Hash （哈希或散列）算法是信息技术领域非常基础也非常重要的技术。它能任意长度的二进 制值（明文）映射为较短的固定长度的二进制值（Hash 值），并且不同的明文很难映射为相 同的 Hash 值。

一、MD5哈希加密算法

- MD5即Message-Digest Algorithm 5（信息-摘要算法 5），用于确保信息传输完整一致。是计算机广泛使用的散列算法之一（又译摘要算法、哈希算法），主流编程语言普遍已有MD5实现。 将数据（如汉字）运算为另一固定长度值，是散列算法的基础原理，MD5的前身有MD2、MD3和MD4。
- MD5一度被广泛应用于安全领域。但是由于MD5的弱点被不断发现以及计算机能力不断的提升，现在已经可以构造两个具有相同MD5的信息，使本算法不再适合当前的安全环境。目前，MD5计算广泛应用于错误检查。例如在一些BitTorrent下载中，软件通过计算MD5和检验下载到的碎片的完整性。
- MD5是输入不定长度信息，输出固定长度128-bits的算法。经过程序流程，生成四个32位数据，最后联合起来成为一个128-bits散列。基本方式为，求余、取余、调整长度、与链接变量进行循环运算。得出结果。
- 已被证明安全性不足应用于商业场景。

二、SHA-1哈希加密算法

- SHA-1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（更早之前被广为使用的散列函数）的后继者。
- SHA安全性优于MD5。
- SHA-1的安全性如今被密码学家严重质疑。

例如：

明文：ambrisno1

SHA-1加密结果：bdbaab32dd08fbfb6141ca9dc68b70feb286b4aa （40位）

三、SHA-2哈希加密算法

- SHA-224、SHA-256、SHA-384，和SHA-512并称为SHA-2。（至少使用 SHA2-256 算法）
- 新的散列函数并没有接受像SHA-1一样的公众密码社区做详细的检验，所以它们的密码安全性还不被大家广泛的信任。
- 虽然至今尚未出现对SHA-2有效的攻击，它的算法跟SHA-1基本上仍然相似；因此有些人开始发展其他替代的散列算法。

例如：

明文：ambrisno1

SHA-224加密结果：3979b3617fb99bca3d2d64dc00ec1ee26fb000c76ce5f716c0e843b8 （56位16进制符）

SHA-256加密结果：3a72f66ac2d89a7798c916c0e069a7a853d1d05e3208d7b75d2c38ac50679c9f （64位16进制符）

SHA-384加密结果：
7b898f7c9ced4f7c6d087b8b8ee482bada4e781ae39946de4b2832395426cd640223b7f4e09488c6a628fef97673fe59 （96位16进制）

SHA-512加密结果：
abbfdfa91432a0fc2babf7768d1e98cbf4b072753683c4c016b7eaa3ce2132e37e7bb0222fd092cc3519cc66a071c55b5c
9a84acea5afaeb0 409abed5dad7be7 （128位16进制符）

四、SHA-3哈希加密算法

- SHA-3，之前名为Keccak算法，是一个加密杂凑算法。
- SHA-3并不是要取代SHA-2，因为SHA-2目前并没有出现明显的弱点。
- 由于对MD5出现成功的破解，以及对SHA-0和SHA-1出现理论上破解的方法，NIST感觉需要一个与之前算法不同的，可替换的加密杂凑算法，也就是现在的SHA-3。

输出长度 可为： 512、384、256、225、64

五、RIPEMD-160哈希加密算法

- RIPEMD-160 是一个 160 位加密哈希函数。
- 它旨在用于替代 128 位哈希函数 MD4、MD5 和 RIPEMD。
- RIPEMD 是在 EU 项目 RIPE（RACE Integrity Primitives Evaluation，1988-1992）的框架中开发的。
- 算法共有4个标准128、160、256和320。
- 在128位和160位的基础上，修改了初始参数和s-box来达到输出为256和320位的目的。所以，256位的强度和128相当，而320位的强度和160位相当。