在线oj项目-加密算法

加密算法

简介

加密算法是一种将明文转换为密文的过程，以保护数据的安全性和机密性。

作用

- **安全性**：存储明文密码是非常不安全的。如果数据库被非法访问或泄露，攻击者可以直接获取所有用户的密码。
- **减少内部风险：**即使企业内有不诚实的员工或管理员，他们也无法轻易获取其他管理员的密码，因为密码是加密存储的。
- **提升用户信任度** 。密码加密有助于提升用户对网站或应用程序的信任感，使其更愿意使用加密保护的网站。

常见的加密算法：

- **可逆算法：**一种可以将加密后的密文还原为原始明文的算法。
  - 对称算法：对称加密(也叫私钥加密)指加密和解密使用相同密钥的加密算法。它要求发送方和接收方在安全通信之前，商定一个密钥。对称算法的安全性依赖于密钥，泄漏密钥就意味着任何人都可以对他们发送或接收的消息解密，所以密钥的保密性对通信的安全性至关重要
  - 非对称算法：非对称加密是指需要两个密钥来进行加密和解密，这两个秘钥分别是公钥（public key）和私钥（private key），如果用公钥对数据进行加密，只有用对应的私钥才能解密。
- **不可逆算法：**一种无法将加密后的密文还原为原始明文的算法。
  - 单向散列（hash）加密：是指把任意长的输入串变化成固定长的输出串，并且由输出串难以得到输入串的加密方法。广泛应用于对敏感数据加密，比如用户密码，请求参数，文件加密等。

BCrypt

Bcrypt是一种哈希加密算法，被广泛应用于存储密码和进行身份验证。并且Bcrypt算法包含一个重要的特性即每次生成的哈希值都不同，这是由于Bcrypt算法在计算时会先生成一个随机的盐值与用户密码一起参与计算最终得到一个加密后的字符串。由于生成的盐值是随机的，所以即使每次使用相同的密码得到结果也是不同的。这样可以有效的防止攻击者使用一些手段破解用户密码。

使用

- **提供加密算法工具类**

```java
import org.springframework.security.crypto.bcrypt.BCryptPasswordEncoder;

/**
 * 加密算法工具类
 */
public class BCryptUtils {
    /**
     * 生成加密后密文
     *
     * @param password 密码
     * @return 加密字符串
     */
    public static String encryptPassword(String password) {
        BCryptPasswordEncoder passwordEncoder = new BCryptPasswordEncoder();
        return passwordEncoder.encode(password);
    }

    /**
     * 判断密码是否相同
     *
     * @param rawPassword     真实密码
     * @param encodedPassword 加密后密文
     * @return 结果
     */
    public static boolean matchesPassword(String rawPassword, String encodedPassword) {
        BCryptPasswordEncoder passwordEncoder = new BCryptPasswordEncoder();
        return passwordEncoder.matches(rawPassword, encodedPassword);
    }
}
```

比特就业课