# Primeiro Trabalho Prático (CI1017)

Frank Wolff Hannemann

29 de setembro de 2025

## 1 Link do Projeto

O código do projeto está disponível no GitHub: https://github.com/frnkwh/criptografia

## 2 Introdução

Este relatório tem como objetivo explicar a cifra de substituição e a cifra de transposição que foram usadas, bem como sua implementação e uso na cifra FCC (*Frank's Crazy Cipher*). O trabalho foi feito em Python e aceita qualquer caractere UTF-8.

## 3 Cifra de Substituição

A cifra de substituição escolhida foi a cifra de Vigenère com autochave. Ao invés de utilizar uma *tabula recta* para fazer a cifra/decifra, foi utilizada a soma dos *unicode points* (utilizando a função "ord()"do Python) com a operação de módulo, para garantir que a soma dos *unicode points* seja um caractere válido.

A cifra começa fazendo a soma dos pontos do primeiro caractere do texto claro com o primeiro da chave, depois faz do segundo caractere do texto claro com o segundo da chave, e assim por diante. Quando acabarem os caracteres da chave, a função usa os caracteres anteriores do texto claro como chave. Por exemplo, se a chave tiver comprimento 3, o quarto caractere do texto é cifrado usando o primeiro caractere do texto como chave, o quinto usando o segundo, assim por diante.

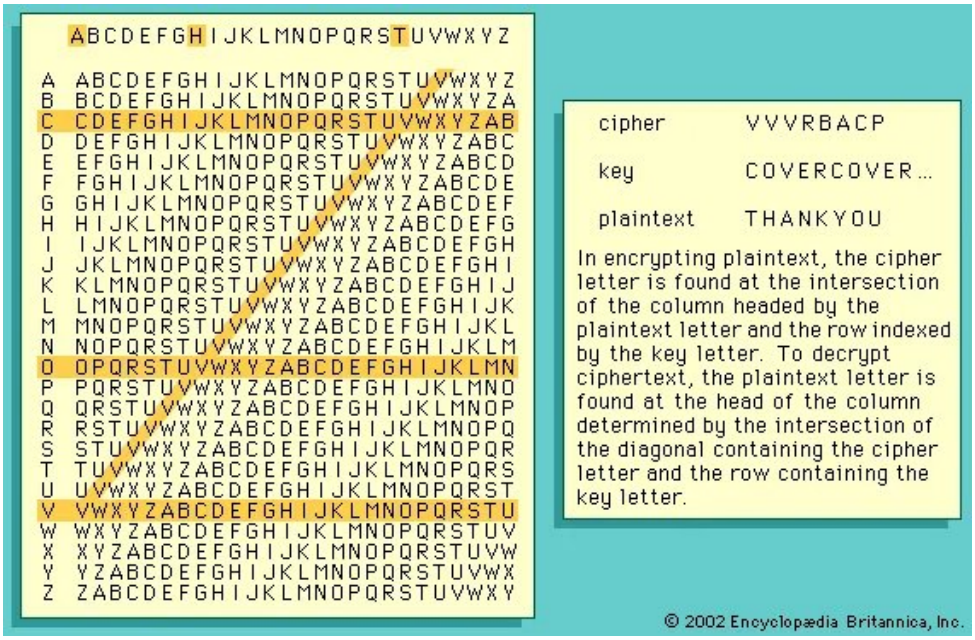



Figura 1: Tabula Recta da cifra de Vigenère

# 4 Cifra de Tranposição

A cifra de transposição escolhida foi a cifra de transposição colunar dupla. Ela consiste em colocar o texto em uma matriz com $n$ colunas, sendo $n$ o tamanho da palavra-chave. Após isso, as colunas são reordenadas de acordo com a ordem alfabética da chave. Depois, a matriz é transposta e o texto é rearranjado na matriz para manter o número de colunas. As colunas são então reordenadas de acordo com a segunda palavra-chave e por fim a matriz é transposta novamente.

# 5 Cifra FCC

A cifra proposta (FCC) é a simples junção da cifra de Vigenère com autochave seguida pela transposição dupla colunar. Esse processo é feito apenas uma vez.

O programa pede duas chaves como entrada. Só a primeira é usada na cifra da substituição e a cifra de transposição usa as duas chaves. Se as duas chaves não tiverem o mesmo tamanho, o programa completa a menor chave com a letra “a” no final até as duas ficarem com o mesmo tamanho.

| J | A | N | E | A | U | S | T | E | N |
|---|---|---|---|---|---|---|---|---|---|
| 5 | 1 | 6 | 3 | 2 | 10 | 8 | 9 | 4 | 7 |
| T | R | A | N | S | P | O | S | I | T |
| I | O | N | C | I | P | H | E | R | S |
| S | C | R | A | M | B | L | E | L | E |
| T | T | E | R | S | L | I | K | E | P |
| U | Z | Z | L | E | P | I | E | C | E |
| S | T | O | C | R | E | A | T | E | A |
| N | I | N | D | E | C | I | P | H | E |
| R | A | B | L | E | A | R | R | A | N |
| G | E | M | E | N | T | | | | |

(a) Primeiro passo: O texto claro é escrito na primeira matriz. (a chave é JANEAUSTEN).

| A | A | E | E | J | N | N | S | T | U |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| R | S | N | I | T | A | T | O | S | P |
| O | I | C | R | I | N | S | H | E | P |
| C | M | A | L | S | R | E | L | E | B |
| T | S | R | E | T | E | P | I | K | L |
| Z | E | L | C | U | Z | E | I | E | P |
| T | R | C | E | S | O | A | A | T | E |
| I | E | D | H | N | N | E | I | P | C |
| A | E | L | A | R | B | N | R | R | A |
| E | N | E | | G | M | | | | T |

(b) As colunas são reordenadas em ordem alfabética de acordo com a chave.

| A | E | R | O | P | L | A | N | E | S |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 3 | 9 | 7 | 8 | 5 | 2 | 6 | 4 | 10 |
| R | O | C | T | Z | T | I | A | E | S |
| I | M | S | E | R | E | E | N | N | C |
| A | R | L | C | D | L | E | I | R | L |
| E | C | E | H | A | T | I | S | T | U |
| S | N | R | G | A | N | R | E | Z | O |
| N | B | M | T | S | E | P | E | A | E |
| N | O | H | L | I | I | A | I | R | S |
| E | E | K | E | T | P | R | P | P | B |
| L | P | E | C | A | T | | | | |

(c) Segundo Passo: As colunas do primeiro passo são colocadas na segunda matriz (que possui a chave AEROPLANES).

| A | A | E | E | L | N | O | P | R | S |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| R | I | O | E | T | A | T | Z | C | S |
| I | E | M | N | E | N | E | R | S | C |
| A | E | R | R | L | I | C | D | L | L |
| E | I | C | T | T | S | H | A | E | U |
| S | R | N | Z | N | E | G | A | R | O |
| N | P | B | A | E | E | T | S | M | E |
| N | A | O | R | I | I | L | I | H | S |
| E | R | E | P | P | P | E | T | K | B |
| L | | P | | T | | C | A | E | |

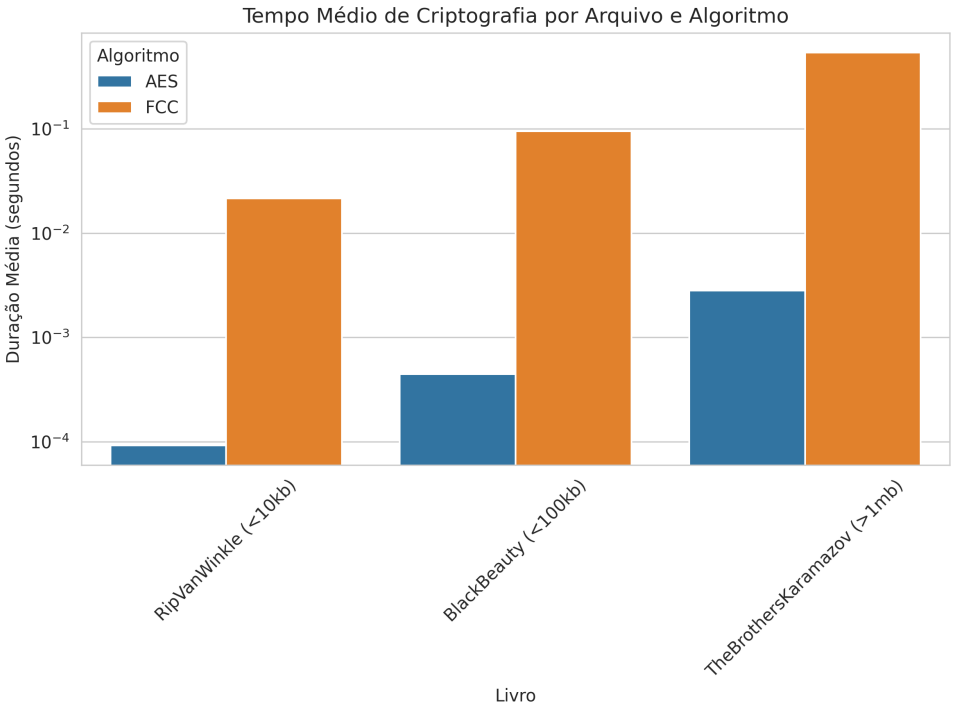
(d) As colunas são novamente reordenadas pela ordem alfabética da palavra chave.

| R | I | A | E | S | N | N | E | L | I |
|---|---|---|---|---|---|---|---|---|---|
| E | E | I | R | P | A | R | O | M | R |
| C | N | B | O | E | P | E | N | R | T |
| Z | A | R | P | T | E | L | T | N | E |
| I | P | T | A | N | I | S | E | E | I |
| P | T | E | C | H | G | T | L | E | C |
| Z | R | D | A | A | S | I | T | A | C |
| S | L | E | R | M | H | K | E | S | C |
| L | U | O | E | S | B | | | | |

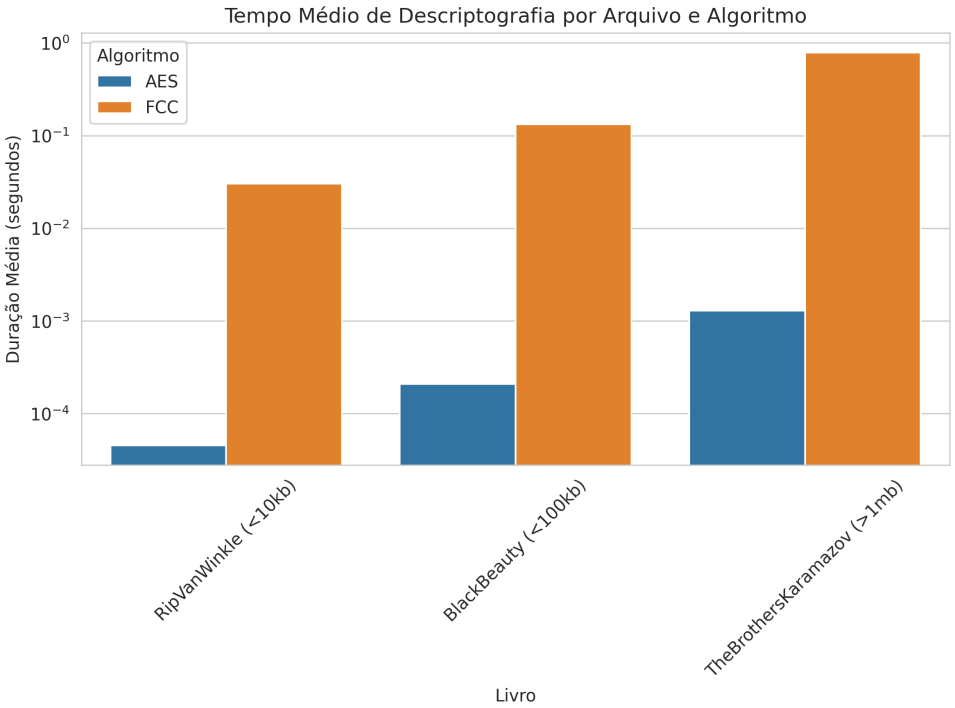
(e) Terceiro passo: As colunas são transpostas novamente e o texto está cifrado.

Figura 2: Representação visual da Cifra de transposição colunar dupla

# 6 Resultados




(a) Tempo médio de criptografia por arquivo e algoritmo.




(b) Tempo médio de descriptografia por arquivo e algoritmo.

Figura 3: Comparação de desempenho entre FCC e AES.