





* Symmetric and Asymmetric hashing algorithm

Symmetric and Asymmetric hashing algorithm are different based on the key it use.

Symmetric encryption use same same key to encrypt and decrypt the plane text , where as Asymmetric encyption use the public and private key to encrypt and decrypt the text.

AES (**Advanced Encryption Standard**) – Most commonly and widely used symmetric block cipher algorithm.

RSA (**Rivest–Shamir–Adleman**) - This is also widely used

To implement AES/RSA , required API are with Java securiy plackage. So no external dependency.

Usecase:

**One way hash:**

Spring Supports major hashing algorithm available in Spring Security package org.springframework.security.\*.

Use case:

We store the confidential information in database in hashed form. User to validate it’s input information hashed by the same algorithm and compare it to the already stored hashed value.

Example: We store user log-in password in database by hashing it. Everytime user login to the system, first his/her password is hashed and then compired with the dabase stored value.

Spring suppot MD5, SHA , Bcrypt and other strong hashing algoriths

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