

ios MD5加密



LYSNote (/u/ec0c8a889343) [+ 关注](#)

2016.10.18 13:16* 字数 721 阅读 2089 评论 9 喜欢 30 阅读 2089 评论 9 喜欢 30

(/u/ec0c8a889343)

MD5加密全称是Message Digest Algorithm 5，译为“消息摘要算法第5版”

MD5加密是最常用的加密方法之一，是从一段字符串中通过相应特征生成一段32位的数字字母混合码。对输入信息生成唯一的128位散列值（32个字符）

MD5生成的是固定的128bit，即128个0和1的二进制位，而在实际应用开发中，通常是以16进制输出的，所以正好就是32位的16进制，说白了也就是32个16进制的数字。

MD5主要特点是 不可逆，相同数据的MD5值肯定一样，不同数据的MD5值不一样（也不是绝对的，但基本是不能一样的）。

MD5算法还具有以下性质：

- 1、压缩性：任意长度的数据，算出的MD5值长度都是固定的。
- 2、容易计算：从原数据计算出MD5值很容易。
- 3、抗修改性：对原数据进行任何改动，哪怕只修改1个字节，所得到的MD5值都有很大区别。
- 4、弱抗碰撞：已知原数据和其MD5值，想找到一个具有相同MD5值的数据（即伪造数据）是非常困难的。
- 5、强抗碰撞：想找到两个不同的数据，使它们具有相同的MD5值，是非常困难的。
- 6、MD5加密是不可解密的，但是网上有一些解析MD5的，那个相当于一个大型的数据库，通过匹配MD5去找到原密码。所以，只要在要加密的字符串前面加上一些字母数字符号或者多次MD5加密，这样出来的结果一般是解析不出来的。

MD5的应用：

由于MD5加密算法具有较好的安全性，而且免费，因此该加密算法被广泛使用

大多数的登录功能向后台提交密码时都会使用到这种算法

注意点：

- (1) 一定要和后台开发人员约定好，MD5加密的位数是16位还是32位(大多数都是32位的)，16位的可以通过32位的转换得到。
- (2) MD5加密区分 大小写，使用时要和后台约定好。



MD5解密:

解密网站:<http://www.cmd5.com/> ([https://link.jianshu.com?](https://link.jianshu.com?t=http://www.cmd5.com/)

t=<http://www.cmd5.com/>)

为了让MD5码更加安全 涌现了很多其他方法 如加盐。盐要足够长足够乱 得到的MD5码就很难查到。

终端代码: `$ echo -n abc|openssl md5` 给字符串abc加密、

苹果包装了MD5加密的方法，使用起来十分的方便。

```
#import@interface MD5Encrypt : NSObject
// MD5加密
/*
*由于MD5加密是不可逆的,多用来进行验证
*/
// 32位小写
+(NSString *)MD5ForLower32Bate:(NSString *)str;
// 32位大写
+(NSString *)MD5ForUpper32Bate:(NSString *)str;
// 16为大写
+(NSString *)MD5ForUpper16Bate:(NSString *)str;
// 16位小写
+(NSString *)MD5ForLower16Bate:(NSString *)str;
@end
```

```
#import "MD5Encrypt.h"
#import <CommonCrypto/CommonDigest.h>

@implementation MD5Encrypt

#pragma mark - 32位 小写
+(NSString *)MD5ForLower32Bate:(NSString *)str{

    //要进行UTF8的转码
    const char* input = [str UTF8String];
    unsigned char result[CC_MD5_DIGEST_LENGTH];
    CC_MD5(input, (CC_LONG)strlen(input), result);

    NSMutableString *digest = [NSMutableString stringWithCapacity:CC_MD5_DIGEST_LENGTH * 2];
    for (NSInteger i = 0; i < CC_MD5_DIGEST_LENGTH; i++) {
        [digest appendFormat:@"%02x", result[i]];
    }

    return digest;
}

#pragma mark - 32位 大写
+(NSString *)MD5ForUpper32Bate:(NSString *)str{

    //要进行UTF8的转码
    const char* input = [str UTF8String];
    unsigned char result[CC_MD5_DIGEST_LENGTH];
    CC_MD5(input, (CC_LONG)strlen(input), result);

    NSMutableString *digest = [NSMutableString stringWithCapacity:CC_MD5_DIGEST_LENGTH * 2];
    for (NSInteger i = 0; i < CC_MD5_DIGEST_LENGTH; i++) {
        [digest appendFormat:@"%02X", result[i]];
    }

    return digest;
}

#pragma mark - 16位 大写
+(NSString *)MD5ForUpper16Bate:(NSString *)str{

    NSString *md5Str = [self MD5ForUpper32Bate:str];

    NSString *string;
    for (int i=0; i<24; i++) {
        string=[md5Str substringWithRange:NSMakeRange(8, 16)];
    }
    return string;
}

#pragma mark - 16位 小写
+(NSString *)MD5ForLower16Bate:(NSString *)str{


    NSString *md5Str = [self MD5ForLower32Bate:str];

    NSString *string;
    for (int i=0; i<24; i++) {
        string=[md5Str substringWithRange:NSMakeRange(8, 16)];
    }
    return string;
}

@end
```

小礼物走一走，来简书关注我

赞赏支持



LYSNote (/u/ec0c8a889343)

写了 13140 字，被 87 人关注，获得了 209 个喜欢

[\(/u/ec0c8a889343\)](#)写了 13140 字，被 87 人关注，获得了 209 个喜欢

+ 关注

“There are two ways of constructing a software design: One way is to make it so simple that there ar...

喜欢

30

更多分享

(http://cwb.assets.jianshu.io/notes/images/6399597



写下你的评论...

9条评论

只看作者

按喜欢排序 按时间正序 按时间倒序



llronMan (/u/8fed18ed70c9)
2楼 · 2016.10.18 20:25

(/u/8fed18ed70c9)
人们说的16位MD5加密，其实是这样的：举例如果产生的MD5加密字符串是：01234567abcdefababcdefab76543210，则16位的MD加密字符是abcdefababcdefab，也就是只是截取了中间的16位。实际上这个操作已经不是MD5加密算法所包括的，而应当是对MD5加密算法结果的二次处理。其它的64位和大小写什么的，都属于对MD5算法结果的二次处理。因为MD5算法产生的结果就是128bit，128个二进制数字

赞 回复

马爷 (/u/99ae8647de1c): @JoanKing (/users/8fed18ed70c9) 所有的 MD5加密出来的都是128个二进制数字吗？

2016.10.19 16:02 回复

添加新评论



llronMan (/u/8fed18ed70c9)
3楼 · 2016.10.18 20:26

(/u/8fed18ed70c9)
http://www.jianshu.com/p/89154c0c213c (http://www.jianshu.com/p/89154c0c213c)

赞 回复



llronMan (/u/8fed18ed70c9)
4楼 · 2016.10.18 20:26

(/u/8fed18ed70c9)
可以交流

赞 回复



z我要是唐僧就留在女儿国 (/u/ee8f8efe3fdf)
5楼 · 2016.10.19 14:57

(/u/ee8f8efe3fdf)
请教下这个加盐 盐是什么呢？

赞 回复

LYSNote (/u/ec0c8a889343): @z我要是唐僧就留在女儿国 (/users/ee8f8efe3fdf) http://blog.csdn.net/blade2001/article/details/6341078 (http://blog.csdn.net/blade2001/article/details/6341078)这里有说明,可以了解下

2016.10.19 15:06 回复

z我要是唐僧就留在女儿国 (/u/ee8f8efe3fdf): @LYSNote (/users/ec0c8a889343) 好的 谢谢

2016.10.19 15:06

回复

添加新评论



z我要是唐僧就留在女儿国 (/u/ee8f8efe3fdf)

6楼 · 2016.10.19 15:05

(/u/ee8f8efe3fdf)

n位随机数吗?

赞

回复

LYSNote (/u/ec0c8a889343): @z我要是唐僧就留在女儿国 (/users/ee8f8efe3fdf) 我理解的是随机数,具体看项目要求

2016.10.19 15:28

回复

添加新评论

被以下专题收入，发现更多相似内容

- + 收入我的专题
- 

iOS Dev... (/c/3233d1a249ca?utm_source=desktop&utm_medium=notes-included-collection)
- 

程序员 (/c/NEt52a?utm_source=desktop&utm_medium=notes-included-collection)
- 

今日看点 (/c/3sT4qY?utm_source=desktop&utm_medium=notes-included-collection)
- 

iOS 开发之路 (/c/266ebad14eb2?utm_source=desktop&utm_medium=notes-included-collection)
- 

iOS资料 (/c/52e990d16633?utm_source=desktop&utm_medium=notes-included-collection)
- 

iOS程序猿 (/c/527cd13a0f17?utm_source=desktop&utm_medium=notes-included-collection)
- 

iOS开发技巧 (/c/243d36ae862f?utm_source=desktop&utm_medium=notes-included-collection)

展开更多

推荐阅读更多精彩内容 > (/)

简书快速编写文章快捷符号(Markdown语法) (/p/28aebede4e4a?utm_...

为什么人家写的简书文章那么漂亮? 各种符号,各种排版 下面我就给大家分享一下,在编写简书文章时,常用的一些特殊符号,以及这些符号组合后的神奇效果 代码块 作为一名程序猿,代码块是在日常整理笔记时不可

LYSNote (/u/ec0c8a889343?utm_campaign=maleskine&utm_content=user&utm_medium=pc_all_hots&utm_source=recommendation)

iOS 3DTouch (/p/11c70052da8c?utm_campaign=m... (/p/11c70052da8c?utm_campaign=maleskine&utm_content=note&utm_...

一.什么是3DTouch? 效果图: 点击icon: Peek (预览) 和Pop (跳至预览的详细信息界面): 看完这个,大家估计都明白了, 就是长按icon图标或者项目里面长按某一

LYSNote (/u/ec0c8a889343?utm_campaign=maleskine&utm_content=user&utm_medium=pc_all_hots&utm_source=recommendation)

《无问西东》| 最好的年纪，最残酷的选择 (/p/9876fbbe4f46?utm_campaign=maleskine&utm_content=note&utm_medium=seo_notes&utm_source=recommendation)

他们的爱与风华， 只问自由；只问深情； 只问盛放；只问初心；只问敢勇。

无问西东。文 | 笙笙不兮 01 《无问西东》是感人的，更是震撼的。 少有电影

笙笙不兮 (/u/86efc6c2408d?utm_campaign=maleskine&utm_content=user&utm_medium=pc_all_hots&utm_source=recommendation)

这是我的大学室友 | 你抽烟喝酒纹身，但你是个好... (/p/f10bb28090c7?utm_campaign=maleskine&utm_content=note&utm_medium=seo_notes&utm_source=recommendation)

我是你眼中的乖乖女，你是我眼中的坏女孩。一场相遇，陪伴至今。 2018年1

月15日 星期一 烟味 ❤️ 你是我见过最好看的女孩子。 在现实生活中能把军训

七小葩 (/u/d90ef3476ae0?utm_campaign=maleskine&utm_content=user&utm_medium=pc_all_hots&utm_source=recommendation)

孤独是春药，一个人的高潮 (/p/47b0d5aa2753?utm_campaign=maleskine&utm_content=note&utm_medium=seo_notes&utm_source=recommendation)

文 | 时青言 01 我时常在想，孤独是什么？ 有人说，它是人们概念化的一种情

感。我又在想，那为什么会有这种情感？ 或许，是因为人的社会群体属性。

时青言 (/u/9787ddc08cad?utm_campaign=maleskine&utm_content=user&utm_medium=pc_all_hots&utm_source=recommendation)

iOS - MD5加密 (/p/34e7ebfd4804?utm_campaign=maleskine&utm_content=note&utm_medium=seo_notes&utm_source=recommendation)

MD5相关知识： 1.MD5:全称是Message Digest Algorithm 5，译为“消息摘要算法第5版”效果：对输入信息生成唯一的128位散列值（32个字符） 2.MD5的特点 （1） 输入两个不同的明文不会得到相同的输出值

🌻 SunshineAutumn (/u/c51fd472a4cd?utm_campaign=maleskine&utm_content=user&utm_medium=seo_notes&utm_source=recommendation)

面向对象的用电信息数据交换协议 (/p/94caedb70f65?utm_campaign=maleskine&utm_content=note&utm_medium=seo_notes&utm_source=recommendation)

国家电网公司企业标准（Q/GDW）- 面向对象的用电信息数据交换协议 - 报批稿：20170802 前言： 排版 by Dr_Ting公众号：庭说移步 tingtalk.me 获得更友好的阅读体验 Q/GDW XXXX-201X《面向对象的用电信

👤 庭说 (/u/a0d04c114c89?utm_campaign=maleskine&utm_content=user&utm_medium=seo_notes&utm_source=recommendation)

OpenSSL (/p/2e69d56e470b?utm_campaign=maleskine&utm_content=note&utm_medium=seo_notes&utm_source=recommendation)

原版：http://blog.csdn.net/jun2ran/article/details/6491375 第一章 前言第二章 证书第三章 加密算法第四章 协议第五章 入门第六章 指令 verify第七章 指令asn1parse第八章 指令CA（一）第九章 指令CA（二...

👤 依忆依意壹懿 (/u/c80bc26f12ed?utm_campaign=maleskine&utm_content=user&utm_medium=seo_notes&utm_source=recommendation)

12.MD5加密简单说明 (/p/1bb78ee92e43?utm_campaign=maleskine&utm_content=note&utm_medium=seo_notes&utm_source=recommendation)



只有注册的时候才是明文，在服务器还有数据库中都是密文，忘记密码即使黑了数据库也找不回来登录的时候也用同样的加密方式，数据库里比对的也是密文，服务器和数据库都是不知道明文的，也不需要知

👤 Honoring_God (/u/867731e25873?utm_campaign=maleskine&utm_content=user&utm_medium=seo_notes&utm_source=recommendation)

iOS MD5加密 (/p/8898b0bb3c94?utm_campaign=maleskine&utm_content=note&utm_medium=seo_notes&utm_source=recommendation)

简介 MD5（单向散列算法）的全称是Message-Digest Algorithm 5（信息-摘要算法）,经过MD5处理后看不到原文，是一种加密算法。 MD5的特点 输入两个不同的明文不会得到相同的输出值根据输出值，不能得

 梦亦趣 (/u/2e2dd05a6825?utm_campaign=maleskine&utm_content=user&utm_medium=seo_notes&utm_source=recommendation)

我愿意为了你去变得更好 (/p/fe2bd911ee33?utm_campaign=maleskin...

其实我很看不惯，为了孩子我怎么样怎么样，我也不喜欢牺牲型的父母，也不打算做这样苦逼的父母，不是我不爱孩子，正是因为我爱他才愿意让他放手去成长。孩子，自从离开母体那一刻就是一个独立的个

 海豚的微笑 (/u/4b99b1f2da3c?utm_campaign=maleskine&utm_content=user&utm_medium=seo_notes&utm_source=recommendation)

(/p/92df34d4fd1f?



utm_campaign=maleskine&utm_content=note&utm_medium=seo_notes&utm_source=recommendation)

至情至性 | 章子怡 (/p/92df34d4fd1f?utm_campaign=maleskine&utm_...

我是在章子怡提起哥哥和梅姑的时候掉下眼泪来的。提到张国荣名字的时候，她哽咽的不像样子。那一刻的动容是她，也是我，是我们。最近几周《演员的诞生》不断地将章子怡推到舆论最前沿，各种地方都能

 宋二菇凉 (/u/86b3f6ea11b4?utm_campaign=maleskine&utm_content=user&utm_medium=seo_notes&utm_source=recommendation)

数字证书相关知识和技术点 (/p/cbf300f92b0f?utm_campaign=malesk...

最近项目中要用到很多第三方证书来进行数字签名,所以有必要把相关知识理清一下 1. 数字证书 数字证书就是互联网通讯中标志通讯各方身份信息的一串数字，提供了一种在Internet上验证通信实体身份的方式。

 YannChee (/u/99259071ab6e?utm_campaign=maleskine&utm_content=user&utm_medium=seo_notes&utm_source=recommendation)

沟通不畅时，你的大脑在做什么？ (/p/e81dac240634?utm_campaign...

最近遇到一个有意思的事情，欣儿和她男朋友都很爱对方，但老是沟通不顺畅，她对此有些疑惑？和男朋友沟通时，到底发生了什么？最近沟通不畅又出现了，最近2个月，欣儿从一家甲方咨询公司职业转换到

 秀丽001 (/u/7b0008dc1be7?utm_campaign=maleskine&utm_content=user&utm_medium=seo_notes&utm_source=recommendation)

Go on (/p/ed2ba01799f5?utm_campaign=maleskine&utm_content=no...

本来是个挺惫懒的一个人，喜欢无事发呆，内心戏狂多，却懒于表露行动，每天有很多想法感悟，可总不愿提笔纪录。好了，终于有了粉丝，还是不要留空给对方才好，那我继续吧.....

 小铃铛的麦田 (/u/330bfb3033b7?utm_campaign=maleskine&utm_content=user&utm_medium=seo_notes&utm_source=recommendation)