Primeiro Trabalho Prático (CI1017)

Lucas Emanuel de Oliveira Santos

29 de setembro de 2025

1 Introdução

Este relatório detalha a cifra CAT (*Caesar and Transposition*), um algoritmo de criptografia desenvolvido em Python que moderniza técnicas clássicas de substituição e transposição, adaptando-as para operar sobre o conjunto completo de caracteres do padrão Unicode (UTF-8).

2 Cifra de Substituição

A cifra de substituição escolhida foi a **Cifra de César**. A cifragem consiste em somar o *unicode point* de cada caractere a um valor de deslocamento, aplicando em seguida uma operação de módulo para garantir que o resultado sempre seja um caractere válido.

3 Cifra de Transposição

A cifra de transposição escolhida foi a **Cifra de Transposição Colunar**. O texto é escrito em uma matriz de acordo com o tamanho da palavra-chave e, em seguida, as colunas são reordenadas pela ordem alfabética da chave. O texto cifrado é obtido pela leitura das colunas na nova ordem.

Exemplo

Considere o texto simples **"ESSE TEXTO FOI CIFRADO"** e a chave **"CIFRA"**.

Tabela 1: Texto claro escrito na matriz segundo a chave CIFRA

C	I	F	R	A
E	S	S	E	T
E	X	T	O	F
O	I	C	I	F
R	A	D	O	-

Tabela 2: Matriz após reordenação das colunas em ordem alfabética da chave (A, C, F, I, R)

A	C	F	I	R
T	E	S	S	E
F	E	T	X	O
F	O	C	I	I
-	R	D	A	O

Por fim, o texto cifrado é obtido lendo as colunas na ordem:

TFF- EEOR STCD SXIA EOIO

Removendo o caractere de preenchimento (-), temos:

TFFEEORSTCDSXIAEOIO

4 Cifra CAT

A Cifra CAT combina as duas cifras descritas anteriormente de forma iterativa, seguindo os seguintes passos:

1. **Entrada:** O algoritmo recebe dois arquivos de texto como entrada:
   - A **chave**, utilizada para gerar as subchaves; caso o usuário forneça uma chave vazia, uma chave padrão é utilizada.
   - O **texto** a ser cifrado ou decifrado.
2. **Processamento da Chave:** A chave é dividida em uma lista de subchaves, formada pelas palavras do texto-chave, com tamanho máximo definido por `MAX_SUBKEYS`.
3. **Cifragem Iterativa:** Para cada subchave da lista, o algoritmo aplica as seguintes transformações no texto claro, nesta ordem:
   (a) A **Cifra de Transposição Colunar**, usando a subchave atual.
   (b) A **Cifra de Substituição de César**, onde o deslocamento é a soma do comprimento da subchave com uma constante pré-definida, para evitar deslocamentos triviais.

O processo de decifragem executa as mesmas operações na ordem inversa (primeiro a substituição inversa, depois a transposição inversa) e utilizando a lista de subchaves também na ordem inversa.

5 Resultados

As figuras abaixo comparam o desempenho de cifragem e decifragem da cifra CAT com o AES para os seguintes livros respectivamente: *Three Little Pigs*, *Pride and Prejudice* e *Little Women*. A chave padrão do CAT foi utilizada em todos os testes.

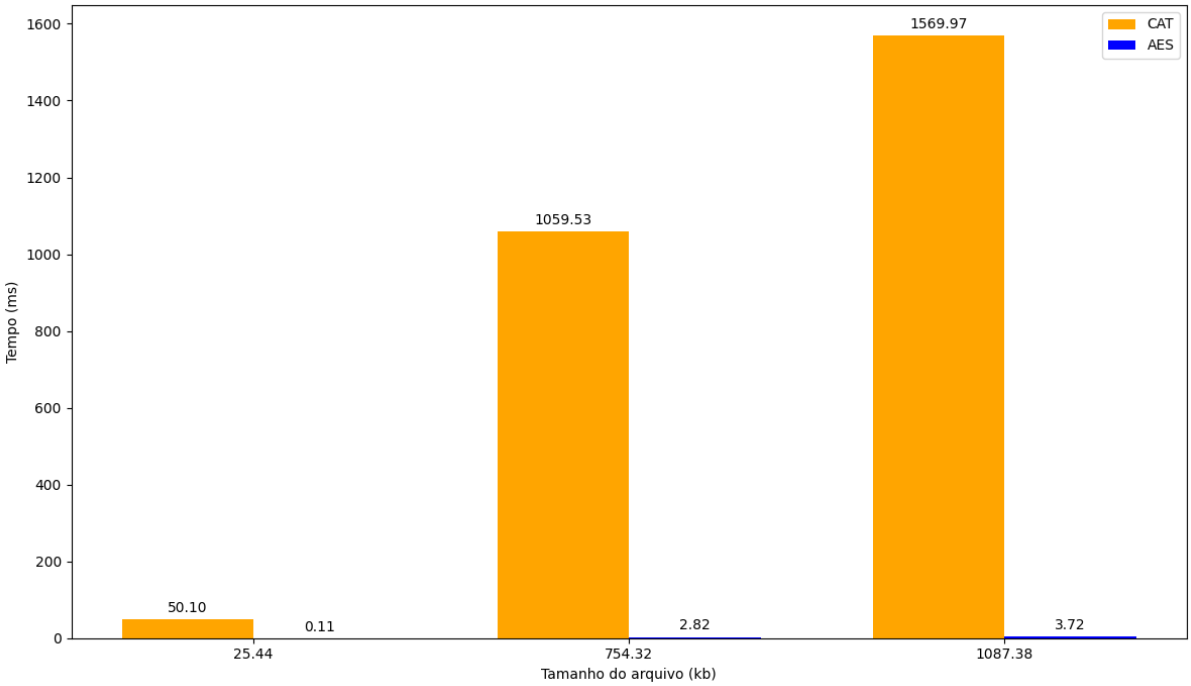

Figura 1: Comparativo de tempo para cifragem (CAT vs. AES).

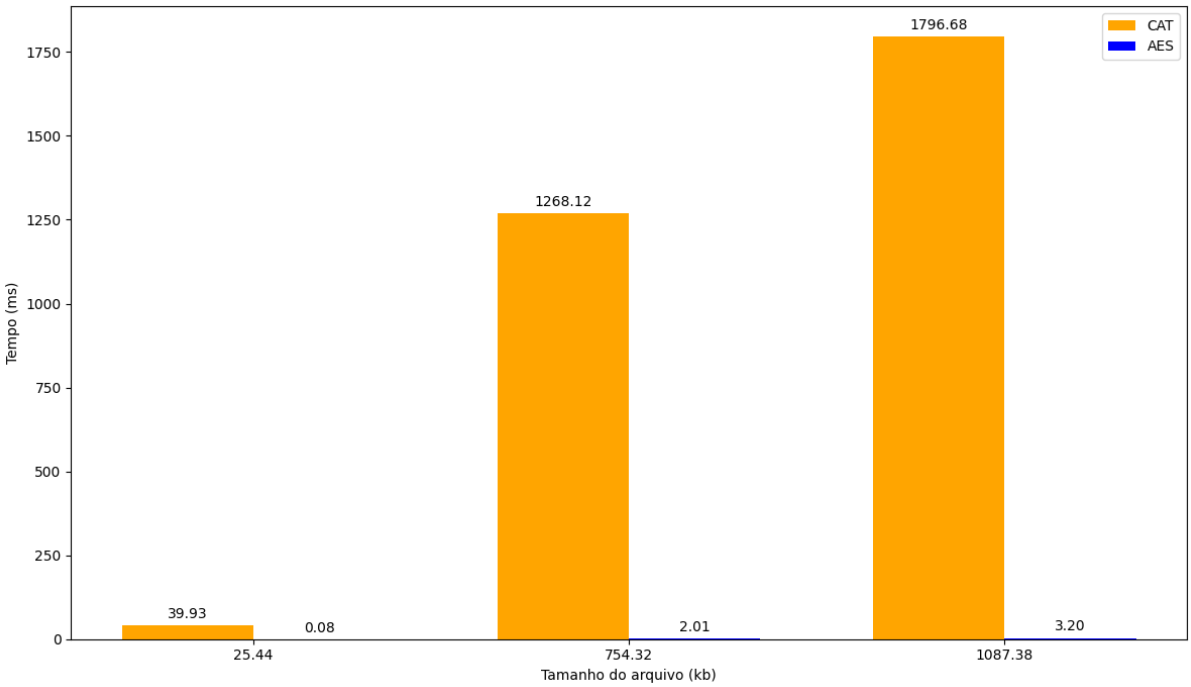

Figura 2: Comparativo de tempo para decifragem (CAT vs. AES).

A origem da disparidade de desempenho está no nível em que cada algoritmo manipula os dados. O AES foi projetado para máxima eficiência, operando diretamente sobre blocos de bytes em baixo nível. A cifra CAT, por outro lado, processa cada caractere individualmente, emulando a lógica de cifras clássicas de substituição e transposição para o conjunto de caracteres do padrão Unicode.

Observação: O desempenho da cifra CAT também depende da chave utilizada. Chaves diferentes podem gerar subchaves de tamanhos distintos, afetando a quantidade de operações de transposição e substituição, e consequentemente o tempo total de cifragem e decifragem.