrutura do relatório deve conter:
  - **Introdução**: Apresente o problema de criptografia e os objetivos do trabalho.
  - **Desenvolvimento**: Explique o processo de determinação do tamanho da chave e como foi realizada a análise de frequência.
  - **Conclusão**: Indique o tamanho da chave utilizada, a palavra-chave encontrada, o título da obra encriptada e os principais desafios enfrentados. Evite incluir trechos de código no relatório, exceto quando absolutamente necessário.
- No Material de Apoio, vocês encontram sete textos cifrados. Cada um é dedicado a um aluno específico. Portanto, para realizar o trabalho, atenham-se ao seu texto.
  - O nome do arquivo indica a quem pertence o texto. O nome do arquivo contém os 5 últimos dígitos da matrícula do aluno. Por exemplo, o arquivo `12345.txt` pertence ao aluno com a matrícula: `9876`**`1234-5.`**

Entregáveis e Avaliação:

- O trabalho deve ser realizado **individualmente**.
- Deve ser entregue um arquivo ".zip" contendo:
  - (*5 pontos*) Código utilizado para atacar o texto cifrado. O código deve ser na linguagem de programação preferencial do aluno. Esse código deve ser **devidamente comentado** e deve possuir um **README** informando os passos para compilação/execução.
  - (*5 pontos*) Um arquivo **.pdf** contendo o relatório em formato de artigo. Utilize o formato disponível em: *https://www.ieee.org/conferences/publishing/templates.html*
- **Deadline: 14/05/2024 até às 23:59 – no Moodle**