

## Relatório

### → Cifrador de César

- Executar:
  - ./output cesar -c -k 'chave' entrada.txt saida.txt (cifrador)
  - ./output cesar -d -k 'chave' entrada.txt saida.txt (decifrador)

### → Análise de frequências

- Executar:
  - ./output analFreq entrada.txt

### → Cifrador de Vernam

- Executar:
  - ./output vernam -c chave.dat entrada.txt saida.txt (cifrador)
  - ./output vernam -d chave.dat entrada.txt saida.txt (decifrador)

#### a. Faça a criptanálise da mensagem cifrada com o cifrador de César e mostre a chave usada. Qual é o texto criptografado?

- Após a realização da criptanálise, utilizando a análise de frequência, a chave encontrada foi 17.
  - O texto criptografado é o seguinte:
    - Pouco conhecimento faz com que as pessoas se sintam orgulhosas. Muito conhecimento, que se sintam humildes. Eh assim que as espigas sem graos erguem desdenhosamente a cabeça para o ceu, enquanto as cheias as baixam para a terra, sua mae.
- Leonardo Da Vinci.

#### b. O algoritmo de Vernam é vulnerável à análise de frequências? Justifique.

- Não, como o algoritmo de Vernam não se utiliza do deslocamento de caracteres, como a cifra de César, a análise de frequência não tem efeito algum nele. Além disso o algoritmo de Vernam não utiliza apenas um número como chave, e sim uma quantidade de números equivalente ao tamanho do texto cifrado, e visto que a análise de frequência só consegue encontrar apenas uma chave o algoritmo de Vernam, de fato, não é vulnerável a análise de frequência.
- i. Como será feita a geração da chave?
- Para a geração da chave foi utilizado o próprio cifrador de César que já havia sido feito. Cifre-se o texto original com alguma chave e utiliza-se o texto cifrado com César como chave para o texto cifrado com Vernam. Desta forma garantimos que a chave sempre irá cumprir com o requisito de ser do mesmo tamanho do texto original.
- ii. É possível usar o algoritmo de Vernam para cifrar uma base de dados? Justifique.
- Dificilmente. Como uma base de dados normalmente contém muitas informações, e para que fosse possível cifrá-la com Vernam seria necessário uma chave do mesmo tamanho de todas as informações

da base de dados, isso tornaria inviável a utilização deste algoritmo na maioria dos casos.

**c. O algoritmo RC4 é vulnerável à análise de frequências? Justifique.**

- Não. O algoritmo RC4 faz uma operação de XOR byte a byte com os bytes de entrada e os bytes da chave, sendo assim ele não se preocupa com os caracteres do texto e sim com seus bytes. Em vista disso uma análise de frequência dos caracteres não faz sentido visto que estes não tem relação com os caracteres originais.