Atitti 摘要算法签名算法校验算法 散列算法SHA1 和 MD5  crc32

目录

[1.1. CRC(Cyclic Redundancy Check,循环冗余校验)算法出现时间较长 1](#_Toc24139)

[1.1.1. 数据摘要算法的测试效率(SHA、MD5和CRC32) - xiaofei08...\_CSDN博客 1](#_Toc5098)

[1.2. MD5消息摘要算法（英语：MD5 Message-Digest Algorithm） 2](#_Toc7685)

[1.3. SHA1安全哈希算法（Secure Hash Algorithm）主要适用于数字签名 2](#_Toc19583)

# 签名算法历史演进 过去 现在 未来

CRC32

MD5

SHA1

LOREM

LOREM

LOREM

## CRC(Cyclic Redundancy Check,循环冗余校验)算法出现时间较长

### [数据摘要算法的测试效率(SHA、MD5和CRC32) - xiaofei08...\_CSDN博客](http://www.baidu.com/link?url=sxpUBYG5-oRabnNrBOI7aS6bQecQgqVi9i8WeA60ybq5NkHpyTWISd1yHJZ5EcePtqBJ-sEgouSHa_xXJBcT3skOzYyXtCS5hpPak9haEb_" \t "https://www.baidu.com/_blank)

2016年9月27日 - CRC算法的优点在于简便、速度快,严格的来说,CRC更应该被称为数据校验算法,但其功能与数据摘要算法类似,因此也作为测试的可选算法。 在W

美国[数据加密标准](https://www.baidu.com/s?wd=%E6%95%B0%E6%8D%AE%E5%8A%A0%E5%AF%86%E6%A0%87%E5%87%86&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao" \t "https://zhidao.baidu.com/question/_blank)（DES）是对称密码算法，就是加密密钥能够从解密密钥中推算出来，反过来也成立。密钥较短，加密处理简单，加解密速度快，适用于加密大量数据的场合。  
RSA是非对称算法，加密密钥和解密密钥是不一样的，或者说不能由其中一个密钥推导出另一个密钥。密钥尺寸大，加解密速度慢，一般用来加密少量数据，比如DES的密钥

## MD5消息摘要算法（英语：MD5 Message-Digest Algorithm）

SHA1 和 MD5 是散列算法，将任意大小的数据映射到一个较小的、固定长度的唯一值。加密性强的散列一定是不可逆的，这就意味着通过散列结果，无法推出任何部分的原始信息。任何输入信息的变化，哪怕仅一位，都将导致散列结果的明显变化，这称之为雪崩效应。散列还应该是防冲突的，即找不出具有相同散列结果的两条信息。具有这些特性的散列结果就可以用于验证信息是否被修改。MD5 比 SHA1 大约快 33%。

## SHA1安全哈希算法（Secure Hash Algorithm）主要适用于数字签名

安全[哈希算法](https://baike.baidu.com/item/%E5%93%88%E5%B8%8C%E7%AE%97%E6%B3%95" \t "https://baike.baidu.com/item/SHA1/_blank)（Secure Hash Algorithm）主要适用于[数字签名](https://baike.baidu.com/item/%E6%95%B0%E5%AD%97%E7%AD%BE%E5%90%8D" \t "https://baike.baidu.com/item/SHA1/_blank)标准 （Digital Signature Standard DSS）里面定义的数字签名算法（Digital Signature Algorithm DSA）。对于长度小于2^64位的消息，SHA1会产生一个160位的[消息摘要](https://baike.baidu.com/item/%E6%B6%88%E6%81%AF%E6%91%98%E8%A6%81/4547744" \t "https://baike.baidu.com/item/SHA1/_blank)。当接收到消息的时候，这个消息摘要可以用来验证数据的完整性。在传输的过程中，数据很可能会发生变化，那么这时候就会产生不同的消息摘要。 SHA1有如下特性：不可以从消息摘要中复原信息；两个不同的消息不会产生同样的消息摘要,(但会有1x10 ^ 48分之一的机率出现相同的消息摘要,一般使用时忽略)。

SHA1在许多安全协议中广为使用，包括TLS和SSL、PGP、SSH、S/MIME和IPsec，曾被视为是[MD5](https://baike.baidu.com/item/MD5" \t "https://baike.baidu.com/item/SHA1/_blank)（更早之前被广为使用的散列函数）的后继者。