## 加密与解密

密码存储几种方式

明文;

不靠谱.

明文的hash值;

彩虹表

明文 + 盐 的hash值;

相对安全

加密算法

更适合。密钥存储。

### 彩虹表

基于字典法: 存储所有明文对应的密文空间复杂度太高.

#### 预计算的哈希链

时间换空间。





H函数就是要破解的哈希函数。

R是规约函数，值域和H函数相反。

R函数举例：假设明文为5位数字，则R函数是取哈希值中前5个数字



时间复杂度: 每个明文最多K次，比暴力破解节约时间。

空间复杂度: 只保存起点、终点，约暴力破解的 1/K。

**问题**

碰撞出现链重叠。

发生在不同位置，则终点不同，很难发现。实际的明文数小于理论上明文数 \* 2。

发生在相同位置，终点相同，容易发现；



#### 彩虹表

解决链重叠问题.



每步的R函数不同。



碰撞时，只要不在同一位置，相同的只有一处，浪费一处的空间。



K 越大，彩虹表所占用空间越少，但花费时间越多。

**加盐作用**

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。

如果所有用户使用的盐值相同，通过彩虹表后，可能得到的是： P1 + S, P2+S, P3+S, 可能猜出盐值。而且，使用同一条hash链就可以了，不需要重复计算。