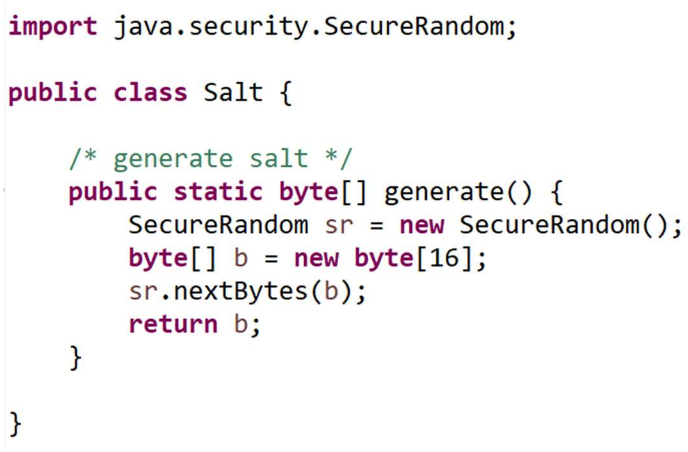
# Tutorial -3

Question:

1. Explain salting technique in the context of the data security.
   Reference: https://www.irjet.net/archives/V4/i11/IRJET-V4I1126.pdf

   Test code:



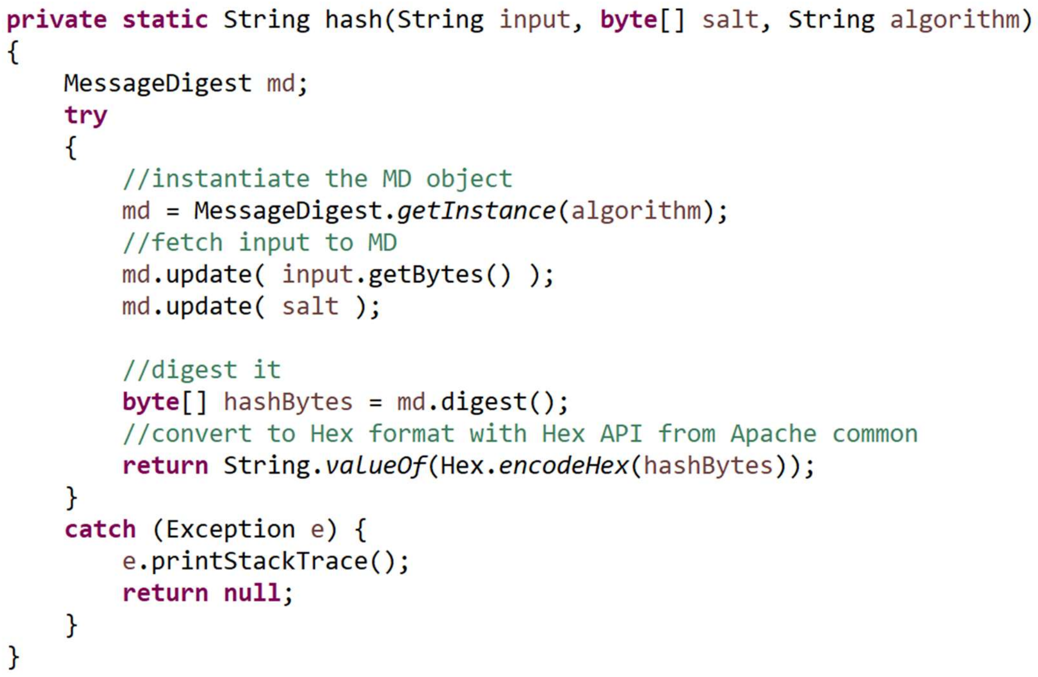
```java
import java.security.SecureRandom;

public class Salt {

    /* generate salt */
    public static byte[] generate() {
        SecureRandom sr = new SecureRandom();
        byte[] b = new byte[16];
        sr.nextBytes(b);
        return b;
    }

}
```

2. Include the salt value in the hashing function. Test your program.



```java
private static String hash(String input, byte[] salt, String algorithm)
{
    MessageDigest md;
    try
    {
        //instantiate the MD object
        md = MessageDigest.getInstance(algorithm);
        //fetch input to MD
        md.update( input.getBytes() );
        md.update( salt );

        //digest it
        byte[] hashBytes = md.digest();
        //convert to Hex format with Hex API from Apache common
        return String.valueOf(Hex.encodeHex(hashBytes));
    }
    catch (Exception e) {
        e.printStackTrace();
        return null;
    }
}
```

3. What is BCrypt? Test the BCrypt hashing function using https://bcrypt.online/

4. Download the BCrypt class. Implement the following requirements.

   Source: https://www.mindrot.org/projects/jBCrypt/

   - Generate the salt using BCrypt
   - Hash the password value with BCrypt
   - Write the salt and hashed password to the text file.
   - Make a login form that inquire the users to enter the password. Verify the password for validity.