



**UNIFACS**  
UNIVERSIDADE SALVADOR  
LAUREATE INTERNATIONAL UNIVERSITIES

**REGINALDA SANTOS SILVA**

**TRABALHO ARQUITETURA DE SOFTWARE  
CRIPTOGRAFIA DE CESAR**

**Salvador  
2020**



**UNIFACS**

UNIVERSIDADE SALVADOR

LAUREATE INTERNATIONAL UNIVERSITIES

## **TRABALHO ARQUITETURA DE SOFTWARE CRIPTOGRAFIA DE CESAR**

Trabalho apresentado à disciplina de Arquitetura de Software pertencente ao curso de Análise e desenvolvimento de sistemas como requisito para obtenção de nota.

Orientador: Professor Galdir Regis

**Salvador**

**2020**

## **Sumário**

1. Introdução	3
2. Descrição textual código Cifras de Cesar	4
3. Caso de uso	5
4. Tipo de arquitetura	5
5. Digrama de classe	6
6. Conclusão	6

## 1. Introdução

Segundo (Wikipedia) muitos desconhecem a história de criptografia de Cesar, estudos informam que a criptografia é tão antiga quanto a própria escrita que já estava presente no sistema hieroglífica dos egípcios. Estudos afirmam que os romanos utilizavam códigos secretos para comunicar planos de batalha. A partir de muitas guerras mundiais e com a invenção do computador houve crescimento da criptografia, e com evolução da tecnologia foi crescendo cada vez mais e sendo incorporados algoritmos matemáticos.

Nos anos 50 ac. Júlio César usou a cifra de substituição, no qual ele alterou as letras mudando as posições, alternando-as e reforçando acrescentava a substituição de letras latinas por gregas, e este código ainda é usado até os nossos dias atuais, denominado de código de César ou cifras de César. Segundo (STALLING, Willian) o texto cifrado é ilegível, pois as letra são substituídas por transposições, quer dizer são usados letra números e símbolos, o texto é envolvido por uma sequência de bits que irão substituir os mesmos por bits de texto cifrado .Conforme exemplo abaixo foram alternadas 03 letras após a original.

Exemplos: Texto normal – UM NOVO BRASIL

Texto cifrado – XPQRYREUDVLO

Texto normal – NUNCA DESISTIR, PERSEVERAR ATÉ O FIM

Texto cifrado – QXQFFDGHVLUWLUSHUNYHUDUDWHRIMP

## 2. Descrição textual Código de Cesar

Foi criado uma variável tipo String que vai informar uma mensagem em um array de caracteres, o array tipo char que vai transformar a mensagem em um array tipo string e cada uma das letras serão guardadas em posições diferentes, transformando a mensagem cifrada. No for o (i) é como contador tamanho do array que será incrementado. O valueOf(array) é transformado em valor String, no qual é lido e interpretado e quando imprimida a mensagem é encriptada. A cada posição de array é somado (+5). O outro array é para fazer a deciptação o processo inverso ocorrendo a subtração da posição menos (-5).

3 Caso de Uso

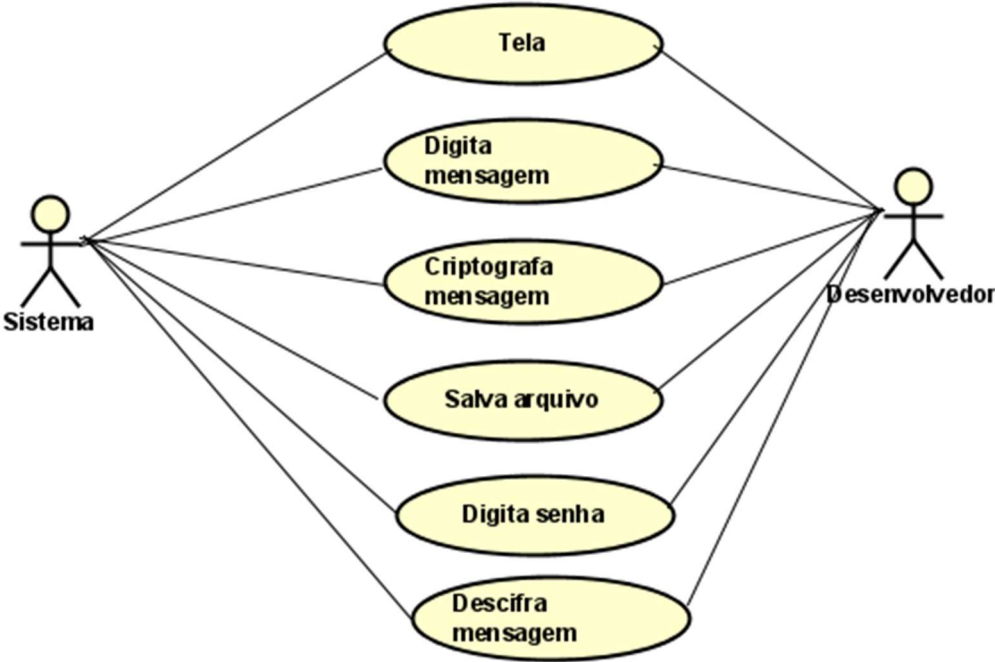
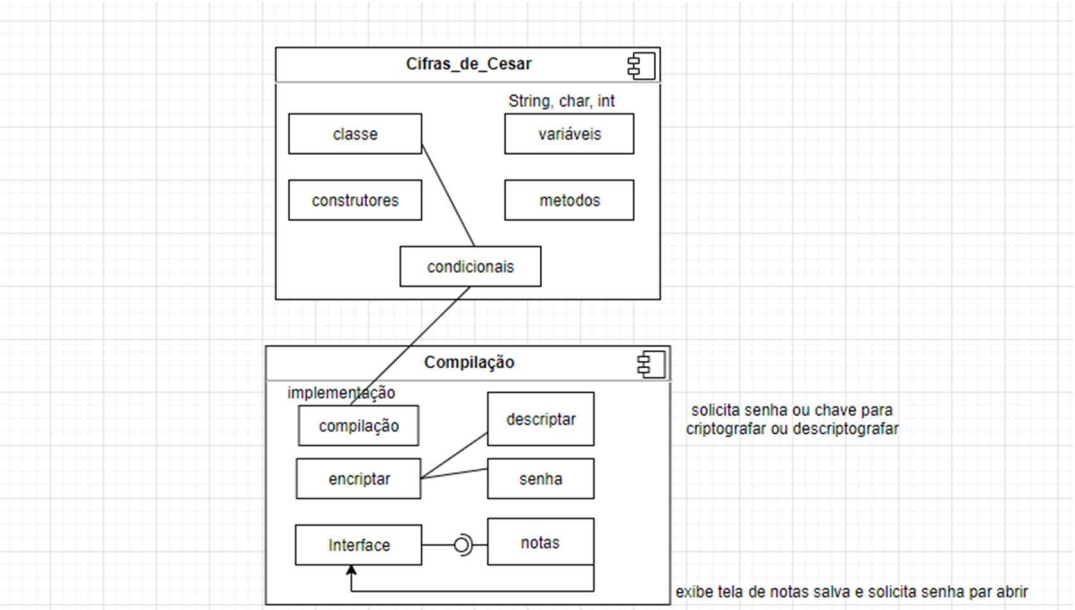


figura 1 Caso de Uso

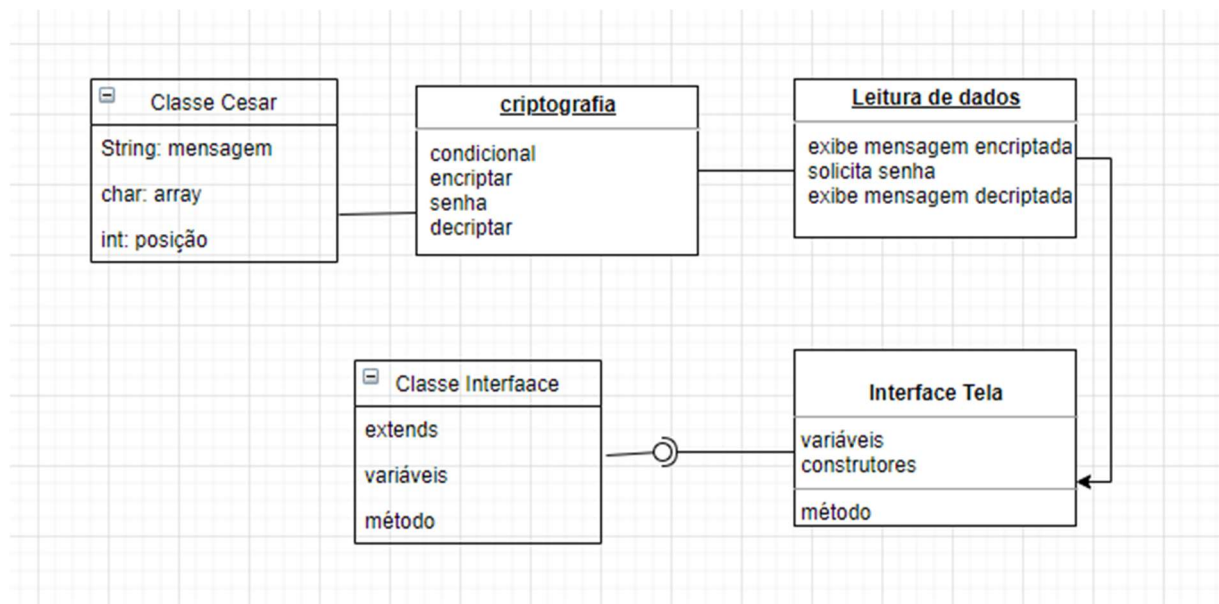
4 Arquitetura Repositório Código Cesar

figura 2 Diagrama de arquitetura estilo Repositório



Segundo (Sommerville) o padrão de arquitetura de Repositório gerencia os dados localizados no repositório central tendo acesso a todos componentes do sistema, sendo que estes componentes não estabelecem comunicação direta com o repositório. A comunicação dos componentes ocorre apenas por intermédio do repositório.

## 5 Diagrama de classe



## 6 Conclusão

No código Cifras de Cesar as variáveis são colocadas em um array de caractere, no qual será escaneada em busca da mensagem digitada, em ler dados a biblioteca que foi importada vai escanear o caminho percorrendo o array de caractere no qual a mensagem será encriptada passando pelas condicionais onde serão incrementadas no caso de encriptar, ou decrementadas ocorrendo a decriptação. Na compilação o sistema solicita que seja digitada a mensagem seguida da senha e é cifrada ou decifrada a mensagem.

### Referências Bibliográficas:

STALLINGS, William. Criptografia e segurança de redes. 6ª edição, Pearson 580

SOMMERVILLE, Ian. Engenharia de Software - 9ª edição. Pearson 548

Disponível em: <[https://pt.wikipedia.org/wiki/Cifra\\_de\\_C%C3%A9sar](https://pt.wikipedia.org/wiki/Cifra_de_C%C3%A9sar)>