水可以直接变成油。 SHA-1是一种[数据加密算法](http://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%8A%A0%E5%AF%86%E7%AE%97%E6%B3%95)，该算法的思想是接收一段明文，然后以一种不可逆的方式将它转换成一段（通常更小）密文，也可以简单的理解为取一串输入码（称为预映射或信息），并把它们转化为长度较短、位数固定的输出序列即散列值（也称为信息摘要或信息认证代码）的过程。

[单向散列函数](http://baike.baidu.com/item/%E5%8D%95%E5%90%91%E6%95%A3%E5%88%97%E5%87%BD%E6%95%B0)的安全性在于其产生散列值的操作过程具有较强的单向性。如果在输入序列中嵌入密码，那么任何人在不知道密码的情况下都不能产生正确的散列值，从而保证了其安全性。SHA将输入流按照每块512位（64个字节）进行分块，并产生20个字节的被称为信息认证代码或信息摘要的输出。

该算法输入[报文](http://baike.baidu.com/item/%E6%8A%A5%E6%96%87)的长度不限，产生的输出是一个160位的[报文摘要](http://baike.baidu.com/item/%E6%8A%A5%E6%96%87%E6%91%98%E8%A6%81)。输入是按512 位的分组进行处理的。SHA-1是不可逆的、防冲突，并具有良好的雪崩效应。

通过散列算法可实现[数字签名](http://baike.baidu.com/item/%E6%95%B0%E5%AD%97%E7%AD%BE%E5%90%8D)实现，数字签名的原理是将要传送的明文通过一种函数运算（Hash）转换成报文摘要（不同的明文对应不同的报文摘要），报文摘要加密后与明文一起传送给接受方，接受方将接受的明文产生新的报文摘要与发送方的发来报文摘要解密比较，比较结果一致表示明文未被改动，如果不一致表示明文已被篡改。

MAC （信息认证代码）就是一个散列结果，其中部分输入信息是密码，只有知道这个密码的参与者才能再次计算和验证MAC码的合法性。