

```
1 package hashfunctions;
2
3 import java.nio.charset.StandardCharsets;
4 import java.security.MessageDigest;
5 import java.security.NoSuchAlgorithmException;
6 import java.security.SecureRandom;
7
8 public class Driver {
9
10     public static void main(String[] args) throws NoSuchAlgorithmException, InterruptedException {
11         System.out.println("SHA-512");
12         testSHA512();
13         System.out.println("BCRYPT");
14         testBcrypt();
15     } //end method main
16
17     static void testBcrypt() throws InterruptedException {
18         long start = System.nanoTime(); //used in calculate time taken to run program
19
20         hashPassword("Daria");
21         hashPassword("password");
22         hashPassword("P4ssW0rd!");
23
24         //calculate time taken to run program
25         Thread.sleep(3000);
26         long duration = (System.nanoTime() - start)/1000000;
27         System.out.println("TIME TAKEN: " + duration + "ms\n\n");
28     } //end method testBcrypt
29
30     static void testSHA512() throws NoSuchAlgorithmException, InterruptedException{
31         long start = System.nanoTime(); //used in calculate time taken to run program
32
33         MessageDigest md = MessageDigest.getInstance("SHA-512"); //hashing function
34         SecureRandom random = new SecureRandom(); //used to generate random salt
35         //specify the plaintext passwords to hash
36         hashPassword(md, random, "Daria");
37         hashPassword(md, random, "password");
38         hashPassword(md, random, "P4ssW0rd!");
```

```
39
40     //calculate time taken to run program
41     Thread.sleep(3000);
42     long duration = (System.nanoTime() - start)/1000000;
43     System.out.println("TIME TAKEN: " + duration + "ms\n");
44 } //end method testSHA512
45
46
47 /**
48  * Method to hash a given password with salt.
49  * Used with BCrypt hashing function.
50  * @param password - the plaintext password to be hashed
51  */
52 static void hashPassword(String password) {
53     String salt = BCrypt.gensalt(15);
54     String hashedPassword = BCrypt.hashpw(password, salt); //hash the password using password and salt
55     System.out.println("Plain text password: " + password
56         + "\nHash value: " + hashedPassword);
57 } //end method hashPassword
58
59
60 /**
61  * Method to hash a given password with salt.
62  * Used with SHA-512 hashing function.
63  * Abstracted from https://www.javaguides.net/2020/02/java-sha-512-hash-with-salt-example.html
64  * @param md - used to hash the password
65  * @param random - used to generate the salt
66  * @param password - the plaintext password to be hashed
67  */
68 static void hashPassword(MessageDigest md, SecureRandom random, String password) {
69     byte[] salt = new byte[16];
70     random.nextBytes(salt);
71     md.update(salt); //add the salt
72     //generate the hash value using digest method
73     byte[] hashedPassword = md.digest(password.getBytes(StandardCharsets.UTF_8));
74     StringBuilder stringBuilder = new StringBuilder();
75     //for loop to convert array of bytes to String
76     for(int i = 0; i<hashedPassword.length; i++) {
```

```
77         stringBuilder.append(Integer.toString((hashedPassword[i] & 0xff) + 0x100, 16).substring(1));
78     } //endfor
79     System.out.println("Plain text password: " + password
80         + "\nHash value: " + stringBuilder.toString());
81 } //end method hashPassword
82 } //end class Driver
```