md5

- description : md5
- author : 오션
- email : shlim@repia.com
- lastupdate : 2022-04-18 Mon

md5

블록 길이 (block length):
하나의 블록에 포함된 기록, 단어 또는 문자의 총수, 블록 길이가 길면 데이터 전송 효율은 좋으나 입출력 (송수신) 버퍼의 길이, 블록 오류율, 블록 검사 방식을 별도로 고려해야 한다.

해시 (Hash)

- 블록 길이(block length)에 맞추기 위해서 메모리에 기입된 의미 없는 정보를 표시한다. (출처 : IT 용어사전)
- 기억 장치 등에서 의미가 없어 불필요하게 된 정보. 일반적으로 자기 디스크나 자기 테이프같이 블록 단위로 정보를 관리하는 보조 기억 장치에서는 작은 크기의 정보라도 하나의 블록에 할당되기 때문에 보조 기억 장치에서 정보가 기록되지 않은 블록이 버려지는 경우가 발생하게 되면 이때 전혀 의미 없는 값들이 대신 존재하게 된다. (출처 : IT용어사전-해시)
- 데이터 길이의 조건을 맞추기 위해 부가하여 기록되는 의미 없는 정보 (출처 : 전자용어사전)

Class MessageDigest

MessageDigest 클래스는 SHA-1 또는 SHA-256과 같은 Message Digest 알고리즘의 기능을 애플리케이션에 제공합니다.
Message Digest는 **임의의 크기를 가진 데이터를 가져와 고정된 길이의 해시값으로 출력하는 안전한 단방향의 해시 함수**입니다.
(Message digests are secure one-way hash functions that take arbitrary-sized data and output a fixed-length hash value.)

모든 Java 플랫폼을 구현하는 것에는 다음의 표준 MessageDigest 알고리즘을 지원해야 합니다.

- MD5
- SHA-1
- SHA-256

이러한 알로리즘들은 Java Cryptography Architecture Standard Algorithm Name Documentation

의MessageDigest Algorithms 섹션 | 에 설명되어 있습니다.

Class DigestUtils

일반적인 MessageDigest 작업을 단순화하는 작업입니다. 이 클래스는 변경할 수 없으며, 스레드로부터 안전합니다. 그러나 일반적으로 이 클래스가 생성하는 MessageDigest 인스턴스는 그렇지 않습니다.

MessageDigestAlgorithms 클래스는 `getDigest(String)` 메소드 및 Digest 알고리즘 이름이 필요한 다른 메소드와 함께 사용될 수 있는 표준 digest 알고리즘에 대한 상수를 제공합니다.

md5Hex

```
public static String md5Hex(String data)
```

Calculates the MD5 digest and returns the value as a 32 character hex string.
MD% digest를 계산하고, 32자의 16진수 문자열로 반환합니다.

```
package com.ocean.cryto.md5;

import org.apache.commons.codec.digest.DigestUtils;

public class MD5HashDemo {

    public static void main(String[] args) {
        // Calculates the MD5 digest for the password text and returns
        // the value as a 32 character hex string
        String password = "s3cretw0rd**";
        String digest = DigestUtils.md5Hex(password);

        // Prints the plain text password, the digest and the Length of the
digest
        System.out.println("Password        = " + password);           //
Password        = s3cretw0rd**
        System.out.println("Password Digest = " + digest);             //
Password Digest = 203c603a7330ab3ea032f4b9f140cf95
        System.out.println("Length          = " + digest.length());    //
Length          = 32

        // Calculates the MD5 digest for the Long texts.
        String md5 = """
                The MD5 message-digest algorithm is a formerly \
                widely used cryptographic hash function that produces \
```

```
                a 128-bit (16-byte) hash value. Specified in RFC 1321, \
                MD5 has been utilized in a wide variety of security \
                applications, and is also commonly used to check data \
                integrity. MD5 was designed by Ron Rivest in 1991 to \
                replace an earlier hash function, MD4. An MD5 hash value \
                is typically expressed as a hexadecimal number, 32 \
                digits long.
                """;
        String fingerprint = DigestUtils.md2Hex(md5);

        // Prints the text, the fingerprint and the Length of the digest / fingerprint
        System.out.println("Text        = " + md5);
        // Text        = The MD5 message-digest algorithm is a formerly widely used cryptographic hash function that produces a 128-bit (16-byte) hash value.
        // Specified in RFC 1321, MD5 has been utilized in a wide variety of security applications, and is also commonly used to check data integrity.
        // MD5 was designed by Ron Rivest in 1991 to replace an earlier hash function, MD4. An MD5 hash value is typically expressed as a hexadecimal number, 32 digits long.
        System.out.println("Fingerprint = " + fingerprint);            // Fingerprint = 09ad24fef35b06e6add520b5c6fff1d6
        System.out.println("Length      = " + fingerprint.length());    // Length      = 32
    }
}
```

용어

용어	설명
SHA	Secure Hash Algorithm, 안전한 해시 알고리즘
SHA-256	충돌 공격에 대해 128비트 보안을 제공하기 위한 256비트 해시 함수
SHA-384	SHA512 출력을 잘라서 얻을 수 있다.
SHA-512	256비트 보안을 제공하기 위한 512비트 해시 함수

Ref Site

Message Digest, FingerPrint - 윈디하나의 솔라나라

Class DigestUtils

Class MessageDigest

How do I calculate the MD5 digest of a string?

패스워드의 암호화와 저장 - Hash(해시)와 Salt(솔트)

RFC1321 - The MD5 Message_Digest Algorithm

Class Hashtable<K,V>

MD5 Hashing in Java

Guide to hashcode() in Java

Java equals()와 hashCode()에 대해

Guideto HashCode() in Java

Hashing Algorithm in Java

[자료구조]Hash의 개념 및 설명

[자료구조/알고리즘]해시(Hash)란?

[Java]Hash란 무엇인가?

Message Digest

MD5

MessageDigest Algorithms

오션,, md5