Relatório - Trabalho 1

Links úteis:

https://www.youtube.com/watch?v=SkJcmCaHqS0

https://www.youtube.com/watch?v=P4z3jAOzT9I

Alunos

- Nataly Lacerda de Oliveira - 190093838
- Pedro Henrique dos Santos - 200026127

Cifração

A cifra de Vigenère é um método de criptografia que utiliza uma chave para cifrar e decifrar mensagens. É uma cifra de substituição polialfabética, o que significa que cada letra da mensagem original é cifrada usando um alfabeto diferente com base na chave. Aqui está uma explicação simples de como fazer a cifra de Vigenère:

Passo 1: Escolher uma Mensagem e uma Chave

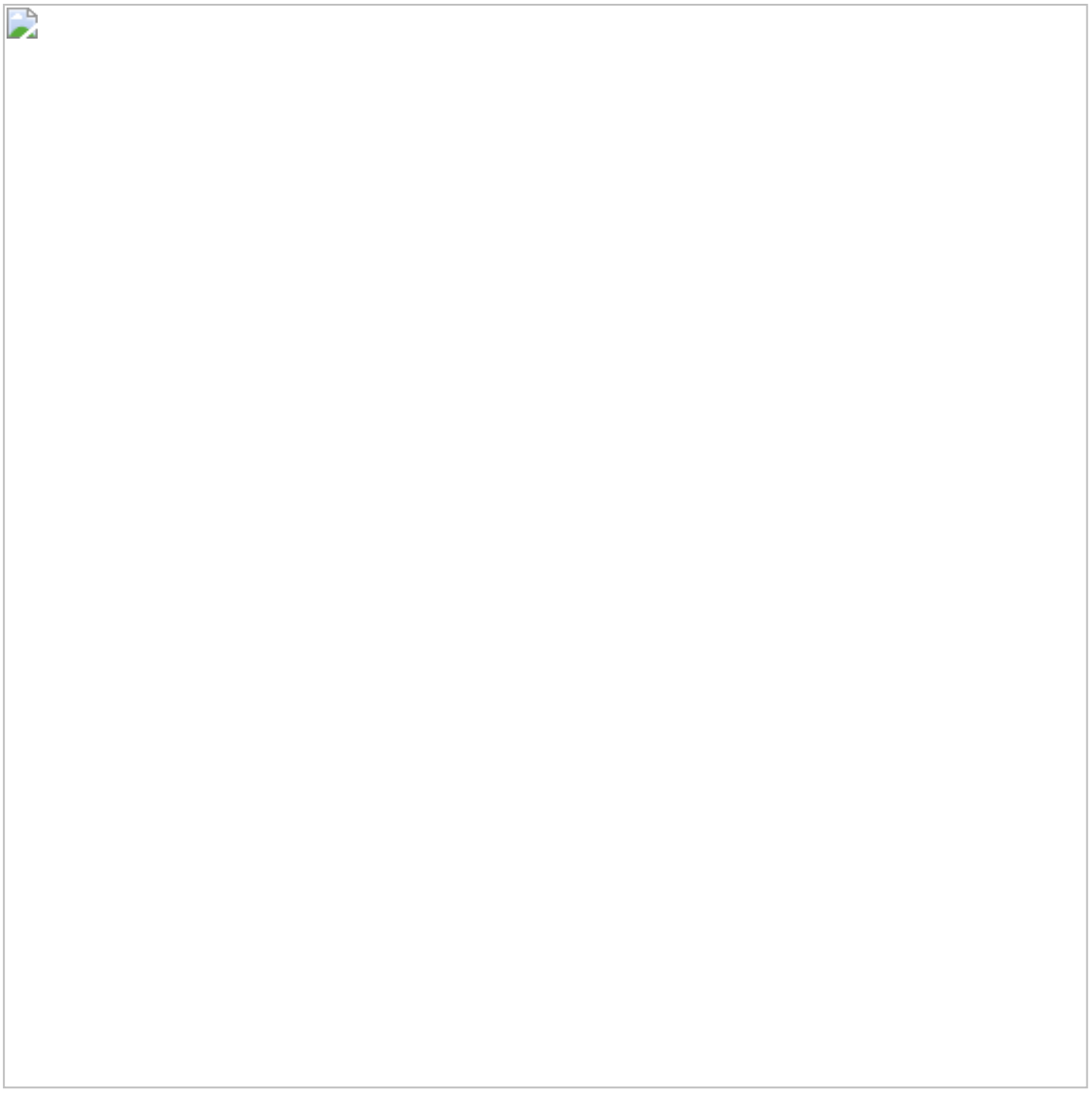
- Primeiro, você precisa escolher a mensagem que deseja cifrar e uma chave que será usada para criptografar a mensagem.
- A mensagem pode ser qualquer texto que você queira proteger.
- A chave é uma palavra ou frase curta que será usada para determinar como cada letra da mensagem será cifrada. Por exemplo, a chave pode ser "CIFRA" ou "SEGURANCA".

Passo 2: Repetir a Chave

- Para usar a chave na cifra de Vigenère, você deve repeti-la para que tenha o mesmo comprimento que a mensagem.
- Se a mensagem for "HELLO" e a chave for "CIFRA", você repetirá a chave até que ela tenha o mesmo comprimento da mensagem: "CIFRACIFRACIFRACIFRA...". Aqui *Hello* e *Cifra* tem o mesmo comprimento, então nesse seria apenas “CIFRA”.

Passo 3: Cifrar a Mensagem

- Agora você está pronto para cifrar a mensagem. Vamos usar um exemplo para ilustrar como isso funciona:
  - Mensagem: HELLO
  - Chave: CIFRA
- Converta cada letra da mensagem e da chave em números, usando uma tabela de correspondência. Por exemplo, 'A' pode ser 0, 'B' pode ser 1, 'C' pode ser 2 e assim por diante.
- Some o valor numérico da letra da mensagem ao valor numérico da letra correspondente da chave e faça o módulo de 26 no resultado. No exemplo:
  - (H (7) + C (2)) % 26 = J (9)
  - (E (4) + I (8)) % 26 = M (12)
  - (L (11) + F (3)) % 26 = O (14)
  - (L (11) + R (17)) % 26 = C (2)
  - (O (14) + A (0)) % 26 = O (14)
- Portanto, a mensagem cifrada é "JMOCO"



Decifração

O processo de decifrar é exatamente o mesmo, porém agora vamos subtrair o valor numérico da letra da cifra com a da chave. Então ficamos com:

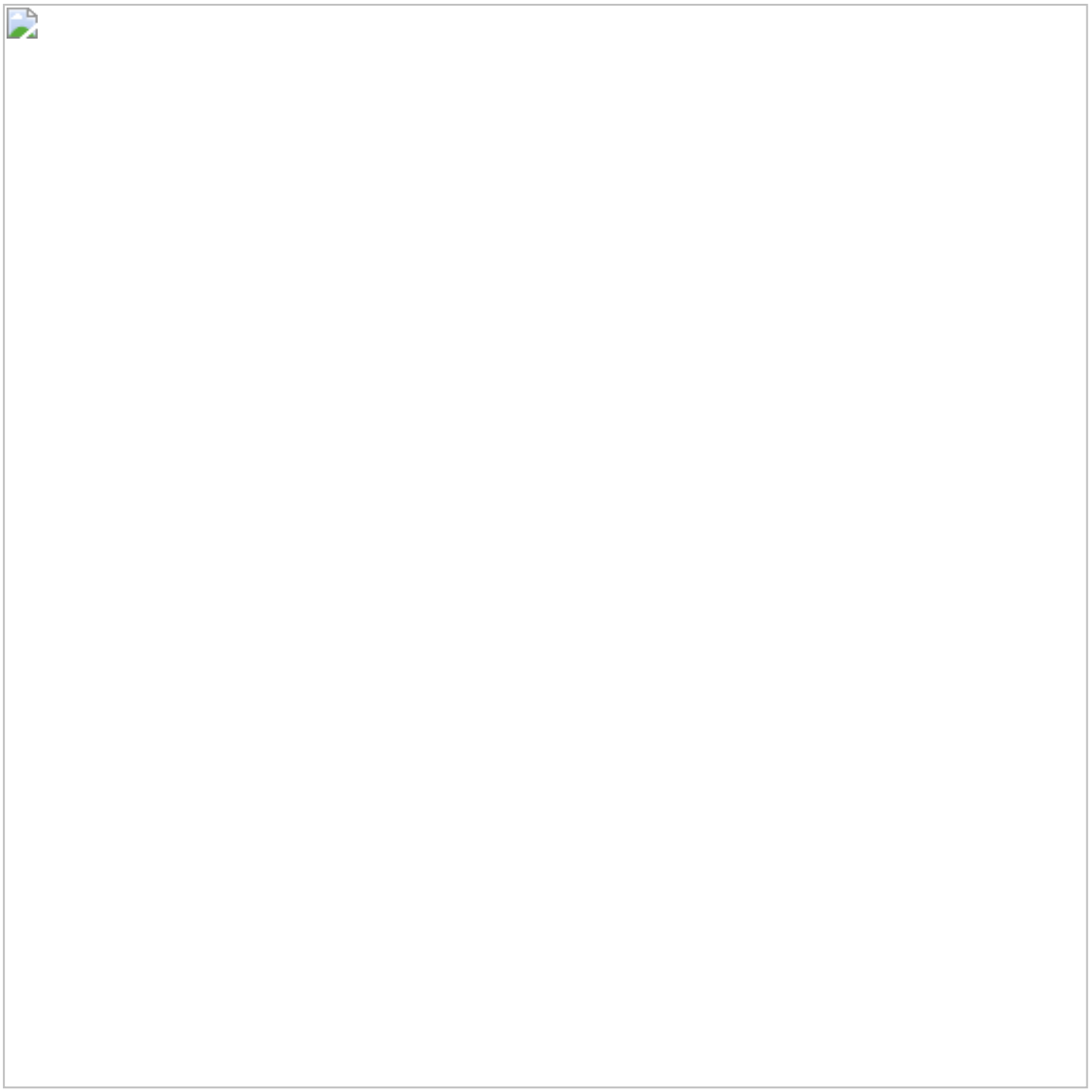
- Cifra: JMOCO
- Chave: CIFRA

Fazendo as operações:

- (J (9) - C (2)) % 26 = H (7)
- (M (12) - I (8)) % 26 = E (4)
- (O (14) - F (3)) % 26 = L (11)

- (C (2) - R (17)) % 26 = L (11)
- (O (14) - A (0)) % 26 = O (14)

Assim recuperamos a mensagem original: HELLO



Ataque

Para quebrar a cifra de Vigenère, podemos seguir esses passos:

1. **Descubra o Tamanho da Chave**: Comece determinando o tamanho da chave. Você pode usar a técnica de análise de frequência, tentando diferentes tamanhos até encontrar padrões nas frequências das letras.
2. **Divida o Texto Cifrado em Grupos**: Divida o texto cifrado em grupos de letras correspondentes ao tamanho da chave que você encontrou.

3. **Analise a Frequência em Cada Grupo**: Em cada grupo, faça uma análise de frequência, identificando a letra mais comum. Suponha que essa letra corresponda à letra mais comum na língua do texto original (por exemplo, 'E' em inglês ou 'A' em português).
4. **Encontre a Chave**: Use a letra mais comum em cada grupo e a letra de referência (por exemplo, 'E' ou 'A') para determinar a letra da chave usada naquele grupo. Repita esse processo para todos os grupos.
5. **Monte a Chave Completa**: Junte as letras da chave de cada grupo para formar a chave completa.
6. **Decifre o Texto**: Use a chave completa para decifrar o texto cifrado usando a cifra de Vigenère inversa.

Seguindo esses passos, você poderá quebrar a cifra de Vigenère e revelar a mensagem original. Lembre-se de que a chave é fundamental para esse processo, e a qualidade da análise de frequência desempenha um papel crucial na determinação da chave correta.

Conclusão

Conseguimos entender bem como funciona a cifra e a implementamos corretamente. Seguimos o vídeo de orientação para a implementação da quebra da cifra, mas não tivemos sucesso. Não entendemos como exatamente poderiamos fazer para dar match nos valores da cifra com a do alfabeto. Então apesar de ficar um pouco perdidos nessa parte, deu pra passear bastante nos conceitos da cifra, e acredito que com um pouquinho mais de tempo podemos fazer uma implementação completa.