

数字信息摘要常见算法

编解码算法

1. Hex 编码

将二进制数据按16进制转换为字符串，1字节=2个字符，编码后体积为2倍。

2. Base64

由MIME规范定义的编码算法，其将3个字节(24位)编码为4个字符。

字符集包括64个，可表示6二进制位的数据，因此一个字符对应一组6bit的数据。

编码后体积约为4/3倍，针对不足位数用=补齐。

HASH 算法

通常也称散列算法，是一种将任意长度的消息变成固定长度的消息摘要算法，不可逆；

1 MD5

Message Digest Algorithm 5，流行度极高，但目前被发现存在碰撞冲突风险；

任意长度输出为128bit=16字节摘要

2 SHA1

SHA 指Security Hash Algorithm，由美国国家安全局NSA设计的安全散列算法系列；

SHA1 输出长度为160bit=20字节摘要

3 SHA256

继SHA1 出现的算法(属于SHA-2类)，安全性较SHA1更高；

SHA256 输出长度为256bit=32字节摘要。

公告



美码师，老码农一枚，喜欢聊聊代码，唠唠职场故事，爱技术也爱生活
欢迎关注我的公众号



昵称：美码师
 园龄：8年5个月
 粉丝：90
 关注：7
 +加关注

<		2019年6月						>
日	一	二	三	四	五	六		
26	27	28	29	30	31	1		
2	3	4	5	6	7	8		
9	10	11	12	13	14	15		
16	17	18	19	20	21	22		
23	24	25	26	27	28	29		

MAC 算法

Message Authentication Code，消息认证码算法，基于HASH算法之上，增加了密钥的支持以提高安全性。具体算法包括HmacMD5/HmacSHA1/HmacSHA256等，输入包括数据及密钥，输出长度与HASH算法一致。密钥可以是任意长度的数据。

代码样例

HEX 编解码



```
/**
 * Write a byte array as hexadecimal String.
 */
public static String byteToHexString(byte[] bytes) {
    return String.valueOf(Hex.encodeHex(bytes));
}

/**
 * Transform an hexadecimal String to a byte array.
 */
public static byte[] hexStringToByte(String hexString) {
    try {
        return Hex.decodeHex(hexString.toCharArray());
    } catch (DecoderException e) {
        throw new RuntimeException(e);
    }
}

// Hex 来自 common-codec 扩展包
// 字节编码片段
private static final char[] DIGITS_LOWER =
```

搜索

找找看

常用链接

我的随笔

我的评论

我的参与

最新评论

我的标签

随笔分类

0.JAVA技术(39)

1.架构设计(3)

2.安全技术(9)

3.前端技术(2)

4.测试技术(2)

5.数据库中间件(21)

7.工具技巧(9)

8.构建技术(5)

9.基础原理(2)

O.开放平台(3)

P.行业相关(1)

S.敏捷管理

Z.心得杂谈(9)

随笔档案

2019年5月 (2)

2019年4月 (4)

2019年3月 (7)

2019年2月 (2)

2018年12月 (2)

2018年11月 (6)

2018年9月 (3)

```

        {'0', '1', '2', '3', '4', '5', '6', '7', '8', '9', 'a', 'b', 'c', 'd', 'e',
        'f'};
    /**
     * @param data
     *      a byte[] to convert to Hex characters
     *
     * @return A char[] containing hexadecimal characters
     * @since 1.4
     */
    protected static char[] encodeHex(final byte[] data) {
        final int l = data.length;
        final char[] out = new char[l << 1];
        // two characters form the hex value.
        for (int i = 0, j = 0; i < l; i++) {
            out[j++] = DIGITS_LOWER [(0xF0 & data[i]) >>> 4];
            out[j++] = DIGITS_LOWER [0x0F & data[i]];
        }
        return out;
    }

```



Base64编解码

```

    /**
     * Encode a String to base64
     *
     * @param value
     *      The plain String

```



2018年8月 (4)
 2018年7月 (8)
 2018年6月 (2)
 2018年5月 (4)
 2018年3月 (3)
 2018年2月 (5)
 2017年10月 (1)
 2017年8月 (1)
 2017年6月 (1)
 2017年3月 (2)
 2017年2月 (1)
 2017年1月 (4)
 2016年12月 (5)
 2016年11月 (1)
 2016年10月 (4)
 2016年9月 (4)
 2016年8月 (1)
 2016年4月 (1)
 2015年12月 (1)
 2015年9月 (3)
 2015年8月 (1)
 2015年7月 (4)
 2015年6月 (1)
 2015年4月 (3)
 2015年3月 (3)
 2011年11月 (2)
 2011年10月 (2)
 2011年9月 (5)

links

[ascii 图表](#)
[ascii艺术字](#)

最新评论

1. Re:Java条形码生成技术-Barcode4j

```

    * @return The base64 encoded String
    */
    public static String encodeBASE64(String value) {
        try {
            return new String(Base64.encodeBase64(value.getBytes("utf-8")));
        } catch (UnsupportedEncodingException ex) {
            throw new RuntimeException(ex);
        }
    }
    /**
     * Decode a base64 value
     *
     * @param value
     *         The base64 encoded String
     * @return decoded binary data
     */
    public static byte[] decodeBASE64(String value) {
        try {
            return Base64.decodeBase64(value.getBytes("utf-8"));
        } catch (UnsupportedEncodingException ex) {
            throw new RuntimeException(ex);
        }
    }
}

```



MD5 实现(SHA1、SHA256类似)



怎么隐藏条形码下方的文本?或者设置为自定义文本?

--习惯沉淀

2. Re:成为高手前必懂的TCP干货

@
海向

--美码师

3. Re:成为高手前必懂的TCP干货

6

--海向

4. Re:redis通过pipeline提升吞吐量

@ericlfredis-stat , 可参考这里的: ...

--美码师

5. Re:redis通过pipeline提升吞吐量

楼主, 请教下性能测评是使用的什么工具? 3Q!

--ericlf

阅读排行榜

1. 使用 openssl 生成证书(62415)
2. mysql 索引过长1071-max key length is 767 byte(56645)
3. Java条形码生成技术-Barcode4j(36608)
4. MQTT服务器搭建-mosquitto1.4.4安装指南(26266)
5. 使用keytool 生成证书(18705)

评论排行榜

1. 情人节, 送女友一桶代码可否? (36)
2. 软能力那点事, 你知多少(18)
3. 老兵的十年职场之路(一)(9)
4. redis通过pipeline提升吞吐量(6)
5. MQTT服务器搭建-mosquitto1.4.4安装指南(6)

```

/**
 * Build an hexadecimal MD5 hash for a String
 *
 * @param value
 *         The String to hash
 * @return An hexadecimal Hash
 */
public static String hexMD5(String value) {
    try {
        MessageDigest messageDigest = MessageDigest.getInstance("MD5");
        messageDigest.reset();
        messageDigest.update(value.getBytes("utf-8"));
        byte[] digest = messageDigest.digest();
        return byteToHexString(digest);
    } catch (Exception ex) {
        throw new RuntimeException(ex);
    }
}

```



推荐排行榜

1. 软能力那点事，你知多少(17)
2. 情人节，送女友一桶代码可否？(15)
3. 老兵的十年职场之路(二)(9)
4. 回顾下自己都写了什么(9)
5. 老兵的十年职场之路(一)(8)

MAC 计算摘要



```

static {
    // add bouncycastle support for md4 etc..
    Security.addProvider(new BouncyCastleProvider());
}
/**
 * 初始化密钥


```

```

*
* @param type
* @return
*/
public static String initHmacKey(MacType type) {
    try {
        KeyGenerator generator = KeyGenerator.getInstance(type.name());
        SecretKey secretKey = generator.generateKey();
        byte[] key = secretKey.getEncoded();
        return Codec.byteToHexString(key);
    } catch (Exception e) {
        throw new RuntimeException(e);
    }
}

/**
* 计算HMAC摘要
*
* @param data
* @param key
* @param type
* @return
*/
public static String computeHmac(byte[] data, String key, MacType type) {
    try {
        byte[] keydata = Codec.hexStringToByte(key);
        SecretKey secretKey = new SecretKeySpec(keydata, type.name());
        Mac mac = Mac.getInstance(secretKey.getAlgorithm());
        mac.init(secretKey);
        byte[] digest = mac.doFinal(data);
        return Codec.byteToHexString(digest);
    } catch (Exception e) {
        throw new RuntimeException(e);
    }
}

```

```
}  
}  

```

bouncycastle 支持

maven 依赖

```
<dependency>  
  <groupId>org.bouncycastle</groupId>  
  <artifactId>bcprov-jdk15on</artifactId>  
  <version>1.54</version>  
</dependency>
```

<http://www.bouncycastle.org/>



作者: [zale](#)

出处: <http://www.cnblogs.com/littleatp/>, 如果喜欢我的文章, 请关注我的公众号

本文版权归作者和博客园共有, 欢迎转载, 但未经作者同意必须保留此段声明, 且在文章页面明显位置给出 [原文链接](#) 如有问题, 可留言咨询.

分类: [2.安全技术](#)

标签: [md5](#), [mac](#), [sha1](#), [sha256](#)

好文要顶

关注我

收藏该文





美码师

[关注 - 7](#)

[粉丝 - 90](#)

[+加关注](#)

0

推荐

0

反对

« 上一篇: [rabbitmq 重复ACK导致消息丢失](#)

» 下一篇: [对称加解密算法解析](#)

posted @ 2016-12-17 18:28 美码师 阅读(5767) 评论(0) 编辑 收藏

[刷新评论](#) [刷新页面](#) [返回顶部](#)



注册用户登录后才能发表评论，请 [登录](#) 或 [注册](#)，[访问网站首页](#)。

【推荐】超50万C++/C#源码：大型实时仿真组态图形源码

【前端】SpreadJS表格控件，可嵌入系统开发的在线Excel

【培训】从Java菜鸟到大牛的成长秘籍 6.18冰点价限时直降1500！

【推荐】程序员问答平台，解决您开发中遇到的技术难题

相关博文：

- 消息摘要算法-MAC算法系列
- java基础---->摘要算法的介绍
- 消息摘要算法-HMAC算法

- 消息摘要算法-HMAC算法
- java加密之消息摘要算法

最新新闻:

- 鱼在水中也憋气
 - 谷歌宣布即将淘汰32位版Android Studio与Android模拟器
 - Mozilla 正式为 Firefox 推出全新 logo
 - 天文学家称月球最大的陨石坑下方隐藏着神秘物质
 - 可循环利用食品包装透明薄膜问世
- » 更多新闻...



Copyright ©2019 美码师