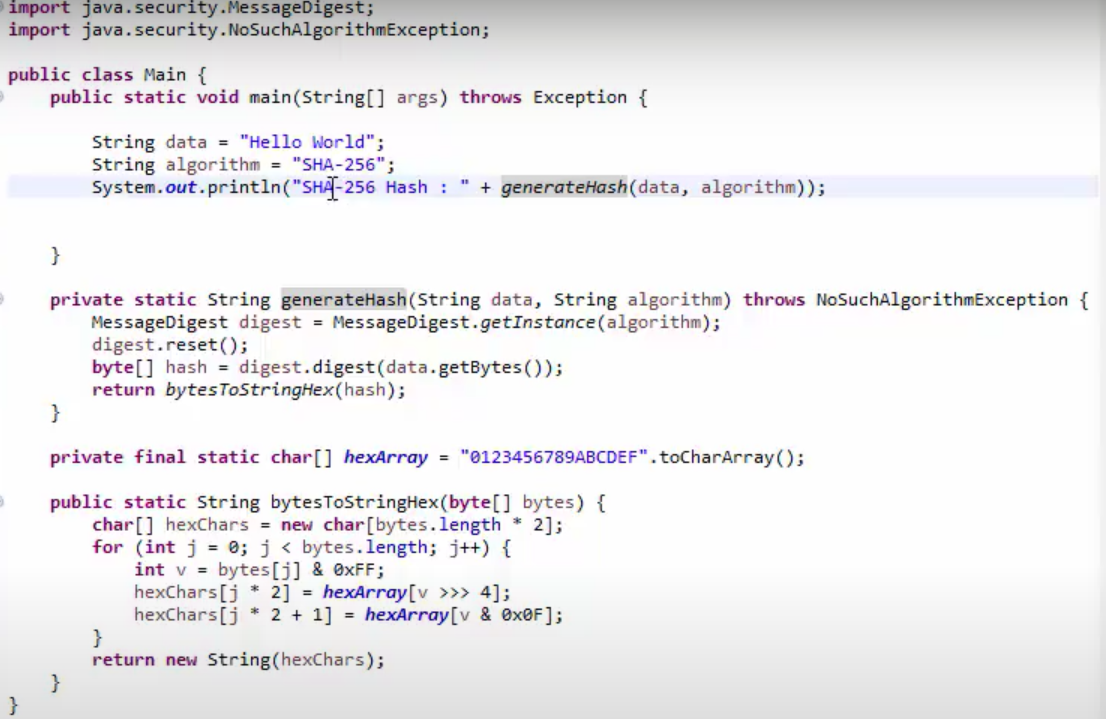
**Encryption:** Encryption is a two way function, using Encryption key we can Decrypt the data.

**Password Hashing:**

MD5, SHA-512(latest version of SHA series) are algorithms, but they are very old so not recommended to use.

**Key Terms:** **One way Hash**(reverse hash is not allowed), **Hash Collision** (If identical output generated by hash Function from 2 unique Input String) , **Avalanche Effect** (If any small changes in input string make drastically changes in output)



**Salted Hash:**



**PBKDF2**, **BCrypt** and **SCrypt** are three recommended algorithms.

PBKDF2- **Password Based Key Derivation Function-2**

Java has implementation of “[**PBKDF2**](https://en.wikipedia.org/wiki/PBKDF2)” algorithm as “[**PBKDF2WithHmacSHA1**](https://docs.oracle.com/javase/7/docs/technotes/guides/security/StandardNames.html#SecretKeyFactory)“

<https://howtodoinjava.com/java/java-security/how-to-generate-secure-password-hash-md5-sha-pbkdf2-bcrypt-examples/>