

算法说明：

首先根据密码学学习的知识知道生日攻击是基于生日悖论的，生日悖论是指，如果一个房间里有 23 个或 23 个以上的人，那么至少有两个人的生日相同的概率要大于 50%。

由此我们可以将它用在碰撞，得到不同 M 有着相同标志。

在这里我们可以假设：取样次数为 N，M: M1-Mn，取值在标志：1-B 中，并且假设分布随机均匀相互独立。取样次数 n 与 B 的关系， $n=1.2*B^{0.5}$ （这是生日悖论中最坏的情况。）证明一下大致应该是这样：M2 不等于 M1 的概率为 $(B-1)/B$ ，同理可得 M3 为 $(B-2)/B$ ，M4 为 $(B-3)/B$...Mn 为 $(B-n+1)/B$ 。因此，其中有碰撞的概率为： $1-(1-1/B)(1-2/B).....(1-(k-1)/B) \geq (1-e)^{-(n^2/2B)}$ 因为 $n=1.2*B^{0.5}$ ，因此 $(1-e)^{-(n^2/2B)}=1-e^{-0.72}=0.53>50\%$ 结论，因此使用生日攻击，我们只需 $2^{(n/2)}$ 次寻找，就有 50% 概率能找到相同标志的两个不同 M。

简述的步骤如下：

1. 随机在 $2^{(n/2)}$ 信息空间中寻找一个 M。
2. 求出相应的 tag 。
3. 寻找是否有碰撞，没有则返回步骤 1。

运行指导：

需要使用 openssl 库的算法，所以需要提前下载安装并配置环境。

运行结果：

（仅展示部分）

```
Microsoft Visual Studio 调试控制台
找到一个16bit前缀碰撞, 共穷搜0次
原始数据: 0
哈希长度: 256
哈希值: 0x2
找到一个16bit前缀碰撞, 共穷搜1次
原始数据: 4
哈希长度: 256
哈希值: 0x8
找到一个16bit前缀碰撞, 共穷搜2次
原始数据: 6
哈希长度: 256
哈希值: 0x12
找到一个16bit前缀碰撞, 共穷搜3次
原始数据: 6
哈希长度: 256
哈希值: 0x14
找到一个16bit前缀碰撞, 共穷搜4次
原始数据: 4
哈希长度: 256
哈希值: 0x14
找到一个16bit前缀碰撞, 共穷搜5次
原始数据: 0
哈希长度: 256
哈希值: 0x12
```