Descrição do Exercício Programa

Prof. Me. Bryan Kano

Especificação dos Entregáveis

O artefato deve conter três entregáveis independentes, cada um responsável por quebrar um tipo distinto de cifra clássica. Nenhum deles precisa possuir interface gráfica. Desenvolva 10 criptogramas para cada. Pode ser feito em grupo.

Opção A: Somente opção 1 - 7,5

Opção B: Somente opção 2 - 7,5

Opção C: Opção 1 e 2 - 9,0

Opção D: Opção 1, 2 e 3 - 10,0

1. Quebra de Cifra de Substituição Livre (Monoalfabética)

Desenvolver um programa capaz de quebrar cifras de substituição livre, utilizando tabelas de frequências, heurísticas e métodos adaptativos.

- Requisitos funcionais:

O programa deve receber como entrada um texto encriptado por qualquer cifra de substituição monoalfabética (sem permutação).

O programa deve produzir como saída:

O texto decifrado.

Uma tabela de correspondência entre caracteres do texto cifrado e do texto claro.

Soluções que gerem múltiplas hipóteses (por exemplo, através de diferentes tabelas de frequência, hill-climbing, simulated annealing, index of coincidence, etc.) serão consideradas mais eficazes.

Para verificar automaticamente se a decodificação produz um texto válido, utilize algum modelo de LLM disponível no Hugging Face, avaliando coerência e legibilidade.

- O que será quebrado:

Substituição livre engloba todas as substituições monoalfabéticas

“Substituição livre” significa:

qualquer mapeamento 1→1 entre caracteres,

mas fixo ao longo de todo o texto,

sem ordem obrigatória,

sem fórmula (pode ser arbitrário).

Isso inclui todas as cifras abaixo:

Cifra de César

É apenas um caso especial de substituição onde o mapeamento é um deslocamento linear.

Cifra de Vigenère com chave de tamanho 1

Também vira uma cifra de César.

Cifra da Tabela Simples de Substituição

O clássico exemplo, exatamente o caso que seu artefato cobre.

Qualquer cifra monoalfabética com alfabeto parcial

(Enigma de criança, ROT13, códigos militares muito antigos etc.)

2. Quebra de Cifra de Permutação Livre

Desenvolver um programa capaz de quebrar cifras baseadas em permutação, utilizando técnicas estatísticas e análise de frequência posicional.

- Requisitos funcionais:

O programa deve receber como entrada um texto cifrado por qualquer cifra de permutação (ex.: transposição simples).

O programa deve produzir como saída:

O texto decifrado.

A correspondência dos índices, isto é, o mapeamento entre posições originais e permutadas.

Pesquisar métodos robustos para quebra, como:

análise de bigramas/trigramas por posição,

hill-climbing,

algoritmos genéticos,

simulated annealing,

digram fitness scoring.

Validar a qualidade do texto decifrado usando um modelo de LLM do Hugging Face, avaliando fluência e coerência.

- O que será quebrado:

Permutação livre engloba todas as transposições clássicas

“Permutação livre” significa:

o texto é reordenado,

mantendo os símbolos intactos,

mas com regras fixas (chaves).

Isso engloba:

Transposição por colunas

Transposição em forma de rail fence

Rotinas do tipo “Leitura em Z”, “espelho”, “rotações de matriz”

Qualquer cifra onde a ordem muda, mas o caractere não muda

Ou seja: qualquer cifra clássica de transposição entra no seu Entregável 2.

3. Quebra Combinada: Substituição Livre + Permutação no Mesmo Criptograma

Desenvolver um programa capaz de quebrar cifras onde substituição monoalfabética e permutação/transposição são aplicadas na mesma mensagem, em qualquer ordem.

- Requisitos funcionais:

O programa deve receber como entrada um texto cifrado que passou simultaneamente por:

uma cifra de substituição livre (monoalfabética),

uma cifra de permutação (transposição ou rearranjo de índices).

O programa deve gerar como saída:

o texto decifrado,

o livro de substituição (mapeamento caractere → caractere),

o mapeamento de permutação (índice original → índice cifrado).

O método pode combinar análises seqenciais ou integradas, por exemplo:

tentativa de reconstrução da ordem do texto com fitness baseado em n-gramas,

tentativa simultânea de substituição + permutação com heurísticas evolutivas,

coordenação entre heurísticas estatísticas e modelos de linguagem.

Validar automaticamente a qualidade das hipóteses com um LLM do Hugging Face, de preferência comparando vários candidatos.

- <u>O que será quebrado:</u>

Quando você combina:

substituição livre

permutação livre

Você cobre praticamente 90% das cifras pré–Primeira Guerra Mundial.

Isso inclui:

Os esquemas militares europeus do século XVIII–XIX

(Eram literalmente substituição + transposição.)

Cifras como “columnar transposition + substitution”

Que eram padrão em espionagem.

A vasta maioria das cifras artesanais em manuscritos históricos

IMPORTANTE: Exceções (o que NÃO é quebrado por esses métodos)

Só para clareza:

Cifras policomáticas como Vigenère com chave longa

Não funcionam porque a frequência “borra”.

Cifras mecânicas como Enigma

Não são simples substituição fixa + permutação fixa.

OTP / Vernam

Aleatoriedade perfeita, impossível.