# SM3 birthday attack

**生日攻击：**

生日问题：一个班60个同学，其中至少两个同学生日相同的概率大于99%；并且只要 23 个同学就能使得概率接近 50%。生日攻击是暴力穷举的一种，它能对任何类型的散列函数进行攻击。

若对于一个散列函数$f$ 其散列长度为$2^n$，我们要对其进行碰撞攻击，也就是找到一组$x_1, x_2$，使得$f(x_1) = f(x_2)$，最暴力的方法就是分别枚举$x_1, x_2$，复杂度是$2^{2n}$.

如果利用生日攻击的理论，只需要枚举出$\sqrt{2^n}$个$x$，就有的概率获得一组碰撞，从而复杂度大大降低。

**碰撞过程：**

```
def attack(num,length = 6):
    hashmap={}
    alphatable = "abcdefghijklmnopqrstuvwxyz"
    i = 0
    for s in itertools.permutations(alphatable,length):
        i+=1
        strs=""
        for k in range(length):
            strs+=s[k]
        data = bytes(strs, encoding='utf-8')
        #切片大小界定碰撞长度
        sign = sm3.sm3_hash(func.bytes_to_list(data))[:7]
        if sign in hashmap:
          print("success")
          return (hashmap[sign],strs)
        else:
            hashmap[sign]=strs
        if i>=num:
            break
    print("fail")
    return (0, 0)
```

**运行结果：**

```
>>>
============= RESTART: C:\Users\dell\Desktop\sm3_birthday_attack.py ============
success
('fdazfoid','fdazpvnm')
>>>
```