

# **UniSenai – Faculdades da indústria**

**Engenharia de Software: Arquitetura de Computadores e Sistemas Operacionais**

**Matheus Gustavo Da Silva Pires**

**Luiz H.**

**Douglas H.**

**Gabriel H.**

**Giovanna A.**

**Vitor S.**

## **TIPOS DE CRIPTOGRAFIA E IMPLEMENTAÇÃO**

**CURITIBA – PR NOVEMBRO DE 2025**

# SUMÁRIO

## **Introdução**

Tipos de Criptografia

2.1 Criptografia Simétrica

2.2 Criptografia Assimétrica

2.3 Funções de Hash

2.4 Cifra de César

2.5 Criptografia Aleatória Desenvolvimento do Site

3.1 Funcionalidades

3.2 Estrutura Técnica

3.3 Explicação Interativa Conclusão Referências

# 1. INTRODUÇÃO

A criptografia é uma das ferramentas mais importantes na segurança da informação. Ela permite proteger dados sensíveis contra acessos não autorizados, garantindo confidencialidade, integridade e autenticidade. Este trabalho apresenta os principais tipos de criptografia utilizados atualmente e descreve a implementação de um site interativo que demonstra o funcionamento da cifra de César, incluindo uma variação com substituições aleatórias.

## 2. TIPOS DE CRIPTOGRAFIA

### 2.1 Criptografia Simétrica

A criptografia simétrica utiliza uma única chave para criptografar e descriptografar dados. É eficiente para grandes volumes de informação, mas exige que a chave seja compartilhada de forma segura entre as partes.

**Exemplos:** AES (Advanced Encryption Standard), DES (Data Encryption Standard).

### 2.2 Criptografia Assimétrica

Utiliza um par de chaves: uma pública para criptografar e uma privada para descriptografar. É amplamente usada em comunicações seguras e certificados digitais.

**Exemplos:** RSA, ECC (Elliptic Curve Cryptography).

### 2.3 Funções de Hash

Transformam dados em um valor fixo e irreversível. São usadas para verificar integridade e autenticar senhas, mas não permitem descriptografia.

**Exemplos:** SHA-256, MD5.

### 2.4 Cifra de César

A cifra de César é uma técnica de criptografia por substituição, considerada uma das mais antigas e simples da história. Seu nome deriva do imperador romano Júlio César, que a utilizava para proteger mensagens militares. O método consiste em substituir cada letra do texto original por outra, deslocada um número fixo de posições no alfabeto.

Por exemplo, com um deslocamento de três posições, a letra "A" torna-se "D", "B" torna-se "E", e assim sucessivamente. O alfabeto é tratado de forma circular, ou seja, após a letra "Z", retorna-se à letra "A". Essa técnica mantém os espaços e caracteres não alfabéticos inalterados, o que facilita a leitura do texto criptografado, mesmo que ele esteja codificado.

A seguir, um exemplo prático com deslocamento de três posições:

Texto original: **ATAQUE AO AMANHECER** Texto criptografado: **DWDTXH DR  
DPDQKHFHU**

Neste exemplo, cada letra foi deslocada três posições à frente no alfabeto. A letra "A" tornou-se "D", "T" tornou-se "W", e assim por diante. Os espaços foram mantidos, e não há alteração em caracteres que não sejam letras (caso existissem).

Apesar de sua simplicidade, a cifra de César é vulnerável a ataques por força bruta e análise de frequência, sendo inadequada para aplicações modernas que exigem alto

nível de segurança. No entanto, ela é amplamente utilizada em contextos educacionais para introduzir os conceitos básicos de criptografia.

## 2.5 Criptografia Aleatória

A criptografia aleatória é uma variação da cifra de substituição, na qual cada caractere do texto original é substituído por outro gerado de forma aleatória. Diferente da cifra de César, que utiliza um deslocamento fixo no alfabeto, essa técnica cria um **mapa de substituição dinâmico**, composto por letras, números e símbolos, que muda a cada execução.

Esse método permite que qualquer caractere — incluindo letras, números, espaços e símbolos — seja criptografado, aumentando a complexidade da codificação. Por exemplo, a letra "A" pode ser substituída por "@", "B" por "7", "C" por "#", e assim por diante. O mapa de substituição é gerado automaticamente e aplicado à frase digitada pelo usuário.

A seguir, um exemplo ilustrativo:

Texto original: **ATAQUE AO AMANHECER** Texto criptografado: @#7\$%& @  
@!&^)(&\*

Neste caso, cada caractere foi substituído por um símbolo ou número aleatório, conforme o mapa gerado. O site desenvolvido exibe esse mapa na aba de explicação, permitindo ao usuário entender como cada caractere foi transformado.

Embora essa técnica não seja segura para uso em ambientes reais, ela é eficaz para fins didáticos, pois demonstra o conceito de substituição não linear e reforça a importância da aleatoriedade na criptografia moderna.

## 3. DESENVOLVIMENTO DO SITE

### 3.1 Funcionalidades

O site desenvolvido possui duas abas principais:

- **Criptografar frase:** permite ao usuário digitar qualquer conteúdo e escolher entre cifra de César tradicional ou criptografia aleatória.
- **Como funciona:** explica passo a passo como a criptografia foi aplicada, com base na entrada do usuário.

### 3.2 Estrutura Técnica

O site foi construído utilizando apenas **HTML, CSS e JavaScript**, sem bibliotecas externas. As principais características técnicas incluem:

- Campo de entrada que aceita qualquer caractere.
- Botão de criptografar e suporte à tecla Enter.
- Validação de entrada com mensagens claras em caso de erro.

- Design responsivo e profissional, com cores neutras e tipografia clara.
- Código comentado e organizado para facilitar manutenção.

### 3.3 Explicação Interativa

A aba de explicação apresenta:

- O funcionamento da cifra de César tradicional.
- Quando escolhida a opção aleatória, exibe o mapa de substituição gerado e como ele foi aplicado à frase.
- Comparação entre os dois métodos, destacando a diferença entre deslocamento fixo e substituição dinâmica.

## 4. CONCLUSÃO

A criptografia é essencial para a segurança digital, e sua compreensão pode ser facilitada por ferramentas interativas. O site desenvolvido cumpre esse papel ao demonstrar de forma clara e acessível o funcionamento da cifra de César e sua variação aleatória. Além disso, reforça conceitos fundamentais de criptografia e validação de dados.

## 5. REFERÊNCIAS

- STALLINGS, William. *Criptografia e segurança de redes*. 6. ed. São Paulo: Pearson, 2017.
- TANENBAUM, Andrew S.; WETHERALL, David J. *Redes de computadores*. 5. ed. São Paulo: Pearson, 2011.
- BRUCE, Schneier. *Applied Cryptography*. Wiley, 1996.
- Documentação oficial do AES: <https://nvlpubs.nist.gov>