**MEMORIAL DESCRITIVO – PROTEÇÃO DOS DADOS PESSOAIS POR MEIO DE CRIPTOGRAFIA.**

**Desenvolvido por: IARA**

**Aplicativo: IARA**

**Participantes:**

* + Davi Arakaki Oliveira de Souza;
  + Enzo Christowam Joaquim;
  + Gustavo Kenzo Shirahata Ota;
  + Letícia Favoretto Pires de Camargo;
  + Lucas Kluska Donini;
  + Luigi Azevedo Biondo;
  + Nicolas Isepe Paz;
  + Ryan Cursino Moraes.

**Sala: 1J**



**Link da documentação adotada:** <https://www.mindrot.org/files/jBCrypt/jBCrypt-0.1-doc/BCrypt.html>

**DESCRIÇÃO**

Ela é uma classe que permite de maneira simples e eficaz, a pseudonimização por criptografia de um texto, e dentro do nosso trabalho ela foi utilizada para criptografar a informação de senha dos usuários.

Seu mecanismo de chave tanto para criptografar, como para descriptografar, se baseia em uma variação exponencial de 2, e admite valores entre 4 e 31 como expoentes, apesar do valor padrão ser 10.

**PRINCIPAIS MÉTODOS**

Ela possui três métodos principais, os quais utilizamos para realizar a criptografia, que são hashpw(), gensalt() e checkpw():

**hashpw**( java.lang.String password, java.lang.String salt ) 🡪 Esse método admite dois parâmetros, um texto, que deverá ser criptografado, e a configuração da chave que será responsável pela operação de criptografia.

Ao fim, o método retorna a senha criptografada.

**Gensalt**( int log\_rounds ) 🡪 Ele é usado para configurar a chave de criptografia e tem apenas 1 parâmetro opcional, que é o valor que servirá para configurar a operação de criptografia.

**OBS**: Dentro do trabalho, esse método foi utilizado para proporcionar o segundo parâmetro do método hashpw() e foi passado como parâmetro o valor 15.

**checkpw**( java.lang.String plaintext, java.lang.String hashed ) 🡪 Ele é usado para comparar um texto com uma senha criptografada, e retorna true, caso o texto seja correspondente com a que foi criptografada, e false, caso a criptografia não seja correspondente.

**IMPORTAÇÃO DA CLASSE**

Dentro do trabalho, utilizamos a seguinte linha de código:

“org.mindrot.jbcrypt.BCrypt”

Assim, trouxemos a classe “BCrypt” que está dentro do pacote “org.mindrot.jbcrypt”.

**MODO DE APLICAÇÃO**

Texto

O conteúdo gerado por IA pode estar incorreto.