Universidade de Brasília – UnB Campus Darcy Ribeiro

Disciplina: Segurança Computacional  
Docente: LORENA DE SOUZA BEZERRA BORGES  
Discente: GUILHERME ARAÚJO DE OLIVEIRA

Matrícula: 190125748

## 1. Introdução

A criptografia é a prática de proteger informações, convertendo dados legíveis em um formato indecifrável, acessível apenas a quem possui a chave correta para decifrá-los. Com raízes que remontam à Antiguidade, a criptografia evoluiu muito e hoje é fundamental na segurança digital, preservando a privacidade e integridade dos dados em redes e aplicativos.

Entre as técnicas clássicas estão as cifras de deslocamento e por transposição. Na **cifra de deslocamento**, como a cifra de César, cada letra do texto é substituída por outra, deslocada um número fixo de posições no alfabeto. Já a **cifra por transposição** reorganiza as letras de acordo com uma regra específica, mantendo o conteúdo original, mas alterando a ordem, como na cifra de colunas. Embora simples e vulneráveis por si só, esses métodos pavimentaram o caminho para os algoritmos complexos usados na criptografia moderna, que protege desde mensagens pessoais até transações bancárias online.

# 2. Objetivos

* Compreender o funcionamento das cifras de deslocamento e transposição.
* Analisar as aplicações e limitações dessas cifras em segurança computacional.
* Implementar exemplos práticos de cada tipo de cifra.

# 3. Revisão Teórica

## 3.1 Cifras de Deslocamento

Conhecida principalmente pela cifra de César, trata-se de uma técnica de substituição onde cada letra do texto original é deslocada um número fixo de posições no alfabeto. Por exemplo, se o deslocamento for de 3 posições, a letra "A" se torna "D", "B" se torna "E", e assim por diante. Essa técnica é simples, mas pode ser facilmente quebrada por métodos modernos de criptoanálise.

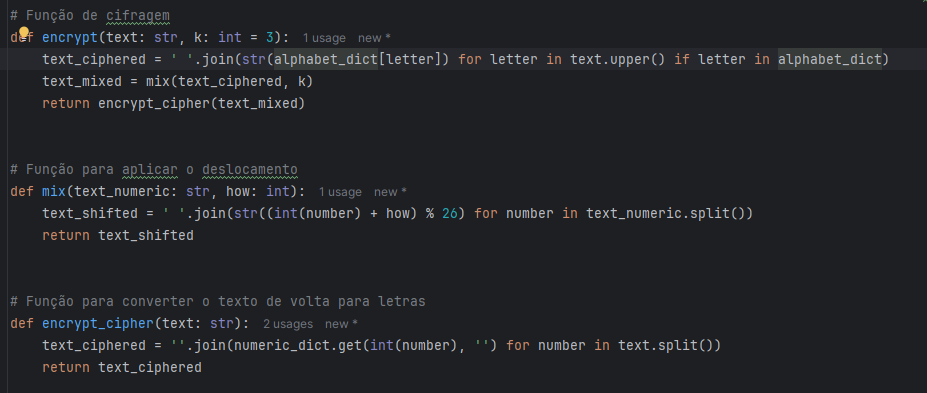
## 3.2 Cifras de Transposição

Nesse tipo de cifra, as letras da mensagem original são reorganizadas de acordo com uma regra específica, sem alterar as letras em si. Um exemplo clássico é a **cifra de colunas**, onde o texto é escrito em linhas de uma grade, e as colunas são reorganizadas de acordo com uma chave específica. Essa técnica preserva o conteúdo do texto original, mas altera sua ordem, dificultando a leitura sem a chave de transposição.

# 4. Implementação e Exemplos

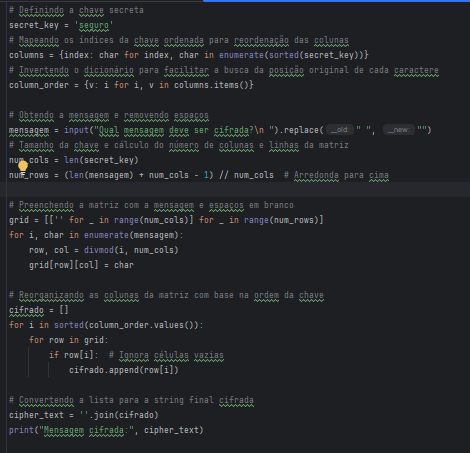
Nesta seção, apresente exemplos práticos de cada tipo de cifra. Mostre o processo de cifragem e decifragem de uma mensagem usando uma cifra de deslocamento e uma cifra de transposição, usando exemplos de código (caso aplicável) ou explicando o processo manualmente.

## 4.1 Exemplo de Cifra de Deslocamento



Aqui temos métodos para encriptação utilizando a cifra de deslocamento e nota-se que caso não tenha um tamanho de deslocamento definido na chamada da função utiliza-se a Cifra de César como padrão, nessa primeira etapa as letras são trocadas por de acordo com a posição no alfabeto, já na função *mix(text\_numeric: int, how: int)* é a função que trata do deslocamento no alfabeto sendo que *text\_numeric* é o texto normal apenas cifrado pela posição no alfabeto e *how* trata-se do quanto essa posição mudará. Agora a função *encrypt\_cipher()* trata-se da função que retorna o texto cifrado já misturado pela função *mix()*.

## 4.2 Exemplo de Cifra de Transposição



Inicialmente é definida uma chave secreta que servirá como base para a cifragem. Em seguida, a mensagem a ser criptografada é inserida em uma matriz. As colunas dessa matriz são organizadas de acordo com a ordem das letras da chave secreta, criando uma espécie de grade. A mensagem é preenchida nessa grade, linha por linha. Após a mensagem ser inserida na matriz, as colunas são reorganizadas de acordo com a ordem pré-definida pela chave secreta. A mensagem cifrada é obtida lendo a matriz coluna por coluna, seguindo a nova ordem. Essa reordenação das colunas embaralha a mensagem original, tornando-a ilegível para quem não conhece a chave secreta. Ao final, a mensagem cifrada é apresentada como resultado.

# 5. Comparação e Análise

As cifras de deslocamento e por transposição, embora ambas sejam métodos clássicos de criptografia, diferem significativamente em termos de segurança, facilidade de implementação e eficiência.

**Segurança**

* **Cifra de Deslocamento**: Este método é relativamente fraco em termos de segurança, já que o espaço de chaves é pequeno (apenas 25 possíveis deslocamentos em um alfabeto de 26 letras), tornando-a vulnerável a ataques de força bruta. Além disso, essa cifra mantém o padrão de frequência das letras, facilitando ataques por análise de frequência.
* **Cifra por Transposição**: Oferece um pouco mais de segurança do que a cifra de deslocamento, já que embaralha o conteúdo sem modificar as letras. Ainda assim, é vulnerável, pois quem conhece a regra de transposição pode reordenar o texto. Análise de frequência ajuda pouco aqui, mas a cifra continua exposta a ataques por anagramas ou testes de ordem de letras.

**Facilidade de Implementação**

* **Cifra de Deslocamento**: Extremamente fácil de implementar, mesmo manualmente, pois envolve apenas um simples deslocamento fixo das letras.
* **Cifra por Transposição**: Embora também simples, pode ser mais trabalhosa manualmente, especialmente se a regra de transposição for complexa (por exemplo, uma cifra de colunas ou cifra de rotações em uma grade).

**Eficiência**

* **Cifra de Deslocamento**: Muito eficiente, pois cada letra é substituída em uma operação direta e constante.
* **Cifra por Transposição**: Relativamente eficiente, mas ligeiramente mais lenta que a cifra de deslocamento devido ao rearranjo das letras.

**Situações de Aplicação**

* **Cifra de Deslocamento**: Historicamente, foi usada em comunicações militares simples (como a cifra de César). Hoje, serve mais para fins educacionais ou em cenários onde a simplicidade é prioritária e a segurança não é crítica.
* **Cifra por Transposição**: Pode ser usada para embaralhar informações em situações onde a ocultação básica seja suficiente, como em jogos, quebra-cabeças ou desafios lúdicos, e para explicar conceitos de criptografia em contextos didáticos.

# 6. Conclusão

Este trabalho abordou os conceitos e características das cifras de deslocamento e transposição, destacando suas diferenças e semelhanças em termos de segurança, facilidade de implementação e eficiência.

A **cifra de deslocamento** funciona substituindo cada letra por outra de acordo com um deslocamento fixo no alfabeto, tornando-a simples de implementar, mas vulnerável a ataques de força bruta e análise de frequência devido ao seu espaço de chaves reduzido. Já a **cifra por transposição** embaralha as letras sem alterá-las, reorganizando-as de acordo com uma regra específica. Embora também seja fácil de implementar, ela oferece um pouco mais de segurança, pois não preserva padrões de frequência de letras, mas ainda assim é suscetível a certos tipos de análise de anagramas.

Ambas as cifras são eficientes, mas diferem em complexidade de implementação. Em termos de segurança, porém, ambas são limitadas, especialmente em comparação a algoritmos modernos de criptografia, que utilizam operações matemáticas complexas e grandes espaços de chaves.

Estudar cifras de deslocamento e transposição é essencial para entender a base da criptografia, pois ajudam a compreender os princípios de substituição e permutação usados em técnicas mais avançadas. Essas cifras ilustram os conceitos fundamentais de ocultação e transformação de dados, que são expandidos em algoritmos modernos para alcançar a robustez exigida pela segurança digital atual.