生日攻击原理：

由此我们可以将它用在碰撞，得到不同 Message 有着相同 tag。
假设：取样次数为 N，M：M1-Mn，取值在 tag：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：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）>= (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 tag 的两个不同 Message。

步骤：

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