**单向加密破解**

**1、暴力破解**

**2、字典发**

**3、哈希链（有长度）——彩虹表前身**

**确定hash链——进行R函数、或者进行0到多次H函数+R函数，判断结果是否在hash链结束集合中**

**确定hash链之后，从hash链头进行计算，如果hash值与给定hash值相等，找到明文**

**R函数——重复hash链问题——解密明文的数量远小于2k**

**4、rainbow tables——每一步使用不同的R函数（R1,R2,R3……Rk）。他解决了重复链的问题，**

**为什么加盐哈希可以抵御彩虹表**

彩虹表在生成的过程中，针对的是特定的函数H，H如果发生了改变，则已有的彩虹表数据就完全无法使用。  
如果每个用户都用一个不同的盐值，那么每个用户的H函数都不同，则必须要为每个用户都生成一个不同的彩虹表。大大提高了破解难度。

作者：风再起时ME  
链接：https://www.jianshu.com/p/732d9d960411  
来源：简书  
著作权归作者所有。商业转载请联系作者获得授权，非商业转载请注明出处。