SHA-3 (Secure Hash Algorithm 3) es una familia de funciones hash criptográficas publicada por el Instituto Nacional de Estándares y Tecnología (NIST) en 2015. A diferencia de las versiones anteriores de SHA (como SHA-1 y SHA-2), SHA-3 se basa en un diseño completamente diferente llamado Keccak, desarrollado por Guido Bertoni, Joan Daemen, Michaël Peeters y Gilles Van Assche.

### Características Principales de SHA-3:

1. \*\*Base en el Algoritmo Keccak\*\*:

- Keccak es un algoritmo basado en la construcción esponja (sponge construction), lo que le permite ser muy flexible y resistente a ciertos tipos de ataques criptográficos.

2. \*\*Diferentes Variantes\*\*:

- SHA-3 incluye varias variantes con diferentes longitudes de salida: SHA3-224, SHA3-256, SHA3-384 y SHA3-512. Estos números indican el tamaño del hash generado en bits.

- También incluye dos versiones extendidas: SHAKE128 y SHAKE256 (SHA-3 Extendable Output Functions), que permiten una longitud de salida variable.

3. \*\*Seguridad\*\*:

- SHA-3 fue diseñado para ser resistente a una amplia gama de ataques criptográficos, incluyendo los ataques de colisión y preimagen, que han afectado a algoritmos más antiguos como MD5 y SHA-1.

4. \*\*Estructura Esponja\*\*:

- La construcción esponja permite que SHA-3 tenga una alta resistencia a colisiones y preimágenes. La estructura interna del Keccak permite absorber (absorb) los datos de entrada y exprimir (squeeze) el hash final en un proceso iterativo.

5. \*\*Independencia de SHA-2\*\*:

- SHA-3 fue desarrollado como una alternativa y un respaldo a SHA-2, en caso de que se encontraran debilidades en SHA-2. Sin embargo, hasta ahora SHA-2 sigue siendo considerado seguro.

6. \*\*Rendimiento\*\*:

- Aunque SHA-3 es generalmente más lento que SHA-2 en software, su diseño permite optimizaciones que pueden mejorar su rendimiento en hardware específico.

### Uso de SHA-3:

- \*\*Hashing de Datos\*\*:

- SHA-3 se utiliza para crear hash de datos, lo que garantiza la integridad de los datos y la autenticidad.

- \*\*Firmas Digitales y Certificados\*\*:

- Es útil en la generación de firmas digitales y certificados, proporcionando una capa adicional de seguridad.

- \*\*Almacenamiento Seguro de Contraseñas\*\*:

- En combinación con técnicas de sal y otros métodos de endurecimiento, SHA-3 puede ser utilizado para almacenar contraseñas de manera segura.

### Implementación en Java:

Para usar SHA-3 en Java, se puede utilizar la clase `MessageDigest` del paquete `java.security`, que incluye soporte para SHA-3 (a partir de Java 9):

```java

import java.security.MessageDigest;

import java.security.NoSuchAlgorithmException;

public class Utilidades {

public static String encriptarSHA3(String texto) {

try {

MessageDigest md = MessageDigest.getInstance("SHA3-256");

byte[] hash = md.digest(texto.getBytes());

StringBuilder sb = new StringBuilder();

for (byte b : hash) {

sb.append(String.format("%02x", b));

}

return sb.toString();

} catch (NoSuchAlgorithmException e) {

throw new RuntimeException(e);

}

}

public static boolean verificarPassword(String passwordIngresada, String passwordAlmacenada) {

String passwordEncriptada = encriptarSHA3(passwordIngresada);

return passwordEncriptada.equals(passwordAlmacenada);

}

}

```

SHA-3 proporciona un alto nivel de seguridad y es una excelente opción para aplicaciones que requieren integridad y autenticidad de datos.