



ーキ、一二甲

Qing



博客等级: 18

博客积分: 78篇

博客访问: 407,859

关注人气: **378**

获赠金笔: **12**

赠出金笔: 0

荣誉徽章: 🔞







相关博文

更多〉〉

推荐博文

- ■2550mAh电
- ■日本雾霾之战: 民众与政府的博弈
- ■南非猎豹冒死捕杀豪猪被扎满嘴刺
- ■别光顾着把枪口对准柴静
- 马来西亚男子与眼镜王蛇接吻(图
- 【早评】降息利好将会在后市中逐
- ■哪些人能从柴静的"穹顶之下"赚
- "深圳机场撞人事件"不是一个人
- ■政采剔除国外品牌: 早该说不了!
- ■【DIY】做一枚宫灯迎元宵





青蛙冒险坐鳄鱼 广西北海银滩美 鼻子 景

Qt之加密算法 ☑ (2013-11-07 13:40:42) [编辑][删除]

+ 转 载 ▼

标签: qt qcryptographichash md5 sha md5加密 分类: Qt

在写这篇文章之前,我曾反复思量关于加密的叫法是否准确,更为严格来说,应该是密码散列-将数据(如中英文字母、特殊字符)通过复杂的算法转换为另一种固定长度的值。

QCryptographicHash类

在Qt中,QCryptographicHash类提供了生成密码散列的方法。该类可以用于生成二进制或文本数据的加密散列值。目前支持MD4、MD5、SHA-1、SHA-224、SHA-256、SHA-384和SHA-512。 这个类在QtCore4.3中被引入。

公共类型

• enum Algorithm { Md4, Md5, Sha1, Sha224, ..., Sha3_512 }

公共方法

- QCryptographicHash(Algorithm method)
- ~QCryptographicHash()
- void addData(const char * data, int length)
- bool addData(QIODevice * device)
- void addData(const QByteArray & data)
- void reset()
- QByteArray result() const

静态公有成员

• QByteArray hash(const QByteArray & data, Algorithm method)

成员类型文档

• enum QCryptographicHash::Algorithm

Chair Golyprodiaphionadh. Migolyman		
常量	取值	描述
QCryptographicHash::Md4	0	生成一个MD4散列
QCryptographicHash::Md5	1	生成一个MD5散列
QCryptographicHash::Sha1	2	生成一个SHA-1散列
QCryptographicHash::Sha224	3	生成一个SHA-224散列(SHA-2)。在Qt5.0介绍
QCryptographicHash::Sha256	4	生成一个SHA-256散列(SHA-2)。在Qt5.0介绍
QCryptographicHash::Sha384	5	生成一个SHA-384散列(SHA-2)。在Qt5.0介绍
QCryptographicHash::Sha512	6	生成一个SHA-512散列(SHA-2)。在Qt5.0介绍
QCryptographicHash::Sha3_224	7	生成一个SHA3-224散列。在Qt5.1介绍
QCryptographicHash::Sha3_256	8	生成一个SHA3-256散列。在Qt5.1介绍
QCryptographicHash::Sha3_384	9	生成一个SHA3-384散列。在Qt5.1介绍
QCryptographicHash::Sha3_512	10	生成一个SHA3-512散列。在Qt5.1介绍

成员函数文档

• QCryptographicHash::QCryptographicHash(Algorithm method) 构造一个可以把数据创建为加密哈希值的对象。

Qt之加密算法_一去、二三里_新浪博客





萨尔瓦多城铁笼 监狱

笼 狮子金沙禁猎[旅馆





潜水员勇喂巨型 双髻鲨

🤦 杯具的飞蛾

俄罗斯山中隐士 生活

查看更多>>

2月3日

谁看过这篇博文 3月2日 ₾ 惘然 abclla 3月2日 ₫ 香草天空17 2月27日 625747 2月13日 2月11日 1aozhang Geeprox 2月9日 🤦 用户31991… 2月9日 2 Y8pj4E5pJn 2月9日 ₫ 用户21017… 2月5日 2月5日 🙎 lynnhua 2月4日

- QCryptographicHash::~QCryptographicHash() 销毁对象。
- void QCryptographicHash::addData(const char * data, int length)

将第一长度字符数据的加密哈希。

• bool QCryptographicHash::addData(QIODevice * device)

从开放的输入输出设备读取数据,直到结束并哈希它。如果成功读取,则返回true。

QtCore5.0中引入此功能。

• void QCryptographicHash::addData(const QByteArray & data)

这个函数的重载addData()。

- QByteArray QCryptographicHash::hash(const QByteArray & data, Algorithm method) [static] 使用此方法返回哈希数据。
- void QCryptographicHash::reset()

重置对象。

• QByteArray QCryptographicHash::result() const

返回最后的哈希值。

举例(对文本为"password"的字符串加密):

(1) 通过静态hase()方法计算

QByteArray byte_array;

byte_array.append("password");

QByteArray hash_byte_array = QCryptographicHash::hash(byte_array, QCryptographicHash::Md5);

QString md5 = hash_byte_array.toHex();

(2) 通过result()方法计算

QByteArray byte array;

byte_array.append("password");

QCryptographicHash hash(QCryptographicHash::Md5);

hash. addData(byte_array); //添加数据到加密哈希值

QByteArray result_byte_array = hash.result(); //返回最终的哈希值

QString md5 = result_byte_array.toHex();

md5结果: 5f4dcc3b5aa765d61d8327deb882cf99,可以去找相应的工具进行验证!

推荐一个网址: http://www.md5.com.cn/。

效果如下:

MD5 Result

Md5: 5f4dcc3b5aa765d61d8327deb882cf99

Result: password

如上所示,无论使用穷举法还是其他手段来破解,都足以说明没有绝对的安全。因为理论上通过逐个查找匹配,是可以破解任何一种密文的,问题只在于如何缩短时间而已。

MD5与SHA-1比较

- 二者均由MD4导出,所以SHA-1和MD5很相似。他们的强度和其它特性也很相似,但还有以下几点不同:
- (1)对强性攻击的安全性:最显著和最重要的区别是SHA-1摘要比MD5要长32位。使用强行技术,产生任何一个报文使其摘要等于给定报文摘要的难度对MD5为2¹²⁸数量级操作,而对SHA-1则是2¹⁶⁰数量级操作。这样,SHA-1对强攻击有更大的优势。
- (2) 对密码分析的安全性:由于MD5的设计,易受密码分析的攻击,相比之下,SHA-1则不然。
- (3) 速度: 相同硬件上, SHA-1运行速度比MD5慢。

碰撞:由于HASH函数产生定长的密文,结果是有限集合。而待处理的明文可以是计算机网络传输的任何信息。也就是说,明文信息是一个无限集合,密文信息却有限,两集合之间无一一对应关系。总有多个不同明文产生相同密文的情况发生,这就是所谓的碰撞。

MD5与SHA-1曾被认为是足够安全的HASH算法,早在1994就有报告称,运算能力最强的机器,平均24天就可能找到一个MD5碰撞。王小云教授的方法已经为短时间内找到MD5与SHA-1碰撞成为可能。虽然如此,也并不意味着两种方法就此失效,再者,也可以通过自己的手段来进一步处理。比如:通过MD5与SHA结合实现。将A进行MD5处理得到B,将A在进行SHA处理得到C,再将B与C结合(比如:相加),也可把结合后的结果再进行MD5加密。这足以将碰撞机滤降至很小很小,所以没有绝对的安全,只有更安全。

注:

技术在于交流、沟通,转载请注明出处并保持作品的完整性。

作者: └☆奋斗ing♥孩子` 原文: http://blog. sina. com. cn/s/blog_a6fb6cc90101ge8c. html.

1 古 ホ

分享: 🚳 微米 🖸 🖂 🥱 🕞 🙏 🙀 豆 🛨

阅读(2414) | 评论(4) | 收藏(0) | 已有4人转载▼ | 喜欢▼ | 打印

已投稿到: 🚧 排行榜

前一篇: QML之ColorDialog 后一篇: QML之FileDialog

评论 重要提示:警惕虚假中奖信息

[发评论]

行潇

不知道楼主,有没有将Qt程序弄成有注册码之类的经验呢

2014-9-5 09:59

回复(1)

好望角

正好在接触这块,可是如何从生成的密码散列中恢复出原来的数据呢?

2014-12-30 16:06

回复(1)

发评论

一去、二三里:



🔲 💣 分享到微博 🖼

■匿名评论

验证码: 请点击后输入验证码 收听验证码

发评论

以上网友发言只代表其个人观点,不代表新浪网的观点或立场。

〈前一篇

后一篇 >

QML之ColorDialog

QML之FileDialog

新浪BLOG意见反馈留言板 不良信息反馈 电话: 4006900000 提示音后按1键(按当地市话标准计费) 欢迎批评指正 新浪简介 | About Sina | 广告服务 | 联系我们 | 招聘信息 | 网站律师 | SINA English | 会员注册 | 产品答疑

> Copyright © 1996 - 2014 SINA Corporation, All Rights Reserved 新浪公司 版权所有